A Study of Fixed-Point-Free Automorphisms and Solvable Groups

By

EMANUEL PSARAS

Submitted in Partial Fulfillment of the Requirements
for the Degree of

MASTER OF SCIENCE

in the

Mathematics
Program
YOUNGSTOWN STATE UNIVERSITY

MAY, 2020

A Study of Fixed-Point-Free
Automorphisms and Solvable Groups

Emanuel Psaras

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:

Emanuel Psaras, Student

Approvals:

Neil Flowers, Ph.D., Advisor

Tom Wakefield, Ph.D., Committee Member

Thomas Madsen, Ph.D., Committee Member

Dr. Salvatore A. Sanders, Dean of Grad. Studies

A Study of Fixed-Point-Free Automorphisms and Solvable Groups

Abstract

In 1903, Ferdinand Georg Frobenius made a conjecture that can be stated as such: let G be a group and $\phi \in Aut(G)$ such that ϕ acts what is called "fixed point freely" on G. Then, G is a *solvable* group. Throughout the rest of the 20th century many different specific cases of this conjecture have been proved (with the cases putting a restriction on the order of ϕ). For example, in 1959 John Thompson proved this for $|\phi| = p$ for some prime p. Later on in the 70's, Elizabeth Ralston proved this result for $|\phi| = pq$ for two primes p & q.

Finally in the 90's the full conjecture was accepted as being proven as a consequence of some results in the landmark Classification of Finite Simple Groups. As a result, an attempt at an all-encompassing and unified proof of this conjecture has been largely abandoned by group theorists. For this thesis, we will look at a specific case of this conjecture where $|\phi| = 4$ (as also done in Gorenstein and Herstein, 1961) and try to give a formal proof whilst introducing the necessary results used as tools in said proof.

TABLE OF CONTENTS

Chapter One

Preliminaries

In order to give a thorough proof for this case of the Frobenius conjecture, a variety of results will need to be used as tools. In this chapter, the results which are considered to be well-known will be mentioned. Proofs of these will not be given since it can safely be assumed these results are already known to the reader.

Theorem 1.1. *(The First Isomorphism Theorem)*

Let G_1, and G_2 be groups and

$$\phi : G_1 \mapsto G_2 \tag{1.1}$$

be a homomorphism. Then

$$G_1/Ker(\phi) \cong \phi(G_1).$$

The First Isomorphism theorem is one of the most well-known results in mathematics, and is followed by the other two isomorphism theorems.

Theorem 1.2. *(The Second Isomorphism Theorem)*

Let G be a group, $N \trianglelefteq G$ and $H \leq G$. Then,

$$HN/N \cong H/H \cap N\ .$$

Theorem 1.3. *(The Third Isomorphism Theorem)*

Let G be a group, $N \trianglelefteq G$, $H \trianglelefteq G$ and $N \leq H$. Then

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

Although the first isomorphism theorem is likely the most commonly used theorem of the three, these isomorphism theorems play an integral role in describing the relationship between groups and their quotients.

The following result also deals with relating groups to quotients, but this time it is with respect to a specific homomorphism. The homomorphism used is defined below.

Remark 1. *Let G be a group and $N \trianglelefteq G$. Then the map,*

$$\phi : G \mapsto G/N \text{ defined by}$$
$$\phi(g) = gN$$

*is often referred to as the **natural** map.*

Due to this homomorphism's common use, most group theorists just refer to it as the "natural" map without explicitly defining it. This way, any time the natural map is mentioned it should be implicitly understood what the map is.

Remark 2. *Throughout this paper, the natural map will be used to get results in the quotient group and then pre-imaging the results back to the original group. Instead of explicitly giving the map every time, it is best to introduce the notation that will be used to implicitly show the use of the natural map (without spending time writing the whole map out). Let G be a group, and $N \trianglelefteq G$. Then, define*

$$\overline{G} = \frac{G}{N}.$$

At face value, the bar symbol looks as if it stands for just the quotient group, but implicitly, the bar can be thought of as the invoking of the natural map. This notation will be used throughout the rest of the paper.

Theorem 1.4. *Let G be a group, $N \trianglelefteq G$. $H \leq G$, and $\phi : G \mapsto G/N$ be the natural map. Then,*

1. $\phi(H) = HN/N$
2. $\phi^{-1}(HN/N) = HN$
3. *If $L \leq G/N$, then $L = K/N$ where $N \leq K \leq G$.*

This theorem is often called the "correspondence theorem" and is often associated with the three isomorphism theorems.

Much like the isomorphism theorems, the Sylow theorems are also fundamental results in group theory. Here is an overview of the three theorems.

Theorem 1.5. *(Sylow's 1^{st}) Let G be a p-group for some prime p. Then $Syl_p(G) \neq \emptyset$.*

Theorem 1.6. *(Sylow's 2^{nd}) Let G be a group, p be a prime, and $H \leq G$ be a p-subgroup. Then $\exists P \in Syl_p(G)$ such that, $H \leq P$.*

Theorem 1.7. *(Sylow's 3^{rd}) Let G be a group. p be a prime, and $n_p = |Syl_p(G)|$. Then*

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

Sylow's theorems are used regularly by group theorists. Their relation with other groups is analogous to the relation of prime numbers to other integers. In other words, they are thought of as fundamental building blocks to every group (much like prime numbers relation to other integers). This, of course, means that there are a myriad of results concerning Sylow (sub)groups used to characterize bigger groups. Some of these results are given below.

Theorem 1.8. *(Frattini Argument) Let G be a group $N \trianglelefteq G$, and $P \in Syl_p(G)$. Then,*

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

Theorem 1.9. *Let G be a group and $N \trianglelefteq G$, $P \in Syl_p(G)$. Then $P \cap N \in Syl_p(N)$ and $G = N_G(P \cap N)N$*

The concept of Sylow subgroups can be generalized to more than just one prime at a time. For these, we defined a set to indicate which primes divide the order of a given group. Such a definition is given below.

Definition: Let G be a group. Define

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

The set $\pi(G)$ is the set of all primes that divide the order of the group. For example, $\pi(\mathbb{Z}_{10}) = \{2, 5\}$. For the generalized notion of Sylow p-subgroups, we sometimes pick many primes that divide the order of the group as opposed to just one. In those cases, we refer to the set $\pi(G)$.

Definition: Let G be a group, π be the set of primes as above, $H \leq G$, and $n \in \mathbb{Z}^+$. Then,

1. $\pi' = \{p|p \text{ is prime and } p \notin \pi\}$.

2. n is a π-number if $\pi(n) \subseteq \pi$.

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

4. H is a Hall π-subgroup of G if H is a π-group and $\frac{|G|}{|H|}$ is a π'-number.

These Hall π-subgroups can be thought of as generalized Sylow p-subgroups. Sylow subgroups are essentially Hall subgroups where the set of primes that make up the subgroup is just the singular prime, p.

Example: In A_5, we have $|A_5| = 2^2 \cdot 3 \cdot 5$. Consider

$$H = \{1, (123), (132), (234), (243), (134), (143), (124), (142), (12)(34), (13)(24), (14)(23)\}.$$

Then, $H \leq A_5$, in fact, $H = (A_5)_5$ (the stabilizer of 5) and $|H| = 12 = 2^2 \cdot 3$. So H is a $\{2,3\}$ group. Moreover, $\frac{|A_5|}{|H|} = 5$ is a $\{2,3\}'$ number, and hence H is a Hall $\{2,3\}$-group.

Since Hall subgroups can be seen as generalizations of Sylow subgroups, it may seem rational to think that some characteristics of Sylow subgroups also extend to Hall subgroups. In many ways these characteristics do extend to Hall subgroups, but, in certain situations, there needs to be additional structure on the original group itself for these characteristics to extend over. This will be discussed later on as it will play a pivotal role in the proof of the final theorem.

Definition: Let G be a group, and S be some nonempty subset $\emptyset \neq S \subseteq G$. The subgroup generated by S is $\langle S \rangle = \{s_1^{n_1} s_2^{n_2} s_3^{n_3} ... s_k^{n_k} | s_i \in S, n_i \in \mathbb{Z}\}$ $\forall 1 \leq i \leq k$.

Proposition 1. *Let G be a group and $\emptyset \neq S \subseteq G$. Then $\langle S \rangle \leq G$.*

Example Consider $G = S_3 = \{1, (123), (132), (12), (13), (23)\}$, and take $S = \{(12), (13)\}$. Then,

$$\langle (12), (13) \rangle = \{(12)^0 = 1, (12)^1, (12)^2 = 1, (13)^0 = 1, (13)^1, (13)^2 = 1, (12)(13) = (132), (13)(12) = (123), (23)\} = \{1, (123), (132), (12), (13), (23)\} = S_3$$

Lemma 1.10. *Let G be a group and $H \leq G$. Define*

$$H^G = \langle h^g | h \in H and\ g \in G \rangle.$$

This is called the normal closure of H in G. Then, $H^G \trianglelefteq G$.

Proof. By Proposition 1, we know that $H^G \leq G$. Now, let $g \in G$ and $x \in H^G$. Then $x = h_1^{g_1} h_2^{g_2} ... h_n^{g_n}$ where $h_i \in H$, $g_i \in G$. Then

$$x^g = \left(\prod_{i=1}^{n} h_i^{g_i} \right)^g = \prod_{i=1}^{n} (h_i^{g_i g}) \in H^G.$$

Thus $H^G \trianglelefteq G$. □

Definition: Let G be a group, $a, b \in G$, $H \leq G$, and $K \leq G$. Then

1. a conjugated by b is notated as $a^b = b^{-1}ab$.
2. The commutator of a and b is denoted $[a, b] = a^{-1}b^{-1}ab$.
3. The derived subgroup is $G^{'} = \langle [a, b] | a, b \in G \rangle$.
4. The commutator subgroup generated by H and K, is $[H, K] = \langle [h, k] | h \in H, k \in K \rangle$

It may be worth while to note that throughout this paper the exponential notation will be used for conjugation.

Theorem 1.11. *Let G be a group, $N \trianglelefteq G$, $H \leq G$, and $a, b \in G$. Then,*

1. *$[a, b] = 1$ iff $ab = ba$.*

2. *$G^{'} \trianglelefteq G$.*

3. *$\frac{G}{G'}$ is abelian.*

4. *If $\frac{G}{N}$ is abelian then $G^{'} \leq N$.*

5. *If $G^{'} \leq H$, then $H \trianglelefteq G$.*

6. *If $H \leq G$, $N \trianglelefteq G$, then $\frac{HN}{N} \leq Z(\frac{G}{N})$ if and only if $[G, H] \leq N$.*

Some results will require the use of direct products of groups, both internal and external. The external direct product is the standard Cartesian product, but the internal direct product is a bit more technical in it's definition which is given below.

Definition: Let G be a group and $\{H_i\}_{i=1}^{n}$ be a collection of subgroups of G. Then, G is called the internal direct product of these subgroups if

1. $G = \Pi_{i=1}^{n} H_i$.

2. $H_i \trianglelefteq G, \forall 1 \leq i \leq n$.

3. $H \cap \Pi_{j \neq i} H_j = 1, \forall 1 \leq i \leq n$.

This is often denoted by $G = \bigoplus_{i=1}^{n} H_i$.

Now it's important to emphasize one's ability to switch from one direct product or the other. The following theorem draws a strong connection between the two types of products.

Theorem 1.12. *Let G be a group and $\{H_i\}_{i=1}^n$ be a collection of subgroups of G such that*

$$G = \bigoplus_{i=1}^n H_i.$$

Then $G \cong \bigtimes_{i=1}^n H_i$ (external direct product).

Proof. We will prove this by induction. Say $n = 2$, then $G = H_1 H_2$ for $H_1 \trianglelefteq G$, $H_2 \trianglelefteq G$ and $H_1 \cap H_2 = 1$. Define

$$\phi : G \mapsto H_1 \times H_2$$

by

$$\phi(h_1 h_2) = (h_1, h_2).$$

To show well-definedness, say $h_1 h_2 = h_3 h_4$, for $h_1, h_3 \in H_1$, and $h_2, h_4 \in H_2$. Then

$$\phi(h_1 h_2) = (h_1, h_2),$$

$$\phi(h_3 h_4) = (h_3, h_4).$$

Now it follows that

$$h_3^{-1} h_1 h_2 = h_4 \implies h_3^{-1} h_1 = h_4 h_2^{-1}.$$

Now, let $x = h_3^{-1} h_1 = h_4 h_2^{-1}$. Then $x \in H_1$, and $x \in H_2$ which means that $x \in H_1 \cap H_2$, but $H_1 \cap H_2 = 1$ and so

$$h_3^{-1} h_1 = h_4 h_2^{-1} = 1.$$

Thus it must be the case that $h_1 = h_3$ and $h_2 = h_4$, and so $(h_1, h_2) = (h_3, h_4)$. Therefore, ϕ is well-defined.

Now for injectivity, say we have

$$(h_1, h_2) = (h_3, h_4).$$

This means that $h_1 = h_3$ and $h_2 = h_4$ and so

$$h_1h_2 = h_3h_2 = h_3h_4.$$

Thus ϕ is injective.

For surjectivity, let $x \in H_1 \times H_2$. Then $x = (h_1, h_2)$ for $h_1 \in H_1, h_2 \in H_2$. Consider $h_1h_2 \in H_1H_2 = G$. Then

$$\phi(h_1h_2) = (h_1, h_2) = x,$$

and so ϕ is surjective.

Now, to show that ϕ is a homomorphism, let $x = h_1h_2$, $y = h_3h_4$ for $h_1, h_3 \in H_1$, $h_2, h_4 \in H_2$. Then evaluating ϕ at xy, we get

$$\phi(xy) = \phi(h_1h_2h_3h_4).$$

Now, consider $[h_1, h_2] = h_1^{-1}h_2^{-1}h_1h_2$. Realize that since both H_1 and H_2 are normal in G, we get that $[h_1, h_2]$ is an element of both H_1 and H_2, and so $[h_1, h_2] \in H_1 \cap H_2 = 1$. So $[h_1, h_2] = 1$ which means that $h_1h_2 = h_2h_1$ (elements from different h_i's commute with each other). So, from above, we have,

$$\phi(h_1h_2h_3h_4) = \phi(h_1h_3h_2h_4) = (h_1h_3, h_2h_4) = (h_1, h_2)+(h_3, h_4) = \phi(h_1h_2)\phi(h_3h_4) = \phi(x)\phi(y).$$

Thus, ϕ is a homomorphism and therefore an isomorphism, (i.e $G \cong H_1 \times H_2$).

Now, the inductive argument follows the same logical steps, and again is dependent on the ability of the h_i's to commute with each other ($[h_i, h_j] = 1$ and so $h_ih_j = h_jh_i$ for any $h_i \in H_i$ and $h_j \in H_J$). Therefore we can see that for $n \in \mathbb{Z}^+$, $G = \bigoplus_{i=1}^{n} H_i \cong \bigtimes_{i=1}^{n} H_i$. □

Chapter Two

Solvability

Many of the results needed to give a proof of the conjecture are not necessarily results that are well-known or immediately obvious, and along with the conjecture itself, these results are integrally connected to the concept of what is known as *solvability*.

Definition Let G be a group. Then G is *solvable* if $\exists$ a subnormal series

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

such that G_i/G_{i+1} is abelian $\forall 0 \leq i \leq n-1$. These quotients are commonly referred to as "factors".

