GROUPS WHOSE SUBGROUPS ARE CYCLIC

By

Murad Jurdak

GROUPS WHOSE SUBGROUPS ARE CYCLIC

By

Murad Jurdak

Submitted in Partial Fulfillment of the Requirements

of the Degree Master of Sciences

in the Mathematics Department of the

American University of Beirut

Beirut, Lebanon

1968

AMERICAN UNIVERSITY OF BEIRUT

GROUPS WHOSE SUBGROUPS ARE CYCLIC

By

Murad Jurdak

Approved: Fawzi M. Yaqub
Advisor

Peter Yff
Member of Committee

David Singmaster
Member of Committee

____
Member of Committee

____

Date of Thesis Presentation: ______________________

TABLE OF CONTENTS

ABSTRACT

A group may fail to have a certain property, although each of its proper subgroups has this property. Many subgroups of this nature are studied: Finite, non-abelian groups all of whose proper subgroups are abelian are studied by G.A. Miller [5]. Infinite abelian groups all of whose proper subgroups are finite are knwon, but the existence of an infinite, non-abelian group with this property is still an open question [3, p.57].

In this thesis we are concerned with non-cyclic groups G satisfying one of the following two properties: (i) every proper subgroup of G is cyclic, (ii) every proper homomorphic image of G is cyclic.

We show that the only abelian groups with property (i) are the direct sum of a group of prime order with itself and p-quasicyclic groups. We show also that the only finite, non-abelian groups with property (i) are the quaternion groups, the non-abelian group of order pq, and all groups G of order p^nq such that $G = [a, b]$ $|a| = p^n$, $|b| = q$, $aba^{-1} = a^k$ $(k > 1)$ and $a^pba^{-p} = b$. For the infinite, non-abelian case, we prove that the existence of such a group with property (i) yields a solution for the Burnside problem when the center of the group is non-trivial. Then we shall give a characterization of all infinite, non-abelian groups G with property (i) when the center of G is trivial, on the assumption that such groups exist. In Chapter III, we prove that the only abelian group with property (ii) is isomorphic to the direct product of group of prime order with itself. We also characterize all finite, non-abelian, solvable groups with property (ii).

ABSTRACT

A group may fail to have a certain property, although each of its proper subgroups has this property. Many subgroups of this nature are studied: Finite, non-abelian groups all of whose proper subgroups are abelian are studied by G.A. Miller [5]. Infinite abelian groups all of whose proper subgroups are finite are knwon, but the existence of an infinite, non-abelian group with this property is still an open question [3, p.57].

In this thesis we are concerned with non-cyclic groups G satisfying one of the following two properties: (i) every proper subgroup of G is cyclic, (ii) every proper homomorphic image of G is cyclic.

We show that the only abelian groups with property (i) are the direct sum of a group of prime order with itself and p-quasicyclic groups. We show also that the only finite, non-abelian groups with property (i) are the quaternion groups, the non-abelian group of order pq, and all groups G of order $p^n q$ such that $G = [a, b]$ $|a| = p^n$, $|b| = q$, $aba^{-1} = a^k$ $(k > 1)$ and $a^p b a^{-p} = b$. For the infinite, non-abelian case, we prove that the existence of such a group with property (i) yields a solution for the Burnside problem when the center of the group is non-trivial. Then we shall give a characterization of all infinite, non-abelian groups G with property (i) when the center of G is trivial, on the assumption that such groups exist. In Chapter III, we prove that the only abelian group with property (ii) is isomorphic to the direct product of group of prime order with itself. We also characterize all finite, non-abelian, solvable groups with property (ii).

CHAPTER I

ABELIAN GROUPS WITH CYCLIC SUBGROUPS

In this chapter we determine all abelian, noncyclic groups G with the property that every proper subgroup of G is cyclic. It will be shown that these groups are either p-quasicyclic or isomorphic to the direct product of a group of prime order with itself.

In this chapter we shall adapt the following standard notation: Abelian groups will be written additively. $|G|$ will denote order of G and $|a|$ the order of the element $a \in G$. $G_1 \oplus G_2 \oplus \dots \oplus G_n$ will denote the direct sum of $G_1, G_2, \dots, G_n$, and $\oplus \sum_{i \in I} G_i$ will denote the weak direct sum of the family of groups $\{G_i \mid i \in I\}$. The group generated by a set M will be denoted by $[M]$, and in particular the cyclic group generated by a will be denoted by $[a]$. C_n will stand for a cyclic group of order n. If S is a proper subset of T, we shall write $S \subset T$. The symbol $(n_1, \dots, n_k)$ will denote the highest common factor of the integers $n_1, \dots, n_k$. Z and R^+ will denote the additive groups of integers and rationals respectively.

I.1.1 <u>Definition</u>: A group G is said to have property P if and only if:

(i) G is non-cyclic, and (ii) Every proper subgroup of G is cyclic.

I.1.2 <u>Examples of infinite abelian groups with property P</u>:

Let C_{p^i} denote the additive cyclic group of order p^i where p is a fixed prime and i is a positive integer. For every $i = 1, 2, \ldots, C_{p^{i+1}}$ has a unique cyclic subgroup H_i of order p^i. Let $f_{i,i+1}$ be an isomorphism of C_{p^i} onto H_i, and let $G = \bigcup_{i=1}^{\infty} f_{i,i+1}(C_{p^i})$ where we identify $f_{i,i+1}(C_{p^i})$ and H_i. Let $x, y \in G$. Then $x, y \in f_{k,k+1}(C_{p^k})$ for some k and we define $x \oplus y = x + y$, where "$+$" is the operation in the group $f_{k,k+1}(C_{p^k})$. Clearly G is an abelian group with respect to the operation $\oplus$. Moreover since $f_{i,i+1}(C_{p^i}) \subset f_{i+1,i+2}(C_{p^{i+1}})$, it follows that G is infinite. We now show that G has property P.

(i) G is non-cyclic: Suppose G is cyclic and let g be its generator. Then $g \in f_{s,s+1}(C_{p^s})$ for some s. Since g is a subgroup of $C_{p^{s+1}}$, $|G| \leq p^{s+1}$. This contradicts the fact that G is infinite. Hence G is non-cyclic.

(ii) Every proper subgroup of G is cyclic: Let H be a proper subgroup of G and let $S = \{|g| \mid g \notin H\}$. Since S is a non-empty set of positive integers, it has a least element p^k. We shall show that H has no elements of order p^k. Since $p^k \in S$, there is an element $g \notin H$ such that $|g| = p^k$. Suppose H has an element g_1 of order p^k. Then g and g_1 are two distinct subgroups of G of order p^k. But g and g_1 are contained in $f_{n,n+1}(C_{p^n})$ for some n. This contradicts the fact that a finite cyclic group cannot have two distinct subgroups of the same order. Hence H has no elements of order p^k and therefore is contained in the cyclic group $f_{k-1,k}(C_{p^{k-1}})$. Hence H is cyclic.

I.1.3 <u>Definition:</u> For a fixed prime p, the group generated by $\{a_n,\ n = 1, 2, \ldots \mid a_{n+1}^p = a_n,\ a_1^p = 1\}$ is called a p-quasicyclic group.

p-quasicyclic groups are discussed in [6]. An example of p-quasicyclic group is the group Z_{p^∞} which is defined as follows. Let R^+ and Z be, respectively, the additive groups of rationals and integers. Let p be a fixed prime and let Z_{p^∞} be the subgroup of R^+/Z generated by $\left\{\overline{\frac{1}{p^n}} \mid n = 1, 2, 3, \ldots.\right\}$, where $\overline{\frac{1}{p^n}}$ denotes the coset $\frac{1}{p^n} + Z$.

Another example of a p-quasicyclic group is the group G constructed in example I.1.3. To see this we note that G is generated by $\{g_n \mid n = 1, 2, 3, \ldots\}$, where each g_n is the generator of the cyclic group $f_{n,n+1}(C_{p^n})$.

We shall now show that all p-quasicyclic groups are isomorphic.

I.1.5 <u>Theorem</u>: All p-quasicyclic groups corresponding to the same prime p are isomorphic.

