A CHARACTERIZATION OF SOME METACYCLIC GROUPS

EUGENE SCHENKMAN

Szasz [1] has recently shown that a group is cyclic if and only if it satisfies condition (A) below.

(A) Every cyclic subgroup of the group is for some positive integer \( k \) the subgroup generated by the \( k \)th powers of the elements of the group.

We shall extend this idea here to show that a metacyclic group whose commutator subgroup has order relatively prime to its index is characterized as a solvable group satisfying condition (B) below.

(B) Every member of a composition series (i.e. every subinvariant subgroup) is for some positive integer \( k \) the subgroup generated by the \( k \)th powers of the elements of the group. (If \( G \) denotes the group, the subgroup will be denoted by \( G(k) \)).

If the hypothesis of solvability is not included it is easy to check that many completely reducible groups and their extensions, (including, for example, all simple groups and all symmetric groups) satisfy condition (B). We were unable to characterize these.

We first list some of the properties of a group satisfying condition (B).

(1) Every subinvariant subgroup is a fully invariant subgroup of \( G \); that is, it is mapped into itself by all endomorphisms of \( G \).

For this is true for all \( G(k) \).

(2) Every homomorphic image of a group satisfying (B) itself also satisfies (B).

For the generators of corresponding normal subgroups are \( k \)th
powers for the same \( k \) both for the group and for its homomorphic image.

(3) A group \( G \) satisfying (B) also satisfies the ascending chain condition for subinvariant subgroups.

For if \( A = G(m) \) is subinvariant in \( G \) and if \( G(k) \) is arbitrary, then since \( k = qm + r \) with \( 0 \leq r < m \) we have \( \text{mod } G(m)^k = g^r \) and again \( \text{mod } G(m)^r = G(k) \); whence it follows that there can be at most \( m \) different subinvariant groups \( G(r) \) containing \( A \).

(4) Each factor of the derived series of a group satisfying (B) is finitely generated.

For if \( G^{(n)} \) is the \( n \)th member of the derived series of \( G \) then the factor group \( G/G^{(n)} \) satisfies (B) by (2), and hence the \((n-1)\)st derived subgroup of this factor is Abelian; it follows that every subgroup of it is subinvariant, consequently by (3) it satisfies the ascending chain condition and hence is finitely generated.

Now if \( G \) is a solvable group satisfying (B), then by (2) \( G \), modulo its derived group \( G' \), satisfies (B) and hence (A) and consequently by Szasz's result, \( G/G' \) is cyclic.

Next we observe that by (4) \( G' \) modulo \( G'' \) is finitely generated. If it is not cyclic we leave it to the reader to convince himself that \( G'/G'' \) has a normal subgroup \( N/G'' \) so that the factor \( (G'/G'')/(N/G'') \) is for some prime \( p \) of order \( p^2 \) and of type \((p, p)\).

By factoring out \( N \) in view of (2) we may assume that our group \( G \) is such that \( G/G' \) is cyclic and \( G' \) is Abelian of type \((p, p)\). We proceed as follows to show that this is not possible.

Let \( G' \) be the direct product of 2 cyclic groups of order \( p \); i.e. \( G' = (a) \times (b) \). And let \( h \) be an element of \( G \) which with \( G' \) generates \( G \). Then by (1) \( hah^{-1} = a^r \) for some integer \( r \) and by (1) \( hbh^{-1} = b^s \) for some integer \( s \). It follows that \( hah^{-1} = a^r b^s \). But by (1) \( hah^{-1} = (ab)^t = a^r b^t \) for some integer \( t \). Hence \( r = s = t \).

Now it is easy to verify (since \( h \) acts like a scalar matrix operating in \( G' \) that the group \( G \) admits the automorphism \( j \) which leaves \( h \) fixed and interchanges \( a \) and \( b \). But then (a) and (b) are not fully invariant contradicting \( D \). We conclude that \( G'/G'' \) is cyclic.

We next show that \( G'' \) consists of the identity element alone. For if \( G'' \) were nontrivial then since \( G'/G'' \) is finitely generated it is possible to find a normal subgroup \( M \) such that \( G'' \) is cyclic over \( M \). But the existence of such a \( G/M \) would contradict Theorem 9, p. 144 of [2] which states essentially that there are no "3-step metacyclic" groups. Hence \( G \) is metacyclic.

