# Reading Project Report


**Daksh Dheer**

(under the supervision of Prof Viji Z. Thomas)

M.S. (Research) Mathematics


# Topics in Finite Group Theory

**October 2024**

# ABSTRACT

Name of the student: **Daksh Dheer** Roll No: **23050**

Thesis title: **Topics in Finite Group Theory** Thesis supervisor: **Prof. Viji Thomas**

The following report explores certain topics in the theory of finite groups, with particular emphasis on several results that are not part of usual curricula. We cover several such crucial results, including the lemmas of Goursat and Ribet, which provide information about the subgroups of direct products of groups. We then discuss an extended notion of normality which helps us provide a theorem of Burnside with an elementary proof. Finally we give an equivalence among the notion of conjugacy with that of local conjugacy by proving Alperin's theorem. We discuss a few results on the Frattini subgroup as well.

The second half of the report is dedicated to studying the transfer homomorphism, first defined (without name) by Issai Schur in 1902. In 1929, Emil Artin applied the same map to Galois groups. In this chapter, we begin by defining this homomorphism and proving several of its properties before moving on to theorems that aid in its computation. We conclude by showing the power of this map in proving several theorems; in this section, the well-known Gauss Lemma from number theory appears as an example of transfer.

# Contents

# Chapter 1

# Results in Group Theory

Throughout this chapter, we will assume that all the groups we work with are finite.

## 1.1 Jordan–Hölder Theorem

A ***finite filtration*** of a group $G$ is a descending sequence of subgroups

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

where $G_{i+1} \triangleleft G_i$ denotes normality of $G_{i+1}$ in $G_i$.

We define $\mathrm{gr}_i(G) := G_i/G_{i+1}$.

The filtration is a ***Jordan–Hölder filtration*** or ***composition series*** of length $n$ if each $\mathrm{gr}_i(G)$ is simple.

**Proposition 1.1.1.** *Every finite group admits a Jordan–Hölder filtration.*

*Proof.* If $G = 1$, then we may take the trivial filtration with $n = 0$. If $G$ is simple, then $G \triangleright 1$ suffices. Suppose $G \neq 1$ and nonsimple. We induct on $|G|$.

The base case is done above. Suppose now $N \triangleleft G$ is of maximal order and $N \neq G$. Then, $G/N$ is simple. Since $|N| < |G|$, we apply the inductive hypothesis to obtain a Jordan–Hölder filtration $(N_i)$ for $N$.

Consider now the filtration $G \triangleright N_0 \triangleright N_1 \triangleright N_2 \triangleright \cdots$

Then, $G/N$ is simple and so is every $N_i/N_{i+1}$, thus this gives a Jordan–Hölder filtration for $G$.

□

**Theorem 1.1.1** (Jordan–Hölder). *Let $(G_i)$ be a Jordan–Hölder filtration. Then, the $\mathrm{gr}_i(G)$ do not depend on the choice of the filtration up to permutation of the indices. In particular, the length is independent of the filtration.*

*Proof.* We may assume that $G \neq 1$, and (by the above proposition) $G$ has a Jordan–Hölder filtration; let $\ell(G)$ denote the length of a shortest one. We use induction on $\ell(G)$.

**Base case:** $\ell(G) = 1$. Then the only Jordan–Hölder filtration is $1 \lhd G$.

**Inductive step:** Suppose that $\ell(G) = n \geq 2$. Let $N$ be the group just below $G$ in a shortest Jordan–Hölder filtration. Thus $N \lhd G$, and $\ell(N)$ and $\ell(G/N)$ are strictly less than $\ell(G)$.

Let $S$ be a simple group and $n(G, (G_i), S)$ denote the number of $j$ such that $\mathrm{gr}_i(G) \cong S$. Note that if $H \leq G$, then $(G_i)$ induces a filtration $(H_i)$ for $H$ by defining $H_i := G_i \cap H$.

