A Self-Contained Review of Thompson's Fixed-Point-Free Automorphism Theorem

by

Mario F. Sracic

Submitted in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in the

Mathematics

Program

YOUNGSTOWN STATE UNIVERSITY

May, 2014

A Self-Contained Review of Thompson's Fixed-Point-Free Automorphism Theorem

Mario F. Sracic

Signature:

Mario F. Sracic, Student Date

Approvals:

Dr. Neil Flowers, Thesis Advisor Date

Dr. Thomas Wakefield, Committee Member Date

Dr. Eric Wingler, Committee Member Date

Dr. Sal Sanders, Associate Dean of Graduate Studies Date

ABSTRACT

In the early 1900s, Frobenius conjectured if a group G admits a fixed-point-free automorphism ϕ, then G must be solvable. During the next half-century, mathematicians would struggle to find a completely group theoretic proof of Frobenius' Conjecture. Between 1960 and 1980, progress was made on the Conjecture only by assuming conditions on the order of ϕ.

In 1959, Thompson proved, for his dissertation, the case assuming the automorphism had prime order and resulted in a stronger condition than solvable [Tho59]; Hernstein and Gorenstein proved the conjecture with an automorphism of order 4 [DG61]; and in 1972, Ralston proved a group admitting a fixed-point-free automorphism with order pq is solvable, where p and q are primes. [Ral72] It was not until the 1980s, with the power of the Classification of Finite Simple Groups, was Frobenius' Conjecture finally proven; however, the proof involved character theory.

In this paper, we consider John Thompson's case of the Frobenius Conjecture:

Theorem ([Tho59])**.** *Let G be a group admitting a fixed-point-free automorphism of prime order. Then G is nilpotent.*

Our goal is to lay a complete framework of the necessary concepts and theorems leading up to, and including, the proof of Thompson's theorem.

Acknowledgments

First and foremost, I would like to thank Dr. Neil Flowers; for his countless hours of instruction and patience, without which this paper would not be possible; for sparking my initial interest in group theory; and for inspiring me to become a professor.

My gratitude goes to Dr. Tom Wakefield and Dr. Eric Wingler, for serving on my graduate committee and their assistance in the improvement of this work.

A special thank you to the Mathematics Department at Youngstown State University; for opening my mind to the wonder and joy of mathematics; for cultivating my mathematical skills; and providing an environment suitable for the enrichment of mathematics.

Finally, I am indebted to the late Dr. J. Douglas Faires, who was a phenomenal instructor, mentor, and friend. I would not be the mathematician I am today without his guidance and support.

Contents

1 Preliminaries

In this paper, we follow Gorenstein's notation indicating group actions and function images by suppressed left exponential notation: using x^g to denote $\phi(g)(x)$ and G^ϕ to denote $\phi(G)$. [Gor07]

Let G be a finite group, H be a subgroup of G, and $a, b \in G$. We will use 1 to represent the identity element of a group. If a is conjugated by b, we shall write $a^b = b^{-1}ab$. If $x, y \in H$ are conjugate in G, we shall say x and y are *fused* in G and write $x \sim_G y$. The set of all primes dividing the order of G will be given by $\pi(G)$. If $b \in G$ has order p^n for some $n \in \mathbb{N} \cup \{0\}$, where p is a prime, we call b a p-element and any element with order complementary to p is called a p'-element. If π is a set of primes and $\pi(G) \subseteq \pi$, then G is called a π-group. On the other hand, if $\pi(G) \nsubseteq \pi$, then G is a π'-group, where π' represents all primes not in π. We will denote $\mathbb{N} \cup \{0\}$ by $\mathbb{N}_0$.

All groups are finite. We assume the reader is familiar with the content of a first year course in abstract algebra, but we will include some relevant results. In the following section, we provide elementary definitions and theorems used repeatedly throughout the paper.

1.1 Elementary Group Theory

Theorem 1.1 (The First Isomorphism Theorem for Groups)**.** *Let G_1 and G_2 be groups, and suppose $\phi : G_1 \to G_2$ is a homomorphism. Then*

$$\frac{G_1}{Ker\ \phi} \cong G_1^{\phi}.$$

Theorem 1.2 (The Second Isomorphism Theorem for Groups)**.** *Let G be a group, $H \leqslant G$, and $N \trianglelefteq G$. Then*

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

Theorem 1.3 (The Third Isomorphism Theorem for Groups)**.** *Let G be a group, $N \trianglelefteq G$, and $N \leqslant H \trianglelefteq G$. Then*

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

Theorem 1.4 (Preimage and Image Theorem)**.** *Let G be a group, $N \trianglelefteq G, H \leqslant G$, and $\phi : G \to G/N$ be defined by*

$$g^{\phi} = gH$$

for all $g \in G$. Then

(*i*) $H^{\phi} = HN/N$.

(*ii*) $(HN/N)^{\phi^{-1}} = HN$.

(*iii*) *If $L \leqslant G/N$, then $L = K/N$, where $N \leqslant K \leqslant G$.*

Lemma 1.1. *Let G be a group, $L \leqslant H \leqslant G$, and $K \leqslant G$. Then $(H \cap K)L = H \cap KL$.*

Lemma 1.2. *Let G be a group, $N \trianglelefteq G$, $A \leqslant G$, and $B \leqslant G$. Then*

$$\frac{AN}{N} \cap \frac{BN}{N} = \frac{AN \cap B}{N} = \frac{A \cap BN}{N}.$$

Theorem (Lagrange)**.** *Let G be a group and $H \leqslant G$. Then $|H|$ divides $|G|$ and*

$$[G : H] = \frac{|G|}{|H|}$$

gives the number of left (or right) cosets of H in G.

Theorem 1.5 (Cauchy)**.** *Let G be a group and $p \in \pi(G)$. If G is abelian, then there exists a nontrivial $x \in G$ such that $x^p = 1$.*

Definition 1.1. *Let G be a group and $a, b \in G$. The* ***commutator*** *of a and b is*

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

The ***commutator subgroup*** *of G is*

$$G' = [G, G] = \langle [a, b] : a, b \in G \rangle.$$

Definition 1.2. *Let G be a group and $H \leqslant G$. The* ***commutator*** *of H and G is*

$$[G,H] = \langle [g,h] : g \in G \text{ and } h \in H \rangle.$$

Lemma 1.3. *Let G be a group, $H \leqslant G$, $K \leqslant G$, and $N \trianglelefteq G$. Then*

$$\frac{[H,K]H}{H} = \left[\frac{HN}{N}, \frac{KN}{N}\right].$$

Lemma 1.4. *Let G be a group, $H \leqslant G$, and $N \trianglelefteq G$. Then $HN/N \leqslant \mathcal{Z}(G/N)$ if and only if $[G,H] \leqslant N$.*

Lemma 1.5. *Let A and B be groups. Then $\mathcal{Z}(A \times B) = \mathcal{Z}(A) \times \mathcal{Z}(B)$.*

Lemma 1.6. *Let A and C be groups such that $B \trianglelefteq A$ and $D \trianglelefteq C$. Then*

$$B \times D \trianglelefteq A \times C,$$

and

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

Theorem (Fundamental Theorem of Finite Abelian Groups)**.** *Let G be a finite abelian group. Then, for some $n \in \mathbb{N}$,*

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}},$$

where p_i is a prime and $r_i \in \mathbb{N}_0$ for $1 \leq i \leq n$.

Lemma 1.7. *Let G be a group and $\{H_i\}_{i=1}^n$ be a collection of subgroups of G. If*

(i) $G = \prod_{i=1}^n H_i$.

(ii) $H_i \cap \prod_{j \neq i} H_j = 1$ *for all* $1 \leq i \leq n$.

(iii) $H_i \trianglelefteq G$ *for all* $1 \leq i \leq n$.

Then $G \cong \bigotimes_{i=1}^n H_i$.

1.2 Group Actions and Sylow's Theorems

Definition 1.3. *Let G be a group and S be a non-empty set. We say G* ***acts*** *on S if there exists a homomorphism $\phi : G \to Sym(S)$, where*

$$Sym(S) = \{\phi : S \to S : \phi \text{ is a bijection}\}$$

is the group of all permutations of S under composition.

Definition 1.4. *Let G be a group, S be a set, $a \in S$, and suppose that G acts on S. The* ***stabilizer*** *in G of a is*

$$G_a = \{g \in G : a^g = a\},$$

and $G_a \leqslant G$.

Definition 1.5. *Let G be a group, S be a set, and $a \in S$. The* ***orbit*** *of G on S containing a is*

$$aG = \{a^g : g \in G\},$$

and $aG \subseteq S$.

Theorem 1.6 (Orbit-Stabilizer Relation)**.** *Let G be a group, S be a set, and $a \in S$. If G acts on S, then*

$$|aG| = \frac{|G|}{|G_a|} = [G : G_a].$$

Proof.

Let $T = \{G_a g : g \in G\}$ and define $\phi : aG \to T$ by $(a^g)^\phi = G_a g$ for all $a^g \in aG$. To show that ϕ is well-defined, let $a^{g_1}, a^{g_2} \in aG$ such that $a^{g_1} = a^{g_2}$. Then $a^{g_1 g_2^{-1}} = a$ and so $g_1 g_2^{-1} \in G_a$. It follows that $G_a g_1 = G_a g_2$, so $(a^{g_1})^\phi = (a^{g_2})^\phi$ and ϕ is well-defined. If $(a^{g_1})^\phi = (a^{g_2})^\phi$, then $G_a g_1 = G_a g_2$, which implies $g_1 g_2^{-1} \in G_a$. Thus $a^{g_1 g_2^{-1}} = a$, or equivalently, $a^{g_1} = a^{g_2}$. Hence ϕ is injective. To show ϕ is surjective, let $G_a x \in T$. Since $x \in G$, we have $a^x \in aG$ and $(a^x)^\phi = G_a x$. Therefore, ϕ is a bijection and $|aG| = |(aG)^\phi| = |T| = [G : G_a]$. □

Definition 1.6. *A group G acts* ***transitively*** *on a set S if there exists a unique orbit such that $S = aG$ for all $a \in S$. That is, for all $c, d \in S$, there exists $g \in G$ such that $c^g = d$.*

Theorem 1.7. *Let G be a group, S be a set such that G acts on S, and suppose $H \leqslant G$. If H acts transitively on S, then*

$$G = G_a H$$

for all $a \in S$.

Proof.

Let $a \in S$. By hypothesis, $S = aH$ and $G_a H \subseteq G$. Let $g \in G$. Since H acts transitively on S, there exists $h \in H$ such that $a^g = a^h$, hence $a^{gh^{-1}} = a$. It follows that $gh^{-1} \in G_a$ and $g \in G_a H$. Therefore, $G = G_a H$ for all $a \in S$. □

Theorem 1.8 (Class Equation)**.** *Let G be a group. Then*

$$|G| = \sum_{a \notin \mathcal{Z}(G)} [G : C_G(a)] + |\mathcal{Z}(G)|,$$

and the above is called the ***class equation*** *of G.*

Definition 1.7. *Let G be a group, p be a prime, and $n \in \mathbb{N}_0$ be maximal such that p^n divides $|G|$. Then*

(*i*) *The p^{th}***-part** *of G is $|G|_p = p^n$.*

(*ii*) *A subgroup H of G is called a* ***Sylow*** *p-****subgroup*** *of G if $|H| = |G|_p$.*

(*iii*) *The set of all Sylow p-subgroups of G is given by $Syl_p(G)$ (or S_p^G).*

Theorem 1.9 (Sylow)**.** *Let G be a group, p be a prime, and H be a p-subgroup of G. Then*

(*i*) $Syl_p(G) \neq \emptyset$.

(*ii*) *There exists $P \in Syl_p(G)$ such that $H \leqslant P$.*

(*iii*) *G acts transitively on $Syl_p(G)$ by conjugation.*

(*iv*) *Let $n_p(G) = |Syl_p(G)|$. Then $n_p(G)$ divides $|G|$ and $n_p(G) \equiv 1 \pmod{p}$.*

Theorem 1.10 (Fixed Point Theorem for Groups)**.** *Let G be a p-group and S be a set such that $p \nmid |S|$. If G acts on S, then there exists $a \in S$ such that $G_a = G$.*

Theorem 1.11 (Frattini Argument)**.** *Let G be a group, $H \trianglelefteq G$, and $P \in Syl_p(H)$. Then $G = N_G(P)H$.*

Proof.

Let $g \in G$. Since $P \leqslant H$, we have $P^g \leqslant H^g = H$ and in addition, $|P^g| = |P| = |H|_p$. Hence $P^g \in Syl_p(H)$. By Sylow, there exists $h \in H$ such that $P = P^{gh}$. Consequently, $gh \in N_G(P)$, so $g \in N_G(P)H$. Thus $G \leqslant N_G(P)H$ and it follows that $G = N_G(P)H$. □

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

(i) $PN/N \in Syl_p(G/N)$.

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

Proof.

For (i), by Lagrange

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

and so PN/N is a p-group because $P \in Syl_p(G)$. Furthermore,

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

and so $[G/N : PN/N]$ is a p'-number. Thus $|PN/N| = |G/N|_p$ and by Sylow, $PN/N \in Syl_p(G/N)$.

Clearly, $P \cap N$ is a p-group. Now

$$\frac{|N|}{|P \cap N|} = \frac{|PN|}{|P|},$$

which implies $[N : P \cap N]$ is a p'-number. Therefore, $P \cap N \in Syl_p(N)$. □

Theorem 1.12 (General Frattini). *Let G be a group, $P \in Syl_p(G)$, and $N \trianglelefteq G$. Then $G = N_G(P \cap N)N$.*

Proof.

By Lemma 1.8, we have $P \cap N \in Syl_p(N)$. The result then follows from the Frattini Argument. $\square$

Lemma 1.9. *Let G be a nontrivial p-group. Then $\mathcal{Z}(G) \neq 1$.*

Proof.

Suppose $\mathcal{Z}(G) = 1$. Now the class equation of G becomes

$$|G| = \sum_{a \notin \mathcal{Z}(G)} [G : C_G(a)] + 1.$$

If p divides $[G : C_G(a)]$ for each $a \notin \mathcal{Z}(G)$, then p divides $\sum_{a \notin \mathcal{Z}(G)}[G : C_G(a)]$. Since G is a p-group, we have p divides $|G| - \sum_{a \notin \mathcal{Z}(G)}[G : C_G(a)] = 1$. This is a contradiction, so there exists $a^* \notin \mathcal{Z}(G)$ such that $p \nmid [G : C_G(a^*)]$. But $[G : C_G(a^*)]$ must be a p-number. Consequently, $[G : C_G(a^*)] = p^0 = 1$. Thus $G = C_G(a^*)$ and $a^* \in \mathcal{Z}(G)$, which is a contradiction. Therefore, $\mathcal{Z}(G) \neq 1$. $\square$

Definition 1.8. *Let G be a group and $\phi : G \to G$. If ϕ is a bijective homomorphism, then ϕ is called an **automorphism** of G. The set of automorphisms of G is $Aut(G)$ and $Aut(G)$ is a group under the operation of composition.*

Definition 1.9. *Let G and H be groups. Then G **acts** on H if there exists a homomorphism $\phi : G \to Aut(H)$. Also, the commutator of h and g is given by*

$$[h, g] = h^{-1}h^g.$$

The commutator of G and H is given by

$$[H, G] = \langle [h, g] : h \in H \text{ and } g \in G \rangle,$$

and $[H, G] \leqslant H$.

Definition 1.10. *Let G and H be groups such that G acts on H. The* ***centralizer*** *of G on H is*

$$C_H(G) = \{h \in H : h^g = h \text{ for all } g \in G\},$$

and $C_H(G) \leqslant H$.

Lemma 1.10. *Let G and H be p-groups. If G acts on H, then $C_H(G) \neq 1$.*

Proof.

Since G acts on H, we have G acts on $S = H \setminus \{1\} \subset H$. Now G is a p-group and $p \nmid |S|$. By the Fixed Point Theorem for Groups (1.10), there exists a nontrivial $a \in S$ such that $G_a = G$. Therefore, $a \in C_H(G)$ and $C_H(G) \neq 1$. $\square$

1.3 Characteristic Subgroups

Definition 1.11. *Let G be a group and $H \leqslant G$. Then H is a* ***characteristic subgroup*** *of G if $H^\phi \leqslant H$ for all $\phi \in Aut(G)$, and we write H char G.*

Lemma 1.11. *Let G be a group. Then*

(*i*) *$\mathcal{Z}(G)$ char G.*

(*ii*) *G' char G.*

Proof.

Let $\phi \in Aut(G)$. For (i), let $g \in G$ and $z \in \mathcal{Z}(G)$. Since ϕ is surjective, there exists $g_1 \in G$ such that $g_1^\phi = g$. Now we have

$$gz^\phi = g_1^\phi z^\phi = (g_1 z)^\phi = (z g_1)^\phi = z^\phi g_1^\phi = z^\phi g,$$

so $z^\phi \in \mathcal{Z}(G)$. Therefore, $\mathcal{Z}(G)$ char G. For (ii), let $\prod_{i=1}^n [a_i, b_i] \in G'$. We then have

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

where $a_i^\phi, b_i^\phi \in G$. Therefore, G' char G. $\square$

Lemma 1.12. *Let G be a group.*

(i) If H char G, then $H^\phi = H$ for all $\phi \in Aut(G)$.

(ii) If H char G, then $H \trianglelefteq G$.

(iii) If K char $H \trianglelefteq G$, then $K \trianglelefteq G$.

(iv) If $P \in Syl_p(G)$ and $P \trianglelefteq G$, then P char G.

Proof.

For (i), let $\phi \in Aut(G)$. By hypothesis, $H^\phi \leqslant H$, but since ϕ is a bijection, $|H^\phi| = |H|$. It follows that $H^\phi = H$. For (ii), let $g \in G$ and $\phi_g \in Aut(G)$ denote the conjugation automorphism. Since H char G, we have $H^{\phi_g} = H$, but $H^{\phi_g} = H^g$. Therefore, $H \trianglelefteq G$. For (iii), let $g \in G$. Since $H \trianglelefteq G$, we have $H^{\phi_g} = H$, so $\phi_g \in Aut(H)$. Now $K^{\phi_g} = K$ since K char H, hence $K \trianglelefteq G$. For (iv), ϕ is a bijection and so $|P^\phi| = |P|$. Thus $P^\phi \in Syl_p(G)$. By Sylow, there exists $g \in G$ such that $P^g = P^\phi$, but $P \trianglelefteq G$. Therefore, $P = P^\phi$ and P char G. □

Definition 1.12. *A group G is* ***characteristically simple*** *if $\{1\}$ and G are its only characteristic subgroups.*

Theorem 1.13. *Let G be a characteristically simple group. Then $G \cong \bigotimes_{i=1}^n G_i$, where the G_i's are simple isomorphic groups.*

Proof.

Let G_1 be a non-trivial normal subgroup of G such that $|G_1|$ is minimal, and $H = \prod_{i=1}^s G_i$, where $G_i \trianglelefteq G, G_i \cong G_1$, and $G_i \cap \prod_{j \neq i} G_j = 1$ for $1 \leq i \leq s$ with s chosen maximal. We claim H char G. Toward a proof, suppose H is not a characteristic subgroup of G. Now there exists $\phi \in Aut(G)$ and an $1 \leq i \leq s$ such that $G_i^\phi \nleqslant H$. It follows from $H \trianglelefteq G$ and $G_i^\phi \trianglelefteq G$ that $H \cap G_i^\phi \trianglelefteq G$. Moreover, $H \cap G_i^\phi < G_i^\phi$. Thus $|H \cap G_i^\phi| < |G_i^\phi| = |G_i| = |G_1|$. By the minimality of $|G_1|$, we have $H \cap G_i^\phi = 1$, so $H < G_i^\phi \prod_{j=1}^s G_j$. However, this contradicts the maximality of s. Therefore, H char G.

Since $H \leqslant G$ is nontrivial and G is characteristically simple, we have $G = H = \prod_{i=1}^{s} G_i$. By Lemma 1.7, $G \cong \bigotimes_{i=1}^{s} G_i$ and the G_i's are isomorphic by construction. Suppose there exist $1 \leq i < j \leq s$ such that $x \in G_i$ and $y \in G_j$. Then

$$[x, y] \in G_i \cap G_j \leqslant G_i \cap \prod_{j \neq i} G_j = 1,$$

and $xy = yx$. Thus $G_i \leqslant C_G(G_j)$ for all $i \neq j$. Let $1 \leq i \leq s$ and suppose $N \trianglelefteq G_i$. It follows from the above that $N \trianglelefteq G$ and $|N| < |G_i| = |G_1|$. By the minimality of $|G_1|$, either $N = 1$ or $N = G_i$, hence G_i is simple. Therefore, $G \cong \bigotimes_{i=1}^{s} G_i$, where the G_i's are simple isomorphic groups. $\square$

Definition 1.13. *Let p be a prime. A group G is an **elementary abelian p-group** if*

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p.$$

Definition 1.14. *Let G be a group and $H \trianglelefteq G$. If $H \neq 1$ and whenever there exists $K \trianglelefteq G$ such that $K \leqslant H$, either $K = 1$ or $K = H$, then H is a **minimal normal subgroup** of G.*

Theorem 1.14. *Let G be a group and H be a minimal normal subgroup of G. Then either there exist simple non-abelian isomorphic subgroups $\{H_i\}_{i=1}^{n}$ such that $H \cong \bigotimes_{i=1}^{n} H_i$, or there exists a prime p such that H is an elementary abelian p-group.*

Proof.

Suppose K char H. By Lemma 1.12(iii), $K \trianglelefteq G$, so $K = 1$ or $K = H$ by the minimality of H. Thus H is characteristically simple and by Theorem 1.13, $H \cong \bigotimes_{i=1}^{n} H_i$, where the H_i's are simple isomorphic groups. If the H_i's are non-abelian, then we are done. Without loss of generality, assume the H_i's are abelian. Now the only subgroups of H_i are $\{1\}$ and H_i. By Cauchy's Theorem, there exists a prime p such that H_i is a p-group and $H_i \cong \mathbb{Z}_p$. Therefore, $H \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$. $\square$

1.4 Nilpotent Groups

Definition 1.15. *Let G be a group. Define*

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

and inductively,

$$\frac{Z_n(G)}{Z_{n-1}(G)} = \mathcal{Z}\left(\frac{G}{Z_{n-1}(G)}\right),$$

where $Z_i(G)$ represents the preimage of $\mathcal{Z}(G/Z_{i-1}(G))$. The ***upper central series*** *of G is*

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

where $Z_i(G) \trianglelefteq G$ for all $i \in \mathbb{N}_0$.

Definition 1.16. *A group G is* ***nilpotent*** *if there exists $n \in \mathbb{N}_0$ such that $Z_n(G) = G$.*

Lemma 1.13. *Let G be an abelian group. Then G is nilpotent.*

Proof.

Since G is abelian, $G = \mathcal{Z}(G) = Z_1(G)$. Therefore, G is nilpotent. $\square$

Lemma 1.14. *Let G be a nilpotent group, $H \leqslant G$, and $N \trianglelefteq G$. Then*

(*i*) *H is nilpotent.*

(*ii*) *G/N is nilpotent.*

Proof.

For (i), we claim $Z_i(G) \cap H \leqslant Z_i(H)$ for all $i \in \mathbb{N}_0$ and proceed by induction on i. Assume $Z_i(G) \cap H \leqslant Z_i(H)$ and show $Z_{i+1}(G) \cap H \leqslant Z_{i+1}(H)$. Toward this result, let $\overline{G} = G/Z_i(G)$ and $\overline{Z_{i+1}(G) \cap H}$ denote the image of $Z_{i+1}(G) \cap H$ in $\overline{G}$. Now $Z_{i+1}(G) \cap H \leqslant Z_{i+1}(G)$, so $\overline{Z_{i+1}(G) \cap H} \leqslant \mathcal{Z}(\overline{G})$. It follows that $[\overline{H}, \overline{Z_{i+1}(G) \cap H}] = 1$, which implies $[HZ_i(G), (Z_{i+1}(G) \cap H)Z_i(G)] \leqslant Z_i(G)$. Since

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

we have $[H, Z_{i+1}(G) \cap H] \leqslant Z_i(G)$. Hence

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

and

$$1 = \frac{[H, Z_{i+1}(G) \cap H]Z_i(H)}{Z_i(H)} = \left[\frac{H}{Z_i(H)}, \frac{(Z_{i+1}(G) \cap H)Z_i(H)}{Z_i(H)}\right].$$

This implies $(Z_{i+1}(G) \cap H)Z_i(H)/Z_i(H) \leqslant \mathcal{Z}(H/Z_i(H)) = Z_{i+1}(H)/Z_i(H)$, so $Z_{i+1}(G) \cap H \leqslant Z_{i+1}(H)$. Thus the claim holds by induction.

Since G is nilpotent, there exists $n \in \mathbb{N}$ such that $Z_n(G) = G$. By the claim, $Z_n(H) \geqslant H \cap Z_n(G) = H \cap G = H$ and so $Z_n(H) = H$. Therefore, H is nilpotent.

For (ii), let $\overline{G} = G/N$ and $\overline{Z_i(G)}$ denote the image of $Z_i(G)$ in $\overline{G}$. Again using induction, we show $\overline{Z_i(G)} \leqslant Z_i(\overline{G})$ for all $i \in \mathbb{N}_0$. Assume $\overline{Z_i(G)} \leqslant Z_i(\overline{G})$. Since $[G, Z_{i+1}(G)] \leqslant Z_i(G)$, we have $[\overline{G}, \overline{Z_{i+1}(G)}] = \overline{[G, Z_{i+1}(G)]} \leqslant \overline{Z_i(G)} \leqslant Z_i(\overline{G})$. Thus

$$1 = \frac{[\overline{G}, \overline{Z_{i+1}(G)}]Z_i(\overline{G})}{Z_i(\overline{G})} = \left[\frac{\overline{G}}{Z_i(\overline{G})}, \frac{\overline{Z_{i+1}(G)}Z_i(\overline{G})}{Z_i(\overline{G})}\right],$$

which implies

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

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

Since G is nilpotent, there exists $n \in \mathbb{N}$ such that $Z_n(G) = G$. By the claim, $\overline{Z_n(G)} \leqslant Z_n(\overline{G})$, but then $\overline{G} \leqslant Z_n(\overline{G})$. Therefore, $Z_n(\overline{G}) = \overline{G}$ and $\overline{G}$ is nilpotent. □

Lemma 1.15. *Let G be a nilpotent group. Then $\mathcal{Z}(G) \neq 1$.*

Proof.

Suppose $\mathcal{Z}(G) = 1$. By hypothesis, there exists $n \in \mathbb{N}_0$ such that $Z_n(G) = G$. We claim $Z_i(G) = 1$ for all $i \in \mathbb{N}_0$ and proceed by induction. Assume $Z_i(G) = 1$. Now

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

and the claim holds by induction. But this implies $Z_n(G) = 1$, which is a contradiction. Therefore, $\mathcal{Z}(G) \neq 1$. □

Lemma 1.16. *Let G be a nilpotent group and $H < G$. Then $H < N_G(H)$.*

Proof.

Since G is nilpotent, there exists $n \in \mathbb{N}_0$ such that $Z_n(G) = G$. Now $H < G$ implies there exists a maximal $1 \leq i < n$ such that $Z_i(G) \leqslant H$ but $Z_{i+1}(G) \nleqslant H$. By Lemma 1.4, $[G, Z_{i+1}(G)] \leqslant Z_i(G) \leqslant H$, so $[H, Z_{i+1}(G)] \leqslant H$. Thus $Z_{i+1}(G) \leqslant N_G(H)$, but $Z_{i+1}(G) \nleqslant H$. Therefore, $H < N_G(H)$. $\square$

Theorem 1.15. *If G is a p-group, then G is nilpotent.*

Proof.

Toward a contradiction, suppose G is not nilpotent. By hypothesis, $\mathcal{Z}(G) \neq 1$. Now we claim $Z_i(G) < Z_{i+1}(G)$ for all $i \in \mathbb{N}_0$. Proceeding by induction, assume $Z_i(G) < Z_{i+1}(G)$. Since G is not nilpotent, $Z_{i+1}(G) < G$. Let $\overline{G} = G/Z_{i+1}(G)$. Then $\overline{G}$ is a p-group and $1 \neq \mathcal{Z}(\overline{G}) = \overline{Z_{i+2}(G)}$. It follows that $Z_{i+1}(G) < Z_{i+2}(G)$ and the claim holds by induction.

From the claim, we have the series $1 = Z_0(G) < Z_1(G) < Z_2(G) < \cdots$, which contradicts the finite order of G. Therefore, G is nilpotent. $\square$

Lemma 1.17. *Let G be a group and P be a p-subgroup of G. If $P \in Syl_p(N_G(P))$, then $P \in Syl_p(G)$.*

Proof.

To the contrary, suppose $P \in Syl_p(N_G(P))$, but $P \notin Syl_p(G)$. By Sylow, there exists $Q \in Syl_p(G)$ such that $P < Q$. Since Q is a p-group, we have Q is nilpotent by Theorem 1.15. Moreover, $P < N_Q(P)$ by Lemma 1.16. Now $P < N_Q(P) \leqslant N_G(P)$, so $P \in Syl_p(N_Q(P))$. But $N_Q(P) \leqslant Q$ is a p-subgroup, hence $P = N_Q(P)$, which is a contradiction. Therefore, $P \in Syl_p(G)$. $\square$

Lemma 1.18. *Let G be a nilpotent group and H be a nontrivial normal subgroup of G. Then $H \cap \mathcal{Z}(G) \neq 1$.*

Proof.

Since G is nilpotent, there exists $n \in \mathbb{N}_0$ such that $Z_n(G) = G$. Define the series $H_0 = H, H_1 = [H_0, G], H_2 = [H_1, G], \ldots$, and inductively, $H_n = [H_{n-1}, G]$. We claim $H_i \leqslant Z_{n-i}(G)$ for all $i \in \mathbb{N}_0$. Using induction on i, assume $H_i \leqslant Z_{n-i}(G)$ and show $H_{i+1} \leqslant Z_{n-i-1}(G)$. Now $H_{i+1} = [H_i, G] \leqslant [Z_{n-i}(G), G] \leqslant Z_{n-i-1}(G)$, and so the claim holds by induction.

It follows from the claim that $H_n \leqslant Z_{n-n}(G) = Z_0(G) = 1$. Let $m \in \mathbb{N}_0$ be minimal with respect to $H_m = 1$. Then $1 = H_m = [H_{m-1}, G]$ and $H_{m-1} \leqslant \mathcal{Z}(G)$. Since $H \trianglelefteq G$, we know $H_{m-1} \leqslant H$ and by the minimality of m, $H_{m-1} \neq 1$. Therefore, $1 \neq H_{m-1} \leqslant H \cap \mathcal{Z}(G)$. $\square$

Lemma 1.19. *Let G be a group and $H \trianglelefteq G$ such that $H \leqslant Z_i(G)$ for all $i \in \mathbb{N}$. Then $Z_i(G)/H = Z_i(G/H)$ for all $i \in \mathbb{N}_0$.*

Proof.

Let $\overline{G} = G/H$ and use induction on i to show $\overline{Z_i(G)} \leqslant Z_i(\overline{G})$. Assume $\overline{Z_i(G)} \leqslant Z_i(\overline{G})$. By Lemma 1.4, we have $[G, Z_{i+1}(G)] \leqslant Z_i(G)$ and consequently, $[\overline{G}, \overline{Z_{i+1}(G)}] = \overline{[G, Z_{i+1}(G)]} \leqslant \overline{Z_i(G)} \leqslant Z_i(\overline{G})$. By the same reasoning, $\overline{Z_{i+1}(G)}/Z_i(\overline{G}) \leqslant \mathcal{Z}(\overline{G}/Z_i(\overline{G})) = Z_{i+1}(\overline{G})/Z_i(\overline{G})$, so $\overline{Z_{i+1}(G)} \leqslant Z_{i+1}(\overline{G})$. Thus the claim holds by induction.

Again proceeding by induction, we show $Z_i(\overline{G}) \leqslant \overline{Z_i(G)}$ for all $i \in \mathbb{N}_0$. Assume $Z_i(\overline{G}) \leqslant \overline{Z_i(G)}$, it follows, $[\overline{G}, Z_{i+1}(\overline{G})] \leqslant Z_i(\overline{G}) \leqslant \overline{Z_i(G)}$. By Lemma 1.4 and the Third Isomorphism Theorem,

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

Thus $Z_{i+1}(\overline{G}) \leqslant Z_{i+1}(\overline{G})\overline{Z_i(G)} \leqslant \overline{Z_{i+1}(G)}$ and the claim holds by induction. Therefore, $\overline{Z_i(G)} = Z_i(\overline{G})$ for all $i \in \mathbb{N}_0$. $\square$

Lemma 1.20. *Let G be a group, $H \trianglelefteq G, K \trianglelefteq G$, and suppose H and K are nilpotent. Then HK is nilpotent.*

Proof.

Use induction on $|G|$. By hypothesis, HK is a group and $HK \trianglelefteq G$. If $HK < G$, then $H \trianglelefteq HK$ and $K \trianglelefteq HK$. Moreover, H and K are still nilpotent. By induction, HK is nilpotent. Without loss of generality, assume $G = HK$. Since K is nilpotent, we have $\mathcal{Z}(K) \neq 1$ by Lemma 1.15. Let $N = [H, \mathcal{Z}(K)]$.

If $N = 1$, then $\mathcal{Z}(K) \leqslant C_G(HK) = C_G(G) = \mathcal{Z}(G) \trianglelefteq G$. Thus $\mathcal{Z}(G) \neq 1$ and $[G : \mathcal{Z}(G)] < |G|$. Let $\overline{G} = G/\mathcal{Z}(G)$. Now $\overline{H} \trianglelefteq \overline{G}$ and $\overline{K} \trianglelefteq \overline{G}$. By the Second Isomorphism Theorem and Lemma 1.14, we have $\overline{H} \cong H/H \cap \mathcal{Z}(G)$ is nilpotent and $\overline{K} \cong K/K \cap \mathcal{Z}(G)$ is nilpotent. Thus by induction, $\overline{H}\,\overline{K} = \overline{HK} = \overline{G}$ is nilpotent. Then there exists $n \in \mathbb{N}$ such that $Z_n(\overline{G}) = \overline{G}$. By Lemma 1.19, $Z_n(\overline{G}) = \overline{Z_n(G)}$, so $HK = G = Z_n(G) = Z_n(HK)$. Therefore, HK is nilpotent.

Suppose $N \neq 1$. Since $\mathcal{Z}(K)$ char $K \trianglelefteq G$, we have $\mathcal{Z}(K) \trianglelefteq G$ by Lemma 1.12(iii). Also, $\mathcal{Z}(K) \leqslant G = N_G(H)$ because $H \trianglelefteq G$. Hence $1 \neq N = [H, \mathcal{Z}(K)] \trianglelefteq H$. By Lemma 1.18,

$$1 \neq N \cap \mathcal{Z}(H) \leqslant \mathcal{Z}(K) \cap \mathcal{Z}(H) \leqslant C_G(HK) = C_G(G) = \mathcal{Z}(G),$$

thus $\mathcal{Z}(G) \neq 1$. Following the same argument as in the previous case, we have HK is nilpotent. □

Lemma 1.21. *Let G_1 and G_2 be nilpotent groups. Then $G_1 \times G_2$ is nilpotent.*

Proof.

Since G_1 and G_2 are nilpotent, there exist $k, l \in \mathbb{N}_0$ such that $Z_k(G_1) = G_1$ and $Z_l(G_2) = G_2$. Let $n = \max\{k, l\}$. Then $Z_n(G_1) = G_1$ and $Z_n(G_2) = G_2$.

Claim: $Z_i(G_1 \times G_2) = Z_i(G_1) \times Z_i(G_2)$ for all $i \in \mathbb{N}_0$.

Use induction on i. If $i = 0$, then $Z_0(G_1 \times G_2) = (1, 1) = \{1\} \times \{1\} = Z_0(G_1) \times Z_0(G_2)$.

Assume $Z_i(G_1 \times G_2) = Z_i(G_1) \times Z_i(G_2)$. Now by Lemma 1.5 and Lemma 1.6,

$$\begin{aligned}\frac{Z_{i+1}(G_1 \times G_2)}{Z_i(G_1 \times G_2)} &= \mathcal{Z}\left(\frac{G_1 \times G_2}{Z_i(G_1 \times G_2)}\right) = \mathcal{Z}\left(\frac{G_1 \times G_2}{Z_i(G_1) \times Z_i(G_2)}\right) \\ &\cong \mathcal{Z}\left(\frac{G_1}{Z_i(G_1)} \times \frac{G_2}{Z_i(G_2)}\right) = \mathcal{Z}\left(\frac{G_1}{Z_i(G_1)}\right) \times \mathcal{Z}\left(\frac{G_2}{Z_i(G_2)}\right) \\ &= \frac{Z_{i+1}(G_1)}{Z_i(G_1)} \times \frac{Z_{i+1}(G_2)}{Z_i(G_2)} \cong \frac{Z_{i+1}(G_1) \times Z_{i+1}(G_2)}{Z_i(G_1) \times Z_i(G_2)}.\end{aligned}$$

Thus $Z_{i+1}(G_1 \times G_2) = Z_{i+1}(G_1) \times Z_{i+1}(G_2)$ and the claim holds by induction.

From the claim, $Z_n(G_1 \times G_2) = Z_n(G_1) \times Z_n(G_2) = G_1 \times G_2$. Therefore, $G_1 \times G_2$ is nilpotent. □

Definition 1.17. *Let G be a group and $H \leqslant G$. If $H < G$ and whenever there exists $K \leqslant G$ such that $H \leqslant K$, either $K = H$ or $K = G$, then H is a* ***maximal subgroup*** *of G.*

Theorem 1.16. *Let G be a nilpotent group and H be a maximal subgroup of G. Then $H \trianglelefteq G$.*

Proof.

By hypothesis, $H < G$. It follows from Lemma 1.16 that $H < N_G(H) \leqslant G$. Thus $G = N_G(H)$ by the maximality of H. Therefore, $H \trianglelefteq G$. □

Theorem 1.17. *Let G be a nilpotent group. Then $G \cong \bigotimes_{P \in S_p^G} P$ with $p \in \pi(G)$.*

Proof.

Let $P \in Syl_p(G)$. If $P \ntrianglelefteq G$, then $N_G(P) < G$, which implies there exists a maximal subgroup M of G such that $N_G(P) \leqslant M$. By Theorem 1.16, $M \trianglelefteq G$ and since $P < M$, we have $P \in Syl_p(M)$. Now $G = N_G(P)M = M$ by the Frattini Argument, but this contradicts M as a maximal subgroup of G. Thus $P \trianglelefteq G$ and $\prod_{P \in S_p^G} P \leqslant G$, where $p \in \pi(G)$. Moreover, for all $Q \in Syl_q(G)$ with $q \neq p$, we have $P \cap Q = 1$, which implies

$$|\prod_{P \in S_p^G} P| = \prod_{P \in S_p^G} |P| = |G|.$$

Hence $G = \prod_{P \in S_p^G} P$. In addition,

$$P \cap \prod_{Q \in S_q^G} Q = 1$$

for all $q \in \pi(G)$ with $p \neq q$. By Lemma 1.7, $G \cong \bigotimes_{P \in S_p^G} P$, where $p \in \pi(G)$. □

Definition 1.18. *Let G be a group. Define $K_1(G) = G, K_2(G) = [K_1(G), G] = G'$, $K_3(G) = [K_2(G), G], \ldots,$ and inductively, $K_n(G) = [K_{n-1}(G), G]$. The **lower central series** of G is*

$$G = K_1(G) \geqslant K_2(G) \geqslant K_3(G) \geqslant \cdots.$$

Theorem 1.18. *Let G be a group. Then G is nilpotent if and only if there exists $n \in \mathbb{N}$ such that $K_n(G) = 1$.*

Proof.

