# The Influence of Subgroup Structure on Finite Groups Which are the Product of Two Subgroups

by

Andrew Summers

Submitted in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in the

Mathematics

Program

YOUNGSTOWN STATE UNIVERSITY

May, 2021

**The Influence of Subgroup Structure on Finite Groups Which are the Product of Two Subgroups**

Andrew Summers

I hereby release this thesis to the public. I understand that this thesis will be made available from the OhioLINK ETD Center and the Maag Library Circulation Desk for public access. I also authorize the University or other individuals to make copies of this thesis as needed for scholarly research.

Signature:

Andrew M. Summers, Student | Date

Approvals:

Dr. Neil Flowers, Thesis Advisor | Date

Dr. Thomas Madsen, Committee Member | Date

Dr. Thomas Wakefield, Committee Member | Date

Dr. Salvatore A. Sanders, Dean of Graduate Studies | Date

**The Influence of Subgroup Structure on Finite Groups Which are the Product of Two Subgroups**


**Abstract**

In group theory, it is often the case that a group can be written as the product of two of its subgroups. Take for example $S_3$, the symmetric group on a set of three elements, which can be written as $S_3 = A_3\langle(12)\rangle$ or alternatively $D_4$, the group of symmetries of a square, which can be written as $D_4 = \langle(1234)\rangle\langle(13)\rangle$. It is therefore natural to wonder what influence the structures of these subgroups have on the structure of the group as a whole.

For example, if $G$ is a group, $H \leq G$ and $K \leq G$ such that $G = HK$, where both $H$ and $K$ are cyclic, one may ask if $G$ is consequently cyclic as well. Moreover, if $G$ is not cyclic, then what, if anything, can be said about its structure? In actuality, it happens that $G$ is, in fact, not cyclic, but solvable. In this master's thesis we establish several important classes of groups which will be used to explore the influence of subgroup structure on groups which are the product of two subgroups. Additionally, we will lead up to the strongest possible statement about the structure of such groups, without placing additional constraints on $H$ and $K$. This result was originally proved by Helmut Wielandt in 1958 under the assumption that the orders of $H$ and $K$ were coprime. These assumptions were later dropped in an improved result by Otto Kegel in 1961.

# Table Of Contents

# Preliminary Results

In order to explore the influence of subgroup structure as completely as possible, we will call on the use of many definitions and theorems. While a majority of these will be provided in the coming pages, some are so integral to any group theoretic argument that they are presumed to be known by the reader. Thus, several well-known definitions and results will be stated in this section with their proofs omitted. We will begin with the isomorphism theorems.

The isomorphism theorems, which have variations for groups, rings, vector spaces, etc. are some of the most widely used results in algebra, which detail the relationships between groups, images under homomorphisms, normal subgroups and quotient groups. The results of the First, Second, and Third Isomorphism Theorems, along with related results, are given here.

**Theorem 1.1.1** (First Isomorphism Theorem)**.**
*Let $G_1$ and $G_2$ be groups and $\phi : G_1 \longrightarrow G_2$ be a homomorphism.*
*Then*

$$\frac{G_1}{Kern(\phi)} \cong \phi(G_1).$$

**Theorem 1.1.2** (Second Isomorphism Theorem)**.**
*Let $G$ be a group, $H \leq G$ and $N \trianglelefteq G$.*
*Then*

$$\frac{HN}{N} \cong \frac{H}{H \cap N.}$$

**Theorem 1.1.3** (Third Isomorphism Theorem)**.**
*Let $G$ be a group, $H \trianglelefteq G$, and $N \trianglelefteq G$ such that $N \leq H$.*
*Then*

$$\frac{G/N}{H/N} \cong \frac{G}{H}.$$

The following lemma, while not an isomorphism theorem, identifies two characteristics of what will be referred to as the natural map, so named for the natural way in which it is defined by the relationship between a group and one of its normal subgroups. This map will be used at several points throughout the coming arguments, including in the statement of Theorem 1.1.5. This theorem is occasionally referred to as the Fourth Isomorphism Theorem or the Correspondence Theorem.

**Lemma 1.1.4.**
*Let $G$ be a group and $N \trianglelefteq G$. Define $\phi : G \longrightarrow G/N$ by $\phi(g) = gN, \ \forall\, g \in G$.*
*Then:*

1. *The natural map is a homomorphism;*
2. *$Kern(\phi) = N$.*

*Proof.* For 1, let $g_1, g_2 \in G$. Then $\phi(g_1 g_2) = g_1 g_2 N = g_1 N g_2 N = \phi(g_1)\phi(g_2)$ and so the natural map is a homomorphism.

For 2, let $g \in Kern(\phi)$. Then $\phi(g) = gN = 1N$ if and only if $1^{-1}g \in N$. But this occurs if and only if $g \in N$. Thus $Kern(\phi) = N$.

□

Using the results established in Lemma 1.1.4, we can now state the correspondence theorem.

**Theorem 1.1.5** (Correspondence Theorem)**.**
*Let $G$ be a group, $N \trianglelefteq G$ and $H \leq G$. Let $\phi$ denote the natural map from Lemma 1.1.4.*
*Then:*

1. $\phi(H) = HN/N$;

2. $\phi^{-1}(HN/N) = HN$;

3. *If $L \leq G/N$, then there exists $N \leq K \leq G$ such that $L = K/N$.*

**Remark.** *Note that the Correspondence Theorem provides two useful results regarding images and preimages under the natural map. Additionally, the third statement gives insight into the structure of quotient groups. Namely that any subgroup of a quotient group is itself a quotient group, formed from a subgroup of $G$ containing the normal subgroup $N$. We will utilize the result regarding preimages many times and will refer to Theorem 1.1.5 simply by saying "taking preimages".*

Another class of theorems which are of vital importance to group theory are the Sylow Theorems, named after Norwegian mathematician Peter Ludwig Sylow. These theorems explore the existence and number of "Sylow $p$-subgroups" of a group $G$, so named for their specific order in relation to the order of $G$. The first of the three Sylow theorems will now be stated.

**Theorem 1.1.6** (Sylow's First Theorem)**.**
*Let $G$ be a group and $p$ be a prime. Then $Syl_p(G)$ is non-empty.*

We will now establish a notation for conjugation which will prove useful for both a consequence of Sylow's Second Theorem, and throughout the upcoming sections.

**Definition 1.1.7** (Exponential Notation for Conjugation)**.**
*Let $G$ be a group, $a, b \in G$, and $H \leq G$.*
*Then:*

1. $b^a = a^{-1}ba$;

2. $H^a = a^{-1}Ha = \{a^{-1}ha \mid h \in H\}$.

**Remark.** *Under this notation, for a group $G$ with $a, b, g \in G$, it follows that $(ab)^g = a^g b^g$. This ability to write the conjugate of a product as the product of conjugates will prove useful in a variety of arguments.*

**Theorem 1.1.8** (Sylow's Second Theorem)**.**
*Let $G$ be a group, $p$ be a prime, and $H \leq G$ be a $p$-subgroup. Then there exists $P \in Syl_p(G)$ such that $H \leq P$.*

**Remark.** *Note that as a consequence of Sylow's second theorem, if $H$ is, in fact, a Sylow $p$-subgroup of $G$, then $H = P^g$ for some $g \in G$, thus making all Sylow $p$-subgroups conjugates of one another.*

This fact proves vital in another important result known as the Frattini argument, which was named for Italian mathematician Giovanni Frattini, and whose proof is included at the end of this section.

**Theorem 1.1.9** (Sylow's Third Theorem)**.**
*Let $G$ be a group, $p$ be a prime, $P \in Syl_p(G)$, and $n_p = |Syl_p(G)|$.*
*Then:*

1. $n_p = \dfrac{|G|}{|N_G(P)|}$;
2. $n_p \mid |G|$;
3. $n_p \equiv 1(mod\ p)$.

**Remark.** *The combination of these three statements proves vital in determining the structure of many finite groups and the Sylow $p$-subgroups they contain.*

For example, we include the following useful corollary.

**Corollary 1.1.10** (Unique Sylow $p$-subgroups are Normal)**.**
*Let $G$ be a group, $p$ be a prime, and $P \in Syl_p(G)$ such that $P$ is the only Sylow $p$-subgroup. Then $P \trianglelefteq G$.*

*Proof.* Since $P$ is unique, it follows that $n_p = |Syl_p(G)| = 1$. Thus, by Sylow's third theorem, we have $1 = \dfrac{|G|}{|N_G(P)|}$ or $|N_G(P)| = |G|$. As previously noted, $N_G(P) \leq G$ and so it must be that $N_G(P) = G$. Thus, $P^g = P$ for every $g \in G$, implying $P \trianglelefteq G$.

□

The Frattini argument can now be stated and proved.

**Theorem 1.1.11** (Frattini Argument)**.**

*Let $G$ be a group, $N \trianglelefteq G$, and $P \in Syl_p(N)$. Then $G = N_G(P)N$.*

*Proof.* Now $P \leq N$ since $P \in Syl_p(N)$. Also, since $N \trianglelefteq G$, we have that $N^g = N$. Thus $P \leq N$ implies that $P^g \subseteq N$ for all $g \in G$.

Since $G$ is a group, $G$ is non-empty and so there exists $g, g^{-1} \in G$. Similarly, since $P \leq N$, $P$ is non-empty since $1 \in P$. Thus $1 = 1^g \in P^g$ and so $P^g$ is non-empty.

Let $p_1^g, p_2^g \in P^g$. Then

$$\begin{aligned} p_1^g (p_2^g)^{-1} &= p_1^g p_2^{g^{-1}} \\ &= g^{-1} p_1 1 p_2 g \\ &= (p_1 p_2)^g \\ &= p^g \text{ (where } p_1 p_2 = p \in P\text{, by closure of } P). \end{aligned}$$

Thus $p^g \in P^g$ and so $P^g \leq N$. Additionally, note that $|P^g| = |P| = |N|_p$, yielding $P^g \in Syl_p(N)$.

As noted earlier, all Sylow $p$-subgroups are conjugate to one another, so there exists $n \in N$ such that $P^g = P^n$ or $P^{gn^{-1}} = P$. Thus, $gn^{-1} \in N_G(P)$, and so $g \in N_G(P)N$. Since $g \in G$ was chosen arbitrarily, we have that $G \leq N_G(P)N$. But $N_G(P) \leq G$ and $N \trianglelefteq G$, so it follows that $N_G(P)N \leq G$, yielding that $G = N_G(P)N$.

□

To conclude the section, a few additional results in basic group theory will be stated.

**Theorem 1.1.12.**

*Let $G$ be a group and $p$ be a prime such that $|G| = p^2$. Then $G$ is abelian.*

**Theorem 1.1.13.**

*Let $G$ be a $p$-group for some prime $p$ and $S$ be a set such that $G$ acts on $S$. If $p$ does not divide $|S|$, then there exists $x \in S$ such that $G_x = G$.*

**Theorem 1.1.14** (Quotients of Cyclic Groups are Cyclic)**.**

*Let $G$ be a cyclic group and $H \leq G$. Then $G/H$ is cyclic.*

**Theorem 1.1.15.**

*Let $G = \langle a \rangle$ be a cyclic group and $d \in \mathbb{Z}^+$ such that $d \mid |G|$. Then there exists a unique $H \leq G$ such that $|H| = d$.*

**Theorem 1.1.16** (Lagrange's Theorem)**.**

*Let $G$ be a group and $H \leq G$. Then $|H| \mid |G|$ and $|G|/|H|$ is the number of distinct left cosets of $H$ in $G$.*

With these results established, the class of solvable groups can now be defined and explored.

# Solvable Groups

The first class of groups we will examine is that of solvable groups, which are so named for their relationship to Galois theory and, more specifically, the proof that a general fifth degree polynomial equation is not solvable by radicals. We will first explore some conditions for the solvability of a group, and then establish a canonical series of subgroups which can be used to determine whether or not any group is solvable.

## 2.1 Solvability

**Definition 2.1.1** (Solvable Group)**.**
*Let $G$ be a group. $G$ is said to be solvable if there exists a subnormal series:*

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1$$

*where $n \in \mathbb{Z}^+ \cup \{0\}$ and each factor, $G_i/G_{i+1}$, is abelian, for all $0 \leq i \leq n-1$.*

**Example** ($S_3$ is solvable)**.**
*Note that $S_3 \trianglerighteq A_3 \trianglerighteq 1$ is a subnormal series where $S_3/A_3 \cong \mathbb{Z}_2$ and $A_3/\{1\} \cong \mathbb{Z}_3$, both of which are abelian. Therefore $S_3$ is a solvable group.*

We will now examine several conditions under which $G$ and related groups are solvable.

**Theorem 2.1.2** (Abelian Groups are Solvable)**.**

*Let $G$ be an abelian group. Then $G$ is solvable.*

*Proof.* Let $G$ be an abelian group. Then $G \trianglerighteq 1$ is a subnormal series and $G/\{1\} \cong G$, which is abelian. Thus $G$ is solvable.

$\square$

**Theorem 2.1.3** ($p$-groups are Solvable)**.**

*Let $G$ be a $p$-group for some prime $p$. Then $G$ is solvable.*

*Proof.* We will proceed by induction on $|G|$. If $|G| = 1$, then $G$ is abelian and therefore solvable by Theorem 2.1.2. Suppose now that the theorem holds for all $p$-groups of order less than $|G|$.

Since $G$ is a $p$-group, $Z(G) \neq 1$. Also, $Z(G) \trianglelefteq G$ and so $G/Z(G)$ is a group. Moreover, since $G$ is a $p$-group, it follows that $|G/Z(G)| = \dfrac{|G|}{|Z(G)|}$ is a power of $p$ and so $G/Z(G)$ is also a $p$-group. Additionally, since $|G/Z(G)| = \dfrac{|G|}{|Z(G)|} < |G|$, by assumption $G/Z(G)$ is solvable. Thus, there exists a subnormal series:

$$\frac{G}{Z(G)} = G_0 \trianglerighteq \frac{G_1}{Z(G)} \trianglerighteq \frac{G_2}{Z(G)} \trianglerighteq \cdots \trianglerighteq \frac{G_n}{Z(G)} = 1,$$

where $n \in \mathbb{Z}^+ \cup \{0\}$ and

$$\frac{G_i/Z(G)}{G_{i+1}/Z(G)}$$

is abelian for all $0 \leq i \leq n-1$.

Taking preimages of each factor yields

$$G \trianglerighteq G_1 \trianglerighteq G_2 \cdots \trianglerighteq Z(G)$$

which is a subnormal series in $G$ which terminates at the center. But then

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \cdots \trianglerighteq Z(G) \trianglerighteq 1$$

is also a subnormal series in $G$. By the Third Isomorphism Theorem we have

$$G_i/G_{i+1} \cong \frac{G_i/Z(G)}{G_{i+1}/Z(G)}$$

which is abelian for each $0 \leq i \leq n-2$. Also note that $Z(G)/\{1\} \cong Z(G)$ which is abelian as well. Thus $G$ is solvable.

□

**Theorem 2.1.4** (Quotients of Solvable Groups are Solvable).
*Let $G$ be a solvable group and $N \trianglelefteq G$. Then $G/N$ is solvable.*

*Proof.* Since $G$ is solvable, there exists a subnormal series:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = 1$$

such that $n \in \mathbb{Z}^+ \cup \{0\}$ and $G_i/G_{i+1}$ is abelian for all $0 \leq i \leq n-1$.
Let $\overline{G} = G/N$. Then

$$\overline{G} = \overline{G_0} \trianglerighteq \overline{G_1} \trianglerighteq \cdots \trianglerighteq \overline{G_n} = 1$$

is a subnormal series as well.

Also

$$\begin{aligned}
\frac{\overline{G_i}}{\overline{G_{i+1}}} &= \frac{G_iN/N}{G_{i+1}N/N} \\
&\cong \frac{G_iN}{G_{i+1}N}, \quad \text{by the Third Isomorphism Theorem} \\
&= \frac{G_iG_{i+1}N}{G_{i+1}N}, \quad \text{since } G_{i+1} \leq G_i \\
&\cong \frac{G_i}{G_i \cap G_{i+1}N}, \quad \text{by the Second Isomorphism Theorem.}
\end{aligned}$$

Note also that for any $x \in G_{i+1}$ and any $y \in G_i \cap G_{i+1}N$, then $x^y \in G_{i+1}$ and so $G_{i+1} \trianglelefteq G_i \cap G_{i+1}N$. Thus by the Third Isomorphism Theorem:

$$\frac{G_i}{G_i \cap G_{i+1}N} \cong \frac{G_i/G_{i+1}}{G_i \cap G_{i+1}N/G_{i+1}}$$

which is abelian since $G_i/G_{i+1}$ is abelian and $G_i \cap G_{i+1}N/G_{i+1} \trianglelefteq G_i/G_{i+1}$. Therefore each $\overline{G_i}/\overline{G_{i+1}}$ is abelian and so $\overline{G} = G/N$ is solvable.