<u>Proof</u>: Let H and G be two p-quasicyclic groups generated, respectively, by $\{h_n,\ n = 1, 2, 3, \ldots \mid h_{n+1}^p = h_n,\ h_1^p = 1\}$, and $\{g_n,\ n = 1, 2, 3, \ldots \mid g_{n+1}^p = g_n,\ g_1^p = 1\}$. By induction we define isomorphisms $\phi_n: [h_n] \to [g_n]$, $n = 1, 2, \ldots$, such that $\phi_{n+1}(h) = \phi_n(h)$ for every $h \in [h_n]$ (i.e. each ϕ_{n+1} is an extension of ϕ_n). Let $\phi: H \to G$ be defined as follows: For every $h \in H$, $h \in h_k$ for some k and we define $\phi(h) = \phi_k(h)$. Since each ϕ_n is an extension of ϕ_{n-1}, it follows that ϕ is well-defined. It is not difficult to show that ϕ is an isomorphism of H onto G.

I.1.6 Corollary: For every prime p, the group Z_{p}^{∞} is isomorphic to the group G of Example I.1.3.

I.1.7 Corollary: Every p-quasicyclic group has property P.

Proof: Every p-quasicyclic group is isomorphic to the group G of Example I.1.3 which was shown to have property P.

I.2 Finitely generated abelian groups with property P:

In this section we determine all finitely generated groups with property P. It will be shown that these groups are isomorphic to the direct product of a group of prime order with itself.

I.2.1 Lemma: The group $G = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_k}$, where each C_{n_i} is the cyclic group of order n_i, is a cyclic group if and only if $(n_1, \ldots, n_k) = 1$.

Proof: Suppose G is cyclic. Let c_i be a generator of C_{n_i}. If $(n_1, n_2, \ldots, n_k) = d \neq 1$, then $\frac{n_1 n_2 \cdots n_k}{d}(c_1, \ldots, c_k)$ $= \left(\frac{n_1 n_2 \cdots n_k}{d} c_1, \ldots, \frac{n_1 n_2 \cdots n_k}{d} c_k\right) = 0$. Hence the order of $(c_1, c_2, \ldots, c_k)$ is less than $n_1 n_2 \cdots n_k$. But $(c_1, c_2, \ldots, c_k)$ generates the group G and hence has order $n_1 n_2 \cdots n_k$. This contradiction shows that $(n_1, n_2, \ldots, n_k) = 1$.

Conversely, if $(n_1, \ldots, n_k) = 1$, then l.c.m. of $n_1, n_2, \ldots, n_k$ is $n_1 n_2 \cdots n_k$. Now $n_1 n_2 \cdots n_k (c_1, c_2, \ldots, c_k) = 0$ and if $|(c_1, \ldots, c_2)| = n$, then $n \mid n_1 n_2 \cdots n_k$. But $n(c_1, \ldots, c_k) = (nc_1, nc_2, \ldots, nc_k) = 0$. Hence $n_i \mid n$ for all $i = 1, \ldots, k$. It follows that $n_1 n_2 \cdots n_k \mid n$ since $n_1 n_2 \cdots n_k =$ l.c.m of $(n_1, \ldots, n_k)$. Hence $n = n_1 n_2 \cdots n_k$, and G is cyclic since it is of order $n_1 n_2 \cdots n_k$ and has an element $(c_1, \ldots, c_k)$ of order $n_1 n_2 \cdots n_k$.

I.2.2 <u>Proposition</u>: A finite abelian group G has property P if and only if G is isomorphic to $C_p \oplus C_p$ for some group of prime order p.

<u>Proof</u>: Suppose $G = C_p \oplus C_p$; then G is non-cyclic by lemmas I.2.1. Since every proper subgroup of G is of order 1 or p, it is cyclic. Hence G has property P. Conversely, suppose G has property P. Then by the fundamental theorem of finitely generated abelian groups[4], $G = C_{n_1} \oplus C_{n_2} \oplus \dots \oplus C_{n_k}$, where each C_{n_i}, is cyclic of order n_i and $n_i \mid n_{i+1}$. If $k \geqslant 3$, then $C_{n_1} \oplus C_{n_2}$ is a proper, non-cyclic subgroup of G since $(n_1, n_2) \neq 1$. Also $k \neq 1$, otherwise G would be cyclic. Therefore $k = 2$. Now n_2 is a prime, otherwise it would have a prime divisor p such that $(n_1, p) = P \neq 1$, and $C_{n_1} \oplus C_p$ would be a proper, non-cyclic subgroup of G. Therefore n_2 a prime & $n_1 = n_2$, since $n_1 \mid n_2$. Hence $G \cong C_p \oplus C_p$.

I.2.3 <u>Lemma</u>: Every finitely generated abelian group G with property P is finite.

<u>Proof</u>: Let G be a finitely generated abelian group with property P. By the basis theorem for finitely generated abelian groups[ ], $G = [c_1] \oplus \dots \oplus [c_r] \oplus [E_1] \oplus \dots \oplus [E_n]$, where each C_i is cyclic of infinite order and each E_i is of order e_i with $e_i \mid e_{i+1}$. Two cases are to be considered:

(i) G has no non-zero element of finite order. Then $G = [c_1] \oplus \dots \oplus [c_r]$. Since G is non-cyclic, $r \neq 1$. On the other hand, if $r > 1$, then $[2c_1] \oplus [c_r]$ would be a proper, non-cyclic subgroup of G contradicting the fact that G has property P. Hence case (i) cannot occur.

(ii) G has elements of finite order. If G also has elements of infinite order, then $r \geq 1$. Hence $[2c_1] \oplus [E_1]$ is a proper, non-cyclic subgroup of G contradicting the fact that G has property P. Hence G has no elements of infinite order and $G = [E_1] \oplus \dots \oplus [E_r]$. Hence G is finite.

I.3. Infinite abelian groups with property P:

It will be shown in this section that an infinite abelian group has property P if and only if it is p-quasicyclic for some prime P. The following theorem is known. It is stated without proof in [6].

I.3.1 Theorem : The group $\overset{+}{R}/_Z$ is isomorphic to the direct sum of p-quasicyclic groups, one for each prime p.

Proof: Let P be the set of all primes. From corollary I.1.6, Z_{p^∞} is p-quasicyclic for every $p \in P$. It will be shown that $\overset{+}{R}/_Z \cong \oplus \sum_{p \in P} Z_{p^\infty}$. Let $x \in \overset{+}{R}/_Z$ be represented by the coset $Z + \frac{n}{m}$, where $n < m$ and $(n,m) = 1$; $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ with the P_i's distinct primes. Now

$$\frac{n}{m} = \frac{\lambda_1}{p_1^{\alpha_1}} + \frac{\lambda_2}{p_2^{\alpha_2}} + \dots + \frac{\lambda_k}{p_k^{\alpha_k}}, \text{ where } (\lambda_i, P_i^{i}) = 1;$$

since if p_i divides λ_i for some $i = 1, \dots, k$, then

$$\frac{n}{m} = \frac{\lambda_1 p_2^{\alpha_2} \dots p_k^{\alpha_k} + \lambda_2 p_1^{\alpha_1} p_3^{\alpha_3} \dots p_k^{\alpha_k} + \dots + \lambda_k p_1^{\alpha_1} \dots p_k^{\alpha_k}}{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}}$$

and p_i divides both m and n which contradicts the fact that $(n, m) = 1$. Hence $Z + \frac{n}{m} = (Z + \frac{\lambda_1}{p_1^{\alpha_1}}) + \dots + (Z + \frac{\lambda_k}{p_k^{\alpha_k}})$, and $\overset{+}{R}/_Z$ is

generated by $\{Z_{p^\infty} | p \in P\}$. Now suppose $[Z_{p_1^\infty}] \cap [\bigcup_{p \neq p_1} Z_{p^\infty}] \neq 0$;
Let $x \neq 0$ be in the intersection; then $x = Z + \frac{\lambda_1}{p_1^{\alpha_1}} = Z + \frac{\lambda_2}{p_2^{\alpha_2}} + \cdots + \frac{\lambda_k}{p_k^{\alpha_k}}$.

Hence

$$\frac{\lambda_1 p_2^{\alpha_2} \cdots p_k^{\alpha_k} - \cdots - \lambda_k p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}} \in Z.$$

But this would imply $p_1^{\alpha_1}$ divides λ_1 and this contradicts the fact that $x \neq 0$. Hence $R^+/Z \cong \oplus \sum_{p \in P} Z_{p^\infty}$.