Suppose G is nilpotent. Then there exists $n \in \mathbb{N}_0$ such that $Z_n(G) = G$.

Claim: $K_i(G) \leqslant Z_{n-i+1}(G)$ for all $1 \leq i \leq n+1$.

Use induction on i. If $i = 1$, then $K_1(G) = G \leqslant G = Z_n(G) = Z_{n-1+1}(G)$. Assume $K_i(G) \leqslant Z_{n-i+1}(G)$ and show $K_{i+1}(G) \leqslant Z_{n-i}(G)$. By Lemma 1.4,

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

and the claim holds by induction. Therefore, $K_{n+1}(G) \leqslant Z_{n-(n+1)+1}(G) = Z_0(G) = 1$ and $K_{n+1}(G) = 1$.

Conversely, suppose there exists $n \in \mathbb{N}$ such that $K_n(G) = 1$.

Claim: $K_{n-i}(G) \leqslant Z_i(G)$ for all $0 \leq i \leq n-1$.

Use induction on i. If $i = 0$, then $K_{n-0}(G) = K_n(G) = \{1\} \leqslant \{1\} = Z_0(G)$. Assume $K_{n-i}(G) \leqslant Z_i(G)$. Since $Z_i(G) \trianglelefteq G$, we have

$$[K_{n-i-1}(G)Z_i(G), G] = [K_{n-i-1}(G), G]Z_i(G) \leqslant K_{n-i}(G)Z_i(G) \leqslant Z_i(G).$$

By Lemma 1.4,

$$\frac{K_{n-i-1}(G)Z_i(G)}{Z_i(G)} \leqslant \mathcal{Z}\left(\frac{G}{Z_i(G)}\right) = \frac{Z_{i+1}(G)}{Z_i(G)},$$

and so $K_{n-i-1}(G) \leqslant K_{n-i-1}(G)Z_i(G) \leqslant Z_{i+1}(G)$. Thus the claim holds by induction. Now $Z_{n-1}(G) \geqslant K_{n-(n-1)}(G) = K_1(G) = G$, but $Z_{n-1}(G) \leqslant G$. Therefore, $Z_{n-1}(G) = G$ and G is nilpotent. □

1.5 Solvable Groups

Definition 1.19. *A group G is **solvable** if there exists a subnormal series*

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

*such that G_i/G_{i+1} is abelian for $0 \leq i \leq n-1$. The quotient groups G_i/G_{i+1} are called **factors** of G.*

Definition 1.20. *Let G be a group. Define $G^{(0)} = G, G^{(1)} = (G^{(0)})' = G'$, $G^{(2)} = (G^{(1)})', \dots,$ and inductively, $G^{(n)} = (G^{(n-1)})'$. The **derived series** of G is*

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

Lemma 1.22. *Let G be a group. Then $G^{(i)} \trianglelefteq G$ for all $i \in \mathbb{N}_0$.*

Proof.

We proceed by induction on i. If $i = 0$, then $G^{(0)} = G \trianglelefteq G$. Assume $G^{(i)} \trianglelefteq G$. Now $G^{(i+1)} = (G^{(i)})'$ char $G^{(i)} \trianglelefteq G$ and $G^{(i+1)} \trianglelefteq G$ by Lemma 1.12(iii). Therefore the result holds by induction. □

Theorem 1.19. *Let G be a group and $H \trianglelefteq G$. Then*

(i) $G' \trianglelefteq G$.

(ii) G/G' is abelian.

(iii) If G/H is abelian, then $G' \leqslant H$.

Proof.

For (i), the result follows because G' char G. For (ii), let $\overline{G} = G/G'$ and $\overline{a}, \overline{b} \in \overline{G}$. Now

$$\overline{a}\overline{b} = \overline{ab} = \overline{baa^{-1}b^{-1}ab} = \overline{ba[a,b]} = \overline{ba} = \overline{b}\overline{a},$$

and it follows that $\overline{G}$ is abelian. For (iii), suppose $\overline{G} = G/H$ is abelian and let $a, b \in G$. Then $\overline{[a,b]} \in \overline{G}$ and

$$\overline{[a,b]} = \overline{a^{-1}b^{-1}ab} = \overline{a^{-1}}\,\overline{b^{-1}}\,\overline{a}\,\overline{b} = \overline{a^{-1}}\,\overline{a}\,\overline{b^{-1}}\,\overline{b} = 1.$$

Thus $[a,b] \in H$ and so $G' \leqslant H$. □

Lemma 1.23. *Let G be a solvable group. Then $G^{(i)} \leqslant G_i$ for all $i \in \mathbb{N}_0$.*

Proof.

Use induction on i. If $i = 0$, then $G^{(0)} = G \leqslant G = G_0$. Assume $G^{(i)} \leqslant G_i$. Now $G^{(i+1)} = (G^{(i)})' \leqslant (G_i)'$, but G_i/G_{i+1} is abelian. By Theorem 1.19, we have $G^{(i+1)} \leqslant (G_i)' \leqslant G_{i+1}$. Therefore the result holds by induction. □

Theorem 1.20. *Let G be a group. Then G is solvable if and only if there exists $n \in \mathbb{N}$ such that $G^{(n)} = 1$.*

Proof.

Suppose there exists $n \in \mathbb{N}$ such that $G^{(n)} = 1$ and consider the derived series

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

By Theorem 1.19, $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$ is abelian for $0 \leq i \leq n-1$. Thus G is solvable. Conversely, suppose G is solvable. Then there exists a subnormal series

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

such that G_i/G_{i+1} is abelian for $0 \leq i \leq n-1$. By Lemma 1.23, $G^{(n)} \leqslant G_n = 1$. □

Lemma 1.24. *Let G be a group, $H \leqslant G$, and $N \trianglelefteq G$. Then $(HN/N)' = H'N/N$.*

Proof.

Let $\overline{G} = G/N$ and $[\overline{h_1n_1}, \overline{h_2n_2}] \in \overline{H}' = (HN/N)'$. Since $N \trianglelefteq G$, $N^h = N$ for all $h \in H$ and

$$\begin{aligned}
[\overline{h_1n_1}, \overline{h_2n_2}] &= \overline{h_1n_1}^{-1}\overline{h_2n_2}^{-1}\overline{h_1n_1}\,\overline{h_2n_2} = \overline{(h_1n_1)^{-1}}\,\overline{(h_2n_2)^{-1}}\,\overline{h_1n_1}\,\overline{h_2n_2} \\
&= \overline{n_1^{-1}h_1^{-1}n_2^{-1}h_2^{-1}h_1n_1h_2n_2} = \overline{h_1^{-1}n_3n_2^{-1}h_2^{-1}h_1h_2n_4n_2} \\
&= \overline{h_1^{-1}h_2^{-1}h_1h_2n_6} = \overline{[h_1, h_2]n_6}.
\end{aligned}$$

Thus $[\overline{h_1n_1}, \overline{h_2n_2}] \in \overline{H'} = H'N/N$ and so $\overline{H}' \leqslant \overline{H'}$. Conversely, let $\overline{[h_1, h_2]n} \in \overline{H'}$. Then

$$\overline{[h_1, h_2]n} = \overline{h_1^{-1}h_2^{-1}h_1h_2n} = \overline{h_1^{-1}h_2^{-1}h_1h_2}\,\overline{n} = \overline{h_1^{-1}h_2^{-1}h_1h_2} = \overline{h_1}^{-1}\overline{h_2}^{-1}\overline{h_1}\,\overline{h_2} = [\overline{h_1}, \overline{h_2}],$$

and so $\overline{[h_1, h_2]n} \in \overline{H}'$. Therefore, $(HN/N)' = H'N/N$. $\square$

Lemma 1.25. *Let G be a solvable group, $H \leqslant G$, and $N \trianglelefteq G$. Then H and G/N are solvable.*

Proof.

By hypothesis, there exists $n \in \mathbb{N}$ such that $G^{(n)} = 1$. We claim $H^{(i)} \leqslant G^{(i)}$ for all $i \in \mathbb{N}_0$ and proceed by induction on i. Assume $H^{(i)} \leqslant G^{(i)}$. Now by the induction hypothesis, $H^{(i+1)} = (H^{(i)})' \leqslant (G^{(i)})' = G^{(i+1)}$. Thus $H^{(i)} \leqslant G^{(i)}$ for all $i \in \mathbb{N}_0$. Therefore, $H^{(n)} \leqslant G^{(n)} = 1$ and H is solvable by Theorem 1.20.

Next, we claim $(G/N)^{(i)} = G^{(i)}N/N$ for all $i \in \mathbb{N}_0$. Using induction on i, if $i = 0$ then $(G/N)^{(0)} = G^{(0)}N/N$. Assume $(G/N)^{(i)} = G^{(i)}N/N$. By Lemma 1.24, we have

$$\left(\frac{G}{N}\right)^{(i+1)} = \left(\left(\frac{G}{N}\right)^{(i)}\right)' = \left(\frac{G^{(i)}N}{N}\right)' = \frac{(G^{(i)})'N}{N} = \frac{G^{(i+1)}N}{N}.$$

Thus $(G/N)^{(i)} = G^{(i)}N/N$ for all $i \in N_0$. It follows that

$$(G/N)^{(n)} = G^{(n)}N/N = \{1\}N/N = N/N = 1.$$

Therefore, G/N is solvable. $\square$

Lemma 1.26. *Let G be a group and $H \trianglelefteq G$. If H and G/H are solvable, then G is solvable.*

Proof.

By hypothesis, there exist $m, n \in \mathbb{N}$ such that $H^{(m)} = 1$ and $(G/H)^{(n)} = 1$. By the claim in Lemma 1.25, $G^{(n)}H/H = (G/H)^{(n)} = 1$, so $G^{(n)} \leqslant H$. Consequently, $G^{(n+m)} = (G^{(n)})^{(m)} \leqslant H^{(m)} = 1$. Therefore, G is solvable. $\square$

Theorem 1.21. *Let G be a group. If G is nilpotent, then G is solvable.*

Proof.

Since G is nilpotent, there exists $n \in \mathbb{N}$ such that

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

is a normal series. Moreover, for $1 \leq i \leq n$,

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

is abelian. Therefore, G is solvable. $\square$

Theorem 1.22. *Let G be a solvable group and H be a minimal normal subgroup of G. Then H is an elementary abelian p-group for some prime p.*

Proof.

By Theorem 1.14, H is an elementary abelian p-group for some prime p or $H \cong \bigotimes_{i=1}^{n} H_i$, where the H_i's are simple non-abelian isomorphic groups. If $H \cong \bigotimes_{i=1}^{n} H_i$, then each H_i is solvable by Lemma 1.25. Now $H_i^{(1)} = H_i' \trianglelefteq H_i$, but H_i is simple and non-abelian, which implies $H_i^{(1)} = H_i$. By an inductive argument, $H_i^{(k)} = (H_i^{(k-1)})' = (H_i)' \trianglelefteq H_i$ and $H_i^{(k)} = H_i$ because H_i is simple. Thus H_i is not solvable and this is a contradiction. Therefore, H is an elementary abelian p-group for some prime p. $\square$

1.6 Semidirect Products

Theorem 1.23. *Let H and K be groups, and suppose that K acts on H via $\phi : K \to Aut(H)$. Set*

$$G = \{(k,h) : k \in K \text{ and } h \in H\},$$

and define the product operation $\cdot$ by

$$(k_1,h_1)\cdot(k_2,h_2) = (k_1k_2, h_1^{k_2^\phi}h_2).$$

Then

(i) $(G,\cdot)$ *is a group.*	*(iv)* $G = H^*K^*$.
(ii) $H^* = \{(1,h) : h \in H\} \cong H$.	*(v)* $H^* \trianglelefteq G$.
(iii) $K^* = \{(k,1) : k \in K\} \cong K$.	*(vi)* $H^* \cap K^* = 1$.

Proof.

For (i), G is closed since $k_2^\phi \in Aut(H)$. Let $(k_i,h_i) \in G$ for $1 \le i \le 3$. Then

$$\begin{aligned}((k_1,h_1)(k_2,h_2))(k_3,h_3) &= (k_1k_2, h_1^{k_2^\phi}h_2)(k_3,h_3) = (k_1k_2k_3, h_1^{(k_2k_3)^\phi}h_2^{k_3^\phi}h_3)\\ &= (k_1,h_1)(k_2k_3, h_2^{k_3^\phi}h_3) = (k_1,h_1)((k_2,h_2)(k_3,h_3)),\end{aligned}$$

so G is associative. Set $(1,1) = (1_K, 1_H)$, where the coordinates are the respective identities of K and H. It follows that $(1,1) \in G$ and $(1,1)$ is the identity of G since $1^\phi \equiv 1 \in Aut(H)$. Furthermore, uniqueness is inherited from K and H. Let $(k,h) \in G$ and consider the element $(k^{-1},(h^{-1})^{(k^{-1})\phi}) \in G$. Now

$$(k,h)(k^{-1},(h^{-1})^{(k^{-1})^\phi}) = (kk^{-1}, h^{(k^{-1})^\phi}(h^{-1})^{(k^{-1})^\phi}) = (kk^{-1},(hh^{-1})^{(k^{-1})^\phi}) = (1,1),$$

and

$$(k^{-1},(h^{-1})^{(k^{-1})^\phi})(k,h) = (k^{-1}k,(h^{-1})^{(k^{-1}k)^\phi}h) = (k^{-1}k,(h^{-1})^{1^\phi}h) = (1,1).$$

Thus $(k,h)^{-1} = (k^{-1},(h^{-1})^{(k^{-1})\phi})$, where uniqueness is inherited. Therefore, G is a group.

For (ii)-(vi): the canonical mapping gives $H^* \cong H$ and $K^* \cong K$. By the definition of G, we have $G = H^*K^*$. Let $(k,1) \in K^*$ and $(1,h) \in H^*$. Now

$$(1,h)^{(k,1)} = (k,1)^{-1}(1,h)(k,1) = (k^{-1},1)(1,h)(k,1) = (k^{-1},h)(k,1) = (1,h^{k^{\phi}}) \in H^*,$$

and so $K^* \leqslant N_G(H^*)$. Moreover, $H^* \leqslant N_G(H^*)$, so $G = H^*K^* \leqslant N_G(H^*)$. Consequently, $G = N_G(H^*)$ and $H^* \trianglelefteq G$. Suppose $(h,k) \in H^* \cap K^*$. By the definition of H^* and K^*, we have $h = 1$ and $k = 1$. Thus $H^* \cap K^* = 1$ and
$|G| = |H^*||K^*| = |H||K|$. $\square$

Definition 1.21. *Let H and K be groups, and suppose that K acts on H via ϕ. The group described in Theorem 1.23 is called the* ***semidirect product*** *of H by K with respect to ϕ and is denoted $H \rtimes_\phi K$.*

2 Representation Theory

In this section, we briefly outline basic concepts from Linear Algebra necessary to understand groups acting over vector spaces. A thorough review of Linear Algebra can be found in [Cur74].

Definition 2.1. *Let F be a field. A* ***vector space*** *V over F is a nonempty set of vectors together with two operations: vector addition, which assigns for each $u, v \in V$, the new vector $v + u \in V$, and scalar multiplication, which assigns for each $\lambda \in F$ and $v \in V$, the new vector $\lambda v \in V$. These operations satisfy the following axioms for all $v, u \in V$ and for all $\alpha, \beta \in F$:*

(i) $(V, +)$ *is an abelian group.*

(ii) $\alpha(u + v) = \alpha u + \alpha v$.

(iii) $(\alpha + \beta)v = \alpha v + \beta v$.

(iv) $(\alpha\beta)u = \alpha(\beta u)$.

(v) $1u = u$.

Definition 2.2. *Let V and W be vector spaces over a field F. A* ***linear transformation*** *of V into W is a function $T : V \to W$ defined by $vT \in W$ for all $v \in V$, such that*

(i) $(v_1 + v_2)T = v_1T + v_2T$ *for all* $v_1, v_2 \in V$.

(ii) $(\alpha v)T = \alpha(vT)$ *for all* $\alpha \in F$ *and for all* $v \in V$.

Theorem 2.1. *Let V and W be vector spaces over a field F, and let $L(V, W)$ denote the set of all linear transformations from V into W. If addition and scalar multiplication are defined as follows, for all $v \in V$:*

(i) $v(S + T) = vS + vT$ *for all* $S, T \in L(V, W)$.

(ii) $v(\alpha T) = \alpha(vT)$ *for all* $T \in L(V, W)$ *and for all* $\alpha \in F$.

Then $L(V, W)$ is a vector space over F.

Definition 2.3. *Let G be a group and V be a vector space over a field F. Then*

(i) $Aut(V,F) = \{T \in L(V,V) : T$ *is nonsingular*$\}$ *is a group under composition.*

(ii) $Aut(V,F) \cong GL_n(F) = \{A \in M_n(F) : \det(A) \neq 0\}$, *where* $M_n(F)$ *is the set of* $n \times n$ *matrices over* F.

(iii) G ***acts*** *on* V *over* F *if there exists a homomorphism* $\phi : G \to Aut(V,F)$ *called a* ***representation*** *of* G *on the vector space* V *over* F.

(iv) G *acts* ***faithfully*** *on* V *over* F *via* ϕ *if* $Ker\ \phi = 1$.

Definition 2.4. *Let G be a group acting on a vector space V over a field F. Then V is called a FG-**module**, or a G-module when F is clear from the context.*

We will use the same notation for the action of a group G on a vector space V over a field F as we use for the action of G on a set:

$$(\alpha u + \beta w)^g = \alpha(u^g) + \beta(w^g)$$

for all $\alpha, \beta \in F$, for all $u, w \in V$, and for all $g \in G$.

Definition 2.5. *Let V be a vector space over a field F and $S \subseteq V$ such that $S \neq \emptyset$. Then S is a **subspace** of V if*

(i) $a + b \in S$ *for all* $a, b \in S$.

(ii) $\lambda a \in S$ *for all* $a \in S$ *and for all* $\lambda \in F$.

For the sake of efficiency, we will invoke the following Lemma in proving a subset of a vector space is a subspace. The proof follows trivially from the definition of a subspace. [Cur74]

Lemma 2.1. *Let V be a vector space over a field F and $S \subseteq V$ be nonempty. Then S is a subspace of V if and only if $\alpha u + \beta w \in S$ for all $\alpha, \beta \in F$ and for all $u, w \in S$.*

Definition 2.6. *Let V be a FG-module and W be a subspace of V. If $w^g \in W$ for all $w \in W$ and for all $g \in G$, then W is a FG-**submodule** of V. In addition, we may call W a G^ϕ-invariant, or a G-invariant subspace of V.*

Theorem 2.2. *Let G be a group acting on a vector space V over a field F. The* ***centralizer*** *of G on V is*

$$C_V(G) = \{v \in V : v^g = v \text{ for all } g \in G\},$$

and $C_V(G)$ is a subspace of V.

Proof.

Let $g \in G$. Since V is a vector space, $0 \in V$ and $0^g = 0$. Thus $0 \in C_V(G)$ and $C_V(G) \neq \emptyset$. Let $u, w \in C_V(G)$ and $\alpha, \beta \in F$. Now

$$(\alpha u + \beta w)^g = \alpha(u^g) + \beta(w^g) = \alpha u + \beta w,$$

so $\alpha u + \beta w \in C_V(G)$. Therefore, $C_V(G)$ is a subspace of V. □

Theorem 2.3. *Let G be a group acting on a vector space V over a field F and suppose $H \trianglelefteq G$. Then $C_V(H)$ is a G-invariant subspace of V.*

Proof.

By Theorem 2.2, $C_V(H)$ is a subspace of V, so $C_V(H) \neq \emptyset$. Let $v \in C_V(H)$, $g \in G$, and $h \in H$. Since $H \trianglelefteq G$, we have $h^{g^{-1}} \in H$. It follows that $v^{h^{g^{-1}}} = v$, or, equivalently, $v^{gh} = v^g$. Thus $v^g \in C_V(H)$ and $C_V(H)$ is G-invariant. □

Definition 2.7. *Let R be a ring. The least positive integer n satisfying $na = 0$ for all $a \in R$ is called the* ***characteristic*** *of R and we write char $R = n$. If no such n exists, we say char $R = 0$.*

Theorem 2.4 (Fixed Point Theorem for Vector Spaces)**.** *Let G be a p-group and suppose that G acts on a vector space V over a field F with char $F = p$. Then $C_V(G) \neq 0$.*

Proof.

Use induction on $|G|$ and let M be a maximal subgroup of G. By Theorem 1.16, $M \trianglelefteq G$, so $[G : M] = p$. Let $y \in G \setminus M$. Now $y^p M = (yM)^p = (yM)^{[G:M]} = 1M$ and so $y^p \in M$. Furthermore, $|M| < |G|$, M is a p-group, and M acts on V over F. By the induction hypothesis, $C_V(M) \neq 0$.

Since $y^p \in M$, we have y^p acts trivially on $C_V(M)$. Thus y satisfies $x^p - 1$ on $C_V(M)$, but $x^p - 1 = (x-1)^p$ since char $F = p$. It follows that 1 is an eigenvalue of y on $C_V(M)$, so there exists a nonzero $w \in C_V(M)$ satisfying $w^y = 1w = w$. Now $M < \langle M, y\rangle \leqslant G$ and $G = \langle M, y\rangle$ by the maximality of M. Thus
$w \in C_V(\langle M, y\rangle) = C_V(G)$ and $C_V(G) \neq 0$. □

2.1 Maschke's Theorem

Definition 2.8. *Let G be a group and p be a prime. Define the unique maximal normal p-subgroup of G by*

$$\mathcal{O}_p(G) = \prod_{P \trianglelefteq G} P,$$

where P is a p-subgroup. Similarly, the unique maximal normal p'-subgroup of G is

$$\mathcal{O}_{p'}(G) = \prod_{P \trianglelefteq G} P,$$

where P is a p'-subgroup.

Definition 2.9. *Let G be a group acting on a vector space V over a field F via ϕ. If $\{0\}$ and V are the only G^ϕ-invariant subspaces (FG-submodules) of V, then G acts irreducibly on V over F via ϕ. We call V an* ***irreducible*** *FG-module.*

Theorem 2.5. *Let G be a group acting faithfully and irreducibly on a vector space V over a field F, and suppose char $F = p$. Then $\mathcal{O}_p(G) = 1$.*

Proof.

Since $\mathcal{O}_p(G)$ is a p-group acting on V, we have $C_V(\mathcal{O}_p(G)) \neq 0$ by the Fixed Point Theorem (2.4). By Theorem 2.3, $C_V(\mathcal{O}_p(G))$ is a G-invariant subspace of V; however, G acts irreducibly on V. Hence $V = C_V(\mathcal{O}_p(G))$ and $\mathcal{O}_p(G)$ acts trivially on V. It follows from the faithful action of G on V that $\mathcal{O}_p(G) = 1$. □

Definition 2.10. *Let V be a vector space over a field F and $\{U_i\}_{i=1}^n$ be subspaces of V. Then V is the* ***direct sum*** *of the U_i's if*

(*i*) $V = U_1 + U_2 + \cdots + U_n$.

(*ii*) $U_i \cap \sum_{j \neq i} U_j = 0$ *for all* $1 \leq i \leq n$.

We denote V as a direct sum of the U_i's by $V = \bigoplus_{i=1}^n U_i$.

Definition 2.11. *A group G acts* ***completely reducibly*** *on a vector space V over a field F if there exist G-invariant subspaces $\{U_i\}_{i=1}^n$ of V such that $V = \bigoplus_{i=1}^n U_i$ and G acts irreducibly on U_i for $1 \leq i \leq n$.*

Lemma 2.2. *Let D be an integral domain. Then there exists a subdomain D' such that*

(*i*) *If char* $D = 0$, *then* $\mathbb{Z} \cong D' \subseteq D$.

(*ii*) *If char* $D = p$ *for some prime* p, *then* $\mathbb{Z}_p \cong D' \subseteq D$.

Proof.

Let $D' = \{m \cdot 1 : m \in \mathbb{Z}\}$, where 1 is unity in D, and $\phi : \mathbb{Z} \to D'$ be defined by $m^\phi = m \cdot 1$. Clearly, ϕ is a surjective ring homomorphism, thus $\mathbb{Z}^\phi = D'$.

For (i), if char $D = 0$, then $m^\phi \neq 0$ for all $m \in \mathbb{Z}^*$. Thus $Ker\ \phi = 0$ and ϕ is injective. By the First Isomorphism Theorem, $\mathbb{Z} \cong \mathbb{Z}/Ker\ \phi \cong \mathbb{Z}^\phi = D' \subseteq D$.

For (ii), if char $D = p$, then $|1| = p$ and $Ker\ \phi = p\mathbb{Z}$. By the First Isomorphism Theorem, $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}^\phi = D' \subseteq D$, but $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$. Therefore, $\mathbb{Z}_p \cong D'$. □

Lemma 2.3. *Let F be a field. Then there exists a subfield F' such that*

(*i*) *If char* $F = 0$, *then* $\mathbb{Q} \cong F' \subseteq F$.

(*ii*) *If char* $F = p$ *for some prime* p, *then* $\mathbb{Z}_p \cong F' \subseteq F$.

Proof.

For (i), since F is an integral domain and char $F = 0$, we have $\mathbb{Z} \cong D' \subseteq F$ by Lemma 2.2. Thus D' is an integral domain in the field F, so F contains a field of quotients $F' \cong \mathbb{Q}$. For (ii), the result follows from Lemma 2.2. □

Theorem 2.6 (Maschke)**.** *Let G be a group acting on a vector space V over a field F and suppose char $F = 0$ or char F is relatively prime to $|G|$. Then G acts completely reducibly on V.*

Proof.

Use induction on $dim_F(V)$. Let $n = |G|$ and char $F = p$. If $p = 0$, then $\mathbb{Q} \subseteq F$ by Lemma 2.3 and so $\frac{1}{n} \in F$. If $p \neq 0$, then $\mathbb{Z}_p \subseteq F$ and it follows from the $\gcd(p, n) = 1$ that $\frac{1}{n} \in F$ is well defined. Thus $n\left(\frac{1}{n}v\right) = \frac{1}{n}(nv) = v$ for all $v \in V$.

Let $0 \neq V_1 \subseteq V$ be a minimal G-invariant subspace. If $V = V_1$, then G acts completely reducibly on V and we are done. Assume $V_1 \subset V$ and let $\mathcal{B} = \{u_i\}_{i=1}^{r} \subseteq V_1$ be a basis for V_1. We may extend $\mathcal{B}$ to a basis for V (Theorem 7.4 in [Cur74]), given by $\{u_i\}_{i=1}^{m}$, and let $W = \text{Span}_F(\{u_i\}_{i=r+1}^{m})$. Clearly, $V = V_1 \oplus W$. Let $\theta : V \to W$ be the projection of V onto W defined by $(v_1 + w)^\theta = w$. Now θ is linear, for if $v_1 + w_1, v_2 + w_2 \in V_1$ then

$$(v_1 + w_1 + v_2 + w_2)^\theta = ((v_1 + v_2) + (w_1 + w_2))^\theta = w_1 + w_2 = (v_1 + w_1)^\theta + (v_2 + w_2)^\theta.$$

Moreover, we claim θ is idempotent−that is, $\theta^2 = \theta$. Let $v_1 + w \in V = V_1 \oplus W$. Then $(v_1 + w)^{\theta^2} = w^\theta = w = (v_1 + w)^\theta$ and $\theta^2 = \theta$.

Let $\psi = \frac{1}{n}\sum_{x \in G} x\theta x^{-1}$. Now ψ is linear since θ is linear and V is a G-module. Let $V_2 = V^\psi$. Then V_2 is a subspace of V since ψ is a linear transformation [Cur74]. Let $y \in G, v \in V$, and for each $x \in G$, set $z_x = y^{-1}x$. As x runs over G, so does z_x, thus

$$v^{\psi y} = \frac{1}{n}\sum_{x \in G} v^{x\theta x^{-1} y} = \frac{1}{n}\sum_{x \in G} v^{y z_x \theta z_x^{-1}} = \frac{1}{n}\sum_{x \in G} v^{y x \theta x^{-1}} = v^{y\psi}.$$

But $(v^y)^\psi \in V_2$ since V is a G-module, hence $V_2 = V^\psi$ is G-invariant.

Let $v_1 \in V_1$ and $x \in G$. Now $v_1^x \in V_1$ since V_1 is G-invariant, so $v_1^{x\theta} = 0$. Thus

$$v_1^\psi = \frac{1}{n}\sum_{x \in G} v_1^{x\theta x^{-1}} = \frac{1}{n}\sum_{x \in G} 0^{x^{-1}} = \frac{1}{n}\sum_{x \in G} 0 = 0,$$

and $V_1^\psi = 0$. Let $v \in V$. Since $(V, +)$ is abelian, we have

$$v - v^\psi = \frac{1}{n}(nv) - \frac{1}{n}\sum_{x \in G} v^{x\theta x^{-1}} = \frac{1}{n}\sum_{x \in G}(v - v^{x\theta x^{-1}}) = \frac{1}{n}\sum_{x \in G}(v^x - v^{x\theta})^{x^{-1}}.$$

Furthermore, $v^x - v^{x\theta} \in V_1$ since θ is the projection of V onto W; $(v^x - v^{x\theta})^{x^{-1}} \in V_1$ since V_1 is G-invariant; and $\frac{1}{n}\sum_{x \in G}(v^x - v^{x\theta})^{x^{-1}} \in V_1$ since V_1 is a vector space over F with $\frac{1}{n} \in F$. Hence $v - v^\psi \in V_1$. Because $V_1^\psi = 0$, we have $(v - v^\psi)^\psi = 0$, but this is equivalent to $v^\psi = v^{\psi^2}$. Thus $\psi = \psi^2$ and ψ is idempotent.

We claim $V = V_1 \oplus V_2$. Let $v \in V$. Now $v = (v - v^\psi) + v^\psi \in V_1 + V_2$ and so $V = V_1 + V_2$. Suppose $u \in V_1 \cap V_2$. Then $u^\psi = 0$ since $V_1^\psi = 0$, but $u \in V_2 = V^\psi$. It follows that there exists $v_0 \in V$ such that $u = v_0^\psi$. This implies $0 = u^\psi = v_0^{\psi^2} = v_0^\psi = u$, so $V_1 \cap V_2 = 0$. Therefore, $V = V_1 \oplus V_2$.

If $V = V_2$, then $V_1 = V_1 \cap V = V_1 \cap V_2 = 0$, which is a contradiction since V_1 is a minimal G-invariant subspace. Hence $V_2 \subset V$ and $dim_F(V_2) < dim_F(V)$. By induction, G acts completely reducibly on V_2, so $V_2 = \bigoplus_{i=1}^s V_{2i}$, where each V_{2i} is an irreducible G-submodule. Now $V = V_1 \oplus V_2 = V_1 \bigoplus_{i=1}^s V_{2i}$, where V_1 is an irreducible G-submodule. Therefore, G acts completely reducibly on V. $\square$

Definition 2.12. *Let G be a group acting on the vector spaces V and W over the field F. Then V and W are* ***isomorphic*** *as G-modules if there exists an isomorphism $\phi : V \to W$ such that $v^{g\phi} = v^{\phi g}$ for all $v \in V$ and for all $g \in G$.*

2.2 Clifford's Theorem

Lemma 2.4. *Let V be a vector space over a field F and S be a subspace of V. The* ***subspace of V generated by S*** *is*

$$\langle S \rangle = \left\{ \textstyle\sum_{i=1}^l m_i s_i : s_i \in S, m_i \in F, 1 \leq i \leq l \textit{ for some } l \in \mathbb{N} \right\}.$$

Proof.

Clearly, $\langle S \rangle \subseteq V$ and $\langle S \rangle \neq \emptyset$. Let $\sum_{i=1}^l m_i s_i, \sum_{j=1}^k r_j t_i \in \langle S \rangle$ and $\alpha, \beta \in F$. Set

$m'_i = \alpha m_i$ for $1 \leq i \leq l$ and $r'_j = \beta r_j$ for $1 \leq j \leq k$. Now

$$\alpha \sum_{i=1}^{l} m_i s_i + \beta \sum_{j=1}^{k} r_j t_i = \sum_{i=1}^{l} \alpha m_i s_i + \sum_{j=1}^{k} \beta r_j t_i = \sum_{i=1}^{l} m'_i s_i + \sum_{j=1}^{k} r'_j t_i \in \langle S \rangle.$$

Therefore, $\langle S \rangle$ is a subspace of V. □

Lemma 2.5. *Let G be a group acting on a vector space V over a field F, $H \trianglelefteq G$, $U \subseteq V$ be an H-submodule, and $W \subseteq V$ be an irreducible H-submodule. Then U/W is an H-submodule.*

Proof.

Let $u + W \in U/W$ and $h \in H$. It follows from U and W being H-submodules, W being irreducible, and $W \neq 0$ that $(u+W)^h = u^h + W^h = u^h + W \in U/W$. Therefore, U/W is an H-submodule. □

Lemma 2.6. *Let G be a group acting on a vector space V over a field F, $H \trianglelefteq G$, and suppose $W \subseteq V$ is an H-submodule. Then W is an irreducible H-submodule if and only if W^g is an irreducible H-submodule for all $g \in G$.*

Proof.

Suppose W is an irreducible H-submodule, and let $g \in G$ and $h \in H$. Now $gh = h^{g^{-1}} g$, where $h^{g^{-1}} \in H$ and for all $w \in W$, we have $w^{gh} = w^{h^{g^{-1}} g} = w_0^g$ for some $w_0 \in W$. Thus W^g is an H-invariant subspace of V. Suppose there exists an H-invariant subspace T of W^g. Now $T^{g^{-1}}$ is an H-invariant subspace of W by the same argument as above, but W is irreducible. Thus $T^{g^{-1}} = 0$ or $T^{g^{-1}} = W$, so $T = 0$ or $T = W^g$. Therefore, W^g is an irreducible H-submodule.

Suppose W^g is an irreducible H-submodule for all $g \in G$. By hypothesis, W is H-invariant. If T is an H-invariant subspace of W, then T^g is an H-invariant subspace of W^g for all $g \in G$. Hence $T^g = 0$ or $T^g = W^g$, but then $T = 0$ or $T = W$. Therefore, W is an irreducible H-submodule. □

Theorem 2.7 (Clifford). *Let G be a group acting irreducibly on a vector space V over a field F and suppose $H \trianglelefteq G$. Then*

(*i*) *$V = \bigoplus_{i=1}^{n} V_i$ such that each V_i is H-invariant, $V_i = \bigoplus_{j=1}^{t_i} X_{ij}$ such that each X_{ij} is an irreducible H-module, and $X_{ij} \cong X_{i'j'}$ (as H-modules) if and only if $i = i'$.*

(*ii*) *Let U be an H-invariant subspace of V. Then $U = \bigoplus_{i=1}^{n} U_i$, where $U_i = U \cap V_i$.*

(*iii*) *t_i is independent of i.*

(*iv*) *G acts transitively on $\{V_i\}_{i=1}^{n}$.*

Proof.

For (*i*), let $W = \bigoplus_{i=1}^{s} W_i$, where $W_i \subset V$ is an irreducible H-module for all $1 \leq i \leq s$ and s is chosen maximal. If W is not G-invariant, there exists an $1 \leq i \leq s$ and $g \in G$ such that $W_i^g \nsubseteq W$, thus $W_i^g \cap W \subset W_i^g$. By Lemma 2.6, W_i^g is an irreducible H-submodule, but $W_i^g \cap W$ is H-invariant, so $W_i^g \cap W = 0$. Hence $W_i^g + W = W_i^g \oplus W = W_i^g \bigoplus_{i=1}^{s} W_i$, which contradicts the maximality of s. Therefore, W is G-invariant and since V is an irreducible G-module, we have $V = W = \bigoplus_{i=1}^{s} W_i$. Now relabel the W_i's as X_{ij}'s such that $X_{ij} \cong X_{i'j'}$ if and only if $i = i'$, and set $V_i = \bigoplus_{j=1}^{t_i} X_{ij}$ for $1 \leq i \leq n$. Then $V = \bigoplus_{i=1}^{n} V_i$, where each V_i is H-invariant and the direct product of irreducible H-modules.

For (*ii*), let U be an H-invariant subspace of V. If $U = V$, then we are done by (*i*). Without loss of generality, assume $U \subset V$. If $W_j \nsubseteq U$, it follows that $U \cap W_j \subset W_j$, but $U \cap W_j$ is H-invariant and W_j is an irreducible H-submodule. Thus $U \cap W_j = 0$ and $U + W_j = U \oplus W_j$. Find all such W_j's and set

$$V^* = U \oplus W_{j_1} \oplus W_{j_2} \oplus \cdots \oplus W_{j_e}. \tag{1}$$

By the construction of V^*, we have $W_j \subseteq V^*$ for all $1 \leq j \leq s$, but $V = \bigoplus_{j=1}^{s} W_j$. Consequently, $V = V^*$.

Let $V' = \bigoplus_{k=1}^{e} W_{j_k}$ and V'' be the direct sum of the remaining W_j's. Now $V = V' \oplus V''$ and by (1), $V = U \oplus V'$. By the Second Isomorphism Theorem,

$$U \cong \frac{U}{\{0\}} = \frac{U}{U \cap V'} \cong \frac{U + V'}{V'} = \frac{V}{V'} = \frac{V' + V''}{V'} \cong \frac{V''}{V' \cap V''} = \frac{V''}{\{0\}} \cong V''.$$

Hence $U \cong V''$ and U is the direct sum of irreducible H-modules. Without loss of generality, assume U is an irreducible H-module. Then it is enough to show there exists an $1 \leq i \leq n$ such that $U \subseteq V_i$.

Suppose $U \nsubseteq V_i$ for all $1 \leq i \leq n$. Now $U \nsubseteq W_j$ for all $1 \leq j \leq s$. Let $W'_m = \bigoplus_{i=1}^{m} W_i$, where $U \nsubseteq W'_m$ and m is chosen maximal. It follows that $U \subseteq W'_{m+1}$. Moreover, $U \cap W'_m \subset U$ and $U \cap W'_m$ is H-invariant. By our assumption, U is an irreducible H-module, so $U \cap W'_m = 0$. Let $\overline{W'_{m+1}} = W'_{m+1}/W'_m$. By the Second Isomorphism Theorem,

$$\overline{U} = \frac{U + W'_m}{W'_m} \cong \frac{U}{U \cap W'_m} = \frac{U}{\{0\}} \cong U.$$

Since U is H-invariant, it follows that $\overline{U}$ is H-invariant. However,

$$\overline{W'_{m+1}} = \frac{W'_{m+1}}{W'_m} = \frac{W'_m + W_{m+1}}{W'_m} \cong \frac{W_{m+1}}{W'_m \cap W_{m+1}} = \frac{W_{m+1}}{\{0\}} \cong W_{m+1},$$

and W_{m+1} is an irreducible H-module. Consequently, $\overline{W'_{m+1}}$ is an irreducible H-module and $\overline{U} \subseteq \overline{W'_{m+1}}$ is H-invariant. Thus $U \cong \overline{U} = \overline{W'_{m+1}} \cong W_{m+1}$.