The rest of this chapter will consist of more results dealing with solvability along with some examples for extra clarity.

Example: The group S_3 is solvable since we have the following subnormal series

$$S_3 \trianglerighteq A_3 \trianglerighteq 1.$$

Also, $|S_3/A_3| = |S_3|/|A_3| = 6/3 = 2$ and so

$$S_3/A_3 \cong \mathbb{Z}_2$$

which is abelian. Similarly, $A_3/1 \cong \mathbb{Z}_3$ is also abelian, and thus S_3 is solvable.

Some groups can easily be identified as solvable groups. The following results categorize some of these.

Lemma 2.1. *Let G be an abelian group. Then G is solvable.*

Proof. Consider the series,

$$G \trianglerighteq 1.$$

Clearly this is a subnormal series and

$$G/1 \cong G$$

which is abelian. Thus G is solvable. □

Lemma 2.2. *Let G be a solvable group and $H \leq G$. Then H is solvable.*

Proof. G is solvable, so $\exists$ a subnormal series,

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

with G_i/G_{i+1} abelian. Now,

$$H = H \cap G = H \cap G_0 \trianglerighteq H \cap G_1 \trianglerighteq \ldots \trianglerighteq H \cap G_n = 1$$

is a subnormal series since the intersection of a subgroup with a normal subgroup is normal in the former group. Also,

$$H \cap G_i/H \cap G_{i+1} = H \cap G_i/H \cap G_i \cap G_{i+1}$$

since $G_{i+1} \trianglelefteq G_i$. Now

$$H \cap G_i / H \cap G_i \cap G_{i+1} \cong \frac{(H \cap G_i)G_{i+1}}{G_{i+1}} \text{ (by Theorem 1.2)}$$
$$\leq \frac{G_i}{G_{i+1}} \text{ (since } (H \cap G_i)G_{i+1} \leq G_i\text{).}$$

But $\frac{G_i}{G_{i+1}}$ is abelian and so $\frac{H \cap G_i}{H \cap G_{i+1}}$ is also abelian. Therefore, H is solvable. □

Now, anytime a situation where there is a subgroup of a solvable group (or some abelian group), any results applying to solvable groups will also apply to these groups. Let us continue exploring results that deal with identifying solvable groups.

Lemma 2.3. *Let G be a solvable group and $N \trianglelefteq G$. Then $\frac{G}{N}$ is solvable.*

Proof. Since G is solvable, $\exists$ a subnormal series

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

such that $\frac{G_i}{G_{i+1}}$ is abelian $\forall\ 0 \leq i \leq n-1$.

Let $\overline{G} = \frac{G}{N}$. Then

$$\overline{G} = \overline{G_0} \trianglerighteq \ldots \trianglerighteq \overline{G_n} = 1$$

is a subnormal series. Also,

$$\overline{G_i}/\overline{G_{i+1}} = \frac{\frac{G_iN}{N}}{\frac{G_{i+1}N}{N}} \cong \frac{G_iN}{G_{i+1}N} \text{ (by theorem 1.3)}$$
$$= \frac{G_iG_{i+1}N}{G_{i+1}N} \text{ (since } G_{i+1} \leq G_i\text{).}$$

Now, by theorem 1.2, we get

$$\frac{G_iG_{i+1}N}{G_{i+1}N} \cong \frac{G_i}{G_i \cap G_{i+1}N}$$
$$\cong \frac{\frac{G_i}{G_{i+1}}}{\frac{G_i \cap G_{i+1}N}{G_{i+1}}} \text{ (by theorem 1.3).}$$

Now, since $\frac{G_i}{G_{i+1}}$ is abelian (by hypothesis) and $G_{i+1} \trianglelefteq G_i$, we get that $\frac{\frac{G_i}{G_{i+1}}}{\frac{G_i \cap G_{i+1}N}{G_{i+1}N}} = \overline{G_i}/\overline{G_{i+1}}$ is abelian. Therefore, $\frac{G}{N}$ is solvable. □

Lemma 2.3 is a useful result, especially in situation when one is working with the natural map or working with quotient groups in general. This next result about solvability is often used in conjunction with Lemma 2.3.

Lemma 2.4. *Let G be a group, $N \trianglelefteq G$ such that N and $\frac{G}{N}$ are solvable. Then G is solvable.*

Proof. Let $\overline{G} = \frac{G}{N}$. Since N and $\overline{G}$ are solvable, $\exists$ a subnormal series

$$\overline{G} = \overline{G}_0 \trianglerighteq \overline{G}_1 \trianglerighteq ... \trianglerighteq \overline{G}_n = 1$$

and

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

(for some m and n), such that $\overline{G}_i/\overline{G}_{i+1}$ and N_i/N_{i+1} are abelian $\forall i$.

Since the pre-image of a normal subgroup is normal, we can take the pre-image of the first series to get

$$G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq ... \trianglerighteq N$$

(since the preimage of the identity under the natural map is the subgroup which was factored out). Now, consider the series

$$G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq ... \trianglerighteq N \trianglerighteq N_1 \trianglerighteq ... \trianglerighteq N_m = 1.$$

We have

$$\frac{G_i}{G_{i+1}} \cong \frac{\frac{G_i}{N}}{\frac{G_{i+1}}{N}} = \overline{G}_i/\overline{G}_{i+1}$$

which is abelian $\forall i$, and we know $\frac{N_i}{N_{i+1}}$ is abelian $\forall i$. Thus, G is solvable. $\square$

The previous two lemmas lead us to a proof of a result about a certain class of groups that show up very often in group theory.

Proposition 2. *Let G be a p-group. Then G is solvable.*

Proof. We will prove this using induction on $|G|$.

If $|G| = p^0$, then $G = \{1\}$. Hence G is abelian and so by Lemma 2.1, G is solvable.

Now, assuming this holds for all values $< |G|$, since G is a p-group, the center $Z(G) \neq \{1\}$. Also, note that $Z(G) \trianglerighteq G$ and so

$$\overline{G} = \tfrac{G}{Z(G)} \text{ is a legitimate group (and also a } p\text{-group).}$$

Moreover, $|\overline{G}| = \frac{|G|}{|Z(G)|} < |G|$ (since the center is non-trivial) and therefore by induction, $\overline{G}$ is solvable. Also since $Z(G)$ is abelian, we know by Lemma 2.1 that it is solvable as well. Therefore, by Lemma 2.4, we get that since $Z(G)$ and $\overline{G} = \frac{G}{Z(G)}$ are both solvable, then G must also be solvable. $\square$

For the previous results, a subnormal series with abelian factors is needed in order to show that a group is solvable. But solvability can be defined through methods through different types of subnormal series. One of these is what's called the *derived series*.

Definition: Let G be a group. The derived series of G is

$$G^{(0)} = G, G^{(1)} = (G^{(0)})' = G', G^{(2)} = (G^{(1)})' = [G^{(1)}, G^{(1)}].$$

Inductively, $G^{(n)} = (G^{(n-1)})'$. Then

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq ...$$

is a subnormal series.

Theorem 2.5. *Let G be a group. Then, G is solvable if and only if $\exists n \in \mathbb{Z}^+ \cup \{0\}$ such that*

$$G^{(n)} = 1.$$

Proof. ($\Leftarrow$) Suppose $\exists n \in \mathbb{Z} \cup \{0\}$ such that $G^{(n)} = 1$. Then, consider the derived series

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \ldots \trianglerighteq G^{(n)} = 1.$$

Now, $\frac{G^{(i)}}{G^{(i+1)}} = \frac{G^{(i)}}{(G^{(i)})'}$, which is abelian by theorem 1.10 $\forall i$. Therefore, G is solvable.

($\Rightarrow$) Suppose G is solvable. Then $\exists$ a subnormal series

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

such that $\frac{G_i}{G_{i+1}}$ is abelian $\forall 0 \le i \le n-1$.

Claim: $G^{(i)} \le G_i \ \forall 0 \le i \le n$. Using induction on i, if $i = 0$, then $G^{(0)} = G \le G = G_0$, and so the claim holds.

Now, if $G^{(i)} \le G_i$, then

$$G^{(i+1)} = (G^{(i)})' \le G_i' \le G_{i+1}$$

and (by theorem 1.10 # 4), since $\frac{G_i}{G_{i+1}}$ is abelian, then $(G_i)' \le G_{i+1}$. Therefore,

$$G^{(i)} \le G_i \ \forall 0 \le i \le n$$

by induction. But then,

$$G^{(n)} \le G_n = 1 \text{ and so}$$
$$G^{(n)} = 1.$$

$\square$

Chapter Three

Nilpotence

Along with solvability, *nilpotence* is a quality of some groups that is studied by those in the group theory world. At first glance, the definitions of the two may seem a bit similar, but there are distinct differences between the two qualities. Nilpotence is a stronger and more restrictive quality for a group to have in comparison to solvability. In some ways, nilpotent groups are slightly closer to being abelian than solvable groups. Nonetheless these concepts are very much related to each other.

Definition: Let G be a group. The upper central series is

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

and inductively,

$$\frac{Z_n(G)}{Z_{n-1}(G)} = Z(\frac{G}{Z_{n-1}(G)}).$$

Then,

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

is a subnormal series.

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

As can be seen, both solvability and nilpotence can be defined through the use of a subnormal series, but the series themselves are not the same. The upper central series is defined through pre-images whereas the subnormal series for solvability is not. Also note how for nilpotence, the subnormal series begins at the identity and terminates at the whole group (the reverse is true for solvability). Some results about nilpotent groups are below. Some of these results are similar to previous results about solvable groups.

Example If G is abelian, then G is nilpotent.

Proof. Since $Z_1(G) = Z(G) = G$ (as G is abelian), then G is clearly nilpotent, as desired. □

Theorem 3.1. *Let G be a p-group. Then G is nilpotent.*

Proof. Suppose G is not nilpotent. Then $Z_i(G) < G \ \forall i \in \mathbb{Z}^+ \cup \{0\}$.

Claim: $Z_i(G) < Z_{i+1}(G) \ \forall i \in \mathbb{Z}^+ \cup \{0\}$. Using induction, if $i = 0$,

$$Z_0(G) = \{1\} < Z(G) = Z_1(G)$$

since G is a p-group. Now, let

$$\overline{G} = \frac{G}{Z_{i+1}(G)}.$$

Since $Z_{i+1}(G) < G$, we know $\overline{G} \neq 1$. Also, since G is a p-group by (), we know, $1 \neq Z(\overline{G}) = Z(\frac{G}{Z_{i+1}(G)}) = \frac{Z_{i+2}(G)}{Z_{i+1}(G)}$. Thus $Z_{i+1} < Z_{i+2}(G)$.

But then we have

$$1 = Z_0(G) < Z_1(G) < Z_2(G) < ... <$$

and this contradicts the assumption that the order of G is finite. Thus, G is nilpotent.

□

Again in a similar vein to solvability, nilpotence can be defined through a different series. Another definition of such a series is the given below, but before that are some results to help motivate this new series.

Lemma 3.2. *Let G be a group and $N \trianglelefteq G$. Then, $[G,N] \trianglelefteq G$*

Proof. Let $x = \Pi_{i=1}^{m}[a_i,b_i]^{n_i} \in [G,N]$ for $m \in \mathbb{Z}^+$, $a_i \in G$, $b_i \in N$ and $n_i \in \mathbb{Z}^+$ $\forall i = 1,\ldots,m$ and let $g \in G$. Then

$$x^g = (\Pi_{i=1}^{m}[a_i,b_i]^{n_i})^g = \Pi_{i=1}^{m}([a_i,b_i]^{n_i})^g = \Pi_{i=1}^{m}([a_i,b_i]^g)^{n_i}.$$

Now, realize that

$$[a,b]^g = (a^{-1}b^{-1}ab)^g = (a^g)^{-1}(b^g)^{-1}a^g b^g = [a^g,b^g]$$

and that $b^g \in N$ since N is normal and so we can see that the product becomes

$$\Pi_{i=1}^{m}[a_i^g,b_i^g]^{n_i} \in [G,N]$$

and so therefore $[G,N] \trianglelefteq G$. □

Lemma 3.3. *Let G be a group, $N \trianglelefteq G$. Then $[G,N] \leq N$.*

Proof. Let $a = \Pi_{i=1}^{m}[g_i, n_i]^{l_i} \in [G,N]$ for $g_i \in G$, and $n_i \in N$. First, note that

$$[g,n] = g^{-1}n^{-1}gn \in N$$

and so $[g,n]^l \in N$ for any $l \in \mathbb{Z}$. From this it follows that any product of these for any $g \in G$, and $n \in N$ will be in N, and so

$$a = \Pi_{i=1}^{m}[g_i, n_i]^{l_i} \in N.$$

Thus, we have that

$$[G,N] \subseteq N,$$

and therefore it follows that

$$[G,N] \leq N.$$

$\square$

Definition: Let G be a group, the <u>Lower Central Series</u> is a central series defined in the following way:

$$K_0(G) = 0,$$

$$K_1(G) = [K_0(G), G] = [G,G] = G'$$

$$K_2(G) = [K_1(G), G] = [[G,G], G]$$

and inductively,

$$K_n(G) = [K_{n-1}, G].$$

Then, using the above lemmas, we have the following subnormal series,

$$G = K_0(G) \trianglerighteq K_1(G) \trianglerighteq K_2(G) \trianglerighteq \ldots$$

Theorem 3.4. *Let G be a group. G is nilpotent if and only if $\exists n \in \mathbb{Z}^+ \cup \{0\}$ such that $K_n(G) = 1$.*

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

CLAIM: $K_i(G) \leq Z_{n-i}(G)\ \forall i \in \mathbb{Z}^+ \cup \{0\}$

Using induction, we can see if $i = 0$,

$$K_0(G) = G \leq G = Z_n(G) = Z_{n-0}(G).$$

Also, we have

$$K_{i+1}(G) = [K_I(G), G] \leq [Z_{n-i}(G), G] \leq Z_{n-i-1}$$

from the above lemma and since

$$\frac{Z_{n-1}(G)}{Z_{n-i-1}(G)} = Z(\frac{G}{Z_{n-i-1}(G)}) = Z_{n-(i+1)}.$$

Thus the claim holds.

But then,

$$K_n(G) \leq Z_{n-n}(G) = Z_0(G) = 1$$

and so we get

$$K_n(G) = 1.$$

($\Leftarrow$) Suppose $\exists n \in \mathbb{Z}^+ \cup \{0\}$ such that $K_n(G) = 1$.

It follows from the above claim that we get an upper central series which begins at 1 and ends back at the original group and so G is nilpotent. $\square$

This definition of nilpotence is more similar to a groups solvability since, this time, the subnormal series terminates at the identity and not the whole group. We can now return to more results about nilpotent groups.

Proposition 3. *Let G be a nilpotent group and $H \leq G$. Then H is nilpotent.*

Proof. Using the upper central series, suppose G is nilpotent. Then $\exists n \in \mathbb{Z}^+ \cup \{0\}$, such that $Z_n(G) = G$.

CLAIM: $Z_I(H) \geq H \cap Z_i(G)$, $\forall 0 \leq i \leq n$.