□

**Theorem 2.1.5** (Solvable Quotients and Normal Subgroups Yield Solvable Groups)**.**
*Let $G$ be a group and $N \trianglelefteq G$ such that $G/N$ and $N$ are solvable. Then $G$ is solvable.*

*Proof.* Let $\overline{G} = G/N$. Since $\overline{G}$ and $N$ are solvable, there exist the following subnormal series:

$$\overline{G} = \overline{G_0} \trianglerighteq \overline{G_1} \trianglerighteq \cdots \trianglerighteq \overline{G_n} = 1$$

and

$$N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_m = 1$$

such that $\overline{G_i}/\overline{G_{i+1}}$ and $N_j/N_{j+1}$ are abelian for all $0 \leq i \leq n-1$ and $0 \leq j \leq m-1$, where $m, n \in \mathbb{Z}^+ \cup \{0\}$.

Note now that by part two of the Correspondence Theorem (Theorem 1.1.5), the preimage of $\overline{G_n}$ is $N$. Thus, taking preimages of the first subnormal series yields

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots G_{n-1} \trianglerighteq N$$

which can be combined with the second subnormal series to create the following subnormal series:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots G_{n-1} \trianglerighteq N \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_m = 1.$$

Now by the Third Isomorphism Theorem, $G_i/G_{i+1} \cong \frac{G_i/N}{G_{i+1}/N} = \overline{G_i}/\overline{G_{i+1}}$, which is abelian for each $0 \leq i \leq n-1$. Thus $G$ is solvable.

□

Lastly, we will identify two cases in which a group is solvable based on the prime factorization of its order.

**Theorem 2.1.6.**

*Let $G$ be a group such that $|G| = pq$, where $p, q$ are both prime and $p < q$. Then $G$ is solvable.*

*Proof.* Consider $Syl_q(G)$, where $n_q = |Syl_q(G)|$. By Sylow's Third Theorem, $n_q||G|$. Thus since both $p$ and $q$ are prime, we have that $n_q = 1, p, q,$ or $pq$.

Also by Sylow's Third Theorem, $n_q \equiv 1(\text{mod } q)$. Note that $q \equiv 0(\text{mod } q)$, $pq \equiv 0(\text{mod } q)$, and $p \equiv p(\text{mod } q)$ since $p < q$. Thus, it must be that $n_q = 1$. Let $Q \in Syl_q(G)$ be the unique Sylow $q$-subgroup of $G$. Then by Corollary 1.1.10, $Q \trianglelefteq G$.

Since $1$ is normal in all groups, we have that $1 \trianglelefteq Q \trianglelefteq G$. Then, since $q$ is prime, $Q/\{1\} \cong \mathbb{Z}_q$, which is abelian. Additionally, $|G/Q| = |G|/|Q| = pq/q = p$. Thus, since $p$ is also prime, $G/Q \cong \mathbb{Z}_p$, which is abelian as well.

Hence $G \trianglerighteq Q \trianglerighteq 1$ is a subnormal series with abelian factors, and so $G$ is solvable.

□

**Theorem 2.1.7.**

*Let $G$ be a group such that $|G| = p^2q$, where $p$ and $q$ are distinct primes. Then $G$ is solvable.*

*Proof.* Note that since $p$ and $q$ are distinct primes, either $p < q$ or $q < p$.

Case 1: $(q < p)$

Assume $q < p$ and consider the possible values for $n_p$. By Sylow's Third Theorem $n_p|\ |G|$ and so $n_p = 1, p, p^2, q, pq,$ or $p^2q$. Additionally, $n_p \equiv 1(\text{ mod } p)$ which reduces the possible values to $1$ or $q$, since all others are equivalent to $0$ modulo $p$.

First, suppose $n_p = 1$ and let $P \in Syl_p(G)$ be the unique Sylow $p$-subgroup of $G$. By Corollary 1.1.10, we have that $P \trianglelefteq G$. Also, $|G/P| = |G|/|P| = p^2q/p^2 = q$. Thus, since $q$ is prime, $G/P \cong \mathbb{Z}_q$ which is abelian.

Note that $|P| = |G|_p = p^2$, meaning $P$ is a $p$-group and therefore solvable by Theorem 2.1.3. Thus, there exists a subnormal series

$$P = P_0 \trianglerighteq P_1 \trianglerighteq \cdots \trianglerighteq P_{n-1} \trianglerighteq P_n = 1$$

such that $P_i/P_{i+1}$ is abelian for all $0 \leq i \leq n-1$.

Then

$$G \trianglerighteq P \trianglerighteq P_1 \trianglerighteq \cdots \trianglerighteq P_{n-1} \trianglerighteq 1$$

is the desired subnormal series, and so $G$ is solvable.

Suppose now that $n_p = q$. Then $q \equiv 1(\mod p)$ by Sylow's Third Theorem, and so $q - 1 \equiv 0(\mod p)$, meaning $p|q-1$. But $q < p$, so $q - 1 < p$. Thus, it must be that $q - 1 = 0$, since $q = n_p \geq 1$. But then $q = 1$, which is a contradiction since $q$ is prime. Thus $n_p \neq q$ and the case is complete.

Case 2: $(p < q)$

Assume now that $p < q$ and consider the possible values of $n_q$. By Sylow's Third Theorem and the fact that $p < q$, either $n_q = 1$ or $n_q = p^2$.

Suppose that $n_q = 1$ and let $Q \in Syl_q(G)$ be the unique Sylow $q$-subgroup of $G$. Again, by Corollary 1.1.10, $Q \trianglelefteq G$. Also, $1 \trianglelefteq Q$ and, since $q$ is prime, $Q/\{1\} \cong \mathbb{Z}_q$, which is abelian. Additionally, $G/Q$ is a group and $|G/Q| = |G|/|Q| = p^2q/q = p^2$. Thus since $G/Q$ is a group of order $p^2$, $G/Q$ is abelian by Theorem 1.1.12, which implies that $G \trianglerighteq Q \trianglerighteq 1$ is the desired subnormal series and so $G$ is solvable.

Finally, suppose $n_q = p^2$. Recall that each Sylow $q$-subgroup has order $|G|_q = q$. Thus, since each distinct Sylow $q$-subgroup intersects the others trivially, there are $p^2(q-1) = p^2q - p^2 = |G| - p^2$ non-identity elements contained in some Sylow $q$-subgroup of $G$.

Now by Sylow's First Theorem, there exists $P \in Syl_p(G)$ with $|P| = |G|_p = p^2$. Let $Q \in Syl_q(G)$ and consider $P \cap Q$. Since $P \cap Q \leq P$ and $P \cap Q \leq Q$, it follows from Lagrange's Theorem that $|P \cap Q| \mid |P|$ and $|P \cap Q| \mid |Q|$. Thus, $P \cap Q = \{1\}$ since $p$ and $q$ are coprime. Hence all Sylow $p$-subgroups and Sylow $q$-subgroups intersect trivially. It follows necessarily that $n_p = 1$ and so $P \trianglelefteq G$ by Corollary 1.1.10.

Since $P$ is a $p$-group, it is solvable by Theorem 2.1.3. Thus, there exists a subnormal series

$$P = P_0 \trianglerighteq P_1 \trianglerighteq \cdots \trianglerighteq P_{n-1} \trianglerighteq P_n = 1$$

such that $P_i/P_{i+1}$ is abelian for all $0 \leq i \leq n-1$, where $n \in \mathbb{Z}^+ \cup \{0\}$. Additionally, $|G/P| =$

$|G|/|P| = p^2q/p^2 = q$. Thus $G/P \cong \mathbb{Z}_q$, which is abelian. Hence

$$G \trianglerighteq P \trianglerighteq P_1 \trianglerighteq \cdots \trianglerighteq P_{n-1} \trianglerighteq P_n = 1$$

is the desired subnormal series, and so $G$ is solvable.

□

## 2.2 Commutators and the Derived Series

While solvable groups are an important class of groups which are used in a wide variety of arguments, it can often be tedious to construct the necessary subnormal series. This is especially true if little is known about the group's structure. Thus, it is desirable to identify a canonical series which characterizes the solvability of a given group.

In this section, such a series will be defined, along with several properties regarding the subgroups from which the series is built.

**Definition 2.2.1** (The Subgroup Generated by a Set).
*Let $G$ be a group and $S$ be a non-empty subset of $G$. Then the subgroup generated by $S$ is given by*

$$\langle S \rangle = \{s_1^{n_1} s_2^{n_2} s_3^{n_3} \cdots s_k^{n_k} : s_i \in S, n_i \in \mathbb{Z}, \textit{ for all } 1 \leq i \leq k,\ k \in \mathbb{Z}^+\}.$$

As defined, it is not necessarily clear that $\langle S \rangle$ forms a subgroup. This will now be proven.

**Theorem 2.2.2** ($\langle S \rangle$ is a Subgroup).
*Let $G$ be a group and $S$ be a non-empty subset of $G$. Then $\langle S \rangle \leq G$.*

*Proof.* Let $s \in S$. Then $s = s^1 \in \langle S \rangle$ and so $\langle S \rangle$ is non-empty.

Now let

$$s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k},\ r_1^{m_1} r_2^{m_2} \cdots r_l^{m_l} \in \langle S \rangle,$$

where $s_i \in S$ for all $1 \leq i \leq k$, $r_j \in S$ for all $1 \leq j \leq l$, $n_i, m_j \in \mathbb{Z}$ for each $i$ and $j$, and $k, l \in \mathbb{Z}^+$.

Then

$$(s_1^{n_1}s_2^{n_2}\cdots s_k^{n_k})(r_1^{m_1}r_2^{m_2}\cdots r_l^{m_l})^{-1} = s_1^{n_1}s_2^{n_2}\cdots s_k^{n_k}r_l^{-m_l}r_{l-1}^{-m_{l-1}}\cdots r_1^{-m_1} \in \langle S\rangle.$$

Thus $\langle S\rangle \leq G$ by the subgroup test.

□

**Example** (Computing $\langle 2,6\rangle \leq \mathbb{Z}_8$)**.**
*Consider $\mathbb{Z}_8$ and $S = \{2,6\} \subseteq \mathbb{Z}_8$. Note that $\langle 2,6\rangle \leq \mathbb{Z}_8$ must contain $0$. Additionally $2 = 2^1 \in \langle 2,6\rangle$ and $6 = 2^3 \in \langle 2,6\rangle$. Since $6 = 2^3$, it follows that any product of powers of $2$ and $6$ will, in fact, simply be a product of powers of $2$.*

*Thus $\langle 2,6\rangle = \langle 2\rangle = \{0,2,4,6\}$.*

This concept of generating a subgroup from a set of elements will now prove useful in defining an important canonical subgroup.

**Definition 2.2.3** (Commutators)**.**
*Let $G$ be a group, $a,b \in G$, $H \leq G$ and $K \leq G$.*
*Then:*

1. *The commutator of $a$ and $b$ is given by $[a,b] = a^{-1}b^{-1}ab$;*

2. *The commutator subgroup generated by $H$ and $K$ is given by $[H,K] = \langle [h,k] : h \in H, k \in K\rangle$;*

3. *The commutator subgroup of $G$ is given by $G' = \langle [x,y] : x,y \in G\rangle$.*

Note that $G'$ is often referred to as the derived subgroup of $G$ as well. Several properties of commutators and the derived subgroup will now be explored.

**Theorem 2.2.4** (Commutator Calculus)**.**

*Let $G$ be a group, $a, b, c \in G$, $H \leq G$, and $K \leq G$.*

*Then:*

1. $[a, b]^c = [c, a][a, bc]$;
2. $[a, b]^c = [ac, b][b, c]$;
3. $[a, b]^c = [a^c, b^c]$;
4. $[a, b]^{-1} = [b, a]$;
5. $[a, bc] = [a, c][a, b]^c$;
6. $[ab, c] = [a, c]^b[b, c]$;
7. $[a, b] = 1$ *if and only if* $ab = ba$;
8. *If* $a \in C_G(b)$, *then* $[a, bc] = [a, c]$;
9. *If* $a \in C_G(b)$, *then* $[ac, b] = [c, b]$.

*Proof.* For 1, let $[a, b] \in G'$.

Then

$$\begin{aligned}
[c, a][a, bc] &= (c^{-1}a^{-1}ca)(a^{-1}(bc)^{-1}a(bc)) \\
&= c^{-1}a^{-1}caa^{-1}c^{-1}b^{-1}abc \\
&= c^{-1}a^{-1}cc^{-1}b^{-1}abc \\
&= c^{-1}a^{-1}b^{-1}abc \\
&= c^{-1}[a, b]c \\
&= [a, b]^c.
\end{aligned}$$

For 2, consider $[ac, b][b, c] \in G'$.

Then

$$\begin{aligned}
[ac, b][b, c] &= ((ac)^{-1}b^{-1}(ac)b)(b^{-1}c^{-1}bc) \\
&= c^{-1}a^{-1}b^{-1}acbb^{-1}c^{-1}bc \\
&= c^{-1}a^{-1}b^{-1}acc^{-1}bc \\
&= c^{-1}a^{-1}b^{-1}abc \\
&= c^{-1}[a, b]c \\
&= [a, b]^c.
\end{aligned}$$

For 3, consider $[a^c, b^c] \in G'$.

Then

$$\begin{aligned}
[a^c, b^c] &= (c^{-1}ac)^{-1}(c^{-1}bc)^{-1}(c^{-1}ac)(c^{-1}bc) \\
&= c^{-1}a^{-1}cc^{-1}b^{-1}cc^{-1}acc^{-1}bc \\
&= c^{-1}a^{-1}b^{-1}abc \\
&= c^{-1}[a, b]c \\
&= [a, b]^c.
\end{aligned}$$

For 4, consider $[a, b]^{-1} \in G'$.

Then

$$\begin{aligned}
[a, b]^{-1} &= (a^{-1}b^{-1}ab)^{-1} \\
&= b^{-1}a^{-1}(b^{-1})^{-1}(a^{-1})^{-1} \\
&= b^{-1}a^{-1}ba \\
&= [b, a].
\end{aligned}$$

Thus $[a, b]^{-1} = [b, a]$.

For 5, consider $[a,c][a,b]^c \in G'$.

Then

$$\begin{aligned} [a,c][a,b]^c &= [a,c]([c,a][a,bc]), \text{ by part 1} \\ &= [a,c][a,c]^{-1}[a,bc], \text{ by part 4} \\ &= [a,bc]. \end{aligned}$$

For 6, consider $[a,c]^b[b,c] \in G'$.

Then

$$\begin{aligned} [a,c]^b[b,c] &= ([ab,c][c,b])[b,c], \text{ by part 2} \\ &= [ab,c][b,c]^{-1}[b,c], \text{ by part 4} \\ &= [ab,c]. \end{aligned}$$

For 7, note that $[a,b]=1$ or $a^{-1}b^{-1}ab=1$ or $ab=ba$.

For 8, let $a \in C_G(b)$ and consider $[a,bc]$.

Then

$$\begin{aligned} [a,bc] &= [a,c][a,b]^c, \text{ by part 5} \\ &= [a,c]1^c, \text{ by part 7, since } a \in C_g(b) \text{ implies } ab=ba \\ &= [a,c]. \end{aligned}$$

Lastly, for 9, let $a \in C_G(b)$ and consider $[ac,b]$.