Suppose $W_{m+1} \subseteq V_i$ for some $1 \leq i \leq n$ and let $\widetilde{V} = V/V_i$. Now $\widetilde{V} = \bigoplus_{j=1}^{r} \widetilde{W_j}$, where

$$\widetilde{W_j} = \frac{W_j + V_i}{V_i} \cong \frac{W_j}{W_j \cap V_i} = \frac{W_j}{\{0\}} \cong W_j,$$

and $\widetilde{W_j}$ is not isomorphic to $W_{m+1} \cong \overline{U} \cong U$. Since $U \nsubseteq V_i$, we have $U \cap V_i \subset U$ and $U \cap V_i$ is H-invariant. Thus $U \cap V_i = 0$ since U is an irreducible H-module and

$$U \cong \frac{U}{\{0\}} = \frac{U}{U \cap V_i} \cong \frac{U + V_i}{V_i} = \widetilde{U}.$$

If $\widetilde{U} \subseteq \widetilde{W_j}$ for some $1 \leq j \leq r$, then $\widetilde{U} = 0$ or $\widetilde{U} = \widetilde{W_j}$ since $\widetilde{U}$ is H-invariant and $\widetilde{W_j} \cong W_j$ is an irreducible H-module. If $\widetilde{U} = 0$, then $U \subseteq V_i$, which is a contradiction.

If $\widetilde{U} = \widetilde{W_j}$, then $\widetilde{W_j} = \widetilde{U} \cong U$, which is also a contradiction. Thus $\widetilde{U} \nsubseteq \widetilde{W_j}$ for all such j. Since $U \nsubseteq V_i$, we have $\widetilde{U} \neq 0$. Repeat the above argument with V and U replaced by $\widetilde{V}$ and $\widetilde{U}$ to result in $\widetilde{U} \cong \widetilde{W_{j^*}}$, where $\widetilde{W_{j^*}} \ncong U$. However, $\widetilde{U} \cong U \cong \widetilde{W_{j^*}}$, which is a contradiction. Hence there exists $1 \leq i \leq n$ such that $U \subseteq V_i$.

For (iv), let $x \in G$, $1 \leq i \leq n$, and $1 \leq j \leq t_i$. By hypothesis, X_{ij} is an irreducible H-module and by Lemma 2.6, X_{ij}^x is an irreducible H-module. From (ii), there exists $1 \leq i' \leq n$ such that $X_{ij}^x \subseteq V_{i'}$. However, $V_{i'} = \bigoplus_{j=1}^{t_{i'}} X_{i'j}$, so there exists $1 \leq j' \leq t_{i'}$ such that $X_{ij}^x \cong X_{i'j'}$. For $1 \leq k \leq t_i$, we have $X_{ij} \cong X_{ik}$ and $X_{ij}^x \cong X_{ik}^x$, but from (i), there exists $1 \leq j'' \leq t_{i'}$ such that $X_{ik}^x \cong X_{i'j''}$. Hence $V_i^x \subseteq V_{i'}$ and $dim_F(V_i^x) \leq dim_F(V_{i'})$. Consider $\langle V_k^g : g \in G\rangle \subseteq V$ for $1 \leq k \leq n$. By Lemma 2.4, $\langle V_k^g : g \in G\rangle$ is a subspace of V and clearly, $\langle V_k^g : g \in G\rangle$ is G-invariant. Since $\langle V_k^g : g \in G\rangle \neq 0$ and G acts irreducibly on V, we have $V = \langle V_k^g : g \in G\rangle$.

By a similar argument in the preceding paragraph, for all $1 \leq l \leq n$, there exists $g \in G$ such that $V_l \subseteq V_k^g$ and $dim_F(V_l) \leq dim_F(V_k^g) = dim_F(V_k)$. By reversing the roles of k and l above, we have $dim_F(V_k) = dim_F(V_l)$. Hence $dim_F(V_i) = dim_F(V_i^x) \leq dim_F(V_{i'}) = dim_F(V_i)$, so $dim_F(V_i^x) = dim_F(V_{i'})$. But $V_i^x \subseteq V_{i'}$ implies $V_i^x = V_{i'}$, thus G acts on V_i for all $1 \leq i \leq n$. Moreover, $V_l \subseteq V_k^{g_1}$ and $V_k \subseteq V_l^{g_2}$ for some $g_1, g_2 \in G$. It follows that $V_l^{g_1^{-1}g_2^{-1}} \subseteq V_k^{g_2^{-1}} \subseteq V_l$, but $g_1^{-1}g_2^{-1}$ is a linear transformation. Hence $dim_F(V_l^{g_1^{-1}g_2^{-1}}) = dim_F(V_l)$, which implies $V_l^{g_1^{-1}g_2^{-1}} = V_k^{g_2^{-1}}$, or equivalently, $V_l^{g_1^{-1}} = V_k$. Therefore, G acts transitively on $\{V_i\}_{i=1}^n$.

For (iii), it follows from $X_{ij}^x \cong X_{i'j'}, dim_F(V_i) = dim_F(V_{i'})$, $V_i^x = V_{i'}$, $V_i^x = \bigoplus_{j=1}^{t_i} X_{ij}^x$, and $V_{i'} = \bigoplus_{j'=1}^{t_{i'}} X_{i'j'}$ that $t_i = t_{i'}$, thus t_i is independent of i. □

Definition 2.13. *The V_i's described in Clifford's Theorem are called **Wedderburn components** of V with respect to H and are denoted by $Wedd_V(H) = \{V_i\}_{i=1}^n$.*

Theorem 2.8. *Let G be a group acting irreducibly on a vector space V over a field F and suppose $z \in \mathcal{Z}(G)$ has an eigenvalue $\lambda \in F$. Then $v^z = \lambda v$ for all $v \in V$. Moreover, if G acts faithfully on V over F, either $z = 1$ or $\lambda \neq 1$.*

Proof.

Let $W = \{v \in V : v^z = \lambda v\}$. Clearly, $W \subseteq V$ is a subspace of V since λ has an associated eigenvector. Let $g \in G$ and $w \in W$. Now $w^{gz} = w^{zg} = (\lambda w)^g = \lambda w^g$, so $w^g \in W$. Thus W is a G-submodule of V. Since G acts irreducibly on V, we have $V = W$.

Suppose G acts faithfully on V over F. If $z \neq 1$ and $\lambda = 1$, then $v^z = \lambda v = v$ for all $v \in V$. Thus z acts trivially on V; however, G acts faithfully on V. Then $z = 1$ and we have a contradiction. Therefore, $z = 1$ or $\lambda \neq 1$. □

Definition 2.14. *Let $n \in \mathbb{N}$. The zeros of $x^n - 1 = 0$ are called the n^{th}* ***roots of unity*** *and they are*

$$\{1, \delta_n, \delta_n^2, \ldots, \delta_n^{n-1}\},$$

where $\delta_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$. We call δ_n^i a ***primitive*** *n^{th}* ***root of unity*** *if*

$$\langle \delta_n^i \rangle = \{1, \delta_n, \delta_n^2, \ldots, \delta_n^{n-1}\}.$$

Definition 2.15. *Let G be a group acting on a vector space V over a field F and $F \subseteq E$ be a field extension. The* ***tensor product*** *of V and E over F is given by*

$$V \otimes_F E = \left\{ \sum_{i=1}^{n} \alpha_i (v_i \otimes e_i) : \alpha_i, e_i \in E \text{ and } v_i \in V \right\}$$

under the following identifications for all $v, v_1, v_2 \in V$, and for all $\alpha, e, e_1, e_2 \in E$:

(i) $v \otimes (e_1 + e_2) = v \otimes e_1 + v \otimes e_2$.

(ii) $(v_1 + v_2) \otimes e = v_1 \otimes e + v_2 \otimes e$.

(iii) $\alpha(v \otimes e) = \alpha v \otimes e = v \otimes \alpha e$.

Moreover, $V \otimes_F E$ is a vector space over E and G acts on $V \otimes_F E$ over E by

$$(v \otimes e)^g = v^g \otimes e,$$

for all $v \in V$, for all $g \in G$, and for all $e \in E$.

Lemma 2.7. $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s} \cong \mathbb{Z}_{n_1 n_2 \cdots n_s}$ *if and only if* $\gcd(n_1, \ldots, n_s) = 1$.

Proof.

Let $Z = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ and suppose $Z \cong \mathbb{Z}_{n_1 n_2 \cdots n_s}$. Now Z is cyclic, hence $(1, 1, \ldots, 1)$ is a generator of Z and $|(1, 1, \ldots, 1)| = \prod_{i=1}^{s} n_i$. Since $\mathbb{Z}_{n_1 n_2 \cdots n_s}$ is a finite cyclic group, we have

$$\prod_{i=1}^{s} n_i = |(1, 1, \ldots, 1)| = lcm(n_1, n_2, \ldots, n_s) = \frac{\prod_{i=1}^{s} n_i}{\gcd(n_1, n_2, \ldots, n_s)}.$$

Thus $\gcd(n_1, n_2, \ldots, n_s) = 1$. Conversely, suppose $\gcd(n_1, n_2, \ldots, n_s) = 1$ and consider $\langle (1, 1, \ldots, 1) \rangle$. Now

$$|\langle (1, 1, \ldots, 1) \rangle| = |(1, 1, \ldots, 1)| = \frac{\prod_{i=1}^{s} n_i}{\gcd(n_1, n_2, \ldots, n_s)} = \prod_{i=1}^{s} n_i = |Z|,$$

thus Z is cyclic. Therefore, Z is isomorphic to $\mathbb{Z}_{n_1 n_2 \cdots n_s}$. □

Lemma 2.8. *Let F be a finite field. Then $F^* = F \setminus \{0\}$ is a cyclic group under multiplication.*

Proof.

Since F is a field, F^* an abelian group. By the Fundamental Theorem of Finite Abelian Groups, $F^* \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$, where the p_i's are prime and $r_i \in \mathbb{N}$ for $1 \leq i \leq k$. By Lemma 2.7, it is enough to show $p_i \neq p_j$ for all $i \neq j$. But this would imply $\gcd(p_1, p_2, \ldots, p_k) = 1$ and it would be enough to show $lcm(p_1^{r_1}, p_2^{r_2}, \ldots, p_k^{r_k}) = \prod_{i=1}^{k} p_i^{r_i}$.

Let $l = lcm(p_1^{r_1}, p_2^{r_2}, \ldots, p_k^{r_k})$ and $\Delta = \prod_{i=1}^{k} p_i^{r_i}$. Since $p_i^{r_i} \big| \Delta$ for all $1 \leq i \leq k$, we have $l \leq \Delta$. Now there exists $t_i \in \mathbb{Z}$ such that $l = p_i^{r_i} t_i$ for each $1 \leq i \leq k$. Set $A_i = \{(1, \ldots, a_i, \ldots, 1) : a_i \in \mathbb{Z}_{p_i^{r_i}}\}$ for each $1 \leq i \leq k$. Now $\bigotimes_{i=1}^{k} \mathbb{Z}_{p_i^{r_i}} = \prod_{i=1}^{k} A_i$. Moreover,

$$(1, \ldots, a_i, \ldots, 1)^{p_i^{r_i}} = (1, \ldots, a_i^{p_i^{r_i}}, \ldots, 1) = (1, \ldots, 1, \ldots, 1)$$

for each $1 \leq i \leq k$. Thus $F^* \cong \bigotimes_{i=1}^{k} \mathbb{Z}_{p_i^{r_i}} = \prod_{i=1}^{k} A_i$, where $a_i \in A_i$ and $a_i^{p_i^{r_i}} = 1$ for all $1 \leq i \leq k$.

Let $f_1 f_2 \cdots f_k \in F^*$, where $f_i \in A_i$ for each $1 \leq i \leq k$, and consider the polynomial $x^l - 1 \in F[x]$. Since $l = p_i^{r_i} t_i$ for $1 \leq i \leq k$, we have

$$(f_1 \cdots f_k)^l - 1 = f_1^l \cdots f_k^l - 1 = f_1^{p_1^{r_1} t_1} \cdots f_k^{p_k^{r_k} t_k} - 1 = 1 \cdots 1 - 1 = 1 - 1 = 0,$$

so $f_1 f_2 \cdots f_k$ is a zero of $x^l - 1$. Thus $|F^*| \leq l$, but $|F^*| = |\bigotimes_{i=1}^k \mathbb{Z}_{p_i^{r_i}}| = \Delta$. Therefore, $l = lcm(p_1^{r_1}, p_2^{r_2}, \ldots, p_k^{r_k}) = \Delta = \prod_{i=1}^k p_i^{r_i}$ and so F^* is isomorphic to the cyclic group $\mathbb{Z}_{p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}}$. □

Theorem 2.9. *Let G be a group acting faithfully and irreducibly on a vector space V over a field F. Then $\mathcal{Z}(G)$ is cyclic.*

Proof.

Case 1: Suppose F contains a primitive $|G|^{th}$ root of unity.

Let $g \in G$. Now g satisfies $x^{|G|} - 1$, so the characteristic polynomial of g divides $x^{|G|} - 1$. Since F contains a primitive $|G|^{th}$ root of unity, it follows that F contains all the eigenvalues of all $g \in G$. Let $z \in \mathcal{Z}(G)$ and $\lambda_z \in F$ be a corresponding eigenvalue of z. Define $\theta : \mathcal{Z}(G) \to F^*$ by $z^\theta = \lambda_z$ for all $z \in \mathcal{Z}(G)$. By Theorem 2.8, $v^z = \lambda_z v$ for all $v \in V$, so θ is well-defined. Let $z_1, z_2 \in \mathcal{Z}(G)$ and $\lambda_{z_1 z_2}$ be an eigenvalue of $z_1 z_2$. Now for all $v \in V$,

$$\lambda_{z_1 z_2} v = v^{z_1 z_2} = (v^{z_1})^{z_2} = (\lambda_{z_1} v)^{z_2} = \lambda_{z_1}(v^{z_2}) = \lambda_{z_1} \lambda_{z_2} v,$$

hence $(z_1 z_2)^\theta = z_1^\theta z_2^\theta$ and θ is a homomorphism. To show injectivity, suppose $z_1^\theta = z_2^\theta$. Then $v^{z_1} = v^{z_2}$ for all $v \in V$, so $v^{z_1 z_2^{-1}} = v$ for all $v \in V$. Thus $z_1 z_2^{-1}$ acts trivially on V; however, G acts faithfully on V and it follows that $z_1 = z_2$. By the First Isomorphism Theorem, $\mathcal{Z}(G) \cong \mathcal{Z}(G)^\theta \leqslant F^*$. Since $\mathcal{Z}(G)^\theta$ is finite, Lemma 2.8 on F implies $\mathcal{Z}(G)^\theta$ is cyclic. Therefore, $\mathcal{Z}(G)$ is cyclic.

Case 2: Suppose F does not contain a primitive $|G|^{th}$ root of unity.

Let ω be a primitive $|G|^{th}$ root of unity, $L = F(\omega)$, and $V_L = V \otimes_F L$. By Definition 2.15, V_L is a vector space over L and G acts on V_L over L by $(v \otimes l)^g = v^g \otimes l$.

Furthermore, L contains a primitive $|G|^{th}$ root of unity. Let $0 \neq W \subseteq V_L$ be a minimal G-invariant subspace, K be the kernel of the action of G on W, and $\overline{G} = G/K$. Now $\overline{G}$ acts irreducibly and faithfully on W over L by the induced map. Since L contains a primitive $|G|^{th}$ root of unity, we have $y^{|G|} = 1$, where y is a primitive root. But $|G| = |\overline{G}| \cdot |K|$ and it follows that $y^{|\overline{G}|} = 1$. Thus L contains a primitive $|\overline{G}|^{th}$ of unity. By Case 1, $\mathcal{Z}(\overline{G})$ is cyclic, so $\overline{\mathcal{Z}(G)}$ is cyclic. Now the Second Isomorphism Theorem implies

$$\overline{\mathcal{Z}(G)} = \frac{\mathcal{Z}(G)K}{K} \cong \frac{\mathcal{Z}(G)}{\mathcal{Z}(G) \cap K},$$

so it is enough to show $\mathcal{Z}(G) \cap K = 1$ to prove $\mathcal{Z}(G)$ is cyclic.

Let $z \in \mathcal{Z}(G) \cap K$. Now z has 1 as an eigenvalue on W and it follows from Theorem 2.8 that z has 1 as an eigenvalue on V_L. However, the characteristic polynomial of z on V_L is the same as the characteristic polynomial of z on V since $(v \otimes l)^g = v^g \otimes l$, hence z has 1 as an eigenvalue on V. By Theorem 2.8, $v^z = 1v = v$ for all $v \in V$, so z acts trivially on V. Thus $z = 1$ since G acts faithfully on V and so $\mathcal{Z}(G) \cap K = 1$. But then $\overline{\mathcal{Z}(G)} \cong \mathcal{Z}(G)$, where $\overline{\mathcal{Z}(G)}$ is cyclic. Therefore, $\mathcal{Z}(G)$ is cyclic. $\square$

Lemma 2.9. *Let G be a group acting irreducibly on a vector space V over a field F and K be the kernel of G on V. If G is abelian, then G/K is cyclic.*

Proof.

Let $\overline{G} = G/K$. Now $\overline{G}$ acts irreducibly and faithfully on V. By Theorem 2.9, $\mathcal{Z}(\overline{G})$ is cyclic. Since G is abelian, we have $\overline{G}$ is abelian, so $\overline{G} = \mathcal{Z}(\overline{G})$ is cyclic. $\square$

Theorem 2.10. *Let G be an abelian group and suppose G acts irreducibly on a vector space V over a field F. If F contains an $|G|^{th}$ root of unity, then $dim_F(V) = 1$.*

Proof.

Let K be the kernel of G on V and $\overline{G} = G/K$. By Lemma 2.9, $\overline{G}$ is cyclic, so $\overline{G} = \langle \overline{x} \rangle$ for some $\overline{x} \in \overline{G}$. Let $g \in G$. Now $\overline{g} \in \overline{G} = \langle \overline{x} \rangle$ and so there exists

$n \in \mathbb{N}_0, (0 \leq n \leq |\overline{G}| - 1)$ such that $\overline{g} = \overline{x}^n = \overline{x^n}$. It follows that $g = x^n k \in \langle x \rangle K$ for some $k \in K$, which implies $G = \langle x \rangle K$.

Let $v_1 \in V$ be a nonzero eigenvector of x and $W = Span_F(v_1)$. Clearly, $0 \neq W \subseteq V$ and W is a subspace of V. Let $g \in G$, $\alpha \in F$, and λ_1 be the corresponding eigenvalue of v_1. Now $(\alpha v_1)^g = (\alpha v_1)^{x^n k} = \alpha (v_1^{x^n})^k = \alpha \lambda_1^n v_1 \in W$ and so W is G-invariant. However, G acts irreducibly on V, which implies $V = W = Span(v_1)$. Therefore, $\{v_1\}$ is a basis for V and $dim_F(V) = 1$. $\square$

Theorem 2.11 (Frobenius, 1901)**.** *Let G be a group and suppose H is a nontrivial subgroup of G such that $H \cap H^g = 1$ for all $g \in G \setminus H$. Then $G = K \rtimes H$, where*

$$K = \left(G \setminus \bigcup_{g \in G} H^g \right) \cup \{1\},$$

$K \trianglelefteq G$, and $C_K(h) = 1$ for all $h \in H \setminus \{1\}$.

Definition 2.16. *Groups satisfying Frobenius' Theorem are called **Frobenius groups** with Frobenius complement H and Frobenius kernel K.*

The only known proof of Frobenius' Theorem involves Character theory and is beyond the scope of this paper. An immediate consequence of Frobenius' Theorem is the following:

Theorem 2.12. *Let G be a Frobenius group with complement H and kernel K. Then*

(*i*) *$G = HK$ with $H \cap K = 1$.*

(*ii*) *$|H| \big| |K| - 1$.*

(*iii*) *Every element of H^* induces by conjugation an automorphism of K which fixes only the identity of K.*

(*iv*) *$C_G(k) \leqslant K$ for all $k \in K \setminus \{1\}$.*

Proof.

See Theorem 7.6, pg. 38 in [Gor07]. $\square$

Theorem 2.13. *Let $G = HA$ be a Frobenius group with kernel H and complement A, H be an elementary abelian q-group, and A be cyclic. Suppose that G acts irreducibly and faithfully on a vector space V over a field F containing a primitive q^{th} root of unity. Then $|Wedd_V(H)| = |A|$.*

Proof.

Let $Wedd_V(H) = \{V_i\}_{i=1}^m$. By Clifford's Theorem (2.7), G acts transitively on $\{V_i\}_{i=1}^m$. Since the V_i's are H-invariant and $G = HA$, we have A acts transitively on $\{V_i\}_{i=1}^m$. Let $V_1 \subseteq \{V_i\}_{i=1}^m$. By Theorem 1.6, $m = |Wedd_V(H)| = [A : A_{V_1}] \leq |A|$.

Suppose $m < |A|$. Let $G_1 = HA_{V_1}, N_1$ be the kernel of G_1 on V_1, and $a_i \in A$, where $V_1^{a_i} = V_i$ for every $1 \leq i \leq m$. Now $N_1^{a_i}$ is the kernel of $G_1^{a_i}$ on $V_1^{a_i}$ for every $1 \leq i \leq m$. Since $A_{V_1} \cap N_1 \leqslant N_1$, we have $(A_{V_1} \cap N_1)^{a_i} \leqslant N_1^{a_i}$, but A is abelian, so $(A_{V_1} \cap N_1)^{a_i} = A_{V_1} \cap N_1$. Hence $A_{V_1} \cap N_1 \leqslant N_1^{a_i}$ for all $1 \leq i \leq m$, which implies $A_{V_1} \cap N_1 \leqslant \bigcap_{i=1}^m N_1^{a_i} = 1$ since G acts faithfully on V. Thus $A_{V_1} \cap N_1 = 1$. Since $N_1 \trianglelefteq G_1$, we have $1 = (A_{V_1} \cap N_1)^g = A_{V_1}^g \cap N_1$ for all $g \in G_1$, but then

$$N_1 \subseteq \left(G_1 \setminus \bigcup_{g \in G_1} A_{V_1}^g \right) \cup \{1\} \subseteq \left(G \setminus \bigcup_{g \in G} A_{V_1}^g \right) \cup \{1\} = H.$$

Let $\overline{G_1} = G_1/N_1 = \overline{H}\ \overline{A_{V_1}}$. Now $\overline{G_1}$ acts faithfully on V_1. By Clifford's Theorem, $V_1 = \bigoplus_{j=1}^{t_1} X_{1j}$, where the X_{1j}'s are irreducible H-modules. By Lemma 2.9, $\overline{H}$ is cyclic because H is abelian. Let $\overline{x} \in \overline{H}$ such that $\overline{H} = \langle \overline{x} \rangle$. Since F contains a primitive q^{th} root of unity, we have $dim_F(X_{1j}) = 1$ by Theorem 2.10 used on $\overline{H}$. Hence $\overline{x}$ acts like a scalar on X_{1j} for each $1 \leq j \leq t_1$, so $\overline{x}$ acts like a scalar on $V_1 = \bigoplus_{j=1}^{t_1} X_{1j}$. Since A_{V_1} fixes V_1, we have $[\overline{x}, \overline{A_{V_1}}]$ acts trivially on V_1. For if $[\overline{x}, \overline{a}] \in [\overline{x}, \overline{A_{V_1}}]$ and $v_1 \in V_1$, then $v_1^{[\overline{x},\overline{a}]} = v_1^{\overline{x}^{-1}\overline{a}^{-1}\overline{x}\ \overline{a}} = \lambda^{-1} v_1^{\overline{a}^{-1}\overline{x}\ \overline{a}} = \lambda^{-1} v_1^{\overline{x}\ \overline{a}} = \lambda^{-1}\lambda v_1^{\overline{a}} = v_1$. However, $\overline{G_1}$ acts faithfully on V_1, so $[\overline{x}, \overline{A_{V_1}}] = 1$. Since $\overline{H} = \langle \overline{x} \rangle$, we have $[\overline{H}, \overline{A_{V_1}}] = 1$ and $[H, A_{V_1}] \leqslant N_1$. It follows from $H \trianglelefteq G$ and A is abelian that $[H, A_{V_1}]^{a_i} = [H, A_{V_1}] \leqslant N_1^{a_i}$ for every $1 \leq i \leq m$. Thus $[H, A_{V_1}] \leqslant \bigcap_{i=1}^m N_1^{a_i} = 1$ and $[H, A_{V_1}] = 1$. Because $G = HA$ is a Frobenius group, we have $C_H(a) = 1$ for all $a \in A \setminus \{1\}$ by Theorem 2.11, but

$[H, A_{V_1}] = 1$. Thus $A_{V_1} = 1$ and so $m = |Wedd_V(H)| = [A : A_{V_1}] = |A|$, which is a contradiction. Therefore, $|Wedd_V(H)| = |A|$. $\square$

Theorem 2.14. *Let $G = PQ$ be a group, Q be a minimal normal elementary abelian q-group, $C_G(Q) = Q$, and suppose $P \cong \mathbb{Z}_p$ for some prime p. If G acts faithfully on a vector space V over a field F with char $F \notin \{p, q\}$, then $C_V(P) \neq 0$.*

Proof.

Case 1: Suppose F contains a primitive q^{th} root of unity.

Let $P = \langle x \rangle$ and use induction on $dim_F(V)$. Since char $F \notin \{p, q\}$, we know either char F is relatively prime with $|G|$ or char $F = 0$. By Maschke's Theorem (2.6), G acts completely reducibly on V. Since G acts faithfully on V, it follows that Q acts faithfully on V. Thus there exists a nontrivial irreducible G-submodule U of V such that Q acts nontrivially on U. Let K be the kernel of G on U. Now $K \trianglelefteq G$ and so $Q \cap K \trianglelefteq G$. Moreover, $Q \cap K < Q$ since Q acts nontrivially on U. Thus $Q \cap K = 1$ by the minimality of Q.

Suppose $k \in K$ is a q-element. By Sylow, there exists $g \in G$ such that $\langle k \rangle \leqslant Q^g$, but $Q^g = Q$. Hence $\langle k \rangle \leqslant Q \cap K = 1$ and K is a p-group. Again by Sylow, there exists $g \in G$ such that $K \leqslant P^g$. But $K \trianglelefteq G$ implies $K = K^{g^{-1}} \leqslant P$, hence $K = 1$ or $K = P$. If $K = P$, then $P \trianglelefteq G$ and $[P, Q] \leqslant P \cap Q = 1$ by coprime orders. But then $P \leqslant C_G(Q) = Q$, which implies $P = 1$. This is a contradiction since $P \cong \mathbb{Z}_p$. Therefore, $K = 1$ and G acts faithfully on U.

If $U \neq V$, then $dim_F(U) < dim_F(V)$, so by the induction hypothesis, $0 \neq C_U(P) \leqslant C_V(P)$. Without loss of generality, assume $U = V$. Then G acts faithfully and irreducibly on $V = U$. Now it follows from $P \cap Q = 1$ and $Q \trianglelefteq G$ that $1 = (P \cap Q)^g = P^g \cap Q$ for all $g \in G$. Hence

$$Q \subseteq \left(G \setminus \bigcup_{g \in G} P^g \right) \cup \{1\}.$$

If $C_Q(x) \neq 1$, then $C_Q(x) \trianglelefteq PQ = G$ since $P = \langle x \rangle$ and Q is abelian, but $C_Q(x) \leqslant Q$. By the minimality of Q, we have $C_Q(x) = Q$. Now $[Q, x] = 1$ and by extension, $[Q, P] = 1$. Thus $P \leqslant C_G(Q) = Q$ and $P = 1$, which is a contradiction. Therefore, $C_Q(x) = 1$.

Clearly, $P \leqslant N_G(P)$. If there exists $n \in N_G(P)$, where n is a q-element, then $[P, n] \leqslant P \cap [P, Q] \leqslant P \cap Q = 1$. Hence $n \in C_Q(P)$, which implies $n \in C_Q(x) = 1$ and $N_G(P)$ is a p-group. Thus $N_G(P) \leqslant P$ and we have $N_G(P) = P$. Let $g \in G \setminus P$. If $P \cap P^g \neq 1$, then $P \cap P^g = P$, so $P \leqslant P^g$. Hence $P = P^g$ and $g \in N_G(P) = P$, which is a contradiction. Thus $P \cap P^g = 1$ and P is a trivial intersection (TI) subgroup. By Frobenius' Theorem (2.11), $\left(G \setminus \bigcup_{g \in G} P^g\right) \cup \{1\} \leqslant G$.

Let $x \in \left(G \setminus \bigcup_{g \in G} P^g\right) \cup \{1\}$ be a p-element. If $x \notin \{1\}$, then $x \in G \setminus \bigcup_{g \in G} P^g$. Now $\langle x \rangle$ is a p-group, so by Sylow, there exists $g \in G$ such that $\langle x \rangle \leqslant P^g$. Then $\langle x \rangle \leqslant \bigcup_{g \in G} P^g$, which is a contradiction. Thus $x = 1$ and $\left(G \setminus \bigcup_{g \in G} P^g\right) \cup \{1\}$ is a q-group. Since $Q \in Syl_q(G)$, we have $\left(G \setminus \bigcup_{g \in G} P^g\right) \cup \{1\} \leqslant Q$ and by Frobenius' Theorem, $\left(G \setminus \bigcup_{g \in G} P^g\right) \cup \{1\} \trianglelefteq G$. It follows from the minimality of Q that

$$Q = \left(G \setminus \bigcup_{g \in G} P^g\right) \cup \{1\}.$$

Thus G is a Frobenius group with kernel Q and complement P.

By Theorem 2.13, $|Wedd_V(Q)| = |P| = p$. Let $Wedd_V(Q) = \{V_i\}_{i=1}^p$. Since the V_i's are Q-invariant and $G = PQ$, we have $P = \langle x \rangle$ acts transitively on $\{V_i\}_{i=1}^p$. Let $V_1^{x^{i-1}} = V_i$ for $1 \leq i \leq p$ and $v_1 \in V_1$ be nonzero. Since $V = \bigoplus_{i=1}^p V_i$, we have $\{v_1^{x^{i-1}}\}_{i=1}^p$ is linearly independent. Thus $v = \sum_{i=1}^p v_1^{x^{i-1}} \neq 0$ and $v^x = \sum_{i=1}^p v_1^{x^i} = v$, so $v \in C_V(P)$. Therefore, $C_V(P) \neq 0$.

Case 2: Suppose F does not contain a primitive q^{th} root of unity.

Let ω be a primitive q^{th} root of unity, $L = F(\omega)$, and $V_L = V \otimes_F L$. Now G acts faithfully on V_L and char $L \notin \{p, q\}$. By Case 1 on V_L over L, we have $C_{V_L}(P) \neq 0$. Therefore, $C_V(P) \neq 0$. $\square$

3 The Transfer Homomorphism

Definition 3.1. *Let G be a group, $H \leqslant G$, $[G : H] = n$, $\{t_i\}_{i=1}^n \subseteq G$ such that $G = \bigcup_{i=1}^n Ht_i$, and suppose $Ht_i = Ht_j$ if and only if $t_i = t_j$. The set $\{t_i\}_{i=1}^n$ is called a **transversal** of H in G. In addition, the set of all transversals of H in G is given by*

$$\mathscr{T} = \{T = \{t_i\}_{i=1}^n \subseteq G : T \text{ is a transversal of } H \text{ in } G\}.$$

Lemma 3.1. *Let G be a group, $H \leqslant G$, $[G : H] = n$, and $\mathscr{T}$ be the set of transversals of H in G. Then G acts on $\mathscr{T}$ by $T^g = \{t_i g\}_{i=1}^n$ for all $g \in G$ and H acts on $\mathscr{T}$ by $T^h = \{ht_i\}_{i=1}^n$ for all $h \in H$.*

Proof.

It is enough to show $\{t_i g\}_{i=1}^n$ and $\{ht_i\}_{i=1}^n$ are indeed transversals of H in G. Let $g \in G$ and $\{t_i\}_{i=1}^n \in \mathscr{T}$. If $Ht_i g = Ht_j g$, then $Ht_i = Ht_j$, but $\{t_i\}_{i=1}^n$ is a transversal of H in G. Thus $t_i = t_j$ and $T^g = \{t_i g\}_{i=1}^n \in \mathscr{T}$. Therefore, G acts on $\mathscr{T}$ by right multiplication.

Let $h \in H$ and $\{t_i\}_{i=1}^n \in \mathscr{T}$. If $Hht_i = Hht_j$, then $Ht_i = Ht_j$, but $t_i = t_j$ since $\{t_i\}_{i=1}^n$ is a transversal of H in G. Therefore, $T^h = \{ht_i\}_{i=1}^n \in \mathscr{T}$ and H acts on $\mathscr{T}$ by left multiplication. □

Definition 3.2. *Let G be a group, $J \trianglelefteq H \leqslant G$, H/J be abelian, $\mathscr{T}$ be the set of transversals of H in G, and suppose $T, U \in \mathscr{T}$. Define the element $T/U \in H/J$ by*

$$T/U = \prod_{i=1}^n Jt_i u_i^{-1}$$

where $T = \{t_i\}_{i=1}^n, U = \{u_i\}_{i=1}^n$, and $t_i u_i^{-1} \in H$ for all $1 \leq i \leq n$.

In Definition 3.2, T/U does not represent a quotient group, but implies an operator on T and U that is denoted T/U.

Theorem 3.1. *Let G be a group, $J \trianglelefteq H \leqslant G$, H/J be abelian, $[G : H] = n$, and $\mathscr{T}$ be the set of transversals of H in G. Then*

(*i*) *$T/T = J$ for all $T \in \mathscr{T}$.*

(*ii*) *$T/U = (U/T)^{-1}$ for all $T, U \in \mathscr{T}$.*

(*iii*) *$T/U = T/V\ V/U$ for all $T, U, V \in \mathscr{T}$.*

Proof.

For (i), let $T \in \mathscr{T}$. The result follows from the definition of T/T.

For (ii), let $T, U \in \mathscr{T}$. Since H/J is abelian, we have

$$T/U = \prod_{i=1}^{n} Jt_i u_i^{-1} = \prod_{i=1}^{n} J(u_i t_i^{-1})^{-1} = \left(\prod_{i=1}^{n} Ju_i t_i^{-1}\right)^{-1} = (U/T)^{-1}.$$

For (iii), let $T, U, V \in \mathscr{T}$. Since H/J is abelian,

$$\begin{aligned} T/U = \prod_{i=1}^{n} Jt_i u_i^{-1} &= \prod_{i=1}^{n} Jt_i v_i^{-1} v_i u_i^{-1} = \prod_{i=1}^{n} Jt_i v_i^{-1} J v_i u_i^{-1} \\ &= \prod_{i=1}^{n} Jt_i v_i^{-1} \prod_{i=1}^{n} J v_i u_i^{-1} = T/V\ V/U. \end{aligned}$$

Therefore, $T/U = T/V\ V/U$. □

Theorem 3.2. *Let G be a group, $J \trianglelefteq H \leqslant G$, H/J be abelian, $[G : H] = n$, $\mathscr{T}$ be the set of transversals of H in G, and suppose $T \in \mathscr{T}$. Define the* ***transfer homomorphism****, $\tau : G \to H/J$ by*

$$g^{\tau} = T^g/T,$$

for all $g \in G$. Then for all $g \in G$, for all $h \in H$, and for all $U \in \mathscr{T}$:

(*i*) *$T^g/U^g = T/U$ and $T^h/U^h = T/U$.*

(*ii*) *τ is independent of T.*

(*iii*) *τ is a homomorphism.*

Proof.

Let $U = \{u_i\}_{i=1}^{n} \in \mathscr{T}$ such that $t_i u_i^{-1} \in H$ for all $1 \leq i \leq n$. For (i), let $g \in G$

and $h \in H$. Now

$$T^g/U^g = \prod_{i=1}^{n} Jt_i g(u_i g)^{-1} = \prod_{i=1}^{n} Jt_i g g^{-1} u_i^{-1} = \prod_{i=1}^{n} Jt_i u_i^{-1} = T/U,$$

and since H/J is abelian,

$$T^h/U^h = \prod_{i=1}^{n} Jht_i(hu_i)^{-1} = \prod_{i=1}^{n} Jht_i u_i^{-1} h^{-1} = \prod_{i=1}^{n} JhJt_i u_i^{-1} Jh^{-1} = \prod_{i=1}^{n} Jt_i u_i^{-1} = T/U.$$

Therefore, $T^g/U^g = T/U$ and $T^h/U^h = T/U$.

For (ii), it follows from Theorem 3.1, part (i), and the abelian property of H/J that

$$\begin{aligned} T^g/T &= T^g/U^g\ U^g/U\ U/T = T/U\ U^g/U\ U/T = U^g/U\ T/U\ U/T \\ &= U^g/U\ T/T = U^g/U\ J \\ &= U^g/U. \end{aligned}$$

Therefore, τ is independent of T.

For (iii), let $x, y \in G$. By Theorem 3.1 and part (i), we have

$$(xy)^\tau = T^{xy}/T = T^{xy}/T^y\ T^y/T = T^x/T\ T^y/T = x^\tau y^\tau.$$

Therefore, τ is a homomorphism. □

Theorem 3.3. *Let G be a group, $J \trianglelefteq H \leqslant G$, H/J be abelian, $[G : H] = n$, $\mathscr{T}$ be the set of transversals of H in G, $T = \{t_i\}_{i=1}^n \in \mathscr{T}$, τ be the transfer of G into H/J, and suppose* $\gcd([G : H], [H : J]) = 1$. *Then $H \cap \mathcal{Z}(G) \cap G' \leqslant J$.*

Proof.

Let $h \in H \cap \mathcal{Z}(G) \cap G'$. By the First Isomorphism Theorem, $G/Ker\ \tau \cong G^\tau \leqslant H/J$, so $G/Ker\ \tau$ is abelian. By Theorem 1.19, $G' \leqslant Ker\ \tau$ and so $h \in Ker\ \tau$. Since $h \in \mathcal{Z}(G)$, we have $J = h^\tau = T^h/T = \prod_{i=1}^n Jt_i h t_i^{-1} = \prod_{i=1}^n Jh = Jh^n$, hence $h^n \in J$. Next $(Jh)^n = Jh^n = J$, so by Lagrange, $|Jh|$ divides $n = [G : H]$ and $|Jh|$ divides $[H : J]$. However, $\gcd([G : H], [H : J]) = 1$, which implies $Jh = J$ and $h \in J$. Therefore, $H \cap \mathcal{Z}(G) \cap G' \leqslant J$. □

Lemma 3.2. *Let G be a group, $J \trianglelefteq H \leqslant G$, H/J be abelian, and $\mathscr{T}$ be the set of transversals of H in G. Define an equivalence relation $\sim$ on $\mathscr{T}$ by $T \sim U$ if and only if $T/U = J$ for all $T, U \in \mathscr{T}$.*

Proof.