Similarly, if $N \lhd G$, then $(G_i)$ gives a filtration $((G/N)_i)$ for $G/N$ by defining $(G/N)_i := G_i/N \cap G_i \cong (G_iN)/N$. Note that this does define a filtration because $G_i \supset G_{i+1} \implies (G_iN)/N \supset (G_{i+1}N)/N$ and $\frac{(G_iN)/N}{(G_{i+1}N)/N} \cong G_iN/G_{i+1}N \cong G_i/G_{i+1}$, which is simple by hypothesis.

In particular, $(G_{i+1}N)/N \lhd (G_iN)/N$.

We have the exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

Now, consider this sequence for every $i$ to get the diagram below:

$$\begin{tikzcd}
1 \arrow[r] & N_{i+1} \arrow[r] \arrow[d] & G_{i+1} \arrow[r] \arrow[d] & (G/N)_{i+1} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & N_i \arrow[r] & G_i \arrow[r] & (G/N)_i \arrow[r] & 1
\end{tikzcd}$$

We apply the Snake Lemma to the diagram above to obtain:

$$1 \longrightarrow \ker(N_{i+1} \to N_i) \longrightarrow \ker(G_{i+1} \to G_i) \longrightarrow \ker((G/N)_{i+1} \to (G/N)_i)$$
$$\longrightarrow \operatorname{coker}(N_{i+1} \to N_i) \longrightarrow \operatorname{coker}(G_{i+1} \to G_i) \longrightarrow \operatorname{coker}((G/N)_{i+1} \to (G/N)_i) \longrightarrow 1$$

which simplifies to the following:

$$1 \longrightarrow N_i/N_{i+1} \longrightarrow G_i/G_{i+1} \longrightarrow (G/N)_i/(G/N)_{i+1} \longrightarrow 1$$

i.e.,

$$1 \longrightarrow \mathrm{gr}_i(N) \longrightarrow \mathrm{gr}_i(G) \longrightarrow \mathrm{gr}_i(G/N) \longrightarrow 1$$

Now, since $(G_i)$ is a Jordan–Hölder filtration, $\mathrm{gr}_i(G) = 1$ or $\mathrm{gr}_i(G)$. Partition the set $I := \{1, 2, \ldots, n\}$ into two sets:

$$I_1 := \{i \in I : \mathrm{gr}_i(N) = 1\}$$

$$I_2 := \{i \in I : \mathrm{gr}_i(N) = \mathrm{gr}_i(G)\}$$

By reindexing $I_1$ (respectively, $I_2$), we obtain a Jordan–Hölder filtration of $N$ (respectively, of $G/N$) of length $|I_1|$ (respectively, $|I_2|$); note that $|I_1| + |I_2| = n$.

The sets $I_1$ and $I_2$ defined above are non-empty; hence, their number of elements is less than $n$, and we can apply the induction hypothesis to $N$ and $G/N$. It shows that $n(N, (N_i)_{i \in I_1}, S)$ and $n(G/N, ((G/N)_i)_{i \in I_2}, S)$ are independent of the choice of filtrations. Since

$$n(G, (G_i)_{i \in I}, S) = n(N, (N_i)_{i \in I_1}, S) + n(G/N, ((G/N)_i)_{i \in I_2}, S),$$

this implies that $n(G, (G_i)_{i \in I}, S)$ is independent of the choice of filtration, which concludes the proof.

□

## 1.2 Subgroups of Products

**Theorem 1.2.1** (Goursat's Lemma)**.** *Let $N_i \lhd G_i$, $i = 1, 2$ and $\varphi : G_1/N_1 \xrightarrow{\sim} G_2/N_2$ be an isomorphism.*

*Let $H_{N_1,N_2,\varphi} := \{(g_1, g_2) : \varphi(g_1 N_1) = g_2 N_2\}$. Then,* *(i)* $\text{proj}_i(H_{N_1,N_2,\varphi}) = G_i$, $i = 1, 2$

*(ii) Every subgroup* $H \leq G_1 \times G_2$ *such that* $\text{proj}_i(H) = G_i$, $i = 1, 2$, *is equal to some* $H_{N_1,N_2,\varphi}$ *for a unique choice of* $N_1, N_2$ *and* $\varphi$.