Then

$$
\begin{aligned}
[ac, b] &= [a, b]^c[c, b], \text{ by part 6} \\
&= 1^c[c, b], \text{ by part 7, since } a \in C_g(b) \text{ implies } ab = ba \\
&= [c, b].
\end{aligned}
$$

□

**Theorem 2.2.5.**

*Let $G$ be a group, $H \leq G$ and $K \leq G$. Then $[H, K] = [K, H]$ and $[H, K] \trianglelefteq \langle H, K\rangle$.*

*Proof.* To show that $[H, K] = [K, H]$, consider $\prod_{i=1}^{n}[h_i, k_i]^{-1} \in [H, K]$, where $h_i \in H$ and $k_i \in K$ for each $1 \leq i \leq n$. Note that $[H, K]$ is a group, so any arbitrary element may be written as the inverse of another element. By part 4 of Theorem 2.2.4, $[h_i, k_i]^{-1} = [k_i, h_i]$ for each $1 \leq i \leq n$. Thus $\prod_{i=1}^{n}[h_i, k_i]^{-1} = \prod_{i=1}^{n}[k_i, h_i] \in [K, H]$ and so $[H, K] \leq [K, H]$.

Similarly, let $\prod_{i=1}^{n}[k_i, h_i]^{-1} \in [K, H]$, where $h_i \in H$ and $k_i \in K$ for all $1 \leq i \leq n$. Again, by part 4 of Theorem 2.2.4, $[k_i, h_i]^{-1} = [h_i, k_i]$ for each $i$. Thus, $\prod_{i=1}^{n}[k_i, h_i]^{-1} = \prod_{i=1}^{n}[h_i, k_i] \in [H, K]$. Therefore $[K, H] \leq [H, K]$ and so $[H, K] = [K, H]$.

To show that $[H, K] \trianglelefteq \langle H, K\rangle$, let $\prod_{i=1}^{n}[h_i, k_i] \in [H, K]$, where $h_i \in H$ and $k_i \in K$ for all $1 \leq i \leq n$. Since $\langle H, K\rangle$ is generated by elements of $H$ and $K$, it is sufficient to show that $[H, K] \trianglelefteq H$ and $[H, K] \trianglelefteq K$.

First, let $x \in H$ and consider $\left(\prod_{i=1}^{n}[h_i, k_i]\right)^x$.
Then

$$
\begin{aligned}
\left(\prod_{i=1}^{n}[h_i, k_i]\right)^x &= \prod_{i=1}^{n}[h_i, k_i]^x \\
&= \prod_{i=1}^{n}[h_i x, k_i][k_i, x], \text{ by part 2 of Theorem 2.2.4} \\
&= \prod_{i=1}^{n}[h_i x, k_i][x, k_i]^{-1}, \text{ by part 4 of Theorem 2.2.4.}
\end{aligned}
$$

Now $h_i x \in H$ for each $i$ by closure of $H$, and so $[h_i x, k_i] \in [H, K]$. Additionally $[x, k_i]^{-1} \in [H, K]$ and so $[h_i x, k_i][x, k_i]^{-1} \in [H, K]$ for each $i$, by closure. Thus $\prod_{i=1}^{n}[h_i x, k_i][x, k_i]^{-1} \in [H, K]$ and so $[H, K] \trianglelefteq H$.

Now let $y \in K$ and consider $(\prod_{i=1}^{n}[h_i, k_i])^y$.

Then

$$\begin{aligned}\left(\prod_{i=1}^{n}[h_i, k_i]\right)^y &= \prod_{i=1}^{n}[h_i, k_i]^y \\ &= \prod_{i=1}^{n}[y, h_i][h_i, k_i y], \text{ by part 1 of Theorem 2.2.4} \\ &= \prod_{i=1}^{n}[h_i, y]^{-1}[h_i, k_i y], \text{ by part 4 of Theorem 2.2.4.}\end{aligned}$$

By a similar argument to the previous case, both $[h_i, y]^{-1} \in [H, K]$ and $[h_i, k_i y] \in [H, K]$ for each $1 \le i \le n$ by closure. Thus $\prod_{i=1}^{n}[h_i, y]^{-1}[h_i, k_i y] \in [H, K]$ and $[H, K] \trianglelefteq K$. Hence $[H, K] \trianglelefteq \langle H, K \rangle$.

□

**Theorem 2.2.6.**

*Let $G$ be a group, $H \le G$, $N \trianglelefteq G$ and $N \trianglelefteq H$. Then $H/N \le Z(G/N)$ if and only if $[G, H] \le N$.*

*Proof.* Now

$$\begin{aligned} H/N \le Z(G/N) \quad &\text{or} \quad gNhN = hNgN, \text{ for all } hN \in H/N \text{ and for all } gN \in G/N \\ &\text{or} \quad ghN = hgN, \text{ for all } h \in H \text{ and for all } g \in G \\ &\text{or} \quad (hg)^{-1}gh \in N, \text{ for all } h \in H \text{ and for all } g \in G \\ &\text{or} \quad g^{-1}h^{-1}gh \in N, \text{ for all } h \in H \text{ and for all } g \in G \\ &\text{or} \quad [g, h] \in N, \text{ for all } h \in H \text{ and for all } g \in G \\ &\text{or} \quad [G, H] \le N. \end{aligned}$$

Thus the theorem holds.

□

**Theorem 2.2.7.**

*Let $G$ be a group, $a, b \in G$, $N \trianglelefteq G$, and $H \leq G$.*

*Then:*

1. *$G' \trianglelefteq G$;*

2. *$G/G'$ is abelian;*

3. *$G/N$ is abelian if and only if $G' \leq N$;*

4. *If $G' \leq H$, then $H \trianglelefteq G$.*

*Proof.* For 1, we know that $G' \leq G$ by Theorem 2.2.2. Let $g \in G$ and $\prod_{i=1}^{n}[a_i, b_i] \in G'$.

Then
$$\left(\prod_{i=1}^{n}[a_i, b_i]\right)^g = \prod_{i=1}^{n}[a_i, b_i]^g = \prod_{i=1}^{n}[a_i^g, b_i^g], \text{ by Theorem 2.2.4, part 3.}$$

Thus, since $a_i^g, b_i^g \in G$, it follows that $\prod_{i=1}^{n}[a_i^g, b_i^g] \in G'$. Therefore $G' \trianglelefteq G$.

For 2, let $aG', bG' \in G/G'$.

Then

$$[aG', bG'] = (aG')^{-1}(bG')^{-1}aG'bG' = a^{-1}G'b^{-1}G'aG'bG' = a^{-1}b^{-1}abG' = [a, b]G'.$$

Note now that $[a, b]G' = 1G'$, since $1^{-1}[a, b] = [a, b] \in G'$. Thus $[aG', bG'] = 1G'$ for all $aG', bG' \in G/G'$. Therefore, by 1, $aG'bG' = bG'aG'$ for all $aG', bG' \in G/G'$. Hence $G/G'$ is abelian.

For 3, consider $G/N$.

Then

$$\begin{aligned}
G/N \text{ is abelian} \quad &\text{or} \quad [aN, bN] = 1N, \text{ for all } a, b \in G \\
&\text{or} \quad [a, b]N = 1N, \text{ for all } a, b \in G \\
&\text{or} \quad 1^{-1}[a, b] \in N, \text{ for all } a, b \in G \\
&\text{or} \quad [a, b] \in N, \text{ for all } a, b \in G \\
&\text{or} \quad G' \leq N.
\end{aligned}$$

Thus $G/N$ is abelian if and only if $G' \leq N$.

Finally, for 4, let $g \in G$ and $h \in H \leq G$. Then $[h, g] \in G' \leq H$. Hence $h^{-1}g^{-1}hg \in H$. By the closure of $H$, it follows that $h(h^{-1}g^{-1}hg) = h^g \in H$. Thus, since $g \in G$ was arbitrary, it follows that $H \trianglelefteq G$.

□

**Remark.** *Note that, by part 3 of the previous theorem, taking $G/G'$ is the most efficient way to create an abelian quotient, as any other applicable normal subgroup will contain $G'$.*

The concept of the derived subgroup will now yield a useful subnormal series which may be examined in any group.

**Definition 2.2.8** (The Derived Series)**.**
*Let G be a group. The derived series of G is defined by:*

$$G^{(0)} = G, G^{(1)} = G', G^{(2)} = (G^{(1)})', \quad \textit{and inductively} \quad G^{(n+1)} = (G^{(n)})'$$

*for all $n \in \mathbb{Z}^+ \cup \{0\}$.*

**Remark.** *Note that since each term in the sequence is the derived subgroup of the previous term, part 1 of Theorem 2.2.7 yields that $G^{(n)} \trianglelefteq G^{(n-1)}$ for each $n$. Additionally, by part 2 of Theorem 2.2.7, it follows that each quotient $G^{(n-1)}/G^{(n)}$ is abelian. Thus, if there exists some $n \in \mathbb{N}$ such that $G^{(n)} = 1$, then the derived series will provide the desired subnormal series to show that G is solvable.*

This characterization of solvability will be proven in the next theorem.

**Theorem 2.2.9** (The Derived Series Characterizes Solvability)**.**
*Let G be a group. Then G is solvable if and only if there exists $n \in \mathbb{Z}^+ \cup \{0\}$ such that $G^{(n)} = 1$.*

*Proof.* ( $\Longleftarrow$ ) Suppose there exists $n \in \mathbb{Z}^+ \cup \{0\}$ such that $G^{(n)} = 1$.
Then

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(n-1)} \trianglerighteq G^{(n)} = 1$$

is a subnormal series of $G$. Additionally, for all $0 \leq i \leq n-1$, the factor $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$ which is abelian by part 2 of Theorem 2.2.7. Thus $G$ is solvable.

( $\Longrightarrow$ ) Now suppose $G$ is solvable. Then there exists a subnormal series

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1$$

where $n \in \mathbb{Z}^+ \cup \{0\}$ and $G_i/G_{i+1}$ is abelian for all $0 \leq i \leq n-1$.

Claim: $G^{(i)} \leq G_i$ for all $0 \leq i \leq n$. We will proceed by induction on $i$.

If $i = 0$, then $G^{(0)} = G \leq G = G_0$. Suppose now that $G^{(i)} \leq G_i$. Then

$$\begin{aligned} G^{(i+1)} &= (G^{(i)})' \\ &= [G^{(i)}, G^{(i)}] \\ &\leq [G_i, G_i], \text{ by inductive hypothesis} \\ &\leq G_{i+1}, \text{ by part 3 of Theorem 2.2.7.} \end{aligned}$$

Thus $G^{(i+1)} \leq G_{i+1}$ and the claim holds. But then $G^{(n)} \leq G_n = 1$ and so $G^{(n)} = 1$.

□

Additionally, the derived series can be used to show that subgroups of solvable groups are also solvable.

**Theorem 2.2.10** (Subgroups of Solvable Groups are Solvable)**.**
*Let $G$ be a solvable group and $H \leq G$. Then $H$ is solvable.*

*Proof.* Since $G$ is solvable, by Theorem 2.2.9, there exists $n \in \mathbb{Z}^+ \cup \{0\}$ such that $G^{(n)} = 1$.

Claim: $H^{(i)} \leq G^{(i)}$, for all $i \in \mathbb{Z}^+ \cup \{0\}$. We will proceed by induction on $i$.

If $i = 0$, then $H^{(0)} = H \leq G = G^{(0)}$. Suppose $H^{(i)} \leq G^{(i)}$.

Then $H^{(i+1)} = (H^{(i)})' \leq (G^{(i)})' = G^{(i+1)}$ or $H^{(i+1)} \leq G^{(i+1)}$. Thus, the claim holds. But then $H^{(n)} \leq G^{(n)} = 1$, and so $H^{(n)} = 1$. Therefore $H$ is solvable.

□

Theorem 2.2.9 shows that the derived series characterizes the solvability of a group. In the following section, another type of canonical series will be introduced which gives rise to yet another important class of groups known as nilpotent groups.

# Nilpotent Groups

The next important class of groups that will be explored are nilpotent groups. First, another canonical series will be defined, which will directly motivate the definition of nilpotent groups. From there, the structure and properties of such groups will be explored.

## 3.1 The Upper Central Series and Nilpotency

In the previous section, it was shown that the derived series lead to a characterization of solvability. We will now define another series which will come to define the class of nilpotent groups.

**Definition 3.1.1** (The Upper Central Series)**.**
*Let $G$ be a group. Define the upper central series of $G$ by:*

$$Z_0(G) = 1,\ Z_1(G) = Z(G),\ \frac{Z_2(G)}{Z_1(G)} = Z\left(\frac{G}{Z_1(G)}\right),\ \ldots$$

*where inductively $Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G))$ for all $n \in \mathbb{Z}^+ \cup \{0\}$.*

**Remark.** *Note that in order to define the terms of the upper central series using quotients, it is necessarily true that $Z_n(G) \trianglelefteq Z_{n+1}(G)$ for all $n$. Thus*

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

*forms a subnormal series. Unlike many subnormal series, however, each $Z_i(G)$ is not only normal in the following term, but in $G$ as well.*

**Theorem 3.1.2.** *Let $G$ be a group. Then $Z_i(G) \trianglelefteq G$ for all $i \in \mathbb{Z}^+ \cup \{0\}$.*

*Proof.* We will proceed by induction on $i$. If $i = 0$, then $Z_0(G) = 1 \trianglelefteq G$. Also, if $i = 1$, then $Z_1(G) = Z(G) \trianglelefteq G$. Suppose now that $Z_i(G) \trianglelefteq G$.

Then $G/Z_i(G)$ is a group and $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)) \trianglelefteq G/Z_i(G)$. Taking preimages, it follows that $Z_{i+1}(G) \trianglelefteq G$ and the theorem holds by induction.

□

In addition to having each term normal in $G$, this series will either stabilize where, for some $n \in \mathbb{Z}^+ \cup \{0\}$, $Z_i(G) = Z_{i+1}(G)$ for all $i > n$, or it will continue until reaching $G$ itself. It is the latter case which defines a nilpotent group.

**Definition 3.1.3** (Nilpotent Group)**.**
*Let $G$ be a group. Then $G$ is nilpotent if there exists $n \in \mathbb{Z}^+ \cup \{0\}$ such that $Z_n(G) = G$.*

Now that nilpotent groups have been defined, several results regarding which types of groups are nilpotent can be shown.

**Theorem 3.1.4** (Abelian Groups are Nilpotent)**.**
*Let $G$ be an abelian group. Then $G$ is nilpotent.*

*Proof.* Recall that $Z_1(G) = Z(G)$. Thus, since $G$ is abelian, $Z_1(G) = Z(G) = G$. Hence $G$ is nilpotent.

□

**Theorem 3.1.5** (Subgroups of Nilpotent Groups are Nilpotent)**.**
*Let $G$ be a nilpotent group and $H \leq G$. Then $H$ is nilpotent.*

*Proof.* Since $G$ is nilpotent, there exists $n \in \mathbb{Z}^+ \cup \{0\}$ such that $Z_n(G) = G$.

Claim: $H \cap Z_i(G) \leq Z_i(H)$ for all $0 \leq i \leq n$. We will proceed by induction on $i$.

If $i = 0$, $H \cap Z_0(G) = H \cap \{1\} \leq \{1\} = Z_0(H)$. Suppose now that $H \cap Z_i(G) \leq Z_i(H)$.

Then

$$\begin{aligned}[H, H \cap Z_{i+1}(G)] &\leq H \cap [G, Z_{i+1}(G)] \\ &\leq H \cap Z_i(G), \text{ by Theorem 2.2.6, since } Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)) \\ &\leq Z_i(H), \text{ by inductive hypothesis.}\end{aligned}$$

Thus $[H, H \cap Z_{i+1}(G)] \leq Z_i(H)$ and so by Theorem 2.2.6

$$\frac{H \cap Z_{i+1}(G) Z_i(H)}{Z_i(H)} \leq Z\left(\frac{H}{Z_i(H)}\right) = \frac{Z_{i+1}(H)}{Z_i(H)}.$$

Taking preimages yields

$$(H \cap Z_{i+1}(G))Z_i(H) \leq Z_{i+1}(H)$$

and therefore $H \cap Z_{i+1}(G) \leq Z_{i+1}(H)$. Thus, the claim holds by induction.

Then $Z_n(H) \geq H \cap Z_n(G) = H \cap G = H$. Hence $Z_n(H) = H$ and so $H$ is nilpotent.

□

**Theorem 3.1.6** (Quotients of Nilpotent Groups are Nilpotent)**.**
*Let $G$ be a group and $N \trianglelefteq G$. Then $G/N$ is nilpotent.*

*Proof.* Since $G$ is nilpotent, there exists $n \in \mathbb{Z}^+ \cup \{0\}$ such that $Z_n(G) = G$. Let $\overline{G} = G/N$.