Let $T, U \in \mathscr{T}$. Now $T/T = J$ by Theorem 3.1(i) and so $\sim$ is reflexive. If $T \sim U$, then $T/U = J$. By Theorem 3.1(ii), $U/T = (T/U)^{-1} = (J)^{-1} = J$, so $U \sim T$ and $\sim$ is symmetric. Finally, if $V \in \mathscr{T}$ such that $T \sim U$ and $U \sim V$, then by Theorem 3.1(iii), $T/V = T/U\ U/V = J\ J = J$. Hence $T \sim V$ and $\sim$ is transitive. Therefore, $\sim$ is an equivalence relation on $\mathscr{T}$. □

Lemma 3.3. *Let G be a group, $J \trianglelefteq H \leqslant G$, H/J be abelian, and $\mathscr{T}$ be the set of transversals of H in G. Define $\Omega = \{[T] : T \in \mathscr{T}\}$ to be the set of equivalence classes on $\mathscr{T}$ under the relation described in Lemma 3.2. Then*

(i) *G acts on Ω by $[T]^g = [T^g]$ for all $g \in G$.*

(ii) *H acts on Ω by $[T]^h = [T^h]$ for all $h \in H$.*

Proof.

Since G and H already act on $\mathscr{T}$ in the prescribed manner by Lemma 3.1, it is enough to show the action is well-defined. Let $g \in G$ and suppose $[T], [U] \in \Omega$ such that $[T]^g = [U]^g$. This implies $T^g \sim U^g$ if and only if $T^g/U^g = J$, which is to say if and only if $T/U = J$. But this is equivalent to $T \sim U$ if and only if $[T] = [U]$. Thus the action of G on Ω is well-defined.

Similarly, let $h \in H$ and suppose $[T]^h = [U]^h$. By Theorem 3.2, $T^h \sim U^h$ is equivalent to $T^h/U^h = J$ if and only if $T/U = J$, which is to say if and only if $T \sim U$, or, equivalently, $[T] = [U]$. Therefore, the action of H on Ω is well-defined. □

Theorem 3.4. *Let G be a group, $J \trianglelefteq H \leqslant G$, H/J be abelian, $[G : H] = n$, $\mathscr{T}$ be the set of transversals of H in G, and suppose* $\gcd([G : H], [H : J]) = 1$. *Then*

(*i*) *H acts transitively on Ω.*

(*ii*) *$H_{[T]} = J$ for all $T \in \mathscr{T}$.*

Proof.

For (i), let $[T], [U] \in \Omega$. Suppose there exists $h \in H$ such that $[T]^h = [U]$. It would follow that $[T^h] = [U]$ if and only if $T^h \sim U$, or, equivalently, $T^h/U = J$. Thus it is enough to show $T^h/U = J$. In addition,

$$T^h/U = T^h/T\ T/U = \prod_{i=1}^{n} Jht_i t_i^{-1} t_i u_i^{-1} = \prod_{i=1}^{n} Jht_i u_i^{-1} = \prod_{i=1}^{n} JhJt_i u_i^{-1} = Jh^n \left(T/U\right).$$

Let $m = [H : J]$. Since $\gcd(n, m) = 1$, there exist $r, s \in \mathbb{Z}$ such that $rn + sm = -1$. Let $h \in H$ such that $Jh = (T/U)^r$. Then

$$Jh^n \left(T/U\right) = \left(T/U\right)^{rn} \left(T/U\right) = \left(T/U\right)^{rn+1} = \left(T/U\right)^{-sm} = J,$$

and H acts transitively on Ω.

For (ii), let $[T] \in \Omega$ and $j \in J$. Now

$$T^j/T = \prod_{i=1}^{n} Jjt_i t_i^{-1} = \prod_{i=1}^{n} Jj = \prod_{i=1}^{n} J = J,$$

which implies $T^j \sim T$, but this is equivalent to $[T^j] = [T]$. Hence $[T]^j = [T]$ and $J \leqslant H_{[T]}$. Conversely, let $h \in H_{[T]}$. Now $[T]^h = [T]$ implies $T^h/T = J$, but

$$J = T^h/T = \prod_{i=1}^{n} Jht_i t_i^{-1} = \prod_{i=1}^{n} Jh = Jh^n$$

and so $h^n \in J$. Let $\overline{H} = H/J$. Then $1 = \overline{h^n} = \overline{h}^n$, so $|\overline{h}|$ divides $n = [G : H]$. Also, $|\overline{h}|$ divides $[H : J]$, but $\gcd([G : H], [H : J]) = 1$. Thus $\overline{h} = 1$ and $h \in J$. This implies $H_{[T]} \leqslant J$, so $H_{[T]} = J$. $\square$

4 Normal p-Complement Theorems

Definition 4.1. *Let G be a group and $J \trianglelefteq H \leqslant G$. Then*

(i) *G **splits** over H if there exists $K \leqslant G$ such that $G = HK$ and $H \cap K = 1$.*

(ii) *G **splits normally** over H if there exists $K \trianglelefteq G$ such that $G = HK$ and $H \cap K = 1$.*

(iii) *G **splits** over H/J if there exists $K \leqslant G$ such that $G = HK$ and $H \cap K = J$.*

(iv) *G **splits normally** over H/J if there exists $K \trianglelefteq G$ such that $G = HK$ and $H \cap K = J$.*

In (i) and (ii), we call K a **complement** and a **normal complement** of H in G, respectively.

Definition 4.2. *Let G be a group and $P \in Syl_p(G)$. If there exists $K \trianglelefteq G$ such that $G = PK$ and $P \cap K = 1$, then we call K a **normal p-complement**.*

Lemma 4.1. *Let G be a group and $P \in Syl_p(G)$. Then G has a normal p-complement if and only if $G = P\mathcal{O}_{p'}(G)$.*

Proof.

Suppose G has a normal p-complement. Now there exists $K \trianglelefteq G$ such that $G = PK$ and $P \cap K = 1$. In addition,

$$|K| = \frac{|K|}{1} = \frac{|K|}{|P \cap K|} = \frac{|PK|}{|P|} = \frac{|G|}{|P|},$$

and so K is a p'-group. Thus $K \leqslant \mathcal{O}_{p'}(G)$ and $G = PK = P\mathcal{O}_{p'}(G)$. Conversely, suppose $G = P\mathcal{O}_{p'}(G)$. Then $\mathcal{O}_{p'}(G) \trianglelefteq G$ and $P \cap \mathcal{O}_{p'}(G) = 1$ by coprime orders. Therefore, G has a normal p-complement. $\square$

Lemma 4.2. *Let G be a group, $P \in Syl_p(G)$, and $P \leqslant H \leqslant G$. If G has a normal p-complement, then H has a normal p-complement.*

Proof.

By hypothesis, $G = P\mathcal{O}_{p'}(G)$ and $\mathcal{O}_{p'}(G) \cap H \trianglelefteq H$ is a p'-subgroup. Thus $\mathcal{O}_{p'}(G) \cap H \leqslant \mathcal{O}_{p'}(H)$. Now

$$H = H \cap G = H \cap P\mathcal{O}_{p'}(G) = P(H \cap \mathcal{O}_{p'}(G)) \leqslant P\mathcal{O}_{p'}(H) \leqslant H.$$

Therefore, $H = P\mathcal{O}_{p'}(H)$ and H has a normal p-complement. □

Lemma 4.3. *Let G be a group and $N \trianglelefteq G$. If G has a normal p-complement, then G/N has a normal p-complement.*

Proof.

Let $\overline{G} = G/N$ and $P \in Syl_p(G)$. By hypothesis, $G = P\mathcal{O}_{p'}(G)$. Furthermore, $\overline{P} \in Syl_p(\overline{G})$ and $\overline{G} = \overline{P}\,\overline{\mathcal{O}_{p'}(G)}$. Since $\overline{\mathcal{O}_{p'}(G)}$ is a normal p'-group, we have $\overline{\mathcal{O}_{p'}(G)} \leqslant \mathcal{O}_{p'}(\overline{G})$. Thus $\overline{G} = \overline{P}\mathcal{O}_{p'}(\overline{G})$ and $\overline{G}$ has a normal p-complement. □

Lemma 4.4. *Let G be a group and $N \trianglelefteq G$ be a p'-subgroup. If G/N has a normal p-complement, then G has a normal p-complement.*

Proof.

Let $P \in Syl_p(G)$ and $\overline{G} = G/N$. Now $\overline{P} \in Syl_p(\overline{G})$ and $\overline{G} = \overline{P}\mathcal{O}_{p'}(\overline{G})$. Since $\mathcal{O}_{p'}(G) \trianglelefteq G$ is a p'-subgroup, we have $\overline{\mathcal{O}_{p'}(G)} \trianglelefteq \overline{G}$ is a p'-subgroup. Thus $\overline{\mathcal{O}_{p'}(G)} \leqslant \mathcal{O}_{p'}(\overline{G})$. Let $\overline{U} = \mathcal{O}_{p'}(\overline{G})$. We then have $U \trianglelefteq G$ and

$$|U| = \frac{|U|}{|N|} \cdot |N| = |\overline{U}||N|,$$

so U is a p'-group. Hence $U \leqslant \mathcal{O}_{p'}(G)$, which implies $\mathcal{O}_{p'}(\overline{G}) = \overline{U} \leqslant \overline{\mathcal{O}_{p'}(G)}$. It follows that $\overline{\mathcal{O}_{p'}(G)} = \mathcal{O}_{p'}(\overline{G})$ and $\overline{G} = \overline{P}\,\overline{\mathcal{O}_{p'}(G)}$. Consequently, $G = P\mathcal{O}_{p'}(G)N = P\mathcal{O}_{p'}(G)$ and G has a normal p-complement. □

4.1 Burnside's Normal p-Complement Theorem

Since the transfer homomorphism is independent of the transversal chosen, we may choose $T \in \mathscr{T}$ in a special manner. Under the hypothesis of Theorem 3.2, we have

$\langle g \rangle$ acts on $S = \{Hx : x \in G\}$ by right multiplication. Then $S = \bigcup_{i=1}^{s} O_i$, where $O_i = \{Hx_i, Hx_i g, Hx_i g^2, \ldots, Hx_i g^{n_i - 1}\}$, $n_i \in \mathbb{N}$, and $x_i g^{n_i} x_i^{-1} \in H$ for each $1 \le i \le s$. If $T = \{x_i g^r : 1 \le i \le s, 0 \le r \le n_i - 1\}$, then $T^g = \{x_i g^r : 1 \le i \le s, 1 \le r \le n_i\}$ and $g^\tau = T^g/T = \prod_{i=1}^{s} Jx_i g^{n_i}(x_i g^{n_i - 1})^{-1} = \prod_{i=1}^{s} Jx_i g x_i^{-1}$, where $x_i g^{n_i} x_i^{-1} \in H$ for $1 \le i \le s$ and $\sum_{i=1}^{s} n_i = n = [G : H]$.

Theorem 4.1. *Let G be a group, $J \trianglelefteq H \leqslant G$, H/J be abelian, $[G : H] = n$, $\mathscr{T}$ be the set of transversals of H in G, τ be the transfer of G into H/J, and suppose* $\gcd([G : H], [H : J]) = 1$. *Then the following are equivalent:*

(*i*) *G splits normally over H/J.*

(*ii*) *Whenever $h_1, h_2 \in H$ are fused in G, it follows that $Jh_1 = Jh_2$.*

(*iii*) *For all $h \in H, h^\tau = Jh^n$.*

(*iv*) *If $T \in \mathscr{T}$, then H acting on T from the left is equivalent to H acting on T from the right.*

Proof.

Suppose G splits normally over H/J. Now there exists $K \trianglelefteq G$ such that $G = HK$ and $H \cap K = J$. Let $h \in H$ and $g \in G$ such that $h^g \in H$. Since $G = HK$, let $g = h_1 k$. Then $h^g = h^{h_1 k} = (h^{h_1})^k = h_2^k$, where $h_2 = h^{h_1}$. Now $[h_2^{-1}, k] = h_2 (h_2^k)^{-1} \in H$, but simultaneously, $[h_2^{-1}, k] = (k^{-1})^{h_2^{-1}} k \in K$. Thus $[h_2^{-1}, k] \in H \cap K = J$, which implies $Jh_2 = Jh_2^k$. Therefore,

$$Jh^g = Jh^{h_1 k} = Jh_2^k = Jh_2 = Jh^{h_1} = (Jh)^{Jh_1} = Jh,$$

since H/J is abelian.

Suppose whenever $h_1, h_2 \in H$ are fused in G, we have $Jh_1 = Jh_2$. Let $h \in H$ and $s \in \mathbb{N}$ be the number of orbits of $\langle h \rangle$ on $\{hx : x \in G\}$. Thus

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

since $\left((h^{n_i})^{x_i^{-1}}\right)^{x_i} = h^{n_i}$ for $1 \le i \le s$.

Suppose for all $h \in H$, we have $h^\tau = Jh^n$. Let $h \in H$ and $T \in \mathscr{T}$. For the sake of clarity, we will briefly use the traditional notation of actions. From our assumption,

$$\begin{aligned} hT/Th = hT/T\ T/Th = hT/T\,(Th/T)^{-1} &= \prod_{i=1}^{n} Jht_it_i^{-1}\ (h^\tau)^{-1} \\ = \prod_{i=1}^{n} Jh(Jh^n)^{-1} = Jh^n(Jh^n)^{-1} = J. \end{aligned}$$

Therefore, $hT \sim Th$.

Let $T \in \mathscr{T}$. By Theorem 3.4, H acts transitively on Ω from the left. Since $hT \sim Th$ for all $h \in H$, we have H acts transitively on Ω from the right. It follows from Theorem 1.7 that $G = G_{[T]}H$. Moreover, $H \cap G_{[T]} = H_{[T]} = J$ by Theorem 3.4, thus G splits over H/J. Now $g \in G_{[T]}$ if and only if $[T]^g = [T]$, which is to say if and only if $[T]^g = [T]$. This is equivalent to $T^g \sim T$, which is to say if and only if $J = T^g/T = g^\tau$, or, equivalently, $g \in Ker\ \tau$. Hence $G_{[T]} = Ker\ \tau \trianglelefteq G$. Therefore, G splits normally over H/J. □

Theorem 4.2 (Burnside)**.** *Let G be a group, $P \in Syl_p(G)$, and suppose $x, y \in C_G(P)$ such that x and y are fused in G. Then x and y are fused in $N_G(P)$.*

Proof.

By hypothesis, there exists $g \in G$ such that $x^g = y$. Since $x, y \in C_G(P)$, we have $P \leqslant C_G(x) \cap C_G(y)$ and $P^g \leqslant C_G(x)^g = C_G(x^g) = C_G(y)$. Thus $P \leqslant C_G(y)$ and $P^g \leqslant C_G(y)$. It follows that $P, P^g \in Syl_p(C_G(y))$. By Sylow, there exists $c \in C_G(y)$ such that $P^{gc} = P$. But then $gc \in N_G(P)$ and $x^{gc} = y^c = y$. Therefore, x and y are fused in $N_G(P)$. □

Definition 4.3. *Let G be a group and π be a set of primes. Define the following:*

(*i*) *The π^{th}-**part** of G is $|G|_\pi = \prod_{p\in\pi} |G|_p$.*

(*ii*) *H is a **Hall** π-**subgroup** of G if $\pi(H) \subseteq \pi$ and $\pi(G/H) \subseteq \pi'$.*

(*iii*) *$Hall_\pi(G) = \{H \leqslant G : H$ is a Hall π-subgroup$\}$.*

Lemma 4.5. *Let G be a group, $H \in Hall_\pi(G)$, and $N \trianglelefteq G$. Then*

(*i*) $HN/N \in Hall_\pi\left(G/N\right)$.

(*ii*) $H \cap N \in Hall_\pi(N)$.

Proof.

For (i), since $H \cap N \leqslant H \in Hall_\pi(G)$, we have

$$\left|\frac{HN}{N}\right| = \frac{|HN|}{|N|} = \frac{|H||N|}{|H \cap N||N|} = \frac{|H|}{|H \cap N|}.$$

Hence HN/N is a π-group. Since $H \in Hall_\pi(G)$, we have by Lagrange,

$$\frac{|G/N|}{|HN/N|} = \frac{|G|/|N|}{|HN|/|N|} = \frac{|G|}{|HN|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|HN|} = \frac{|G|/|H|}{|HN|/|H|},$$

so $[G/N : HN/N]$ is a π'-number. Therefore, $HN/N \in Hall_\pi\left(G/N\right)$.

For (ii), $H \cap N$ is a π-group because $H \in Hall_\pi(G)$. Moreover,

$$\frac{|N|}{|H \cap N|} = \frac{|HN|}{|H|},$$

and it follows that $[N : H \cap N]$ is a π'-number. Therefore, $H \cap N \in Hall_\pi(N)$. $\square$

Lemma 4.6. *Let G be a group and $H \in Hall_\pi(G)$. If $H \trianglelefteq G$, then H char G.*

Proof.

Let $x \in G$ be a π-element. Since $|Hx|$ divides $|x|$, we have Hx is a π-element. Then $Hx = 1$ since G/H is a π'-group, so $x \in H$. Thus H must contain all π-elements of G. Now let $h \in H$ and $\phi \in Aut(G)$. Since h is a π-element, it follows that h^ϕ is a π-element. By the above, $h^\phi \in H$ and $H^\phi \leqslant H$. Therefore, H char G. $\square$

Theorem 4.3 (Hall)**.** *Let G be a solvable group and π be a set of primes. Then*

(*i*) $Hall_\pi(G) \neq \emptyset$.

(*ii*) *If K is a π-subgroup of G and $M \in Hall_\pi(G)$, there exists $g \in G$ such that $K \leqslant M^g$.*

Proof.

Let G be a counterexample such that $|G|$ is minimal, N be a nontrivial minimal normal subgroup of G, and $\overline{G} = G/N$. It follows from Theorem 1.22 that N is an elementary abelian p-group for some prime p.

Case 1: $p \in \pi$.

Since G is solvable, we have $\overline{G}$ is solvable. By the minimality of $|G|$, there exists $\overline{H} \in Hall_\pi(\overline{G})$. Now

$$|H| = \frac{|H|}{|N|} \cdot |N| = |\overline{H}||N|,$$

so H is a π-group. In addition, $[G:H] = [\overline{G}:\overline{H}]$ and so $[G:H]$ is a π'-number since $\overline{H} \in Hall_\pi(\overline{G})$. Therefore, $H \in Hall_\pi(G)$.

Let $K \leqslant G$ be a π-subgroup and $M \in Hall_\pi(G)$. Clearly, $\overline{K} \leqslant \overline{G}$ is a π-subgroup and by Lemma 4.5, $\overline{M} \in Hall_\pi(\overline{G})$. By the minimality of $|G|$, there exists $\overline{g} \in \overline{G}$ such that $\overline{K} \leqslant \overline{M}^{\overline{g}} = \overline{M^g}$, so $K \leqslant M^gN$. Since $M^g \leqslant M^gN \leqslant G$ and $|M^g| = |M|$, we have $M^g \in Hall_\pi(G)$. By Lemma 4.5, $M^g \cap N \in Hall_\pi(N)$ and

$$\frac{|M^gN|}{|M^g|} = \frac{|N|}{|M^g \cap N|}.$$

However, N is a p-group, thus $[N : M^g \cap N] = 1$ and $M^gN = M^g$. This implies $K \leqslant M^g$, which is a contradiction.

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

Let $\overline{H} \in Hall_\pi(\overline{G})$. If $H < G$, then H is solvable by Lemma 1.25, so by the minimality of $|G|$, there exists $H_1 \in Hall_\pi(H)$. Furthermore, H_1 is a π-group and

$$\frac{|G|}{|H_1|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|H_1|} = \frac{|\overline{G}|}{|\overline{H}|} \cdot \frac{|H|}{|H_1|}.$$

Thus $H_1 \in Hall_\pi(G)$.

Suppose $K \leqslant G$ is a π-subgroup and let $M \in Hall_\pi(G)$. Now $\overline{K}$ is a π-group and $\overline{M} \in Hall_\pi(\overline{G})$ by Lemma 4.5. By the minimality of $|G|$, there exists $\overline{g} \in \overline{G}$ such that $\overline{K} \leqslant \overline{M}^{\overline{g}} = \overline{M^g}$ and $K \leqslant M^gN$. Now $|\overline{M}^{\overline{g}}| = |\overline{M}| = |\overline{H}|$ and so $|M^gN| = |H| < |G|$. Since $K \leqslant M^gN$ and $M^g \in Hall_\pi(M^gN)$, we have from the minimality of $|G|$ that there exists $g_1 \in M^gN$ such that $K \leqslant M^{gg_1}$. However, this is a contradiction.

If $G = H$, then $\overline{G} = \overline{H}$ and $\overline{G}$ is a π-group. Let $1 \neq \overline{R}$ be a minimal normal subgroup of $\overline{G}$. By Theorem 1.22, $\overline{R}$ is an elementary abelian q-group for some $q \in \pi$. Then $R \trianglelefteq G$ and R is a pq-group. Let $Q \in Syl_q(R)$. By Lemma 1.8, $\overline{Q} \in Syl_q(\overline{R})$, but $\overline{R}$ is a q-group. Thus $\overline{Q} = \overline{R}$ and $R = QN$. By the Frattini Argument, $G = N_G(Q)R = N_G(Q)QN = N_G(Q)N$. Since G has no normal π-subgroups, $N_G(Q) < G$. Now $N_G(Q)$ is solvable, so there exists $N_1 \in Hall_\pi(N_G(Q))$ by the minimality of $|G|$. Also, N_1 is a π-group and

$$\frac{|G|}{|N_1|} = \frac{|G|}{|N_G(Q)|} \cdot \frac{|N_G(Q)|}{|N_1|} = \frac{|N_G(Q)N|}{|N_G(Q)|} \cdot \frac{|N_G(Q)|}{|N_1|} = \frac{|N|}{|N \cap N_G(Q)|} \cdot \frac{|N_G(Q)|}{|N_1|}.$$

Thus $N_1 \in Hall_\pi(G)$ and $Hall_\pi(G) \neq \emptyset$.

Let $K \leqslant G$ be a π-subgroup and $M \in Hall_\pi(G)$. Now $\overline{M} \in Hall_\pi(\overline{G})$, $|\overline{M}| = |\overline{H}| = |\overline{G}|$, and $G = MN$. Suppose $|K| = |M|$. Since $R \trianglelefteq G$, we have $K \cap R, M \cap R \in Syl_q(R)$ by Lemma 1.8. By Sylow, there exists $r \in R$ such that $K \cap R = (M \cap R)^r = M^r \cap R^r = M^r \cap R$. Also, $K \leqslant N_G(K \cap R) = N_G(M^r \cap R) = N_2$ and $M^r \leqslant N_G(M^r \cap R) = N_2$. Now $K \leqslant N_2$ is a π-subgroup, $M^r \in Hall_\pi(N_2)$ since $|M^r| = |M|$, and $N_2 < G$ since G has no normal π-subgroups. By the minimality of $|G|$, there exists $n \in N_2$ such that $K \leqslant M^{rn}$, which is a contradiction.

If $|K| < |M|$, then $K \cap N \leqslant M \cap N = 1$ by coprime orders. This implies $|KN| < |MN| = |G|$. Furthermore, $K \leqslant KN$ is a π-subgroup and KN is solvable. In addition, $M \cap KN \leq M$ is a π-subgroup and

$$\frac{|KN|}{|M \cap KN|} = \frac{|KNM|}{|M|} = \frac{|KG|}{|M|} = \frac{|G|}{|M|},$$

hence $M \cap KN \in Hall_\pi(KN)$. By the minimality of $|G|$, there exists $g_2 \in KN$ such that $K \leqslant (M \cap KN)^{g_2} \leqslant M^{g_2}$, which is a contradiction. Therefore, no such counterexample G exists. $\square$

Theorem 4.4. *Let G be a group and $A \in Hall_\pi(G)$ such that A is abelian. Then G splits normally over A if and only if whenever $a_1, a_2 \in A$ such that a_1 and a_2 are fused in G, it follows that $a_1 = a_2$.*

Proof.

Now $\{1\} \trianglelefteq A \leqslant G$ and $A/\{1\} \cong A$ is abelian. Since $A \in Hall_\pi(G)$, we have $\gcd([G : A], [A : \{1\}]) = 1$. By Theorem 4.1, G splits normally over A if and only if G splits normally over $A/\{1\}$, which is to say, whenever $a_1, a_2 \in A$ such that a_1 and a_2 are fused in G, it follows that $\{1\}a_1 = \{1\}a_2$, or, equivalently, $a_1 = a_2$. □

Theorem 4.5 (Burnside's Normal p-Complement Theorem)**.** *Let G be a group and $P \in Syl_p(G)$ such that $P \leqslant \mathcal{Z}(N_G(P))$. Then G has a normal p-complement.*

Proof.

Since $P \leqslant \mathcal{Z}(N_G(P))$, we know P is abelian and $P \in Hall_\pi(G)$, where $\pi = \{p\}$. By Theorem 4.4, it is enough to show whenever $a_1, a_2 \in P$ such that $a_1 \sim_G a_2$, it follows that $a_1 = a_2$. Let $x, y \in P$ such that $x \sim_G y$. Now $x, y \in C_G(P)$, so by Burnside's Theorem (4.2), there exists $n \in N_G(P)$ such that $x = y^n$. But $y \in P \leqslant \mathcal{Z}(N_G(P))$, so $x = y^n = y$. Therefore, G has a normal p-complement. □

Theorem 4.6. *Let G be a group, $A \in Hall_\pi(G)$ such that A is abelian and $A \trianglelefteq G$. Then G splits over A and G acts transitively on the complements of A in G.*

Proof.

Now $\{1\} \trianglelefteq A \leqslant G$ and $A/\{1\} \cong A$ is abelian. Since $A \in Hall_\pi(G)$, we have $\gcd([G : A], [A : \{1\}]) = 1$. Also, G acts on Ω from the left since $A \trianglelefteq G$. By Theorem 3.4, A acts transitively on $\Omega = \{[T] : T \in \mathscr{T}\}$, so $G = G_{[T]}A$ by Theorem 1.7. In addition, $A \cap G_{[T]} = A_{[T]} = 1$ by Theorem 3.4. Thus G splits over A.

Suppose there exists $K \leqslant G$ such that $G = AK$ and $A \cap K = 1$. We want to show K is conjugate to $G_{[T]}$. By the Second Isomorphism Theorem, we have

$$|K| = \frac{|K|}{1} = \frac{|K|}{|A \cap K|} = \frac{|AK|}{|A|} = \frac{|G|}{|A|}. \tag{2}$$

If there exist $k_1, k_2 \in K$ such that $Ak_1 = Ak_2$, then $k_1k_2^{-1} \in A \cap K = 1$ and $k_1 = k_2$. Thus $K \in \mathscr{T}$ and $[K] \in \Omega$. Since A acts transitively on Ω, there exists $a \in A$ such that $[T]^a = [K]$. It follows from $K \leqslant G_{[K]}$ that $K^{a^{-1}} \leqslant G_{[K]}^{a^{-1}} = G_{[K]^{a^{-1}}} = G_{[T]}$, and by (2),

$$|K| = |K^{a^{-1}}| \leq |G_{[T]}| = \frac{|G_{[T]}|}{|A \cap G_{[T]}|} = \frac{|AG_{[T]}|}{|A|} = \frac{|G|}{|A|} = |K|.$$

Thus $|K^{a^{-1}}| = |G_{[T]}|$, so $K^{a^{-1}} = G_{[T]}$. Therefore, K and $G_{[T]}$ are conjugate. $\square$

Theorem 4.7 (Schur-Zassenhaus Part 1). *Let G be a group and $H \in Hall_\pi(G)$. If $H \trianglelefteq G$, then G splits over H.*

Proof.

Use induction on $|G|$ and let $P \in Syl_p(H)$. By the Frattini Argument, $G = N_G(P)H$. Let $N = N_G(P)$ and suppose $N < G$. It then follows $H \cap N \trianglelefteq N$, $H \cap N$ is a π-group, and

$$\frac{|N|}{|H \cap N|} = \frac{|NH|}{|H|} = \frac{|G|}{|H|}.$$

Thus $H \cap N \in Hall_\pi(N)$. By the induction hypothesis, N splits over $H \cap N$, so there exists $K \leqslant N$ such that $N = K(H \cap N)$ and $K \cap (H \cap N) = 1$. Moreover, $G = NH = K(H \cap N)H = KH$ and $K \cap H \leqslant K \cap H \cap N = 1$. Therefore, G splits over H.

If $N = N_G(P) = G$, then $P \trianglelefteq G$. Now $\mathcal{Z}(P)$ char $P \trianglelefteq G$, so $\mathcal{Z}(P) \trianglelefteq G$ by Lemma 1.12. Since P is a p-group, we have $\mathcal{Z}(P) \neq 1$ by Lemma 1.9. Let $\overline{G} = G/\mathcal{Z}(P)$. Now $\overline{H} \in Hall_\pi(\overline{G})$ by Lemma 4.5, and $\overline{H} \trianglelefteq \overline{G}$. Since $|\overline{G}| < |G|$, we have $\overline{G}$ splits over $\overline{H}$ by induction. Then there exists $\overline{K} \leqslant \overline{G}$ such that $\overline{G} = \overline{K}\,\overline{H}$ and $\overline{K} \cap \overline{H} = 1$. Consequently, $G = KH\mathcal{Z}(P) = K\mathcal{Z}(P)H = KH$ and $K \cap H \leqslant \mathcal{Z}(P)$. Now by the Second Isomorphism Theorem,

$$|\overline{K}| = \frac{|\overline{K}|}{|\overline{H} \cap \overline{K}|} = \frac{|\overline{H}\,\overline{K}|}{|\overline{H}|} = \frac{|\overline{G}|}{|\overline{H}|},$$

so $\overline{K}$ is a π'-group; however, $\mathcal{Z}(P)$ is a π-group. Hence $\mathcal{Z}(P) \in Hall_\pi(K)$ and $\mathcal{Z}(P) \leqslant P \leqslant H$. Moreover, $\mathcal{Z}(P) \trianglelefteq K$ and $\mathcal{Z}(P)$ is abelian. By Theorem 4.6, K splits over $\mathcal{Z}(P)$, which implies there exists $K_0 \leqslant K$ such that $K = K_0\mathcal{Z}(P)$ and

$K_0 \cap \mathcal{Z}(P) = 1$. Thus $G = HK = HK_0\mathcal{Z}(P) = HK_0$ and

$$H \cap K_0 \leqslant K \cap H \cap K_0 \leqslant \mathcal{Z}(P) \cap K_0 = 1.$$

Therefore, G splits over H. $\square$

Theorem 4.8 (Schur-Zassenhaus Part 2)**.** *Let G be a group, $H \in Hall_\pi(G)$, $H \trianglelefteq G$, and suppose either H is solvable or G/H is solvable. Then G splits over H and G acts transitively on the complements of H in G.*

Proof.

Use induction on $|G|$. By Schur-Zassenhaus Part 1, G splits over H. Suppose $K_1 \leqslant G$ and $K_2 \leqslant G$, where $G = HK_i$ and $H \cap K_i = 1$ for $1 \leq i \leq 2$.

Case 1: Suppose H is solvable.

Since H' char $H \trianglelefteq G$, it follows from Lemma 1.12 that $H' \trianglelefteq G$. If $H' = 1$, then H is abelian and the result follows from Theorem 4.6. Without loss of generality, assume $H' \neq 1$ and let $\overline{G} = G/H'$. Now $\overline{G} = \overline{H}\,\overline{K_i}$, $\overline{H} \cap \overline{K_i} = 1$ for $1 \leq i \leq 2$, $\overline{H} \trianglelefteq \overline{G}$, and by Lemma 4.5, $\overline{H} \in Hall_\pi(\overline{G})$.

By the induction hypothesis, there exists $\overline{g} \in \overline{G}$ such that $\overline{K_2} = \overline{K_1}^{\overline{g}} = \overline{K_1^g}$, so $K_1^g H' = K_2 H'$. Since H is solvable, we have $H' < H$ and so $K_2H' < K_2H = G$. Furthermore, $K_2 \cap H' \leqslant K_2 \cap H = 1$ and

$$K_1^g \cap H' = K_1^g \cap H'^g = (K_1 \cap H')^g \leqslant (K_1 \cap H)^g = 1.$$

Now $H' \trianglelefteq K_2H'$ and H' is a π-group. Moreover, since $H \in Hall_\pi(G)$ and

$$\frac{|K_2H'|}{|H'|} = \frac{|K_2|}{|K_2 \cap H'|} = |K_2| = \frac{|K_2|}{|H \cap K_2|} = \frac{|K_2H|}{|H|} = \frac{|G|}{|H|},$$

we have $H' \in Hall_\pi(K_2H')$. By induction, there exists $g_1 \in K_2H'$ such that $K_1^{gg_1} = K_2$. Therefore, G acts transitively on the complements of H.

Case 2: Suppose G/H is solvable.

Let R/H be a minimal normal subgroup of G/H. Since G/H is solvable, we have R/H is an elementary abelian p-group by Theorem 1.22. Now

$$|R| = \frac{|R|}{|H|} \cdot |H|,$$

so R is a $p\pi$-group. Since $H \in Hall_\pi(G)$, we have G/H is a π'-group, which implies $p \notin \pi$. In addition, for $1 \leq i \leq 2$,

$$|K_i| = \frac{|K_i|}{|H \cap K_i|} = \frac{|HK_i|}{|H|} = \frac{|G|}{|H|}$$

and so K_1 and K_2 are π'-groups. By Lemma 1.8, $K_1 \cap R, K_2 \cap R \in Syl_p(R)$ and from Sylow, there exists $r \in R$ such that $K_2 \cap R = (K_1 \cap R)^r = K_1^r \cap R$. Since $R \trianglelefteq G$, it follows that $K_1^r \cap R \trianglelefteq K_1^r$ and $K_2 \cap R \trianglelefteq K_2$. Thus $K_1^r \leqslant N_G(K_1^r \cap R) = N_G(K_2 \cap R)$ and $K_2 \leqslant N_G(K_2 \cap R)$.

Let $N = N_G(K_2 \cap R)$ and $\overline{N} = N/K_2 \cap R$. By Lemma 1.2,

$$\overline{N} = \overline{N \cap G} = \overline{N \cap HK_2} = \overline{N(K_2 \cap R) \cap HK_2} = \overline{N} \cap \overline{H}\,\overline{K_2} = (\overline{N} \cap \overline{H})\overline{K_2},$$

and similarly, $\overline{N} = \overline{N \cap G} = \overline{N \cap HK_1^r} = \overline{N} \cap \overline{H}\,\overline{K_1^r} = (\overline{N} \cap \overline{H})\overline{K_1^r}$. Also,

$$(\overline{N} \cap \overline{H}) \cap \overline{K_2} = \overline{N} \cap \overline{H} \cap \overline{K_2} = \overline{N \cap H \cap K_2} \leqslant \overline{H \cap K_2} = 1,$$

and similarly, $\overline{N} \cap \overline{H} \cap \overline{K_1^r} = 1$. Since $H \trianglelefteq G$, we have $H \cap N \trianglelefteq N$ and by Lemma 1.2, $\overline{H \cap N} = \overline{H} \cap \overline{N} \trianglelefteq \overline{N}$. By the Third Isomorphism Theorem,

$$\frac{\overline{N}}{\overline{H} \cap \overline{N}} = \frac{\overline{N}}{\overline{H \cap N}} \cong \frac{N}{(H \cap N)(K_2 \cap R)} \cong \frac{\dfrac{N}{H \cap N}}{\dfrac{(H \cap N)(K_2 \cap R)}{H \cap N}},$$

however, $N/H \cap N \cong NH/H \leqslant G/H$ and G/H is a solvable π'-group. Thus $\overline{N}/\overline{H} \cap \overline{N}$ is a solvable π'-group and $\overline{H} \cap \overline{N} \in Hall_\pi(\overline{N})$. By induction, there exists $\overline{n} \in \overline{N}$ such that $\overline{K_2} = \overline{K_1^r}^{\overline{n}} = \overline{K_1^{rn}}$ and $K_2 = K_2(K_2 \cap R) = K_1^{rn}(K_2 \cap R)$. Now $n \in N_G(K_2 \cap R)$ and $K_2 \cap R = K_1^r \cap R \leqslant K_1^r$, which implies $K_2 \cap R = (K_2 \cap R)^n \leqslant K_1^{rn}$. Therefore, $K_1^{rn} = K_2$ and G acts transitively on the complements of H in G. $\square$

Theorem 4.9. *Let G be a π-group and $A \leqslant Aut(G)$ be a π'-subgroup such that either G or A is solvable. Then for each $p \in \pi(G)$, there exists $P \in Syl_p(G)$ such that P is A-invariant.*

Proof.

Let $G^* = G \rtimes_{id} A$ and $P \in Syl_p(G)$. Now $G \trianglelefteq G^*$, so by the Frattini Argument, $G^* = N_{G^*}(P)G$. Let $N = N_{G^*}(P)$. By Theorem 1.23, $G^*/G = AG/G \cong A/A\cap G \cong A$, so G^*/G is a π'-group. Hence $G \in Hall_\pi(G^*)$. Now $G \cap N \trianglelefteq N$ and $N/N \cap G \cong NG/G \leqslant G^*/G \cong A$, which implies $G \cap N \in Hall_\pi(N)$. Since G or A is solvable, $N \cap G$ or $N/N \cap G$ is solvable, respectively. By Schur-Zassenhaus Part 1, N splits over $N \cap G$. Hence there exists $B \leqslant N$ such that $N = B(N \cap G)$ and $B \cap (N \cap G) = 1$. Again, since G or A is solvable, G or G^*/G is solvable, respectively. By Schur-Zassenhaus Part 2, G^* splits over G and G^* acts transitively on the complements of G in G^*. By Theorem 1.23, $G^* = AG$, $A \cap G = 1$, and A is a complement of G. Furthermore, $G^* = NG = B(N \cap G)G = BG$ and $B \cap G = B \cap N \cap G = 1$. Thus B is a complement of G. Since $G^* = AG$, there exists $g \in G$ such that $A = B^g \leqslant N^g = N_{G^*}(P)^g = N_{G^*}(P^g)$. Therefore, $P^g \in Syl_p(G)$ and P^g is A-invariant. $\square$

4.2 The Focal Subgroup

Definition 4.4. *Let G be a group and $H \leqslant G$. The* ***Focal Subgroup*** *of H in G is*

$$Foc_G(H) = \langle [h, g] : h \in H, g \in G, [h, g] \in H \rangle.$$

Equivalently, we may write

$$Foc_G(H) = \langle h_1^{-1}h_2 : h_1, h_2 \in H, h_1 \sim_G h_2 \rangle = \langle h_1 h_2^{-1} : h_1, h_2 \in H, h_1 \sim_G h_2 \rangle.$$

Moreover, $H' \leqslant Foc_G(H) \trianglelefteq H$.

If there is no fusion in G of H, then $Foc_G(H) = H'$, so $[Foc_G(H) : H']$ measures the amount of fusion of H in G.

Theorem 4.10. *Let G be a group and $H \leqslant G$ such that* $\gcd([G : H], [H : H']) = 1$. *Then $Foc_G(H) = G' \cap H$ and G splits normally over*

$$\frac{H}{G' \cap H} = \frac{H}{Foc_G(H)}.$$

Proof.