If $i = 0$,

$$Z_0(H) = \{1\} \geq \{1\} = H \cap \{1\} = H \cap Z_0(G).$$

Also,

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

by induction, part 6 of theorem 1.10, and by noting that

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

Thus we have that $[H \cap Z_{i+1}(G), H] \leq Z_i(H)$ and so, again by pt. 6 of theorem 1.10,

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

But then, $(H \cap Z_{i+1}(G))Z_i(H) \leq Z_{i+1}(H)$ and so $H \cap Z_{i+1}(G) \leq Z_{i+1}(H)$ and thus the claim holds by induction.

Then,

$$Z_n(H) \geq H \cap Z_n(G) = H \cap G = H$$

and so $Z_n(H) = H$ and therefore H is nilpotent. □

Proposition 4. *Let G be a nilpotent group, $N \trianglelefteq G$. Then, $\frac{G}{N}$ is nilpotent.*

Proof. Using the lower central series, since G is nilpotent $\exists n \in \mathbb{Z}^+ \cup \{0\}$ such that $K_n(G) = 1$. Let $\overline{G} = \frac{G}{N}$.

CLAIM: $\overline{K_i(G)} = K_i(\overline{G})$, $\forall i$.

If $i = 0$, then

$$\overline{K_0(G)} = \overline{G} = K_0(\overline{G}).$$

Also, we have

$$\overline{K_{i+1}(G)} = \overline{[K_i(G), G]} = [\overline{K_i(G)}, \overline{G}] = [K_i(\overline{G}), \overline{G}] = K_{i+1}(\overline{G}).$$

Thus the claim holds by induction.

Now,

$$K_n(\overline{G}) = \overline{K_n(G)} = \overline{1}$$

and therefore $\overline{G} = \frac{G}{N}$ is nilpotent. □

The following result gives a connection between nilpotence and solvability and therefore it will be introduced as a theorem, rather than a proposition.

Theorem 3.5. *Let G be a nilpotent group. Then G is solvable.*

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

$$G = Z_n(G) \trianglerighteq Z_{n-1}(G) \trianglelefteq Z_{n-2}(G) \trianglerighteq ... \trianglerighteq Z_0(G) = 1$$

and also

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

is clearly abelian $\forall i$. Therefore G is solvable. □

The above theorem shows that nilpotence implies solvability. But the opposite implication does not hold, meaning that there are properties held by solvable groups that are not held by nilpotent groups.

Example:

Recall result lemma 2.4. Consider $G = S_3$ and $N = \langle(123)\rangle \trianglelefteq G$. Now,

$$|N| = 3$$

and so $N \cong \mathbb{Z}_3$ so N is abelian, and therefore nilpotent. Also realize that

$$|\frac{G}{N}| = \frac{|G|}{|N|} = \frac{6}{3} = 2,$$

and so $\frac{G}{N} \cong \mathbb{Z}_2$ which is abelian and therefore nilpotent. But $Z(S_3) = 1$ and so

$$\frac{Z_2(S_3)}{Z_1(S_3)} = Z(\frac{S_3}{Z_1(S_3)}) = Z(\frac{S_3}{Z(S_3)}) = Z(\frac{S_3}{\{1\}}) \cong Z(S_3) = \{1\}$$

and so inductively, we can see that $Z_i(S_3) = \{1\}$ for all i which means that the upper central series will never reach S_3. Therefore S_3 is not nilpotent.

The above example demonstrates the lack of an equivalent result of lemma 2.4 for nilpotence, and further indicates that nilpotence enforces a bit more of a restricted structure upon a group as opposed to solvability. The following results show a few peculiar properties of nilpotent groups, which would lead one to draw a connection between nilpotence and p-groups.

Theorem 3.6. *Let $G \neq 1$ be a nilpotent group. Then $Z(G) \neq 1$.*

Proof. Since G is nilpotent and $G \neq 1$, $\exists n \in \mathbb{Z}^+$ such that

$$K_n(G) = 1.$$

Let i be minimal such that

$$K_i(G) = 1.$$

Then, $K_{i-1}(G) \neq 1$, and also

$$1 = K_i(G) = [K_{i-1}(G), G]$$

and therefore by theorem 1.10 it follows that

$$1 \neq K_{i-1} \leq Z(G)$$

and so $Z(G) \neq 1$. $\square$

Theorem 3.7. *Let G be a nilpotent group and $H < G$. Then $H < N_G(H)$.*

Proof. Since G is nilpotent, $\exists n \in \mathbb{Z}^+$ such that $Z_n(G) = G$. Since $H < G$, let i be maximal such that

$$Z_i(G) \leq H.$$

Then $Z_{i+1} \nleq H$ and,

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

Thus $Z_{i+1}(G) \leq N_G(H)$ and so $H < N_G(H)$. $\square$

Now for a definition before some further results, which will be needed in showing a fairly significant result about nilpotent groups.

Definition: Let G be a group, and $M \leq G$. Then M is a <u>maximal subgroup of G</u> if the following two conditions hold:
(1) $M \neq G$
(2) Whenever $\exists H \leq G$ such that $M \leq H \leq G$ then either $H = M$ or $H = G$.

Theorem 3.8. *Let G be a nilpotent group, and $M \leq G$ be a maximal subgroup. Then $M \trianglelefteq G$.*

Proof. Since M is a maximal subgroup of G, we know that $M \neq G$. Thus, by theorem 3.7,

$$M < N_G(M) \leq G.$$

$\square$

Hence $G = N_G(M)$, and therefore $M \trianglelefteq G$.

Theorem 3.9. *Let G be a nilpotent group. Then,*

$$G \cong \bigtimes_{\substack{P \in Syl_p(G) \\ p \in \pi(G)}} P.$$

Proof. Let $P \in Syl_p(G)$. If $N_G(P) < G$, then $\exists$ a maximal subgroup M of G such that $N_G(P) \leq M$. Since G is nilpotent, by theorem 3.8, $M \trianglelefteq G$. Now,

$$P \leq N_G(P) \leq M,$$

and so $P \leq M$. Then $P \in Syl_p(M)$. Thus, by the Frattini argument, we have

$$G = N_G(P)M \leq MM = M$$

and so $G = M$ ($\Rightarrow\Leftarrow$). This contradicts the maximality of M. Thus, it must be the case that $N_G(P) = G$, which means $P \trianglelefteq G$. But then we can see that

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

But realize that

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

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

$$P \cap \prod_{\substack{Q \in Syl_q(G) \\ q \in \pi(G) - \{p\}}} Q = 1$$

$\forall P \in Syl_p(G)$. Thus by theorem 1.11, $G \cong \bigtimes_{\substack{P \in Syl_p(G) \\ p \in \pi(G)}} P$. □

Thus from theorem 3.9, we can see that a group being nilpotent means that it must break down into a product of Sylow p-subgroups, but we also wonder if the opposite implication is true. It would be nice to be able to completely characterize the property of nilpotence to simply just products of Sylow p-subgroups, and the next theorem helps achieve this. The following proposition leading up to the theorem will be used as tools for the proof of said theorem.

Proposition 5. *Let A, C be groups, and $B \trianglelefteq A$, $D \trianglelefteq C$. Then $B \times D \trianglelefteq A \times C$ and also, $\frac{A \times C}{B \times D} \cong \frac{A}{B} \times \frac{C}{D}$.*

Proposition 6. *Let A and B be groups. Then $Z(A \times B) = Z(A) \times Z(B)$.*

Proof. For $(\subseteq)$, let $x = (a, b) \in Z(A \times B)$, $(h, k) \in A \times B$. Then $(ah, bk) = (a, b)(h, k) = (h, k)(a, b) = (ha, kb)$. Thus we have that $ah = ha$, and $bk = kb$ and so $a \in Z(A)$, $b \in Z(B)$. Thus $(a, b) \in Z(A) \times Z(B)$.

For $(\supseteq)$, let $(a, b) \in Z(A) \times Z(B)$. Then $a \in Z(A)$, $b \in Z(B)$. Now, let $h \in A$, $k \in B$. Then $ah = ha$, and $bk = kb$. Thus we get that

$$(a, b)(h, k) = (ah, bk) = (ha, kb) = (h, k)(a, b)$$

and so $(a, b) \in Z(A \times B)$. Therefore $Z(A \times B) = Z(A) \times Z(B)$. □

Proposition 7. *Let A and B be groups such that $A \cong B$. Then $Z(A) \cong Z(B)$*

Proof. Suppose for groups A, B we have $A \cong B$. Then $\exists \phi : A \mapsto B$ such that ϕ is a bijective homomorphism. Realize that for $x \in Z(A)$ and $a \in A$, we have

$$\phi(x)\phi(a) = \phi(xa) = \phi(ax) = \phi(a)\phi(x).$$

Thus it must be the case that $\phi(x) \in Z(B)$. It follows that $\phi(Z(A)) \leq Z(B)$. Since ϕ is is an isomorphism, then $\phi^{-1} : B \mapsto A$ is also a homomorphism, and so for $b \in Z(B), y \in B$ we have

$$\phi^{-1}(b)\phi^{-1}(y) = \phi^{-1}(by) = \phi^{-1}(yb) = \phi^{-1}(y)\phi^{-1}(b).$$

So $\phi^{-1}(b) \in Z(A)$ which means $\phi^{-1}(Z(B)) \leq Z(A)$ and hence $\phi(Z(A)) = Z(B)$. Therefore, $\phi|_{Z(A)}$ is an isomorphism and we get $Z(A) \cong Z(B)$. □

Theorem 3.10. *Let A, B be nilpotent groups. Then $A \times B$ is nilpotent.*

Proof. Since A and B are nilpotent, $\exists k, l \in \mathbb{Z}^+ \cup \{0\}$ such that $Z_k(A) = A$ and $Z_l(B) = B$. Let $n = max\{k, l\}$.

CLAIM: $Z_i(A \times B) = Z_i(A) \times Z_i(B)$, $\forall\ i \in \mathbb{Z}^+ \cup \{0\}$.

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

Now

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

by propositions 5 and 6 above. Now, furthermore, we have

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

Now looking at this we can realize that

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

and so tracing back a bit, we have

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

Thus, by pre-imaging, we get

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

Now, $Z_n(A \times B) = Z_n(A) \times Z_n(B) = A \times B$ and thus $A \times B$ is nilpotent. $\square$

Chapter Four

Automorphisms

In preparation for the main results of this paper, it may be beneficial to give some background and results on automorphisms of groups. We can start with a definition.

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

$$Aut(G) = \{\phi : G \mapsto G | \phi \text{ is an automorphism}\}.$$

Automorphisms can be split into two types, inner and outer. The *inner automorphisms* are defined as,

$$Inn(G) = \{\phi \in Aut(G) | \phi(x) = g^{-1}xg \ \forall x \in G, \text{ for } g \in G\}.$$

It is a fact that $Inn(G) \trianglelefteq Aut(G)$. The *outer automorphisms* are defined as,

$$Out(G) = \frac{Aut(G)}{Inn(G)}.$$

The inner automorphism maps are also commonly denoted as ϕ_g, where g is the group element that the map conjugates everything by. The following definition deals with subgroups left invariant by a groups automorphisms.

Definition: Let G be a group and $H \leq G$. Then H is a *characteristic* subgroup if $\phi(H) = H, \forall \phi \in Aut(G)$.

This is commonly denoted by H char G. Subgroups that exhibit this behavior are highlighted because they can be useful when trying to prove a result about the parent group. Some examples of characteristic subgroups are shown below.

Example: 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 $\phi \in Aut(G)$, $\exists g_1 \in G$ such that $g = \phi(g_1)$. Then,

$$\phi(z)g = \phi(z)\phi(g_1) = \phi(zg_1) = \phi(g_1 z)\phi(g_1)\phi(z) = g\phi(z).$$

Thus $\phi(z) \in Z(G)$, and so $\phi(Z(G)) \leq Z(G)$, but since ϕ is one-to-one, we can realize that $|\phi(Z(G))| = |Z(G)|$. Thus we have $\phi(Z(G)) = Z(G)$ and hence $Z(G)$ char (G). $\square$

Example Let G be a group. Then G' char G.

Proof. Let $\phi \in Aut(G)$, $x = \prod_{i=1}^{m}[a_i, b_i]^{n_i} \in G'$ for $a_i, b_i \in G$, and $n_i \in \mathbb{Z}$. Then, realize that for $a, b, c, d \in G$,

$$\phi([a,b][c,d]) = \phi(a^{-1}b^{-1}abc^{-1}d^{-1}cd) = [\phi(a), \phi(b)][\phi(c), \phi(d)].$$

Therefore, we can see that

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

and so $\phi(G') \leq G'$ and since $\phi \in Aut(G)$, it follows that $\phi(G') = G'$. Hence, G' char G. $\square$

Theorem 4.1. *Let G be a group. Then the following hold:*

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

2. *If H char K char G then H char G.*

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

Proof. For (1), since H char G, then $\phi(H) = H \ \forall \phi \in Aut(G)$. Thus $\forall \pi \in Inn(G)$, $\pi(H) = H$ or $g^{-1}Hg = H \ \forall g \in G$. Thus $H \trianglelefteq G$. Now for (2), let $\phi \in Aut(G)$. Since K char G, we know $\phi(K) = K$. Thus $\phi|_K \in Aut(K)$. But since H char K, $\phi|_K(H) = H$ and so $\phi(H) = H$, meaning that H char G. For (3), let $g \in G$. Then, $\phi_g \in Aut(G)$. Since $K \trianglelefteq G$, we get $\phi_g(K) = K$ and so it follows that $\phi_g|_K \in Aut(K)$. Now, since H char K, $\phi_g|_K(H) = H$ and so $\phi(H) = H$. Thus $g^{-1}Hg = H$, and so $H \trianglelefteq G$. □

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

Example: $\mathbb{Z}_p$ for some prime p is characteristic. In fact, any simple group is characteristic.

Theorem 4.2. *Let G be a characteristically simple group. Then G is isomorphic to the direct product of isomorphic groups.*

Proof. Let $1 \neq G_1 \trianglelefteq G$ such that $|G_1|$ is minimal and let $H = \prod_{i=1}^{s} G_i$ such that

1. $G_i \trianglelefteq G \ \forall 1 \leq i \leq s$.

2. $G_i \cong G_1 \ \forall 1 \leq i \leq s$.

3. $G_i \cap \prod_{j \neq i} G_j = 1 \ \forall 1 \leq i \leq s$.

4. s is maximal.

If H is not a characteristic subgroup of G, then $\exists \phi \in Aut(G)$ and $\exists\ 1 \leq i \leq s$ such that $\phi(G_i) \not\leq H$. Then, $\phi(G_i) \cap H \leq \phi(G_i)$. Since $G_i \trianglelefteq G\ \forall 1 \leq i \leq s$, we know $H \trianglelefteq G$. Also, since $G_i \trianglelefteq G$, we get that $\phi(G_i) \trianglelefteq G$. Thus $\phi(G_i) \cap H \trianglelefteq G$. But

$$|\phi(G_i) \cap H| < |\phi(G_i)| = |G_i| = |G_1|.$$

Therefore $\phi(G_i) \cap H = 1$, by the minimality of $|G_1|$.

Now, $\phi(G_i) \trianglelefteq G$, $\phi(G_i) \cong G_i \cong G_1$, and $\phi(G_i) \cap \prod_{i=1}^{s} G_i = 1$. But then, we get

$$H = \prod_{i=1}^{s} G_i < \phi(G_i) \prod_{i=1}^{s} G_i,$$

a contradiction to the maximallity of s. Thus, H is a characteristic subgroup of G. Since G is characteristically simple and $H \neq 1$, we get $G = H = \prod_{i=1}^{s} G_i \cong \bigtimes_{i=1}^{s} G_i$.