Claim: $\overline{Z_i(G)} \leq Z_i(\overline{G})$, for all $0 \leq i \leq n$. We will proceed again by induction on $i$.

If $i = 0$, then $\overline{Z_0(G)} = \overline{\{1\}} = Z_0(\overline{G})$ and the base case holds. Suppose $\overline{Z_i(G)} \leq Z_i(\overline{G})$.

Now

$$\begin{aligned}[\overline{G}, \overline{Z_{i+1}(G)}] &= \overline{[G, Z_{i+1}(G)]}, \text{ since the natural map is a homomorphism} \\ &\leq \overline{Z_i(G)}, \text{ by Theorem 2.2.6} \\ &\leq Z_i(\overline{G}), \text{ by inductive hypothesis.}\end{aligned}$$

Then

$$\frac{\overline{Z_{i_1}(G)} Z_i(\overline{G})}{Z_i(\overline{G})} \leq Z\left(\frac{\overline{G}}{Z_i(\overline{G})}\right) = \frac{Z_{i+1}(\overline{G})}{Z_i(\overline{G})}$$

by Theorem 2.2.6. Taking preimages yields

$$\overline{Z_{i+1}(G)}Z_i(\overline{G}) \leq Z_{i+1}(\overline{G})$$

and so $\overline{Z_{i+1}(G)} \leq Z_{i+1}(\overline{G})$. Thus, the claim holds by induction.

Then $Z_n(\overline{G}) \geq \overline{Z_n(G)} = \overline{G}$. But it cannot be that $\overline{G} < Z_n(\overline{G})$ and so it must be that $\overline{G} = Z_n(\overline{G})$. Hence $\overline{G} = G/N$ is nilpotent.

□

**Theorem 3.1.7.**

*Let $G$ be a group such that $G/Z(G)$ is nilpotent. Then $G$ is nilpotent.*

*Proof.* Let $\overline{G} = G/Z(G)$. Since $\overline{G}$ is nilpotent, there exists $n \in \mathbb{Z}^+ \cup \{0\}$ such that $Z_n(\overline{G}) = \overline{G}$.

Claim 1: $\overline{Z_i(G)} \leq Z_i(\overline{G})$, for all $i \in \mathbb{Z}^+ \cup \{0\}$. We will proceed by induction on $i$.

If $i = 0$, then $\overline{Z_0(G)} = \overline{1} = Z_0(\overline{G})$. Suppose $\overline{Z_i(G)} \leq Z_i(\overline{G})$.

Now

$$\begin{aligned} [\overline{G}, \overline{Z_{i+1}(G)}] &= \overline{[G, Z_{i+1}(G)]} \\ &\leq \overline{Z_i(G)}, \text{ by Theorem 2.2.6} \\ &\leq Z_i(\overline{G}), \text{ by inductive hypothesis.} \end{aligned}$$

Thus, $[\overline{G}, \overline{Z_{i+1}(G)}] \leq Z_i(\overline{G})$ and so

$$\frac{\overline{Z_{i+1}(G)}}{Z_i(\overline{G})} \leq Z\left(\frac{\overline{G}}{Z_i(\overline{G})}\right) = \frac{Z_{i+1}(\overline{G})}{Z_i(\overline{G})}.$$

Taking preimages yields $\overline{Z_{i+1}(G)} \leq Z_{i+1}(\overline{G})$ and so claim 1 holds by induction.

Claim 2: $Z_i(\overline{G}) \leq \overline{Z_i(G)}$, for all $i \in \mathbb{Z}^+ \cup \{0\}$. Again, we will proceed by induction on $i$.

If $i = 0$, then $Z_0(\overline{G}) = \overline{1} = \overline{Z_0(G)}$. Suppose $Z_i(\overline{G}) \leq \overline{Z_i(G)}$. Let $\overline{U} = U/Z(G) = Z_{i+1}(\overline{G})$.

Then

$$\begin{aligned}\overline{[G,U]} &= [\overline{G},\overline{U}]\\ &= [\overline{G}, Z_{i+1}(\overline{G})]\\ &\leq Z_i(\overline{G}), \text{ by Theorem 2.2.6}\\ &\leq \overline{Z_i(G)}, \text{ by inductive hypothesis.}\end{aligned}$$

Thus $\overline{[G,U]} \leq \overline{Z_i(G)}$. Taking preimages yields $[G,U]Z(G) \leq Z_i(G)$. Hence $[G,U] \leq Z_i(G)$. Then

$$\frac{UZ_i(G)}{Z_i(G)} \leq Z\left(\frac{G}{Z_i(G)}\right) = \frac{Z_{i+1}(G)}{Z_i(G)}$$

and so $UZ_i(G) \leq Z_{i+1}(G)$. But $Z_i(G) \leq Z_{i+1}(G)$, so $U \leq Z_{i+1}(G)$ and it follows that $\overline{U} \leq \overline{Z_{i+1}(G)}$. However, $\overline{U} = Z_{i+1}(\overline{G})$, so $Z_{i+1}(\overline{G}) \leq \overline{Z_{i+1}(G)}$, and claim 2 holds.

By a combination of the two claims, $\overline{Z_i(G)} = Z_i(\overline{G})$, for all $i \in \mathbb{Z}^+ \cup \{0\}$. Then $\overline{G} - Z_n(\overline{G}) = \overline{Z_n(G)}$. Taking preimages yields $G = Z_n(G)$ and so $G$ is solvable.

□

**Theorem 3.1.8** ($p$-Groups are Nilpotent)**.**

*Let $G$ be a $p$-group. Then $G$ is nilpotent.*

*Proof.* Toward a contradiction, suppose $G$ is not nilpotent. Then $Z_i(G) < G$ for every $i \in \mathbb{Z}^+ \cup \{0\}$.

Claim: $Z_i(G) < Z_{i+1}(G)$, for all $i \in \mathbb{Z}^+ \cup \{0\}$. We will proceed by induction on $i$.

Since $G$ is a $p$-group, if $i = 0$, then $Z_1(G) = Z(G) \neq \{1\} = Z_0(G)$. Thus $Z_0(G) < Z_1(G)$. Suppose $Z_i(G) < Z_{i+1}(G)$.

Now $Z_{i+1}(G) \trianglelefteq G$ by Theorem 3.1.2, so $\overline{G} = G/Z_{i+1}(G)$ is a group. Since $G$ is a $p$-group, it follows that $\overline{G}$ is a $p$-group as well. Additionally $|\overline{G}| = |G/Z_{i+1}(G)| = |G|/|Z_{i+1}(G)| < |G|$ and, since $G$ is not nilpotent, $\overline{G} \neq 1$.

Thus

$$1 \neq Z(\overline{G}) = Z\left(\frac{G}{Z_{i+1}(G)}\right) = \frac{Z_{i+2}(G)}{Z_{i+1}(G)}.$$

Hence $Z_{i+1}(G) < Z_{i+2}(G)$ and the claim holds by induction. Then the upper central series never stabilizes, or

$$1 = Z_0(G) < Z_1(G) < Z_2(G) < Z_3(G) < \cdots < Z_n(G) < \cdots$$

which is a contradiction, since $|G| = p^n < \infty$, where $n \in \mathbb{Z}^+ \cup \{0\}$. Thus $G$ is nilpotent.

$\square$

**Remark.** *Theorem 3.1.8 shows that every $p$-group is nilpotent. In fact, there are other structural connections between $p$-groups and nilpotent groups, which will be explored more thoroughly in the following section.*

## 3.2 Additional Properties of Nilpotent Groups

In this section, the structure of nilpotent groups will be explored in greater detail, including a link between nilpotent groups and the solvable groups introduced in part two, and the similarities between the structures of $p$-groups and nilpotent groups. We will begin with the former.

**Theorem 3.2.1** (Nilpotent Groups are Solvable)**.**
*Let $G$ be a nilpotent group. Then $G$ is solvable.*

*Proof.* Since $G$ is nilpotent, there exists $n \in \mathbb{Z}^+ \cup \{0\}$ such that $Z_n(G) = G$. Consider now the upper central series:

$$G = Z_n(G) \trianglerighteq Z_{n-1}(G) \trianglerighteq \cdots \trianglerighteq Z_0(G) = 1$$

which is a subnormal series. Also $Z_{i+1}(G)/Z_i(G) = Z\left(G/Z_i(G)\right)$ which is the center of a group, and therefore abelian for all $0 \leq i \leq n-1$. Hence $G$ is solvable.

$\square$

Following the result of Theorem 3.2.1, it is natural to ask if all solvable groups are necessarily nilpotent. We will turn to a notable characteristic of $p$-groups to provide a method for finding a counterexample. Namely, the fact that $p$-groups have a non-trivial center. It will now be shown that the same is true for nilpotent groups.

**Theorem 3.2.2** (Non-Trivial Nilpotent Groups Have Non-Trivial Centers)**.**
*Let $G$ be a non-trivial nilpotent group. Then $Z(G) \neq 1$.*

*Proof.* Toward a contradiction, suppose $Z(G) = 1$.

Claim: $Z_i(G) = 1$ for every $i \in \mathbb{Z}^+ \cup \{0\}$. We will proceed by induction on $i$.

If $i = 0$, then $Z_0(G) = 1$ by definition. If $i = 1$, then $Z_1(G) = Z(G) = 1$. Suppose now that $Z_i(G) = 1$.

Then

$$Z_{i+1}(G) \cong \frac{Z_{i+1}(G)}{\{1\}} = \frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right)$$

But

$$Z\left(\frac{G}{Z_i(G)}\right) = Z\left(\frac{G}{\{1\}}\right) \cong Z(G) = Z_1(G) = 1$$

and so $Z_{i+1}(G) = 1$. Thus, the claim holds by induction. But then $Z_i(G) = 1$ for all $i$, and so there does not exist $n \in \mathbb{Z}^+ \cup \{0\}$ such that $Z_n(G) = G$. This is a contradiction since $G$ is nilpotent. Hence $Z(G) \neq 1$.

□

Theorem 3.2.2 will now prove useful in showing that certain groups of smaller order are not nilpotent. Recall from a previous example that $S_3$ is solvable with the subnormal series $S_3 \trianglerighteq A_3 \trianglerighteq 1$. We can now examine its center to show that not all solvable groups are nilpotent.

**Example** ($S_3$ is not Nilpotent)**.**
*Recall that $S_3 = \{1, (12), (13), (23), (123), (132)\}$. Consider $Z(S_3)$.*

*Clearly $1 \in Z(S_3)$. Note that*

$$(12)(13) = (132) \neq (123) = (13)(12)$$

$$(12)(23) = (123) \neq (132) = (23)(12)$$

$$(13)(132) = (23) \neq (12) = (132)(13)$$

$$(13)(123) = (12) \neq (23) = (123)(13).$$

*Therefore $(12), (13), (23), (123), (132) \notin Z(S_3)$ and so $Z(S_3) = 1$. Thus, $S_3$ is not nilpotent by Theorem 3.2.2.*

Another shared trait with $p$-groups is the containment of proper subgroups within their normalizers. This result will be proven after establishing a relationship between the commutator subgroup of two subgroups and the normalizer of a subgroup.

**Theorem 3.2.3.**
*Let $G$ be a group, $H \leq G$ and $K \leq G$ such that $[H, K] \leq H$. Then $K \leq N_G(H)$.*

*Proof.* Now $K \leq G$, so $k \in G$ for all $k \in K$. Also $[H, K] \leq H$, and so $[h, k] \in H$ for all $h \in H$ and for all $k \in K$. Then since $h \in H$ and $[h, k] \in H$, by the closure of $H$, we have that

$$h[h, k] = hh^{-1}k^{-1}hk = h^k \in H$$

for all $h \in H$ and for all $k \in K$. Thus $H^k \leq H$ for all $k \in K$. But $|H^k| = |H|$ and so $H^k = H$ for all $k \in K$. Thus $K \leq N_G(H)$.

□

This result allows for the proof that normalizers of proper subgroups "grow" in a nilpotent group.

**Theorem 3.2.4** (Normalizers of Proper Subgroups "Grow" in Nilpotent Groups)**.**
*Let $G$ be a nilpotent group and $H < G$. Then $H < N_G(H)$.*

*Proof.* Since $G$ is nilpotent, there exists $n \in \mathbb{Z}^+ \cup \{0\}$ such that $Z_n(G) = G$. Let $0 \leq i \leq n$ be maximal, where $Z_i(G)$ is the largest (in terms of order) term of the upper central series such that $Z_i(G) \leq H$. Then $Z_{i+1}(G)$ is not contained in $H$ be the maximality of $i$.

Now

$$[H, Z_{i+1}(G)] \leq [G, Z_{i+1}(G)] \leq Z_i(G) \leq H$$

where the second containment follows from Theorem 2.2.6 and the third follows from the choice of $i$. Then $[H, Z_{i+1}(G)] \leq H$, and so by Theorem 3.2.3, we have that $Z_{i+1}(G) \leq N_G(H)$.

Since $Z_{i+1}(G)$ is not contained in $H$, there exists $x \in Z_{i+1}(G) \leq N_G(H)$ such that $x \notin H$. Thus, $H < N_G(H)$.

□

Theorem 3.2.4 has given rise to another property of nilpotent groups. In fact, it will begin a chain of equivalent properties which characterize nilpotency, similar to the way the derived series characterizes solvability. First, a definition must be established.

**Definition 3.2.5** (Maximal Subgroups)**.**
*Let $G$ be a group and $M \leq G$. Then $M$ is a maximal subgroup of $G$ if:*

1. *$M \neq G$;*
2. *Whenever there exists $H \leq G$ such that $M \leq H \leq G$, then either $H = M$ or $H = G$. (i.e. there are no proper subgroups "between" $M$ and $G$ in the subgroup lattice of $G$)*

**Example** (Maximal Subgroups of $\mathbb{Z}_{12}$)**.**
*Consider the subgroup lattice of $\mathbb{Z}_{12} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. It can be written as:*

$$\begin{tikzcd}
& \mathbb{Z}_{12} \arrow[dl, dash] \arrow[dr, dash] & \\
\langle 2 \rangle \arrow[d, dash] \arrow[drr, dash] & & \langle 3 \rangle \arrow[d, dash] \\
\langle 4 \rangle \arrow[dr, dash] & & \langle 6 \rangle \arrow[dl, dash] \\
& \langle 0 \rangle &
\end{tikzcd}$$

*This lattice shows that $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal subgroups of $\mathbb{Z}_{12}$, while $\langle 4 \rangle$, $\langle 6 \rangle$, and $\langle 0 \rangle$ are not.*

The concept of maximal subgroups will now be used to show another property of nilpotent groups.

**Theorem 3.2.6** (Maximal Subgroups are Normal in Nilpotent Groups)**.**
*Let $G$ be a nilpotent group and $M$ be a maximal subgroup of $G$. Then $M \trianglelefteq G$.*

*Proof.* By definition, since $M$ is a maximal subgroup of $G$, we have that $M < G$. By Theorem 3.2.4, since $G$ is nilpotent, $M < N_G(M) \leq G$. Thus by the maximality of $M$, we have $N_G(M) = G$ and so $M \trianglelefteq G$.

□

**Remark.** *Note that Theorem 3.2.4 implies Theorem 3.2.6. We will now see that Theorem 3.2.6 will imply yet another property of nilpotent groups. However, a few definitions and results are required first.*

**Definition 3.2.7** (External Direct Product)**.**
*Let $A$ and $B$ be groups. The external direct product of $A$ and $B$ is given by*

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

**Definition 3.2.8** (Internal Direct Product)**.**
*Let $G$ be a group, $n \in \mathbb{Z}^+$, and $H_i \leq G$ for all $1 \leq i \leq n$ such that:*

1. $G = \prod_{i=1}^{n} H_i$ *;*
2. $H_i \trianglelefteq G$ *for all* $1 \leq i \leq n$*;*
3. $H_i \bigcap \prod_{j \neq i} H_j = 1$ *for all* $1 \leq i \leq n$.

*Then $G$ is said to be the internal direct product of the $H_i$'s.*

**Remark.** *Note that, while the above definitions appear quite different, they are essentially the same; the main difference being that the external direct product is created from arbitrary groups, which may not be contained in the same group, while the internal direct product is created from subgroups of a common group.*

It will now be shown that the two are, in fact, isomorphic to one another. This fact, along with Theorem 3.2.6, will yield the next property of nilpotent groups.