Let $J = Foc_G(H)$. Then $H' \leqslant J \trianglelefteq H$ and so H/J is abelian by Theorem 1.19. Now $[H : J] \cdot [J : H'] = [H : H']$, so $[H : J]$ divides $[H : H']$, which implies $\gcd([G : H], [H : J]) = 1$. Let $h_1, h_2 \in H$ such that $h_1 \sim_G h_2$. Now $h_1 h_2^{-1} \in Foc_G(H) = J$ and so $Jh_1 = Jh_2$. By Theorem 4.1, G splits normally over H/J. Hence there exists $K \trianglelefteq G$ such that $G = HK$ and $H \cap K = J$. Also,

$$\frac{G}{K} = \frac{HK}{K} \cong \frac{H}{H \cap K} = \frac{H}{J},$$

and G/K is abelian, which implies $G' \leqslant K$ by Theorem 1.19. Then $J \leqslant G' \cap H \leqslant K \cap H = J$ and we have $Foc_G(H) = J = G' \cap H$. Therefore, G splits normally over $H/Foc_G(H) = H/G' \cap H$. □

Theorem 4.11 (The Focal Subgroup Theorem)**.** *Let G be a group and $P \in Syl_p(G)$. Then $Foc_G(P) = G' \cap P$.*

Proof.

Since $P \in Syl_p(G)$, we have $\gcd([G : P], [P : P']) = 1$. By Theorem 4.10, $Foc_G(P) = G' \cap P$. □

Definition 4.5. *Let G be a group and $p \in \pi(G)$. Define the subgroup generated by all Sylow p'-subgroups of G by*

$$\mathcal{O}^p(G) = \langle Q \in Syl_q(G) : q \neq p \rangle.$$

Lemma 4.7. *Let G be a group and $P \in Syl_p(G)$. Then*

(*i*) $\mathcal{O}^p(G) \trianglelefteq G$.

(*ii*) $G = \mathcal{O}^p(G)P$.

(*iii*) $G/\mathcal{O}^p(G)$ *is a p-group.*

(*iv*) *If G is abelian, then $\mathcal{O}^p(G)$ is a p'-group.*

(*v*) *If $N \trianglelefteq G$ and $\overline{G} = G/N$, then $\mathcal{O}^p(\overline{G}) = \overline{\mathcal{O}^p(G)}$.*

Proof.

For (i), let $Q \in Syl_q(G)$ such that $q \neq p$ and $g \in G$. Now $|Q^g| = |Q| = |G|_q$ and so $Q^g \in Syl_q(G)$. Therefore, $Q^g \leqslant \mathcal{O}^p(G)$ and $\mathcal{O}^p(G) \trianglelefteq G$.

For (ii), let $q \in \pi(G)$ and suppose $|G|_q = q^n$ for some $n \in \mathbb{N}$. If $q = p$, then $p^n = |P|$ divides $|\mathcal{O}^p(G)P|$. If $q \neq p$, let $Q \in Syl_q(G)$. Then $q^n = |G|_q = |Q|$, but $Q \leqslant \mathcal{O}^p(G)P$. Thus $q^n = |Q|$ divides $|\mathcal{O}^p(G)P|$, but then $|G|$ divides $|\mathcal{O}^p(G)P|$. Therefore, $G = \mathcal{O}^p(G)P$.

For (iii), let $\overline{G} = G/\mathcal{O}^p(G)$ and $Q \in Syl_q(G)$, where $q \neq p$. Then $\overline{Q} \in Syl_q(\overline{G})$, but $Q \leqslant \mathcal{O}^p(G)$, hence $\overline{Q} = 1$. Therefore, $q \notin \pi(\overline{G})$ and $\overline{G}$ is a p-group.

For (iv), since G is abelian, we have $H \trianglelefteq G$ for all $H \leqslant G$. Thus $\mathcal{O}^p(G) = \prod_{Q \in S_q^G} Q$, where $q \neq p$ and $|\mathcal{O}^p(G)| = \prod_{Q \in S_q^G} |Q|$, where $q \neq p$. Therefore, $\mathcal{O}^p(G)$ is a p'-group.

For (v), let $Q \in Syl_q(G)$ such that $q \neq p$. Then $\overline{Q} \in Syl_q(\overline{G})$ and $\overline{Q} \leqslant \mathcal{O}^p(\overline{G})$. Thus $\overline{\mathcal{O}^p(G)} \leqslant \mathcal{O}^p(\overline{G})$. Conversely, let $\overline{Q} \in Syl_q(\overline{G})$. Now $Q \leqslant G$, but Q is not necessarily a q-group. Let $Q_0 \in Syl_q(Q)$. Then $\overline{Q_0} \in Syl_q(\overline{Q})$ and $\overline{Q_0} = \overline{Q}$, or, equivalently, $Q = Q_0N$. By Sylow, we have $Q_0 \leqslant \mathcal{O}^p(G)$. Thus $\overline{Q} = \overline{Q_0} \leqslant \overline{\mathcal{O}^p(G)}$ and $\mathcal{O}^p(\overline{G}) \leqslant \overline{\mathcal{O}^p(G)}$. Therefore, $\mathcal{O}^p(\overline{G}) = \overline{\mathcal{O}^p(G)}$. $\square$

Definition 4.6. *Let G be a group and $p \in \pi(G)$. Then $G/G'\mathcal{O}^p(G)$ is an abelian p-group. We call this quotient the* ***p-residual*** *of G.*

Theorem 4.12. *Let G be a group and $P \in Syl_p(G)$. Then*

$$\frac{G}{G'\mathcal{O}^p(G)} \cong \frac{P}{P \cap G'}.$$

Proof.

Let $\overline{G} = G/G'$ and $R = G'\mathcal{O}^p(G)$. By Lemma 4.7(ii), $G = P\mathcal{O}^p(G) = PG'\mathcal{O}^p(G)$ and so $\overline{G} = \overline{P}\,\overline{R}$. Now $\overline{P} \cap \overline{R} = \overline{P} \cap \overline{G'\mathcal{O}^p(G)} = \overline{P} \cap \overline{\mathcal{O}^p(G)} = \overline{P} \cap \mathcal{O}^p(\overline{G})$ and $\overline{G}$ is abelian. It follows from Lemma 4.7(iv) that $\mathcal{O}^p(\overline{G})$ is a p'-group, so $\overline{P} \cap \mathcal{O}^p(\overline{G}) = 1$. Therefore, by the Second and Third Isomorphism Theorems,

$$\frac{G}{G'\mathcal{O}^p(G)} = \frac{G}{R} \cong \frac{\overline{G}}{\overline{R}} = \frac{\overline{P}\,\overline{R}}{\overline{R}} \cong \frac{\overline{P}}{\overline{P} \cap \overline{R}} = \frac{\overline{P}}{\{1\}} \cong \overline{P} = \frac{PG'}{G'} \cong \frac{P}{P \cap G'}. \qquad \square$$

Theorem 4.13. *Let G be a group and $P \in Syl_p(G)$ such that P is abelian. Then*

$$\frac{G}{\mathcal{O}^p(G)} \cong \frac{N_G(P)}{\mathcal{O}^p(N_G(P))}.$$

Proof.

Let $H = N_G(P)$. By Lemma 4.7(ii), $G = \mathcal{O}^p(G)P$, so by the Second Isomorphism Theorem,

$$\frac{G}{\mathcal{O}^p(G)} = \frac{\mathcal{O}^p(G)P}{\mathcal{O}^p(G)} \cong \frac{P}{P \cap \mathcal{O}^p(G)}.$$

Since P is abelian, $P/P \cap \mathcal{O}^p(G)$ is abelian and by the above, $G/\mathcal{O}^p(G)$ is abelian. Hence $G' \leqslant \mathcal{O}^p(G)$ and $G/\mathcal{O}^p(G)$ is the p-residual of G. By a similar argument, since $P \in Syl_p(H)$, we have $H = \mathcal{O}^p(H)P$ and $H/\mathcal{O}^p(H)$ is the p-residual of H.

Clearly, $Foc_H(P) \leqslant Foc_G(P)$. Let $x_1, x_2 \in P$ such that $x_1 \sim_G x_2$. Since P is abelian, we know $x_1, x_2 \in C_G(P)$. It follows from Burnside's Theorem that $x_1 \sim_H x_2$, hence $x_1 x_2^{-1} \in Foc_H(P)$. Now we have $Foc_G(P) \leqslant Foc_H(P)$, so $Foc_G(P) = Foc_H(P)$. By Theorem 4.12 and the Focal Subgroup Theorem (4.11),

$$\frac{G}{\mathcal{O}^p(G)} \cong \frac{P}{P \cap G'} = \frac{P}{Foc_G(P)} = \frac{P}{Foc_H(P)} = \frac{P}{P \cap H'} \cong \frac{H}{\mathcal{O}^p(H)} = \frac{N_G(P)}{\mathcal{O}^p(N_G(P))}. \qquad \square$$

Theorem 4.14. *Let G be a group, $P \in Syl_p(G)$, P be abelian, and suppose $P \trianglelefteq G$. If Q is a p-complement of G and $G = \mathcal{O}^p(G)$, then $N_G(Q) = Q$.*

Proof.

Let $R = N_G(Q)$ and $P_0 = P \cap R$. Suppose there exists $Q \leqslant G$ such that $G = PQ$ and $P \cap Q = 1$. Now Q is a p'-group since

$$|Q| = \frac{|Q|}{|P \cap Q|} = \frac{|PQ|}{|P|} = \frac{|G|}{|P|}.$$

Moreover, $Q \trianglelefteq R$, $P_0 \trianglelefteq R$, and $[P_0, Q] \leqslant P_0 \cap Q = 1$ by coprime orders. Thus $G = PQ \leqslant C_G(P_0)$ and $G = C_G(P_0)$. Therefore, $P_0 \leqslant \mathcal{Z}(G)$.

Let $\overline{G} = G/G'$. Now $\overline{G}$ is abelian and $\mathcal{O}^p(\overline{G})$ is a p'-group by Lemma 4.7. However, $G = \mathcal{O}^p(G)$ implies $\overline{G} = \overline{\mathcal{O}^p(G)} = \mathcal{O}^p(\overline{G})$ is a p'-group. Thus $p \notin \pi(\overline{G})$, so $|G|_p = |G'|_p$. By Sylow, $P \leqslant G'$ since $P \trianglelefteq G$. Furthermore, we have $\{1\} \trianglelefteq P \leqslant G$, $P/\{1\} \cong P$ is abelian, and $\gcd([G : P], [P : \{1\}]) = 1$. By Theorem 3.3, $P_0 \leqslant \mathcal{Z}(G) \cap G' \cap P = 1$. Therefore,

$$N_G(Q) = R = R \cap G = R \cap PQ = (R \cap P)Q = P_0Q = Q. \qquad \square$$

Theorem 4.15. *Let G be a group, $J \trianglelefteq H \leqslant G$, H/J be nilpotent, and suppose* $\gcd([G : H], [H : J]) = 1$. *Then the following are equivalent:*

(*i*) *G splits normally over H/J.*

(*ii*) *Whenever $h_1, h_2 \in H$ are fused in G, it follows Jh_1 and Jh_2 are fused in H/J.*

Proof.

Suppose G splits normally over H/J. Then the result follows from Theorem 4.1.

To show the remaining implication, use induction on $[H : J]$. Let $\overline{H} = H/J$ and $\mathcal{Z}(\overline{H}) = \overline{J_1}$. Now $\overline{J_1} \trianglelefteq \overline{H}$ and $J \trianglelefteq J_1 \trianglelefteq H \leqslant G$. Furthermore, $H/J_1 \cong \overline{H}/\overline{J_1}$ implies $\overline{H}/\overline{J_1}$ is nilpotent, and since $[H : J_1]$ divides $[H : J]$, it follows that the $\gcd([G : H], [H : J_1]) = 1$. If there exist $h_1, h_2 \in H$ such that $h_1 \sim_G h_2$, then by assumption, $\overline{h_1} \sim_{\overline{H}} \overline{h_2}$. This implies there exists $\overline{h} \in \overline{H}$ such that $\overline{h_2} = \overline{h_1}^{\overline{h}} = \overline{h_1^h}$. But then $h_1^h h_2^{-1} \in J \leqslant J_1$, so $J_1 h_1^h \sim_{H/J_1} J_1 h_2$.

If $[H:J]=[H:J_1]$, then $|J|=|J_1|$ and $[J:J_1]=1$. Hence $\mathcal{Z}(\overline{H})=\overline{J_1}=1$, but $\overline{H}$ is nilpotent. This implies $\overline{H}=\mathcal{Z}(\overline{H})=1$, so $\overline{H}$ is abelian and the result follows from Theorem 4.1. Without loss of generality, assume $[H:J_1]<[H:J]$. By the induction hypothesis, G splits normally over H/J_1, so there exists $K_1 \trianglelefteq G$ such that $G=HK_1$ and $H\cap K_1=J_1$. Now

$$\frac{G}{K_1}=\frac{HK_1}{K_1}\cong\frac{H}{H\cap K_1}=\frac{H}{J_1},$$

and $J\trianglelefteq J_1\leqslant K_1$. Moreover, $\overline{J_1}=\mathcal{Z}(\overline{H})$ is abelian, $|\overline{J_1}|$ divides $|\overline{H}|$,

$$\frac{|G|}{|H|}=\frac{|G|}{|K_1|}\cdot\frac{|K_1|}{|H|}=\frac{|H||K_1|}{|H\cap K_1||K_1|}\cdot\frac{|K_1|}{|H|}=\frac{|H|}{|J_1|}\cdot\frac{|K_1|}{|H|}=\frac{|K_1|}{|J_1|}, \tag{3}$$

and $\gcd([G:H],[H:J])=1$. Consequently, $\gcd([J_1:J],[K_1:J_1])=1$.

Suppose $x_1,x_2\in J_1$ such that $x_1\sim_{K_1}x_2$. By hypothesis, $\overline{x_1}\sim_{\overline{H}}\overline{x_2}$. Since $\overline{x_1},\overline{x_2}\in\overline{J_1}$, we have $\overline{x_1}=\overline{x_2}$ and $\overline{x_1}\sim_{\overline{J_1}}\overline{x_2}$. Now $[J_1:J]<[H:J]$; otherwise, $\overline{H}$ is abelian and the result follows from Theorem 4.1. By induction on $J\trianglelefteq J_1\leqslant K_1$, K_1 splits normally over J_1, so there exists $K\trianglelefteq K_1$ such that $K_1=KJ_1$ and $K\cap J_1=J$. Then $HK=HJ_1K=HK_1=G$ and $J\leqslant H\cap K=H\cap K_1\cap K=J_1\cap K_1=J$. Therefore, G splits over $\overline{H}$.

Let $h\in H$. Now $J\leqslant K\trianglelefteq K_1\trianglelefteq G$ implies $J=J^h\leqslant K^h\leqslant K_1^h=K_1$, and so $J\leqslant K\cap K^h$. By the Second Isomorphism Theorem, $K^hK/K\cong K^h/K^h\cap K$ and $[K^hK:K]=[K^h:K^h\cap K]$. Now $[K^hK:K]$ divides $[K_1:K]$, but

$$\frac{|K_1|}{|K|}=\frac{|KJ_1|}{|K|}=\frac{|J_1|}{|K\cap J_1|}=\frac{|J_1|}{|J|},$$

where $[J_1:J]$ divides $[H:J]$. Thus $[K^hK:K]$ divides $[H:J]$. Because $J\leqslant K\cap K^h$, $[K^hK:K]=[K^h:K\cap K^h]$ divides $[K^h:J]$ and by (3),

$$\frac{|K^h|}{|J|}=\frac{|K|}{|J|}=\frac{|K|}{|K\cap J_1|}=\frac{|KJ_1|}{|J_1|}=\frac{|K_1|}{|J_1|}=\frac{|G|}{|H|}.$$

Thus $[K^hK:K]$ is a common divisor of $[G:H]$ and $[H:J]$, so $[K^hK:K]=1$ and $K^h\leqslant K$. It follows that $K^h=K$ and $K\trianglelefteq HK=G$. Therefore, G splits normally over $\overline{H}$. □

4.3 Frobenius' Normal p-Complement Theorem

Theorem 4.16. *Let G be a group, $P \in Syl_p(G)$, and suppose $N_G(Q)/C_G(Q)$ is a p-group for all $Q \leqslant P$. If $P^* \in Syl_p(G)$ and $x \in P \cap P^*$, then there exists $y \in C_G(x)$ such that $P^* = P^y$.*

Proof.

Let $Q = P \cap P^*$, $x \in Q$, and proceed by induction on $[P : Q]$. If $[P : Q] = 1$, then $P = Q = P \cap P^*$, so $P \leqslant P^*$ and $P = P^*$. Thus we may chose $1 \in C_G(x)$, where $P^1 = P = P^*$. Assume $Q < P$ and $Q < P^*$. Since P is a p-group, we have P is nilpotent and $Q < N_P(Q) \leqslant N_G(Q)$ by Lemma 1.16. Now $N_P(Q)$ is a p-group, so by Sylow, there exists $Q_1 \in Syl_p(N_G(Q))$ such that $N_P(Q) \leqslant Q_1$. Again by Sylow, there exists $P_1 \in Syl_p(G)$ such that $Q_1 \leqslant P_1$. Thus $x \in Q < N_P(Q) \leqslant P \cap Q_1 \leqslant P \cap P_1$ and $[P : P \cap P_1] < [P : Q]$. By induction, there exists $y_1 \in C_G(x)$ such that $P^{y_1} = P_1$. By the same argument as above, $Q < N_{P^{y_1}}(Q) \leqslant N_G(Q)$ and $N_{P^{y_1}}(Q)$ is a p-group. By Sylow, there exists $w \in N_G(Q)$ such that $N_{P^{y_1}}(Q) \leqslant Q_1^w$.

Let $\overline{N_G(Q)} = N_G(Q)/C_G(Q)$. Now $\overline{Q_1} \in Syl_p(\overline{N_G(Q)})$ and $|\overline{Q_1}| = |\overline{N_G(Q)}|$ since $\overline{N_G(Q)}$ is a p-group. Thus $\overline{Q_1} = \overline{N_G(Q)}$ and $N_G(Q) = Q_1 C_G(Q)$. Since $w \in N_G(Q)$, we have $w = q_1 c$ for some $q_1 \in Q_1$ and $c \in C_G(Q)$, so $Q_1^w = Q_1^{q_1 c} = Q_1^c$. Without loss of generality, assume $w \in C_G(Q) \leqslant C_G(x)$ and let $u = (y_1 w)^{-1}$. From the above,

$$Q < N_{P^*}(Q) \leqslant P^* \cap Q_1^w \leqslant P^* \cap P_1^w = P^* \cap P^{y_1 w} = P^* \cap P^{u^{-1}}.$$

Since $u \in C_G(x)$, we have $x = x^u \in Q^u < N_{P^*}(Q)^u \leqslant (P^*)^u$. Hence $x \in P \cap (P^*)^u$ and $x = x^{u^{-1}} \in P^* \cap P^{u^{-1}}$. Also, since $Q < P^* \cap P^{u^{-1}}$, we have

$$\frac{|P^{u^{-1}}|}{|P^* \cap P^{u^{-1}}|} < \frac{|P^{u^{-1}}|}{|Q|} = \frac{|P|}{|Q|},$$

and $[N_G(Q)^{u^{-1}} : C_G(Q)^{u^{-1}}] = [N_G(Q) : C_G(Q)]$ is a p-number. By the induction hypothesis, there exists $y_2 \in C_G(x)$ such that $(P^*)^{y_2} = P^{u^{-1}}$. Therefore,
$P = (P^*)^{y_2 u} = (P^*)^{y_2 (y_1 w)^{-1}}$ and $y_2(y_1 w)^{-1} \in C_G(x)$. $\square$

Theorem 4.17. *Let G be a group, $J \trianglelefteq H \leqslant V \leqslant G$, H/J be nilpotent, and* $\gcd([G:H],[H:J]) = 1$. *Further suppose, whenever $h_1, h_2 \in H$ are fused in G, it follows that h_1 and h_2 are fused in V. Then the following are equivalent:*

(i) G splits normally over H/J.

(ii) V splits normally over H/J.

Proof.

Suppose G splits normally over H/J. Now there exists $K \trianglelefteq G$ such that $G = HK$ and $H \cap K = J$. Since $K \trianglelefteq G$, we have $K \cap V \trianglelefteq V$. Furthermore,

$$V = V \cap G = V \cap HK = H(V \cap K),$$

and $H \cap (V \cap K) = H \cap K = J$. Therefore, V splits normally over H/J.

Suppose V splits normally over H/J and $h_1, h_2 \in H$ are fused in G. By hypothesis, $h_1 \sim_V h_2$. Now $[V:H]$ divides $[G:H]$ and $\gcd([V:H],[H:J]) = 1$. Hence $Jh_1 \sim_{H/J} Jh_2$ by Theorem 4.15. By Theorem 4.15 on $J \trianglelefteq H \leqslant G$, we have G splits normally over H/J. $\square$

Theorem 4.18 (Frobenius' Normal p-Complement Theorem)**.** *Let G be a group and $P \in Syl_p(G)$. Then G has a normal p-complement if and only if one of the following conditions are satisfied:*

(i) $N_G(Q)/C_G(Q)$ is a p-group for all $Q \leqslant P$.

(ii) $N_G(Q)$ has a normal p-complement for all $Q \leqslant P$.

Proof.

For (i), suppose G has a normal p-complement. Now there exists $K \trianglelefteq G$ such that $G = PK$ and $P \cap K = 1$. Let $Q \leqslant P$. Since

$$|K| = \frac{|K|}{|P \cap K|} = \frac{|PK|}{|P|} = \frac{|G|}{|P|},$$

we have K is a p'-group. Moreover, $K \cap N_G(Q) \trianglelefteq N_G(Q)$ and $Q \trianglelefteq N_G(Q)$. Thus $[K \cap N_G(Q), Q] \leqslant Q \cap K \cap N_G(Q) = 1$ by coprime orders. Hence $K \cap N_G(Q) \leqslant C_G(Q)$.

By the Second Isomorphism Theorem,

$$\frac{N_G(Q)}{K \cap N_G(Q)} \cong \frac{N_G(Q)K}{K} \leqslant \frac{G}{K} = \frac{PK}{K} \cong \frac{P}{P \cap K},$$

so $N_G(Q)/K \cap N_G(Q)$ is a p-group. By Lemma 4.7,

$$\frac{\mathcal{O}^p(N_G(Q))}{K \cap N_G(Q)} = \mathcal{O}^p\left(\frac{N_G(Q)}{K \cap N_G(Q)}\right) = 1,$$

thus $\mathcal{O}^p(N_G(Q)) \leqslant K \cap N_G(Q) \leqslant C_G(Q)$. Again by Lemma 4.7, $N_G(Q)/C_G(Q)$ is a p-group.

Conversely, suppose $N_G(Q)/C_G(Q)$ is a p-group for all $Q \leqslant P$ and let $V = N_G(P)$. Now $P \trianglelefteq V$ and $P \in Syl_p(V)$. By Schur-Zassenhaus Part 1, V splits over P, so there exists $W \leqslant V$ such that $V = PW$ and $P \cap W = 1$. Since W is a p'-group, we have $W = \langle Q : Q \in Syl_q(W), q \in \pi(W)\rangle$ and so $W \leqslant \mathcal{O}^p(V)$. Now

$$\frac{\mathcal{O}^p(V)C_G(P)}{C_G(P)} \leqslant \frac{N_G(P)}{C_G(P)}$$

is a p-subgroup, but $\mathcal{O}^p(V)C_G(P)/C_G(P)$ is a homomorphic image of a p'-group. Thus $\mathcal{O}^p(V)C_G(P)/C_G(P) = 1$ and $\mathcal{O}^p(V) \leqslant C_G(P)$. This implies $W \leqslant C_G(P) \leqslant N_G(P)$ and $W \trianglelefteq WP = V$. Hence V splits normally over $P \cong P/\{1\}$. Now $\{1\} \trianglelefteq P \leqslant V \leqslant G$, $P/\{1\}$ is nilpotent, and $\gcd([G : P], [P : \{1\}]) = 1$.

Let $x \in P$ and $g \in G$ such that $x^g \in P$. Now $x \in P \cap P^{g^{-1}}$ and by Theorem 4.16, there exists $y \in C_G(x)$ such that $P^y = P^{g^{-1}}$ or, equivalently, $P^{yg} = P$. Hence $yg \in N_G(P) = V$. Also, $x^{yg} = x^g$ implies $x \sim_V x^g$. By Theorem 4.17 used on $\{1\} \trianglelefteq P \leqslant V \leqslant G$, we have G splits normally over $P/\{1\} \cong P$, so G has a normal p-complement.

For (ii), suppose G has a normal p-complement. Now there exists $K \trianglelefteq G$ such that $G = PK$ and $P \cap K = 1$. Let $Q \leqslant P, N = N_G(Q)$, and $P_0 \in Syl_p(N)$. Now $K \cap N \trianglelefteq N$ and by the Second Isomorphism Theorem,

$$\frac{N}{N \cap K} \cong \frac{KN}{K} \leqslant \frac{G}{K} = \frac{PK}{K} \cong \frac{P}{P \cap K}.$$

Hence $N/N \cap K$ is a p-group. Let $\overline{N} = N/N \cap K$. Now $\overline{P_0} \in Syl_p(\overline{N})$, but $\overline{N}$ is a

p-group, so $\overline{P_0} = \overline{N}$. Thus $N = P_0(N \cap K)$ and it follows from Sylow that there exists $g \in G$ with $P_0 \leqslant P^g$. Then

$$P_0 \cap N \cap K \leqslant P^g \cap N \cap K \leqslant P^g \cap K = P^g \cap K^g = (P \cap K)^g = 1,$$

and $N = N_G(Q)$ has a normal p-complement.

Conversely, suppose $N_G(Q)$ has a normal p-complement for all $Q \leqslant P$. Let $Q \leqslant P, N = N_G(Q)$, and $P_0 \in Syl_p(N)$. Now there exists $K \trianglelefteq N$ such that $N = P_0K$ and $P_0 \cap K = 1$. Moreover, K is a p'-group, $K \trianglelefteq N$, and $Q \trianglelefteq N$. Consequently, $[Q, K] \leqslant Q \cap K = 1$ and $K \leqslant C_G(Q)$. By the Second Isomorphism Theorem,

$$\frac{N}{K} = \frac{P_0K}{K} \cong \frac{P_0}{P_0 \cap K} \cong P_0,$$

so N/K is a p-group. In addition,

$$\frac{N_G(Q)}{C_G(Q)} \cong \frac{N_G(Q)/K}{C_G(Q)/K}$$

is a p-group. Therefore by (i), G has a normal p-complement. $\square$

5 The Journey to Replacement Theorems

5.1 The Thompson Subgroup

Definition 5.1. *Let P be a p-group and define the set*

$$\mathcal{A}(P) = \{A \leqslant P : A \text{ is abelian and } |A| \text{ is maximal}\}.$$

*The **Thompson subgroup** of P is given by $J(P) = \langle A : A \in \mathcal{A}(P)\rangle$.*

Lemma 5.1. *If P is a p-group, then $\mathcal{A}(P) \neq 1$.*

Proof.

Toward a contradiction, suppose $\mathcal{A}(P) = 1$ and let $|P| = p^n$ for some $n \in \mathbb{N}_0$. Now there exists $H \leqslant P$ such that $|H| = p$. Hence $H \cong \mathbb{Z}_p$ and H is abelian. It follows that $H \in \mathcal{A}(P) = 1$, which is contradiction. Therefore, $\mathcal{A}(P) \neq 1$. □

Theorem 5.1. *Let P be a p-group and $A \in \mathcal{A}(P)$. Then $A = C_P(A)$.*

Proof.

Since $A \in \mathcal{A}(P)$, we have A is abelian and $A \leqslant C_P(A)$. Let $x \in C_P(A)$. Now $x \in N_P(A)$, so $\langle x\rangle A \leqslant P$. But then $A \leqslant \langle x\rangle A \leqslant P$, where $\langle x\rangle A$ is abelian. By the maximality of $|A|$, $A = \langle x\rangle A$ and $x \in A$. Therefore, $A = C_P(A)$. □

Theorem 5.2. *Let G be a group and $P \in Syl_p(G)$. Then*

(i) *$J(P)$ char P.*

(ii) *If $A \leqslant H \leqslant P$ and $A \in \mathcal{A}(P)$, then $J(H) \leqslant J(P)$. If $J(P) \leqslant H \leqslant P$, then $J(P) = J(H)$.*

(iii) *If $Q \in Syl_p(G)$ such that $J(P) \leqslant Q$, then $J(P) = J(Q)$.*

(iv) *If $J(P) \leqslant H \leqslant G$ and H is a p-group, then $J(P)$ char H.*

Proof.

For *(i)*, let $\phi \in Aut(P)$ and $A \in \mathcal{A}(P)$. Now A^ϕ is abelian, $|A^\phi| = |A|$, and $A^\phi \leqslant P$. Consequently, $A^\phi \in \mathcal{A}(P)$, so $J(P)^\phi \leqslant J(P)$. Therefore, $J(P)$ char P.

For (ii), since $A \leqslant H \leqslant P$ and $A \in A(P)$, we know the orders of elements from $A(H)$ are the same as the orders of elements from $A(P)$. Hence $A(H) \subseteq A(P)$ and so $J(H) \leqslant J(P)$. If $J(P) \leqslant H \leqslant P$, then by above, we have $J(H) \leqslant J(P)$. It follows from $J(P) \leqslant H$ that $A(P) \subseteq A(H)$. Thus $J(P) \leqslant J(H)$, so $J(P) = J(H)$.

For (iii), let $Q \in Syl_p(G)$, where $J(P) \leqslant Q$. By Sylow, there exists $g \in G$ such that $Q = P^g$. Now $Q = P^g \cong P$ and

$$J(Q) = \langle A^g : A \in A(P) \rangle = \langle A : A \in A(P) \rangle^g = J(P)^g.$$

Thus $|J(Q)| = |J(P)^g| = |J(P)|$. Since $P \cong Q$, elements of $A(P)$ and $A(Q)$ have the same order, but $J(P) \leqslant Q$. Hence $A(P) \subseteq A(Q)$ and $J(P) \leqslant J(Q)$. Therefore, $J(P) = J(Q)$.

For (iv), suppose $J(P) \leqslant H \leqslant G$ and H is a p-group. By Sylow, there exists $Q \in Syl_p(G)$ such that $H \leqslant Q$. Now $J(P) \leqslant Q$ and so by (iii), $J(P) = J(Q)$. Hence $J(Q) \leqslant H \leqslant Q$ and by (ii), $J(H) = J(Q) = J(P)$. The result from (i). $\square$

5.2 Properties of Commutators

Lemma 5.2. *Let G be a group, $x, y, z \in G$, $[y, z] = 1$, and suppose $[x, G]$ is abelian. Then $[x, y, z] = [x, z, y]$.*

Proof.

Let $g \in G$. Now $[x, g] \in [x, G]$ and

$$[g, x] = g^{-1}x^{-1}gx = (x^{-1}g^{-1}xg)^{-1} = [x, g]^{-1} \in [x, G].$$

Since $[x, G]$ is abelian,

$$\begin{aligned}
[x,y,z] &= [[x,y],z] = [x^{-1}y^{-1}xy, z] = (x^{-1}y^{-1}xy)^{-1}z^{-1}(x^{-1}y^{-1}xy)z \\
&= y^{-1}x^{-1}yxz^{-1}x^{-1}y^{-1}xyz = x^{-1}xy^{-1}x^{-1}yxz^{-1}x^{-1}y^{-1}xyz \\
&= x^{-1}[x^{-1},y][x^{-1},z]z^{-1}y^{-1}xyz = x^{-1}[x^{-1},z][x^{-1},y]z^{-1}y^{-1}xzy \\
&= x^{-1}xz^{-1}x^{-1}zxy^{-1}x^{-1}yz^{-1}y^{-1}xzy = z^{-1}x^{-1}zxy^{-1}x^{-1}yy^{-1}z^{-1}xzy \\
&= z^{-1}x^{-1}zxy^{-1}x^{-1}z^{-1}xzy = [x,z]^{-1}y^{-1}[x,z]y = [[x,z],y] \\
&= [x,z,y].
\end{aligned}$$

Therefore, $[x, y, z] = [x, z, y]$. $\square$

Lemma 5.3. *Let G be a group and $a, b, c \in G$. Then*

(i) $[ab, c] = [a, c][a, c, b][b, c]$.

(ii) $[a, b, a] = [a^b, a]$.

Proof.

For (i), let $a, b, c \in G$. Then

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

Therefore, $[a, c][a, c, b][b, c] = [ab, c]$.

For (ii), let $a, b \in G$. Then

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

Therefore, $[a, b, a] = [a^b, a]$. $\square$

Lemma 5.4. *Let G be a group and $x \in G$. Then $[x^n, g] \in [x, G]$ for all $g \in G$, $n \in \mathbb{N}$.*

Proof.

We proceed by induction on n. Let $g \in G$. If $n = 2$, we have by Lemma 5.3,

$$[x^2, g] = [xx, g] = [x, g][x, g, x][x, g] = [x, g][x^g, x][x, g] = [x, g][x, x^g]^{-1}[x, g] \in [x, G].$$

Assume $[x^n, g] \in [x, G]$ for all $g \in G$. By Lemma 5.3 and the induction hypothesis,

$$\begin{aligned}
[x^{n+1}, g] &= [x^n x, g] = [x^n, g][x^n, g, x][x, g] = [x^n, g][x^n, g]^{-1}x^{-1}[x^n, g]x[x, g] \\
&= [x^n, g][g, x^n]x^{-1}[x^n, g]x[x, g] = [x^n, g]g^{-1}x^{-n}gx^n x^{-1}x^{-n}g^{-1}x^n gx[x, g] \\
&= [x^n, g]g^{-1}x^{-n}gx^{-1}g^{-1}x^n gx[x, g] = [x^n, g](g^{-1}x^n g)^{-1}x^{-1}(g^{-1}x^n g)x[x, g] \\
&= [x^n, g][(x^n)^g, x][x, g] = [x^n, g][x, (x^n)^g]^{-1}[x, g].
\end{aligned}$$

Therefore, $[x^{n+1}, g] \in [x, G]$ and the result holds by induction. □

Theorem 5.3 (Properties of Commutators)**.** *Let G be a group, $H \leqslant G$, $K \leqslant G$, $x, y, z \in G$, and $n \in \mathbb{N}$. Then*

(*i*) $[xy, z] = [x, z]^y[y, z]$.

(*ii*) $[x, yz] = [x, z][x, y]^z$.

(*iii*) $[x, y]^{-1} = [y, x]$.

(*iv*) $[x, y] = x^{-1}x^y$.

(*v*) $[G, H] \trianglelefteq G$.

(*vi*) $[H, K] \trianglelefteq \langle H, K\rangle$.

(*vii*) $\binom{n+1}{2} = \binom{n}{2} + n$.

(*viii*) $[x, y, x] = [x^y, x]$.

(*ix*) *If $[x, y] \in C_G(x) \cap C_G(y)$, then*

  (*a*) $[x, y]^n = [x, y^n] = [x^n, y]$,

  (*b*) $(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}$.

Proof.

Properties (*i*)-(*iv*) are proven by direct computation.

For (*v*), let $g, g_1 \in G$ and $h \in H$. Now

$$\begin{aligned}
[g_1, h]^g &= g^{-1}g_1^{-1}h^{-1}g_1 hg = (g_1 g)^{-1}h^{-1}g_1 ghh^{-1}g^{-1}hg \\
&= [g_1 g, h][h, g] = [g_1 g, h][g, h]^{-1} \in [G, H].
\end{aligned}$$

Therefore, $[G, H] \trianglelefteq G$.

For (vi), let $h, h_1 \in H$ and $k, k_1 \in K$. By (i), $[hh_1, k] = [h, k]^{h_1}[h_1, k]$, so $[h, k]^{h_1} = [hh_1, k][h_1, k]^{-1} \in [H, K]$. Similarly, $[h, kk_1] = [h, k_1][h, k]^{k_1}$ and $[h, k]^{k_1} = [h, k_1]^{-1}[h, kk_1] \in [H, K]$. Therefore, $[H, K] \trianglelefteq \langle H, K\rangle$.

For (vii),

$$\begin{aligned}\binom{n+1}{2} &= \frac{(n+1)!}{2!(n+1-2)!} = \frac{(n+1)!}{2!(n-1)!} = \frac{(n+1)(n)}{2} = \frac{n^2+n}{2} \\ &= \frac{n^2-n+2n}{2} = \frac{n(n-1)}{2} + n = \frac{n!}{2!(n-2)!} + n = \binom{n}{2} + n.\end{aligned}$$

For $(viii)$, by direct computation we have

$$\begin{aligned}[x, y, x] &= [x, y]^{-1}x^{-1}[x, y]x = [y, x]x^{-1}[x, y]x \\ &= y^{-1}x^{-1}yxx^{-1}x^{-1}y^{-1}xyx = (y^{-1}xy)^{-1}x^{-1}(y^{-1}xy)x \\ &= (x^y)^{-1}x^{-1}(x^y)x = [x^y, x].\end{aligned}$$

Therefore, $[x, y, x] = [x^y, x]$.

For (ix), let $[x, y] \in C_G(x) \cap C_G(y)$ and use induction on n. If $n = 1$, then $[x, y]^1 = [x, y^1]$. Suppose $[x, y]^n = [x, y^n]$. Now by the induction hypothesis, $[x, y]^{n+1} = [x, y][x, y]^n = [x, y][x, y^n]$. Since $[x, y] \in C_G(x) \cap C_G(y)$, we have

$$\begin{aligned}[x, y][x, y^n] &= [x, y]x^{-1}y^{-n}xy^n = x^{-1}y^{-n}x[x, y]y^n = x^{-1}y^{-n}xx^{-1}y^{-1}xyy^n \\ &= x^{-1}y^{-n-1}xy^{n+1} = x^{-1}y^{-(n+1)}xy^{n+1} = [x, y^{n+1}].\end{aligned}$$

Therefore, $[x, y]^n = [x, y^n] = [x^n, y]$ for all $n \in \mathbb{N}_0$ by induction.

For (b), use induction on n. If $n = 2$, then

$$\begin{aligned}x^2y^2[y, x]^{\binom{2}{2}} &= x^2y^2[y, x] = xxyy[x, y] = xxy[y, x]y \\ &= xxyy^{-1}x^{-1}yxy = xyxy = (xy)^2.\end{aligned}$$

Assume $(xy)^n = x^n y^n [y,x]^{\binom{n}{2}}$. By (a) and (vii),

$$\begin{aligned}
(xy)^{n+1} &= (xy)^n xy = x^n y^n [y,x]^{\binom{n}{2}} xy = x^n y^n [y^{\binom{n}{2}}, x] xy = x^n y^n y^{-\binom{n}{2}} x^{-1} y^{\binom{n}{2}} xxy \\
&= x^n y^n y^n y^{-n} y^{-\binom{n}{2}} x^{-1} y^{\binom{n}{2}} y^n y^{-n} xxy = x^n y^{2n} y^{-\binom{n}{2}-n} x^{-1} y^{\binom{n}{2}+n} y^{-n} xxy \\
&= x^n y^{2n} y^{-\binom{n+1}{2}} x^{-1} y^{\binom{n+1}{2}} y^{-n} xxy = x^n y^{2n} y^{-\binom{n+1}{2}} x^{-1} y^{\binom{n+1}{2}} x x^{-1} y^{-n} xxy \\
&= x^n y^{2n} [y^{\binom{n+1}{2}}, x] x^{-1} y^{-n} xxy = x^n y^{2n} [y,x]^{\binom{n+1}{2}} x^{-1} y^{-n} xxy \\
&= x^n y^{2n} x^{-1} y^{-n} xxy [y,x]^{\binom{n+1}{2}} = x^n y^{2n} x^{-1} y^{-n} x y^n y^{-n} xy [y,x]^{\binom{n+1}{2}} \\
&= x^n y^{2n} [x, y^n] y^{-n} xy [y,x]^{\binom{n+1}{2}} = x^n y^{2n} y^{-n} x [x, y^n] y [y,x]^{\binom{n+1}{2}} \\
&= x^n y^n x x^{-1} y^{-n} x y^n y [y,x]^{\binom{n+1}{2}} = x^n x y^n y [y,x]^{\binom{n+1}{2}} \\
&= x^{n+1} y^{n+1} [y,x]^{\binom{n+1}{2}}.
\end{aligned}$$

Therefore, $(xy)^n = x^n y^n [y,x]^{\binom{n}{2}}$ for all $n \in \mathbb{N}_0$ by induction. □

Lemma 5.5. *Let G be a group, $a, b, c \in G$ such that $c \in C_G(b)$ and $b \in C_G(a)$. Then $[ab, c] = [a, c]$.*

Proof.