*Proof.* (i) Let $g_1 \in G_1$. By surjectivity of $\varphi$, $\exists g_2 \in G_2$ such that $\varphi(g_1N_1) = g_2N_2$.

Then, $h = (g_1, g_2) \in H$ and $\text{proj}_1(H) = g_1$. Since $g_1$ was arbitrary, $\text{proj}_1(H) \supseteq G_1$, i.e., $\text{proj}_1(H) = G_1$. Similarly, $\text{proj}_2(H) = G_2$.

(ii) Define $N_i := H \cap G_i$, $i = 1, 2$ where $G_1$ denotes $G_1 \times \{e_2\}$ and $G_2$ denotes $\{e_1\} \times G_2$.

**Claim:** $N_1 = H \cap G_1 = H \cap (G_1 \times \{e_2\})$ is normal in $H$ and $G_2$.

Consider $(e_1, g) \in (h, e_2) \in (e_1, g)^{-1} = (h, e_2) \in N_1$, i.e., $(e_1, g)N(e_1, g)^{-1} = N$, i.e., $N_1$ is normal in $G_2$.

Now, consider arbitrary $(g_1, e_2) \in N_1$ and $(h_1, h_2) \in H$. Then, we have

$$(h_1, h_2)(g_1, e_2)(h_1, h_2)^{-1} = (h_1g_1h_1^{-1}, e_2) \in G_1.$$

Moreover, $(h_1, h_2), (g_1, e_2), (h_1, h_2)^{-1}$ are all in $H$, hence $(h_1g_1h_1^{-1}, e_2) \in H$, i.e., $(h_1g_1h_1^{-1}, e_2) \in N_1$. Therefore, $N_1$ is normal in $H$, and the claim is proved.

Consider

$$H \cdot G_2 := \{(h_1, h_2)(e_1, g_2) : (h_1, h_2) \in H, g_2 \in G_2\}$$
$$= \{(h_1, h_2g_2) : (h_1, h_2) \in H, g_2 \in G_2\}$$

$H \cdot G_2$ is a well-defined subgroup since $G_2$ is normal in $G_1 \times G_2$, i.e., $H \cdot G_2 \leq G_1 \times G_2$. We will show that $H \cdot G_2 = G_1 \times G_2$.

Let $(g_1', g_2') \in G_1 \times G_2$ be arbitrary. Since $\text{proj}_i(H) = G_i$, $\exists (g_1', t_1) \in H$ and $(t_1, g_2') \in H$ such that $\text{proj}_1(g_1', t_2) = g_1'$ and $\text{proj}_2(t_1, g_2') = g_2'$.

For $(h_1, h_2) := (g_1', t_2) \in H$ and $(e_1, g_2) = (e_1, t_2^{-1}g_2') \in G_2$, we have

$$(h_1, h_2)(e_1, g_2) = (g_1', g_2'), \text{ so } H \cdot G_2 \supseteq G_1 \times G_2.$$

Hence, $H \cdot G_2 = G_1 \times G_2$.

**Claim:** $N_1$ is normal in $G_1$.

Consider $(g_1, e_2)(n_1, e_2)(g_1, e_2)^{-1} = (g_1 n_1 g_1^{-1}, e_2)$. We will show this belongs to $N_1$.

Since $N_1$ is normal in both $H$ and $G_1$, it is normal in $H \cdot G_2$ as well, because

$$hg_2 n_1 g_2^{-1} h^{-1} = h(g_2 n_1 g_2^{-1})h^{-1} = hn' h^{-1} = n'' \in N_1.$$

Hence, $N_1$ is normal in $H \cdot G_2 = G_1 \times G_2$.

