A GENERALIZATION OF SYLOW'S THEOREM

by

Teri M. Thomas

Submitted in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in the

Mathematics

Program

YOUNGSTOWN STATE UNIVERSITY

August, 2009

A GENERALIZATION OF SYLOW'S THEOREM

Teri M. Thomas

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:

Teri M. Thomas, Student Date

Approvals:

Dr. Neil Flowers, Thesis Advisor Date

Dr. Eric Wingler, Committee Member Date

Dr. Tom Wakefield, Committee Member Date

Peter J. Kasvinky, Dean of School of Graduate Studies and Research Date

ABSTRACT

In the study of group theory, it is common to break up a complex group into simpler subgroups in order to arrive at a structure that is easier to analyze and understand. It is also sometimes possible to reconstruct the original group from these subgroups. Although this is not always possible, we can apply this process to finite solvable groups and derive some theorems regarding these groups. Sylow's Theorem and Hall's Theorem are among the most famous results. Hall's Theorem, which is regarded as an extension of Sylow's Theorem, states that if a group G is solvable and is of some order mn, where m is prime to n, then G has a subgroup of order m and all subgroups of this order are conjugate. When $p = \pi$, a Hall π-subgroup is simply a Sylow p-subgroup. While Sylow's Theorem is valid for any finite group, Hall subgroups need not exist in nonsolvable groups. For example, A_5 has order $60 = 3 \cdot 20$, but it has no subgroups of order 20. This is demonstrated within the paper. Hall's Theorem has been the starting point for the theory of finite solvable groups developed over the past seventy years, although those results are not given here.

ACKNOWLEDGEMENTS

I would like to offer my sincere gratitude to Dr. Neil Flowers for his wealth of knowledge and unending patience through this venture. Without his support, I would not have been successful in the completion of this thesis nor the acquisition of knowledge of group theory. I also thank him for his confidence in my ability to use LaTeX, even when I had my doubts.

I want to thank Drs. Eric Wingler and Tom Wakefield for their time and contributions to this thesis. Their input and suggestions have been extremely helpful, and I appreciate their willingness to review my work despite their many other commitments.

I would also like to thank Dr. Frank Ingram for his patience and compassion, and for introducing me to the world of abstract algebra. In considering various mathematical topics, I found abstract algebra and group theory to be the most interesting and exciting, and I credit him for that association.

I offer my thanks to the faculty and staff of the Mathematics Department. Everyone has been more than generous and accommodating, and extraordinarily patient with me as I have strived to complete this degree. Drs. Nathan Ritchey and Jamal Tartir have always given me good advice, which has been greatly appreciated, and has assisted me in achieving my goals.

I want to thank Andy, Jacob, Rabekah, Dylan, and Derek for all their support and sacrifice during this quest. I love you guys, and thank you for believing in me even when I didn't believe in myself.

Finally, I want to thank Dr. Charles Singler. Words cannot express how much you have done for me, and continue to do. I only hope that I can follow in your example and inspiration and continue to be successful in the field of education.

Contents

1 Introduction

We begin with French mathematician Augustin Cauchy, born in August 1789. He worked directly with Lagrange and Laplace, which led to his very famous theorem which states:

If G is a finite group and p is a prime number dividing the order of G, then G contains an element of order p.

That is,

If G is a finite group and p is a prime number dividing the order of G, then there exists $x \in G$ such that $x^p = 1$.

This result was published sometime between 1844 and 1846, in one of the over 800 publications that Cauchy produced. Cauchy died in May 1857.

During this time, another noted mathematician contributed greatly to the field of group theory. He was Peter Sylow, born in Norway in December 1832. Sylow had encountered Cauchy's work during his studies abroad, and in 1862 asked whether Cauchy's Theorem could be further generalized. He did so in 1872, proving Sylow's Theorem, which states:

If p^n is the largest power of the prime p to divide the order of the group G, then:

(1) G has subgroups of order p^n.

(2) G has $1 + kp$ such subgroups.

(3) Any two of such subgroups are conjugate, and the number of such groups is 1 (mod p).

(4) The number of such subgroups divides the order of G.

Sylow spent most of his later years teaching and editing the work of his peers, and died in 1918.

One other renowned mathematician continued to study Sylow's work, namely Philip Hall. Hall was born in England in April 1904, and made huge advances in the field of group theory, further generalizing Sylow's results in 1927 and formally publishing his findings in 1932. Hall's Theorem states:

If a group G is solvable and is of some order mn, where m is prime to n, then G has a subgroup of order m and all subgroups of this order are conjugate.

Hall received many honors and awards for his work in group theory, and died in December 1982.

2 Preliminaries

Definition: A nonempty set G equipped with the operation * is said to form a **group** under that operation if the operation obeys the following laws, called **group axioms**:

(1) **Closure:** For any $a, b \in G$, we have $a * b \in G$.

(2) **Associativity:** For any $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$.

(3) **Identity:** There exists an element $e \in G$ such that for all $a \in G$ we have $a*e = e*a = a$. Such an element $e \in G$ is called the **identity** in G.

(4) **Inverse:** For each $a \in G$ there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$. Such an element $a^{-1} \in G$ is called an **inverse** of a in G.

Definition: A nonempty subset H of a group G is a **subgroup** of G if H is a group under the same operation as G. In this case we write $H \leq G$.

We now will suppress the notation and write $a * b$ as ab and the identity e as 1. We also will assume that G is a finite group.

Theorem 2.1 *A nonempty subset H of a group G is a subgroup of G if and only if the following condition holds:*

For every $a, b \in H, ab^{-1} \in H$.

Definition: Let G be a group. Then the **center** of G, denoted $Z(G)$, consists of the elements of G that commute with every element of G. In other words:

$$Z(G) = \{a \in G \mid ga = ag \text{ for all } g \in G\}.$$

We note that $1g = g = g1$ for all $g \in G$, so $1 \in Z(G)$, and the center is a nonempty subset of G. In addition, $Z(G) \leq G$.

Definition: Let G be a group and $a \in G$. Then the **centralizer** of a in G, denoted $C_G(a)$, is the set of all elements of G that commute with a. In other words,

$$C_G(a) = \{g \in G \mid ag = ga\}.$$

We also note here that $C_G(a) \leq G$.

We now consider maps between groups.

Definition: A map $\phi : G \to G'$ from a group G to a group G' is called a **homomorphism** if

$$\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in G.$$

Definition: Let $\phi : G \to G'$ be a homomorphism. Then the **kernel** of ϕ is the set $\{g \in G \mid \phi(g) = 1\}$, denoted $Ker(\phi)$.

Definition: A homomorphism $\phi : G \to G'$ that is one-to-one and onto is called an **isomorphism**. Two groups G and G' are **isomorphic**, written $G \cong G'$, if there exists some isomorphism $\phi : G \to G'$.

Definition: Let G be a group and $H \leq G$. Then if $ghg^{-1} \in H$ for all $g \in G$ and for all $h \in H$, we say H is a **normal** subgroup of G, denoted $H \trianglelefteq G$.

Theorem 2.2 *Let $\phi : G \to G'$ be a homomorphism. Then*

$$Ker\phi \trianglelefteq G.$$

Example: $Z(G) \trianglelefteq G$, since the elements of $Z(G)$ commute with every element of G.

Definition: Let H be a subgroup of a group G. Then

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

is called the **normalizer** of H in G, and $N_G(H) \leq G$.

As we explore the construction of groups, we need to understand the relation between homomorphisms and their images. When considering a normal subgroup K of a group G, we find that K is the kernel of some homomorphism ϕ from $G \to G'$. The construction of G' and the homomorphism ϕ leads us to quotient groups.

Definition: Let G be a group, $H \leq G$, and $a \in G$. Then the set $aH = \{ah \mid h \in H\}$ is called a **left coset** of H in G, and the set $Ha = \{ha \mid h \in H\}$ is called a **right coset** of H in G.

Definition: Let G be a group and $H \trianglelefteq G$. Then the group consisting of the cosets of H in G under the operation $(aH)(bH) = (ab)H$ is called the **quotient group** of G by H, written G/H.

Theorem 2.3 *Let G be a group, $N \trianglelefteq G$, $H \leq N$, and $\phi : G \to \frac{G}{N}$ by $\phi(g) = gN$ for all $g \in G$. Then*

(1) $\phi(H) = \frac{HN}{N}$.

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

(3) $L \leq \frac{G}{N}$*. Then there exists* $N \leq K \leq G$ *such that* $L = \frac{K}{N}$.