**Theorem 3.2.9** (External Direct Products and Internal Direct Products are Isomorphic)**.**
*Let $G$ be a group, $n \in \mathbb{Z}^+$, and $\{H_i\}_{i=1}^{n}$ be a collection of subgroups of $G$ such that $G$ is the internal direct product of the $H_i$'s. Then $G \cong H_1 \times H_2 \times \cdots \times H_n$.*

*Proof.* By definition, since $G$ is the internal direct product of the $H_i$'s, $G = \prod_{i=1}^{n} H_i$ where each $H_i \trianglelefteq G$ and $H \bigcap \prod_{i \neq j} H_j = 1$.

Note that for all $k \neq i$, $H_k \subset \prod_{i \neq j} H_j$ since each $h_k \in H_k$ can be written as $h_k 111 \cdots 1$. Thus $H_i \bigcap \prod_{i \neq j} H_j = 1$ implies $H_i \cap H_k = 1$ for all $k \neq i$.

Let $h_i \in H_i$, $h_j \in H_j$ where $i \neq j$, and consider $[h_i, h_j]$. Now $[h_i, h_j] = (h_i^{-1}h_j^{-1}h_i)h_j \in H_j$ since $H_j \trianglelefteq G$. Also, $[h_i, h_j] = h_i^{-1}(h_j^{-1}h_ih_j) \in H_i$ since $H_i \trianglelefteq G$. Thus $[h_i, h_j] \in H_i \cap H_j = 1$ since $i \neq j$. By part 7 of Theorem 2.2.4, $[h_i, h_j] = 1 \implies h_ih_j = h_jh_i$. Since $h_i$ and $h_j$ were chosen arbitrarily, it follows that all elements of distinct subgroups commute.

Now define

$$\phi : H_1 \times H_2 \times \cdots \times H_n \longrightarrow \prod_{i=1}^{n} H_i$$

by $\phi((h_1, h_2, \cdots, h_n)) = h_1h_2 \cdots h_n$. It will not be shown that $\phi$ is an isomorphism.

<u>$\phi$ is well-defined</u>

Let $(h_1, h_2, \cdots, h_n), (k_1, k_2, \cdots, k_n) \in H_1 \times H_2 \times \cdots \times H_n$ such that $(h_1, h_2, \cdots, h_n) = (k_1, k_2, \cdots, k_n)$. Then $h_i = k_i$ for all $1 \leq i \leq n$. Thus $h_1h_2 \cdots h_n = k_1k_2 \cdots k_n$ and so $\phi((h_1, h_2, \cdots, h_n)) = \phi((k_1, k_2, \cdots, k_n))$ and $\phi$ is well-defined.

<u>$\phi$ is a homomorphism</u>

Let $(h_1, h_2, \cdots, h_n), (k_1, k_2, \cdots, k_n) \in H_1 \times H_2 \times \cdots \times H_n$ where $h_i, k_i \in H_i$ for all $1 \leq i \leq n$. Then

$$\begin{aligned}
\phi((h_1, h_2, \cdots, h_n)(k_1, k_2, \cdots, k_n)) &= \phi((h_1k_1, h_2k_2, \cdots, h_nk_n)) \\
&= h_1k_1h_2k_2 \cdots h_nk_n \\
&= h_1h_2 \cdots h_ng_1g_2 \cdots g_n, \text{ since elements of distinct } H_i\text{'s commute} \\
&= \phi((h_1, h_2, \cdots, h_n))\phi((k_1, k_2, \cdots, k_n)).
\end{aligned}$$

Thus $\phi$ is a homomorphism.

<u>$\phi$ is onto</u>

Let $h_1h_2 \cdots h_n \in \prod_{i=1}^{n} H_i$ where $h_i \in H_i$ for each $1 \leq i \leq n$. Then by definition there exists $(h_1, h_2, \cdots, h_n) \in H_2 \times \cdots \times H_n$ such that $\phi((h_1, h_2, \cdots, h_n)) = h_1h_2 \cdots h_n$. Hence $\phi$ is onto.

<u>$\phi$ is one-to-one</u>

Suppose now that there exist $(h_1, h_2, \cdots, h_n), (k_1, k_2, \cdots, k_n) \in H_1 \times H_2 \times \cdots \times H_n$ such that $\phi((h_1, h_2, \cdots, h_n)) = \phi((k_1, k_2, \cdots, k_n))$.

Then

$$\begin{aligned} & h_1 h_2 \cdots h_n = k_1 k_2 \cdots k_n \\ \text{or} \quad & k_1^{-1} h_1 = k_2 k_3 \cdots k_n h_n^{-1} h_{n-1}^{-1} \cdots h_2^{-1} \\ \text{or} \quad & k_1^{-1} h_1 = k_2 h_2^{-1} k_3 h_3^{-1} \cdots k_n h_n^{-1}, \text{ since elements of distinct subgroups commute.} \end{aligned}$$

Now $k_1^{-1} h_1 \in H_1$ and $k_1^{-1} h_1 = k_2 h_2^{-1} k_3 h_3^{-1} \cdots k_n h_n^{-1} \in \prod_{j \neq 1} H_j$. But then $k_1^{-1} h_1 \in H_1 \bigcap \prod_{j \neq 1} H_j$. Since $H_1 \bigcap \prod_{j \neq 1} H_j = 1$, it follows that $k_1^{-1} h_1 = 1$ or $h_1 = k_1$.

Then $1 = k_2 h_2^{-1} k_3 h_3^{-1} \cdots k_n h_n^{-1}$ implies $k_2^{-1} h_2 = k_3 h_3^{-1} k_4 h_4^{-1} \cdots k_n h_n^{-1}$ and so

$$k_2^{-1} h_2 = k_3 h_3^{-1} k_4 h_4^{-1} \cdots k_n h_n^{-1} = 1 k_3 h_3^{-1} k_4 h_4^{-1} \cdots k_n h_n^{-1} \in \prod_{j \neq 2} H_j.$$

Since $H_2 \bigcap \prod_{j \neq 2} H_j = 1$, we have $k_2^{-1} h_2 = 1$ or $h_2 = k_2$. By repeating this argument, it follows that $h_i = k_i$ for all $1 \leq i \leq n$ and so $\phi$ is one-to-one.

Therefore $\phi$ is an isomorphism and so $H_1 \times H_2 \times \cdots \times H_n \cong \prod_{i=1}^{n} H_i$.

$\square$

**Remark.** *Due to the internal and external direct products being isomorphic, it is common to simply refer to "the direct product" without specifying which one. It is in this way we will refer to it throughout the remainder of the paper, with internal or external being explicitly shown or stated only when necessary.*

Before proving the next equivalent property of nilpotent groups, one more definition is needed.

**Definition 3.2.10.**

*Let G be a group. Then* $\pi(G) = \{p : p \text{ is prime and } p \mid |G|\}$.

Noting these definitions and results, the next property of nilpotent groups will now be stated and proved.

**Theorem 3.2.11.**

*Let G be a nilpotent group. Then G is isomorphic to the direct product of its Sylow* $p$*-subgroups for distinct* $p$*. That is,* $G \cong P_1 \times P_2 \times \cdots \times P_n$ *where* $P_i \in Syl_{p_i}(G)$ *for each* $p_i \in \pi(G)$*, with* $n \in \mathbb{Z}^+$ *and* $1 \leq i \leq n$*.*

*Proof.* Let $p \in \pi(G)$ and $P \in Syl_p(G)$. If $P$ is not normal in $G$, then $N_G(P) < G$. Thus, there exists a maximal subgroup $M$ such that $N_G(P) \leq M$.

Since $G$ is nilpotent, by Theorem 3.2.6, $M \trianglelefteq G$. Also, $P \leq N_G(P)$ and so $P \leq M$. But $P \in Syl_p(G)$ and $P \leq M$, so it must be that $P \in Syl_p(M)$. Then by Theorem 1.1.11, $G = N_G(P)M$. However, $N_G(P) \leq M$ and so $G = N_G(P)M = M$. This is a contradiction, since $M$ is a maximal subgroup of $G$ and therefore cannot be equal to $G$. Hence, it must be that $P \trianglelefteq G$.

Since $P \trianglelefteq G$, where $P \in Syl_p(G)$ for each $p \in \pi(G)$, $\prod_{\substack{P \in Syl_p(G),\\ p \in \pi(G)}} P$ is a group and

$$\left| \prod_{\substack{P \in Syl_p(G),\\ p \in \pi(G)}} P \right| = \prod_{\substack{P \in Syl_p(G),\\ p \in \pi(G)}} |P| = |G|.$$

Note that the first equality follows by Lagrange's Theorem, since the orders of any two $P$ are coprime.

Thus

$$G = \prod_{\substack{P \in Syl_p(G),\\ p \in \pi(G)}} P .$$

Additionally, because Sylow $p$-subgroups and Sylow $q$-subgroups intersect trivially for $p \neq q$, we have that

$$P \bigcap \prod_{\substack{Q \in Syl_q(G),\\ q \in \pi(G) \setminus \{p\}}} Q = 1$$

for all $P \in Syl_p(G)$ and for all $p \in \pi(G)$.

Thus, by definition, we have that $G$ is the internal direct product of its Sylow $p$-subgroups for distinct $p$. It follows by the isomorphism established in Theorem 3.2.11 that $G \cong P_1 \times P_2 \times \cdots \times P_n$ where $P_i \in Syl_{p_i}(G)$ for each $p_i \in \pi(G)$, with $n \in \mathbb{Z}^+$ and $1 \leq i \leq n$.

$\square$

Note that Theorem 3.2.6 implies Theorem 3.2.11, as the normality of maximal subgroups lead to each $P$ being normal in $G$. To close the section, three more results will be established in order to show that Theorem 3.2.11 implies Theorem 3.2.4, thus establishing three equivalent properties to being nilpotent.

**Theorem 3.2.12** (The Center of a Direct Product is the Direct Product of the Centers)**.**
*Let $A$ and $B$ be groups, then $Z(A \times B) = Z(A) \times Z(B)$.*

*Proof.* Suppose $(a, b) \in Z(A \times B)$ where $a \in A$ and $b \in B$. Also, let $(x, y) \in A \times B$ where $x \in A$ and $y \in B$.

Then $(a, b)(x, y) = (x, y)(a, b)$, or $(ax, by) = (xa, yb)$. Thus, $ax = xa$ and so $a \in Z(A)$. Similarly, $by = yb$ and so $b \in Z(B)$. Thus, $(a, b) \in Z(A) \times Z(B)$. Hence, $Z(A \times B) \leq Z(A) \times Z(B)$.

Now suppose $(a, b) \in Z(A) \times Z(B)$ where $a \in Z(A)$ and $b \in Z(B)$. Let $(x, y) \in A \times B$ such that $x \in A$ and $y \in B$.

Then $(a, b)(x, y) = (ax, by) = (xa, yb)$ since $a \in Z(A)$ and $b \in Z(B)$. Also, $(xa, yb) = (x, y)(a, b)$. Thus, $(a, b)(x, y) = (x, y)(a, b)$ and so $(a, b) \in Z(A \times B)$. Therefore $Z(A) \times Z(B) \leq Z(A \times B)$ and it follows that $Z(A \times B) = Z(A) \times Z(B)$.

$\square$

**Theorem 3.2.13.**
*Let $A, B, C,$ and $D$ be groups such that $C \trianglelefteq A$ and $D \trianglelefteq B$. Then*

$$\frac{A \times B}{C \times D} \cong \frac{A}{C} \times \frac{B}{D}.$$

*Proof.* Since $C \trianglelefteq A$ and $D \trianglelefteq B$, both $A/C$ and $B/D$ are groups. Thus, $A/C \times B/D$ is a group.

Let $\phi : A \times B \longrightarrow A/C \times B/D$ be defined by $\phi((a,b)) = (aC, bD)$ for all $(a,b) \in A \times B$. Suppose $(a,b), (x,y) \in A \times B$. Then

$$\begin{aligned}
\phi((a,b))\phi((x,y)) &= (aC, bD)(xC, yD) \\
&= (aCxC, bDyD) \\
&= (axC, byD) \\
&= \phi((ax, by)) \\
&= \phi((a,b)(x,y)).
\end{aligned}$$

Thus $\phi$ is a homomorphism.

Suppose now that $(a,b) \in Kern(\phi)$. Then

$$\begin{aligned}
(a,b) \in Kern(\phi) \quad &\text{if and only if} \quad \phi((a,b)) = (1C, 1D) \\
&\text{if and only if} \quad (aC, bD) = (1C, 1D) \\
&\text{if and only if} \quad aC = 1C \;\text{ and }\; bD = 1D \\
&\text{if and only if} \quad 1^{-1}a \in C \;\text{ and }\; 1^{-1}b \in D \\
&\text{if and only if} \quad a \in C \;\text{ and }\; b \in D \\
&\text{if and only if} \quad (a,b) \in C \times D.
\end{aligned}$$

Thus $Kern(\phi) = C \times D$.

Note that $\phi$ is clearly onto by design. Thus $\phi(A \times B) = \dfrac{A}{C} \times \dfrac{B}{D}$.

Therefore, by the First Isomorphism Theorem

$$\frac{A \times B}{Kern(\phi)} \cong \phi(A \times B)$$

or

$$\frac{A \times B}{C \times D} \cong \frac{A}{C} \times \frac{B}{D}.$$

$\square$

**Theorem 3.2.14** (Direct Products of Nilpotent Group are Nilpotent)**.**

*Let $A$ and $B$ be nilpotent groups. Then $A \times B$ is nilpotent.*

*Proof.* Since $A$ and $B$ are nilpotent, there exist $m, n \in \mathbb{Z}^+ \cup \{0\}$ such that $Z_m(A) = A$ and $Z_n(B) = B$. Let $k = max\{m, n\}$.

Claim: $Z_i(A \times B) = Z_i(A) \times Z_i(B)$, for all $0 \leq i \leq k$. We will proceed by induction on $i$.

If $i = 0$, then $Z_0(A \times B) = (1, 1) = \{1\} \times \{1\} = Z_0(A) \times Z_0(B)$. Suppose $Z_i(A \times B) = Z_i(A) \times Z_i(B)$. Then

$$\begin{aligned}
\frac{Z_{i+1}(A \times B)}{Z_i(A \times B)} &= Z\left(\frac{A \times B}{Z_i(A \times B)}\right) \\
&= Z\left(\frac{A \times B}{Z_i(A) \times Z_i(B)}\right), \text{ by inductive hypothesis} \\
&\cong Z\left(\frac{A}{Z_i(A)} \times \frac{B}{Z_i(B)}\right), \text{ by Theorem 3.2.13} \\
&= Z\left(\frac{A}{Z_i(A)}\right) \times Z\left(\frac{B}{Z_i(B)}\right), \text{ by Theorem 3.2.12} \\
&= \frac{Z_{i+1}(A)}{Z_i(A)} \times \frac{Z_{i+1}(B)}{Z_i(B)} \\
&\cong \frac{Z_{i+1}(A) \times Z_{i+1}(B)}{Z_i(A) \times Z_i(B)}, \text{ by Theorem 3.2.13} \\
&= \frac{Z_{i+1}(A) \times Z_{i+1}(B)}{Z_i(A \times B)}, \text{ by inductive hypothesis.}
\end{aligned}$$

Thus

$$\frac{Z_{i+1}(A \times B)}{Z_i(A \times B)} = \frac{Z_{i+1}(A) \times Z_{i+1}(B)}{Z_i(A \times B)}.$$

Taking preimages yields $Z_{i+1}(A \times B) = Z_{i+1}(A) \times Z_{i+1}(B)$ and so the claim holds by induction. But then $Z_k(A \times B) = Z_k(A) \times Z_k(B) = A \times B$. Hence $A \times B$ is nilpotent.