Now, $(g_1 n_1 g_1^{-1}, e_2) \in N$, because $(g_1 n_1 g_1^{-1}, e_2) = (g_1, g_2)(n_1, e_2)(g_1, g_2)^{-1} \in N$, as $N$ is normal in $G_1 \times G_2$.

Hence, $(g_1, e_2)(n_1, e_2)(g_1, e_2)^{-1} \in N$, i.e., $N_1$ is normal in $G_1$. Similarly, $N_2$ is normal in $G_2$.

Thus, we have uniquely determined $N_i \lhd G_i$, $i = 1, 2$.

Now, consider the following diagram:

$$\begin{tikzcd}
G_1 \times G_2 \arrow[r, "f"] \arrow[dr, "f_1 \circ f"'] & \overline{G_1} \times \overline{G_1} \arrow[d, "f_1"] \\
& \overline{G_1}
\end{tikzcd}$$

Consider the restriction of the map $f_1 \circ f$ to $H$

$$\theta := (f_1 \circ f)\big|_H : H \to G_1/N_1,\ (h_1, h_2) \mapsto h_1 N_1.$$

Then,

$$K := \ker(\theta) = \{(h_1, h_2) : h_1 N_1 = N_1\} = \{(h_1, h_2) : h_1 \in N_1\}$$

**Claim:** $N_1 \times N_2 \subseteq K$.

Let $(n_1, n_2) \in N_1 \times N_2$. Then $\theta(n_1, n_2) = f_1(n_1, n_2 N_2) = n_1 N_1 = N_1$, i.e., $(n_1, n_2) \in K$.

Thus, $\theta$ induces a map

$$\Phi : H/(N_1 \times N_2) \to G_1/N_1,\ (h_1, h_2)(N_1 \times N_2) \mapsto h_1 N_1.$$

Since $\theta$ is a homomorphism, $\Phi$ is also a homomorphism.

We now define $\Psi : G_1/N_1 \to H/(N_1 \times N_2) : g_1N_1 \mapsto (g_1, t)(N_1 \times N_2)$, where $t$ comes from the fact that $\text{proj}_1(H) = G_1$.

**$\Psi$ is a homomorphism:** Consider $g_1N_1, g_1'N_1 \in G_1/N_1$. Let $\Psi(g_1N_1) = (g_1, t)(N_1 \times N_2)$ and $\Psi(g_1'N_1) = (g_1', t')(N_1 \times N_2)$. Now,

$$\Psi(g_1N_1) \cdot \Psi(g_1'N_1) = (g_1, t)(N_1 \times N_2) \cdot (g_1', t')(N_1 \times N_2) = (g_1g_1', tt')(N_1 \times N_2)$$

To prove homomorphism, we need to show

$$(g_1g_1', tt')(N_1 \times N_2) = (g_1g_1', t'')(N_1 \times N_2),$$

i.e., it suffices to prove that $t'' \equiv tt' \mod N_2$.

Since $(g_1g_1', tt')$, $(g_1g_1', t''t'')^{-1}(g_1g_1', tt') \in H$, we have $(e_1, (t'')^{-1}tt') \in H$ and clearly $(e_1, (t'')^{-1}tt') \in G_2$. Thus, $(e_1, (t'')^{-1}tt') \in H \cap G_2 = N_2 \implies t'' \equiv tt' \mod N_2$.

Hence, $\Psi$ is a homomorphism.

Consider

$$\Phi \circ \Psi(g_1, t)(N_1 \times N_2) = \Phi((g_1, t)(N_1 \times N_2)) = g_1N_1, \text{ i.e., } \Phi \circ \Psi = \text{Id}_{G_1/N_1}$$

and

$$\Psi \circ \Phi(h_1h_2)(N_1 \times N_2) = \Psi(h_1N_1) = (h_1, t)(N_1 \times N_2)$$

**Claim:** $(h_1, h_2)(N_1 \times N_2) = (h_1, t_1)(N_1 \times N_2) \iff h_2t_1^{-1} \in N_2$

We identify $h_2t_1^{-1}$ with $(e_1, h_2t_1^{-1})$ since $N_2 = H \cap G_2$ and $G_2$ is viewed as a subgroup of $G_1 \times G_2$ under the identification $G_2 = \{e_1\} \times G_2$.