I.3.2 Definition: A group is locally cyclic if each of its finitely generated subgroups is cyclic.

Locally cyclic groups are discussed in [6] from which the proof of the following theorem is adapted.

I.3.3 Definition: A group G is said to be torsion (periodic) each of its elements has finite order. It is torsion - free if no element, other than the identity, has finite order

I.3.4 Theorem: If a group is locally cyclic, then it is isomorphic either to a subgroup of R^+ or of R^+/Z.

Proof: If G is locally cyclic then G is abelian and, moreover, either a torsion group or torsion-free; for if a is an element of non-trivial finite order, and b an element of infinite order then $[a, b]$ is $[a] \oplus [b]$ which is not cyclic. If G is a torsion group let $G_p = \{a \in G \mid |a| = p^n \text{ for some } n\}$ and this is clearly a subgroup of G. G_p has at most one subgroup a_k of order P^k; for if a and b are elements of order P^k, then $|[a, b]| = P^k$ and $[a, b] = [a] = [b]$. Since $[a_{k+1}] \supset [a_k]$, either there is a maximum a_k and G_p is cyclic of order p^k, or G_p is an ascending union of cyclic groups of order P^k and G_p

is p-quasicyclic. Since $G = \bigoplus \sum_{p \in P} G_p$ and each G_p is a subgroup of a p-quasicyclic group then G is a subgroup of $R^+/_Z$ by Theorem I.3.1.

If G is torsion-free, then for any element $a \in G$ and any $n \in Z$, there is at most one element $x \in G$ such that $nx = a$; for if $nx = ny = a$; then $n(x - y) = 0$ and $x = y$. Now let $c \neq 0$ be a fixed element of G and define c_n to be the element of G such that $nc_n = c$, if c_n exists; otherwise define c_n to be zero. Then $[c_n, n \in Z] = G$; for if $x \in G$, since $[x,c]$ is cyclic, there is a generator c_n of $[x, c]$ and a natural number n with $nc_n = c$ and $x = kc = knc_n$. If now for each integer $i \geqslant 1$, G_i is the cyclic group $[c_1, c_2, \ldots, c_i] = [a_i]$, then $G_i \subseteq G_{i+1}$ and there are natural number m_i such that $a_i = m_i a_{i+1}$. By induction we define isomorphisms $\phi_n: G_n \rightarrow \left[\prod_{k=1}^{n} \frac{1}{m_k}\right]$ by $\phi_n(a_n) = \prod_{k=1}^{n} \frac{1}{m_k}$. Since $a_i = m_i a_{i+1}$ then $\phi_{n+1}(g) = \phi_n(g)$ for every $g \in G_n$. Let $\phi: G \rightarrow R$ be defined by $\phi(g) = \phi_k(g)$ since $g \in G_k$ for some k. ϕ is well-defined since $a_i = ma_{i+1}$. It is easy to show that ϕ is an isomorphism into R^+. Hence G is isomorphic to a subgroup of R^+.

I.3.5 <u>Lemma</u>: No subgroup of R^+ has property P.

<u>Proof</u>: Let G be a subgroup of R^+. Suppose G is not finitely generated. Then G is generated by an infinite set $S = \left\{\frac{n_1}{m_1}, \frac{n_2}{m_2}, \ldots\right\}$ such that no finite subset of S generates G. There is no loss of generality in assuming that $m_1 \neq m_2 \neq \ldots \neq m_k \neq \ldots$. Let P_1 be a prime factor of m_1, $P_2 \neq P_1$ a prime factor of m_2, ..., $P_i \neq P_{i-1}$ a prime factor of m_i, ... Consider $H = \left[\frac{1}{P_2}, \frac{1}{P_3}, \ldots\right]$. Clearly H is a proper subgroup of G since $\frac{n_1}{P_1} \in G$ and $\frac{n_1}{P_1} \notin H$. H is non-cyclic since if $H = \left[\frac{n}{m}\right]$

with $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ (p_i's are distinct primes), then $\frac{1}{p_{k+1}^{\alpha_{k+1}}} = \frac{qn}{m}$ and this would imply that $p_{k+1}^{\alpha_{k+1}}$ is a prime factor of m. Hence a contradiction. So G does not have property P.

I.3.6 Theorem: If G is an infinite, abelian group then G has property P if and only if G is p-quarsicyclic for some prime P.

Proof: Suppose G has property P, then every proper subgroup of G is cyclic. In particular, since G is not finitely generated (Lemma I.2.3) every finitely generated subgroup of G is cyclic, i.e. G is locally cyclic. By Theorem I.3.3 G is either isomorphic to a subgroup of R^+ or of R^+/Z. By lemma I.3.4 G is isomorphic to a subgroup of R^+/Z. By Proposition I.3.1 G is isomorphic to $\bigoplus\sum_{p\in P} G_p$ where P is a set of primes and each G_p is a subgroup of a p-quasicyclic group, i.e. G_p is either finite cyclic or p-quasicyclic. Now we prove that not all G_p are cyclic. Since if they are, then P is an infinite set otherwise G is cyclic. Consider $H = \bigoplus\sum_{p\in P-\{p_o\}} G_p$ where $p_o \in P$. Clearly H is a non-cyclic subgroup otherwise $P - \{p_o\}$ is finite contradicting P is infinite. H is also proper since H has no element of order p_o. This contradicts the hypothesis that G has property P; and therefore at least one G_p is p-quasicyclic. It follows that $G \cong G_p$, otherwise G_p will be isomorphic to a proper, non-cyclic subgroup of G. The converse of the theorem is just corollary I.1.7.

To sum up the results of this section, we state the following theorem:

I.3.6 <u>Theorem</u>: An abelian group G has property P if and only if $G \cong C_p \oplus C_p$ for some cyclic group of prime order p or G is isomorphic to p-quasicyclic group for some prime P.

CHAPTER II

NON-ABELIAN GROUPS WITH CYCLIC SUBGROUPS

In this chapter we investigate non-abelian groups with property P. It will be shown in section 2.1 that the only finite non-abelian groups with property P are: The quaternion group, groups of order pq and groups G of order $p^n q$ on two generators a and b with $[b] \triangleleft G$, $a^{p^n} = b^q = e$ and $a^p b = ba^p$. In section 2.2, it will be shown that the existence of an infinite non-abelian group G with property P reduces to Burnside problem when the center of G is non-trivial. When G is not periodic and $Z(G) = e$, we shall give a characterization of such groups if they exist.

In this chapter, we shall use the multiplicative notation. The identity will be denoted by e and the center of a group G by Z(G). $H \triangleleft G$, where H is a subgroup of G, will mean: H is normal in G. The direct product of the subgroups $H_1, H_2, \ldots, H_2$ will be denoted by $H_1 \otimes H_2 \otimes \ldots \otimes H_n$.

II.1 <u>Finite non-abelian groups with property P</u>:

First we show that the only p-group with property P is the quaternion group. To prove this we need the following propositions and lemmas.

II.1. <u>Proposition</u>: Let H be a normal, cyclic subgroup of G. If H_1 is a subgroup of H, then $H_1 \triangleleft G$.

Proof: case (i): H is finite cyclic. Let $g \in G$; then $gH_1g^{-1} \subseteq H$, since $H \triangleleft G$. If $gH_1g^{-1} \not\subseteq H_1$, then the cyclic group H would have two distinct subgroups of the same order, namely H_1 and gH_1g^{-1}. This contradiction shows that $gH_1g^{-1} = H_1$, hence $H_1 \triangleleft G$.

Case (ii): H is infinite cyclic. Let $H = [a]$ and let $g \in G$. Since $H \triangleleft G$, the inner automorphism τ_g of G maps H into itself. Since τ_g maps a generator of H into a generator of H, $\tau_g(a) = a$ or a^{-1}. Now $H_1 = [a^k]$ for some k; hence $\tau_g(H_1) = [\tau_g(a^k)] = [a^k]$ or $[a^{-k}]$. Hence $\tau_g(H_1) = H_1$ and $H_1 \triangleleft G$.

II.1.2 Lemma: If G is a non-abelian group having property P, then G is generated by two elements.