Now, suppose $N \trianglelefteq G_i$ for some $1 \leq i \leq s$. Then for $x = g_1 g_2 ... g_s \in G$, $n \in N$,

$$n^x = g_s^{-1} .... g_1^{-1} n g_1 ... g_s.$$

Also, realize that for any $i \neq j$, $[G_i, G_j] = 1$. which means that $g_i g_j = g_j g_i$, $\forall g_i \in G_i$, $g_j \in G_j$. This implies that $n^x = n$, and so $N \trianglelefteq G$. But $|N| \leq |G_i| = |G_1|$ and $|G_1|$ is minimal so $N = 1$ or $N = G_i$. Therefore, G_i is simple. $\square$

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

1. $N \trianglelefteq G$.

2. Whenever $\exists H \leq N$ such that $H \trianglelefteq G$, then $H = 1$ or $H = N$.

3. $N \neq 1$.

Minimal normal subgroups are useful, especially in situations where a normal subgroup gets factored out of a solvable group. These subgroups have nice structure and are more controllable. A result about their structure is below.

Definition: Let p be a prime, and N be a group. Then N is an *elementary abelian p-group* if $N \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$.

Proposition 8. *Let G be a group such that $G = G'$. Then, G is not solvable.*

Proof. Suppose G is solvable. Then $\exists n \in \mathbb{Z}^+ \cup \{0\}$ such that $G^{(n)} = 1$.
CLAIM: $G^{(i)} = G \; \forall \; i$.

If $i = 0$, $G^{(0)} = G$. Also, $G^{(i+1)} = (G^{(i)})' = (G) = G'$ by induction. Thus, $G^{(i)} = G$ for all i, a contradiction to the derived series terminating. Thus, G is not solvable. ☐

Lemma 4.3. *Let G be a solvable and simple group. Then, $G \cong \mathbb{Z}_p$ for some prime p.*

Proof. Now, G is simple so $\{1\}$ and G are the only normal subgroups of G. Also, since G is solvable, $\exists n \in \mathbb{Z}^+ \cup \{0\}$ such that $G^{(n)} = 1$. So we have the subnormal series,

$$G = G^{(0)} \trianglerighteq G^{(1)} = G' \trianglerighteq G^{(2)} \trianglerighteq \ldots \trianglerighteq G^{(n)} = 1.$$

So, $G' \trianglelefteq G$, which means that $G' = 1$ or $G' = G$ since G is simple. Now since G is solvable, and by proposition 8 above, $G' \neq G$, so it must be true that $G' = 1$. So, the subnormal series becomes $G = G^{(0)} \trianglerighteq G^{(1)} = G' = 1$, or, $G \trianglerighteq 1$. Therefore, G must be abelian. Now, all subgroups of an abelian group are normal, and since G is abelian, it must have no proper non-trivial subgroups. Now, by Cauchy's theorem, if $|G| = m$ then for some prime p such that $p|m$, there exists a subgroup of order

p. Since G is simple, it must be the case that $m = p$ (or else there would be a proper subgroup), and so $|G| = p$. So by the classification of finite abelian groups, $G \cong \mathbb{Z}_p$ $\square$

Theorem 4.4. *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 N is a minimal normal subgroup of G, we know N is characteristically simple. By theorem 4.2,

$$N \cong \bigtimes_{i=1}^{n} N_i$$

with each N_i being simple isomorphic groups. Since G is solvable, we get that N_i is solvable $\forall\ 1 \leq i \leq n$. Thus, since the N_i's are isomorphic groups, by lemma 4.3, $\exists$ prime p such that $N_i \cong \mathbb{Z}_p\ \forall\ 1 \leq i \leq n$. Therefore $N \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$ is an elementary abelian p-group. $\square$

The significance of the above theorem is clear, as it completely characterizes minimal normal subgroups of solvable groups. Now, if a situation were to ever arise where one of these subgroups is factored out of the original group (under the natural map), then the resulting quotient group (along with images and preimages of given subgroups) is much easier to understand and control. Now, recalling the definition of Hall π-subgroups, the following theorem shows how these groups truly are generalized notions of Sylow subgroups when it comes to solvable groups.

Proposition 9. *Let G be a group, $N \trianglelefteq G$ and $P \in Syl_p(G)$ for some prime p. Then, $\frac{PN}{N} \in Syl_p(\frac{G}{N})$.*

Proof. Now, by the second isomorphism theorem, we know that

$$\frac{|PN|}{|N|} = \left|\frac{PN}{N}\right| = \left|\frac{P}{P \cap N}\right| = \frac{|P|}{|P \cap N|}$$

which is a p-number, since P is a p-group. Thus $\frac{PN}{N}$ is a p-subgroup of $\frac{G}{N}$. Also, since $P \in Syl_p(G)$, we know that $\frac{|G|}{|P|}$ is a p'-number. But,

$$\frac{|G|}{|P|} = \frac{|G|}{|PN|} \cdot \frac{|PN|}{|P|}$$

and since we know $\frac{|G|}{|P|}$ is a p'-number, it follows that $\frac{|G|}{|PN|}$ must also be a p'-number. Now, realize that

$$\frac{\left|\frac{G}{N}\right|}{\left|\frac{PN}{N}\right|} = \frac{\frac{|G|}{|N|}}{\frac{|PN|}{|N|}} = \frac{|G|}{|PN|}$$

is a p'-number and therefore $\frac{PN}{N} \in Syl_p(\frac{G}{N})$ □

We can generalize this result for Hall subgroups.

Proposition 10. *Let G be a group, $N \trianglelefteq G$, and $H \in Hall_\pi(G)$. Then $\frac{HN}{N} \in Hall_\pi(\frac{G}{N})$.*

Proof. Follows a similar argument as the previous proposition. □

Proposition 11. *Let G be a group, $H \leq G$, $K \leq G$ and $L \leq H$. Then, $H \cap KL = (H \cap K)L$.*

Proof. Let $x \in H \cap KL$. Then $x \in H$ and $x \in KL$. So $x = kl$ for some $k \in K$, and $l \in L$. We also have that $k = xl^{-1} \in H$. Thus $k \in H \cap K \implies x = kl \in (H \cap K)L$ and so $H \cap KL \subseteq (H \cap K)L$.

Now, let $x \in (H \cap K)L$. Then $x = gl$ for $g \in H \cap K$, $l \in L$. Also $gl \in HL = H$ and $gl \in KL$. Thus $x = gl \in H \cap KL$ and so $(H \cap K)L \subseteq H \cap KL$. Therefore $(H \cap K)L = H \cap KL$. □

Theorem 4.5. *(**Hall's Theorem**) Let G be a solvable group, and π be a set of primes. Then,*

1. *$\exists R \in Hall_\pi(G)$.*

2. *Every π-subgroup of G is in a conjugate of R.*

Proof. Using induction on $|G|$, if $|G| = 1$, then $G = \{1\}$. Then, $\pi(G) = \varnothing \subseteq \pi$ and so G is a π-group. Also,

$$\pi\left(\frac{G}{\{1\}}\right) = \pi(G) = \varnothing \subseteq \pi'.$$

So $G \in Hall_\pi(G)$, giving (1), and since $G \leq G = G^1$, we see that (2) holds as well.

Now, suppose the theorem holds for all solvable groups of order $< |G|$. Let N be a minimal normal subgroup of G, and $\overline{G} = \frac{G}{N}$. Since G is solvable, then by theorem 4.4, N is an elementary abelian p-group, for some prime p.

CASE 1: Say $p \in \pi$.

Now, since G is solvable, we know by lemma 2.3, $\overline{G}$ is solvable. Thus, since $|\overline{G}| < |G|$, $\exists \overline{H} \in Hall_\pi(\overline{G})$. Then this means that $H \leq G$, and

$$|H| = \left|\frac{H}{N}\right| \cdot |N| = |\overline{H}| \cdot |N|$$

is a π-number. Thus H is a π-group, and

$$\frac{|G|}{|H|} = \frac{\frac{|G|}{|N|}}{\frac{|H|}{|N|}} = \frac{|\overline{G}|}{|\overline{H}|}$$

is a π'-number. Hence, $H \in Hall_\pi(G)$, giving (1).

Now, let L be a π-subgroup of G. Then $\overline{L} \leq \overline{G}$ is a π–group. Hence, by induction, $\exists \overline{g} \in \overline{G}$ such that $\overline{L} \leq \overline{H}^{\overline{g}} = \overline{H^g}$. But then

$$L \leq LN \leq H^g$$

and so $L \leq H^g$, giving (2).

CASE 2: $p \notin \pi$ and G has no normal π-subgroups.

<u>If $H < G$</u>, Then since G is solvable, by lemma 2.2 H is solvable. Thus, by induction, $\exists K \in Hall_{\pi}(H)$. Then K is a π-group and

$$\frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = \frac{\frac{|G|}{|N|}}{\frac{|H|}{|N|}} \cdot \frac{|H|}{|K|} = \frac{|\overline{G}|}{|\overline{H}|} \cdot \frac{|H|}{|K|}$$

is a π'-number. Thus $K \in Hall_{\pi}(G)$, giving (1). Let L be a π-subgroup. Then $\overline{L} \leq \overline{G}$ is a π-subgroup. Thus, by induction, $\exists \overline{g} \in \overline{G}$ such that $\overline{L} \leq \overline{H}^{\overline{g}}$. But then $L \leq LN \leq H^g$ and so $L^{g^{-1}} < H$ is a π-subgroup, and so $\exists x \in H$ such that $L^{g^{-1}} \leq K^x$. But then $L \leq K^{xg}$, giving (2). <u>If $G = H$</u>, Then $\overline{G} = \overline{H}$ is a $\pi-$group. Let $\overline{M}$ be a minimal normal subgroup of $\overline{G}$. Since $\overline{G}$ is solvable, by theorem 4.4, $\overline{M}$ is an elementary abelian q-group with $q \in \pi$. Since $\overline{M} \trianglelefteq \overline{G}$, we know $M \trianglelefteq G$. Let $Q \in Syl_q(M)$. By Proposition 9, we know $\overline{Q} \in Syl_q(\overline{M})$, and so $\overline{M} = \overline{Q}$. But $M = QN$. By the Frattini argument,

$$G = N_G(Q)M = N_G(Q)QN = N_G(Q)N.$$

Since $N \trianglelefteq G$, we know $N \cap N_G(Q) \trianglelefteq N_G(Q)$. Also, since N is abelian,

$$N \cap N_G(Q) \trianglelefteq N.$$

Thus, $N \cap N_G(Q) \trianglelefteq N_G(Q)N = G$. Since N is a minimal normal subgroup of G, we get $N \cap N_G(Q) = N$, or $N \cap N_G(Q) = 1$.
If $N \cap N_G(Q) = N$,
then $N \leq N_G(Q)$ and so $G = N_G(Q)N = N_G(Q)$. Thus $Q \trianglelefteq G$, but we said G has no normal π-subgroups and so this is a contradiction (since Q is a π-group). Therefore $N \cap N_G(Q) = 1$. Now,

$$|G| = |N_G(Q)N| = \frac{|N_G(Q)| \cdot |N|}{|N \cap N_G(Q)|} = |N_G(Q)| \cdot |N|.$$

Then, $|N_G(Q)| = \frac{|G|}{|N|} = |\overline{G}|$ is a π-number and so $N_G(Q)$ is a π-group. Also, $\frac{|G|}{|N_G(Q)|} = |N|$ is a π'-number ($p \notin \pi$). Thus $H_1 = N_G(Q) \in Hall_{\pi}(G)$, giving (1). Let $L \leq G$ be a

π-group. Now,

$$LN = LN \cap G = LN \cap H_1 N = (LN \cap H_1)N,$$

and thus we have that

$$\frac{|LN|}{|LN \cap H_1|} = \frac{|(LN \cap H_1)N|}{|LN \cap H_1|} = \frac{|N|}{|LN \cap H_1 \cap N|}$$

which is a π'-number. Since $LN \cap H_1$ is a π-group, we get that $LN \cap H_1 \in Hall_\pi(LN)$. Also, $L \leq LN$ is a π-group.

If $LN < G$, then by induction, $\exists y \in LN$ such that $L \leq (LN \cap H_1)^y) \leq H_1^y$, giving (2).

If $LN = G$, since $N \leq M$, we get $G = LM$. Thus

$$|L| \cdot |N| = |G| = \frac{|L| \cdot |M|}{|L \cap M|}.$$

Thus $|N| = \frac{|M|}{|L \cap M|}$ is a π'-number and so $L \cap M \in Syl_q(M)$. Thus $\exists z \in M$ such that $(L \cap M) = Q^z$. Since $M \trianglelefteq G$, we get $M \cap L \trianglelefteq L$. Thus $L \leq N_G(M \cap L)$, and so

$$L \leq N_G(Q^z) = N_G(Q)^z = H_1^z$$

giving (2). □

Lemma 4.6. *Let G be a group, $H \leq G$, and $K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.*

Proof. Suppose $HK = KH$. Since $H \leq G$ and $K \leq G$, we know $H \neq \{\emptyset\} \neq K$. Thus $\exists h \in H$ and $\exists k \in K$. But then $hk \in HK$ and so $HK \neq \{\emptyset\}$.
Let $h_1k_1, h_2k_2 \in HK$. Then

$$h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$$

and since $HK = KH$, $\exists h_3k_3$ such that $h_3k_3 = (k_1k_2^{-1})h_2^{-1}$. Now continuing with the above expression, we get

$$h_1k_1k_2^{-1}h_2^{-1} = h_1h_3k_3 \in HK.$$

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

Now, suppose $HK \leq G$ and let $hk \in HK$. Then $(hk)^{-1} \in HK$, or $k^{-1}h^{-1} \in HK$. So $\exists h_1 \in H$ and $k_1 \in K$ such that $k^{-1}h^{-1} = h_1k_1$. Thus $hk = k_1^{-1}h_1^{-1} \in KH$ and so we get het $HK \subseteq KH$.

Now, let $kh \in KH$. Then $h^{-1}k^{-1} \in HK$. Since $HK \leq G$, we get $(h^{-1}k^{-1})^{-1} \in HK$ or $kh \in HK$. Thus $KH \subseteq HK$ and hence $KH = HK$. □

Theorem 4.7. *Let G be a group, $H \leq G$, and $K \leq G$ such that $gcd\left(\frac{|G|}{|H|}, \frac{|G|}{|K|}\right) = 1$. Then,*

1. $G = HK$.
2. $\frac{|G|}{|H \cap K|} = \frac{|G|}{|H|} \cdot \frac{|G|}{|K|}$.

Proof. Now,

$$\frac{|G|}{|H \cap K|} = \frac{|G|}{|K|} \cdot \frac{|K|}{|K \cap H|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|H \cap K|}.$$

Then $\frac{|G|}{|H|} \Big| \frac{|G|}{|H \cap K|}$ and $\frac{|G|}{|K|} \Big| \frac{|G|}{|H \cap K|}$ and since $gcd\left(\frac{|G|}{|H|}, \frac{|G|}{|K|}\right) = 1$, then we have that

$$\frac{|G|}{|H|} \cdot \frac{|G|}{|K|} \Big| \frac{|G|}{|H \cap K|},$$

and so it is obviously true that

$$\frac{|G|}{|H|} \cdot \frac{|G|}{|K|} \leq \frac{|G|}{|H \cap K|}.$$

Thus, by doing some basic algebra, we have that $|G| \leq \frac{|H||K|}{|H \cap K|} = |HK|$. Thus $G = HK$, giving (1).