Finally we must show that if \( G \) is not cyclic \( G' \) has order prime to its index. Let us suppose to the contrary that some prime \( p \) divides
both the order and the index of \( G' \). We assume here that \( p \) divides infinity; but also note that if \( G/G' \) has infinite order then by (3) \( G' \) consists only of the identity. In view of (2) by factoring out the appropriate normal subgroup we may assume that \( G' \) is cyclic of order \( p \). Since \( G \) is not cyclic it must be a split extension of \( G' \) by a cyclic subgroup of order \( p^\mu g \), where \( p^\mu \neq 1 \) by assumption and where \( g \) is prime to \( p \). It follows that \( G \) can be represented as the direct product of a cyclic group of order \( p^\mu \) by a metacyclic group of order \( pg \). But then it is easy to verify that \( G' \) cannot be \( G(k) \) for any integer \( k \) and hence the group does not satisfy (B). We conclude that \( G' \) must have order prime to its index; and have completed the proof of one part of the following theorem.

**Theorem.** A group is solvable and satisfies condition (B) if and only if it is a metacyclic group whose commutator subgroup has index prime to its order.

To complete the proof of the Theorem it must be shown that if \( G \) is metacyclic with the order \( m \) of \( G' \) prime to its index \( n \), then every subinvariant subgroup is a \( G(k) \) for some \( k \). We will suppose that \( a \) is a generator of \( G' \) and that \( b \) is an element of order \( n \) which together with \( a \) generates \( G \); and will prove first by induction on the group order that every subinvariant subgroup of \( G \) is normal in \( G \). The induction will be based on the fact that since subgroups and homomorphic images of cyclic groups are cyclic, then by Theorem 11 of [2, p. 145], subgroups and homomorphic images of metacyclic groups are metacyclic (or cyclic).

Now let \( H \) be a subinvariant subgroup of \( G \) of prime order \( p \). If \( p \) divides \( m \) then \( H \) is a subgroup of \( G' \); in fact, \( H \) is then \( G'(m/p) \) and hence is normal in \( G \). If \( p \) divides \( n \) then \( H \) and \( G' \) generate a group \( K \) of order \( pm \) in which \( H \) is a Sylow subgroup. Since \( H \) is subinvariant in \( G \) it is subinvariant in \( K \) and by the induction hypothesis \( H \) is normal in a proper maximal normal subgroup \( M \) of \( K \). By the maximality of \( M \) either \( M \) or \( K \) is normalizer of \( H \) in \( K \). Since \( H \) is a Sylow subgroup of \( K \), \( M \) cannot be the normalizer of \( H \) since the normalizer of a Sylow subgroup is its own normalizer which would contradict that \( M \) is normal in \( K \). We conclude that \( H \) is normal in \( K \) and that \( H \) and \( G' \) commute elementwise. From this we will show that \( H \) is in the center of \( G \). For the cyclic group \( B \) generated by \( b \) must intersect \( K \) in a group of order \( p \) and hence contains \( H \) since \( H \) is the only Sylow \( p \)-subgroup of \( K \). It follows that \( H \) commutes elementwise both with \( a \) and with \( b \) the generators of \( G \). Hence \( H \) is in the center of \( G \) and is normal in \( G \).
The above argument shows that a minimal subinvariant subgroup of $G$ is normal in $G$. Now let $L$ be an arbitrary subinvariant subgroup of $G$. $L$ contains a minimal subinvariant subgroup $H$ which is normal in $G$. By the induction assumption $L/H$ is normal in $G/H$; hence $L$ is normal in $G$ as was to be shown. We have shown that every subinvariant subgroup of $G$ is normal in $G$.

Suppose next that the normal subgroup $L$ has order $rs$ where $n = rt$ and $m = sv$. Then the index of $L$ in $G$ is $tv$ and thus $G(tv)$ is contained in $L$. On the other hand $a^s$ is of order $s$ and is in $G(tv)$; also $b^t$ is of order $r$ and is in $G(tv)$. It follows that $G(tv)$ has order at least $rs$ and hence $G(tv) = L$. This completes the proof of the Theorem.

Bibliography


Louisiana State University and Agricultural and Mechanical College