Proof: Since G is non-cyclic, G is generated by at least two elements. But G is non-abelian, so there exist $a, b \in G$ such that $ab \neq ba$. $[a, b]$ is not a proper subgroup of G because if it were then it would be cyclic and this would imply that $ab = ba$. Hence $[a, b] = G$.

II.1.3 Proposition: Let G be a non-abelian group with property P. If H is a subgroup of Z(G), then $G/_H$ has property P.

Proof: First we show that $G/_H$ is non-cyclic. Suppose $G/_H$ is cyclic and let $G/_H = [cH]$. Since G is non-abelian there exist $a, b \in G$ such $ab \neq ba$. Clearly $a, b \notin H$. Consider the cosets $aH, bH \in G/_H$. Since $G/_H$ is cyclic, $aH = c^nH$ and $bH = c^mH$ for some integers n and m. It follows that $ac^{-n} \in H$ and $bc^{-m} \in H$.

Now $(ab)c^{-m}\, c^{-n} = ac^{-n}\, bc^{-m}$ $\qquad (bc^{-m} \in H \subseteq Z(G))$.

$= bac^{-n}\, c^{-m}$ $\qquad (ac^{-n} \in H \subseteq Z(G))$.

Hence $ab = ba$ which is a contradiction. Therefore G is non-cyclic.

Next we show that every proper subgroup of $G/_H$ is cyclic. Let G_1 be a proper subgroup of $G/_H$. By the second isomorphism theorem [4] $G_1 = A/_H$ where $H \subset A \subset G$. But G has property P; therefore A and H are cyclic. Hence G_1 is isomorphic to the homomorphic image of a cyclic group. Hence G_1 is cyclic.

II.1.4 <u>Lemma</u>: A non-abelian group G of order P^3, where P is an odd prime, does not have property P.

<u>Proof</u>: There are two non-abelian groups of order P^3 for an odd prime p([2], p. 51):

(a) $G = [a, b]$, $a^{p^2} = b^p = e$, $b^{-1}ab = a^{1+p}$.

(b) $G = [a, b, c]$, $a^p = b^p = c^p = e$, $ab = bac$, $ca = ac$, $cb = bc$.

(a) G, being a p-group, has a non-trivial center. Moreover, $Z(G) \not\leq [b]$ and $Z(G) \not\leq [a]$, otherwise G would be abelian. It follows that $Z(G) = [a^p]$, otherwise we would have $Z(G) \cap [a] = (e)$, hence $G \cong Z(G) \otimes [a]$ contradicting the fact that G is non-abelian. Now since $[a^p] = Z(G)$ and $b \notin [a]$, it follows that $[a^p][b]$ is a proper, non-cyclic subgroup of G. Hence G does not have property P in this case.

(b) In this case c commutes with a and b. Hence $[c] \subseteq Z(G)$. Hence $[c][a]$ is a proper, non-cyclic subgroup of G. Therefore G does not have property P.

II.1.5 <u>Lemma</u>: The only group G of order 2^3 which has property P is the quaternion group.

<u>Proof</u>: There are two non-abelian groups of order 2^3

(a) Dihedral group: $G = [a, b]$, $a^4 = b^2 = e$, $ba = a^3b$.

(b) Quaternion group: $G = [a, b]$, $a^2 = b^2$, $ba = a^3b$.

(a) The multiplication table of G is:

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

It is readily verified from this table that $H = \{e, a^2, b, a^2b\}$ is a subgroup and that $|a^2| = |b| = |a^2b| = 2$. Hence H is proper, non-cyclic subgroup and this shows that the dihedral group of order 2^3 does not have property P.

(b) The following is the multiplication table for the Quaternion group of order 2^3.

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	e	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	b	ab	a^2b	a	e	a^3	a^2

It is readily verified from this table that:

$|a^2| = 2$ and $|a| = |a^3| = |b| = |ab| = |a^2b| = |a^3b| = 2^2$.

Thus every subgroups of order 4 must contain an element of order 4 and hence is cyclic. Therefore the Quaternion group has Property P.

II.1.6 __Lemma__: No non-abelian group of order 2^4 has property P.

__Proof__: It is shown in Carmichael [1] that there are just four abstract non-abelian groups of order 2^4 each of which contains an element of order 2^3.

(a) $G = [P, Q]$, $P^{2^3} = 1$, $Q^2 = P^4$, $Q^{-1} PQ = P^{-1}$

(this is derived on the assumption that G has only one subgroup of order 2).

(b) $G = [P, Q]$, $P^{2^3} = Q^2 = 1$, $QPQ = P^{1+2^2}$

(c) $G = [P, Q]$, $P^{2^3} = Q^2 = 1$, $(PQ)^2 = P^{2^2}$.

(d) $G = [P, Q]$, $P^{2^3} = Q^2 = (PQ)^2 = 1$.

In (b), (c) and (d): $|P| = 2^3$, $|Q| = 2$ and $[P] \cap [Q] = e$.

Now $Z(G) \neq e$, since G is a p-group. On the other hand, $Z(G) \not\subseteq [P]$ and $Z(G) \not\subseteq [Q]$, otherwise G is abelian. Therefore, $Z(G) \subset [P]$ otherwise G is abelian. Let $Z(G) \otimes [Q] = H$. Then H is proper, since it does not have any elements of order 2^3. Also H is non-cyclic since $|Z(G)|$ and $|Q|$ are not relatively prime. Hence G does not have property P, for the cases (b), (c), (d). Suppose that the group G, given in (a), has property P. Let G_1 be the unique subgroup of order 2. Then $G_1 \subseteq Z(G)$, since $|Z(G)|$ is at least 2. Also since $G_1 \subseteq Z(G)$, $G_1 \triangleleft G$. Hence by II.1.3, G/G_1 has property P and $|G/G_1| = 2^3$. By lemma II.1.4, G/G_1 is the quaternion group, hence G/G_1 has a unique subgroup of order 2. By the second isomorphism theorem, G has a unique subgroup of order 2^2 containing G_1. It follows that $[Q] = [P^2]$, since both of them are of order 2^2 and contain G_1. Thus $Q \in [P]$, hence P and Q commute; i.e. G is abelian which is a contradiction. Hence G does not have property P.

II.1.7 <u>Proposition</u>: A non-abelian, finite p-group G has property P if and only if G is the quaternion group.

<u>Proof</u>: Let G be a non-abelian group of order p^n. Since G is non-abelian, we may assume that $n \geq 3$. Also in view of lemmas II.1.4, II.1.5 and II.1.6, we may assume that $n > 3$ if p is odd,

and $n > 4$ if $p = 2$. Suppose G has property P. G, being a p-group, has a non-trivial center. Let $H_1 \subseteq Z(G)$, where H_1 is a subgroup of G of order p. By proposition II.1.3 $G/H_1 = G_1$ has property P, and $|G_1| = p^{n-1}$. G_1, again has a non-trivial center; so let $H_2 \subseteq Z(G_1)$, where H_2 is a subgroup of G_1 of order p. By II.1.3. $G/H_2 = G_2$ has property P and $|G_2| = p^{n-2}$. Continuing in this way we obtain G_{n-4} of order p^4 and having property P. So if $p = 2$, this already contradicts II.1.6. If $p \neq 2$ we continue to obtain G_{n-3} of order p^3 and having property P and this contradicts II.1.4.

Hence the only p-group with property P is the quaternion group.

Finite non-abelian groups in which every subgroup is abelian are discussed by G. A. Miller in [5]. The following theorem is proved there:

II.1.8 <u>Theorem:</u> The order of a non-abelian group which contains only abelian subgroups cannot be divisible by more than two distinct primes and if such a group has more than one sylow subgroup, one of these subgroups is of type (1, 1, ..., 1) and the others are cyclic.

II.1.9 <u>Proposition</u>: A non-abelian group G of order $p^n q (n > 1)$, p and q are distinct primes with $G = [a, b]$, $a^{p^n} = b^q = e$, $bab^{-1} = a^p$ and $a^{-1}ba = b^k$ for some $k > 1$, has property P.