To prove the claim, we need only show $(e_1, h_2t_1^{-1}) \in H$ since it is already in $G_2$.

But $(h_1, h_2) \in H$ and $(h_1, t_1)^{-1} \in H \implies (h_1, h_2)(h_1, t_1)^{-1} = (e_1, h_2t_1^{-1}) \in H$.

Thus, we are done.

Hence, $\Psi \circ \Phi = \mathrm{Id}_{H/(N_1 \times N_2)}$. Therefore, $\Phi$ is an isomorphism.

We have

$$\Phi : \frac{H}{N_1 \times N_2} \xrightarrow{\sim} \frac{G_1}{N_1} : (h_1, h_2)(N_1 \times N_2) \mapsto h_1 N_1$$

$$\Psi : \frac{G_1}{N_1} \xrightarrow{\sim} \frac{H}{N_1 \times N_2} : g_1 N_1 \mapsto (g_1, t)(N_1 \times N_2)$$

Similarly, we have

$$\Phi' : \frac{H}{N_1 \times N_2} \xrightarrow{\sim} \frac{G_2}{N_2} : (h_1, h_2)(N_1 \times N_2) \mapsto h_2 N_2$$

and so we have an isomorphism

$$f : \frac{G_1}{N_1} \xrightarrow{\Psi} \frac{H}{N_1 \times N_2} \xrightarrow{\Phi'} \frac{G_2}{N_2} \ : \ g_1 N_1 \mapsto (g_1, t)(N_1 \times N_2) \mapsto tN_2$$

We note that if $f(g_1 N_1) = tN_2$, then

$$(g_1, t) \in H \tag{1.1}$$

(since $g_1 N_1 \mapsto (g_1, t)(N_1 \times N_2) \mapsto tN_2$ under $\Phi$).

We now need to show that $H = H_{N_1, N_2, f} = \mathrm{graph}(f) =: H'$

$\underline{H' \subseteq H}$: Let $(h_1', h_2') \in H'$, i.e., $f(h_1' N_1) = h_2' N_2$, hence by (1.1), $(h_1', h_2') \in H$.

$\underline{H \subseteq H'}$: Let $(h_1, h_2) \in H$. We have $f(h_1 N_1) = tN_2$, for some $t \in G_2$.

Hence, $h_1 N_1 \mapsto (h_1, t)(N_1 \times N_2) \mapsto tN_2$. We need to prove that $tN_2 = h_2 N_2$, i.e., $h_2 t^{-1} \in N_2$, i.e., $(e_1, h_2 t^{-1}) \in H \cap G_2$. Clearly, $(e_1, h_2 t^{-1}) \in G_2$. Now, $(h_1, h_2) \in H$ and $(h_1, t) \in H$ by (1.1). Thus, $(h_1, h_2)(h_1, t)^{-1} = (e_1, h_2 t^{-1}) \in H$, so $h_2 t^{-1} \in N_2$, and hence $tN_2 = h_2 N_2$. Therefore, $h_1 N_1 \mapsto h_2 N_2$, and so $(h_1, h_2) \in H'$.

To show uniqueness of $f$, suppose there exists an isomorphism $\lambda : G_1/N_1 \xrightarrow{\sim} G_2/N_2$ such that $f \neq \lambda$.

Consider $H_f'$ and $H_\lambda'$. Both of these are equal to the set $H$, hence $H_f' = H_\lambda'$.

Since $f \neq \lambda$, there exists $g_1N_1 \in G_1/N_1$ such that $f(g_1N_1) \neq \lambda(g_1N_1)$.