Theorem 2.4 (Lagrange's Theorem). *Let G be a group and $H \leq G$. Then*

(1) $|H|$ *divides* $|G|$.

(2) $|G|/|H|$ *is equal to the number of distinct cosets of* H.

Theorem 2.5 (Fundamental Theorem of Finite Abelian Groups). *Let G be an abelian group of finite order. Then*

(1) $G \cong \mathbf{Z}_{p_1^{a_1}} \times \mathbf{Z}_{p_2^{a_2}} \times \cdots \times \mathbf{Z}_{p_s^{a_s}}$
where the primes p_i are not necessarily unique.

(2) The direct product is unique except for the order of factors.

At this point, we need to look at three isomorphism theorems, which provide us with information on subgroups of an original group G, and subgroups of the quotient group created from the homomorphic image of a group G and a normal subgroup of G, the kernel of the homomorphism. These theorems allow us to determine the solvability of a group, which is necessary for our main result.

Theorem 2.6 (First Isomorphism Theorem). *Let $\phi : G \to G'$ be a homomorphism, with kernel K. Then*

$$G/K \cong \phi(G).$$

Theorem 2.7 (Second Isomorphism Theorem). *Let G be a group, K a normal subgroup of G, and H any subgroup of G. Then*

$$HK/K \cong H/(H \cap K).$$

Theorem 2.8 (Third Isomorphism Theorem). *Let G be a group, $H \trianglelefteq G$, and $K \trianglelefteq G$ such that $K \leq H$. Then*

$$G/H \cong \frac{(G/K)}{(H/K)}.$$

We are now ready to consider group actions.

3 Groups Acting on Sets

We will start with some basic definitions and examples.

Definition: Let S be a set, and
$Sym(S) = \{\phi : S \to S \mid \phi$ is one-to-one and onto $\}$. Then $(Sym(S), \circ)$ is a group.

Example: $Sym(\{1, 2, 3\}) = S_3$, which is a group.

Definition: A group G **acts** on a set S if there exists a homomorphism $\phi : G \to Sym(S)$.

Definition: Let G be a group, and S be a set, such that G acts on S via ϕ. Then G acts **faithfully** on S if $Ker\phi = \{1\}$.

We will also suppress the notation here, from $\phi(g)(a)$ to ga.

Definition: Let G be a group acting on a set S, and $a \in S$. The **orbit** of G on S containing a is

$$Ga = \{ga \mid g \in G\} \subseteq S.$$

Definition: Let G be a group acting on a set S. The action of G on S is **transitive** if there is only one orbit, or, given any $a, b \in S$, there exists a $g \in G$ such that $a = gb$.

Example: Let G be a group, and $g \in G$. Then G acts on itself via ϕ, defined by $\phi(g)(x) = gx$ for all $g, x \in G$ (left multiplication). To show this is an action, we must verify that ϕ is one-to-one, onto, and a homomorphism. We start with one-to-one. Let $x, y \in G$ such that $\phi(g)(x) = \phi(g)(y)$. Then by definition,

$$\begin{aligned} gx &= gy \\ g^{-1}gx &= g^{-1}gy \\ x &= y. \end{aligned}$$

Thus $\phi(g)$ is one-to-one.

Now we consider onto. For all $y \in G$, we must show there exists $x \in G$ such that $\phi(g)(x) = y$. Let $x = g^{-1}y$. Then,

$$\begin{aligned} \phi(g)(x) &= \phi(g)(g^{-1}y) \\ &= gg^{-1}y \\ &= y. \end{aligned}$$

Thus $\phi(g)$ is onto. To show ϕ is a homomorphism, we let $g_1, g_2 \in G$. Then

$$\begin{aligned} \phi(g_1g_2)(x) &= g_1g_2x \\ &= g_1(\phi(g_2)(x)) \\ &= \phi(g_1)(\phi(g_2)(x)) \\ &= (\phi(g_1)\phi(g_2))(x). \end{aligned}$$

Thus $\phi(g)$ is a homomorphism.

We can now consider if this action is transitive and/or faithful.
For transitivity, let $x, y \in G$. We want to show that there exists $g \in G$ such that $gx = y$. Choose $g = yx^{-1}$. Then

$$\begin{aligned} \phi(g)(x) &= (yx^{-1})x \\ &= y(x^{-1}x) \\ &= y. \end{aligned}$$

Therefore, G acts transitively on G in this way.
To show faithful, we want $Ker\phi = \{x \mid \phi(x) = 1\} = \{1\}$. Choose $x \in Ker\phi$. Then $\phi(x) = 1$. Now let $y \in G$. Then

$$\begin{aligned} \phi(x)(y) &= y \\ xy &= y \\ xyy^{-1} &= yy^{-1} \\ x &= 1. \end{aligned}$$

Therefore, G acts faithfully on G.

Theorem 3.1 *Let a group G act on a set S. Then*

$$S = \bigcup_{a \in S} Ga$$

and the union can be chosen to be disjoint.

Proof. Since $Ga = \{ga \mid g \in G\} \subseteq S$ for all $a \in S$, clearly

$$\bigcup_{a \in S} Ga \subseteq S.$$

Now let $b \in S$. Then $b = 1b \in Gb$. Then

$$S \subseteq \bigcup_{a \in S} Ga.$$

Therefore,

$$S = \bigcup_{a \in S} Ga.$$

Now we claim if there are two elements $a, b \in S$ such that $Ga \cap Gb \neq \emptyset$, then $Ga = Gb$.

Let $g_1, g_2 \in G$ such that $g_1 a = g_2 b$. Then

$$\begin{aligned}
g_1^{-1}(g_1 a) &= g_1^{-1}(g_2 b) \\
(g_1^{-1} g_1) a &= (g_1^{-1} g_2) b \\
1a &= (g_1^{-1} g_2) b \\
a &= g_1^{-1} g_2 b.
\end{aligned}$$

Now

$$\begin{aligned}
Ga &= \{ga \mid g \in G\} \\
&= \{g(g_1^{-1} g_2 b) \mid g \in G\} \\
&= \{gb \mid g \in G\} \\
&= Gb.
\end{aligned}$$

Hence, the claim holds, and the union can be chosen to be disjoint.

Definition: Let a group G act on a set S, and $a \in S$. Then the **stabilizer** in G of a is

$$G_a = \{g \in G \mid ga = a\}.$$

Theorem 3.2 *Let a group G act on a set S, and $a \in S$. Then*

$$G_a \leq G.$$

Theorem 3.3 *Let a group G act on a set S, and $a \in S$. Then*

$$|Ga| = \frac{|G|}{|G_a|}.$$

Proof. Let $T = \{gG_a \mid g \in G\}$. Define $\theta : Ga \to T$ by $\theta(ga) = gG_a$.
First we need to show that θ is well defined.
Let $g_1a, g_2a \in Ga$, and suppose $g_1a = g_2a$. Show $\theta(g_1a) = \theta(g_2a)$.
Since $g_1a = g_2a$, $g_2^{-1}g_1a = a$. Therefore, $g_2^{-1}g_1a \in G_a$. Then

$$\begin{aligned} g_1G_a &= g_2G_a \\ \theta(g_1a) &= \theta(g_2a). \end{aligned}$$

Therefore, θ is well defined.

Now we must show θ is one-to-one and onto.

Suppose there exists $g_1a, g_2a \in Ga$ such that $\theta(g_1a) = \theta(g_2a)$.
Show $g_1a = g_2a$.

$$\begin{aligned} \theta(g_1a) &= \theta(g_2a) \\ g_1G_a &= g_2G_a \\ g_2^{-1}g_1 &\in G_a \\ g_2^{-1}g_1a &= a \\ g_1a &= g_2a. \end{aligned}$$

Therefore, θ is one-to-one.

Now let $x \in G$, and $xG_a \in T$. Then $\theta(xa) = xG_a$, and $xa \in Ga$.
Therefore, θ is onto.

Thus, $|Ga| = |T|$, where $|T|$ is the number of left cosets of G_a.
And so, by Theorem 2.4,

$$|Ga| = \frac{|G|}{|G_a|}.$$

Definition: Let G be a finite group, and let p be a prime. Then G is a **p-group** if there exists $n \in \mathbf{Z}^+ \bigcup \{0\}$ such that $|G| = p^n$.

Example: $|D_4| = 8 = 2^3$, so D_4 is a 2-group.