<u>Proof</u>: A typical element g G is of the form $g = a^{k_1} b^{k_2} \dots a^{k_n}$. Thus

$$
\begin{aligned}
gbg^{-1} &= (a^{k_1} b^{k_2} \dots b^{k_{n-1}} a^{k_n}) b (a^{-k_n} b^{-k_{n-1}} \dots b^{-k_2} a^{-k_1}) \\
&= a^{k_1} b^{k_2} \dots b^{k_{n-1}} a^{k_n - 1} (aba^{-1}) a^{-k_n - 1} b^{-k_{n-1}} \dots b^{-k_2} a^{-k_1} . \\
&= a^{k_1} b^{k_2} \dots b^{k_{n-1}} a^{k_n - 1} (b^{-k}) a^{-k_n\ 1} b^{-k_{n-1}} \dots b^{-k_2} a^{-k_1} . \\
&= a^{k_1} b^{k_2} \dots b^{k_{n-1}} (b^{-k})^{k_n} b^{-k_{n-1}} \dots b^{-k_2} a^{-k_1} .
\end{aligned}
$$

Continuing in this way, we see that gbg^{-1} reduces to b^m for some integer m. So $gbg^{-1} \in [b]$ for all $g \in G$. Hence $[b] \triangleleft G$.

Now suppose that G satisfies the hypothesis of the theorem. Let H be a proper subgroup of G. If $|H| \leq q$, then clearly H is cyclic. If $|H| = p^m$, $m \leq n$, then H is contained in a sylow subgroup S_p(2 ,p.44), and since S_p is conjugate to $[a]$, S_p and hence H are cyclic. Thus we may assume that $|H| = qp^k$, $1 \leq k < n$.

Since $[b] \triangleleft G$, $[b]$ is the only subgroup of G of order q. Since H has a subgroup of order q, it follows that $[b] \subset H$. Moreover, $[b] \triangleleft H$, since $[b] \triangleleft G$. H also has a subgroup K of order p^k, but we shall now show that $K \subseteq Z(G)$. K is contained in a sylow subgroup S_p. Since S_p is conjugate to $[a]$, there is an inner automorphism τ of G which maps $[a]$ onto S_p. Since a^p commutes with b, $a^p \in Z(G)$. Hence $[a^p] \triangleleft G$ and τ maps $[a^p]$ onto itself. Thus $[a^p] \subset S_p$. Since $|a^p| = p^{n-1}$, and the cyclic group S_p cannot have two distinct subgroups of the same order, it follows that $K \subseteq [a^p] \subseteq Z(G)$.

Now H has two normal subgroups $[b]$ and K whose intersection is e. Hence $H = [b] \otimes K$ and since $|[b]|$ and $|K|$ are relatively prime, H is cyclic. This completes the proof of the proposition.

II.2.10 <u>Theorem</u>: A finite non-abelian group G has property P if and only if

(a) $|G| = pq$ where p and q are distinct primes, or

(b) G is the quaternion group, or

(c) $|G| = p^n q$, p and q are distinct primes and $n > 1$, where $G = [a, b]$ with $a^{p^n} = b^q = e$, $a^p = ba^pb^{-1}$ and $a^{-1}ba = b^k$ for some $k > 1$.

<u>Proof</u>: Suppose G has property P. Then every proper subgroup of G is abelian and hence $|G| = p^nq^m$ by theorem II.1.8. By the same theorem, m and n cannot be both greater than 1, otherwise G would have a proper subgroup of type (1, 1, ...,1) which is not cyclic. Hence $m = 1$ or $m = 0$. If $m = 0$, then G is a p-group and by II.1.7. G is the quaternion group. If $n = m = 1$, then $|G| = pq$ and the only possible proper subgroups are of order 1 or p or q which are cyclic.

The only case left is that where $|G| = p^nq$ $(n > 1)$. The sylow subgroups of G are cyclic since G has property P. So there are $a, b \in G$, $|a| = p^n$, $|b| = q$ and $ab \neq ba$ (otherwise G would be abelian). We claim that $[a]$ is not normal in G. Suppose $[a] \triangleleft G$. Since $[a]$ is cyclic, $[a^p] \triangleleft G$ (Proposition 2.1.1). Hence $[b][a^p]$ is a subgroup of G of order $p^{n-1}q$. Since G has property P, $[b][a^p]$ is cyclic; hence $a^pb = ba^p$. Now since $[a] \triangleleft G$, $b^{-1}ab = a^k$, where $k < p^n$. Thus $b^{-1}a^pb = a^{kp}$; and since a^p commutes with b, $a^p = a^{kp}$. Hence $p(k-1) \equiv 0 \ (p^n)$. Hence p^{n-1} is a divisor of $k - 1$. Thus $k - 1 = \lambda p^{n-1}$, where $1 \leq \lambda < p$ since $k - 1 < p^n$. Thus $b^{-1}ab = a^k = a^{\lambda p^{n-1}+1}$. Hence $aba^{-1} = ba^{\lambda p^{n-1}}$. Hence $|ba^{\lambda p^{n-1}}| = |aba^{-1}| = |b| = q$. But $a^{\lambda p^{n-1}} = (a^p)^{\lambda p^{n-2}} \in [a^p]$. Hence $a^{\lambda p^{n-1}}$ commutes with b and $e = (ba^{\lambda p^{n-1}})^q = b^qa^{\lambda qp^{n-1}} = a^{\lambda qp^{n-1}}$. Hence $\lambda qp^{n-1} \equiv 0 (\text{mod } p^n)$. But this is a contradiction since p and q are relatively prime and $\lambda < p$.

Hence $[a]$ is not normal in G. Now we prove that $[b] \triangleleft G$. It is known that a group of order $p^n q$ is non-simple [1, 292]. If G has a normal subgroup H of order $p^k q$ $(k \geq 1)$, then the subgroup of H of order q is normal in G and hence $[b] \triangleleft G$. So the only case left is when G has a normal subgroup H_1 of order p^k for some $k \geq 1$. Now if $G_1 = G/H_1$ has a normal subgroup of order $p^\ell q$ for some $\ell \geq 1$, then by the second isomorphism theorem, G has a normal subgroup of order $p^\ell q$, hence $[b] \triangleleft G$. Therefore G_1 has a normal subgroup of order p^{i_2}. Hence G has a normal subgroup of order $p^{i_1 + i_2}$. Continuing in this way, we get $[a] \triangleleft G$, which is a contradiction. Hence $[b] \triangleleft G$. Hence $a^{-1}ba = b^k$. It remains to prove that $a^p b = ba^p$. Now $G/[b]$ is a p-group of order p^n and so it has a normal subgroup of order p^{n-1}. By the second isomorphism theorem, G has a normal subgroup H of order $p^{n-1}q$. Let K be a normal subgroup of H of order p^{n-1}. Since H is cyclic, $K \triangleleft G$ (II.1.1). It follows that $K \subset [a]$ (since $K \triangleleft G$, K is contained in every p-sylow group). Hence $K = [a^p]$ since $[a^p]$ is the only subgroup of $[a]$ of order p^{n-1}. But $a^p \in H$ and $[b] \subset H$ since H has a subgroup of order q and the only subgroup of G of order q is $[b]$ $([b] \triangleleft G)$. Hence $a^p b = ba^p$, since H is cyclic.

Conversely, if $|G| = pq$, then G has property P since every proper subgroup of G is of prime order. If G is the quaternion group, then G has property P by II.1.7. If G is as described in (c) then G has property P by II.1.9.

II.2. Infinite Non-abelian groups with property P

II.2.1 **Lemma**: Let G be an infinite, non-abelian group with property P. If $1 < |Z(G)| < \infty$, then G is periodic.

Proof: Since $Z(G)$ is cyclic, every element of $Z(G)$ is of finite order. Let $a \notin Z(G)$ and consider $C(a) = \{x \mid x \in G, xax^{-1} = a\}$. Clearly $Z(G) \subseteq C(a)$. But $C(a)$ is cyclic and has an element of finite order $\neq e$, namely the generator of $Z(G)$. Hence $C(a)$ is finite cyclic and this implies that the order of a is finite. Hence G is periodic.

II.2.2 **Lemma**: Let G be a non-abelian infinite group with property P such that $|Z(G)|$ is infinite; then $Z(G)$ is a maximal normal subgroup of G.