Now, for (2), we also have $|G| = |HK| = \frac{|H| \cdot |K|}{|H \cap K|}$ and so $|G| \cdot |G| = \frac{|G| \cdot |H| \cdot |K|}{|H \cap K|}$. Thus, we get that $\frac{|G|}{|H|} \cdot \frac{|G|}{|K|} = \frac{|G|}{|H \cap K|}$, giving (2). □

Theorem 4.8. *Let G be a group and $H_i < G$ such that H_i is solvable $\forall\ 1 \le i \le 3$ and $gcd\left(\frac{|G|}{|H_i|}, \frac{|G|}{|H_j|}\right) = 1$, $\forall\ i \neq j$. Then, G is solvable.*

Proof. Using induction on $|G|$, let N be a minimal normal subgroup of H_1. By theorem (4.4), N is an elementary abelian p-group, for some prime, p. By Sylow's theorem, $\exists P \in Syl_p(G)$ such that $N \le P$. Since $gcd\left(\frac{|G|}{|H_2|}, \frac{|G|}{|H_3|}\right) = 1$, we get that $p \nmid \frac{|G|}{|H_2|}$ or $p \nmid \frac{|G|}{|H_3|}$. WLOG, say $p \nmid \frac{|G|}{|H_2|}$, then $|G|_p = |H_2|_p$. By Sylow's theorem, $\exists x \in G$ such that $P^x \le H_2$. Since $N \le P$, we get $N^x \le P^x$ and so $N^x \le H_2$. Also since $N \trianglelefteq H_1$, we get $N^x \trianglelefteq H_1^x$. Now,

$$gcd\left(\frac{|G|}{|H_1^x|}, \frac{|G|}{|H_2|}\right) = gcd\left(\frac{|G|}{|H_1|}, \frac{|G|}{|H_2|}\right) = 1,$$

by theorem (4.7), $G = H_1^x H_2$. Let $K = (N^x)^G$. Then, by lemma (1.10), $K \trianglelefteq G$ and so $\overline{G} = \frac{G}{K}$ is a group. Also,

$$K = (N^x)^G = (N^x)^{H_1^x H_2} = (N^x)^{H_2} \le H_2 < G$$

since $N^x \trianglelefteq H_1^x$ and $N^x \le H_2$. Thus, $1 \neq K < G$. Now, since H_i is solvable for each i, by lemma (2.3), $\overline{H_i}$ is solvable for each i. Now,

$$\frac{|G|}{|H_iK|} \cdot \frac{|H_iK|}{|H_i|} = \frac{|G|}{|H_i|}$$

and so $\frac{|G|}{|H_iK|} \Big| \frac{|G|}{|H_i|}$ $\forall\ 1 \le i \le 3$. Thus, since $gcd\left(\frac{|G|}{|H_i|}, \frac{|G|}{|H_j|}\right) = 1\ \forall\ i \neq j$, we get $gcd\left(\frac{|G|}{|H_iK|}, \frac{|G|}{|H_jK|}\right) = 1\ \forall\ i \neq j$. Thus,

$$gcd\left(\frac{|\overline{G}|}{|\overline{H_i}|}, \frac{|\overline{G}|}{|\overline{H_j}|}\right) = gcd\left(\frac{|G|}{|H_iK|}, \frac{|G|}{|H_jK|}\right) = 1.$$

Since $|\overline{G}| = \frac{|G|}{|K|} < |G|$, we get that $\overline{G} = \frac{G}{K}$ is solvable by induction. Since $K \le H_2$ and H_2 is solvable, we get that K is solvable by lemma (2.2). Thus G is solvable by lemma (2.4). $\square$

Theorem 4.9. Phillip Hall *Let G be a group. Then G is solvable if and only if $Hall_{p'}(G) \neq \emptyset$, $\forall\ p \in \pi(G)$.*

Proof. ($\Rightarrow$) Suppose G is solvable. Then, by Hall's theorem, $Hall_{p'}(G) \neq \emptyset$.

($\Leftarrow$) Suppose $Hall_{p'}(G) \neq \emptyset$, $\forall\ p \in \pi(G)$. Using induction on $|\pi(G)|$, if $|\pi(G)| = 1$. Then G is a p-group, and thus solvable by proposition 2. If $|\pi(G)| = 2$, then G is a pq-group, and thus G is solvable by Bender's theorem (Bender, 1972). WLOG, say $|\pi(G)| \geq 3$. Let

$$|G| = \prod_{i=1}^{m} p_i^{n_i}$$

where p_i is prime, $m \in \mathbb{Z}^+$, and $n_i \in \mathbb{Z}^+\ \forall\ 1 \leq i \leq m$. Let $H_i \in Hall_{p_i'}(G)$, $\forall\ 1 \leq i \leq 3$. Then,

$$gcd\left(\frac{|G|}{|H_i|}, \frac{|G|}{|H_j|}\right) = gcd\left(p_i^{n_i}, p_j^{n_j}\right) = 1$$

$\forall\ i \neq j$. By theorem (4.7), $G = H_iH_j$ and $\frac{|H_i|}{|H_i \cap H_j|} = \frac{|G|}{|H_j|} = p_j^{n_j}$ is a p_j-number. Thus, $H_i \cap H_j \in Hall_{p_j'}(H_i)\ \forall\ 1 \leq i \leq 3$, $1 \leq j \leq 3$. Thus, $Hall_{p'}(H_i) \neq \emptyset$, also

$$|\pi(H_i)| = |\pi(G)| - 1 < |\pi(G)|$$

$\forall\ 1 \leq i \leq 3$. Therefore, by induction, H_i is solvable, for all $1 \leq i \leq 3$ and thus, by theorem (4.8), G is solvable. $\square$

Hall's Theorem (Hall, 1928) has been a foundational tool for many modern group theorists. Later on, we will see how it will be of use in the proof of the final theorem. At times, it may be useful to focus on the image of elements under automorphisms and see how given group elements and their images relate to each other. The following definition is motivated by this line of thought.

Definition: Let G be a group, $H \leq G$. Then, H is called ϕ- *invariant* if $\phi(H) \leq H$.

Proposition 12. *Suppose G is a group, $\phi \in Aut(G)$, and $H \leq G$ such that H is ϕ–invariant. Then, $N_G(H)$ and $C_G(H)$ are ϕ-invariant.*

Proof. Let $h \in H$, and $g \in N_G(H)$. Then, $\phi(h) \in H$ and $h^g \in H$. Thus $\phi(h^g) \in H$, but $\phi(h^g) = \phi(h)^{\phi(g)} \in H$. Thus $\phi(g) \in N_G(H)$, and so $N_G(H)$ is ϕ-invariant.

Now, let $h \in H$, $g \in C_G(H)$. The, $gh = hg$, and we have that $\phi(gh) = \phi(hg)$ by well-definedness. So

$$\phi(g)\phi(h) = \phi(gh) = \phi(hg) = \phi(h)\phi(g)$$

and since $\phi(h) \in H$, we see that $\phi(g) \in C_G(H)$. Thus, $C_G(H)$ is ϕ-invariant.

□

Definition: Let G be a group, $\phi \in Aut(G)$, and $g \in G$. Define

1. $[g, \phi] = g^{-1}\phi(g)$.

2. $[G, \phi] = \langle [g, \phi] \mid g \in G \rangle$.

3. $C_G(\phi) = \{g \in G | \ \phi(g) = g\}$.

Proposition 13. *Let G be a group, $\phi \in Aut(G)$, and $g \in G$. Then, $C_G(\phi) \leq G$.*

Proof. Clearly $1 \in C_G(\phi)$ since ϕ is a homomorphism, and so $C_G(\phi) \neq \emptyset$. Now, let $a, b \in C_G(\phi)$. So we know, $\phi(a) = a$, and $\phi(b) = b \implies b^{-1} = \phi(b)^{-1} = \phi(b^{-1})$. Thus

$$ab^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1})$$

and so $ab^{-1} \in C_G(\phi)$. Therefore $C_G(\phi) \leq G$. □

Definition: Let G be a group, and $\phi \in Aut(G)$. Then ϕ is *fixed-point-free* if $C_G(\phi) = \{1\}$.

We will now focus on some results about these fixed-point-free automorphisms.

Theorem 4.10. *Let G be a group, $\phi \in Aut(G)$, suppose $C_G(\phi) = 1$, and $|\phi| = n$. Then,*

1. $G = \{x^{-1}\phi(x) | \ x \in G\}$.

2. $x\phi(x)\phi^2(x)\phi^3(x)...\phi^{n-1}(x) = 1\ \forall x \in G$.

Proof. Let $S = \{x^{-1}\phi(x) |\ x \in G\}$.

CLAIM: $S = G$.

Clearly, $S \subseteq G$ (since $\phi \in Aut(G)$). Now, suppose $\exists x, y \in G$ such that $x \neq y$ and $x^{-1}\phi(x) = y^{-1}\phi(y)$. Then $yx^{-1} = \phi(y)\phi(x)^{-1} = \phi(yx^{-1})$. Thus, $yx^{-1} \in C_G(\phi) = 1$. Hence, $yx^{-1} = 1 \implies y = x$, a contradiction. Therefore $|S| = |G|$, and so $G = S$.

For (2), let $x \in G$.By (1), $\exists y \in G$ such that $x = y^{-1}\phi(y)$. Then,

$$x\phi(x)\phi^2(x)...\phi^{n-1}(x) = y^{-1}\phi(y) = y^{-1}\phi(y)\phi(y)^{-1}\phi^2(y)(\phi^2(y))^{-1}...(\phi^{n-1}(y))^{-1}\phi^n(y),$$

which simplifies down to

$$y^{-1}\phi^n(y) = y^{-1}y = 1,$$

as desired. □

Proposition 14. *Let G be a group, and $P \leq G$ be a p-subgroup of G, such that $P \in Syl_p(N_G(P))$. Then, $P \in Syl_p(G)$.*

Proof. Suppose $P \notin Syl_p(G)$. Then, $\exists Q \in Syl_p(G)$, such that $P < Q$. Thus, we know that since Q is a p-group, $P < N_Q(P)$. But then we have $P < N_Q(P) \leq N_G(P)$, a contradiction since $N_Q(P)$ is a p-group and $P \in Syl_p(N_G(P))$. Thus $P \in Syl_p(G)$. □

Theorem 4.11. *Let G be a group, $\phi \in Aut(G)$, and $C_G(\phi) = 1$. Then*

1. *$\exists$ a unique $P \in Syl_p(G)$ such that P is ϕ-invariant $\forall\ p \in \pi(G)$.*

2. *If $U \leq G$ is a ϕ-invariant p-subgroup, then $U \leq P$.*

Proof. For (1), let $P \in Syl_p(G)$. Since ϕ is one-to-one, we get $|\phi(P)| = |P|$. Thus $\phi(P) \in Syl_p(G)$, and by Sylow's $2nd$ theorem, $\exists g \in G$ such that $\phi(P) = P^g$. By theorem (4.10), $\exists x \in G$ such that $g = x^{-1}\phi(x)$. Now, consider $P^{x^{-1}}$. Then, $P^{x^{-1}} \in Syl_p(G)$ and

$$\phi(P^{x^{-1}}) = \phi(P)^{\phi(x)^{-1}} = P^{g\phi(x)^{-1}} = P^{x^{-1}}.$$

Thus $P^{x^{-1}}$ is ϕ-invariant. Now, suppose $P, Q \in Syl_p(G)$ are each ϕ-invariant. By Sylow's theorem, $\exists g \in G$ such that $P^g = Q$. Then,

$$P^g = Q = \phi(Q) = \phi(P^g) = \phi(P)^{\phi(g)} = P^{\phi(g)}.$$

Thus $P^g = P^{\phi(g)}$ or $P = P^{\phi(g)g^{-1}}$. Hence $\phi(g)g^{-1} \in N_G(P)$. Since P is ϕ-invariant, by proposition 12, $N_G(P)$ is ϕ-invariant. Also $C_{N_G(P)}(\phi) \leq C_G(\phi) = 1$, and thus $C_{N_G(P)}(\phi) = 1$. By theorem 4.10, $\exists n \in N_G(P)$ such that $\phi(g)g^{-1} = \phi(n)n^{-1}$. Hence $\phi(n^{-1}g) = n^{-1}g$. So $n^{-1}g = 1$, since $n^{-1}g \in C_G(\phi)$, and so $g = n$. Then,

$$Q = P^g = P^n = P,$$

and so $Q = P$ giving (1).

For (2), let $U \leq G$ and let $P_0 \leq G$ be a maximal ϕ–invariant p-subgroup such that $U \leq P_0$. Since P_0 is ϕ-invariant, by proposition 12, $N_G(P_0)$, is ϕ-invariant. Moreover $C_{N_G(P_0)}(\phi) \leq C_G(\phi) = \{1\}$ and so $C_{N_G(P_0)} = 1$. Therefore, by (1), $\exists!\ P \in Syl_p(N_G(P_0))$ such that P is ϕ-invariant. Now, $P_0 \trianglelefteq N_G(P_0)$ and P_0 is a p-group. So, it follows that $P_0 \leq P$.

CLAIM: $P_0 \in Syl_p(N_G(P_0))$.

If $P_0 \notin Syl_p(N_G(P_0))$, then $P_0 < P$. Since P is a p-group and $P_0 < P$ we get $P_0 < N_G(P_0)$. Again, by proposition 12, since P and P_0 are ϕ-invariant, we know $N_G(P_0)$ is ϕ–invariant. But then we get,

$$U \leq P_0 < N_G(P_0),$$

a contradiction to the maximallity of P_0. Thus $P_0 \in Syl_p(N_G(P_0))$ and by proposition 13, $P_0 \in Syl_p(G)$. Thus $U \leq P_0$ and P_0 is the ϕ-invariant Sylow p subgroup of G. $\square$

These fixed-point-free automorphisms can be induced from the original group to a quotient group, which could prove useful in scenarios where induction is used as a proving tool. The following theorem fills in the details for how this works.