□

**Remark.** *Using the result from Theorem 3.2.14, we can see that any group which is the product of nilpotent groups is itself nilpotent. Note that for any group $G$, $P \in Syl_p(G)$ is a $p$-group and is therefore nilpotent by Theorem 3.1.8. Thus any group which is the product of it's Sylow $p$-subgroups for distinct $p$ is nilpotent. This nilpotency implies that normalizers "grow" by Theorem 3.2.4, which in turn implies that all maximal subgroups are normal by Theorem 3.2.6. Thus, we have found three properties equivalent to being nilpotent, with each implying the next.*

To close the section, these equivalent properties will be stated, and are as follows:

**Remark** (Equivalent Properties to Nilpotency)**.**
*Let $G$ be a group. Then the following are equivalent:*

1. *$G$ is nilpotent;*
2. *If $H < G$, then $H < N_G(H)$;*
3. *If $M$ is a maximal subgroup of $G$, then $M \trianglelefteq G$;*
4. *$G \cong P_1 \times P_2 \times \cdots \times P_n$, where $P_i \in Syl_{p_i}(G)$ for each $p_i \in \pi(G)$, with $n \in \mathbb{Z}^+$ and $1 \leq i \leq n$.*

In the next section, group automorphisms and characteristic subgroups will be defined and explored, which will provide a variety of results and complete the necessary information to begin exploring the influence of subgroup structure on groups which are the product of two subgroups.

# Automorphisms, Characteristic Subgroups, and Minimal Normal Subgroups

In this part of the thesis, we will establish the remaining definitions and results necessary to begin examining groups which are the product of two subgroups. Namely, a few more useful types of subgroups will be established, along with automorphisms, as well as the relationships between the two.

## 4.1 Automorphisms and Characteristic Subgroups

**Definition 4.1.1** (Automorphisms)**.**
*Let $G$ be a group and suppose $\phi : G \longrightarrow G$. Then $\phi$ is an automorphism if $\phi$ is a one-to-one and onto homomorphism. The set of all such automorphisms of a group is given by:*

$$Aut(G) = \{\phi : G \longrightarrow G : \phi \textit{ is an automorphism } \}.$$

**Remark.** *$Aut(G)$ forms a group under function composition.*

In fact, conjugation of a group by any of its elements generates an automorphism- a fact which will now be proven. Once formally defined, the structure of the set of these automorphisms within $Aut(G)$ will be explored.

**Theorem 4.1.2** (Conjugation Generates an Automorphism)**.**

*Let $G$ be a group and $g \in G$. Define $\phi_g : G \longrightarrow G$ by $\phi_g(x) = x^g$, for all $x \in G$. Then $\phi_g \in Aut(G)$.*

*Proof.* First, we will show that $\phi_g$ is well-defined and one-to-one. Let $x, y \in G$. Then $x = y$ if and only if $x^g = y^g$, if and only if $\phi_g(x) = \phi_g(y)$. Thus, $\phi_g(x)$ is well-defined and one-to-one.

To see that $\phi_g$ is onto, let $y \in G$. By the closure of $G$, $x = y^{g^{-1}} \in G$. Then

$$\phi_g(x) = x^g = (y^{g^{-1}})^g = y.$$

Hence $\phi_g$ is onto.

Lastly, to show $\phi$ is a homomorphism, let $x, y \in G$. Then

$$\begin{aligned}
\phi_g(x)\phi_g(y) &= x^g y^g \\
&= g^{-1}xgg^{-1}yg \\
&= g^{-1}xyg \\
&= (xy)^g \\
&= \phi_g(xy).
\end{aligned}$$

Thus, $\phi_g$ is a homomorphism and so $\phi_g \in Aut(G)$.

□

**Definition 4.1.3** (Inner Automorphisms)**.**

*Let $G$ be a group. We define the set of inner automorphisms as*

$$Inn(G) = \{\phi_g : g \in G\}$$

*where $\phi_g$ is the automorphism generated from conjugation by the element $g \in G$, as described in previous theorem.*

The set $Inn(G)$ not only forms a subgroup of $Aut(G)$, but is actually normal in $Aut(G)$. This will be shown in the following theorem.

**Theorem 4.1.4.**

*Let $G$ be a group. Then $Inn(G) \trianglelefteq Aut(G)$.*

*Proof.* Let $\phi_g \in Inn(G)$, $\psi \in Aut(G)$, $x \in G$, and $y \in G$ such that $\psi(x) = y$. By theorem 4.1.2, $\phi_g \in Aut(G)$. It follows by the group structures of $G$ and $Aut(G)$ that $Inn(G) \leq Aut(G)$. Thus, it remains to show that $Inn(G)$ is normal in $Aut(G)$.

Consider

$$\begin{aligned}
\phi_g^{\psi}(x) &= (\psi^{-1} \circ \phi_g \circ \psi)(x) \\
&= (\psi^{-1} \circ \phi_g)(y) \\
&= \psi^{-1}(y^g) \\
&= \psi^{-1}(g^{-1})\psi^{-1}(y)\psi^{-1}(g), \text{ since } \psi \text{ is a homomorphism} \\
&= \psi^{-1}(g^{-1})x\ \psi^{-1}(g).
\end{aligned}$$

But $\psi$ is a homomorphism, and so $\psi^{-1}(g^{-1}) = (\psi^{-1})^{-1}(g) = \psi(g)$. Thus $\psi^{-1}(g^{-1})x\ \psi^{-1}(g) = \psi(g)x\ \psi^{-1}(g) = x^{\psi^{-1}(g)}$.

But $\psi \in Aut(G)$ and $Aut(G)$ is a group. Hence $\psi^{-1} \in Aut(G)$. Thus, there exists $g_0 \in G$ such that $\psi^{-1}(g) = g_0$. But then $x^{\psi^{-1}(g)} = x^{g_0} = \phi_{g_0}(x)$, where $\phi_{g_0} \in Inn(G)$ since $g_0 \in G$. Therefore $Inn(G) \trianglelefteq Aut(G)$.

□

**Remark.** *The choice of name for $Inn(G)$ implies the existence of "outer" automorphisms of a group $G$. By the result of Theorem 4.1.4, we can define the group of outer automorphisms as $Out(G) = Aut(G)/Inn(G)$.*

Having defined and briefly explored a group's automorphisms, we can now identify another type of subgroup, whose special properties become apparent thanks to the elements of $Aut(G)$.

**Definition 4.1.5** (Characteristic Subgroups)**.**
*Let $G$ be a group and $H \leq G$. Then $H$ is a characteristic subgroup of $G$ if $\phi(H) \leq H$ for all $\phi \in Aut(G)$. We denote this as $H$ char $G$.*

**Remark.** *If $H$ char $G$, then $\phi(H) \leq H$. However, each $\phi \in Aut(G)$ is a bijection, and so $|\phi(H)| = |H|$. Thus, $\phi(H) = H$. Essentially, characteristic subgroups are invariant under all of the group's automorphisms, much in the same way that normal subgroups are invariant under conjugation by any of the group's elements.*

We will now identify a few characteristic subgroups which reside in any group and prove that they are, in fact, characteristic.

**Theorem 4.1.6** (The Center is a Characteristic Subgroup)**.**
*Let $G$ be a group. Then $Z(G)$ char $G$.*

*Proof.* Let $\phi \in Aut(G)$, $z \in Z(G)$, and $g \in G$. Since $\phi$ is onto, there exists $x \in G$ such that $\phi(x) = g$. Then

$$\begin{aligned} g^{\phi(z)} &= \phi(x)^{\phi(z)} \\ &= \phi(x^z), \text{ since } \phi \text{ is a homomorphism} \\ &= \phi(x), \text{ since } z \in Z(G) \\ &= g. \end{aligned}$$

Thus $g^{\phi(z)} = g$, or $g\phi(z) = \phi(z)g$, and so $\phi(z) \in Z(G)$. Hence $Z(G)$ char $G$.

□

**Theorem 4.1.7** (The Derived Subgroup is a Characteristic Subgroup)**.**
*Let $G$ be a group. Then $G'$ char $G$.*

*Proof.* Let $\phi \in Aut(G)$ and $\displaystyle\prod_{i=1}^{n}[a_i, b_i] \in G'$, where $n \in \mathbb{Z}^+$. Now $G' \leq G$ and so $[a_i, b_i] \in G$ for all $1 \leq i \leq n$. Thus

$$\begin{aligned} \phi\left(\prod_{i=1}^{n}[a_i, b_i]\right) &= \prod_{i=1}^{n} \phi\left([a_i, b_i]\right), \text{ since } \phi \text{ is a homomorphism} \\ &= \prod_{i=1}^{n} \left[\phi(a_i), \phi(b_i)\right], \text{ since } \phi \text{ is an isomorphism.} \end{aligned}$$

Since $\phi \in Aut(G)$, $\phi(a_i) \in G$ and $\phi(b_i) \in G$ for all $1 \leq i \leq n$, and so $[a_i, b_i] \in G'$ for each $i$. Thus

$$\phi\left(\prod_{i=1}^{n}[a_i, b_i]\right) = \prod_{i=1}^{n}[\phi(a_i), \phi(b_i)] \in G'$$

and therefore $G'$ char $G$.

$\square$

We will now identify some properties of characteristic subgroups and their relationship with a group's normal subgroups.

**Theorem 4.1.8.**

*Let $G$ be a group, $H \leq G$, and $K \leq G$. Then:*

1. *If $H$ char $G$, then $H \trianglelefteq G$;*

2. *If $H$ char $K$ and $K \trianglelefteq G$, then $H \trianglelefteq G$.*

*Proof.* For 1, let $g \in G$. By Theorem 4.1.2, $\phi_g \in Aut(G)$. Since $H$ char $G$, it follows by definition and from a previous remark that $\phi_g(H) = H$. But then $H^g = H$, and so $H \trianglelefteq G$.

For 2, let $g \in G$. Then $\phi_g \in Aut(G)$. Since $K \trianglelefteq G$, it follows that $\phi_g \in Aut(K)$. Then because $H$ char $K$, we have that $H^g = \phi_g(H) \leq H$ and so $H^g = H$. Hence $H \trianglelefteq G$.

$\square$

**Remark.** *Note that under most circumstances, normality is not a transitive property. Thus, for a group $G$ with subgroups $H \leq G$ and $K \leq G$, it is not necessarily true that $H \trianglelefteq K \trianglelefteq G$ implies $H \trianglelefteq G$. The presence of $H$ as a characteristic subgroup of $K$ is required. This lack of transitivity will be illustrated with a specific example.*

**Example.** *Consider $A_4$ with subgroups $K = \{1, (12)(34), (13)(24), (14)(23)\}$ and $H = \{1, (12)(34)\}$.*

*Recall that conjugation preserves cycle type. Thus since all elements of $K$ are $2-2-$cycles, we have that $k^a \in K$ for all $k \in K$ and for all $a \in A_4$. Thus $K \trianglelefteq A_4$.*

*Additionally, note that* $1^k = 1 \in H$*, for all* $k \in K$*. Checking the remaining elements of* $H$ *conjugated by the remaining elements of* $K$ *yields:*

$$\begin{aligned}(12)(34)^{(12)(34)} &= (12)(34) \in H\\ (12)(34)^{(13)(24)} &= (12)(34) \in H\\ (12)(34)^{(14)(23)} &= (12)(34) \in H.\end{aligned}$$

*Thus* $H \trianglelefteq K$*.*

*However*

$$\begin{aligned}(12)(34)^{(143)} &= (143)^{-1}(12)(34)(143)\\ &= (14)^{-1}(13)^{-1}(12)(34)(13)(14)\\ &= (14)(13)(12)(34)(13)(14)\\ &= (14)(23) \notin H.\end{aligned}$$

*Therefore* $H \ntrianglelefteq A_4$*.*

The previous example highlights one structural influence imparted by the presence of characteristic subgroups. Namely, their ability to guarantee the transitivity of normal subgroups. It is also true that a lack of characteristic subgroups affects the structure of a group. We will investigate the effects of a shortage of characteristic subgroups, along with an additional type of subgroup, in the following section.

## 4.2 Characteristically Simple Groups and Minimal Normal Subgroups

Recall that a group $G$ is called simple if its only normal subgroups are $1$ and $G$. Theorem 4.1.8 established a relationship between characteristic subgroups and normal subgroups, and as such, we may define what it means for a group to be characteristically simple and what this means for its structure.

**Definition 4.2.1** (Characteristically Simple Groups)**.**

*Let $G$ be a group. Then $G$ is called characteristically simple if it has $1$ and $G$ as its only characteristic subgroups.*

**Remark.** *The definitions for simple and characteristically simple groups are closely related in that all simple groups are characteristically simple. Suppose $G$ is simple and $H$ char $G$. By part 1 of Theorem 4.1.8, we have $H \trianglelefteq G$. But $G$ is simple, so either $H = 1$ or $H = G$, making $G$ characteristically simple as well.*

**Example.** *Using the previous remark, it is easy to find examples of characteristically simple groups. We now have that $A_n$ is characteristically simple for all $n \geq 5$ and $\mathbb{Z}_p$ is characteristically simple for any prime $p$.*

We will now see that being characteristically simple relates a group's structure to that of simple groups.

**Theorem 4.2.2.**

*Let $G$ be a characteristically simple group. Then $G$ is isomorphic to the direct product of simple isomorphic groups.*

*Proof.* Let $G_1 \trianglelefteq G$ such that $G_1 \neq 1$ and $|G_1|$ is minimal. Also, let $\{G_i\}_{i=1}^{s}$ be a collection of subgroups of $G$ such that $G_i \cong G_1$ for all $1 \leq i \leq s$, $G_i \trianglelefteq G$ for all $1 \leq i \leq s$, $G_i \bigcap \prod_{j \neq i} G_j = 1$ for all $1 \leq i \leq s$, and $s \in \mathbb{Z}^+$ is maximal. Lastly, let $H = \prod_{i=1}^{s} G_i$. Then since $G_i \trianglelefteq G$ for all $1 \leq i \leq s$, it follows that $H \trianglelefteq G$.

Now, if $H$ is not a characteristic subgroup of $G$, then there exists $1 \leq i \leq s$ and $\phi \in Aut(G)$ such that $\phi(G_i) \not\leq H$. Since $G_i \trianglelefteq G$ and $\phi \in Aut(G)$, we have that $\phi(G_i) \trianglelefteq G$. Thus $\phi(G_i) \cap H \trianglelefteq G$.

Because $\phi(G_i) \not\leq H$, it follows that $\phi(G_i) \cap H < \phi(G_i)$. But then, since $\phi \in Aut(G)$ and $G_i \cong G_1$, we have $|\phi(G_i) \cap H| < |\phi(G_i)| = |G_i| = |G_1|$. Therefore $\phi(G_i) \cap H = 1$ by the minimality of $|G_1|$.

Now $\phi(G_i) \cong G_i \cong G_1$ or $\phi(G_i) \cong G_1$. Also, $\phi(G_i) \bigcap \prod_{i=1}^{s} G_i = \phi(G_i) \cap H = 1$. Thus, $\phi(G_i)$ is disjoint from each $G_i$ and satisfies the properties necessary to be included in $H$. Hence $H < \phi(G_i) \prod_{i=1}^{s} G_i$ which is a contradiction to the maximality of $s$. Therefore $H$ char $G$.

Since $H \neq 1$ and $G$ is characteristically simple, we have that

$$G = H = \prod_{i=1}^{s} G_i \cong G_1 \times G_2 \times \cdots \times G_s$$

by Theorem 3.2.9.

Let $1 \leq i \leq s$. If $N \trianglelefteq G_i$, then $N \trianglelefteq \prod_{i=1}^{s} G_i = G$ since all elements of $G_i$ commute with all elements of $G_j$, where $i \neq j$. But $|N| \leq |G_i| = |G_1|$ and so by the minimality of $|G_1|$, either $|N| = 1$ or $|N| = |G_1|$. Hence $N = 1$ or $N = G_i$, yielding that $G_i$ is simple for all $1 \leq i \leq s$. Thus $G = \prod_{i=1}^{s} G_i \cong G_1 \times G_2 \times \cdots \times G_s$ and so $G$ is isomorphic to the direct product of simple isomorphic groups.

□

For the remainder of this section, we will turn our attention to minimal normal subgroups and elementary abelian $p$-groups, both of which will be defined shortly. Combining these concepts with the previous results regarding solvability and simple isomorphic groups will yield the remaining theorems necessary to structurally examine groups which are the product of two subgroups in the coming section.