Proof: Let $N \triangleleft G$ and $N \supset Z(G)$. Now $N = [x]$ where $x \notin Z(G)$. Let m be the smallest positive power such that $x^m \in Z(G)$, then $Z(G) = [x^m]$. Consider $C(x) = \{g \mid g \in G, xg = gx\}$ and let $y \notin C(x)$. Since $N \triangleleft G$, $yxy^{-1} = x^k$ for some $k > 1$. Now $(yxy^{-1})^m = x^{km} = yx^my^{-1}$. But $x^m \in Z(G)$, so $yx^my^{-1} = yy^{-1}x^m = x^{mk}$. Hence $k = 1$ since $Z(G)$ is not finite. This contradicts the definition of k.

II.2.3 **Lemma**: Let G be a non-abelian infinite group with property P, such that $|Z(G)| \neq 1$; then $G/_{Z(G)}$ is periodic.

Proof: Let $\bar{a} \neq e$ be the coset in $G/_{Z(G)}$ represented by a. Since the subgroup $[a]Z(G)$ is abelian, it is proper and hence cyclic. Thus if $[a] \cap Z(G) = e$, then $[a]Z(G) = [a] \otimes Z(G)$ which is not cyclic. This contradiction shows that $[a] \cap Z(G) \neq e$. Hence $a^n \in Z(G)$ for some positive integer n. Hence $|\bar{a}| = n$ and $G/_{Z(G)}$ is periodic.

As a result of the above lemmas we conclude that if G is an infinite, non-abelian group with property P, then the following hold:

(a) If $1 \neq |Z(G)| < \infty$, then G is finitely generated, infinite, non-abelian group which is periodic (Lemma II.2.1). Whether such groups exist or not is the unsolved Burnside problem ([2], p.320).

(b) If $1 \neq |Z(G)|$ is infinite, then $G/_{Z(G)}$ is periodic and has property P (proposition II.1.3). If $G/_{Z(G)}$ is infinite then we have the same situation as in (a); that is $G/_{Z(G)}$ is a Burnside group. If $G/_{Z(G)}$ is finite, then $G/_{Z}$ is simple, otherwise there would be a normal subgroup of G containing Z(G) properly which contradicts II.2.2. Since all non-abelian finite groups with property P are not simple, G does not have property P.

Thus the existence of an infinite, non-abelian group with property P and non-trivial center yields a solution to the Burnside problem. Hence we shall assume that $Z(G) = e$. We shall give a characterization of infinite non-abelian groups G with property P when $Z(G) = e$, , on the assumption that such a group exists. But first we shall prove that such a group is simple.

II.2.4 <u>Lemma</u>: Let G be an infinite, non-abelian group with property P; then G is simple if and if $Z(G) = e$.

<u>Proof</u>: If G is simple then clearly $Z(G) = e$. Conversely, let $Z(G) = e$, and suppose that $e \neq H \lhd G$. Clearly H is cyclic, so let $H = [h]$. Consider $C(h) = \{g \in G \mid gh = hg\}$. Then $C(h) \neq G$, otherwise $e \neq h \in Z(G)$. Hence C(h) is cyclic. Let $C(h) = [a]$. It is not difficult to see that if $b \notin [a]$, then $G = [a, b]$. (If $[a, b] \subset G$, then $[a, b]$ is cyclic; hence $b \in [a]$). We consider

two cases:

(i) $H \subset [a]$ and (ii) $H = [a]$.

(i) Since $H \subset [a]$, it follows that $H = [a^n]$ where $n > 1$. Let $b \notin [a]$. Then we claim that $H[b]$ is a proper subgroup. For if it is not, then $a \in H[b]$. Hence $a = (a^n)^k b^m$; hence $a^{1-nk} = b^m$. Now if $b^m = e$, then $a^{1-nk} = e$, and hence $a = a^{nk}$. Hence $a \in [a^n] = H$, contrary to our assumptions that $H \subset [a]$. Hence $e \neq b^m \in [a]$, hence b^m commutes with a and b and so $e \neq b^m \in Z(G)$ which is a contradiction. So $H[b]$ is a proper subgroup of G and hence cyclic. Therefore b commutes with a^n and this implies that $e \neq a^n \in Z(G)$ which is a contradiction.

(ii) $H = [a]$: If $[a]$ has a proper subgroup H' i.e. ($e \neq H' \subset [a]$), the same arguement as in case (i), with H' playing the role of H, will give the result. Suppose $[a]$ does not have any proper subgroups. Then $|a| = p$ for some prime p. Then as was shown above, $G = [a, b]$; and since $[a] \lhd G$, $G = [a][b]$. If $|b| < \infty$, then $|G| = p\,|[b]|$ is finite which is a contradiction. It follows that $|b| = \infty$. Now $[a][b^2] \subset G$, otherwise $b = a^k b^{2n}$ and so $b^{1-2n} = a^k$ and this would imply $e \neq b^{1-2n} \in [b] \cap [a] \subseteq Z(G)$. Hence $[a][b^2]$ is cyclic and so $e \neq b^2 \in Z(G)$ which is a contradiction.

II.2.5 <u>Theorem</u>: Let G be an infinite, non-abelian group such that G is not periodic and $Z(G) = e$, then G has property P if and only if:

$$G = \bigcup_{i \in I} C(a_i), \text{ where } \{a_i \mid i \in I\} \text{ is a subset of } G \text{ and}$$

for every $i \in I$, $C(a_i) = \{g \in G \mid g a_i = a_i g\}$, and where

(i) For all $i \in I$, $C(a_i)$ is a maximal cyclic subgroup of G.

(ii) $C(a_i) \cap C(a_j) = e$ if $i \neq j$.

(iii) If $e \neq x \in C(a_i)$, $e \neq y \in C(a_j)$ and $i \neq j$, then $G = [x, y]$.

(iv) I is an infinite set.

<u>Proof</u>: Suppose G has property P. Clearly $G = \bigcup_{g \in G} C(g)$. If H is a subgroup of G such that $C(g) \subsetneq H \subset G$, then H is cyclic and hence $H = C(g)$. Thus $C(g)$ is a maximal subgroup of G for every $e \neq g \in G$. $h \notin C(g)$, then $G = [h, C(g)]$, otherwise $[h, C(g)]$ would be a proper subgroup containing $C(g)$ properly. From this it follows that for every $g, h \in G$, $C(g) \cap C(h) = e$ or $C(g) = C(h)$. Thus we can choose a subset $\{a_i \mid i \in I\}$ of G such that $G = \bigcup_{i \in I} C(a_i)$, where each $C(a_i)$ is maximal and cyclic and where $C(a_i) \cap C(a_j) = e$ if $i \neq j$. It remains to prove (iii) and (iv).

(iii) Let $x \in C(a_i)$ and $y \in C(a_j)$, where $x \neq e$ and $y \neq e$ and $i \neq j$. If $[x, y] \neq G$, then $[x, y]$ is cyclic and generated by an element in $C(a_k)$ for some k. It then follows that $e \neq C(a_i) \cap C(a_k) \subsetneq Z(G)$ or $e \neq C(a_j) \cap C(a_k) \subsetneq Z(G)$.

(iv) I is infinite: For every $i \in I$, let $C(a_i) = [a_i']$. Since G is not periodic, let a'_1 be of infinite order and let $a_2' \neq e$ be such that $|a_2'| = n$ (a similar arguement will hold if $|a_2'| = \infty$) and $a_1' a_2' \neq a_2' a_1'$. Then $a_1' a_2' \notin [a_1']$, otherwise $a_1' a_2' = (a_1')^k$ hence $a_2' = (a_1')^{k-1}$, so either $a_2 = e$ or $Z(G) \neq e$ and both conclusions contradict the hypothesis.

Similarly $a_1' a_2' \in [a_2]$ and $(a_1')^k a_2' \notin [a_1']$ and $\notin [a_2']$ for all $k \geq 1$.

Hence $a_1' a_2' \in [a_3]$ (say) i.e. $a_1 a_2 = a_3^n$. Now $(a_1')^2 a_2' \notin [a_3']$, otherwise $(a_1')^2 a_2' = (a_3')^m$. Hence $a_1' a_1' a_2' = (a_3')^m$. Hence $a_1'(a_3')^n = (a_3')^m$. Hence $a_1' = (a_3')^{m-n}$ and this is a contradiction.

Similarly $(a_1')^k a_2' \notin [a_3']$ for all $k \geq 2$. Since $(a_1')^2 a_2' \notin [a_1'] \cup [a_2'] \cup [a_3']$, $(a_1')^2 a_2' \in [a_4']$ (say).