Let $f(g_1N_1) = t_1N_2$ and $\lambda(g_1N_1) = t_2N_2$. Then, $(g_1, t_1) \in H'_f$ and $(g_1, t_2) \in H'_\lambda$.
Since $H'_f = H'_\lambda$, and $G_1/N_1 \cong G_2/N_2$, it must be that $t_1N_2 = t_2N_2$.
However, this contradicts the fact that $f(g_1N_1) \neq \lambda(g_1N_1)$. Hence, $f = \lambda$. This concludes the proof.

□

*Remark* 1.1. We know that

$$\frac{H}{H \cap G_1} = \frac{H}{N_1} \cong \frac{HG_1}{G_1} \cong \frac{G_1 \times G_2}{G_1} \cong G_2$$

by the isomorphism given by

$$f_1 : (h_1, h_2)N_1 \mapsto (h_1, h_2)(g_1, e_2)G_1 \mapsto (h_1g_1, h_2)G_1 \mapsto h_2$$
$$(e_1, t_2)N_2 \hookleftarrow (e_1, t_2)(e_1, t_2^{-1})(e_1, g_2)G_1 \hookleftarrow (e_1, g_2)G_1 \hookleftarrow g_2$$

Now, we have the natural map

$$\frac{H}{N_1} \xrightarrow{\pi} \frac{H}{N_1 \times N_2} : (h_1, h_2)N_1 \mapsto (h_1, h_2)(N_1 \times N_2)$$

**Claim:** $\ker \pi = N_2$

Consider

$$\ker \pi = \{(h_1, h_2)(N_1 \times \{e_2\}) : (h_1, h_2) \in N_1 \times N_2\}$$

Now, $f_1 : H/N_1 \xrightarrow{\sim} G_2$. Let $(h_1, h_2)N_1 \in \ker \pi$.

Then, $f((h_1, h_2)N_1) = h_2$ and $(h_1, h_2) \in N_1 \times N_2$ (since $(h_1, h_2) \in \ker \pi$)

Thus, $\ker \pi = \{m \in G : (h_1, h_2) \in N_1 \times N_2\} = N_2 \subseteq G_2$. This proves the claim.

Similarly, if we consider

$$\frac{H}{N_2} \cong \frac{H}{H \cap G_2} \cong \frac{HG_2}{G_2} \cong \frac{G_1 \times G_2}{G_2} \cong G_1$$

and the isomorphism $f_2 : (h_1, h_2)N_2 \mapsto h_1$, and take the natural map

$$\frac{H}{N_2} \xrightarrow{\pi'} \frac{H}{N_1 \times N_2} : (h_1, h_2)N_2 \mapsto (h_1, h_2)(N_1 \times N_2),$$

then we get $\ker \pi' = N_1 \subseteq G_1$

Thus, by first isomorphism theorem, we have

$$\frac{G_1}{N_1} \cong \frac{H/N_2}{N_1} \cong \frac{H}{N_1 \times N_2}$$

and

$$\frac{G_2}{N_2} \cong \frac{H/N_1}{N_2} \cong \frac{H}{N_1 \times N_2}, \text{ i.e., } \frac{G_1}{N_1} \cong \frac{G_2}{N_2}$$

The map is

$$\begin{aligned} \Theta : \frac{G_1}{N_1} \implies \frac{H/N_2}{N_1} \implies \frac{H}{N_1 \times N_2} \implies \frac{H/N_1}{N_2} \implies \frac{G_2}{N_2} \\ g_1N_1 \mapsto (e_1, t_2)N_1 \mapsto (e_1, t_2)(N_1 \times N_2) \mapsto ((e_1, t_2)N_1)N_2 \mapsto t_2N_2 \end{aligned}$$

This is the same map $f$ that we obtained in the earlier proof.