By Theorem 5.3 and the hypothesis, $[ab, c] = [a, c]^b [b, c] = [a, c]^b = [a, c]$. □

Lemma 5.6 (Three Subgroups Lemma)**.** *Let G be a group, $H \leqslant G, L \leqslant G, K \leqslant G$, and suppose $[H, K, L] = 1$ and $[K, L, H] = 1$. Then $[L, H, K] = 1$.*

Proof.

Let $h \in H, k \in K$, and $l \in L$. Consider the element $[h, k^{-1}, l]^k [k, l^{-1}, h]^l [l, h^{-1}, k]^h$. It follows from direct computation that

$$[h, k^{-1}, l]^k [k, l^{-1}, h]^l [l, h^{-1}, k]^h = k^{-1} [h, k^{-1}, l] k l^{-1} [k, l^{-1}, h] l h^{-1} [l, h^{-1}, k] h = 1.$$

By hypothesis, $[h, k^{-1}, l] = 1$ and $[k, l^{-1}, h] = 1$, which implies $[h, k^{-1}, l]^k = 1$ and $[k, l^{-1}, h]^l = 1$. From the above, $1 = [l, h^{-1}, k]^h$, or, equivalently, $[l, h^{-1}, k] = 1$. Therefore, $[L, H, K] = 1$. □

5.3 Thompson Replacement Theorem

Definition 5.2. *Let G be a group, $A \leqslant G$, and $B \leqslant G$. If $[B, A, A] = 1$, then A* ***acts quadratically*** *on B.*

Theorem 5.4. *Let P be a p-group, $A \in A(P)$, and $B \leqslant P$. Then $B \leqslant N_P(A)$ if and only if A acts quadratically on B.*

Proof.

Suppose $B \leqslant N_P(A)$. The result follows since A is abelian. Conversely, suppose $[B, A, A] = 1$. Now $[B, A] \leqslant C_P(A) = A$ by Theorem 5.1. This implies for all $[b, a] \in [B, A]$, there exists $a_1 \in A$ such that $a_1 = [b, a] = (a^{-1})^b a$. It follows that $(a^{-1})^b = a_1 a^{-1} \in A$. Therefore, $B \leqslant N_P(A)$. □

Theorem 5.5. *Let P be a p-group, $A \in A(P)$, $x \in P$, and suppose $M = [x, A]$ is abelian. Then $MC_A(M) \in A(P)$.*

Proof.

Let $C = C_A(M)$. It follows from M and C being abelian, and $[M, C] = 1$ that MC is abelian. Thus it is enough to show $|MC| \geq |A|$.

By Theorem 5.1, $A = C_P(A)$, so

$$C \cap M \leqslant C_M(A) = M \cap C_P(A) = M \cap A \leqslant C_A(M) \cap M = C \cap M.$$

Hence $C \cap M = C_M(A)$. Furthermore,

$$|MC| = \frac{|M||C|}{|M \cap C|} = \frac{|M||C_A(M)|}{|C_M(A)|},$$

and so it is enough to show $[M : C_M(A)] \geq [A : C_A(M)]$. For if true,

$$\frac{|M|}{|C \cap M|} = \frac{|M|}{|C_M(A)|} \geq \frac{|A|}{|C_A(M)|} = \frac{|A|}{|C|}$$
$$\frac{|M||C|}{|C \cap M|} \geq |A|.$$

Let $u, v \in A$ such that $C_A(M)u \neq C_A(M)v$, it follows that $[x, u], [x, v] \in M$. If $C_M(A)[x, u] = C_M(A)[x, v]$, then $y = [x, u]^{-1}[x, v] \in C_M(A)$. Now $y = (x^u)^{-1} x^v$

and since $y \in C_M(A)$, $y = y^{u^{-1}} = ((x^u)^{-1}x^v)^{u^{-1}} = x^{-1}x^{vu^{-1}} = [x, vu^{-1}]$. Hence $[x, vu^{-1}] \in C_M(A)$, so $[x, vu^{-1}, a] = 1$ for all $a \in A$. Since A is abelian and $vu^{-1} \in A$, we have $[vu^{-1}, a] = 1$ for all $a \in A$. By Lemma 5.2, $[x, a, vu^{-1}] = 1$ for all $a \in A$. Thus $vu^{-1} \in C_A(M)$ and so $C_A(M)u = C_A(M)v$, which is a contradiction. Therefore, $[M : C_M(A)] \geq [A : C_A(M)]$ and $MC_A(M) \in A(P)$. $\square$

Theorem 5.6 (Thompson Replacement Theorem)**.** *Let P be a p-group, $A \in A(P)$, $B \leqslant P$, B be abelian, and suppose $A \leqslant N_P(B)$, but $B \nleqslant N_P(A)$. Then there exists $A^* \in A(P)$ such that*

(*i*) $A \cap B < A^* \cap B$.

(*ii*) $A^* \leqslant N_P(A)$.

Proof.

Since $A \leqslant N_P(B)$, we have $B \trianglelefteq AB \leqslant P$. Let $N = N_B(A)$. Since B is abelian and $A \leqslant N_P(B)$, we have $N \trianglelefteq AB$. Moreover, $N < B$ because $B \nleqslant N_P(A)$. Let $\overline{AB} = AB/N$. Now $\overline{B} \trianglelefteq \overline{AB}$ and $\overline{B}$ is nontrivial. Since $\overline{AB}$ is a p-group, we have $\overline{B} \cap \mathcal{Z}(\overline{AB}) \neq 1$ by Theorem 1.15 and Lemma 1.18. Hence there exists a nontrivial $\overline{x} \in \overline{B} \cap \mathcal{Z}(\overline{AB})$ such that $[\overline{x}, \overline{A}] = 1$ and $[x, A] \leqslant N$. Let $M = [x, A]$. Now $M < B$ and M is abelian. By Theorem 5.5, $A^* = MC_A(M) \in A(P)$. Furthermore, $C_A(M) \leqslant N_P(A)$ and $M \leqslant N = N_B(A) \leqslant N_P(A)$. It follows that

$$A^* = MC_A(M) \leqslant N_P(A).$$

Since $\overline{x} \in \overline{B} \cap \mathcal{Z}(\overline{AB})$ is nontrivial, we have $x \notin N$ and $M = [x, A] \nleqslant A$. Now $x \in B$ and $x \in C_P(A \cap B)$. Also, $A \leqslant C_P(A \cap B)$ since A is abelian. Hence

$$M = [x, A] \leqslant C_P(A \cap B) \leqslant N_P(A \cap B),$$

and $M(A \cap B) \leqslant P$. However, $M \nleqslant A$, so $A \cap B < M(A \cap B) \leqslant A^* \cap B$. Therefore, $A \cap B < A^* \cap B$. $\square$

5.4 Glauberman Replacement Theorem

Definition 5.3. *Let G be a group, $H \leqslant G$, and $K \leqslant G$. Define $[H, K; 0] = H$, $[H, K; 1] = [[H, K; 0], K] = [H, K], [H, K; 2] = [[H, K; 1], K] = [H, K, K], \ldots,$ and inductively, $[H, K; n] = [[H, K; n-1], K]$.*

Definition 5.4. *Let G be a nilpotent group and $n+1$ be minimal such that the lower central series of G terminates at 1–that is, $K_{n+1}(G) = 1$. We say the **nilpotency class** of G is n and write $cl(G) = n$.*

Theorem 5.7. *Let $P = BA$ be a p-group, $B \trianglelefteq P$, A be abelian, $B' \leqslant \mathcal{Z}(P)$, $\overline{P} = P/B'$, and suppose n is minimal with respect to $[B, A; n]$ being abelian. Then*

(i) $K_i(\overline{P}) = [\overline{B}, \overline{A}; i-1]$ for all $i \geq 2$.

(ii) $[B, A; i+1] \leqslant [B, A; i]$ for all $i \geq 0$.

(iii) If $[B, A; n+1] = 1$, then $n \leq 2$ and $cl(P) \leq 4$.

Proof.

For (i), since B' char $B \trianglelefteq P$, we know $B' \trianglelefteq P$. By the Second and Third Isomorphism Theorems,

$$\frac{\overline{P}}{\overline{B}} \cong \frac{P}{B} = \frac{BA}{B} \cong \frac{A}{A \cap B},$$

and so $\overline{P}/\overline{B}$ is abelian. It follows that $K_i(\overline{P}/\overline{B}) = 1$ for all $i \geq 2$, which implies $K_i(\overline{P}) \leqslant \overline{B}$ for all $i \geq 2$. Moreover, $\overline{B}$ is abelian. Let $\overline{x} \in K_i(\overline{P}), \overline{a} \in \overline{A}$, and $\overline{b} \in \overline{B}$. By Theorem 5.3 and since $\overline{B}$ is abelian, we have $[\overline{b}\overline{a}, \overline{x}] = [\overline{b}, \overline{x}]^{\overline{a}}[\overline{a}, \overline{x}] = [\overline{a}, \overline{x}]$. Hence $[K_i(\overline{P}), \overline{P}] = [K_i(\overline{P}), \overline{A}]$ for all $i \geq 2$.

We proceed by induction on i. Suppose $i = 2$ and let $\overline{a} \in \overline{A}, \overline{b} \in \overline{B}$, and $\overline{x} \in \overline{P}$. Now $[\overline{a}\overline{b}, \overline{x}] = [\overline{a}, \overline{x}]^{\overline{b}}[\overline{b}, \overline{x}] = [\overline{a}, \overline{x}][\overline{b}, \overline{x}]$ since $[\overline{a}, \overline{x}] \in \overline{P}' = K_2(\overline{P}) \leqslant \overline{B}$. Thus $K_2(\overline{P}) = [\overline{P}, \overline{P}] = [\overline{A}, \overline{P}][\overline{B}, \overline{P}]$. Furthermore, $\overline{A}$ is abelian, $\overline{B} \trianglelefteq \overline{P}$, and $\overline{B'} = 1$. By Theorem 5.3, we have

$$[\overline{A}, \overline{P}] = [\overline{A}, \overline{B}\ \overline{A}] = [\overline{A}, \overline{A}][\overline{A}, \overline{B}]^{\overline{A}} = [\overline{A}, \overline{B}],$$

and

$$[\overline{B},\overline{P}] = [\overline{B},\overline{B}\ \overline{A}] = [\overline{B},\overline{A}][\overline{B},\overline{B}]^{\overline{A}} = [\overline{B},\overline{A}] = [\overline{A},\overline{B}].$$

Hence $K_2(\overline{P}) = \overline{P}' = [\overline{P},\overline{P}] = [\overline{B},\overline{A}] = [\overline{B},\overline{A};1]$. Assume $K_i(\overline{P}) = [\overline{B},\overline{A};i-1]$. Now

$$K_{i+1}(\overline{P}) = [K_i(\overline{P}),\overline{P}] = [K_i(\overline{P}),\overline{A}] = [[\overline{B},\overline{A};i-1],\overline{A}] = [\overline{B},\overline{A};i].$$

Therefore, (i) holds by induction.

For (ii), it is enough to show $A \leqslant N_P([B,A;i])$ for all $i \in \mathbb{N}_0$ and we proceed by induction on i. If $i = 0$, then $A \leqslant N_P(B) = N_P([B,A;0])$ since $B \trianglelefteq P$. Assume $A \leqslant N_P([B,A;i])$ and let $a \in A$. Now

$$[B,A;i+1]^a = [[B,A;i],A]^a = [[B,A;i]^a,A] = [[B,A;i],A] = [B,A;i+1],$$

so $A \leqslant N_P([B,A;i+1])$. Thus $A \leqslant N_P([B,A;i])$ for all $i \geq 0$. Therefore, $[B,A;i+1] = [[B,A;i],A] \leqslant [B,A;i]$ for all $i \geq 0$.

For (iii), if $[B,A;n+1] = 1$, then $[\overline{B},\overline{A};n+1] = 1$. By (i), we have $K_{n+2}(\overline{P}) = [\overline{B},\overline{A};n+1] = 1$, which implies $\overline{K_{n+2}(P)} = K_{n+2}(\overline{P}) = 1$. Hence $K_{n+2}(P) \leqslant B' \leqslant \mathcal{Z}(P)$ and $K_{n+3}(P) = [K_{n+2}(P),P] \leqslant [\mathcal{Z}(P),P] = 1$. Let $m = \lfloor \frac{1}{2}(n+4) \rfloor$. Since $n \geq 1$, we have $m \geq 2$, and by the definition of m, $2m \geq n+3$. Now $[K_m(P),K_m(P)] \leqslant K_{2m}(P) \leqslant K_{n+3}(P) = 1$, thus $K_m(P)$ is abelian and $K_m(\overline{P}) = \overline{K_m(P)}$ is abelian. By (i), $K_m(\overline{P}) = [\overline{B},\overline{A};m-1]$ is abelian and by the minimality of n, $n \leq m-1 \leq \frac{1}{2}(n+4) - 1 = \frac{1}{2}n + 1$. Now $n \leq \frac{1}{2}n + 1$ implies $n \leq 2$. Thus $K_{n+3}(P) = 1$ and $n \leq 2$. Therefore, $n+3 \leq 5$ and $cl(P) \leq 4$. $\square$

Theorem 5.8 (Glauberman Replacement Theorem)**.** *Let P be a p-group, p be odd, $B \trianglelefteq P$ such that $B' \leqslant \mathcal{Z}(J(P))$, $cl(B) \leq 2$, and suppose $A \in A(P)$ such that $B \nleqslant N_P(A)$. Then there exists $A^* \in A(P)$ such that*

(i) $A \cap B < A^* \cap B$.

(ii) $A^* \leqslant N_P(A)$.

Proof.

Use induction on $|P|$. Since $B \trianglelefteq P$, we have $AB \leqslant P$. If $AB < P$, then since $A \leqslant AB$, we have $A(AB) \subseteq A(P)$. By Theorem 5.2(ii), $J(AB) \leqslant J(P)$. Now $[\mathcal{Z}(J(P)), A] = 1$, so $\mathcal{Z}(J(P)) \leqslant C_P(A) = A$ by Theorem 5.1. It follows that $[J(AB), \mathcal{Z}(J(P))] = 1$ and since $\mathcal{Z}(J(P)) \leqslant A \leqslant J(AB)$, we have $\mathcal{Z}(J(P)) \leqslant \mathcal{Z}(J(AB))$. Thus $B' \leqslant \mathcal{Z}(J(AB))$. Moreover, $A \in A(AB)$ and $A \leqslant AB$. Since $B \trianglelefteq P$, we have $B \trianglelefteq AB$. By the induction hypothesis, there exists $A^* \in A(AB)$ such that $A \cap B < A^* \cap B$ and $A^* \leqslant N_{AB}(A) \leqslant N_P(A)$. Thus $A^* \in A(P)$ and we are done.

Without loss of generality, assume $P = AB$ and let n be chosen minimal with respect to $[B, A; n]$ being abelian.

Case 1: $[B, A; n+1] \neq 1$.

Let $r \in \mathbb{N}$ be minimal such that $[B, A; r] = 1$. Since $n \geq 1$, we have $r \geq n + 2 \geq 3$ by Theorem 5.7. By the minimality of r, $1 \neq [B, A; r-1] = [[B, A; r-2], A]$, so $A \nleqslant C_P([B, A; r-2])$. Hence there exists $x \in [B, A; r-3]$ such that $A \nleqslant C_P([x, A])$. Let $M = [x, A]$. Now $M \leqslant [B, A; r-2] \leqslant [B, A; n]$ and so M is abelian since $r-2 \geq n$. By Theorem 5.5, $A^* = MC_A(M) \in A(P)$. Now

$$[B, A \cap B, A] \leqslant [B', A] \leqslant [\mathcal{Z}(J(P)), A] = 1,$$

and $[A \cap B, A, B] \leqslant [A, A, B] = [1, B] = 1$ since A is abelian. By the Three Subgroups Lemma (5.6), $[A, B, A \cap B] = 1$, and it follows that $A \cap B \leqslant C_P([A, B]) \leqslant C_P([B, A; i])$ for all $i \geq 1$. Hence $A \cap B \leqslant C_P(M)$. Since A is abelian and $A \nleqslant C_P(M)$, we have $M \nleqslant A$, which implies $M \leqslant B$ because $P = AB$. Thus $A^* \cap B \geqslant M(A \cap B) > A \cap B$. By Lemma 5.5,

$$[A^*, A, A] = [MC_A(M), A, A] = [M, A, A] \leqslant [[B, A; r-2], A, A] = [B, A; r] = 1,$$

so $[A^*, A] \leqslant C_P(A) = A$. Therefore, $A^* \leqslant N_P(A)$.

Case 2: $[B, A; n+1] = 1$.

Since $cl(B) \leq 2$, we know $K_3(B) = 1, K_2(B) = 1$, or $K_1(B) = 1$. If $K_3(B) = 1$, then $[B, B, B] = [B', B] = 1$ and so $B' \leqslant \mathcal{Z}(B)$. In any case, $B' \leqslant \mathcal{Z}(J(AB)) = \mathcal{Z}(J(P))$. It follows from Theorem 5.7 that $n \leq 2$ and $cl(P) \leq 4$. If $n = 1$, then $[B, A; 2] = [B, A, A] = 1$, hence $[B, A] \leqslant C_P(A) = A$. This implies $B \leqslant N_P(A)$, which is a contradiction. Thus $n = 2$ and $[B, A; 3] = 1$.

Let $u, v \in A, x \in B$, and $w = [x, v] \in [B, A] \leqslant B$. By the Three Subgroups Lemma, $[x, u, w]^{u^{-1}}[u^{-1}, w^{-1}, x]^w[w^{-1}, x^{-1}, u^{-1}]^x = 1$. Since $B \trianglelefteq P$, all three commutators are contained in B' and $[w^{-1}, x^{-1}, u^{-1}] = 1$ since $B' \leqslant \mathcal{Z}(P)$. Hence $[x, u, w][u^{-1}, w^{-1}, x] = 1$. Since $[u^{-1}, w^{-1}]$ and $x \in B$, we have by (ix) and (iii) of Theorem 5.3,

$$[x, u, w] = [u^{-1}, w^{-1}, x]^{-1} = \left[[u^{-1}, w^{-1}]^{-1}, x\right] = [w^{-1}, u^{-1}, x]. \tag{4}$$

Let $\overline{P} = P/B'$. Now $[B, A; 3] = 1$ implies $[B, A, A] \leqslant C_P(A) = A$, and by Theorem 5.7, $K_i(\overline{P}) = [\overline{B}, \overline{A}; i-1] \leqslant \overline{B}$ for all $i \geq 2$. Thus $[\overline{B}, \overline{A}, \overline{A}] \leqslant \overline{A} \cap \overline{B}$ and $\overline{P} = \overline{A}\,\overline{B}$. Since $\overline{A}$ and $\overline{B}$ are abelian, we have $[\overline{B}, \overline{A}, \overline{A}] \leqslant \mathcal{Z}(\overline{A}\,\overline{B}) = \mathcal{Z}(\overline{P})$. By Theorem 5.3$(ix)$ and Lemma 5.2 with $[\overline{u}, \overline{v}] = 1$,

$$\left[[\overline{x}, \overline{v}]^{-1}, \overline{u}^{-1}\right] = \left[[\overline{x}, \overline{v}], \overline{u}^{-1}\right]^{-1} = \left([[\overline{x}, \overline{v}], \overline{u}]^{-1}\right)^{-1} = [\overline{x}, \overline{v}, \overline{u}] = [\overline{x}, \overline{u}, \overline{v}]. \tag{5}$$

From (4) and (5), we have

$$[\overline{w}^{-1}, \overline{u}^{-1}] = [[\overline{x}, \overline{u}], [\overline{x}, \overline{v}]] = [[\overline{x}, \overline{u}], \overline{w}] = [\overline{w}^{-1}, \overline{u}^{-1}, \overline{x}] = [[\overline{x}, \overline{u}, \overline{v}], \overline{x}]\,, \tag{6}$$

but interchanging $\overline{u}$ and $\overline{v}$ in (6) results in $[[\overline{x}, \overline{v}], [\overline{x}, \overline{u}]] = [[\overline{x}, \overline{v}, \overline{u}], \overline{x}] = [[\overline{x}, \overline{u}, \overline{v}], \overline{x}]$. Hence

$$[[\overline{x}, \overline{u}], [\overline{x}, \overline{v}]] = [[\overline{x}, \overline{v}], [\overline{x}, \overline{u}]] = [[\overline{x}, \overline{u}], [\overline{x}, \overline{v}]] = [[\overline{x}, \overline{u}], [\overline{x}, \overline{v}]]^{-1}\,.$$

It then follows from Theorem 5.3(ii), Lemma 5.5, and $B' \leqslant \mathcal{Z}(P)$ that

$$\begin{aligned}\left[\overline{[x,u]}, \overline{[x,v]}\right] &= \left[\overline{[x,u]}, \overline{[x,v]}\right]^{-1} \\ [[x,u]z_1, [x,v]z_2] &= [[x,u]z_3, [x,v]z_4]^{-1} \\ [[x,u],[x,v]] &= [[x,u],[x,v]]^{-1}.\end{aligned}$$

Thus $[[x,u],[x,v]]^2 = 1$. Because p is an odd prime, we have $[[x,u],[x,v]] = 1$, so $[x,A]$ is abelian for all $x \in B$. However, $B \nleqslant N_P(A)$ and $[B,A] \nleqslant A$, so there exists $x \in B$ such that $[x,A] \nleqslant A$.

Let $M = [x,A]$. Now M is abelian and by Theorem 5.5, $A^* = MC_A(M) \in A(P)$. As in Case 1, we have $A \cap B \leqslant C_P([B,A]) \leqslant C_P(M)$. Since $M \nleqslant A$, $A \cap B \leqslant C_A(M)$, and $B \trianglelefteq P$, we have $A^* \cap B \geqslant M(A \cap B) > A \cap B$. By Theorem 5.3,

$$[A^*, A, A] = [MC_A(M), A, A] = [M, A, A] \leqslant [B, A, A, A] = [B, A, 3] = 1.$$

Therefore, $[A^*, A] \leqslant C_P(A) = A$ and so $A^* \leqslant N_P(A)$. $\square$

6 p-Separability and p-Solvability

Definition 6.1. *Let G be a group. A* ***composition series*** *of G is a subnormal series of the form*

$$G = G_1 \trianglerighteq G_2 \trianglerighteq G_3 \trianglerighteq \cdots \trianglerighteq G_n = 1,$$

where G_i/G_{i+1} is simple for $1 \leq i \leq n-1$. The quotient groups G_i/G_{i+1} are called ***composition factors*** *of G.*

Definition 6.2. *Let G be a group and π be a set of primes.*

*(i) G is a π-**separable** group if every composition factor of G is a π-group or a π'-group.*

*(ii) G is a π-**solvable** group if every composition factor of G is a π'-group or a p-group for some $p \in \pi$.*

Similarly, we define p-separable and p-solvable groups when $\pi = \{p\}$.

The Jordan-Hölder Theorem (Theorem 2.8, pg. 6, [Gor07]) proves two composition series of a group are of the same length and the factors are unique up to isomorphism.

Theorem (Schreier)**.** *Let $A \trianglerighteq B \trianglerighteq C$ be a subnormal series, and suppose A/B and B/C are abelian. Then the series can be refined to a composition series*
$A \trianglerighteq D \trianglerighteq B \trianglerighteq C$, where the factors are simple and abelian.

Proof.

Theorem 2.7, pg. 6 in [Gor07]. □

Theorem 6.1. *Let G be a group. Then*

(i) G is π-separable if and only if G is π'-separable.

(ii) G is p-separable if and only if G is p-solvable for all $p \in \pi(G)$.

(iii) If G is π-solvable, then G is π-separable.

(iv) G is solvable if and only if G is p-solvable for all $p \in \pi(G)$.

Proof.

For (i), suppose G is π-separable. Now every composition factor of G is a π-group or a π'-group. Equivalently, every composition factor of G is a $(\pi')'$-group or a π'-group, respectively. Thus G is π'-separable.

For (ii), let $p \in \pi(G)$ and suppose G is p-separable. Now every composition factor of G is a p-group or a p'-group. Thus G is p-solvable. The converse is trivial.

For (iii), suppose G is π-solvable. Now every composition factor of G is a π'-group or a p-group for some $p \in \pi$. Since a p-group is a π-group for $p \in \pi$, we have G is π-separable.

For (iv), suppose G is solvable and let $p \in \pi(G)$. Now there exists a subnormal series $G = H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_m = 1$, where H_i/H_{i+1} is abelian for $1 \leq i \leq m-1$. By Schreier's Theorem, we can refine to a composition series $G = G_1 \trianglerighteq \cdots \trianglerighteq G_n = 1$, where G_i/G_{i+1} is simple and abelian for $1 \leq i \leq n-1$. Then G_i/G_{i+1} is cyclic of prime order for $1 \leq i \leq n-1$, which implies for every $1 \leq i \leq n-1$, there exists a prime p_i such that G_i/G_{i+1} is a p_i-group. Moreover, for every $1 \leq i \leq n-1$, either $p_i = p$ or $p_i \neq p$. Thus all composition factors are p-groups or p'-groups. Therefore, G is p-solvable.

Conversely, let $G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1$ be a composition series of G, where each factor is simple and for all $1 \leq i \leq n-1$, G_i/G_{i+1} is a p-group or a p'-group for all $p \in \pi(G)$. Since $[G_i : G_{i+1}]$ divides $|G|$ for all $1 \leq i \leq n-1$, there exists $p_i \in \pi(G)$ such that G_i/G_{i+1} is a p_i-group. Let $\overline{G_i} = G_i/G_{i+1}$ for each $1 \leq i \leq n-1$. Since $\overline{G_i}$ is a p_i-group, we know $\overline{G_i}$ is solvable. It follows that there exists a subnormal series $\overline{G_i} = \overline{G_{i1}} \trianglerighteq \overline{G_{i2}} \trianglerighteq \cdots \trianglerighteq \overline{G_{ik_i}} = 1, (k_i \in \mathbb{N})$ such that $\overline{G_{ij}}/\overline{G_{i(j+1)}} \cong G_{ij}/G_{i(j+1)}$ is abelian for all $1 \leq i \leq n-1$ and for all $1 \leq j \leq k_i - 1$. Hence we have a subnormal series

$$G = G_{11} \trianglerighteq G_{12} \trianglerighteq \cdots \trianglerighteq G_2 = G_{21} \trianglerighteq G_{22} \trianglerighteq \cdots \trianglerighteq G_3 \trianglerighteq \cdots$$
$$\trianglerighteq G_{n-1} = G_{(n-1)1} \trianglerighteq G_{(n-1)2} \trianglerighteq \cdots \trianglerighteq G_n = 1,$$

and

$$\frac{G_{ij}}{G_{i(j+1)}} \cong \frac{G_{ij}/G_{j+1}}{G_{i(j+1)}/G_{j+1}}$$

is abelian for all $1 \leq i \leq n-1$ and for all $1 \leq j \leq k_i - 1$. Therefore, G is solvable. $\square$

Definition 6.3. *Let G be a group and π be a set of primes. Define the unique maximal normal π-subgroup of G by*

$$\mathcal{O}_\pi(G) = \prod_{P \trianglelefteq G} P,$$

where P is a π-group. We can similarly define $\mathcal{O}_{\pi'}(G)$.

Lemma 6.1. *Let G be a group and π be a set of primes. Then $\mathcal{O}_\pi(G)$ char G.*

Proof.

Let $\phi \in Aut(G)$ and $Q \trianglelefteq G$ be a π-subgroup. Now $Q^\phi \trianglelefteq G$ and Q^ϕ is a π-group. Thus $Q^\phi \leqslant \mathcal{O}_\pi(G)$ and $\mathcal{O}_\pi(G)$ char G. $\square$

Definition 6.4. *Let G be a group and π be a set of primes. Define*

$$\mathcal{O}_{\pi'}\left(\frac{G}{\mathcal{O}_\pi(G)}\right) = \frac{\mathcal{O}_{\pi,\pi'}(G)}{\mathcal{O}_\pi(G)}, \quad \mathcal{O}_\pi\left(\frac{G}{\mathcal{O}_{\pi,\pi'}(G)}\right) = \frac{\mathcal{O}_{\pi,\pi',\pi}(G)}{\mathcal{O}_{\pi,\pi'}(G)}, \ldots,$$

*and so on. The π-**series** of G is the normal series*

$$1 \trianglelefteq \mathcal{O}_\pi(G) \trianglelefteq \mathcal{O}_{\pi,\pi'}(G) \trianglelefteq \mathcal{O}_{\pi,\pi',\pi}(G) \trianglelefteq \cdots .$$

Lemma 6.2. *Let G be a group. Then $\mathcal{O}_\pi(G/\mathcal{O}_\pi(G)) = 1$.*

Proof.

Suppose $H/\mathcal{O}_\pi(G) \trianglelefteq G/\mathcal{O}_\pi(G)$ is a π-subgroup. Now $H \trianglelefteq G$ and

$$|H| = \frac{|H|}{|\mathcal{O}_\pi(G)|} \cdot |\mathcal{O}_\pi(G)|,$$

so H is a π-group. Thus $H \leqslant \mathcal{O}_\pi(G)$ and $H/\mathcal{O}_\pi(G) = 1$. Therefore, $\mathcal{O}_\pi(G/\mathcal{O}_\pi(G)) = 1$. $\square$

Theorem 6.2. *Let G be a group and π be a set of primes.*

(i) If G is π-separable and N is a minimal normal subgroup of G, then N is a π-group or a π'-group.

(ii) If G is π-separable, $H \leqslant G$, and $N \trianglelefteq G$, then H and G/N are π-separable.

(iii) If G is π-solvable, $H \leqslant G$, and $N \trianglelefteq G$, then H and G/N are π-solvable.

(iv) G is π-separable if and only if the π-series terminates at G.

Proof.

For (i), since N is a minimal normal subgroup, we know N is characteristically simple. By Theorem 1.13, $N \cong \bigotimes_{i=1}^{n} N_i$, where the N_i's are simple isomorphic groups. Refine the series $N_1 \trianglerighteq 1$ to a composition series of G,

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_m = N_1 \trianglerighteq 1.$$

Since G is π-separable, $N_1 \cong N_1/\{1\}$ is either a π-group or a π'-group. Thus $N = \bigotimes_{i=1}^{n} N_i$ is either a π-group or a π'-group.

For (ii), let $N = N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_m = 1$ be a composition series of N and refine to a composition series of G,

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_k = N = N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_m = 1.$$

Let $\overline{G} = G/N$. Now

$$\overline{G} = \overline{G_1} \trianglerighteq \overline{G_2} \trianglerighteq \cdots \trianglerighteq \overline{G_k} = 1$$

is a composition series of $\overline{G}$. If G is π-separable, then $\overline{G_i}/\overline{G_{i+1}} \cong G_i/G_{i+1}$ is a π-group or a π'-group for each $1 \leq i \leq k-1$. Thus $\overline{G}$ is π-separable.

If $H = G$, then we are done. Assume $H < G$ and proceed by induction on $|G|$. Let N be a minimal normal subgroup of G and $\overline{G} = G/N$. If G is π-separable, then $\overline{G}$ is π-separable by the above. Now $\overline{H} < \overline{G}$ and so by induction, $\overline{H}$ is π-separable. Let $\overline{H} = \overline{H}_1 \trianglerighteq \overline{H}_2 \trianglerighteq \cdots \trianglerighteq \overline{H}_k = 1$ be a composition series of $\overline{H}$. Since $\overline{H} \cong HN/N \cong H/H \cap N$, we have $H = H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H \cap N$ and it remains to show $H \cap N$ is π-separable. By (i), N is a π-group or a π'-group, so $H \cap N$ is a π-group or a π'-group, respectively. This implies any composition factor of $H \cap N$ is a π-group or a π'-group. Thus $H \cap N$ is π-separable. Therefore, H is π-separable.

For (iii), let $N = N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_m = 1$ be a composition series of N and refine to a composition series of G,

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_k = N = N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_m = 1.$$

Let $\overline{G} = G/N$. Now

$$\overline{G} = \overline{G_1} \trianglerighteq \overline{G_2} \trianglerighteq \cdots \trianglerighteq \overline{G_k} = 1$$

is a composition series of $\overline{G}$. If G is π-solvable, then $\overline{G_i}/\overline{G_{i+1}} \cong G_i/G_{i+1}$ is a π'-group or a p-group for some $p \in \pi$ for each $1 \leq i \leq k-1$. Thus $\overline{G}$ is π-solvable.

If $H = G$, then we are done. Assume $H < G$ and proceed with induction on $|G|$. Let N be a minimal normal subgroup of G and $\overline{G} = G/N$. If G is π-solvable, then $\overline{G}$ is π-solvable. Now $\overline{H} < \overline{G}$ and so by induction, $\overline{H}$ is π-solvable. As before, since $\overline{H} \cong HN/N \cong H/H \cap N$, it remains to show $H \cap N$ is π-solvable. Again by (i), N is a π-group or a π'-group. If N is a π-group, then N is π-solvable since $N \trianglelefteq G$. Thus N is a p-group for some $p \in \pi$ and $H \cap N$ is a p-group. Thus all composition factors of $H \cap N$ are p-groups. If N is a π'-group, then $H \cap N$ is a π'-group and so are all the composition factors of $H \cap N$. Hence $H \cap N$ is π-solvable. Therefore, H is π-solvable.

For (iv), suppose the π-series terminates at G. Refine the normal series

$$1 \trianglelefteq \mathcal{O}_\pi(G) \trianglelefteq \mathcal{O}_{\pi,\pi'}(G) \trianglelefteq \mathcal{O}_{\pi,\pi',\pi}(G) \trianglelefteq \cdots \trianglelefteq G, \tag{7}$$

to a composition series of G,

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1. \tag{8}$$

Since all the factors in (7) are π-groups or π'-groups, the same is true for all factors in (8). Thus G is π-separable. Conversely, suppose G is π-separable, but the π-series does not terminate at G. Consider a case where $\mathcal{O}_\pi(G) = \mathcal{O}_{\pi,\pi'}(G)$. Now

$\mathcal{O}_{\pi'}(G/\mathcal{O}_\pi(G)) = \mathcal{O}_{\pi,\pi'}(G)/\mathcal{O}_\pi(G) = 1$ and $\mathcal{O}_\pi(G/\mathcal{O}_\pi(G)) = 1$. Thus there exists $L \trianglelefteq G$ such that $\mathcal{O}_\pi(G/L) = \mathcal{O}_{\pi'}(G/L) = 1$. Let $\overline{G} = G/L$ and $\overline{N}$ be a minimal normal subgroup of $\overline{G}$. By (ii), $\overline{G}$ is π-separable since G is π-separable and by (i), $\overline{N}$ is a π-group or a π'-group. Since $\overline{N} \trianglelefteq \overline{G}$, we have $\overline{N} \leqslant \mathcal{O}_\pi(\overline{G}) \cup \mathcal{O}_{\pi'}(\overline{G}) = 1$. This implies $\overline{N} = 1$, a contradiction. Therefore, the π-series must terminate at G. □

Theorem 6.3. *Let G be a π-separable group. If $\mathcal{O}_{\pi'}(G) = 1$, then*

$$C_G(\mathcal{O}_\pi(G)) \leqslant \mathcal{O}_\pi(G).$$

Proof.

Let $H = \mathcal{O}_\pi(G), C = C_G(H)$, and suppose $C \nleqslant H$. Since $H \trianglelefteq G$, we have $C \trianglelefteq G$, and since $\mathcal{O}_\pi(C)$ char $C \trianglelefteq G$, we have $\mathcal{O}_\pi(C) \trianglelefteq G$. Now $\mathcal{O}_\pi(C) \leqslant H = \mathcal{O}_\pi(G)$ and $\mathcal{O}_\pi(C) \leqslant \mathcal{Z}(H)$ because $[\mathcal{O}_\pi(C), H] = 1$. Since $\mathcal{Z}(H)$ char $H \trianglelefteq G$, we have $\mathcal{Z}(H) \trianglelefteq G$. Now $[H, \mathcal{Z}(H)] = 1$ implies $\mathcal{Z}(H) \leqslant C$. Thus $\mathcal{Z}(H) \trianglelefteq C$, but $\mathcal{Z}(H)$ is a π-group. Therefore, $\mathcal{Z}(H) \leqslant \mathcal{O}_\pi(C)$ and $\mathcal{O}_\pi(C) = \mathcal{Z}(H)$.

Since G is π-separable, C is π-separable by Theorem 6.2. It follows from $C \nleqslant H$ and $\mathcal{O}_\pi(C) \leqslant H$ that $\mathcal{O}_\pi(C) < C$. Thus $\mathcal{O}_\pi(C) < \mathcal{O}_{\pi,\pi'}(C)$. Let $L = \mathcal{O}_{\pi,\pi'}(C)$. Now $L/\mathcal{O}_\pi(C) = \mathcal{O}_{\pi'}(C/\mathcal{O}_\pi(C))$ is a π'-group, hence $\mathcal{O}_\pi(C) \in Hall_\pi(L)$ and $\mathcal{O}_\pi(C) \trianglelefteq L$. By Schur-Zassenhaus Part 1, L splits over $\mathcal{O}_\pi(C)$, so there exists $K \leqslant L$ such that $L = K\mathcal{O}_\pi(C)$ and $K \cap \mathcal{O}_\pi(C) = 1$. Now

$$|K| = \frac{|K|}{1} = \frac{|K|}{|K \cap \mathcal{O}_\pi(C)|} = \frac{|K\mathcal{O}_\pi(C)|}{|\mathcal{O}_\pi(C)|} = \frac{|L|}{|\mathcal{O}_\pi(C)|},$$

and so K is a π'-group. In addition,

$$\frac{|L|}{|K|} = \frac{|K\mathcal{O}_\pi(C)|}{|K|} = \frac{|\mathcal{O}_\pi(C)|}{|K \cap \mathcal{O}_\pi(C)|},$$

so $K \in Hall_{\pi'}(L)$. Moreover, $[K, \mathcal{O}_\pi(C)] \leqslant [C, \mathcal{O}_\pi(C)] = [C, \mathcal{Z}(H)] = 1$ and $K \trianglelefteq K\mathcal{O}_\pi(C) = L$. By Lemma 4.6, K char L. Since $L \trianglelefteq G$, we have $K \trianglelefteq G$ and it follows that $K \leqslant \mathcal{O}_{\pi'}(G) = 1$. Then $L = \mathcal{O}_\pi(C)$, which is a contradiction. Therefore, $C_G(\mathcal{O}_\pi(G)) \leqslant \mathcal{O}_\pi(G)$. □

Theorem 6.4. *Let G be a p-solvable group and $P \in Syl_p(G)$. Then*

$$C_G(P \cap \mathcal{O}_{p',p}(G)) \leqslant \mathcal{O}_{p',p}(G).$$

Proof.