By a similar arguement $(a_1')^3 a_2' \notin [a_4'] \cup [a_3'] \cup [a_2'] \cup [a_1']$.

By induction it follows that for every k, $(a_1')^k a_2 \notin \bigcup_{i=1}^{k+1} [a_i']$.

Now a_1' is of infinite order, so we can have infinitely many $a_k' = (a_1')^k a_2'$. If $i \neq j$ then $a_i' a_j' \neq a_j' a_i'$ because if $(a_1')^i a_2'(a_1')^j a_2' = (a_1')^j a_2' (a_1')^i a_2'$ then $(a_1')^{i-j} a_2' = a_2'(a_1')^{i-j}$ i.e. a_2' commutes with $(a_1')^{i-j}$ and $(a_1')^{i-j} \in C(a_2')$. It follows that $(a_1')^{i-j} = e$ and so $(a_1')^i = (a_1')^j$ which contradicts $i \neq j$. Hence I is an infinite set.

Conversely, suppose that the conditions given in the theorem hold. Clearly G is non-cyclic. Let H be a proper subgroup of G and suppose $H \cap C(a_i) \neq e$ and $H \cap C(a_j) \neq e$, where $i \neq j$. Let $e \neq x \in H \cap C(a_i)$ and $e \neq y \in H \cap C(a_j)$. Then by (iii) $[x, y] = G$ and hence H is not a proper subgroup of G contrary to our choice of H. It follows $H \subseteq C(a_i)$ for some i and so H is cyclic since $C(a_i)$ is cyclic by (ii).

II.2.6 <u>Example</u>: The following is an example of infinite, non-abelian group which is the disjoint union of countably many cyclic groups. Let M be the group of 2 x 2 non-singular matrices, and let $G = [a, b]$, where $a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ be a subgroup of M. Then $ab = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and

$ba = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, thus $ab \neq ba$. It can be checked easily that $|a| = |b| = 2$, and that elements of G are of the form: $(ab)^k$, $(ba)^n$, $(ab)^k a$ or $(ba)^n b$, where k and n are arbitrary integers. Now $(ab)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and by induction $(ab)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ so ab is of infinite order.

$(ba)^2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$ and by induction $(ba)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ so ba is of infinite order also.

Moreover, $(ab)^k a = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -k \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & -k \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, hence $|(ab)^k a| = 2$.

And $(ba)^n b = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & n \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ hence $|(ba)^n b| = 2$.

All subgroups of order 2 are necessarily disjoint. An element of infinite order is of the form $(ab)^k$ or $(ba)^k$. Now $(ba)^k = ((ba)^{-1})^{-k} = (a^{-1} b^{-1})^{-k} = (ab)^{-k}$. So we have only one subgroup of infinite order namely $[ab]$. Now we prove that $[ab] \triangleleft G$.

$$(ab)^n a (ab^k a^{-1}(ab)^{-n} = (ab)^n (ba)^k (ab)^{-n} \in [ab]$$

and

$$(ab)^n b(ab)^k b^{-1}(ab)^{-n} = (ba)^n (ba)^k (ab)^{-n} \in [ab].$$

So for any $g \in G$, $g(ab)g^{-1} \in [ab]$. Hence $[a\, b] \triangleleft G$.

Now the number of subgroups of G of order 2 is infinite since $|(ab)^k a| = 2$ for every k and $(ab)^k a \neq (ab)^{k+1} a$ otherwise $aba = a$ and $ab = e$. It should be noticed that G does not have property P since $[(ab)^2, a]$ is non-cyclic (ab is of infinite order and a of finite order). Furthermore, $[(ab)^2, a]$ is proper. Otherwise $ab \in [(ab)^2, a]$, hence $ab = (ab)^{2k} a$ (Since $[ab] \triangleleft G$, $[(ab)^2] \triangleleft G$ and $[(ab)^2, a] = [(ab)^2][a]$). Hence $(ab)^{2k-1} = a$ which is a contradiction since ab is of infinite order and a of finite order. Hence G does not have property P.

CHAPTER III

GROUPS WITH CYCLIC HOMOMORPHIC IMAGES

In this chapter we shall be concerned with non-cyclic groups G with the property that every proper homomorphic image of G is cyclic. For abelian groups, it will be shown that the only group with this property is the direct sum of a group of prime order with itself. Non-abelian, finite groups with this property seem to form a large class of groups, for example all finite symmetric groups S_n with $n \geq 5$ and simple groups. We shall give a characterization for non-abelian finite solvable groups with the above property.

The notation for the abelian case (section III.1) is the same as in chapter I, and for the non-abelian case(section III.2) as in Chapter II. G' will denote the commutator subgroup of G, G'' the commutator subgroup of G' and so on.

II.1. <u>Finite Abelian Groups With Property Q</u>:

II.1.1 <u>Definition</u>: A non-cyclic group G is said to have property Q if and only if for any non-trivial, normal subgroup N of G, $G/_N$ is cyclic.

II.1.2 <u>Proposition</u>: A finite abelian group G has property Q if and only if G is isomorphic to $C_p \oplus C_p$ for some group of prime order p.

<u>Proof</u>: Suppose $G = C_p \oplus C_p$; then G is non-cyclic by

lemma I.2.1. Since every proper subgroup of G is of order 1 or p, it follows that any proper homomorphic image of G is of order p or 1 and hence cyclic.

Conversely, suppose G has property Q. Then by the fundamental theorem of finitely generated abelian groups [4], $G = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_k}$, where each C_{n_i} is cyclic of order n_i and n_i divides n_{i+1}. If $k \geq 3$, then $G/C_{n_3} = C_{n_1} \oplus C_{n_2} \oplus C_{n_4} \oplus \cdots \oplus C_{n_k}$ is non-cyclic since $(n_1, n_2) \neq 1$.. Moreover $k \neq 1$, otherwise G would be cyclic. Hence $k = 2$ and $G = C_{n_1} \oplus C_{n_2}$. Suppose that n_2 is not a. prime and let p be a prime such that $p \mid n_1$ and $p \mid n_2$. Let $m = \frac{n_2}{p}$ and let C_m be a subgroup of C_{n_2}. Then $G/C_m = C_{n_1} \oplus C_p$. But $C_{n_1} \oplus C_p$ is non-cyclic since $(n_1, p) = p \neq 1$. Hence $n_2 = p$ and $n_1 = n_2$, so $G = C_p \oplus C_p$.

III.1.4 <u>Lemma:</u> Every finitely generated abelian group with property Q is finite.

<u>Proof</u>: Let G be a finitely generated abelian group with property Q. By the basis theorem of finitely generated abelian groups [4], $G = [C_1] \oplus \cdots \oplus [C_r] \oplus [E_1] \oplus \cdots \oplus [E_n]$ where each C_i is of infinite order and $e_{v+1} \mid e_v$ $(v = 1, \ldots, n-1)$ $(|E_v| = e_v)$. Suppose G is not finite. Then $r \geq 1$; and since G is not cyclic, either $r > 1$ or $n \geq 1$. If $r > 1$, then $[2c_1]$ is a subgroup of G and $G/[2c_1] = [C_1]/[2C_1] \oplus \cdots \oplus [C_r] \oplus [E_1] \oplus \cdots \oplus [E_n]$. But $[C_1]/[2C_1]$ is of order 2. Thus $G/[2C_1]$ contains elements of finite and infinite order, hence not cyclic. Thus we may assume that $r = 1$ and $n \geq 1$. Let $m = e_1 e_2 \cdots e_n$. Then

$G/[mC_1] = [C_1]/[mC_1] \oplus [E_1] \oplus \cdots \oplus [E_n]$. Since $\left| C_1/[mC_1] \right| = m$,

$G/[mC_1]$ is not cyclic by lemma I.2.1. Thus the assumption that G is infinite contradicts the hypothesis that G has property Q. This completes the proof.

III.1.5 Lemma: No infinite abelian group has property Q.