Theorem 4.12. *Let G be a group, $N \trianglelefteq G$ be ϕ-invariant, and $\phi \in Aut(G)$ such that $C_G(\phi) = 1$. Then, ϕ induces a fixed-point-free action on $\frac{G}{N}$.*

Proof. Let $\overline{G} = \frac{G}{N}$, define $\phi : \overline{G} \mapsto \overline{G}$ by

$$\phi(\overline{g}) = \overline{\phi(g)}$$

$\forall \overline{g} \in \overline{G}$. (NOTE: this map is technically $\phi|_{\overline{G}}$, but will just continue to be referred to as ϕ). To show ϕ is well-defined, let $\overline{g_1}$, $\overline{g_2}$ such that $\overline{g_1} = \overline{g_2}$. That means, $g_1N = g_2N \implies g_2^{-1}g_1 \in N$, and so since N is ϕ–invariant, we get $\phi(g_2^{-1}g_1) \in N$. Thus, we have $\phi(g_1)N = \phi(g_2)N$ or, in other words $\overline{\phi(g_1)} = \overline{\phi(g_2)}$ and so ϕ is well-defined. Now, let $\overline{a}, \overline{b} \in \overline{G}$. then,

$$\phi(\overline{a}\overline{b}) = \phi(aNbN) = \phi(abN) = \phi(\overline{ab}) = \overline{\phi(ab)} = \phi(ab)N = \overline{\phi(a)\phi(b)} = \overline{\phi(a)}\;\overline{\phi(b)}.$$

Thus, ϕ is a homomorphism. Let $\overline{a} \in \overline{G}$. Then, $a \in G$, since $\phi \in Aut(G)$, $\exists b \in G$ such that $\phi(b) = a$. Then $\overline{b} \in \overline{G}$ and $\phi(\overline{b}) = \overline{\phi(b)} = \overline{a}$ and so ϕ is onto. If $\overline{a}, \overline{b} \in \overline{G}$ such that $\phi(\overline{a}) = \phi(\overline{b})$. Then,

$$\overline{\phi(a)} = \overline{\phi(b)}$$

meaning that $\phi(b)^{-1}\phi(a) = \phi(b^{-1}a) \in N$. Now, since N is ϕ–invariant, $\phi(N) \leq N \implies \phi(N) = N$ and so $\phi(b^{-1}a) \in \phi(N)$ and so $\exists n \in N$ such that $\phi(b^{-1}a) = \phi(n)$. Since $\phi \in Aut(G)$ we get $b^{-1}a = n \in N$, so $\overline{a} = \overline{b}$, and so ϕ is one-to-one.

Now, let $\overline{a} \in C_{\overline{G}}(\phi)$, then $\phi(\overline{a}) = \overline{a}$. In other words, $\overline{\phi(a)} = \overline{a} \implies a^{-1}\phi(a) \in N$. Since

N is ϕ-invariant and $C_N(\phi) \le C_G(\phi) = 1$, we get that ϕ acts fixed-point-freely on N. By theorem (4.10) $\exists n \in N$ such that $a^{-1}\phi(a) = n^{-1}\phi(n) \implies \phi(an^{-1}) = an^{-1}$ and thus $an^{-1} \in C_G(\phi) = 1$. Thus $an^{-1} = 1$ so $a = n$. Hence $\overline{a} = 1$, and so $C_{\overline{G}}(\phi) = 1$. □

Now, finally, for some results about fixed-point-free automorphisms with specific orders.

Theorem 4.13. *Let G be a group, $\phi \in Aut(G)$ and $C_G(\phi) = 1$ such that $|\phi| = 2$. Then G is abelian.*

Proof. Let $x \in G$. By theorem (4.10), we know

$$x\phi(x) = 1 \implies \phi(x) = x^{-1}.$$

Thus, if $y \in G$, then

$$xy = (y^{-1}x^{-1})^{-1} = (\phi(y)\phi(x))^{-1} = \phi(yx)^{-1} = (x^{-1}y^{-1})^{-1} = yx$$

and hence, G is abelian. □

Thus, in a situation where there exists a fixed-point-free automorphism, ϕ, of order 2, not only do we know the group must be abelian, we also know exactly what map ϕ has to be. So, in some ways, the order of the automorphism characterizes the automorphism itself. Now for another result involving a fixed-point-free automorphism of a different order.

Theorem 4.14. *Let G be a group, $\phi \in Aut(G)$ and $C_G(\phi) = 1$, such that $|\phi| = 3$. Then, G is nilpotent.*

Proof. Now, recall that we have characterized the quality of a group's nilpotence as being equivalent to many other statements. One of those statement was that all Sylow-p subgroups are normal $\forall p \in \pi(G)$. Thus, to show nilpotence, we need only show that Sylow-p subgroups are normal in G.

So suppose G is *not* nilpotent. Then $\exists P \in Syl_p(G)$ such that $P \ntrianglelefteq G$ and P is ϕ–invariant, by theorem (4.11). Hence, by Sylow's theorem ($n_p \neq 1$) and so $\exists Q \in Syl_p(G)$ such that $P \neq Q$. Since $|P| = |Q| = |G|_p$, we get $Q \not\subseteq P$. Then, $\exists x \in Q - P$, and since $C_G(\phi) = 1$ and $|\phi| = 3$, by theorem (4.10), we get

$$x\phi(x)\phi^2(x) = 1 = \phi^2(x)\phi(x)x \implies x\phi(x) = (\phi^2(x))^{-1} = \phi(x)x.$$

Let $H = \langle x, \phi(x) \rangle$. Then by proposition 2, $H \leq G$, also since $x\phi(x) = \phi(x)x$, we know H is abelian. Since $x \in Q$, we know x is a p-element. Also, since $\phi \in Aut(G)$, we know $|\phi(x)| = |x|$, and so $\phi(x)$ is a p-element.

Thus, since $x\phi(x) = \phi(x)x$, it follows that all elements of H are p-elements. Hence, H is an abelian p-group. Since $\phi(x) \in H$, $\phi(\phi(x)) = \phi^2(x) = x^{-1}\phi(x)^{-1} \in H$. Since $H = \langle x, \phi(x) \rangle$ we get that H is a ϕ-invariant p-group. Thus by theorem (4.10) we get that $x \in H \leq P$, a contradiction. Therefore, G is nilpotent. $\square$

Chapter Five

Transfer

The transfer is one of the more commonly used tools in group theory. It arises from the action of a group on an abelian section of a subgroup's cosets. Some insight on this will be given throughout this chapter.

Definition: Let G be a group and $H \leq G$. Then, $\exists \{g_i\}_{i=1}^{n} \subseteq G$ such that

$$G = \bigcup_{i=1}^{n} Hg_i,$$

and the union is disjoint. We call $\{g_i\}_{i=1}^{n}$ a transversal of H in G, and

$$\mathscr{T} = \{T |\ T \text{ is a transversal of H in G}\}.$$

Remark: For $T = \{t_i\}_{i=1}^{n}$, $U = \{u_i\}_{i=1}^{n} \in \mathscr{T}$, after re-indexing of the sets, we can assume $t_i u_i^{-1} \in H$, $\forall i = 1, \ldots, n$.

Theorem 5.1. *Let G be a group, $J \trianglelefteq H \leq G$, such that $\frac{H}{J}$ is abelian, and $T = \{t_i\}_{i=1}^{n}$, $S = \{s_i\}_{i=1}^{n}$, $U = \{u_i\}_{i=1}^{n} \in \mathscr{T}$. Define $\frac{T}{U} \in \frac{H}{J}$, by*

$$\frac{T}{U} = \prod_{i=1}^{n} J t_i u_i^{-1}$$

and for $g \in G$, define

$$Tg = \{t_i g\}_{i=1}^n.$$

Then,

1. $\frac{T}{T} = J$.

2. $(\frac{T}{U})^{-1} = \frac{U}{T}$.

3. $\frac{T}{U} \cdot \frac{U}{S} = \frac{T}{S}$, $\forall S, T, U \in \mathscr{T}$.

4. $\frac{Tg}{Ug} = \frac{T}{U}$

Proof. For (1),

$$\frac{T}{T} = \prod_{i=1}^n J t_i t_i^{-1} = \prod_{i=1}^n J1 = J.$$

For (2),

$$\frac{T}{U} \cdot \frac{U}{T} = \prod_{i=1}^n J t_i u_i^{-1} \prod_{i=1}^n J u_i t_i^{-1},$$

and since $\frac{H}{J}$ is abelian, we can rewrite that as

$$\prod_{i=1}^n J t_i u_i^{-1} J u_i t_i^{-1} = \prod_{i=1}^n J1 = J.$$

Thus, we get that $(\frac{T}{U})^{-1} = \frac{U}{T}$. For (3), realize that

$$\frac{T}{U} \cdot \frac{U}{S} = \prod_{i=1}^n J t_i u_i^{-1} \prod_{i=1}^n J u_i s_i^{-1} = \prod_{i=1}^n J t_i u_i^{-1} J u_i s_i^{-1} = \prod_{i=1}^n J t_i s_i^{-1} = \frac{T}{S}.$$

Now, finally, for (4), observe that

$$\frac{Tg}{Ug} = \prod_{i=1}^n J t_i g g^{-1} u_i^{-1} = \prod_{i=1}^n J t_i u_i^{-1} = \frac{T}{U}.$$

□

Theorem 5.2. *Let G be a group, $J \trianglelefteq H \leq G$ such that $\frac{H}{J}$ is abelian, and $T \in \mathscr{T}$. Define the transfer of G into $\frac{H}{J}$, τ by*

$$\tau(g) = \frac{Tg}{T}, \ \forall g \in G.$$

Then,

1. *τ is a homomorphism.*

2. *τ doesn't depend on T (or any transversal).*

Proof. For (1), if $g_1, g_2 \in G$, then

$$\tau(g_1 g_2) = \frac{Tg_1g_2}{T} = \frac{Tg_1g_2}{Tg_2} \cdot \frac{Tg_2}{T} = \frac{Tg_1}{T} \cdot \frac{Tg_2}{T} = \tau(g_1)\tau(g_2),$$

by theorem (5.1). For (2), let $U \in \mathscr{T}$, $g \in G$. Then

$$\frac{Tg}{T} = \frac{Tg}{Ug} \cdot \frac{Ug}{U} \cdot \frac{U}{T} = \frac{T}{U} \cdot \frac{Ug}{U}\frac{U}{T} = \frac{T}{U} \cdot \frac{Ug}{U} \cdot \left(\frac{T}{U}\right)^{-1} = \frac{Ug}{U}.$$

Thus, we can see that τ is independent of T. □

Here, τ is commonly referred to as the "transfer homomorphism". Again, as seen from the last theorem, it is important to note that this homomorphism does not depend on the choice of a transversal, which can be helpful since this means a transversal can be freely chosen based on convenience.

Proposition 15. *Let G be a group, $H \trianglelefteq G$, $g \in G$, $n \in \mathbb{Z}$ such that $g^n \in H$ and $gcd(\frac{|G|}{|H|}, n) = 1$. Then, $g \in H$.*

Proof. Let $m = \frac{|G|}{|H|}$. Since $gcd(m,n) = 1$, $\exists x, y \in \mathbb{Z}$ such that $mx + ny = 1$, and so $mx = 1 - ny$. Now, realize that

$$gH = g^{1-ny}H,$$

since $(g^{1-ny})^{-1}g = g^{ny-1}g = g^{ny} = (g^n)^y \in H$. But $1 - ny = mx$, and so we have

$$gH = g^{mx}H = (g^xH)^m = 1H.$$

Thus we get that $gH = 1H \implies g \in H$. $\square$

Theorem 5.3. *Let G be a group, $J \trianglelefteq H \leq G$, $\frac{H}{J}$ is abelian, $\frac{|G|}{|H|} = m$, $\frac{|H|}{|J|} = n$, and $gcd(m,n) = 1$. Then, $H \cap Z(G) \cap G' \leq J$.*

Proof. Let $h \in H \cap Z(G) \cap G'$, and $\tau : G \mapsto \frac{H}{J}$ be the transfer homomorphism, and $T \in \mathscr{T}$, $T = \{t_i\}_{i=1}^n$. Then, by the first isomorphism theorem,

$$\frac{G}{Kern\tau} \cong \tau(G) \leq \frac{H}{J}$$

is abelian. Thus $\frac{G}{kern\tau}$ is abelian and so by theorem (1.11), $G' \leq Kern\tau$, but then $h \in G'$ and so $h \in Kern\tau$. Hence, $J = \tau(h) = \frac{Th}{T} = \frac{hT}{T}$ (since $h \in Z(G)$), and realize that

$$\frac{hT}{T} = \prod_{i=1}^{m} Jht_it_i^{-1} = \prod_{i=1}^{m} Jh = Jh^m.$$

Therefore $h^m \in J$, and so by proposition 15, we get $h \in J$, thus

$$H \cap \ Z(G) \cap G' \leq J.$$

$\square$

Definition: Let G be a group, $J \trianglelefteq H \leq G$, $\frac{H}{J}$ be abelian, $\mathscr{T} = \{T |\ T$ is a transversal of H in G$\}$, and $T, U \in \mathscr{T}$. Define $\sim$ on $\mathscr{T}$ by, $T \sim U$ is $\frac{T}{U} = J$.

<u>Comment:</u> By theorem 5.1, $\sim$ is an equivalence relation on $\mathscr{T}$. Let $\Omega = \{[T] | T \in \mathscr{T}\}$ be the set of equivalence classes. Notice that G and H act on Ω by

$$g[T] = [Tg^{-1}]$$

and

$$h[T] = [hT],$$

$\forall g \in G$ and $\forall h \in H$.

Theorem 5.4. *Let G be a group, $J \trianglelefteq H \leq G$, $\frac{H}{J}$ be abelian, $\frac{|G|}{|H|} = m$, $\frac{|H|}{|J|} = n$, $\mathscr{T} = \{T |\ T$ is a transversal of H in $G\}$, $\Omega = \{[T] |\ T \in \mathscr{T}\}$, and $gcd(m,n) = 1$. Then,*

1. *H acts transitively on Ω.*
2. *$H_{[T]} = J$, $\forall [T] \in \Omega$.*

Proof. For (1), let $T, U \in \mathscr{T}$. It's enough to show that $\exists h \in H$ such that $hT \sim U$. Since $gcd(m,n) = 1$, $\exists x, y \in \mathbb{Z}$ such that $xm + yn = -1$. Now, $(\frac{T}{U})^n = J$, and so $(\frac{T}{U})^{-n} = J \implies (\frac{T}{U})^{-ny} = J$. Let $h \in H$ such that $(\frac{T}{U})^x = Jh$. Then,

$$\frac{hT}{U} = \frac{hT}{T} \cdot \frac{T}{U} = \prod_{i=1}^{m} Jht_i t_i^{-1} \cdot \frac{T}{U} = Jh^m \cdot \frac{T}{U} = \left(\frac{T}{U}\right)^{mx} \cdot \left(\frac{T}{U}\right) = \left(\frac{T}{U}\right)^{mx+1} = \left(\frac{T}{U}\right)^{-ny} = J.$$

Thus $hT \sim U$ and so H acts transitively on Ω. For (2), let $j \in J$. Then $\frac{jT}{T} = \prod_{i=1}^{m} Jjt_i t_i^{-1} = \prod_{i=1}^{m} Jj = J$. Thus, $jT \sim T$ and so $j \in H_{[T]}$, and therefore $J \leq H_{[T]}$. Now, let $h \in H_{[T]}$. Then, $hT \sim T$ and so $J = \frac{hT}{T} = \prod_{i=1}^{m} Jht_i t_i^{-1} = Jh^m$. Therefore, $h^m \in J$, and by proposition 15, we get $h \in J$. Thus $H \leq J$ and therefore $H_{[T]} = J$. $\square$

Remark:

Let G be a group, $J \trianglelefteq H \leq G$, $\frac{H}{J}$ be abelian, $\frac{|G|}{|H|} = m$, and $\mathscr{T}, \sim, \Omega, \tau$ be defined as they have been in the previous theorems.