Example: $|\mathbf{Z}_5 \times \mathbf{Z}_5| = 25 = 5^2$, so $\mathbf{Z}_5 \times \mathbf{Z}_5$ is a 5-group.

Example: $|S_3| = 6 = 2 \cdot 3$, which is not a power of a prime, so S_3 is not a p-group.

Theorem 3.4 (Fixed Point Theorem). *Let G be a p-group, and S be a set such that G acts on S. If p does not divide $|S|$, then there exists $a \in S$ such that $G = G_a$.*

Proof. Since G acts on S, we know $S = \dot{\bigcup}_{a \in S} Ga$ by Theorem 3.1. Therefore,

$$\begin{aligned} |S| &= |\dot{\bigcup_{a \in S}} Ga| \\ &= \sum_{a \in S} |Ga| \\ &= \sum_{a \in S} \frac{|G|}{|G_a|}. \end{aligned}$$

Now if p divides $\frac{|G|}{|G_a|}$ for all $a \in S$, then p divides $\sum_{a\in S} \frac{|G|}{|G_a|} = |S|$, which is a contradiction. Therefore, there exists $a \in S$ such that p does not divide $\frac{|G|}{|G_a|}$. But since G is a p-group, we know $\frac{|G|}{|G_a|}$ is a power of p. This implies $\frac{|G|}{|G_a|} = p^0 = 1$. Thus $\frac{|G|}{|G_a|} = 1$, or $|G| = |G_a|$. Consequently,

$$G = G_a.$$

Now as we approach Sylow's Theorem, we need to address Cauchy's Theorem and the class equation.

Theorem 3.5 (Cauchy's Theorem). *Let G be a group, p be a prime such that p divides $|G|$. Then there exists*

$$1 \neq x \in G \textit{ such that } x^p = 1.$$

Proof. Let

$$S = \{(x_1, x_2, ..., x_p) \mid x_i \in G \text{ for all } 1 \leq i \leq p, \prod_{i=1}^{p} x_i = 1 \text{ and } x_i \text{ not all } 1\}.$$

To show $S \neq \emptyset$, let $1 \neq x \in G$. Then $(x, x^{-1}, 1, 1, ..., 1) \in S$. Now $\mid S \mid = \mid G \mid^{p-1} \cdot 1 - 1$. Since p divides $|G|$, p divides $|G|^{p-1} \cdot 1$. If p divides $|S|$, then p divides $|G|^{p-1} \cdot 1 - |S| = 1$, which is a contradiction. Therefore, p does not divide $|S|$.

Now let $\mathbf{Z_p} = \{0, 1, 2, ..., p-1\} = \langle 1 \rangle$ act on S by
$1((x_1, x_2, ..., x_p)) = (x_p, x_1, ..., x_{p-1})$ for all $(x_1, x_2, ..., x_p) \in S$. Since $\mathbf{Z_p}$ is a p-group and p does not divide $|S|$, by Theorem 3.4, there exists
$(x_1, x_2, ..., x_p) \in S$ such that $(\mathbf{Z_p})_{(x_1, x_2, ..., x_p)} = \mathbf{Z_p}$.

Hence,

$$\begin{aligned}
(x_1, x_2, ..., x_{p-1}, x_p) &= 1(x_1, x_2, ...x_{p-1}, x_p) = (x_p, x_1, x_2, ..., x_{p-1}) \\
(x_1, x_2, ..., x_{p-1}, x_p) &= 2(x_1, x_2, ...x_{p-1}, x_p) = (x_{p-1}, x_p, x_1, ..., x_{p-2}) \\
&\vdots \\
(x_1, x_2, ..., x_{p-1}, x_p) &= (p-1)(x_1, x_2, ...x_{p-1}, x_p) = (x_2, x_3, ..., x_{p-1}, x_p, x_1).
\end{aligned}$$

Thus $x_1 = x_2 = x_3 = \cdots = x_{p-1} = x_p = x$. But then $x \neq 1$ and $x^p = \prod_{i=1}^{p} x_i = 1$.

Theorem 3.6 (The Class Equation). *Let G be a group. Then*

$$|G| = \sum_{a \notin Z(G)} \frac{|G|}{|C_G(a)|} + |Z(G)|.$$

Proof. Let G act on itself by conjugation. Then by Theorem 3.1

$$\begin{aligned}
G &= \dot{\bigcup_{a \in G}} Ga. \\
\text{Hence, } |G| &= |\dot{\bigcup_{a \in G}} Ga| \\
&= \sum_{a \in G} |Ga| \\
&= \sum_{a \in G} \frac{|G|}{|G_a|} \\
&= \sum_{a \in G} \frac{|G|}{|C_G(a)|} \\
&= \sum_{a \notin Z(G)} \frac{|G|}{|C_G(a)|} + |Z(G)|.
\end{aligned}$$

We are ready to consider Sylow's Theorem.

4 Sylow's Theorem

We will again start with a definition and some examples.

Definition: Let G be a group, p be a prime, and $n \in \mathbf{Z}^+ \cup \{0\}$ such that p^n divides $|G|$, but p^{n+1} does not divide $|G|$. Then

(1) $|G|_p = p^n$, called the **pth part of** G.

(2) A subgroup $P \leq G$ is called a **Sylow p-subgroup** if $|P| = |G|_p$.

(3) $Syl_p(G)$ is the set of all Sylow p-subgroups of G.

Example: $S_3 = \{1, (123), (132), (12), (13), (23)\}$, $|S_3| = 3! = 6 = 2 \cdot 3$. Then $|S_3|_2 = 2^1$ and $|S_3|_3 = 3^1$, where $\langle (12) \rangle = \{1, (12)\} \in Syl_2(S_3)$, $\langle (13) \rangle = \{1, (13)\} \in Syl_2(S_3)$, $\langle (23) \rangle = \{1, (23)\} \in Syl_2(S_3)$ and
$\langle (123) \rangle = \{1, (123), (132)\} \in Syl_3(S_3)$.

Example:
$A_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$,
$|A_4| = \frac{4!}{2} = 12 = 2^2 \cdot 3$. Then $|A_4|_2 = 2^2$ and $|A_4|_3 = 3^1$, where
$\langle (12)(34) \rangle = \langle (13)(24) \rangle = \langle (14)(23) \rangle =$
$\{1, (12)(34), (13)(24), (14)(23)\} \in Syl_2(A_4)$,and
$\langle (123) \rangle = \{1, (123), (132)\} \in Syl_3(A_4)$,
$\langle (124) \rangle = \{1, (124), (142)\} \in Syl_3(A_4)$,
$\langle (134) \rangle = \{1, (134), (143)\} \in Syl_3(A_4)$,
$\langle (234) \rangle = \{1, (234), (243)\} \in Syl_3(A_4)$.

Theorem 4.1 (Sylow's Theorem). *Let G be a group, and p be a prime. Then*

(1) $Syl_p(G) \neq \emptyset$.

(2) If $H \leq G$ is a p-subgroup, then there exists $P \in Syl_p(G)$ such that $H \leq P$.

(3) G acts transitively on $Syl_p(G)$ by conjugation.

(4) $|Syl_p(G)| \equiv 1 (mod\ p)$.

(5) $|Syl_p(G)|$ divides $|G|$ and $|Syl_p(G)| = \dfrac{|G|}{|N_G(P)|}$ for all $P \in Syl_p(G)$.

Proof. (1). We will use induction to complete this proof.

If $|G| = 1$ or p does not divide $|G|$, then $|G|_p = p^0$, and so $\{1\} \in Syl_p(G)$. Without loss of generality, $|G| > 1$, p divides $|G|$, and $Syl_p(G) \neq \emptyset$ holds for all groups of order less than $|G|$. We now want to show this is true for all groups of order$|G|$.

Suppose p does not divide $|Z(G)|$. By the class equation,

$$|G| = \sum_{a \notin Z(G)} \frac{|G|}{|C_G(a)|} + |Z(G)|.$$

If p divides $\dfrac{|G|}{|C_G(a)|}$ for all $a \notin Z(G)$, then

$$p \text{ divides } \sum_{a \notin Z(G)} \frac{|G|}{|C_G(a)|}.$$

But then, since p divides $|G|$, we get

$$p \text{ divides } |G| - \sum_{a \notin Z(G)} \frac{|G|}{|C_G(a)|} = |Z(G)|,$$

which is a contradiction. So, there exists at least one of the summands which p does not divide. Hence, there exists $a \notin Z(G)$ such that p does not divide $\frac{|G|}{|C_G(a)|}$. Thus $|G|_p = |C_G(a)|_p$.
Also, $C_G(a) < G$, since $a \notin Z(G)$. Thus $|C_G(a)| < |G|$, and so by induction, there exists $P \in Syl_p(C_G(a))$. But since $|G|_p = |C_G(a)|_p$, we get $P \in Syl_p(G)$.