Let $\overline{G} = G/\mathcal{O}_{p'}(G)$ and $\overline{K} = \mathcal{O}_{p'}(\overline{G})$. By Lemma 6.2, $\overline{K} = 1$. Since G is p-solvable, we have $\overline{G}$ is p-separable by Theorem 6.1(ii). It follows from Theorem 6.3 that $C_{\overline{G}}(\mathcal{O}_p(\overline{G})) \leqslant \mathcal{O}_p(\overline{G})$. Since $\mathcal{O}_{p',p}(G) \trianglelefteq G$, we have $P \cap \mathcal{O}_{p',p}(G) \in Syl_p(\mathcal{O}_{p',p}(G))$. Let $L = \mathcal{O}_{p',p}(G)$. Now $\overline{L} = \overline{\mathcal{O}_{p',p}(G)} = \mathcal{O}_p(\overline{G})$ is a p-group, so $\overline{P \cap L} = \overline{L} = \mathcal{O}_p(\overline{G})$. Thus

$$\overline{C_G(P \cap L)} \leqslant C_{\overline{G}}(\overline{P \cap L}) = C_{\overline{G}}(\mathcal{O}_p(\overline{G})) \leqslant \mathcal{O}_p(\overline{G}) = \overline{L},$$

which implies

$$C_G(P \cap L)\mathcal{O}_{p'}(G) \leqslant L\mathcal{O}_{p'}(G) = \mathcal{O}_{p',p}(G)\mathcal{O}_{p'}(G) = \mathcal{O}_{p',p}(G).$$

Therefore, $C_G(P \cap L) = C_G(P \cap \mathcal{O}_{p',p}(G)) \leqslant \mathcal{O}_{p',p}(G)$. □

6.1 p-Constrained and p-Stability

Definition 6.5. *Let G be a group and p be a prime. Then G is p-**constrained** if*

$$C_G(P) \leqslant \mathcal{O}_{p',p}(G),$$

for all $P \in Syl_p(\mathcal{O}_{p',p}(G))$.

Theorem 6.5. *Let G be a p-constrained group.*

(i) *If $\mathcal{O}_{p'}(G) < G$, then $\mathcal{O}_{p'}(G) < \mathcal{O}_{p',p}(G)$.*

(ii) *Let $\overline{G} = G/\mathcal{O}_{p'}(G)$. Then $C_{\overline{G}}(\mathcal{O}_p(\overline{G})) \leqslant \mathcal{O}_p(\overline{G})$.*

(iii) *If $P \in Syl_p(\mathcal{O}_{p',p}(G))$ and $Q \leqslant G$ is a p'-subgroup such that P acts on Q, then $Q \leqslant \mathcal{O}_{p'}(G)$.*

Proof.

For (i), suppose $\mathcal{O}_{p'}(G) < G$. If $\mathcal{O}_{p',p}(G) = \mathcal{O}_{p'}(G)$, then $\mathcal{O}_{p',p}(G)$ is a p'-group and $\{1\} \in Syl_p(\mathcal{O}_{p',p}(G))$. Since G is p-constrained, $C_G(\{1\}) \leqslant \mathcal{O}_{p',p}(G) = \mathcal{O}_{p'}(G)$. However, $C_G(\{1\}) = G$, so $G \leqslant \mathcal{O}_{p',p}(G)$. This implies $G = \mathcal{O}_{p'}(G)$, which is a contradiction. Therefore, $\mathcal{O}_{p'}(G) < \mathcal{O}_{p',p}(G)$.

For (ii), let $P \in Syl_p(\mathcal{O}_{p',p}(G))$. Now $\overline{P} \in Syl_p(\overline{\mathcal{O}_{p',p}(G)})$, but $\overline{\mathcal{O}_{p',p}(G)}$ is a p-group. Thus $\overline{P} = \overline{\mathcal{O}_{p',p}(G)}$ and $P\mathcal{O}_{p'}(G) = \mathcal{O}_{p',p}(G)$. Since $\mathcal{O}_{p',p}(G) \trianglelefteq G$, we have by the Frattini Argument, $G = N_G(P)\mathcal{O}_{p',p}(G) = N_G(P)P\mathcal{O}_{p'}(G) = N_G(P)\mathcal{O}_{p'}(G)$. Hence $\overline{G} = \overline{N_G(P)}$. Then there exists $C \leqslant N_G(P)$ such that

$$\overline{C} = C_{\overline{G}}(\overline{P}) = C_{\overline{G}}(\overline{\mathcal{O}_{p',p}(G)}) = C_{\overline{G}}(\mathcal{O}_p(\overline{G})).$$

Now $[\overline{P}, \overline{C}] = 1$ implies $[P, C] \leqslant \mathcal{O}_{p'}(G)$, and we have $[P, C] \leqslant P$ since $C \leqslant N_G(P)$. Thus $[P, C] \leqslant P \cap \mathcal{O}_{p'}(G) = 1$ and $C \leqslant C_G(P) \leqslant \mathcal{O}_{p',p}(G)$ since G is p-constrained. Therefore, $\overline{C} = C_{\overline{G}}(\mathcal{O}_p(\overline{G})) \leqslant \overline{\mathcal{O}_{p',p}(G)} = \mathcal{O}_p(\overline{G})$.

For (iii), let $\overline{G} = G/\mathcal{O}_{p'}(G), P \in Syl_p(\mathcal{O}_{p',p}(G))$, and $Q \leqslant G$ be a p'-subgroup such that $P \leqslant N_G(Q)$. By the same argument as in (ii), $\overline{P} = \overline{\mathcal{O}_{p',p}(G)} = \mathcal{O}_p(\overline{G}) \trianglelefteq \overline{G}$. Now $\overline{P} \leqslant \overline{N_G(Q)} \leqslant N_{\overline{G}}(\overline{Q})$ and $[\overline{P}, \overline{Q}] \leqslant \overline{P} \cap \overline{Q} = 1$. It follows from (ii) that

$$\overline{Q} \leqslant C_{\overline{G}}(\overline{P}) = C_{\overline{G}}(\mathcal{O}_p(\overline{G})) \leqslant \mathcal{O}_p(\overline{G}).$$

Consequently, $\overline{Q} = 1$ since $\mathcal{O}_p(\overline{G})$ is a p-group. Therefore, $Q \leqslant \mathcal{O}_{p'}(G)$. □

Definition 6.6. *Let G be a group and p be a prime. Then G is called p-**stable** if*

(i) *p is odd.*

(ii) *$\mathcal{O}_p(G) \neq 1$.*

(iii) *Whenever $P \leqslant G$ is a p-subgroup, $P\mathcal{O}_{p'}(G) \trianglelefteq G$, $A \leqslant N_G(P)$, and A is a p-group acting quadratically on P, it follows that*

$$\frac{AC_G(P)}{C_G(P)} \leqslant \mathcal{O}_p\left(\frac{N_G(P)}{C_G(P)}\right).$$

Lemma 6.3. *Let G be a group, $N \trianglelefteq G, L \trianglelefteq G$, $L \leqslant N$, and L be a p-group. If $\mathcal{O}_p(G/N) = 1$, then $\mathcal{O}_p(G/L) \leqslant N/L$.*

Proof.

Let $\overline{G} = G/L$ and $\overline{U} = \mathcal{O}_p(\overline{G})$. Now $\overline{U} \trianglelefteq \overline{G}$, $U \trianglelefteq G$, and

$$|U| = \frac{|U|}{|L|} \cdot |L| = |\overline{U}| \cdot |L|,$$

so U is a p-group. Since $U \trianglelefteq G$, we have $UN/N \trianglelefteq G/N$ and $[UN : N] = [U : U \cap N]$. Thus UN/N is a p-group and $UN/N \leqslant \mathcal{O}_p(G/N) = 1$, which implies $U \leqslant UN \leqslant N$. Therefore, $\overline{U} = \mathcal{O}_p(\overline{G}) \leqslant \overline{N}$. $\square$

Theorem 6.6. *Let G be a group, p be a prime such that G is p-stable and p-constrained, $P \in Syl_p(G)$, $A \trianglelefteq P$, and suppose A is abelian. Then $A \leqslant \mathcal{O}_{p',p}(G)$.*

Proof.

Let $Q = P \cap \mathcal{O}_{p',p}(G)$. By Lemma 1.8, $Q \in Syl_p(\mathcal{O}_{p',p}(G))$. Let $\overline{G} = G/\mathcal{O}_{p'}(G)$. Now $\overline{Q} \in Syl_p(\overline{\mathcal{O}_{p',p}(G)})$, but $\overline{\mathcal{O}_{p',p}(G)} = \mathcal{O}_p(\overline{G})$, so $\overline{\mathcal{O}_{p',p}(G)}$ is a p-group. Thus $\overline{Q} = \overline{\mathcal{O}_{p',p}(G)} = \mathcal{O}_p(\overline{G})$ and $\mathcal{O}_{p',p}(G) = Q\mathcal{O}_{p'}(G) \trianglelefteq G$. Now $Q \trianglelefteq P$ since $\mathcal{O}_{p',p}(G) \trianglelefteq G$, and so $A \leqslant N_G(Q)$. Moreover, $[Q, A, A] \leqslant [A, A] = 1$, which means A acts quadratically on Q. It follows from the p-stability of G that

$$\frac{AC_G(Q)}{C_G(Q)} \leqslant \mathcal{O}_p\left(\frac{N_G(Q)}{C_G(Q)}\right). \tag{9}$$

Furthermore, G is p-constrained, $C_G(Q) \leqslant \mathcal{O}_{p',p}(G) = Q\mathcal{O}_{p'}(G)$, and $\overline{C_G(Q)} \leqslant \overline{\mathcal{O}_{p',p}(G)} = \overline{Q}$. By the Frattini Argument,

$$G = N_G(Q)Q\mathcal{O}_{p'}(G) = N_G(Q)\mathcal{O}_{p'}(G).$$

Therefore, $\overline{G} = \overline{N_G(Q)}$.

Let $\widetilde{N_G(Q)} = N_G(Q)/C_G(Q)$ and $\widetilde{U} = \mathcal{O}_p(\widetilde{N_G(Q)})$. Now $\widetilde{U} \trianglelefteq \widetilde{N_G(Q)}$, so $U \trianglelefteq N_G(Q)$. Let $U_0 \in Syl_p(U)$. By Lemma 1.8, $\widetilde{U_0} \in Syl_p(\widetilde{U})$, but $\widetilde{U}$ is a p-group. Hence $\widetilde{U_0} = \widetilde{U}$ and $U = U_0C_G(Q)$. Then $\overline{U} = \overline{U_0}\,\overline{C_G(Q)}$ and by the Second Isomorphism Theorem,

$$\frac{\overline{U}}{\overline{C_G(Q)}} = \frac{\overline{U_0}\,\overline{C_G(Q)}}{\overline{C_G(Q)}} \cong \frac{\overline{U_0}}{\overline{U_0 \cap C_G(Q)}},$$

which implies $\overline{U}/\overline{C_G(Q)}$ is a p-group. Furthermore, $\overline{U} \trianglelefteq \overline{N_G(Q)} = \overline{G}$ and

$$\frac{\overline{U}}{\overline{C_G(Q)}} \trianglelefteq \frac{\overline{N_G(Q)}}{\overline{C_G(Q)}} = \frac{\overline{G}}{\overline{C_G(Q)}}.$$

Thus $\overline{U}/\overline{C_G(Q)} \leqslant \mathcal{O}_p(\overline{N_G(Q)}/\overline{C_G(Q)})$. By (9), we have $AC_G(Q) \leqslant U$ and so $\overline{AC_G(Q)} \leqslant \overline{U}$. Also, $\overline{Q} \trianglelefteq \overline{N_G(Q)}$ and $\mathcal{O}_p(\overline{N_G(Q)}/\overline{Q}) = \mathcal{O}_p(\overline{G}/\mathcal{O}_p(\overline{G})) = 1$ by Lemma 6.2. And from Lemma 6.3,

$$\frac{\overline{AC_G(Q)}}{\overline{C_G(Q)}} \leqslant \frac{\overline{U}}{\overline{C_G(Q)}} \leqslant \mathcal{O}_p\left(\frac{\overline{N_G(Q)}}{\overline{C_G(Q)}}\right) = \mathcal{O}_p\left(\frac{\overline{G}}{\overline{C_G(Q)}}\right) \leqslant \frac{\overline{Q}}{\overline{C_G(Q)}}.$$

Therefore, $\overline{A} \leqslant \overline{A}\,\overline{C_G(Q)} \leqslant \overline{Q}$ and $A \leqslant A\mathcal{O}_{p'}(G) \leqslant Q\mathcal{O}_{p'}(G) = \mathcal{O}_{p',p}(G)$. $\square$

Theorem 6.7. *Let G be a p-stable group, $B \trianglelefteq G$ be a p-subgroup, and $P \in Syl_p(G)$. Then $B \cap \mathcal{Z}(J(P)) \trianglelefteq G$.*

Proof.

Let G be a counterexample such that $|B|$ is minimal and Let $B_1 = \langle (Z \cap B)^G \rangle$ be the normal closure of $Z \cap B$, where $Z = \mathcal{Z}(J(P))$. Since $B \trianglelefteq G$, we have $B_1 \leqslant B$, B_1 is a p-group, and $B_1 \trianglelefteq G$. If $B_1 < B$, then $B_1 \cap Z \trianglelefteq G$ by the minimality of $|B|$. By the definition of B_1, we have $Z \cap B = Z \cap B_1$, so $Z \cap B \trianglelefteq G$. This is a contradiction since B is a counterexample. Therefore, $B = B_1$. Now B' char $B \trianglelefteq G$ and $B' \trianglelefteq G$ by Lemma 1.12. Also, B' is a p-group and by Theorem 1.18, $B' = K_2(B) < B$ since B is nilpotent. By the minimality of $|B|$, $Z \cap B' \trianglelefteq G$.

We claim $B' \leqslant Z$. Now Z char $J(P)$ char P, Z char P, and by Lemma 1.12, $Z \trianglelefteq P$. Since B is a normal p-group, we have $B \leqslant P$ from Sylow. It follows that $[Z \cap B, B] \leqslant Z \cap [B, B] = Z \cap B'$. Let $g \in G$. By the above,

$$[(Z \cap B)^g, B] = [Z \cap B, B]^g \leqslant (Z \cap B')^g \leqslant Z \cap B',$$

so $B' = [B, B] = [B, B_1] = [B, \langle (Z \cap B)^G \rangle] \leqslant Z \cap B'$. Therefore, $B' = Z \cap B'$ and $B' \leqslant Z$. Moreover, $[Z \cap B, B'] \leqslant [Z, Z] = 1$ and

$$[B, B'] = [B_1, B'] = [\langle (Z \cap B)^G \rangle, B'] \leqslant [Z, Z] = 1.$$

Thus $cl(B) \leqslant 2$.

Let $L \trianglelefteq G$ such that $L \leqslant N_G(Z \cap B)$ and $|L|$ is maximal. Now $P \cap L \in Syl_p(L)$ and by the Frattini Argument, $G = N_G(P \cap L)L$. If $J(P) \leqslant P \cap L$, then by Theorem 5.2(i), $J(P)$ char $P \cap L$. This implies $N_G(P \cap L) \leqslant N_G(J(P))$ and $G = N_G(J(P))L$. Similarly, since $Z = \mathcal{Z}(J(P))$ char $J(P)$, we have $N_G(J(P)) \leqslant N_G(Z)$ and $G = N_G(Z)L$. Hence $Z \cap B \trianglelefteq N_G(Z)L = G$, which is a contradiction. Therefore, $J(P) \nleqslant P \cap L$.

By the Glauberman Replacement Theorem (5.8), there exists $A \in A(P)$ such that $[B, A, A] \leqslant [A, A] = 1$. Furthermore, G is p-stable, $B\mathcal{O}_{p'}(G) \trianglelefteq G$, and B is a p-group. Consequently,

$$\frac{AC_G(B)}{C_G(B)} \leqslant \mathcal{O}_p\left(\frac{N_G(B)}{C_G(B)}\right) \leqslant \mathcal{O}_p\left(\frac{G}{C_G(B)}\right). \tag{10}$$

Since $B \trianglelefteq G$, we have $C_G(B) \trianglelefteq G$. Now $L \leqslant LC_G(B) \trianglelefteq G$, but $LC_G(B) \leqslant N_G(Z \cap B)$. By the maximality of $|L|$, $L = LC_G(B)$ and it follows that $C_G(B) \leqslant L$.

We claim $AL/L \leqslant \mathcal{O}_p(G/L)$. Let $\widetilde{G} = G/C_G(B)$ and $\widetilde{U} = \mathcal{O}_p(\widetilde{G})$. Now $\widetilde{U} \trianglelefteq \widetilde{G}$ and $U \trianglelefteq G$. Let $U_0 \in Syl_p(U)$. Then $\widetilde{U_0} \in Syl_p(\widetilde{U})$, but $\widetilde{U}$ is a p-group. Thus $\widetilde{U_0} = \widetilde{U}$ and $U = U_0C_G(B) \trianglelefteq G$. By (10), $A \leqslant U \trianglelefteq G$, so $AL/L \leqslant UL/L \trianglelefteq G/L$. Moreover,

$$\frac{UL}{L} = \frac{U_0C_G(B)L}{L} = \frac{U_0L}{L} \cong \frac{U_0}{U_0 \cap L},$$

and UL/L is a p-group. Therefore, $AL/L \leqslant UL/L \leqslant \mathcal{O}_p(G/L)$.

Let $\overline{G} = G/L$ and $\overline{K} = \mathcal{O}_p(\overline{G})$. Now $L \leqslant K \trianglelefteq G$ and $P \cap K \in Syl_p(K)$. Then $\overline{P \cap K} \in Syl_p(\overline{K})$, but since $\overline{K}$ is a p-group, $\overline{P \cap K} = \overline{K}$. Thus $K = (P \cap K)L$. It follows from $Z \trianglelefteq P$ and $B \trianglelefteq G$ that $K = (P \cap K)L \leqslant N_G(Z \cap B)$. By the maximality of $|L|$, we have $K = L$ and $\overline{K} = \mathcal{O}_p(\overline{G}) = 1$.

Since $\overline{A} \leqslant \mathcal{O}_p(\overline{G}) = 1$, we have $A \leqslant L$ and $A \leqslant P \cap L$, so $A \in A(P \cap L)$. By Theorem 5.2(ii), $A \leqslant J(P \cap L)$ and $J(P \cap L) \leqslant J(P)$. Thus by Theorem 5.1,

$$Z \cap B = \mathcal{Z}(J(P)) \cap B \leqslant C_P(A) = A \leqslant J(P \cap L) \leqslant J(P),$$

and $Z \cap B \leqslant \mathcal{Z}(J(P \cap L))$. Let $X = \mathcal{Z}(J(P \cap L))$. Since X char $P \cap L$, we have

$N_G(P \cap L) \leqslant N_G(X)$. But $G = N_G(P \cap L)L$ and so $G = N_G(X)L$. Hence

$$B = B_1 = \langle (Z \cap B)^G \rangle = \langle (Z \cap B)^{N_G(X)L} \rangle = \langle (Z \cap B)^{N_G(X)} \rangle \leqslant \langle X^{N_G(X)} \rangle \leqslant X.$$

Since $J(P) \nleqslant P \cap L$, there exists $A_1 \in A(P)$ such that $A_1 \nleqslant P \cap L$. This implies $A_1 \nleqslant L$, thus $[B, A_1, A_1] \neq 1$.

Let $A_1 \in A(P)$ such that $A_1 \nleqslant L$ and $|A_1 \cap B|$ is maximal. By the above, $[B, A_1, A_1] \neq 1$, so $B \nleqslant N_G(A_1)$. By the Thompson Replacement Theorem (5.6), there exists $A^* \in A(P)$ such that $A_1 \cap B < A^* \cap B$ and $A^* \leqslant N_G(A_1)$. Now $A^* \leqslant L$ by the maximality of $|A_1 \cap B|$, which implies $A^* \leqslant P \cap L$, so $A^* \leqslant J(P \cap L)$. Thus $B \leqslant X \leqslant C_P(A^*) = A^* \leqslant N_G(A_1)$ and $[B, A_1, A_1] = 1$, which is a contradiction. Therefore, no such counterexample G exists. □

Lemma 6.4. *Let G be a group, $P \leqslant G$ be a p-subgroup, $H \trianglelefteq G$ be a p'-subgroup, and $\overline{G} = G/H$. Then*

(i) $\overline{N_G(P)} = N_{\overline{G}}(\overline{P})$.

(ii) $\overline{C_G(P)} = C_{\overline{G}}(\overline{P})$.

Proof.

For (i), let $\overline{n} \in \overline{N_G(P)}$. Now $\overline{P} = \overline{P^n} = \overline{P}^{\overline{n}}$, so $\overline{n} \in N_{\overline{G}}(\overline{P})$ and it follows that $\overline{N_G(P)} \leqslant N_{\overline{G}}(\overline{P})$. Conversely, let $\overline{n} \in N_{\overline{G}}(\overline{P})$. Now $\overline{P} = \overline{P}^{\overline{n}} = \overline{P^n}$ and $P^n H = PH$. Since $H \cap P = 1$, we have $P^n, P \in Syl_p(PH)$. By Sylow, there exists $h \in H$ such that $P^{nh} = P$. Hence $nh \in N_G(P)$, so $\overline{n} \in \overline{N_G(P)}$. Therefore, $\overline{N_G(P)} = N_{\overline{G}}(\overline{P})$.

For (ii), we immediately have $\overline{C_G(P)} \leqslant C_{\overline{G}}(\overline{P})$. Let $\overline{C} = C_{\overline{G}}(\overline{P})$. Now $[\overline{P}, \overline{C}] = 1$ and so $[P, C] \leqslant H \leqslant C$. From (i), $\overline{C} \leqslant N_{\overline{G}}(\overline{P}) = \overline{N_G(P)}$. Thus $C \leqslant N_G(P)H$ and by Lemma 1.1, $C = C \cap N_G(P)H = (C \cap N_G(P))H = N_C(P)H$. This implies $[P, N_C(P)] \leqslant P \cap [P, C] \leqslant P \cap H = 1$ and $N_C(P) \leqslant C_G(P)$. It follows that
$C = N_C(P)H \leqslant C_G(P)H$. Therefore, $\overline{C} = C_{\overline{G}}(\overline{P}) \leqslant \overline{C_G(P)}$ and $C_{\overline{G}}(\overline{P}) = \overline{C_G(P)}$. □

It is common to say "the normalizer passes" and "the centralizer passes" when the conditions of Lemma 6.4 are satisfied.

Lemma 6.5. *Let G be a group and $\overline{G} = G/\mathcal{O}_{p'}(G)$. If G is p-stable and p-constrained, then $\overline{G}$ is p-stable and p-constrained.*

Proof.

By hypothesis, $\mathcal{O}_{p'}(\overline{G}) = 1$. Thus $\mathcal{O}_{p',p}(\overline{G}) \cong \mathcal{O}_{p',p}(\overline{G})/\mathcal{O}_{p'}(\overline{G}) = \mathcal{O}_p(\overline{G}/\mathcal{O}_{p'}(\overline{G}))$, so $\mathcal{O}_{p',p}(\overline{G})$ is a p-group. As a result, it is enough to show $C_{\overline{G}}(\mathcal{O}_{p',p}(\overline{G})) \leqslant \mathcal{O}_{p',p}(\overline{G})$. Now $\overline{\mathcal{O}_{p',p}(G)} = \mathcal{O}_p(\overline{G}) \trianglelefteq \overline{G}$ is a p-subgroup and it follows that
$\overline{\mathcal{O}_{p',p}(G)}/\mathcal{O}_{p'}(\overline{G}) \trianglelefteq \overline{G}/\mathcal{O}_{p'}(\overline{G})$ is a p-subgroup. This implies

$$\frac{\overline{\mathcal{O}_{p',p}(G)}}{\mathcal{O}_{p'}(\overline{G})} \leqslant \mathcal{O}_p\left(\frac{\overline{G}}{\mathcal{O}_{p'}(\overline{G})}\right) = \frac{\mathcal{O}_{p',p}(\overline{G})}{\mathcal{O}_{p'}(\overline{G})},$$

and so $\overline{\mathcal{O}_{p',p}(G)} \leqslant \mathcal{O}_{p',p}(\overline{G})$. By Theorem 6.5 with $\pi = \{p\}$,

$$C_{\overline{G}}(\mathcal{O}_{p',p}(\overline{G})) \leqslant C_{\overline{G}}(\overline{\mathcal{O}_{p',p}(G)}) = C_{\overline{G}}(\mathcal{O}_p(\overline{G})) \leqslant \mathcal{O}_p(\overline{G}) = \overline{\mathcal{O}_{p',p}(G)} \leqslant \mathcal{O}_{p',p}(\overline{G}).$$

Therefore, $C_{\overline{G}}(\mathcal{O}_{p',p}(\overline{G})) \leqslant \mathcal{O}_{p',p}(\overline{G})$ and $\overline{G}$ is p-constrained.

Let $\overline{P} \leqslant \overline{G}$ be a p-subgroup such that $\overline{P}\mathcal{O}_{p'}(\overline{G}) \trianglelefteq \overline{G}$ and $\overline{A} \leqslant N_{\overline{G}}(\overline{P})$ be a p-subgroup acting quadratically on $\overline{P}$. Since $\mathcal{O}_{p'}(\overline{G}) = 1$, we have $\overline{P} \trianglelefteq \overline{G}$. Let $A_0 \in Syl_p(A)$ and $P_0 \in Syl_p(P)$. Since $\overline{A}$ and $\overline{P}$ are p-subgroups, we have $\overline{A} = \overline{A_0}$ and $\overline{P} = \overline{P_0}$. Moreover, $P_0\mathcal{O}_{p'}(G) \trianglelefteq G$ and $\overline{A_0} \leqslant N_{\overline{G}}(\overline{P_0}) = \overline{N_G(P_0)}$, which implies $A_0 \leqslant A_0\mathcal{O}_{p'}(G) \leqslant N_G(P_0)\mathcal{O}_{p'}(G)$. Also, $A_0 \in Syl_p(N_G(P_0)\mathcal{O}_{p'}(G))$ since $\mathcal{O}_{p'}(G)$ is a p'-group. By Sylow, there exists $x \in N_G(P_0)\mathcal{O}_{p'}(G)$ such that $A_0^x \leqslant N_G(P_0)$. Since $\overline{A}$ acts quadratically on $\overline{P}$, it follows that $\overline{A_0}$ acts quadratically on $\overline{P_0}$. Furthermore, $\overline{x} \in \overline{N_G(P_0)} = N_{\overline{G}}(\overline{P_0})$ and $[\overline{P_0}, \overline{A_0}^{\overline{x}}, \overline{A_0}^{\overline{x}}] = 1$, which implies

$$[P_0\mathcal{O}_{p'}(G), A_0^x\mathcal{O}_{p'}(G), A_0^x\mathcal{O}_{p'}(G)] \leqslant \mathcal{O}_{p'}(G).$$

Thus $[P_0, A_0^x, A_0^x] \leqslant \mathcal{O}_{p'}(G) \cap P_0 = 1$. Since G is p-stable,

$$\frac{A_0^x C_G(P_0)}{C_G(P_0)} \leqslant \mathcal{O}_p\left(\frac{N_G(P_0)}{C_G(P_0)}\right) \quad \text{and} \quad \frac{\overline{A_0^x C_G(P_0)}}{\overline{C_G(P_0)}} \leqslant \mathcal{O}_p\left(\frac{\overline{N_G(P_0)}}{\overline{C_G(P_0)}}\right).$$

By Lemma 6.4 with $\overline{P_0} = \overline{P}$ and $\overline{A_0} = \overline{A}$, we have

$$\frac{\overline{A}^{\overline{x}} C_{\overline{G}}(\overline{P})}{C_{\overline{G}}(\overline{P})} \leqslant \mathcal{O}_p\left(\frac{N_{\overline{G}}(\overline{P})}{C_{\overline{G}}(\overline{P})}\right) \quad \text{implies} \quad \left(\frac{\overline{A}C_{\overline{G}}(\overline{P})}{C_{\overline{G}}(\overline{P})}\right)^{C_{\overline{G}}(\overline{P})\overline{x}} \leqslant \mathcal{O}_p\left(\frac{N_{\overline{G}}(\overline{P})}{C_{\overline{G}}(\overline{P})}\right).$$

Thus

$$\frac{\overline{A}C_{\overline{G}}(\overline{P})}{C_{\overline{G}}(\overline{P})} \leqslant \mathcal{O}_p\left(\frac{N_{\overline{G}}(\overline{P})}{C_{\overline{G}}(\overline{P})}\right)^{(C_{\overline{G}}(\overline{P})\overline{x})^{-1}} = \mathcal{O}_p\left(\frac{N_{\overline{G}}(\overline{P})}{C_{\overline{G}}(\overline{P})}\right)$$

follows from

$$\mathcal{O}_p\left(\frac{N_{\overline{G}}(\overline{P})}{C_{\overline{G}}(\overline{P})}\right) \trianglelefteq \frac{N_{\overline{G}}(\overline{P})}{C_{\overline{G}}(\overline{P})}.$$

Therefore, $\overline{G}$ is p-stable. □

Theorem 6.8 (Glauberman's ZJ Theorem)**.** *Let G be a p-stable and p-constrained group, and $P \in Syl_p(G)$. If $\mathcal{O}_p(G) \neq 1$, then $G = N_G(\mathcal{Z}(J(P)))\mathcal{O}_{p'}(G)$.*

Proof.

We proceed by induction on $|G|$. Let $\overline{G} = G/\mathcal{O}_{p'}(G)$ and suppose $\mathcal{O}_{p'}(G) \neq 1$. Since $\mathcal{O}_p(G)$ a normal p-group, we have $\overline{\mathcal{O}_p(G)}$ is a normal p-group and $\overline{\mathcal{O}_p(G)} \leqslant \mathcal{O}_p(\overline{G})$. If $\overline{\mathcal{O}_p(G)} = 1$, then $\mathcal{O}_p(G) \leqslant \mathcal{O}_{p'}(G) \neq 1$. This implies $\mathcal{O}_p(G) = 1$, which is a contradiction. Thus $\overline{\mathcal{O}_p(G)} \neq 1$. Moreover, $\overline{P} \in Syl_p(\overline{G})$. By the induction hypothesis, $\overline{G} = N_{\overline{G}}(\mathcal{Z}(J(\overline{P})))\mathcal{O}_{p'}(\overline{G})$, but $\mathcal{O}_{p'}(\overline{G}) = 1$ and so $\overline{G} = N_{\overline{G}}(\mathcal{Z}(J(\overline{P})))$. By Lemma 6.4, $\overline{G} = \overline{N_G(\mathcal{Z}(J(P)))}$ and it follows that $G = N_G(\mathcal{Z}(J(P)))\mathcal{O}_{p'}(G)$.

Without loss of generality, assume $\mathcal{O}_{p'}(G) = 1$. Now $\mathcal{Z}(J(P))$ char $J(P)$ char P, $\mathcal{Z}(J(P)) \trianglelefteq P$, and $\mathcal{Z}(J(P))$ is abelian. By Theorem 6.6, $\mathcal{Z}(J(P)) \leqslant \mathcal{O}_{p',p}(G)$. Since $\mathcal{O}_{p',p}(G) \trianglelefteq G$ and $\mathcal{O}_{p'}(G) = 1$, we have $\mathcal{O}_{p',p}(G)$ is a p-group and $\mathcal{O}_{p',p}(G) \leqslant \mathcal{O}_p(G)$. By Theorem 6.7, $\mathcal{O}_p(G) \cap \mathcal{Z}(J(P)) \trianglelefteq G$, but $\mathcal{Z}(J(P)) \leqslant \mathcal{O}_{p',p}(G) \leqslant \mathcal{O}_p(G)$. Hence $\mathcal{O}_p(G) \cap \mathcal{Z}(J(P)) = \mathcal{Z}(J(P))$. Therefore, $\mathcal{Z}(J(P)) \trianglelefteq G$ and $G = N_G(\mathcal{Z}(J(P)))$. □

6.2 Some Groups of Matrices

Definition 6.7. *Let p be a prime, $r \in \mathbb{N}$, and $q = p^r$.*

(*i*) *The **general linear group** is given by*

$$GL_n(q) = \{A \in M_n(GF(q)) : \det(A) \neq 0\}.$$

(ii) *The* ***special linear group*** *is given by*

$$SL_n(q) = \{A \in GL_n(q) : \det(A) = 1\}.$$

(iii) *The* ***projective special linear group*** *is given by*

$$L_n(q) = PSL_n(q) = \frac{SL_n(q)}{\mathcal{Z}(SL_n(q))}.$$

Theorem 6.9. *Let p be a prime, $r \in \mathbb{N}$, and $q = p^r$. Then*

(i) *$GL_n(q)$ is a group under matrix multiplication.*

(ii) $SL_n(q) \leqslant GL_n(q)$.

(iii) $|GL_2(q)| = (q^2 - 1)(q^2 - q)$.

(iv) $|SL_2(q)| = (q^2 - 1)(q^2 - q)/(q - 1)$.

Proof.

For *(i)*, let $A = [a_{ij}], B = [b_{ij}] \in GL_n(q)$ and set $[c_{ij}] = C = AB$. From [Cur74], $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$, so $c_{ij} \in GF(q)$ and $C \in M_n(GF(q))$. Moreover, $\det(C) = \det(AB) = \det(A)\det(B) \neq 0$. Hence $C \in GL_n(q)$. Furthermore, $GL_n(q)$ is associative; has an identity matrix $I_n = [e_{ij}]$, where

$$e_{ij} = \begin{cases} 1, & \text{for } i = j \\ 0, & \text{for } i \neq j, \end{cases}$$

such that $AI_n = I_nA = A$ for all $A \in GL_n(q)$; and every $A \in GL_n(q)$ is invertible since $\det(A) \neq 0$. Therefore, $GL_n(q)$ is a group under matrix multiplication.

For *(ii)*, let $A, B \in SL_n(q)$. Now $AB^{-1} \in GL_n(q)$ by *(i)* and

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)\det(B)^{-1} = 1.$$

Thus $AB^{-1} \in SL_n(q)$ and $SL_n(q) \leqslant GL_n(q)$ by the Subgroup Test.

For *(iii)*, from [Cur74], an equivalent condition for a matrix having nonzero determinant is for a matrix to have linearly independent rows. Consider a matrix in $GL_2(q)$. There are q^2 possible combinations of elements from $GF(q)$ to form the first row; however, the first row must be nonzero. Thus there are $q^2 - 1$ possibilities for row one. The second row cannot be a multiple of the first and there are q possible multiples of row one. In total, there are q^2-q possible choices for row two. Therefore, $|GL_2(q)| = (q^2-1)(q^2-q)$.

For (iv), define $\det : GL_n(q) \to GF(q)^*$ by $A^{\det} = \det(A)$ for all $A \in GL_n(q)$. Clearly, det is a homomorphism. Let $a \in GF(q)^*$ and consider $A = \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \in GL_2(q)$. Then $A^{\det} = a$ and so det is surjective. Now $A \in SL_2(q)$ if and only if $A^{\det} = 1$, or, equivalently, $A \in Ker \det$. Hence $SL_2(q) = Ker \det$. By the First Isomorphism Theorem,

$$\frac{GL_2(q)}{SL_2(q)} = \frac{GL_2(q)}{Ker \det} \cong GL_2(q)^{\det} = GF(q)^*,$$

and

$$\left|\frac{GL_2(q)}{SL_2(q)}\right| = \frac{|GL_2(q)|}{|SL_2(q)|} = |GF(q)^*| = q-1.$$

Therefore, $|SL_2(q)| = (q^2-1)(q^2-q)/(q-1)$. □

Theorem 6.10. *The Sylow 2-subgroups of $SL_2(3)$ are non-abelian.*

Proof.

By Theorem 6.9, $|SL_2(3)| = (3^2-1)(3^2-3)/(3-1) = 2^3 \cdot 3$ and so $|SL_2(3)|_2 = 2^3$. Consider $P = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 2 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 2 & 2 \end{smallmatrix}\right)\}$. Clearly, $P \in Syl_2(SL_2(3))$; however, $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right)$. Therefore, P is non-abelian and all other Sylow 2-subgroups of $SL_2(3)$ are conjugate to P. □

Definition 6.8. *Let G and K be groups. Then K is **involved** in G if there exists $N \trianglelefteq H \leqslant G$ such that $K \cong H/N$.*

Definition 6.9. *Let G be a group and p be a prime. Then G is **strongly p-solvable** if G is p-solvable and either,*

(i) $p \geq 5$, or

(ii) $p = 3$ and $SL_2(3)$ is not involved in G.

Theorem 6.11. *Let G be a group with abelian Sylow 2-subgroups. Then $SL_2(3)$ is not involved in G.*

Proof.

Toward a contradiction, suppose there exists $N \trianglelefteq H \leqslant G$ such that $H/N \cong SL_2(3)$. Let $P_1 \in Syl_2(H)$. By Sylow, there exists $P \in Syl_2(G)$ such that $P_1 \leqslant P$. Since P is abelian, it follows that P_1 is abelian. Moreover, $P_1N/N \in Syl_2(H/N)$ and P_1N/N is abelian. Since $H/N \cong SL_2(3)$, we have Sylow 2-subgroups of $SL_2(3)$ are abelian. However, this contradicts Theorem 6.10. Therefore, $SL_2(3)$ is not involved in G. □

Theorem 6.12. *Let G be a group. If G is strongly p-solvable, then G is p-constrained.*

Proof.

By hypothesis, G is p-solvable. Let $P_1 \in Syl_p(\mathcal{O}_{p',p}(G))$ and $H = \mathcal{O}_{p',p}(G)$. Now there exists $P \in Syl_p(G)$ such that $P_1 \leqslant P$. Moreover, $P \cap H \leqslant H$ and $P \cap H$ is a p-group. By Sylow, there exists $h \in H$ such that $P \cap H \leqslant P_1^h$, so $P_1 \leqslant P \cap H \leqslant P_1^h$, but $|P_1| = |P_1^h|$. Thus $P_1 = P \cap H = P \cap \mathcal{O}_{p',p}(G)$ and by Theorem 6.4,

$$C_G(P_1) = C_G(P \cap \mathcal{O}_{p',p}(G)) \leqslant \mathcal{O}_{p',p}(G).$$

Therefore, G is p-constrained. □

Lemma 6.6. *Let G be a group, $P \in Syl_p(G), N \trianglelefteq G$ be a p'-subgroup, and $\overline{G} = G/N$. Then*

(*i*) $\overline{J(P)} \leqslant J(\overline{P})$.

(*ii*) $\overline{\mathcal{Z}(J(P))} \leqslant \mathcal{Z}(J(\overline{P}))$.

(*iii*) $\overline{N_G(\mathcal{Z}(J(P)))} \leqslant N_{\overline{G}}(\mathcal{Z}(J(\overline{P})))$.

Proof.