Let $g \in G$, and let $\langle g \rangle$ act on $X = \{Hx |\ x \in G\}$ by right multiplication. Then

$$X = \bigcup_{i=1}^{s} \mathscr{O}_i,$$

where, $s \in \mathbb{Z}^+$, and $\mathscr{O}_i$ is an orbit $\forall\ 1 \le i \le s$. Then,

$$\mathscr{O}_i = \{Hx_i, Hx_i g, Hx_i g^2, ..., Hx_i g^{n_i - 1}\},$$

where $n_i \in \mathbb{Z}^+$, and $x_i g_i^{n_i} x_i^{-1} \in H$, $\forall\ 1 \le i \le s$. Let $T = \{x_i g^r |\ 0 \le r \le n_i - 1$, and $1 \le i \le s\}$. Then, $T \in \mathscr{T}$, and $Tg = \{x_i g^r |\ 0 \le r \le n_i$ and $1 \le i \le s\}$. Then,

$$\tau(g) = \prod_{i=1}^{s} J x_i g^{n_i} x_i^{-1},$$

and $x_i g^{n_i} x_i^{-1} \in H$, $\forall\ 1 \le r \le s$, and $\sum_{i=1}^{s} n_i = m$.

Definition: Let G be a group and $J \trianglelefteq H \le G$. Then,

1. $\underline{G \text{ splits over } H}$ if $\exists K \le G$ such that $G = HK$ and $H \cap K = 1$. We call K a $\underline{\text{complement}}$ of H in G, and if $K \trianglelefteq G$, we call it a $\underline{\text{normal complement}}$ of H in G and we say G splits *normally* over H.

2. $\underline{G \text{ splits over } \frac{H}{J}}$ if $\exists K \le G$ such that $G = HK$ and $H \cap K = J$. If K is normal, we say G splits *normally* over $\frac{H}{J}$.

Example

Consider S_3. We know $\langle (12) \rangle \le S_3$, moreover we know $S_3 = \langle (12) \rangle \langle (123) \rangle$ and $\langle (12) \rangle \cap \langle (123) \rangle = 1$. Also, realize that $\langle (123) \rangle = A_3 \trianglelefteq S_3$. Thus we can say that S_3 splits normally over $\langle (12) \rangle$.

Proposition 16. *Let G be a group, S be a set such that G acts on S. If $H \le G$ and H acts transitively on S, then $G = G_a H$, $\forall a \in S$.*

Proof. Let $g \in G$ and let $a, b \in S$ such that $ga = b$ (since G acts on S Now, since H acts transitively on S, $\exists h \in H$ such that $b = ha$. Thus we get,

$$ga = ha \implies h^{-1} ga = a,$$

and so $h^{-1} g \in G_a \implies g \in G_a H$. Thus $G \subseteq G_a H$, and since we clearly have $G_a H \subseteq G$, we get $G = G_a H$. □

Theorem 5.5. *Let G be a group, $J \trianglelefteq H \leq G$, $\frac{H}{J}$ be abelian, $\frac{|G|}{|H|} = m$, $\frac{|H|}{|J|} = n$, $gcd(m,n) = 1$ and $\mathscr{T}, T, \sim, \Omega$, and τ be as they were in the previous theorems. Then, the following are equivalent:*

1. *G splits normally over $\frac{H}{J}$.*
2. *Whenever $\exists h_1, h_2 \in H$ such that h_1 and h_2 are conjugate in G, then $Jh_1 = Jh_2$.*
3. *$\tau(h) = Jh^m \ \forall h \in H$.*
4. *$Th \sim hT$, $\forall h \in H$.*

Proof. $(1) \implies (2)$: Suppose G splits normally over $\frac{H}{J}$. Then, $\exists K \trianglelefteq G$, $G = HK$ and $H \cap K = J$. Let $g \in G$, $h \in H$, such that $h^g \in H$, then $\exists h_1 \in H$, $k \in K$ such that $g = h_1 k$. Let $h_{h_1} = h_2$. Since $K \trianglelefteq G$, we get,

$$[k, h_2^{-1}] = k^{-1} h_2 k h_2^{-1} \in K,$$

but also realize that,

$$K^{-1} h_2 k h_2^{-1} = h_2^k h_2^{-1} = h^{h_1 k} h_2^{-1} = h^g h_2^{-1} \in H.$$

So, $[k, h_2^{-1}] \in H \cap K = J$. Thus, $Jh^g = Jh_2$, and so $Jh^g = Jh^{h_1} = Jh^{Jh_1} = Jh$, since $\frac{H}{J}$ is abelian, yielding (2).

$(2) \implies (3)$: Suppose (2) holds and let $h \in H$. By choosing the transversal, T, as in the previous remark in this chapter , we get

$$\tau(h) = \prod_{i=1}^{s} J x_i h^{n_i} x_i^{-1} = \prod_{i=1}^{s} J h^{n_i},$$

by (2). Thus we get

$$\prod_{i=1}^{s} J h^{n_i} = J h^{\sum_{i=1}^{s} n_i} = J h^m,$$

giving (3).

(3) $\implies$ (4): Suppose $\tau(h) = Jh^m \ \forall h \in H$, and let $h \in H$. Then,

$$\frac{Th}{hT} = \frac{Th}{T} \cdot \frac{T}{hT} = \frac{Th}{T} \cdot \left(\frac{hT}{T}\right)^{-1} = \tau(h) \cdot \left(\prod_{i=1}^{s} Jht_i t_i^{-1}\right)^{-1} = Jh^m \cdot (Jh^m)^{-1} = J$$

and thus, we have $hT \sim Th$.

(4) $\implies$ (1) : Suppose $hT \sim Th \ \forall h \in H$. Then, by theorem 5.4, H acts transitively on Ω on the right. By proposition (16), $G = G_{[T]}H$. Also, $G_{[T]} \cap H = H_{[T]} = J$, again by theorem 5.4. Finally, realize that for $g \in G_{[T]}$, we have

$$[T]g = [T] \implies [Tg] = [T] \implies Tg \sim T \implies \frac{Tg}{T} \iff \tau(g) = J \iff g \in Kern\tau,$$

and thus $G_{[T]} = Kern(\tau) \trianglelefteq G$. Thus G splits normally over $\frac{H}{J}$, and so (1) holds. □

Theorem 5.6. *Let G be a group, $A \in Hall_\pi(G)$ and A be abelian. Then G splits normally over A if and only if whenever $\exists a_1, a_2 \in A$ such that a_1 is conjugate in G to a_2 then, $a_1 = a_2$.*

Proof. Now $\{1\} \trianglelefteq A \leq G$, $\frac{A}{\{1\}} \cong A$ is abelian and $gcd\left(\frac{|G|}{|A|}, \frac{|A|}{|1|}\right) = gcd\left(\frac{|G|}{|A|}, |A|\right) = 1$, since $A \in Hall_\pi(G)$. Now, G splits normally over $A \iff G$ splits normally over $\frac{A}{\{1\}} \iff$ whenever $\exists a_1, a_2 \in A$ such that a_1 is conjugate to a_2, then $\{1\}a_1 = \{1\}a_2$ by theorem 5.5, and this is true if and only if whenever $\exists a_1, a_2 \in A$ such that a_1 is conjugate to a_2 then $a_1 = a_2$. □

Theorem 5.7. *Let G be a group, $P \in Syl_p(G)$, $x \in Z(G)$, and $y \in Z(P)$ such that x and y are conjugate in G. Then, x and y are conjugate in $N_G(P)$.*

Proof. Now, $\exists g \in G$, such that $x^g = y$. Since $x, y \in Z(P)$, we know $P \leq C_G(x) \cap C_G(y)$. Thus $P \in Syl_p(C_G(y))$, and also, since $P \leq C_G(x)$, we get

$$P^g \leq C_G(x) = C_G(x^g) = C_G(y).$$

Thus by Sylow's theorem, $\exists c \in C_G(y)$ such that $P^{gc} = P$. Then, $gc \in N_G(P)$ and $x^{gc} = y^c = y$. $\square$

The following theorem was first stated and proved by Burnside in the early 20th century. Since then, it has found extensive use as a tool for many group theorists.

Theorem 5.8. *Let G be a group, $P \in Syl_P(G)$ such that $P \leq Z(N_G(P))$. Then G splits normally over P.*

Proof. Since $P \leq Z(N_G(P))$, we know P is abelian. Suppose $x, y \in P$ such that x is conjugate to y in G. Since P is abelian, we have $P = Z(P)$, and so $x, y \in Z(P)$. So, by theorem (5.7), $\exists n \in N_G(P)$ such that $x^n = y$. But, $x \in P \leq Z(N_G(P))$ and so $x^n = x$, thus $x = y$ and so G splits normally over P, by theorem (5.6). $\square$

Chapter Six

Final Result

The main result of this paper is similar to the results at the end of chapter four. This result is separate, as it requires the use of all the weaponry introduced throughout this paper, along with a some auxiliary results mentioned in the lead up to the final result in this chapter. It is formally stated in the following pages.

Proposition 17. *Let G be a group of odd order. If $g \in G$ then $|g^2| = |g|$.*

Proof. Let $g \in G$, $|G|$ odd with $|g| = n, |g^2| = m$. Now since the order of $|G|$ is odd, then the order of all the elements must also be odd by LaGrange's theorem and so we can say $|g| = n = 2k - 1$ for $k \in \mathbb{Z}^+$. Now,

$$(g^2)^n = (g^n)^2 = 1^2 = 1,$$

and so $n \mid m$. Also, we have that

$$g^n = g^{2k-1} = 1 \implies g^{2k} = g \implies (g^{2k})^m = (g^{2m})^k = 1^k = 1 = g^m,$$

and so $m|n$. Thus $m = n$, as desired. $\square$

Proposition 18. *Let G be a group of odd order. If $g, x \in G$ such that $g^2 \in C_G(x)$, then $g \in C_G(x)$.*

Proof. Let $g, x \in G$, $g^2 \in C_G(x)$. Now since $|G|$ is odd, we know $|g|$ is also odd, i.e $\exists k \in \mathbb{Z}^+$ such that $g^{2k-1} = 1 \implies g^{2k} = (g^2)^k = g$. Now, $C_G(x)$ is a group, and since $g^2 \in C_G(x)$ we must have $(g^2)^k = g^{2k} = g \in C_G(x)$. □

Proposition 19. *Let G be a group, $N \trianglelefteq G$, $H \leq G$, and $\overline{G} = \frac{G}{N}$. Then, $N_{\overline{G}}(\overline{H}) = \overline{N_G(HN)}$*

Proof. Let $\overline{g} \in \overline{N_G(HN)}$. Then $g \in N_G(HN)N = N_G(HN)$. So, $(HN)^g = HN \implies \overline{HN}^{\overline{g}} = \overline{HN}$, or, in other words, $\overline{H}^{\overline{g}} = \overline{H}$. Thus, $\overline{g} \in N_{\overline{G}}(\overline{H})$ and we have $\overline{N_G(HN)} \leq N_{\overline{G}}(\overline{H})$.

Now, let $\overline{g} \in N_{\overline{G}}(\overline{H})$. Then $\overline{G}^{\overline{g}} = \overline{H}$, or $\overline{H^g} = \overline{H}$. Thus, by pre-imaging, we get that $H^g N = HN$, and since $N \trianglelefteq G$ we know that $N^g = N$. Hence, $H^g N^g = (HN)^g = HN$, and thus $g \in N_G(HN) \implies \overline{g} \in \overline{N_G(HN)}$ which implies that $N_{\overline{G}}(\overline{H}) \leq \overline{N_G(HN)}$. Therefore $N_{\overline{G}}(\overline{H}) = \overline{N_G(HN)}$. □

Proposition 20. *Let G be a group, $\phi \in Aut(G)$, $N \trianglelefteq G$ be ϕ−invariant and $\overline{G} = \frac{G}{N}$. Then $|\overline{\phi}|$ on $\overline{G}$ divides $|\phi|$ on G.*

Proof. Let $\overline{g} \in \overline{G}$. Then, $\overline{\phi}^{|\phi|}(\overline{g}) = \overline{\phi^{|\phi|}(g)} = \overline{g}$. Thus $\overline{\phi}^{|\phi|} = 1$, and so $|\overline{\phi}|$ on $\overline{G}$ divides $|\phi|$ on G. □

Lemma 6.1. *Let G be a group, $\phi \in Aut(G)$, and $n \in \mathbb{Z}^+$. Then, $C_G(\phi^n)$ is ϕ−invariant.*

Proof. Let $g \in C_G(\phi^n)$. Then, we know that $\phi^n(g) = g$. Now consider $\phi^n(\phi(g)$. Realize that

$$\phi^n(\phi(g)) = \phi(\phi^n(g)) = \phi(g),$$

and so $\phi(g) \in C_G(\phi^n)$. Thus, $C_G(\phi^n)$ is ϕ−invariant. □

Now, $k_2^{-1}h_2^{-1} \in KH$ and so $\exists hk \in HK$ such that $k_2^{-1}h_2^{-1} = hk$. Thus, from above we can write,

$$h_1k_1k_2^{-1}h_2^{-1} = h_1k_1hk \in HK$$

and so $HK \leq G$.

Now, for one final proposition before the main result.

Proposition 21. *Let G be a group, $H \leq G$, and $K \leq N_G(H)$. Then $HK \leq G$.*

Proof. Let $x = h_1k_1, y = h_2k_2 \in HK$, for $h_1, h_2 \in H, k_1, k_2 \in K$. We know that $h_1^{k_1} \in H$, since $K \leq N_G(H)$. Also, $(h_1^{k_1})^{k_2^{-1}} \in H$ and it follows that $(h_1^{k_1})^{k_2^{-1}} h_2^{-1} \in H \implies ((h_1^{k_1})^{k_2^{-1}} h_2^{-1})^{k_2k_1^{-1}} \in H$. Realize that

$$((h_1^{k_1})^{k_2^{-1}} h_2^{-1})^{k_2k_1^{-1}} = (k_2k_1^{-1})^{-1}k_2k_1^{-1}h_1k_1k_2^{-1}h_2^{-1}k_2k_1^{-1} = h_1k_1k_2^{-1}h_2^{-1}k_2k_1^{-1} \in H.$$

Thus, it follows that $h_1k_1k_2^{-1}h_2^{-1}k_2k_1^{-1}(k_1k_2^{-1}) = h_1k_1k_2^{-1}h_2^{-1} = xy^{-1} \in HK$, and so $HK \leq G$.

□

Theorem 6.2. *Let G be a group, $\phi \in Aut(G)$, and $C_G(\phi) = 1$ such that $|\phi| = 4$. Then, G is solvable.*

Proof. We will introduce a list of claims and verify them.

Claim (1): $|G|$ is odd.

Consider $\langle\phi\rangle \leq Aut(G)$. Now since $\phi \in Aut(G)$, we know $\langle\phi\rangle$ acts on G (as a set). Since G is the set being acted on, we get

$$G = \langle\phi\rangle 1 \cup \bigcup_{i=1}^{n} \langle\phi\rangle g_i,$$

where $n \in \mathbb{Z}^+$, $g_i \neq 1 \in G$, $\forall\ 1 \leq i \leq n$. Then, $\langle\phi\rangle g_i = \{g_i, \phi(g_i), \phi^2(g_i), \phi^3(g_i)\}$, since $|\phi| = 4$. Also, since $g_i \neq 1$ and $C_G(\phi) = 1$, we know $g_i \neq \phi(g_i)$.

If $\phi^2(g_i) = g_2$, then $\phi^3(g_i) = \phi(g_i)$, and so $|\langle\phi\rangle g_i| = 2$.