If p divides $|Z(G)|$, then by Theorem 3.5, there exists $1 \neq z \in Z(G)$ such that $z^p = 1$. Then $\langle z \rangle \trianglelefteq G$ and so $\frac{G}{\langle z \rangle}$ is a group. Also,

$$\left| \frac{G}{\langle z \rangle} \right| = \frac{|G|}{|\langle z \rangle|} < |G|.$$

Hence by induction, there exists $P \in Syl_p\left(\frac{G}{\langle z \rangle}\right)$.
Now let $\phi : G \to \frac{G}{\langle z \rangle}$ be defined by $\phi(G) = g\langle z \rangle$ for all $g \in G$. Then ϕ is a homomorphism, and $Ker\phi = \langle z \rangle$. Then $\langle z \rangle \leq \phi^{-1}(P) \leq G$. Since $\langle z \rangle \trianglelefteq G$, then $\langle z \rangle \trianglelefteq \phi^{-1}(P)$ and so $\frac{\phi^{-1}(P)}{\langle z \rangle}$ is a group. Now

$$\begin{aligned}
\frac{\phi^{-1}(P)}{\langle z \rangle} &= \{g\langle z \rangle \mid g \in \phi^{-1}(P)\} \\
&= \{g\langle z \rangle \mid \phi(g) \in P\} \\
&= \{g\langle z \rangle \mid g\langle z \rangle \in P\} \\
&= P.
\end{aligned}$$

Now

$$
\begin{aligned}
|\phi^{-1}(P)| &= \frac{|\phi^{-1}(P)|}{|\langle z\rangle|}\cdot|\langle z\rangle| \\
&= |P|\cdot|\langle z\rangle| \\
&= \left|\frac{G}{\langle z\rangle}\right|_p\cdot|\langle z\rangle| \\
&= \frac{|G|_p}{|\langle z\rangle|_p}\cdot|\langle z\rangle| \\
&= \frac{|G|_p}{p}\cdot p \\
&= |G|_p.
\end{aligned}
$$

Thus $\phi^{-1}(P)\in Syl_p(G)$, and $Syl_p(G)\neq\emptyset$.

(2). Let $H\leq G$ be a p-subgroup. By part (1), there exists $P\in Syl_p(G)$. Let G act on $S=\{gP\mid g\in G\}$ by left multiplication. Then H acts on S in the same way. Now by Theorem 2.4, $|S|=\dfrac{|G|}{|P|}$. But then p does not divide $\dfrac{|G|}{|P|}=|S|$ since $P\in Syl_p(G)$. Now by Theorem 3.4, since the p-group H acts on S and p does not divide S, there exists $gP\in S$ such that $H_{gP}=H$. Now $H=H_{gP}\leq G_{gP}=gPg^{-1}$. But $gPg^{-1}\leq G$ and $|gPg^{-1}|=|P|=|G|_p$. Hence, $H\leq gPg^{-1}$ and $gPg^{-1}\in Syl_p(G)$.

(3). Let $P,Q\in Syl_p(G)$, and let G act on $Syl_p(G)$ by conjugation. Since P is a p-subgroup and Q is a Sylow p-subgroup, by the same argument used in part (2), there exists $g\in G$ such that $P\leq gQg^{-1}$. Then

$$|G|_p=|P|\leq|gQg^{-1}|=|Q|=|G|_p.$$

Hence $|P|=|gQg^{-1}|$, and so $P=gQg^{-1}$. Therefore, since all the subgroups are conjugate to each other, G acts transitively on $Syl_p(G)$ by conjugation.

(4). Let $P \in Syl_p(G)$. Then P acts on $Syl_p(G)$ by conjugation, and. let $\{P_1, P_2, \ldots, P_r\}$ be all conjugates of P. Since G acts on $Syl_p(G)$ by conjugation, P acts on $\{P_1, P_2, \ldots, P_r\}$ by conjugation. Renumber the elements of $\{P_1, P_2, \ldots, P_r\}$ so that the first n elements of $\{P_1, P_2, \ldots, P_r\}$ are representive of the P-orbits and $P \neq P_i$ for any i. Then there exists $n \in \mathbf{Z}^+$ and $P_i \in Syl_p(G)$ such that

$$\begin{aligned}
Syl_p(G) &= PP \cup \bigcup_{i=1}^{n} PP_i \\
\text{and so } |Syl_p(G)| &= |PP \cup \bigcup_{i=1}^{n} PP_i| \\
&= |PP| + \sum_{i=1}^{n} |PP_i| \\
&= |\{P\}| + \sum_{i=1}^{n} |PP_i| \\
&= 1 + \sum_{i=1}^{n} \frac{|P|}{|P_{P_i}|} \\
&= 1 + \sum_{i=1}^{n} \frac{|P|}{|N_P(P_i)|}.
\end{aligned}$$

If there exists $1 \leq i \leq n$ such that $\dfrac{|P|}{|N_P(P_i)|} = 1$, then $P = N_P(P_i) \leq N_G(P_i)$. Since $P \in Syl_p(G)$, we get $P \in Syl_p(N_G(P_i))$. Also, $P_i \leq N_G(P_i)$ and so $P_i \in Syl_p(N_G(P_i))$. Hence, by part (3), there exists $n \in N_G(P_i)$ such that $P = nP_in^{-1} = P_i$. Hence, $P = P_i \in PP \cap PP_i = \emptyset$. But this is a contradiction. Therefore, p divides $\dfrac{|P|}{|N_P(P_i)|}$ for all $1 \leq i \leq n$, and so

$$p \text{ divides } \sum_{i=1}^{n} \frac{|P|}{|N_P(p_i)|} = |Syl_p(G)| - 1.$$

Therefore, $|Syl_p(G)| \equiv 1 (\text{mod } p)$.

(5). By part (3), G acts transitively on $Syl_p(G)$ by conjugation. Thus, $Syl_p(G) = GP$, where $P \in Syl_p(G)$. Then

$$\begin{aligned} |Syl_p(G)| &= |GP| \\ &= \frac{|G|}{|G_p|} \\ &= \frac{|G|}{|N_G(P)|}. \end{aligned}$$

Therefore, $|Syl_p(G)|$ divides $|G|$.

Theorem 4.2 *Let G be a group, $P \in Syl_p(G)$, and $N \trianglelefteq G$. Then*

$$P \cap N \in Syl_p(N).$$

Proof. We know $P \cap N \leq N$ is a p-subgroup since P is a p-group. By Theorem 4.1, there exists $P_0 \in Syl_p(N)$ such that $P \cap N \leq P_0$. Also by Theorem 4.1, there exists $g \in G$ such that $P_0 \leq gPg^{-1}$. Then

$$\begin{aligned} P \cap N &\leq P_0 \\ &\leq gPg^{-1} \cap N \\ &= gPg^{-1} \cap gNg^{-1} \\ &= g(P \cap N)g^{-1}. \end{aligned}$$

But $|P \cap N| = |g(P \cap N)g^{-1}|$, and so $P \cap N = P_0 \in Syl_p(N)$.

Theorem 4.3 (Frattini Argument) *Let G be a group, $N \trianglelefteq G$, and $P \in Syl_p(N)$. Then*

$$G = N_G(P)N.$$

Proof. Clearly, $G \supseteq N_G(P)N$, since G is a group. Now let $g \in G$. Then $g^{-1} \in G$. Then $P \leq N$ implies $g^{-1}P(g^{-1})^{-1} \leq g^{-1}N(g^{-1})^{-1}$. But since $N \trianglelefteq G$, $g^{-1}N(g^{-1})^{-1} = N$ and so $g^{-1}P(g^{-1})^{-1} \leq N$. Now $|g^{-1}P(g^{-1})^{-1}| = |P| = |G|_p$, and so $g^{-1}Pg \in Syl_p(N)$. By Theorem 4.1, there exists $n \in N$ such that $ng^{-1}Pgn^{-1} = P$. Hence, $ng^{-1} \in N_G(P)$. Thus there exists $x \in N_G(P)$ such that $ng^{-1} = x$, or $g = x^{-1}n \in N_G(P)N$. Therefore, $G \subseteq N_G(P)N$, and consequently, $G = N_G(P)N$.