**Definition 4.2.3** (Minimal Normal Subgroups)**.**
*Let $G$ be a group and $N \trianglelefteq G$. Then $N$ is a minimal normal subgroup if $N \neq 1$ and whenever $K \leq N$ such that $K \trianglelefteq G$, then either $K = 1$ or $K = N$.*

**Remark.** *Note that minimal normal subgroups behave in a similar manner to maximal subgroups. A minimal normal subgroup of a group $G$ will have no non-trivial, proper normal subgroups contained in it, much like a maximal subgroup would have no proper subgroups containing it.*

**Definition 4.2.4** (Elementary Abelian $p$-Groups)**.**
*Let $G$ be a group and $p$ be a prime. Then $G$ is an elementary abelian $p$-group if $G \cong \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n}$ for some $n \in \mathbb{Z}^+$.*

These definitions, along with the following proof, will yield the remaining results of this section.

**Theorem 4.2.5** (Simple Abelian Groups are Isomorphic to Cyclic Groups of Prime Order)**.**
*Let $G$ be a simple abelian group. Then $G \cong \mathbb{Z}_p$ for some prime $p$.*

*Proof.* Note that if $G = 1$, then $G \neq \mathbb{Z}_p$ for any prime $p$. Without loss of generality, assume $G \neq 1$. Then there exists $g \in G$ such that $g \neq 1$.

Since $G$ is an abelian group, every subgroup of $G$ is normal. However, since $G$ is simple, its only normal subgroups are $1$ and $G$. Thus it must be that $1$ and $G$ are the only subgroups of $G$.

Consider $\langle g \rangle$. Since $\langle g \rangle \leq G$, either $\langle g \rangle = 1$ or $\langle g \rangle = G$. It cannot be that $\langle g \rangle = 1$ since $g \in \langle g \rangle$ and $g \neq 1$. Hence $\langle g \rangle = G$ and so $G$ is cyclic.

Suppose now that $G$ has composite order. Then there exist $m, n \in \mathbb{Z}^+$ such that $m, n > 1$, $gcd(m, n) = 1$, and $|G| = |\langle g \rangle| = |g| = mn$. Consider $\langle g^m \rangle = \{1, g^m, g^{2m}, \cdots, g^{(n-1)m}\}$. Now $\langle g^m \rangle \leq G$, so either $\langle g^m \rangle = 1$ or $\langle g^m \rangle = G$. But $m < mn$ and so $g^m \neq 1$. Thus, $\langle g^m \rangle \neq 1$. Hence $\langle g^m \rangle = G = \langle g \rangle$.

But then $|\langle g^m \rangle| = |G| = |\langle g \rangle|$ and so $n = mn$ or $m = 1$, a contradiction. Thus $\langle g^m \rangle \neq 1$ and $\langle g^m \rangle \neq G$. This is, again, a contradiction since $G$ is a simple abelian group and therefore has no non-trivial subgroups. Thus $G$ has prime order.

Then $G$ is a cyclic group of prime order and so $G \cong \mathbb{Z}_p$ for some prime $p$.

□

**Theorem 4.2.6.**
*Let $G$ be a solvable group and $N$ be a minimal normal subgroup of $G$. Then $N$ is an elementary abelian $p$-group for some prime $p$.*

*Proof.* Since $G$ is solvable and $N \leq G$, we know $N$ is solvable by theorem 2.2.10. Let $K$ char $N$. Then since $N \trianglelefteq G$, by part 2 of theorem 4.1.8, $K \trianglelefteq G$. But $N$ is a minimal normal subgroup, so $K = 1$ or $K = N$. Thus, $N$ is characteristically simple.

Then by Theorem 4.2.2, there exists a collection of subgroups of $N$, say $\{N_i\}_{i=1}^{n}$, such that for all $1 \leq i \leq n$, we have $N = \prod_{i=1}^{n} N_i$, $N_i \trianglelefteq N$, $N_i \bigcap \prod_{i \neq j} N_j = 1$, and each $N_i$ is a simple isomorphic group.

Suppose there exists $1 \leq i \leq n$ such that $N_i$ is non-abelian. Now $N_i' \trianglelefteq N_i$ and so $N_i' = 1$ or $N_i' = N_i$. But $N_i$ is non-abelian so it cannot be that $N_i' = 1$. Thus, $N_i' = N_i$ and so $N_i$ is not solvable. This is a contradiction since $N_i \leq N$ and $N$ is solvable. Thus $N_i$ is abelian for all $1 \leq i \leq n$.

Since each $N_i$ is a simple abelian group, by Theorem 4.2.5, there exists a prime $p$ such that $N_i \cong \mathbb{Z}_p$ for all $1 \leq i \leq n$. But then

$$N = \prod_{i=1}^{n} N_i \cong N_1 \times N_2 \times \cdots \times N_n = \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n}$$

and so $N$ is an elementary abelian $p$-group.

□

**Theorem 4.2.7.**

*Let $G$ be a $p$-group for some prime $p$ and $N \trianglelefteq G$ such that $N \neq 1$. Then $N \cap Z(G) \neq 1$.*

*Proof.* Since $N \trianglelefteq G$, we know $G$ acts on $N$ by conjugation. Then $G$ acts on $S = N - \{1\}$ by conjugation as well. Note that $|S| = |N| - 1$. Thus, if $p \mid |S|$, then since $p \mid |N|$, we have that $p \mid |N| - |S| = 1$. This is a contradiction since no prime divides 1. Therefore $p \not| \, |S|$.

Thus, since $G$ is a $p$-group, by Theorem 1.1.13, there exists $a \in S$ such that $G_a = G$. But $G_a = C_G(a)$ since $G$ is acting by conjugation, and so $G = C_G(a)$. Hence $a \neq 1$ and $a \in N \cap Z(G)$.

□

**Theorem 4.2.8.**

*Let $G$ be a nilpotent group and $N \trianglelefteq G$ such that $N \neq 1$. Then $N \cap Z(G) \neq 1$.*

*Proof.* Let $N_1 \leq N$ such that $N_1$ is a minimal normal subgroup of $G$. Since $G$ is nilpotent, by Theorem 3.2.1, $G$ is solvable. Additionally, by Theorem 4.2.6, $N_1$ is an elementary abelian $p$-group for some prime $p$.

Now by Sylow's Second Theorem, there exists $P \in Syl_p(G)$ such that $N_1 \leq P$. Hence $N_1 \trianglelefteq P$ and $N_1 \neq 1$. Then by Theorem 4.2.7, $N_1 \cap Z(P) \neq 1$. Since $G$ is nilpotent, $Z(P) \leq Z(G)$. Thus, $1 \neq N_1 \cap Z(P) \leq N_1 \cap Z(G)$ or $N_1 \cap Z(G) \neq 1$.

□

**Theorem 4.2.9** (Products of Normal Nilpotent Subgroups are Nilpotent)**.**
*Let $G$ be a group, $M \trianglelefteq G$ be nilpotent and $N \trianglelefteq G$ be nilpotent. Then $MN \trianglelefteq G$ is nilpotent.*

*Proof.* Since $M \trianglelefteq G$ and $N \trianglelefteq G$, it follows that $MN \trianglelefteq G$. We will proceed by induction on $|G|$.

If $|G| = 1$, then $G = 1$ and so $M = 1$ and $N = 1$. Thus $MN = 1 \trianglelefteq G$. Also 1 is trivially nilpotent since $Z_0(1) = 1$. Suppose the theorem holds for all groups of order less than $|G|$.

If $MN < G$, then $M \trianglelefteq MN$ is nilpotent and $N \trianglelefteq MN$ is nilpotent. Since $|MN| < |G|$, by the inductive hypothesis, $MN$ is nilpotent and the proof is complete. Thus it must be that $G = MN$.

Claim: $Z(G) \neq 1$.

Since $M$ is nilpotent, $Z(M) \neq 1$ by Theorem 3.2.2. Consider $[Z(M), N]$. If $[Z(M), N] = 1$ then $1 \neq Z(M) \leq C_G(MN) = Z(G)$, and the claim holds. Suppose instead that $[Z(M), N] \neq 1$. Then $Z(M)$ char $M \trianglelefteq G$ and so $Z(M) \trianglelefteq G$ by Theorem 4.1.8. Thus since $N \trianglelefteq G$, we have that $[Z(M), N] \trianglelefteq G$ and so $1 \neq [Z(M), N] \trianglelefteq N$.

Because $N$ is nilpotent, by Theorem 4.2.8, $1 \neq [Z(M), N] \cap Z(N)$. But $1 \neq [Z(M), N] \cap Z(N) \leq Z(M) \cap Z(N) \leq Z(G)$, since $G = MN$. Thus $Z(G) \neq 1$ and the claim holds.

Let $\overline{G} = G/Z(G)$. Then $\overline{G} = \overline{MN}$. Since $M \trianglelefteq G$ and $N \trianglelefteq G$, we have that $\overline{M} \trianglelefteq \overline{G}$ and $\overline{N} \trianglelefteq \overline{G}$. Also, since $M$ and $N$ are nilpotent, Theorem 3.1.6 yields that $\overline{M}$ and $\overline{N}$ are nilpotent.

Now $|\overline{G}| < |G|$ and so by induction hypothesis $\overline{MN} \trianglelefteq \overline{G}$ and $\overline{MN}$ is nilpotent. But $\overline{MN} = \overline{G} = G/Z(G)$ and so $G/Z(G)$ is nilpotent. Thus by Theorem 3.1.7, $G = MN$ is nilpotent.

□

With these results in hand, an exploration into the structure of groups which are the product of two subgroups can begin.

# Groups Which are the Product of Two Subgroups

In the final section, we will explore a variety of results regarding the structure and properties of groups which are the product of two of their subgroups. First, the necessary conditions for a product of two subgroups to remain a subgroup will be established.

**Theorem 5.1.1.**
*Let $G$ be a group, $H \leq G$ and $K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.*

*Proof.* ( $\Longrightarrow$ ) Suppose $HK \leq G$. Let $hk \in HK$, where $h \in H$ and $k \in K$. Since $HK \leq G$, we know $(hk)^{-1} = k^{-1}h^{-1} \in HK$. Thus, there exists $h_1 \in H$ and $k_1 \in K$ such that $k^{-1}h^{-1} = h_1k_1$. Then $(k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1}$ or $hk = k_1^{-1}h_1^{-1} \in KH$. Thus $HK \subseteq KH$.

Now let $kh \in KH$, where $k \in K$ and $h \in H$. Then $h^{-1}k^{-1} \in HK$ and so $kh = (h^{-1}k^{-1})^{-1} \in HK$. Hence $KH \subseteq HK$ and $HK = KH$.

( $\Longleftarrow$ ) Suppose now that $HK = KH$. Since $H \leq G$, we have that $H$ is non-empty. $K$ is also non-empty for the same reason. Thus there exists $h \in H$ and $k \in K$. Then $hk \in HK$ and so $HK$ is non-empty.

Let $h_1k_1, h_2k_2 \in HK$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then $k_1k_2^{-1}h_2^{-1} \in KH = HK$. Hence there exists $h_3 \in H$ and $k_3 \in K$ such that $k_1k_2^{-1}h_2^{-1} = h_3k_3$. Now

$$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_3k_3 \in HK.$$

Thus $HK \leq G$ by the subgroup test.

□

**Theorem 5.1.2.**

*Let $G$ be a group, $H \leq G$ and $K \leq G$ such that $G = HK$. Then $G = H^x K^y$ for all $x, y \in G$.*

*Proof.* Notice that $HK \leq G$. Then by Theorem 5.1.1, $HK = KH$ and so $G = KH$. Let $x, y \in G$. Then $yx^{-1} \in G = KH$. Thus, there exists $k \in K$ and $h \in H$ such that $yx^{-1} = kh^{-1}$. Since $G = HK$, by the closure of $H$ and $K$, we have $G = H^h K^k$. Conjugation by $h^{-1}$ yields

$$G = G^{h^{-1}} = H^{h^{-1}} K^{kh^{-1}} = HK^{kh^{-1}} = HK^{yx^{-1}}$$

or $G = HK^{yx^{-1}}$. Conjugating again by $x$ yields $G = G^x = H^x K^{yx^{-1}x} = H^x K^y$ or $G = H^x K^y$.

□

**Theorem 5.1.3.**

*Let $G$ be a group, $H \leq G$, $K \leq G$, $A \leq G$ and $B \leq G$ such that $G = HK$, $H$ is conjugate to $A$ and $K$ is conjugate to $B$. Then $G = AB$ and there exists $g \in G$ such that $H^g = A$ and $K^g = B$.*

*Proof.* Since $K$ is conjugate to $B$ and $G = HK = KH$, by Theorem 5.1.2, there exists $h \in H$ and $k \in K$ such that $K^{kh} = B$. Then $K^h = B$.

Now $G = HK$ and so $G = G^h = H^h K^h = HK^h = HB$. Since $H$ is conjugate to $A$, there exists $h_1 \in H$ and $b \in B$ such that $H^{h_1 b} = A$, or $H^b = A$. Then $H^{hb} = H^b = A$ and $K^{hb} = B^b = B$. Therefore, conjugating $G = HK$ by $hb$ yields

$$G = G^{hb} = H^{hb} K^{hb} = H^b B^b = AB.$$

Thus $G = AB$, $H^{hb} = A$ and $K^{hb} = B$.

□

These results regarding the ability to conjugate subgroups will now help construct a Sylow $p$-subgroup of a group $G = HK$ using the Sylow $p$-subgroups of $H \leq G$ and $K \leq G$.

**Theorem 5.1.4.**

*Let $G$ be a group, $p$ be a prime, $H \leq G$ and $K \leq G$ such that $G = HK$. Then there exists $P \in Syl_p(H)$ and $Q \in Syl_p(K)$ such that $PQ \in Syl_p(G)$.*

*Proof.* Let $R \in Syl_p(G)$. By Sylow's second theorem, there exist $x, y \in G$ such that $P^x \leq R$ and $Q^y \leq R$. By Theorems 5.1.2 and 5.1.3, $G = H^x K^y$ and there exists $g \in G$ such that $H^{xg} = H$ and $K^{yg} = K$. Then $P^{xg} \leq H^{xg} = H$ and $Q^{yg} \leq K^{yg} = K$. Thus, $P^{xg} \in Syl_p(H)$ and $Q^{yg} \in Syl_p(K)$.

Now $P^{xg} \leq R^g$ and $Q^{yg} \leq R^g$. Thus, $P^{xg}Q^{yg} \subseteq R^g$. Also $|P^{xg} \cap Q^{yg}| \leq |H \cap K|_p$. But then

$$|R^g| = |R| = |G|_p = |HK|_p = \frac{|H|_p |K|_p}{|H \cap K|_p} = \frac{|P^{xg}||Q^{yg}|}{|H \cap K|_p} \leq \frac{|P^{xg}||Q^{yg}|}{|P^{xg} \cap Q^{yg}|} = |P^{xg}Q^{yg}|.$$

Thus $P^{xg}Q^{yg} = R^g \in Syl_p(G)$.

□

**Theorem 5.1.5.**

*Let $G$ be a group. $H \leq G$, $K \leq G$ such that $G = HK$, and $H \leq L \leq G$. Then $L = H(L \cap K)$.*

*Proof.* Since $H \leq L$ and $L \cap K \leq L$, then $H(L \cap K) \subseteq L$ by the closure of $L$.

Let $l \in L$. Then since $l \in G = HK$, there exist $h \in H$ and $k \in K$ such that $l = hk$. Then $k = h^{-1}l$ and so $k \in L$. Thus, $h^{-1}l = k \in L \cap K$ or $l \in H(L \cap K)$. Hence $L \subseteq H(L \cap K)$. But both $H$ and $L \cap K$ are subgroups of $L$ so it must be that $L = H(L \cap K)$.

□

Theorem 5.1.5 illuminates the influence $H$ and $K$ have on other subgroups of $G$ which contain them. We will now explore the influence $H$ and $K$ have on $G$ as a whole- particularly when $H$ and $K$ are cyclic.

**Theorem 5.1.6.**

*Let $G$ be a group, $H \leq G$ and $K \leq G$ such that $G = HK$. If $H$ and $K$ are cyclic, then $G$ is solvable.*

*Proof.* Suppose the theorem is false and let $G$ be a minimal counterexample. Since $H$ and $K$ are cyclic, there exist $h \in H$ and $k \in K$ such that $H = \langle h \rangle$ and $K = \langle k \rangle$.