If $\phi^2(g_i) \neq g_i$, then $\phi^2(g_i) = \phi(\phi(g_i)) \neq \phi(g_i)$, and in this case, if $\phi^2(g_i) = \phi^3(g_i)$, then by applying ϕ^{-2} we get $g_i = \phi(g_i)$, a contradiction. Thus in this case, $|\langle\phi\rangle g_i| = 4$. Therefore, $|\langle\phi\rangle g_i| = 2$ or 4, $\forall\ 1 \leq i \leq n$. Thus

$$|G| = |\langle\phi\rangle 1| + \sum_{i=1}^{n} |\langle\phi\rangle g_i| = 1 + 2k$$

for some $k \in \mathbb{Z}^+$, since each individual order is even, and since the order of the trivial orbit is just 1. Thus, $|G|$ is odd.

Now, let $\theta = \phi^2$, so $|\theta| = 2$, and let $F = C_G(\theta)$, and $I = \{g \in G |\ \theta(g) = g^{-1}\}$. Then, $F \leq G$ and $\{\emptyset\} \neq I \subseteq G$.

Claim (2): F is abelian.

If $f \in F$, then

$$\theta(\phi(f)) = \phi^2(\phi(f)) = \phi^3(f) = \phi(\phi^2(f)) = \phi(\theta(f)) = \phi(f).$$

Therefore, $\phi(f) \in F$ and so F is ϕ-invariant. Hence, ϕ (or $\phi|_F$)$\in Aut(F)$. Also, $C_F(\phi) \leq C_G(\phi) = 1$, and so $C_F(\phi) = 1$. Moreover, if $1 \neq f \in F$, then $\phi(f) \neq f$, but $\phi^2(f) = \theta(f) = f$, and so $|\phi| = 2$ on F. Thus, by theorem (4.13), F is abelian.

Claim(3): $G = IF = FI$.

Let $x \in G$. Then, $\theta(x^{-1}\theta(x)) = \theta(x)^{-1}\theta^2(x) = \theta(x)^{-1}\phi^4(x) = \theta(x)^{-1}x = (x^{-1}\theta(x))^{-1}$. Thus $x^{-1}\theta(x) \in I$. Now, using right cosets, if $x, y \in G$ such that $Fx \neq Fy$, then $yx^{-1} \notin F$, and so $\theta(yx^{-1}) \neq yx^{-1}$ or $\theta(y)\theta(x)^{-1} \neq yx^{-1}$. Thus $y^{-1}\theta(y) \neq x^{-1}\theta(x)$ and so $|I| \geq \frac{|G|}{|F|}$. Now, let $x, y \in I$ such that $x \neq y$. If (using left cosets) $xF = yF$, then $\exists f \in F$ such that $x = yf$ and so $\theta(x) = \theta(yf) = \theta(y)\theta(f)$. So $x^{-1} = y^{-1}f$, or $(yf)^{-1} = y^{-1}f \implies f^{-1}y^{-1} = y^{-1}f$ and so we get

$$f^{-1} = y^{-1}fy.$$

Hence $y^{-1}f^{-1}y = y^{-2}fy^2$, but we know that $y^{-1}f^{-1}y = (y^{-1}fy)^{-1}$ and so we have $(y^{-1}fy)^{-1} = y^{-2}fy^2$, or $(f^{-1})^{-1} = y^{-2}fy^2 \implies f = y^{-2}fy^2$. Thus, $y^2 \in C_G(f)$. Since

$|G|$ is odd, we get that $y \in C_G(f)$ and by above, that means that $f^{-1} = y^{-1}yf = f$ and so $f^2 = 1$. Again since $|G|$ is odd, it follows that $f = 1$ and so we get $x = y$, a contradiction to what our hypothesis. Thus $xF \neq yF$ and so $|I| \leq \frac{|G|}{|F|}$ and hence, $|I| = \frac{|G|}{|F|}$. Thus $G = \bigcup_{g_i \in I} g_i F = IF$ and by a similar argument, we get that $G = FI$.

Claim (4): Let $f_1, f_2 \in F$ and $g \in G$ such that $f_1 = f_2^g$. Then $f_1 = f_2$.

Since F is abelian and $G = FI$, we get that f_1 and f_2 being conjugate in G boiling down to f_1 and f_2 being conjugate in I. So $\exists g \in I$ such that $f_1 = f_2^g$. Thus, $\theta(f_1) = \theta(f_2^g) \implies f_1 = f_2^{\theta(g)} = f_2^{g^{-1}}$. Hence, $f_2^g = f_2^{g^{-1}} \implies f_2^{g^2} = f_2$, and thus $g^2 \in C_G(f_2)$ and since $|G|$ is odd we get $g \in C_G(f_2)$. Therefore $f_1 = f_2$.

Claim (5): If $H \leq F$, then $H \leq Z(N_G(H))$.

Let $H \leq F$, $h \in H$, and $g \in N_G(H)$. Now, $H \leq N_G(H)$ and $h^g \in H$, and so $h^g \in F$. But $h \in F$ and $h = (h^g)^{g^{-1}}$ so h and h^g are conjugate (in G). Thus, by (4), $h = h^g$, and so $h \in C_G(g)$. Hence, it follows that $H \leq Z(N_G(H))$.

Claim (6): Let $g \in I$. Then, $[g, \phi(g)] = 1$.

Since $C_G(\phi) = 1$, and $|\phi| = 4$, we get by theorem 4.10, that $g\phi(g)\phi^2(g)\phi^3(g) = 1$ or $g\phi(g)\theta(g)\phi(\theta(g)) = 1 \implies g\phi(g)g^{-1}\phi(g)^{-1} = 1$, or $g\phi(g) = \phi(g)g$. Thus $[g, \phi(g)] = 1$.

Claim (7): Let $p \in \pi(G)$ and $P \in Syl_p(G)$ be $\phi-$invariant. Then $F \leq N_G(P)$.

If $P \cap F = 1$, then since P is $\phi-$invariant we know that P is also $\theta-$invariant. Also, $C_P(\theta) = P \cap C_G(\theta) = P \cap F = 1$. Moreover, $|\theta| = 1$ or 2 on P. If $|\theta| = 1$ on P, then $P \leq F$, and since F is abelian we get $P \trianglelefteq F$. So we have $F \leq N_G(P)$ and the claim is proved. So, if $|\theta| = 2$ on P, then $\theta(x) = x^{-1}$ $\forall x \in P$ and so $P \subseteq I$. Let $x \in P$ and $f \in F$. Then $\theta(f^{-1}xf) = f^{-1}x^{-1}f = (f^{-1}xf)^{-1}$, and so $P^f \subseteq I$. Now, if $P^f \neq P$, then $\exists x \in P^f \backslash P$. Let $H = \langle x, \phi(x) \rangle$. Then, by (7), H is abelian which would make it an abelian $p-$group. Finally, since $x \in P^f \subseteq I$, we have H is a $\phi-$invariant p-group and so by theorem 4.11 we have that $x \in H \leq P$, a contradiction. Thus $P^f = P$, and so $F \leq N_G(P)$.

If $P \cap F \neq 1$, we use induction on $|G|$. Then, $P \cap F$ is a $\phi-$invariant $p-$group such that $F \leq N_G(P \cap F)$.Let $P \cap F \leq P_1$where P_1 is a maximal $\phi-$invariant p-group such that $F \leq N_G(P_1)$. Since P_1 is a $\phi-$invariant $p-$group, by theorem 4.11, $P_1 \leq P$.

If $N_G(P_1) \neq G$, then $N_G(P_1)$ is $\phi-$invariant and $C_{N_G(P_1)}(\phi) \leq C_G(\phi) = 1$. By theorem 4.11, $\exists P_2 \in Syl_p(N_G(P_1))$ such that P_2 is $\phi-$invariant. By induction, $F \leq N_G(P_2)$.Now, $P_1 \trianglelefteq N_G(P_1)$ and P_1 is a $p-$group and so it follows that $P_1 \leq P_2$. Suppose $P_1 \neq P_2$, say $P_1 < P_2$. Then, $P_1 < N_{P_2}(P_1)$, but $N_{P_2}(P_1)$ is a $\phi-$invariant $p-$group and $F \leq N_{P_2}(P_1)$ which contradicts the maximallity of P_1. Thus $P_1 = P_2 \in Syl_p(N_G(P_1))$, and by proposition 14, we get $P_1 \in Syl_p(G)$ and it's $\phi-$invariant. Thus, by theorem 4.11, $P = P_1$, and so $F \leq N_G(P)$.

Now, if $G = N_G(P_1)$, then $P_1 \trianglelefteq G$. Let $\overline{G} = \frac{G}{P_1}$, then $\overline{G}$ is $\phi-$invariant and $C_{\overline{G}}(\phi) = 1$, by theorem 4.12. Also, $\overline{P} \in Syl_P(\overline{G})$ is $\phi-$invariant. Moreover, $\overline{F} = \overline{C_G(\theta)} = C_{\overline{G}}(\theta)$. Now it follows that $|\phi| = 2$ or 4 on $\overline{G}$ and, in either case, $\overline{F} \leq N_{\overline{G}}(\overline{P})$ by induction. But $\overline{F} \leq N_{\overline{G}}(\overline{P}) = \overline{N_G(PP_1)} = \overline{N_G(P)}$, and so $F < FP_1 \leq N_G(P)P_1 = N_G(P)$, as desired.

Claim (8): If $A \leq G$ is $\phi-$invariant, and $B \leq G$ is $\phi-$invariant such that $F \leq N_G(A) \cap N_G(B)$, then $ABF \leq G$ is $\phi-$invariant.

Now, since A, B and F are $\phi-$invariant and $F \leq N_G(A) \cap N_G(B)$, we know $AF \leq G$ is $\phi-$invariant and $BF \leq G$ is $\phi-$invariant. Thus it's enough to show that $ABF = BFA$. But $BFA = BAF$ since $AF \leq G$ and by proposition (21) . Thus we only need to show $ABF = BAF$. Also, since $|ABF| = |BAF|$, then to verify our claim, it's enough to show that $BAF \subseteq ABF$. Which, again can be simplified down to showing that $BA \subseteq ABF$.

Let $ba \in BA$. By claim (3), we can write $A = (A \cap I)(A \cap F)$, and $B = (B \cap F)(B \cap I)$. Then, $a = a_1 f_1$, $b = f_2 b_1$, where $a_1 \in (A \cap I), f_1 \in (A \cap F), f_2 \in (B \cap F), b_1 \in (B \cap I)$. Then, $ba = f_2 b_1 a_1 f_1$. Since $F \leq N_G(A) \cap N_G(B)$, it's enough to show $b_1 a_1 \in ABF$. Since $G = FI$, $\exists f \in F$, $h \in I$ such that $b_1^{-1} a_1^{-1} = fh$. Applying θ to both sides,we get $b_1 a_1 = fh^{-1}$, but from above we get that $h^{-1} = a_1 b_1 f$. Hence $b_1 a_1 = f a_1 b_1 f = a_2 f b_1 f = a_2 b_2 f^2$, where $a_2 \in A, b_2 \in B$, since $F \leq N_G(A) \cap N_G(B)$. Thus, $b_1 a_1 \in ABF$ and so $ABF \leq G$ is $\phi-$invariant.

Final Claim (9): Let $n \in \mathbb{Z}^+$ such that $n \leq |\pi(G)|$, $\{p_i\}_{i=1}^n \subseteq \pi(G)$, and $P_i \in Syl_{p_i}(G)$ such that each P_i is $\phi-$invariant $\forall\ 1 \leq i \leq n$. Then, $P_1 P_2 P_3 ... P_n \leq G$.

Using induction on n, if $n = 1$, then $P_1 \leq G$ and the claim holds. Now, let $H = P_1 P_2 P_3 ... P_{n-1}$. Then, by induction, we can say that $H \leq G$. Also, since P_i is $\phi-$invariant $\forall i$, H is $\phi-$invariant. Moreover, by claim (7), $F \leq N_G(P_i)$ $\forall 1 \leq i \leq n-1$. Thus we can say that $F \leq N_G(H)$. Now, by claim (8), we have $K = HP_nF \leq G$. Let $Q \in Syl_q(F)$ such that $q \notin \{p_i\}_{i=1}^n$. Then it follows that $Q \in Syl_q(K)$, since they would share the same number of primes q. Also, by claim (5), $Q \leq Z(N_G(Q))$. But then $Q \leq Z(N_K(Q))$, and thus by Burnside's theorem, K splits normally over Q. In other words, $\exists K_q \trianglelefteq K$ such that $K = K_q Q$, and $K_q \cap Q = 1$. Let $\overline{K} = \frac{K}{K_q}$. Then,

$$\overline{K} = \frac{K}{K_q} = \frac{K_q Q}{K_q},$$

and by the second isomorphism theorem we get

$$\frac{K_q Q}{K_q} \cong \frac{Q}{Q \cap K_q} = \frac{Q}{\{1\}} \cong Q.$$

Thus, $\overline{K}$ is a q–group, but then $\overline{H} = \overline{P_n} = 1$ since $q \notin \{p_i\}_{i=1}^n$. Hence $H \leq K_q$, and $P_n \leq K_q$, meaning that $HP_n \leq K_q$.

Now, repeat this process for all such primes q, and let $L = \bigcap_{\substack{q \in \pi(F) \\ q \notin \{p_i\}_{i=1}^n}} K_q$. Then, $L \leq G$. Since $gcd\left(\frac{|K|}{|K_q|}, \frac{|K|}{|K_r|}\right) = 1 \ \forall q \neq r$, by theorem 4.7, we get

$$\frac{|K|}{|L|} = \frac{|K|}{|\bigcap K_q|} = \prod_{\substack{q \in \pi(F) \\ q \notin \{p_i\}_{i=1}^n}} \frac{|K|}{|K_q|} = \prod_{\substack{q \in \pi(F) \\ q \notin \{p_i\}_{i=1}^n}} |Q| = \prod_{\substack{Q \in Syl_q(F) \\ q \notin \{p_i\}_{i=1}^n}} |Q| = \frac{|K|}{|HP_n|}.$$

Thus $|L| = |HP_n|$, but $HP_n \leq L$ and so $HP_n = L \leq G$. But $HP_n = P_1 P_2 P_3 ... P_{n-1} P_n \leq G$ and the claim holds. From this we can see that it is possible to construct any Hall subgroup for any combination of primes in $\pi(G)$, and so this means that $Hall_{p'}(G) \neq \varnothing \ \forall p \in \pi(G)$, and hence, by Theorem (4.9), G is solvable. □

REFERENCES

Bender, Helmut (1972). "A Group Theoretic Proof of Burnside's pa qb-Theorem." In: *Mathematische Zeitschrift* 126, pp. 327–338. URL: http://eudml.org/doc/171744.

Gorenstein, Daniel and I.N Herstein (1961). "Finite Groups Admitting a Fixed-Point-Free Automorphism of Order 4". In: *American Journal of Mathematics* 83.1, pp. 71–78. URL: http://www.jstor.org/stable/2372721?origin=JSTOR-pdf.

Hall, P. (1928). "A Note on Soluble Groups". In: *Journal of the London Mathematical Society* s1-3.2, pp. 98–105. ISSN: 0024-6107. DOI: 10.1112/jlms/s1-3.2.98.