We now need to look at some additional conditions necessary for our main result, beginning with solvable groups.

5 Solvable Groups

Definition: A group G is **solvable** if there exists a normal series

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

such that $\dfrac{G_i}{G_{i+1}}$ is abelian for all $0 \leq i \leq n-1$.

Example: S_3 is solvable since $S_3 \trianglerighteq A_3 \trianglerighteq 1$ and $\left|\dfrac{S_3}{A_3}\right| = \dfrac{|S_3|}{|A_3|} = \dfrac{6}{3} = 2$ where $\dfrac{S_3}{A_3} \cong \mathbf{Z_2}$ is abelian and $\dfrac{A_3}{\{1\}} \cong \mathbf{Z_3}$ is abelian.

Example: Let G be an abelian group. Then G is solvable since $G \trianglerighteq 1$ and $\dfrac{G}{\{1\}}$ is abelian.

Example: A_4 is solvable since $A_4 \trianglerighteq H \trianglerighteq \{1\}$ where $H = \{1, (12)(34), (14)(23), (13)(24)\}$ and $\left|\dfrac{A_4}{H}\right| = \dfrac{|A_4|}{|H|} = \dfrac{12}{4} = 3$. Thus $\dfrac{A_4}{H} \cong \mathbf{Z_3}$ is abelian and $\dfrac{H}{\{1\}} \cong H$ is abelian.

Example: A_5 is not solvable, since A_5 is simple and nonabelian.

Theorem 5.1 *Let G be a solvable group, and $H \leq G$. Then H is solvable.*

Proof. Since G is solvable, there exists $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$ such that $\frac{G_i}{G_{i+1}}$ is abelian for all $0 \leq i \leq n-1$. Then
$H = H \cap G_0 \trianglerighteq H \cap G_1 \trianglerighteq \cdots \trianglerighteq H \cap G_n = 1$. Now we take an arbitrary factor and show that it is abelian. Choose $\frac{H \cap G_i}{H \cap G_{i+1}}$ for some i. Then

$$\begin{aligned} \frac{H \cap G_i}{H \cap G_{i+1}} &= \frac{H \cap G_i}{H \cap G_i \cap G_{i+1}} \text{ since } G_i \supseteq G_{i+1} \\ &\cong \frac{(H \cap G_i)(G_{i+1})}{G_{i+1}} \text{ by Theorem 2.7} \\ &\leq \frac{G_i}{G_{i+1}}. \end{aligned}$$

But $\frac{G_i}{G_{i+1}}$ is abelian. So $\frac{(H \cap G_i)(G_{i+1})}{G_{i+1}}$ is abelian. Hence, $\frac{H \cap G_i}{H \cap G_{i+1}}$ is abelian since it is isomorphic to abelian group. Therefore, H is solvable.

Theorem 5.2 *Let G be a solvable group and $N \trianglelefteq G$. Then $\frac{G}{N}$ is solvable.*

Proof. Since G is solvable, there exists $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$ such that $\frac{G_i}{G_{i+1}}$ is abelian for all $0 \leq i \leq n-1$. Then

$$\frac{G}{N} = \frac{G_0}{N} \trianglerighteq \frac{G_1 N}{N} \trianglerighteq \frac{G_2 N}{N} \trianglerighteq \cdots \trianglerighteq \frac{G_n N}{N} = N.$$

Now we will choose an arbitrary factor and show it is abelian to establish the solvability of $\frac{G}{N}$.

$$\begin{aligned} \frac{G_i N}{N} \Big/ \frac{G_{i+1} N}{N} &\cong \frac{G_i N}{G_{i+1} N} \text{ by Theorem 2.8} \\ &= \frac{G_i G_{i+1} N}{G_{i+1} N} \text{ since } G_i \supseteq G_{i+1} \\ &\cong \frac{G_i}{G_i \cap G_{i+1} N} \text{ by Theorem 2.7} \\ &\cong \frac{G_i}{G_{i+1}} \Big/ \frac{G_i \cap G_{i+1} N}{G_{i+1}} \text{ by Theorem 2.8.} \end{aligned}$$

Since the quotient of an abelian group is also abelian, and $\frac{G_i}{G_{i+1}}$ is abelian for all $0 \le i \le n-1$, $\frac{G_iN}{N} \Big/ \frac{G_{i+1}N}{N}$ is abelian. Therefore, $\frac{G}{N}$ is solvable.

We now need to expand the concept of a normal subgroup to further apply these previous theorems.

Definition: Let G be a group and $N \le G$. Then N is a **minimal normal subgroup** if:

(1) $1 \ne N \trianglelefteq G$.

(2) If $H \le N$ such that $H \trianglelefteq G$, then $H = \{1\}$ or $H = N$.

Example: A_3 is a minimal normal subgroup of S_3. To see this, $\{1\} \ne A_3 \trianglelefteq S_3$ and suppose $H \le A_3$ such that $H \trianglelefteq S_3$. Then since $|A_3| = 3$, $|H| = 1$ or $|H| = 3$. Therefore, $H = \{1\}$ or $H = A_3$, which makes A_3 a minimal normal subgroup of S_3.

Example: Consider $H \le D_4$, where $H = \{1, (12)(34), (13)(24), (14)(23)\}$. Then $\{1\} \ne H \trianglelefteq D_4$. Now $Z(D_4) = \{1, (13)(24)\} \le H$, and $Z(D_4) \trianglelefteq D_4$. But $Z(D_4) \ne \{1\}$ and $Z(D_4) \ne H$. Therefore, H is not a minimal subgroup of D_4.

Definition: Let G be a group. Then $\phi : G \to G$ is an **automorphism** if ϕ is one-to-one, onto, and a homomorphism.

Definition: Let $\mathbf{Aut(G)}$ denote the group of all automorphisms on G under compostition, ie

$$Aut(G) = \{\phi : G \to G \mid \phi \text{ is automorphism}\}.$$

Example: Let $G = 2\mathbf{Z}$, and define $\phi : 2\mathbf{Z} \to 2\mathbf{Z}$ by $\phi(x) = 2x$ for all $x \in 2\mathbf{Z}$. For ϕ to be an automorphism, we need to show that ϕ is a homomorphism, one-to-one, and onto.

To show ϕ is a homomorphism, let $x, y \in G$. Then

$$\begin{aligned}\phi(x+y) &= 2(x+y)\\ &= 2x+2y\\ &= \phi(x)+\phi(y).\end{aligned}$$

Therefore, ϕ is a homomorphism. For ϕ to be one-to-one, consider

$$\begin{aligned}\phi(x) &= \phi(y)\\ 2x &= 2y\\ x &= y.\end{aligned}$$

Therefore, ϕ is one-to-one.
Now we look at onto. We need for all $y \in G$, there exists $x \in G$ such that $\phi(x) = y$. If there exists $x \in 2\mathbf{Z}$ such that $\phi(x) = 2$, then we get $2x = 2$, or $x = 1$, a contradiction. Therefore, ϕ is not onto.
Therefore, ϕ is not an automorphism.

Example: Let G be a group and $g \in G$. Define $\phi : G \to G$ by $\phi(x) = gxg^{-1}$ for all $x \in G$. We want to show that ϕ is an automorphism.
To show ϕ is a homomorphism, let $x, y \in G$. Then

$$\begin{aligned}\phi(xy) &= gxyg^{-1}\\ &= gxg^{-1}gyg^{-1}\\ &= \phi(x)\phi(y).\end{aligned}$$

Therefore, ϕ is a homomorphism.

To show ϕ is one-to-one, consider

$$\begin{aligned} \phi(x) &= \phi(y) \\ gxg^{-1} &= gyg^{-1} \\ x &= y. \end{aligned}$$

Therefore, ϕ is one-to-one.
Now we look at onto. Let $x \in G$. Then $g^{-1}xg \in G$. So

$$\begin{aligned} \phi(g^{-1}xg) &= g(g^{-1}xg)g^{-1} \\ &= x. \end{aligned}$$

Therefore, ϕ is onto.
Combining these results, we have that ϕ is an automorphism.

Definition: Let G be a group, and $H \leq G$. Then H is a **characteristic subgroup** of G if $\phi(H) \leq H$ for all automorphisms ϕ of G, and is denoted H *char* $\leq G$.