Proof: Suppose G is an infinite abelian group with property Q. By III.1.4, we can assume that G is not finitely generated. Let G be generated by an infinite set S and assume that no finite subset of S generates G. Let $a_1 \neq e$ be in G and let $H_1 = [a_1]$. Since G is not finitely generated there is $a_2 \in G$ such that $a_2 \notin H_1$. Let $H_2 = [a_1, a_2]$; then $H_1 \subset H_2 \subset G$. Let $a_3 \in G$ such that $a_3 \notin H_2$. Let $H_3 = [a_1, a_2, a_3]$; then $H_1 \subset H_2 \subset H_3 \subset G$. Continuing in this way we can construct an infinite ascending chain of subgroups $H_1 \subset H_2 \subset \ldots \subset H_n \ldots$.

Suppose G has property Q. Then G/H_1 is cyclic. And, by the second isomorphism theorem [4], G/H_1 has an infinite ascending chain of subgroups $\bar{H}_2 \subset \bar{H}_3 \subset \ldots \subset \bar{H}_n \subset \ldots$. Let $\bar{a}$ be a generator of G/H_1 and for every n, let $\bar{h}_n$ be a generator $\bar{H}_n$. Then each $h_n = (a)^{k_n}$ for some k_n. Since $\bar{H}_2 \subset \bar{H}_n$ for every $n > 2$, we have $k_2 > k_n$, for every $n > 2$. This contradiction completes the proof. We summerize the forgoing results in the following theorem:

3.I.6 Theorem: An abelian group G has property Q if and only if G is the direct sum of a group of prime order with itself.

III.2 Finite non-abelian groups with Property Q:

In this section we shall give some examples of finite non-abelian groups with property Q. Then we shall give a characterization of solvable groups with property Q.

Examples: (i) The symmetric group S_n has property Q, for all $n \geq 5$. In this case A_n, the alternating group, is the only non-trivial normal subgroup of G. But $|G/A_n| = 2$, so G/A_n is cyclic. Therefore S_n has property Q for all $n \geq 5$.

(ii) A non-abelian group G of order pq has property Q. Since G is non-cyclic, only one sylow subgroup is normal, say H of order p. Then G/H is of prime order and hence cyclic.

(iii) Simple non-abelian groups have property Q since they do not have nontrivial normal subgroups.

In proposition II.1.3. we proved that if G is non-abelian and $H \subseteq Z(G) \neq e$, then G/H has property P; in particular G/H is non-cyclic. Clearly in this case G does not have property Q. We state this as a lemma for reference.

III.2.1 Lemma: Let G be a non-abelian group with $Z(G) \neq e$. Then G does not have property Q.

III.2.2 Corollary: No p-group has property Q.

Now we give a characterization of solvable groups with property Q. First we recall the following definition and theorem [2]:

III.2.3 Definition: Let H and K be two groups and suppose that for every $h \in H$ there exists an automorphism τ_h of K such $\tau_{h_2}(\tau_{h_1}(k)) = \tau_{h_1h_2}(k)$ for every $k \in K$. Then the symbols (h, k), $h \in H$, $k \in K$ form a group under the product rule

$$(h_1, k_1)\cdot(h_2, k_2) = (h_1h_2, \tau_{h_2}(k_1)k_2)$$

called the semidirect of K by H.

III. 2.4 <u>Theorem</u>: G is the semidirect of K by H if and only if

(i) $K \triangleleft G$

(ii) $G = HK$.

(iii) $H \cap K = e$.

III. 2.5 <u>Theorem</u>: Let G be a non-abelian solvable group of order $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then G has property Q if and only if G is the semidirect product of a group H of order $P_i^{\alpha_i}$ for one $i = 1, 2, \ldots, k$. and a cyclic subgroup M of order $p_1^{e_1} p_2^{e_2} \ldots p_i^{e_i-\alpha_i} \ldots p_k^{e_k}$, where (i) H is abelian of type (1, 1, ..., 1). (ii) H is a normal subgroup of G which is contained in every other non-trivial normal subgroup of G.

<u>Proof</u>: Suppose G has property Q. Since $G_1'' \triangleleft G$, $G'' = e$ or G/G'' is cyclic. Suppose $G'' \neq e$; then $G/_{G''}$ is cyclic. Hence $G'' \supseteq G'$. Hence $G'' = G'$ contradicting the solvability of G. Hence $G'' = e$ and G' is abelian. If $e \neq K \triangleleft G$, then $G/_K$ is cyclic and so $K \supseteq G'$ i.e. G' is contained in every normal, nontrivial subgroup of G. We prove now that G' is of order $P_i^{\alpha_i}$ and type (1, 1, ..., 1).

Suppose $|G'| = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Let P_i be the p_i-sylow subgroup of G' for all $i = 1, \ldots, k$. $P_i \triangleleft G'$ (G' is abelian) and $G' \triangleleft G$. Now for every $g \in G$, $g P_i g^{-1} \subseteq G'$. But $|gP_i g^{-1}| = p_i^{\alpha_i}$ and P_i is the only subgroup of G' of order $p_i^{\alpha_i}$. Hence $gP_i g^{-1} = P_i$ and $P_i \triangleleft G$ for all $i = 1, \ldots, k$. Since every normal subgroup of G contains G', it follows that G' has only one sylow subgroup, thus $G' = P_i$ for some i, $1 \leq i \leq k$. Consider $C = \{g \mid g \in G', |g| \leq p_i\}$.

C is a subgroup of G, since G' is abelian. We now prove that $C \triangleleft G$. Let $c \in C$ and $g \in G$; then $|gcg^{-1}| = |c| = p_i$. It follows that $gCg^{-1} \subseteq C$ and consequently $C \triangleleft G$. Hence $C \supseteq G'$ and consequently $G' = C$, since C is a subgroup of G'. Therefore G' is an abelian p_i-group with no element of order greater than p_i. Hence G' is of order $p_i^{\alpha_i}$ and type (1, 1, ..., 1).

We prove now that G is the semidirect product of G' and a cyclic subgroup of order $p_1^{e_1} \ldots p_i^{e_i - \alpha_i} \ldots p_k^{e_k}$. Now G/G' is cyclic and of order $p_1^{e_1} \ldots p_i^{e_i-\alpha_i} \ldots p_k^{e_k}$. Let $G/G' = [aG']$. Hence (aG')

$$(aG')^{p_1^{e_1} \ldots p_i^{e_i-\alpha_i} \ldots p_k^{e_k}} = G' \text{ i.e. } a^{p_1^{e_1} \ldots p_i^{e_i-\alpha_i} \ldots p_k^{e_k}} \in G'.$$

Consider $[G', a]$ and suppose it is a proper subgroup of G. Let $e \neq b \notin [G', a]$. It follows that $bG' = (aG')^k$ for some k. Hence $ba^{-k} \in G'$. Hence $b \in [G', a]$ since $a^k \in [G', a]$ and this is a contradiction. Hence $[G', a] = G$. Now $G' \cap [a] = e$, otherwise $e \neq G' \cap [a] \subseteq Z(G)$ since any element in $G' \cap [a]$ commutes with any element in G' and with a. Thus $Z(G) \neq e$ contradicting Lemma III.3.1. It follows that G is the semidirect product of G' and a and this completes the proof in this direction. Conversely, let G satisfy the hypothesis of the theorem. Now G/H is cyclic since $|G/H| = p_1^{e_1} \ldots p_i^{e_i - \alpha_i} \ldots p_k^{e_k}$ and aH (where a is the generator of M) is of order $p_1^{e_1} \ldots p_i^{e_i-\alpha_i} \ldots p_k^{e_k}$. Let $e \neq N$ be a proper normal subgroup of G. By (ii) $N \supseteq H$. Hence by the second isomorphism theorem $\frac{G/H}{N/H} \cong G/N$. Therefore G/N is cyclic since it is the homorphic image of a cyclic group. Hence G has property Q.

REFERENCES

1. Carmichael, R.D., Introduction to the theory of groups of finite order.

2. Hall, M., Jr., The Theory of Groups, The Macmillan Co., New York, 1959.

3. Kurosh, A. G., The Theory of Groups, Vols. 1 and 2, translated, Chelsea Publishing Co., New York, 1955.

4. Ledermann, W., Introduction to the Theory of Finite Groups, Oliver and Boyd, 1961.

5. Miller, G.A., Blichfeldt, H.F., Dickson, L. E., Theory and application of Finite Groups, Dover Publications, Inc., New York, 1961.

6. Schenkman, E., Group Theory, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1965.