Without loss of generality, suppose $|K| \leq |H|$. If $H \cap H^k = 1$, then

$$|HH^k| = \frac{|H||H^k|}{|H \cap H^k|} = |H||H| \geq |H||K| \geq |HK| = |G|.$$

Thus $G = HH^k$. Then by Theorem 5.1.2, we have $G = HH = H$ or $G = H$. But then $G$ is cyclic and therefore solvable by Theorem 2.1.2, since every cyclic group is abelian. This is a contradiction, so it must be that $H \cap H^k \neq 1$.

Then there exists a prime $p$ such that $p \mid |H \cap H^k|$. Since $H \cap H^k \leq H$ and $H$ is cyclic, then $H \cap H^k$ is cyclic. By Theorem 1.1.15, there exists $L \leq H \cap H^k$ such that $|L| = p$. Now $L \leq H^k$ and so $L^{k^{-1}} \leq H$. Also $L \leq H$ and $|L| = |L^{k^{-1}}|$. Thus, since $H$ is cyclic, by Theorem 1.1.15, $L = L^{k^{-1}}$ or $L^k = L$.

Now $N_G(L) \supseteq \langle H, K \rangle = H\langle k \rangle = HK = G$. Thus, $N_G(L) = G$ and so $L \trianglelefteq G$. Let $\overline{G} = G/L$. Then $\overline{G} = \overline{H}\,\overline{K}$ and by Theorem 1.1.14, $\overline{H}$ and $\overline{K}$ are cyclic. Moreover, $|\overline{G}| = |G/L| = |G|/|L| < |G|$. Thus, by the minimality of $|G|$, we get $\overline{G} = G/L$ is solvable. Also, $L \leq H$ and $H$ is cyclic. Then $L$ is cyclic and therefore solvable by Theorem 2.1.2.

But then $L \trianglelefteq G$ is solvable and $G/L$ is solvable, so by Theorem 2.1.5, $G$ is solvable. This is, again, a contradiction. Thus $G$ is solvable and the theorem holds.

$\square$

**Remark.**

*Note that, under the conditions presented in Theorem 5.1.6, it cannot be proven that $G$ is cyclic, abelian, or even nilpotent. Being a solvable group is essentially the strongest structural conclusion that can be drawn in regards to $G$. This fact will now be illustrated by an example of a group which meets the above criteria, but is not cyclic, abelian, or nilpotent.*

**Example.**

*Consider $S_3$ and note that $S_3 = A_3\langle(12)\rangle \cong \mathbb{Z}_3\mathbb{Z}_2$.*

*Now both $\mathbb{Z}_3$ and $\mathbb{Z}_2$ are cyclic, and therefore abelian, and thus nilpotent by Theorem 3.1.4, but $S_3$ is none of these.*

After the result presented in Theorem 5.1.6, it is natural to ask what the effect on $G$ will be if the conditions on $H$ and $K$ are "weakened". Specifically, if $H$ and $K$ are abelian instead of cyclic, will $G$ retain its solvable status? It will now be shown that this is indeed the case.

**Theorem 5.1.7.**

*Let $G$ be a group, $H \leq G$ and $K \leq G$ such that $G = HK$. If $H$ and $K$ are abelian, then $G$ is solvable and $G^{(2)} = 1$.*

*Proof.* Now $[H, K] \leq G'$. Since $[H, K] \trianglelefteq \langle H, K\rangle$ by Theorem 2.2.5, we have that $H \leq N_G([H, K])$ and $K \leq N_G([H, K])$. Thus $G = HK \leq N_G([H, K])$ and so $G = N_G([H, K])$. Hence $[H, K] \trianglelefteq G$. Since $G = HK$, $[H, K] \trianglelefteq G$, and by parts 5 and 6 of Theorem 2.2.4, we have that $G' \leq [H, K]$. Thus $G' = [H, K]$.

Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$\begin{aligned}
[h_1, k_1]^{h_2 k_2} &= [h_1, k_1^{h_2}]^{k_2}, \text{ since } H \text{ is abelian} \\
&= [h_1, h_3 k_3]^{k_2}, \text{ for some } h_3 \in H \text{ and } k_3 \in K\text{, since } G = HK \\
&= [h_1, k_3]^{k_2}, \text{ by part 8 of Theorem 2.2.4} \\
&= [h_1^{k_2}, k_3], \text{ since } K \text{ is abelian} \\
&= [h_4 k_4, k_3], \text{ for some } h_4 \in H \text{ and } k_4 \in K\text{, since } G = HK \\
&= [h_4, k_3], \text{ by part 9 of Theorem 2.2.4}
\end{aligned}$$

or $[h_1, k_1]^{h_2 k_2} = [h_4, k_3]$. Also, note that

$$\begin{aligned}
[h_1, k_1]^{k_2 h_2} &= [h_1^{k_2}, k_1]^{h_2}, \text{ since } K \text{ is abelian} \\
&= [h_4 k_4, k_1]^{h_2}, \text{ since } G = HK \\
&= [h_4, k_1]^{h_2}, \text{ by part 9 of Theorem 2.2.4} \\
&= [h_4, k_1^{h_2}], \text{ since } H \text{ is abelian} \\
&= [h_4, h_3 k_3], \text{ since } G = HK \\
&= [h_4, k_3], \text{ by part 8 of Theorem 2.2.4.}
\end{aligned}$$

Thus $[h_1, k_1]^{h_2 k_2} = [h_1, k_1]^{k_2 h_2}$ or $[h_1, k_1]^{h_2 k_2 h_2^{-1} k_2^{-1}} = [h_1, k_1]$. But then $[h_1, k_1]^{[h_2^{-1}, k_2^{-1}]} = [h_1, k_1]$ or $[h_2^{-1}, k_2^{-1}] \in C_G([h_1, k_1])$, for all $h_2 \in H$ and for all $k_2 \in K$. Thus since $h_2^{-1}$ and $k_2^{-1}$ were arbitrary, we have that $[H, K] \leq C_G([h_1, k_1])$ and so $[h, k] \in Z([H, K])$ for all $[h, k] \in [H, K]$. Hence $[H, K] = G'$ is abelian. It follows that $G^{(2)} = 1$ and so $G$ is solvable.

□

Theorem 5.1.7 will now allow for the proof of two more results regarding the relationships of subgroups $H$ and $K$ to other subgroups within $G$, under the same conditions that $G = HK$ and both $H$ and $K$ are abelian.

**Theorem 5.1.8.**

*Let $G$ be a group, $H \leq G$, $K \leq G$ where both $H$ and $K$ are abelian and $G = HK$. If $H \neq G$ or $K \neq G$, then there exists $N \trianglelefteq G$ such that $N \neq G$ and either $H \leq N$ or $K \leq N$.*

*Proof.* Suppose the theorem is false and let $G$ be a minimal counterexample. By Theorem 5.1.7, $G$ is solvable. Let $N$ be a minimal normal subgroup of $G$. Then by Theorem 4.2.6, $N$ is an elementary abelian $p$-group for some prime $p$.

Since $N \trianglelefteq G$, we have that $HN \leq G$. Suppose $HN < G$, and let $\overline{G} = G/N$. Then since $G = HK$, it follows that $\overline{G} = \overline{H}\ \overline{K}$. Moreover, since $H$ and $K$ are abelian, both $\overline{H}$ and $\overline{K}$ are abelian as well. Additionally, $\overline{H} \neq \overline{G}$ and $|\overline{G}| < |G|$. Thus, by the minimality of $G$, there exists $\overline{N_1} = N_1/N \trianglelefteq G$ such that $\overline{N_1} \neq G$ and either $\overline{H} \leq \overline{N_1}$ or $\overline{K} \leq \overline{N_1}$.

Then $N_1 \trianglelefteq G$, $N_1 \neq G$ and either $H \leq HN \leq N_1$ or $K \leq KN \leq N_1$. This is a contradiction, and so it must be that $G = HN = KN$.

Suppose now that $G$ is a $p$-group. Since $H \neq G$, there exists a maximal subgroup $M < G$ such that $H \leq M$. Since $G$ is a $p$-group, we have that $G$ is nilpotent by Theorem 3.1.8. Thus by Theorem 3.2.6, $M \trianglelefteq G$. Also, $M \neq G$ and $H \leq M$, which is a contradiction. Hence $G$ is not a $p$-group.

Now there exists a prime $q \neq p$ such that $q \mid |G|$. Let $P \in Syl_q(H)$ and $Q \in Syl_q(K)$. Since $H$ and $K$ are abelian, we know $P \trianglelefteq H$ and $Q \trianglelefteq K$. Thus $P$ and $Q$ are unique Sylow $q$-subgroups of $H$ and $K$ respectively, by Corollary 1.1.10. Hence, by Theorem 5.1.4, $PQ \in Syl_q(G)$.

Note that

$$|PQ| = |G|_q = |HN|_q = \frac{|H|_q |N|_q}{|H \cap N|_q} = \frac{|H|_q \cdot 1}{1} = |H|_q = |P|.$$

Thus $|PQ| = |P|$. But $P \leq PQ$ and so $P = PQ$. Similarly, $Q = PQ$ and so $P = Q$. Then $P = Q \trianglelefteq HK = G$. Let $N_2 \leq P$ such that $N_2$ is a minimal normal subgroup of $G$. By the argument used for $N$, it follows that $G = HN_2 = KN_2$. But $G = HN_2 \leq HP = H$ and $G = KN_2 \leq KP = KQ = K$. Thus $G = H$ and $G = K$.

This is a contradiction since either $H \neq G$ or $K \neq G$. Thus, the theorem holds.

$\square$

**Theorem 5.1.9.**

*Let $G$ be a group, $H \leq G$, $K \leq G$ where both $H$ and $K$ are abelian and $G = HK$. Then there exists $N \trianglelefteq G$ such that $N \neq 1$ and either $N \leq H$ or $N \leq K$.*

*Proof.* Suppose the theorem is false and let $G$ be a minimal counterexample.

Claim: There exists $U \trianglelefteq G$ such that $U \neq G$, $H \leq U$ or $K \leq U$ and $Z(U) \neq 1$.

Suppose $G' \cap H \neq 1$. Then $H \leq HG' \trianglelefteq G$ and $1 \neq G' \cap H \leq Z(HG')$ since both $H$ and $G'$ are abelian. Then without loss of generality, suppose $G' \cap H = G' \cap K = 1$. By Theorem 5.1.8, there exists $U \trianglelefteq G$ such that $U \neq G$ and either $H \leq U$ or $K \leq U$. Suppose $H \leq U$. Since $G = HK$ and $H \leq U$, by Theorem 5.1.5, $U = HK_1$, where $K_1 < K$.

Note that $|U| < |G|$. Thus, by the minimiality of $G$, there exists $1 \neq L \trianglelefteq U$ such that $L \leq H$ or $L \leq K_1$. Suppose $L \leq H$. Now $[U, L] \leq L \cap G' \leq H \cap G' = 1$. Thus $1 \neq L \leq Z(U)$ and so the claim holds.

Let $hk \in Z(U)$ where $h \in H$ and $k \in K$. Also, let $k_1 \in K_1$. Then $hk_1k = k_1hk$ and $hkk_1 = hk_1k$. Thus $hk_1k = k_1hk$ or $hk_1 = k_1h$. Hence $h \in Z(U)$. Therefore $h^{-1} \in Z(U)$ and it follows that $k \in Z(U)$. But then $Z(U) = H_1K_2$ where $H_1 \leq H$ and $K_2 \leq K$.

If $K_2 \neq 1$, then $C_G(K_2) \geq UK = HK_1K = HK = G$, and so $K_2 \trianglelefteq G$ with $K_2 \leq K$. This is a contradiction. Thus, suppose $K_2 = 1$. Then $H_1 = Z(U)$ char $U \trianglelefteq G$ and so $H_1 \trianglelefteq G$ by Theorem 4.1.8. Note also that $1 \neq Z(U) = H_1$ and $H_1 \leq H$.

Hence the theorem holds.

$\square$

With Theorem 5.1.9, we conclude the final proof regarding groups which are the product of two subgroups. The results of this section point to the natural conclusion of this exploration, which is, in fact, the strongest possible result regarding a group's structure under the given conditions. This conclusion is the result of a sequence of papers from the 1950's and 60's, whose statements will be given here. Additionally, a final example will be presented which illustrates that if the structure of $H$ and $K$ are weakened any further, then no meaningful conclusion can be drawn about the group in general.

In Theorem 5.1.6, it was shown that if $G = HK$ and both $H$ and $K$ were cyclic subgroups of $G$, then $G$ was solvable. In Theorem 5.1.7, the structures of $H$ and $K$ were weakened to being abelian, and it was shown that $G$ remained a solvable group. Therefore, it is natural to wonder if $G$ is solvable yet again, when both $H$ and $K$ are nilpotent. This result was first proved by German mathematician Helmut Wielandt in 1958, albeit with a condition imposed on the orders of $H$ and $K$.

**Theorem 5.1.10** (Helmut Wielandt's Result)**.**
*Let $G$ be a group, $H \leq G$ be nilpotent, $K \leq G$ be nilpotent such that $G = HK$ and $gcd(|H|, |K|) = 1$. Then $G$ is solvable.*

A short while later, in 1961, this result was improved upon by another German mathematician, Otto Kegel. This time, there were no restrictions placed upon the orders of $H$ and $K$.

**Theorem 5.1.11** (Otto Kegel's Result)**.**
*Let $G$ be a group, $H \leq G$ be nilpotent, and $K \leq G$ be nilpotent such that $G = HK$. Then $G$ is solvable.*

This result is, in fact, the strongest possible conclusion that can be made regarding $G$, without imposing additional conditions on $H$ and $K$. To see that this is the case, we will naturally weaken the structure of $H$ and $K$ again such that both $H$ and $K$ are solvable, and show that the same cannot necessarily be said for $G$.

**Example.**

*Consider* $A_5$ *and recall that* $|A_5| = \frac{5!}{2} = 60 = 2^2 \cdot 3 \cdot 5$.

*Now* $(A_5)_5 \cong A_4$, *and* $|(A_5)_5| = |A_4| = \frac{4!}{2} = 2^2 \cdot 3$. *Also,* $H = \langle (12345) \rangle \leq A_5$ *such that* $|H| = 5$, *since* $(12345)$ *is an element of order* $5$. *Note that*

$$|(A_5)_5 H| = \frac{|(A_5)_5||H|}{|(A_5)_5 \cap H|} = \frac{2^2 \cdot 3 \cdot 5}{1} = |A_5|.$$

*Thus* $A_5 = (A_5)_5 H$, *where* $(A_5)_5$ *is solvable by Theorem 2.1.7 and* $H$ *is solvable by Theorem 2.1.2. Hence* $A_5$ *is the product of two solvable subgroups.*

*Claim:* $A_5^{(i)} = A_5$, *for all* $i \in \mathbb{Z}^+ \cup \{0\}$.

*If* $i = 0$, *then* $A_5^{(0)} = A_5$. *If* $i = 1$, *then* $A_5^{(1)} = A_5' \trianglelefteq A_5$. *But* $A_5$ *is simple, so* $A_5' = 1$ *or* $A_5' = A_5$. *Since* $A_5$ *is not abelian, it cannot be that* $A_5' = 1$. *Thus,* $A_5' = A_5^{(1)} = A_5$.

*Suppose* $A_5^{(i)} = A_5$. *Then* $A_5^{(i+1)} = (A_5^{(i)})' = A_5' = A_5^{(1)} = A_5$, *and so the claim holds.*

*Thus, there does not exist* $n \in \mathbb{Z}^+ \cup \{0\}$ *such that* $A_5^{(n)} = 1$, *and so* $A_5$ *is not solvable by Theorem 2.2.9.*

The above example confirms that Otto Kegel's result is the strongest possible statement about the structure of $G$ under the given conditions, and is thus the natural end to this exploration on the structure of groups which are the product of two subgroups.

# References

W.R. Scott, *Group Theory*, Prentice Hall, 1964.

Kegel, O.H. Produkte nilpotenter Gruppen. *Arch. Math* **12,** 90-93 (1961). url: https://doi.org/10.1007/BF01650529

Wieland t, H. Über Produkte von nilpotenten Gruppen, *Illinois J. Math* **2,** 611-618 (1958). url: https://projecteuclid.org/journals/illinois-journal-of-mathematics/volume-2/issue-4B/%c3%9cber-Produkte-von-nilpotenten-Gruppen/10.1215/ijm/1255448333.full?tab=ArticleFirstPage