Example: Let $G = \mathbf{Z_{10}}$. Then $\langle 2 \rangle \leq \mathbf{Z_{10}}$. We want to show that $\langle 2 \rangle$ is a characteristic subgroup of $\mathbf{Z_{10}}$. If $\phi : \mathbf{Z_{10}} \to \mathbf{Z_{10}}$ is an automorphism, then $|2| = 5$ and

$$\begin{aligned} 5\phi(2) &= \phi(2) + \phi(2) + \phi(2) + \phi(2) + \phi(2) \\ &= \phi(2 + 2 + 2 + 2 + 2) \\ &= \phi(0) \\ &= 0. \end{aligned}$$

So $|\phi(2)|$ divides 5. Hence, $|\phi(2)| = 1$ or $|\phi(2)| = 5$. If $|\phi(2)| = 1$, then $\phi(2) = 0$. But $\phi(0) = 0$, so then $\phi(2) = \phi(0)$, which contradicts the one-to-oneness of the automorphism ϕ. Therefore, $|\phi(2)| = 5 = |2|$.

Hence,

$$\begin{aligned} |\phi(\langle 2 \rangle)| &= |\langle \phi(2) \rangle| \\ &= |\phi(2)| \\ &= |2| \\ &= 5 \end{aligned}$$

and since $\mathbf{Z_{10}}$ has one subgroup of order 5, namely $\langle 2 \rangle$, we get $\phi(\langle 2 \rangle) = \langle 2 \rangle$, and $|\phi(2)| = 5 = |2|$. So $|\langle \phi(2) \rangle| = |\phi(2)| = |2| = |\langle 2 \rangle|$. Since $\mathbf{Z_{10}}$ is cyclic it has only one subgroup of order 5. Hence $\langle \phi(2) \rangle = \langle 2 \rangle$. But then, since ϕ is a homomorphism, $\phi(\langle 2 \rangle) = \langle \phi(2) \rangle = \langle 2 \rangle$. Therefore, $\langle 2 \rangle$ *char* $\leq \mathbf{Z_{10}}$.

Definition: A group G is **characteristically simple** if $\{1\}$ and G are its only characteristic subgroups.

Example: $\mathbf{Z_p}$ is characteristically simple since $\{1\}$ and $\mathbf{Z_p}$ are its only subgroups (by Theorem 2.4).

We can generalize this definition more by stating that if a group is simple, then it is characteristically simple. We will use A_5 as an example.

Example: A_5 is characteristically simple. We can show this by contradiction. Suppose H *char* $\leq A_5$, and let $g \in A_5$. Define $\phi : A_5 \to A_5$ by $\phi(x) = gxg^{-1}$ for all $x \in A_5$. Then ϕ is an automorphism. Since H *char* $\leq A_5$, $\phi(H) \leq H$. Hence, $gHg^{-1} \leq H$, which means $H \trianglelefteq A_5$. But A_5 is simple, and therefore has no nontrivial proper normal subgroups. Therefore, $H = \{1\}$ or $H = A_5$, which means that A_5 is characteristically simple.

Theorem 5.3 *Let G be a characteristically simple group. Then*

$$G \cong G_1 \times G_2 \times \cdots \times G_s \text{ such that } G_i \text{ are isomorphic simple groups.}$$

Proof. Let G be a characteristically simple group and let $\{1\} \neq G_1 \trianglelefteq G$ such that $|G_1|$ is minimal. Also, let $H = \prod_{i=1}^{s} G_i$ such that

(1) $G_i \cong G_1$ for all $1 \leq i \leq s$

(2) $G_i \trianglelefteq G$ for all $1 \leq i \leq s$

(3) $G_i \cap \prod_{j \neq i} G_j = \{1\}$ for all $1 \leq i \leq s$

(4) s is maximal.

Then since $G_i \trianglelefteq G$ for all $1 \leq i \leq s$, we get $H \trianglelefteq G$ as the product of normal subgroups is normal. If H is not a characteristic subgroup of G, then there exists $1 \leq i \leq s$ and $\phi \in Aut(G)$ such that $\phi(G_i) \not\leq H$. Then $\phi(G_i) \cap H < \phi(G_i)$. Moreover, since $G_i \trianglelefteq G$, we know $\phi(G_i) \trianglelefteq G$. Hence, since $H \trianglelefteq G$, we get $\phi(G_i) \cap H \trianglelefteq G$. But

$$\begin{aligned} |\phi(G_i) \cap H| &< |\phi(G_i)| \\ &= |G_i| \\ &= |G_1|. \end{aligned}$$

Hence, $\phi(G_i) \cap H = \{1\}$ by the minimality of $|G_1|$. Also,
$\phi(G_i) \cap \prod_{i=1}^{s} G_i = \phi(G_i) \cap H = \{1\}$. Moreover, from condition (1),
$\phi(G_i) \cong G_i \cong G_1$. But then $\prod_{i=1}^{s} G_i < \phi(G_i) \times \prod_{i=1}^{s} G_i$, contradicting the maximality of s. Therefore, H *char* $\leq G$ and since $H \neq \{1\}$ and G is characteristically simple, we get $G = H = \prod_{i=1}^{s} G_i$.

Now we need to show that these are isomorphic simple groups. We know that they are isomorphic from condition (1). So now let $1 \leq i \leq s$ and $N \leq G_i$ such that $N \triangleleft G_i$. We need to show $N = \{1\}$ or $N = G_i$ to show G_i is simple.

If $x \in G_j$ for some $j \neq i$ and $n \in N$ (which implies $n \in G_i$ since $N \lhd G_i$), then $xnx^{-1}n^{-1} \in G_i$. Also, $xnx^{-1}n^{-1} \in G_j$. So, $xnx^{-1}n^{-1} \in G_i \cap G_j \leq G_i \cap \prod_{j \neq i} G_j = \{1\}$ from condition (3). This implies $xnx^{-1}n^{-1} = 1$. Hence $xn = nx$ and so $G_j \leq C_G(N)$ for all $j \neq i$. But then $N \trianglelefteq \prod_{i=1}^{s} G_i = G$. Now $|N| \leq |G_i| = |G_1|$. Hence by the minimality of $|G_1|$, $|N| = 1$ or $|N| = |G_1|$. Therefore, $N = \{1\}$ or $N = G_i$, and so G_i is simple.

We can now determine what minimal normal subgroups of solvable groups look like.

Theorem 5.4 *Let G be a solvable group, and N be a minimal normal subgroup of G. Then*

$$N \cong \mathbf{Z_p} \times \mathbf{Z_p} \times \cdots \times \mathbf{Z_p} \text{ for some prime } p.$$

Proof. If $L \; char \leq N$ and $g \in G$, define $\phi : N \to N$ by $\phi(n) = gng^{-1}$ for all $n \in N$. Since $N \trianglelefteq G$, we get $\phi \in Aut(N)$. But since $L \; char \leq N$, we know $\phi(L) \leq L$. Hence, $gLg^{-1} \leq L$ and $L \trianglelefteq G$. Since N is a minimal normal subgroup of G, $L = \{1\}$ or $L = N$. Thus N is characteristically simple, which means it has no other characteristic subgroups. By Theorem 5.3, $N \cong \prod_{i=1}^{s} N_i$ where the N_i are isomorphic simple groups. We consider N_1. If N_1 is not abelian, then since N_1 is simple, the only normal series in N_1 is $N_1 \trianglerighteq \{1\}$. But $\frac{N_1}{\{1\}} \cong N_1$ which is not abelian, and so N_1 is not solvable. But $N \leq G$, and G is solvable. This contradicts Theorem 5.1. So therefore, N_i has to be abelian for all $1 \leq i \leq s$. Now, since N_i is simple for all $1 \leq i \leq s$, we get $\{1\}$ and N_i are the only subgroups of N_i for all $1 \leq i \leq s$. But then by Theorem 3.5, N_i is a p-group for some prime p, and $N_i \cong \mathbf{Z_p}$. Thus, $N \cong \mathbf{Z_p} \times \mathbf{Z_p} \times \cdots \times \mathbf{Z_p}$ (s factors).

We are now ready to introduce our main result.

6 Hall's Theorem

Definition: Let G be a group and π be a set of primes. Then:

(1) $\pi^{'} = \{p \mid p \text{ is prime and } p \notin \pi\}$.

(2) $\pi(G) = \{p \mid p \text{ is prime and } p \text{ divides } |G|\}$.

(3) G is a π-group if $\pi(G) \subseteq \pi$.

(4) A subgroup $H \leq G$ is called a **Hall π-subgroup** if H is a π-group and $\pi\left(\frac{G}{H}\right) \subseteq \pi'$.