For (i), let $A \in A(P)$. Now $\overline{A} \leqslant \overline{P}, \overline{A}$ is abelian, and

$$|\overline{A}| = \frac{|AN|}{|N|} = \frac{|A|}{|A \cap N|} = |A|,$$

by the coprime orders of N and A. Thus $\overline{A} \in A(\overline{P})$, which implies $\overline{J(P)} \leqslant J(\overline{P})$.

For (ii), let $z \in \mathcal{Z}(J(P))$. Now $z \in J(P)$, so $\overline{z} \in \overline{J(P)}$. Clearly, $\overline{z} \in \mathcal{Z}(\overline{J(P)})$, but by (i), $\mathcal{Z}(\overline{J(P)}) \leqslant \mathcal{Z}(J(\overline{P}))$. Thus $\overline{z} \in \overline{\mathcal{Z}(J(P))} \leqslant \mathcal{Z}(\overline{J(P)}) \leqslant \mathcal{Z}(J(\overline{P}))$.

For (iii), $J(P)$ is a p-group, so $\mathcal{Z}(J(P))$ is a p-group. By Lemma 6.4 and (ii), we have $\overline{N_G(\mathcal{Z}(J(P)))} \leqslant N_{\overline{G}}(\overline{\mathcal{Z}(J(P))}) \leqslant N_{\overline{G}}(\mathcal{Z}(J(\overline{P})))$. □

Theorem 6.13. *Let G be a group. If G is strongly p-solvable, then G is p-stable.*

Proof.

See Theorem 5.3, pg. 235 in [Gor07]. □

Theorem 6.14 (Glauberman-Thompson Normal p-Complement)**.** *Let G be a group and $P \in Syl_p(G)$, where p is odd. If $N_G(\mathcal{Z}(J(P)))$ has a normal p-complement, then G has a normal p-complement.*

Proof.

Let G be a counterexample such that $|G|$ is minimal. If there exists $H < G$ such that $P \leqslant H$, then $P \in Syl_p(H)$. Furthermore, $\mathcal{Z}(J(P))$ char $J(P)$ char P, so $\mathcal{Z}(J(P))$ char P and $\mathcal{Z}(J(P)) \trianglelefteq P$. Thus $P \leqslant N_H(\mathcal{Z}(J(P))) \leqslant N_G(\mathcal{Z}(J(P)))$. By Lemma 4.2, $N_H(\mathcal{Z}(J(P)))$ has a normal p-complement and it follows from the minimality of $|G|$, H has a normal p-complement. Since G is a counterexample, we have by Frobenius' Theorem (2.11) there exists $H \leqslant G$ such that H is a p-group, $N = N_G(H)$ has no normal p-complements, and $|N|_p$ is maximal.

We may assume $P \cap N \in Syl_p(N)$; otherwise from Sylow, there exists $P_0 \in Syl_p(N)$ such that $P \cap N \leqslant P_0$. Also by Sylow, there exists $g \in G$ such that $P_0 \leqslant P^g$, but again, there exists $n \in N$ such that $P^g \cap N \leqslant P_0^n$. Now $P_0 \leqslant P^g \cap N \leqslant P_0^n$, but $|P_0| = |P_0^n|$, thus $P^g \cap N = P_0 \in Syl_p(N)$. But then $N_G(\mathcal{Z}(J(P^g))) = N_G(\mathcal{Z}(J(P)))^g$ has a normal p-complement since $N_G(\mathcal{Z}(J(P)))$ has a normal p-complement. Without loss of generality, we may take $P = P^g$.

Suppose $P \nleqslant N = N_G(H)$. Let $R = P \cap N, L = N_N(\mathcal{Z}(J(R)))$, and $M = N_G(\mathcal{Z}(J(R)))$. Now $R < P$ and $L \leqslant M$. By Lemma 1.16 on P, $R < N_P(R)$ and $\mathcal{Z}(J(R))$ char R, thus $R < N_P(R) \leqslant N_P(\mathcal{Z}(J(R))) \leqslant P \cap M$. It follows that $|M|_p \geq |P \cap M| > |R| = |N|_p, M = N_G(\mathcal{Z}(J(R)))$, and $\mathcal{Z}(J(R))$ is a p-group. By the maximality of $|N|_p$, M must have a normal p-complement. Now $\mathcal{Z}(J(R))$ char $J(R)$ char R, so $R \leqslant N_N(\mathcal{Z}(J(R))) = L \leqslant M$. By Lemma 4.2, L has a normal p-complement, but $L = N_N(\mathcal{Z}(J(R)))$ and $R = P \cap N \in Syl_p(N)$. Also, $N < G$ since $P \nleqslant N$. By the minimality of $|G|$, N has a normal p-complement, but this is a contradiction. Thus $P \leqslant N$. If $N < G$, then N has a normal p-complement, which is again a contradiction. Therefore, $P \leqslant N = N_G(H) = G$ and $H \trianglelefteq G$.

We claim $\mathcal{O}_{p'}(G) = 1$. Suppose not and let $\overline{G} = G/\mathcal{O}_{p'}(G)$. Now $\overline{P} \in Syl_p(\overline{G})$, p is odd, and $N_{\overline{G}}(\mathcal{Z}(J(\overline{P}))) = \overline{N_G(\mathcal{Z}(J(P)))}$ has a normal p-complement by Lemma 4.3. By the minimality of $|G|$, $\overline{G}$ has a normal p-complement. Hence $\overline{G} = \overline{P}\mathcal{O}_{p'}(\overline{G})$, but $\mathcal{O}_{p'}(\overline{G}) = 1$, so $\overline{G} = \overline{P}$. It follows that $G = P\mathcal{O}_{p'}(G)$ and G has a normal p-complement. This is a contradiction, so $\mathcal{O}_{p'}(G) = 1$.

Since H is a p-group and $H \trianglelefteq G$, we have by Sylow, $H \leqslant P$. If $P = H$, then $P \trianglelefteq G$. Also, $\mathcal{Z}(J(P))$ char $P \trianglelefteq G$ implies $\mathcal{Z}(J(P)) \trianglelefteq G$ and $G = N_G(\mathcal{Z}(J(P)))$. Now G has a normal p-complement and this is a contradiction, so $H < P$. Since $H \trianglelefteq G$ and $\mathcal{O}_p(G) \trianglelefteq G$, we have $N = N_G(H) = G = N_G(\mathcal{O}_p(G))$. Thus $N_G(\mathcal{O}_p(G))$ has no normal p-complement, $\mathcal{O}_p(G)$ is a p-group, and $|N_G(\mathcal{O}_p(G))|_p = |N|_p$. Without loss of generality, assume $H = \mathcal{O}_p(G)$.

Let $\widetilde{G} = G/H$. Since $H < P$, we have $\widetilde{P} \in Syl_p(\widetilde{G})$ is nontrivial. Let $\widetilde{N_1} = N_{\widetilde{G}}(\mathcal{Z}(J(\widetilde{P})))$ and $\widetilde{H_1} = \mathcal{Z}(J(\widetilde{P}))$. Since $\widetilde{P} \neq 1$, we have $\mathcal{Z}(\widetilde{P}) \neq 1$, which implies there exist maximally abelian subgroups of $\widetilde{P}$. Hence $J(\widetilde{P}) \neq 1$, which implies $\widetilde{H_1} \neq 1$ and $H < H_1$. Also, $\widetilde{N_1} = N_{\widetilde{G}}(\widetilde{H_1}) = \widetilde{N_G(HH_1)} = \widetilde{N_G(H_1)}$, so $N_1 = N_G(H_1)$. Since H_1 is a p-group and $H < H_1$, we have $H_1 \ntrianglelefteq G$; otherwise, $H_1 \leqslant H$. Thus $N_1 = N_G(H_1) < G$. Now $\widetilde{P} \leqslant \widetilde{N_1}$ and $P \leqslant N_1 < G$. By our work in the introduction,

N_1 has a normal p-complement, so $\widetilde{N_1}$ has a normal p-complement by Lemma 4.3. By the minimality of $|G|$, $\widetilde{G}$ has a normal p-complement. It follows that $\widetilde{G} = \widetilde{P}\mathcal{O}_{p'}(\widetilde{G}) = P\widetilde{\mathcal{O}_{p,p'}(G)}$ and $G = P\mathcal{O}_{p,p'}(G)H = P\mathcal{O}_{p,p'}(G)$. Now

$$\frac{G}{\mathcal{O}_{p,p'}(G)} = \frac{P\mathcal{O}_{p,p'}(G)}{\mathcal{O}_{p,p'}(G)} \cong \frac{P}{P \cap \mathcal{O}_{p,p'}(G)}$$

is a p-group, which implies

$$\frac{G}{\mathcal{O}_{p,p'}(G)} = \mathcal{O}_p\left(\frac{G}{\mathcal{O}_{p,p'}(G)}\right) = \frac{\mathcal{O}_{p,p',p}(G)}{\mathcal{O}_{p,p'}(G)}.$$

Thus $G = \mathcal{O}_{p,p',p}(G)$. By Theorem 6.2($iv$), G is p-separable and by Theorem 6.1(ii), G is p-solvable.

Now we want to show G is strongly p-solvable. If $p \geq 5$, then G is strongly p-solvable since G is p-solvable. If $p = 3$, then we must show $SL_2(3)$ is not involved in G. By the coprime action of $\widetilde{P}$ on $\mathcal{O}_{p'}(\widetilde{G})$, we have for all $q \in \pi(\mathcal{O}_{p'}(\widetilde{G}))$, there exists $\widetilde{Q} \in Syl_q(\mathcal{O}_{p'}(\widetilde{G}))$ such that $\widetilde{P} \leqslant N_{\widetilde{G}}(\widetilde{Q})$. Since $\mathcal{Z}(\widetilde{Q})$ char $\widetilde{Q}$, we have $\widetilde{P} \leqslant N_{\widetilde{G}}(\mathcal{Z}(\widetilde{Q}))$. Let $\widetilde{G_1} = \widetilde{P}\mathcal{Z}(\widetilde{Q})$ and $\widetilde{Q_1} = \mathcal{Z}(\widetilde{Q})$. Now $G_1 = PQ_1$, where Q_1 is a q-group. In addition, $1 = [\mathcal{Z}(\widetilde{Q}), \mathcal{Z}(\widetilde{Q})] = [\widetilde{Q_1}, \widetilde{Q_1}]$ and so $[Q_1, Q_1] \leqslant H \cap Q_1 = 1$. Thus Q_1 is abelian. If $G_1 < G$, then G_1 has a normal p-complement, where Q_1 is the normal p-complement. It follows that $[Q_1, H] \leqslant H \cap Q_1 = 1$ and $Q_1 \leqslant C_G(H) = C_G(\mathcal{O}_p(G)) \leqslant \mathcal{O}_p(G)$ by Theorem 6.3 because G is p-separable and $\mathcal{O}_{p'}(G) = 1$. Hence $Q_1 = 1$ and $\widetilde{Q_1} = \mathcal{Z}(\widetilde{Q}) = 1$. This is a contradiction since $\widetilde{Q} \in Syl_q(\mathcal{O}_{p'}(\widetilde{G}))$. Thus $G = G_1 = PQ_1$, where P is a 3-group, and Q_1 is a q-group for $q \neq 3$. Now the Sylow 2-subgroups of G are abelian since Q_1 is abelian. By Theorem 6.11, $SL_2(3)$ is not involved in G. Therefore, G is strongly p-solvable.

Since G is strongly p-solvable, G is p-constrained by Theorem 6.12, and by Theorem 6.13, G is p-stable. Now $H \leqslant \mathcal{O}_p(G)$ is nontrivial, so by Glauberman's ZJ-Theorem (6.8), $G = N_G(\mathcal{Z}(J(P)))\mathcal{O}_{p'}(G)$, but $\mathcal{O}_{p'}(G) = 1$. Thus $G = N_G(\mathcal{Z}(J(P)))$, but then G has a normal p-complement. This is a contradiction since G is a counterexample. Therefore, no such counterexample exists. $\square$

7 Fixed-Point-Free Automorphisms

Definition 7.1. *Let G be a group and $\phi \in Aut(G)$. The* ***centralizer*** *in G of ϕ is*

$$C_G(\phi) = \{g \in G : g^\phi = g\},$$

and $C_G(\phi) \leqslant G$. We say the automorphism ϕ acts ***fixed-point-freely*** *on G if $C_G(\phi) = 1$.*

Definition 7.2. *Let G be a group and $\phi \in Aut(G)$. Then $[g, \phi] = g^{-1}g^\phi$ for all $g \in G$.*

Theorem 7.1. *Let G be a group, $\phi \in Aut(G)$, $C_G(\phi) = 1$, and suppose $|\phi| = n$ for some $n \in \mathbb{N}$. Then*

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

(ii) $gg^\phi g^{\phi^2} \cdots g^{\phi^{n-1}} = 1$ *for all* $g \in G$.

Proof.

For (i), suppose $x, y \in G$ such that $[x, \phi] = [y, \phi]$. Now $x^{-1}x^\phi = y^{-1}y^\phi$, so $yx^{-1} = (yx^{-1})^\phi$. Hence $yx^{-1} \in C_G(\phi) = 1$ and $y = x$. Thus $|\{[g, \phi] : g \in G\}| = |G|$, but $\{[g, \phi] : g \in G\} \leqslant G$. Therefore, $G = \{[g, \phi] : g \in G\}$. Similarly, if $x^\phi x^{-1} = y^\phi y^{-1}$ for some $x, y \in G$, then $(y^{-1}x)^\phi = y^{-1}x$ and $y^{-1}x \in C_G(\phi) = 1$. Thus $x = y$ and $|\{g^\phi g^{-1} : g \in G\}| = |G|$. Therefore, $G = \{g^\phi g^{-1} : g \in G\}$.

For (ii), let $g \in G$. By (i), there exists $x \in G$ such that $g = [x, \phi] = x^{-1}x^\phi$. Now

$$\begin{aligned} gg^\phi g^{\phi^2} \cdots g^{\phi^{n-1}} &= x^{-1}x^\phi \left(x^{-1}x^\phi\right)^\phi \left(x^{-1}x^\phi\right)^{\phi^2} \cdots \left(x^{-1}x^\phi\right)^{\phi^{n-1}} \\ &= x^{-1}x^\phi \left(x^\phi\right)^{-1} x^{\phi^2} \left(x^{\phi^2}\right)^{-1} x^{\phi^3} \left(x^{\phi^3}\right)^{-1} \cdots \\ &\quad\ x^{\phi^4} \left(x^{\phi^4}\right)^{-1} \cdots \left(x^{\phi^{n-1}}\right)^{-1} x^{\phi^n} \\ &= x^{-1}x^{\phi^n} = x^{-1}x = 1. \end{aligned}$$

Therefore, $gg^\phi g^{\phi^2} \cdots g^{\phi^{n-1}} = 1$. □

Theorem 7.2. *Let G be a group and $\phi \in Aut(G)$ such that $C_G(\phi) = 1$. Then*

(*i*) *For each $p \in \pi(G)$, there exists a unique $P \in Syl_p(G)$ that is ϕ-invariant.*

(*ii*) *If $H \leqslant G$ is a ϕ-invariant p-subgroup, then $H \leqslant P$.*

Proof.

For (i), let $P \in Syl_p(G)$. Now $|P^\phi| = |P|$, so $P^\phi \in Syl_p(G)$. By Sylow, there exists $g \in G$ such that $P^\phi = P^g$ and by Theorem 7.1, there exists $x \in G$ such that $g = [x, \phi] = x^{-1}x^\phi$. Since $|P^{x^{-1}}| = |P|$, we have $P^{x^{-1}} \in Syl_p(G)$. Also, $(x^\phi)^{-1} = g^{-1}x^{-1}$ and

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

Thus $(P^{x^{-1}})^\phi = P^{x^{-1}}$, $P^{x^{-1}} \in Syl_p(G)$, and $P^{x^{-1}}$ is ϕ-invariant.

To show uniqueness, suppose $P, Q \in Syl_p(G)$ are ϕ-invariant. By Sylow, there exists $g \in G$ such that $P^g = Q$. Now $P^g = Q = Q^\phi = (P^g)^\phi = P^{g^\phi}$, so $P = P^{g^\phi g^{-1}}$ and $g^\phi g^{-1} \in N_G(P)$. Since P is ϕ-invariant, we have $N_G(P)$ is ϕ-invariant. Moreover, $C_{N_G(P)}(\phi) \leqslant C_G(\phi) = 1$, so ϕ acts fixed-point-freely on $N_G(P)$. By Theorem 7.1, there exists $n \in N_G(P)$ such that $g^\phi g^{-1} = n^\phi n^{-1}$. Then

$$n^{-1}g = \left(n^\phi\right)^{-1} g^\phi = (n^{-1})^\phi g^\phi = (n^{-1}g)^\phi,$$

and $n^{-1}g \in C_G(\phi) = 1$. Thus $g = n \in N_G(P)$ and $Q = P^g = P$.

For (ii), let $P \in Syl_p(G)$ be the unique ϕ-invariant Sylow p-subgroup of G guaranteed by (i) and $P_1 \leqslant G$ be a maximal ϕ-invariant p-subgroup such that $H \leqslant P_1$. Since P_1 is ϕ-invariant, $N_G(P_1)$ is ϕ-invariant. Moreover, $C_{N_G(P_1)}(\phi) \leqslant C_G(\phi) = 1$. By ($i$), there exists a unique $P_2 \in Syl_p(N_G(P_1))$ such that P_2 is ϕ-invariant. Now $P_1 \trianglelefteq N_G(P_1)$ is a p-subgroup, so $P_1 \leqslant P_2$. Then $H \leqslant P_1 \leqslant P_2$ and by the maximality of P_1, we have $P_1 = P_2$. Thus $P_1 \in Syl_p(N_G(P_1))$. By Lemma 1.17, $P_1 \in Syl_p(G)$ and P_1 is ϕ-invariant. It follows from the uniqueness of P that $P_1 = P$. Therefore, $H \leqslant P$. □

Theorem 7.3. *Let G be a group, $\phi \in Aut(G)$, $C_G(\phi) = 1$, $N \trianglelefteq G$ be ϕ-invariant, and $\overline{G} = G/N$. Define the induced homomorphism on $\overline{G}$ by*

$$\overline{g}^{\phi} = \overline{g^{\phi}},$$

for all $\overline{g} \in \overline{G}$. Then $C_{\overline{G}}(\phi) = 1$.

Proof.

Let $\overline{a}, \overline{b} \in \overline{G}$. If $\overline{a} = \overline{b}$, then $b^{-1}a \in N$ and $a = bn$ for some $n \in N$. Since N is ϕ-invariant, $\overline{a}^{\phi} = \overline{a^{\phi}} = \overline{(bn)^{\phi}} = \overline{b^{\phi}n^{\phi}} = \overline{b^{\phi}}\ \overline{n^{\phi}} = \overline{b^{\phi}} = \overline{b}^{\phi}$. Thus $\overline{a}^{\phi} = \overline{b}^{\phi}$ and ϕ is well-defined. It remains to show $\phi \in Aut(\overline{G})$.

Let $\overline{a}, \overline{b} \in \overline{G}$. Now $(\overline{a}\overline{b})^{\phi} = \overline{(ab)^{\phi}} = \overline{a^{\phi}b^{\phi}} = \overline{a^{\phi}}\ \overline{b^{\phi}} = \overline{a}^{\phi}\overline{b}^{\phi}$, and ϕ is a homomorphism. Let $\overline{a} \in \overline{G}$. Then $a \in G$ and so there exists $b \in G$ such that $b^{\phi} = a$. It follows that $\overline{a} = \overline{b^{\phi}} = \overline{b}^{\phi}$ and ϕ is surjective on $\overline{G}$. To show ϕ is injective, suppose $\overline{a}^{\phi} = \overline{b}^{\phi}$. Now $\overline{a^{\phi}} = \overline{b^{\phi}}$ and $(b^{\phi})^{-1}a^{\phi} = (b^{-1}a)^{\phi} \in N$. Since N is ϕ-invariant and ϕ is surjective on G, we have $N^{\phi} = N$. Thus there exists $n \in N$ such that $(b^{-1}a)^{\phi} = n^{\phi}$ and since ϕ is injective on G, we have $b^{-1}a = n \in N$. This implies $\overline{a} = \overline{b}$. Therefore, $\phi \in Aut(\overline{G})$.

Finally, if $\overline{a} \in C_{\overline{G}}(\phi)$, then $\overline{a}^{\phi} = \overline{a}$ and $a^{-1}a^{\phi} \in N$. Now $C_N(\phi) \leqslant C_G(\phi) = 1$, so by Theorem 7.1, there exists $n \in N$ such that $a^{-1}a^{\phi} = [n, \phi] = n^{-1}n^{\phi}$. Hence $na^{-1} = (na^{-1})^{\phi}$ and na^{-1} is a fixed-point of ϕ. However, $C_G(\phi) = 1$ forces $n = a$ and $\overline{a} = 1$. Therefore, $C_{\overline{G}}(\phi) = 1$. □

7.1 Some Examples

We provide some examples exemplifying the relationship between Thompson's Theorem and Frobenius' Conjecture.

Theorem 7.4. *Let G be a group, $\phi \in Aut(G)$, $C_G(\phi) = 1$, and suppose $|\phi| = 2$. Then G is abelian.*

Proof.

By Theorem 7.1, $xx^{\phi} = 1$ for all $x \in G$, so $x^{\phi} = x^{-1}$ for all $x \in G$. Let $x, y \in G$.

Now $xy = (y^{-1}x^{-1})^{-1} = \left(y^{\phi}x^{\phi}\right)^{-1} = \left((yx)^{\phi}\right)^{-1} = ((yx)^{-1})^{-1} = yx$. Therefore, G is abelian. $\square$

By Lemma 1.13, G is nilpotent and from Theorem 1.21, G is solvable. Thus Frobenius' Conjecture holds true.

Theorem 7.5. *Let G be a group, $\phi \in Aut(G)$, $C_G(\phi) = 1$, and suppose $|\phi| = 3$. Then G is nilpotent.*

Proof.

Suppose G is not nilpotent. Since $C_G(\phi) = 1$, there exists a $P \in Syl_p(G)$ such that $P \ntrianglelefteq G$ and P is ϕ-invariant by Theorem 7.2. Let $Q \in Syl_p(G)$ such that $Q \neq P$. Now $Q \nleqslant P$ and there exists $x \in Q \setminus P$. By Theorem 7.1, $xx^{\phi}x^{\phi^2} = 1$ and $x^{\phi^2}x^{\phi}x = 1$, which implies $xx^{\phi} = \left(x^{\phi^2}\right)^{-1} = x^{\phi}x$.

Let $H = \langle x^{\phi}, x\rangle$. Now H is abelian since $xx^{\phi} = x^{\phi}x$. Since $|x|$ is a p-number, we know $|x^{\phi}|$ is a p-number and H is a p-group. Clearly, $x^{\phi} \in H$. Moreover, $(x^{\phi})^{\phi} = x^{\phi^2} = (x^{\phi}x)^{-1} \in H$, so H is ϕ-invariant. By Theorem 7.2, $H \leqslant P$, which places $x \in P$, a contradiction. Therefore, G is nilpotent. $\square$

By Theorem 1.21, G is solvable. Therefore, Frobenius' Conjecture holds true.

Definition 7.3. *Let G be a group and $A \leqslant Aut(G)$. The* ***centralizer*** *in G of A is*

$$C_G(A) = \{g \in G : g^{\phi} = g \text{ for all } \phi \in A\},$$

and $C_G(A) \leqslant G$.

Definition 7.4. *Let G be a group and p be a prime. Define*

$$\Omega_1(G) = \langle g \in G : g^p = 1\rangle,$$

where $\Omega_1(G)$ char G.

8 The Proof of Thompson's Theorem

Theorem 8.1 (Thompson). *Let G be a group, $\phi \in Aut(G)$, $C_G(\phi) = 1$ and suppose $|\phi| = r$ for some prime r. Then G is nilpotent.*

Proof.

Let G be a counterexample such that $|G|$ is minimal. Suppose there exists $1 \neq N \lhd G$ such that N is ϕ-invariant and $N < G$. Now $\phi \in Aut(N)$ since N is ϕ-invariant. Let $|\phi| = k$ on N and $|\phi| = l$ on G/N, where $k \leq r$ and $l \leq r$. If $k < r$, then $\langle \phi^k \rangle \leqslant \langle \phi \rangle$ and $k = |\langle \phi^k \rangle| \big| |\langle \phi \rangle| = r$, which implies $k = 1$ or $k = r$. Respectively, we have $\langle \phi^k \rangle = \langle \phi \rangle$ or $\langle \phi^k \rangle = 1$. If $\langle \phi^k \rangle = 1$, then $\phi^k = 1, r \big| k$, and $r \leq k$. This is a contradiction, so $\langle \phi^k \rangle = \langle \phi \rangle$. But then $1 \neq N \leqslant C_G(\langle \phi^k \rangle) = C_G(\langle \phi \rangle) = C_G(\phi) = 1$ and we have another contradiction, thus $k = r$. Suppose $l < r$. By a similar argument, we have $\langle \phi^l \rangle = \langle \phi \rangle$. Now $[G/N, \phi^l] = 1$, so $[G/N, \langle \phi^l \rangle] = 1$. Hence $[G, \phi^l] \leqslant N$ and $[G, \langle \phi^l \rangle] \leqslant N$. By Theorem 7.1, $G = [G, \phi]$, but $[G, \phi] \leqslant [G, \langle \phi \rangle] = [G, \langle \phi^l \rangle] \leqslant N$. This is a contradiction and so $l = r$. Now $N < G, C_N(\phi) \leqslant C_G(\phi) = 1$, $|\phi| = r$ on N, and $\phi \in Aut(N)$. Thus N is nilpotent by the minimality of $|G|$. Also, $C_{G/N}(\phi) = 1$ by Theorem 7.3, $|\phi| = r$ on G/N, and $\phi \in Aut(G/N)$. It follows from the minimality of $|G|$ that G/N is nilpotent. Therefore, N and G/N are solvable by Theorem 1.21, and G is solvable by Lemma 1.26.

Suppose G contains no nontrivial proper normal ϕ-invariant subgroups. If G is a 2-group, then G is nilpotent, which is a contradiction. Thus $\pi(G)$ contains primes other than 2. By Theorem 7.2, there exists $P \in Syl_p(G)$ such that P is ϕ-invariant and p is odd. Now $\mathcal{Z}(J(P))$ is nontrivial and $\mathcal{Z}(J(P))$ char P, so $\mathcal{Z}(J(P))$ is ϕ-invariant. Since $1 \neq \mathcal{Z}(J(P)) < G$, it follows that $N = N_G(\mathcal{Z}(J(P))) < G$, where N is ϕ-invariant. Also, $C_N(\phi) \leqslant C_G(\phi) = 1$. By the minimality of $|G|$, N is nilpotent. Thus N has a normal p-complement and so by Glauberman-Thompson (6.14), G has a normal p-complement. Hence $G = P\mathcal{O}_{p'}(G)$. Since $\mathcal{O}_{p'}(G)$ char G, we have

$\mathcal{O}_{p'}(G) \trianglelefteq G$ and $\mathcal{O}_{p'}(G)$ is ϕ-invariant. By our assumption, $\mathcal{O}_{p'}(G) = 1$ or $\mathcal{O}_{p'}(G) = G$. Respectively, $G = P$ or $P = 1$. In either case, we have a contradiction, so G contains a minimal ϕ-invariant subgroup. Therefore, G is solvable.

Let $1 \neq N \trianglelefteq G$ such that N is minimal with respect to being ϕ-invariant. Then N is characteristically simple and by Theorem 1.13, $N \cong \bigotimes_{i=1}^{n} N_i$, where the N_i's are simple isomorphic groups. If there exists $1 \leq i \leq n$ such that N_i is non-abelian, then $1 \neq N_i' \trianglelefteq N_i$, so $N_i' = N_i^{(1)} = N_i$ since N_i is simple. But then $N_i^{(k)} = N_i$ for all $k \in \mathbb{N}$ and N_i is not solvable by Theorem 1.20. However, G is solvable and we have a contradiction to Lemma 1.25. Thus N_i is abelian for all $1 \leq i \leq n$. Since N_i is simple, we have $N_i \cong \mathbb{Z}_p$ for some prime p. Therefore, $N \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ is an elementary abelian p-group.

Let $\overline{G} = G/N$. Using a previous argument, $\overline{G}$ is nilpotent by the minimality of $|G|$. If $\overline{G}$ is a p-group, then $|G| = |\overline{G}| \cdot |N|$ and G is a p-group. Hence G is nilpotent by Theorem 1.15. This is a contradiction. By Theorem 7.2, there exists $\overline{Q} \in Syl_q(\overline{G})$ such that $\overline{Q}$ is ϕ-invariant. Since $\overline{Q}$ is a q-group, $\mathcal{Z}(\overline{Q}) \neq 1$ and $\Omega_1(\mathcal{Z}(\overline{Q})) \neq 1$. Also, since $\overline{G}$ is nilpotent, $\Omega_1(\mathcal{Z}(\overline{Q}))$ char $\mathcal{Z}(\overline{Q})$ char $\overline{Q} \trianglelefteq \overline{G}$ and $\Omega_1(\mathcal{Z}(\overline{Q})) \trianglelefteq \overline{G}$ by Lemma 1.12. Moreover, $\Omega_1(\mathcal{Z}(\overline{Q}))$ is ϕ-invariant since $\Omega_1(\mathcal{Z}(\overline{Q}))$ char $\overline{Q}$. Let $1 \neq \overline{M_0} \leqslant \Omega_1(\mathcal{Z}(\overline{Q}))$ be minimal with respect to being ϕ-invariant. Because $\overline{G}$ is nilpotent, $\overline{M_0} \leqslant \Omega_1(\mathcal{Z}(\overline{Q})) \leqslant \mathcal{Z}(\overline{Q}) \leqslant \mathcal{Z}(\overline{G})$, so $\overline{M_0} \trianglelefteq \overline{G}$. Since $\overline{M_0}$ is ϕ-invariant, $\overline{M_0} = \overline{M_0}^{\phi} = \overline{M_0^{\phi}}$ and $M_0^{\phi} \leqslant M_0^{\phi}N = M_0$. Thus M_0 is ϕ-invariant and $M_0 \trianglelefteq G$. Now $C_{M_0}(\phi) \leqslant C_G(\phi) = 1$ and it follows from Theorem 7.2 that there exists $M \in Syl_q(M_0)$, where M is ϕ-invariant. Now $\overline{M} \in Syl_q(\overline{M_0})$, but $\overline{M_0}$ is a q-group, so $\overline{M} = \overline{M_0}$. Therefore, $MN = M_0$.

We claim $G = MN$. Suppose $G \neq MN$. Now MN is ϕ-invariant, $C_{MN}(\phi) \leqslant C_G(\phi) = 1$, and $|\phi| = r$. Thus MN is nilpotent by the minimality of $|G|$. Furthermore, $M \in Syl_q(MN)$, $M \trianglelefteq MN$, M char $MN = M_0 \trianglelefteq G$, and $M \trianglelefteq G$ by Lemma 1.12. Let $\widetilde{G} = G/M$. By a similar argument as above, $\widetilde{G}$ is nilpotent. Then

$\widetilde{G} \times \overline{G}$ is nilpotent by Lemma 1.21. Let $\theta : G \to \widetilde{G} \times \overline{G}$ be defined by $g^\theta = (\widetilde{g}, \overline{g})$ for all $g \in G$. Clearly, θ is a homomorphism with Ker $\theta = M \cap N = 1$ by coprime orders. By the First Isomorphism Theorem, $G \cong G/Ker\ \theta \cong G^\theta \leqslant \widetilde{G} \times \overline{G}$, so G is nilpotent by Lemma 1.14, which is a contradiction. Thus $G = MN$.

If $r = p$, then $\langle \phi \rangle$ is a p-group and acts on the p-group N. By Lemma 1.10, $1 \neq C_N(\langle \phi \rangle) \leqslant C_G(\phi) = 1$, which is a contradiction. Thus $r \neq p$. Similarly, if $r = q$, let $\langle \phi \rangle$ act on M and we result in a similar contradiction, so $r \neq q$. Now we claim M is an elementary abelian q-group. Since M' char M, we have M' is ϕ-invariant. Thus $\overline{M'} \leqslant \overline{M} = \overline{M_0}$ and $\overline{M'}$ is ϕ-invariant. By the minimality of $\overline{M_0}$, either $\overline{M'} = 1$ or $\overline{M'} = \overline{M}$. If $\overline{M'} = \overline{M}$, then $M'N = MN$, but $M \cap N = 1$ and $M' = M$. Hence M cannot be nilpotent; however, M is a q-group. This is a contradiction, so $\overline{M'} = 1$. It follows that $M' \leqslant M \cap N = 1$ and M is abelian. Thus $\Omega_1(M)$ is abelian and it is enough to show $\Omega_1(M) = M$. Now $\Omega_1(M)$ char M and $\overline{\Omega_1(M)}$ char $\overline{M} = \overline{M_0}$, where $\overline{\Omega_1(M)}$ is ϕ-invariant. By the minimality of $\overline{M_0}$, either $\overline{\Omega_1(M)} = 1$ or $\overline{\Omega_1(M)} = \overline{M}$. If $\overline{\Omega_1(M)} = 1$, then $\Omega_1(M) \leqslant M \cap N = 1$, which is a contradiction since M is a q-group. Thus $\overline{\Omega_1(M)} = \overline{M}$ and $\Omega_1(M)N = MN$, but $\Omega_1(M) \cap N \leqslant M \cap N = 1$, so $\Omega_1(M) = M$. Therefore, M is an elementary abelian q-group.

Next we claim $C_M(N) = 1$. Since M and N are ϕ-invariant, we have $C_M(N)$ is ϕ-invariant. Now $\overline{C_M(N)} \leqslant \overline{M} = \overline{M_0}$ and $\overline{C_M(N)}$ is ϕ-invariant. By the minimality of $\overline{M_0}$, either $\overline{C_M(N)} = 1$ or $\overline{C_M(N)} = \overline{M}$. If $\overline{C_M(N)} = \overline{M}$, then $C_M(N)N = MN$. But $M \cap N = 1$, so $M = C_M(N)$. Thus $M \trianglelefteq MN = G$ and $N \trianglelefteq G$, where M and N are nilpotent. By Lemma 1.20, G is nilpotent, which is a contradiction. Hence $\overline{C_M(N)} = 1$ and $C_M(N) \leqslant M \cap N = 1$. Therefore, $C_M(N) = 1$.

Since M is ϕ-invariant, $\langle \phi \rangle$ acts in M in the natural manner. Thus $G^* = M \rtimes_{id} \langle \phi \rangle$ is a group by Theorem 1.23. Let G^* act on N over $\mathbb{Z}_p$ via $\theta : G^* \to Aut(N)$ defined by $n^{(m,\phi^k)^\theta} = (n^{\phi^k})^m$ for all $n \in N$ and for all $(m, \phi^k) \in G^*$. By Theorem 1.23, $|G^*| = rq^n$ for some $n \in \mathbb{N}$. Since p, q, and r are distinct primes, $\gcd(rq^n, char\ \mathbb{Z}_p) = 1$.

We claim M is a minimal normal subgroup of G^*. Suppose $L \leqslant M$ such that $L \trianglelefteq G^*$. Since M is elementary abelian q-group, we have L is an elementary abelian q-group, so L char M. Now $\overline{L}$ char $\overline{M} = \overline{M_0}$ and $\overline{L}$ is ϕ-invariant. By the minimality of $\overline{M_0}$, either $\overline{L} = 1$ or $\overline{L} = \overline{M}$. If $\overline{L} = 1$, then $L \leqslant N$, where N is a p-group. Thus $L = 1$ since L is a q-group with $q \neq p$. If $\overline{L} = \overline{M}$, then $LN = MN$ and since $L \cap N \leqslant M \cap N = 1$, we have $L = M$. Therefore, M is a minimal normal elementary abelian q-subgroup of G^*.

Clearly, $M \leqslant C_{G^*}(M)$. Let $(m, \phi^k) \in C_{G^*}(M)$ for $1 \leq k \leq r$ and suppose $k < r$. Now for all $x \in M$, $(m, \phi^k)(x, 1) = (x, 1)(m, \phi^k)$ and $(mx^{\phi^k}, \phi^k) = (xm, \phi^k)$. This implies $mx^{\phi^k} = xm$, but M is abelian, so $x^{\phi^k} = x$ for all $x \in M$. Thus $\phi^k = 1$ and $r \leq k$, which is a contradiction. Hence $k = r$, $\phi^k = 1$, and $(m, \phi^k) = (m, 1)$, which implies $C_{G^*}(M) = M$. Moreover, since $\langle\phi\rangle$ is cyclic and $|\phi| = r$, we have $\langle\phi\rangle \cong \mathbb{Z}_r$.

Suppose $(m, \phi^k) \in Ker\ \theta$, where $1 \leq k \leq r$. Now $(m, \phi^k)^\theta = 1$ and for all $n \in N$, $(n^{\phi^k})^m = n$ and $n^{\phi^k} m = mn$. If $k < r$, then $\langle\phi^k\rangle = \langle\phi\rangle$ and $C_M(\phi) \leqslant C_G(\phi) = 1$. Moreover,

$$C_M(\phi) \leqslant C_M(\phi^k) \leqslant C_M(\langle\phi^k\rangle) = C_M(\langle\phi\rangle) \leqslant C_M(\phi).$$

Thus $C_M(\phi^k) = C_M(\phi) = 1$, so ϕ^k acts fixed-point-freely on M. By Theorem 7.1, $M = \{[m, \phi^k] : m \in M\}$ and so there exists $m_1 \in M$ such that
$m = [m_1, \phi^k] = m_1^{\phi^k} m_1^{-1}$. Now for all $n \in N$ we have, $n^{\phi^k} m_1^{\phi^k} m_1^{-1} = m_1^{\phi^k} m_1^{-1} n$ and $(n^{m_1})^{\phi^k} = n^{m_1}$. Thus $n^{m_1} \in C_G(\phi^k) = 1$, so $n = 1$, but then $N = 1$. This is a contradiction and so $k = r$. It follows that $\phi^k = 1$ and $nm = mn$. Hence $m \in C_M(N) = 1$ and $m = 1$. Therefore, $(m, \phi^k) = (1, 1), Ker\ \theta = (1, 1)$, and G^* acts faithfully on N over $\mathbb{Z}_p$.

By Theorem 2.14, $1 \neq C_N(\langle\phi\rangle) \leqslant C_G(\langle\phi\rangle) = C_G(\phi) = 1$, which is a contradiction. Therefore, no such counterexample G exists. $\square$

References

[Cur74] Charles W. Curtis. *Linear Algebra: An Introductory Approach.* Springer, New York, New York, 1974.

[DG61] I.N. Herstein Daniel Gorenstein. Finite Groups Admitting a Fixed-Point-Free Automorphism of Order 4. *American Journal of Mathematics*, 83(1):71–78, 1961.

[Gor07] Daniel Gorenstein. *Finite Groups.* AMS Chelsea Publishing, Providence, Rhode Island, second edition, 2007.

[Ral72] Elizabeth Wall Ralston. Solvability of Finite Groups Admitting Fixed-Point-Free Automorphisms of Order rs. *Journal of Algebra*, 23(1):164–180, 1972.

[Tho59] John Thompson. Finite Groups with Fixed-Point-Free Automorphisms of Prime Order. *Proceedings of the National Academy of Sciences of the United States of America*, 45(4):578–581, 1959.

Index