(5) $Hall_{\pi}(G)$ is the set of all Hall π-subgroups of G.

Example: $|D_{15}| = 30 = 2 \cdot 3 \cdot 5$. Let $H = \langle(1, 2, 3, ..., 15)\rangle$. Then $|H| = 15 = 3 \cdot 5$, so $H \in Hall_{\{3,5\}}(D_{15})$.

Example: $Hall_{\{2,5\}}(A_5) = \emptyset$. If $H \in Hall_{\{2,5\}}(A_5)$, then $|A_5| = \frac{5!}{2} = 2^2 \cdot 3 \cdot 5$ and $|H| = 2^2 \cdot 5 = 20$. Let A act on $S = \{gH \mid g \in A_5\}$ by left multiplication via ϕ. Now $|S| = \frac{|A_5|}{|H|} = \frac{60}{20} = 3$ by Theorem 2.4. Hence $\phi : A_5 \to Sym(S) \cong S_3$. Now $Ker\phi \trianglelefteq A_5$ and so $Ker\phi = \{1\}$ or $Ker\phi = A_5$ since A_5 is simple.

Consider $Ker\phi = A_5$. Then

$$\begin{aligned} A_5 &= Ker\phi \\ &= \bigcap_{x \in A_5} xHx^{-1} \\ &\leq H \\ &\leq A_5 \end{aligned}$$

and so we get $A_5 = H$ if $Ker\phi = A_5$, which is a contradiction. Therefore, $Ker\phi \neq A_5$, and $Ker\phi = \{1\}$. Then

$$A_5 = \frac{A_5}{\{1\}} = \frac{A_5}{Ker\phi} \cong \phi(A_5) \leq S_3.$$

Hence, we get $60 = |A_5|$ divides $|S_3| = 6$, which is a contradiction. Therefore, $Ker\phi \neq \{1\}$.

Therefore, $H \notin Hall_{\{2,5\}}(A_5)$, and so $Hall_{\{2,5\}}(A_5) = \emptyset$.

But consider $(A_5)_1$ in $|A_5| = 2^2 \cdot 3 \cdot 5$. Then $(A_5)_1 \cong A_4$ and so $|(A_5)_1| = |A_4| = \frac{4!}{2} = 12 = 2^2 \cdot 3$. Thus $(A_5)_1 \in Hall_{\{2,3\}}(A_5)$.

Theorem 6.1 *Let G be a group, π be a set of primes, $H \in Hall_\pi(G)$, and $N \trianglelefteq G$. Then*

$$\frac{HN}{N} \in Hall_\pi\left(\frac{G}{N}\right).$$

Proof. Now

$$\begin{aligned} \left|\frac{HN}{N}\right| &= \frac{|HN|}{|N|} \\ &= \frac{\frac{|H||N|}{|H \cap N|}}{|N|} \text{ by Theorem 2.7} \\ &= \frac{|H|}{|H \cap N|}. \end{aligned}$$

But since $H \in Hall_\pi(G)$, $\pi(H) \subseteq \pi$, and so $\pi\left(\frac{H}{H \cap N}\right) \subseteq \pi$. Thus $\pi\left(\frac{HN}{N}\right) \subseteq \pi$, and $\frac{HN}{N}$ is a π-group.

Also,

$$\begin{aligned}\frac{\left|\frac{G}{N}\right|}{\left|\frac{HN}{N}\right|} &= \frac{\frac{|G|}{|N|}}{\frac{|HN|}{|N|}} \\ &= \frac{|G|}{|HN|}.\end{aligned}$$

But $\frac{|G|}{|H|} = \frac{|G|}{|HN|} \cdot \frac{|HN|}{|N|}$ and so $\frac{|G|}{|HN|}$ divides $\frac{|G|}{|H|}$. But $\pi\left(\frac{G}{H}\right) \subseteq \pi'$ since $H \in Hall_\pi(G)$. Hence, since $\frac{|G|}{|HN|}$ divides $\frac{|G|}{|H|}$, we get $\pi\left(\frac{G}{HN}\right) \subseteq \pi'$. Thus, $\frac{HN}{N} \in Hall_\pi\left(\frac{G}{N}\right)$.

Theorem 6.2 (Hall's Theorem) *Let G be a solvable group and π be a set of primes. Then:*

(1) $Hall_\pi(G) \neq \emptyset$.

(2) If $K \leq G$ is a π-subgroup and $M \in Hall_\pi(G)$, then there exists $g \in G$ such that $K \leq gMg^{-1}$.

Proof. We will use induction to complete this proof.

We start with $|G| = 1$. Then $\{1\} \in Hall_\pi(G)$. Now we assume that the theorem holds for all solvable groups of order less than $|G|$. We want to show that the theorem holds for groups of order $|G|$.

Let N be a minimal normal subgroup of G. Since $N \trianglelefteq G$, $\frac{G}{N}$ is a group, and since G is solvable, $N \cong \mathbf{Z_p} \times \mathbf{Z_p} \times \cdots \times \mathbf{Z_p}$ for some prime p. Now, since G is solvable, by Theorem 5.2, $\frac{G}{N}$ is solvable. Moreover, $\left|\frac{G}{N}\right| = \frac{|G|}{|N|} < |G|$ since $N \neq \{1\}$ because N is minimal normal subgroup. By induction, there exists $\frac{H}{N} \in Hall_\pi\left(\frac{G}{N}\right)$. Then $H \leq G$.

We first consider the case when $p \in \pi$.
Then $|H| = \frac{|H|}{|N|} \cdot |N|$. But $\pi\left(\frac{H}{N}\right) \subseteq \pi$ since $\frac{H}{N} \in Hall_\pi(\frac{G}{N})$ and $\pi(N) \subseteq \pi$ since $p \in \pi$. Thus $\pi(H) \subseteq \pi$, and so H is a π-group.
Also, $\frac{|G|}{|H|} = \frac{\frac{|G|}{|N|}}{\frac{|H|}{|N|}}$, and $\pi\left(\frac{\frac{G}{N}}{\frac{H}{N}}\right) \subseteq \pi'$ since $\frac{H}{N} \in Hall_\pi\left(\frac{G}{N}\right)$. Thus $\pi\left(\frac{G}{H}\right) \subseteq \pi'$, and so $H \in Hall_\pi(G)$. Therefore, $Hall_\pi(G) \neq \emptyset$.
Now if $K \leq G$ is a π-subgroup and $M \in Hall_\pi(G)$, then $\frac{KN}{N} \leq \frac{G}{N}$ is a π-subgroup and $\frac{MN}{N} \in Hall_\pi\left(\frac{G}{N}\right)$ by Theorem 6.1. Again, since $\frac{G}{N}$ is solvable and $\left|\frac{G}{N}\right| < |G|$, by induction there exists $gN \in \frac{G}{N}$ such that

$$\begin{aligned} \frac{KN}{N} &\leq (gN)\left(\frac{MN}{N}\right)(gN)^{-1} \\ &= \frac{g(MN)g^{-1}}{N}. \end{aligned}$$

Taking preimages, we get $K \leq KN \leq g(MN)g^{-1}$. Then

$$\begin{aligned} |gMNg^{-1}| &= |MN| \\ &= \frac{|M||N|}{|M \cap N|}. \end{aligned}$$

Now since $M \in Hall_\pi(G)$, we get $\pi(gMNg^{-1}) \subseteq \pi$, and so $gMNg^{-1}$ is a π-group. But $gMg^{-1} < gMNg^{-1}$ and $|gMg^{-1}| = |M|$, and so
$gMg^{-1} \in Hall_\pi(G)$ since $M \in Hall_\pi(G)$. Hence, $gMg^{-1} = gMNg^{-1}$, giving us $K \leq gMNg^{-1} = gMg^{-1}$. Therefore, condition (2) is satisfied, and the theorem holds for $p \in \pi$.

Now consider the case when $p \notin \pi$.
We may assume G has no normal π-subgroups. Now by induction, there exists $\frac{H}{N} \in Hall_{\pi}\left(\frac{G}{N}\right)$. Taking preimages, we get $H \leq G$. If $H \neq G$, we know $|H| < |G|$. Also, H is solvable since G is solvable by Theorem 5.1. So by induction, there exists $H_1 \in Hall_{\pi}(H)$. Now

$$\begin{aligned} \frac{|G|}{|H_1|} &= \frac{|G|}{|H|} \cdot \frac{|H|}{|H_1|} \\ &= \frac{\frac{|G|}{|N|}}{\frac{|H|}{|N|}} \cdot \frac{|H|}{|H_1|}. \end{aligned}$$

Thus $\pi\left(\frac{G}{H_1}\right) \subseteq \pi'$ since $\frac{H}{N} \in Hall_{\pi}\left(\frac{G}{N}\right)$ and $H_1 \in Hall_{\pi}(H)$. Hence, $H \in Hall_{\pi}(G)$, yielding condition (1) of the theorem. Now let $K \leq G$ be a π-subgroup and $M \in Hall_{\pi}(G)$. Then $\frac{MN}{N} \in Hall_{\pi}\left(\frac{G}{N}\right)$, and $\frac{KN}{N} \leq \frac{G}{N}$ is a π-subgroup. Since $\left|\frac{G}{N}\right| < |G|$ by induction, there exists $gN \in \frac{G}{N}$ such that $\frac{KN}{N} \leq (gN)\left(\frac{MN}{N}\right)(gN)^{-1}$. Taking preimages, we get
$K \leq KN \leq g(MN)g^{-1}$ as before. Thus $K \leq KN \leq gMg^{-1}N$. Now

$$\begin{aligned} \left|\frac{H}{N}\right| &= \left|\frac{MN}{N}\right| \text{ since both are in } Hall_{\pi}\left(\frac{G}{N}\right) \\ \frac{|H|}{|N|} &= \frac{|MN|}{|N|} \\ |H| &= |MN|. \end{aligned}$$

But $|MN| = |gMNg^{-1}| = |gMg^{-1}N|$. Thus, $|gMg^{-1}N| = |H|$, and so $gMg^{-1}N \neq G$ since $H \neq G$. Thus, $|gMg^{-1}N| < |G|$, and $gMg^{-1}N$ is solvable by Theorem 5.1. Moreover, $K \leq gMg^{-1}N$ is a π-group and $gMg^{-1} \in Hall_{\pi}(gMg^{-1}N)$. Thus by induction, there exists $g_1 \in gMg^{-1}N$ such that $K \leq g_1(gMg^{-1})g_1^{-1} = g_1gM(g_1g)^{-1}$, yielding condition (2) of the theorem.

Now if $H = G$, then $\frac{G}{N} = \frac{H}{N}$ is a π-group, since $\frac{H}{N} \in Hall_\pi\left(\frac{G}{N}\right)$. Let $\frac{R}{N}$ be a minimal normal subgroup of $\frac{G}{N}$. Then since $\frac{G}{N}$ is solvable by Theorem 5.2, we know $\frac{R}{N}$ is an elementary q-group for some prime q, where $q \neq p$. Then $\frac{R}{N} \trianglelefteq \frac{G}{N}$ implies $R \trianglelefteq G$. Since $|R| = \frac{|R|}{|N|} \cdot |N|$, R is a pq-group.
Now let $Q \in Syl_q(R)$. Hence, $\frac{QN}{N} \in Syl_q\left(\frac{R}{N}\right)$ and so $\frac{R}{N} = \frac{QN}{N}$, or $R = QN$. By Theorem 4.3,

$$\begin{aligned} G &= N_G(Q)R \\ &= N_G(Q)QN \\ &= N_G(Q)N. \end{aligned}$$

If $N_G(Q) = G$, then Q is a normal π-subgroup of G since $q \in \pi$. But this is a contradiction. Therefore, $N_G(Q) \neq G$, and so $|N_G(Q)| < |G|$. Now since $N_G(Q)$ is solvable, there exists $H_1 \in Hall_\pi(N_G(Q))$ by induction. Also

$$\begin{aligned} \left|\frac{G}{H_1}\right| &= \frac{|G|}{|N_G(Q)|} \cdot \frac{|N_G(Q)|}{|H_1|} \\ &= \frac{|N_G(Q)N|}{|N_G(Q)|} \cdot \frac{|N_G(Q)|}{|H_1|} \\ &= \frac{|N|}{|N \cap N_G(Q)|} \cdot \frac{|N_G(Q)|}{|H_1|} \end{aligned}$$

which is a π'-number since $p \notin \pi$, $H_1 \in Hall_\pi(N_G(Q))$. Thus, $H_1 \in Hall_\pi(G)$, yielding condition (1) of the theorem.

Now let $K \leq G$ be a π-subgroup and $M \in Hall_\pi(G)$. We can show K lies in a conjugate of M.
If $|K| = |M|$, then by Theorem 4.2, $K \cap R$, $M \cap R \in Syl_q(R)$. So by Theorem 4.1, there exists $r \in R$ such that $r(M \cap R)r^{-1} = (K \cap R)$, or $rMr^{-1} \cap R = K \cap R$. Since $R \trianglelefteq G$, we get $K \cap R \trianglelefteq K$ and $rMr^{-1} \cap R \trianglelefteq rMr^{-1}$. Hence, $K \leq N_G(K \cap R) = N_G(rMr^{-1} \cap R)$, and
$rMr^{-1} \leq N_G(rMr^{-1} \cap R) = N_G(K \cap R)$.

Let $N_1 = N_G(K \cap R)$. If $N_1 = G$, then $N_G(K \cap R) = G$, and so $(K \cap R) \trianglelefteq G$. But $K \cap R$ is a π-subgroup, which is a contradiction. Therefore, $N_1 \neq G$ and $|N_1| < |G|$.
Now $K \leq N$ is a π-group, and since $rMr^{-1} \in Hall_\pi(G)$, we know $rMr^{-1} \in Hall_\pi(N_1)$. Since N_1 is solvable, by induction there exists $n \in N_1$ such that $K \leq nrMr^{-1}n^{-1} = (nr)M(nr)^{-1}$, yielding condition (2) of the theorem.

Now if $|K| < |M|$, then $\frac{MN}{N} \in Hall_\pi\left(\frac{G}{N}\right)$ by Theorem 6.1.
Since $\frac{H}{N} \in Hall_\pi\left(\frac{G}{N}\right)$, we know

$$\begin{aligned}
\left|\frac{MN}{N}\right| &= \left|\frac{H}{N}\right| \\
\frac{|MN|}{|N|} &= \frac{|H|}{|N|} \\
|MN| &= |H| = |G|.
\end{aligned}$$

Hence, $G = H = MN$. Since $N \trianglelefteq G$, $KN \leq G$. Also,

$$\begin{aligned}
\left|\frac{KN}{N}\right| &= \frac{|K||N|}{|K \cap N|} \\
&= \frac{|K||N|}{1} \text{ since } K \text{ is a } \pi\text{-group and } N \text{ is a } \pi'\text{-group} \\
&= \frac{|K||N|}{|M \cap N|} \\
&< \frac{|M||N|}{|M \cap N|} \\
&= |MN| \\
&= |G|.
\end{aligned}$$

Therefore, $|KN| < |G|$. Also, since KN is solvable, the theorem holds for KN by induction.

Now $K \leq KN$ is a π-subgroup and $M \cap KN \leq KN$ is a π-subgroup, so

$$\begin{aligned}\frac{|KN|}{|M \cap KN|} &= \frac{|KNM|}{|M|} \\ &= \frac{|KG|}{|M|} \\ &= \frac{|G|}{|M|}\end{aligned}$$

so $\pi\left(\frac{KN}{M \cap KN}\right) \subseteq \pi'$. Therefore, $M \cap KN \in Hall_\pi(KN)$. So by induction, there exists $x \in KN$ such that

$$\begin{aligned}K &\leq x(M \cap KN)x^{-1} \\ &= xMx^{-1} \cap xKNx^{-1} \\ &\leq xMx^{-1}\end{aligned}$$

which yields condition (2) of the theorem.

Consequently, the proof is complete, and Hall's Theorem holds for solvable groups.

References

[1] Dummit, David S. and Foote, Richard M., *Abstract Algebra 3rd ed.*, John Wiley and Sons Inc., (2004).

[2] Fraleigh, John B., *A First Course in Abstract Algebra 4th ed.*, Addison-Wesley Publishing Co., (1988).

[3] Hall, Philip, "A Note on Soluble Groups", *Journal of the London Mathematical Society*, Volume 2, p 98-105, (1928).

[4] Papatonopoulou, Aigli, *Algebra Pure and Applied*, Prentice Hall, (2002).

[5] Robinson, Derek J. S., *An Introduction to Abstract Algebra*, Walter de Gruyter, (2003).