**Theorem 1.2.2** (Goursat's Lemma – Classical Version)**.** *Let $G, H$ be groups. There exists a bijection between the set $\mathcal{S}$ of subgroups of $G \times H$ and the set $\mathcal{T}$ of all triples $(A/B, C/D, \varphi)$ where $B \lhd A \leq G$, $D \lhd C \leq H$, and $\varphi : A/B \to C/D$ is an isomorphism.*

We first describe how to correspond a given triple to a subgroup.

**Lemma 1.2.1.** *Let $(A/B, C/D, \varphi) \in \mathcal{T}$. Define $U_\varphi = \{(g, h) \in A \times C : \varphi(gB) = hD\}$.*

*Then $U_\varphi$ is a subgroup of $G \times H$.*

*Proof.* Let $(g, h), (g', h') \in U_\varphi$. Then $\varphi(gB) = hD$ and $\varphi(g'B) = h'D$.

Consider $(g, h)(g', h') = (gg', hh')$. Then,

$$\varphi(gg'B) = \varphi(gB \cdot g'B) = \varphi(gB) \cdot \varphi(g'B) = hD \cdot h'D = hh'D.$$

Hence, $(gg', hh') \in U_\varphi$.

Now, consider

$$\varphi(gB) = \varphi((gB)^{-1}) = (\varphi(gB))^{-1} = (hD)^{-1} = h^{-1}D,$$

i.e., $(g^{-1}, h^{-1}) \in U_\varphi$. Hence, $U_\varphi$ is a subgroup of $G \times H$.

□

We now describe how to correspond a given subgroup to a triple in $\mathcal{T}$.

**Lemma 1.2.2.** *For a subgroup $U \in \mathcal{S}$, define:*

$$A_U = \{g \in G : (g, h') \in U \textit{ for some } h' \in H\}, B_U = \{g \in G : (g, 1) \in U\},$$

$$C_U = \{h \in H : (g', h) \in U \textit{ for some } g' \in G\}, D_U = \{h \in H : (1, h) \in U\}.$$

*Define $\varphi_U : A_U/B_U \to C_U/D_U$ by $\varphi_U(gB_U) := hD_U$ whenever $(g, h) \in U$.*

*Then, $(A_U/B_U, C_U/D_U, \varphi_U) \in \mathcal{T}$, i.e., $B_U \lhd A_U \leq G$, $D_U \lhd C_U \leq H$, and $\varphi_U$ is an isomorphism.*

*Proof.* **Claim:** The following subgroup properties hold:

- $\underline{A_U \leq G \text{ and } C_U \leq H}$: Let $a, a' \in A_U$. Then there exist $h, h' \in H$ such that $(a, h), (a', h') \in U$. Since $(a, h)(a', h') = (aa', hh') \in U$, it follows that $aa' \in A_U$. Also, $(a', h')^{-1} = (a'^{-1}, h'^{-1}) \in U$, so $a'^{-1} \in A_U$. Hence, $A_U \leq G$. A similar argument shows that $C_U \leq H$.
- $\underline{B_U \lhd A_U \text{ and } D_U \lhd C_U}$: Let $b \in B_U$, $a \in A_U$. Then $(b, 1) \in U$, and there exists $h \in H$ such that $(a, h) \in U$. Then $(a, h)(b, 1)(a, h)^{-1} = (aba^{-1}, 1) \in U \implies aba^{-1} \in B_U$. Hence, $B_U \lhd A_U$. Similarly, $D_U \lhd C_U$.

**Claim:** $\varphi_U$ is an isomorphism.

Consider

$$\varphi_U : A_U/B_U \to C_U/D_U : gB_U \mapsto hD_U \text{ whenever } (g, h) \in U,$$

and

$$\psi_U : C_U/D_U \to A_U/B_U : hD_U \mapsto gB_U \text{ whenever } (g, h) \in U.$$

<ins>Well-definedness:</ins> Suppose $\varphi_U(gB_U) = \varphi_U(g'B_U)$. Now since $g, g' \in A_U$, there exist $h, h' \in C_U$

such that $(g,h),(g',h') \in U$. Then we have $hD_U = h'D_U \implies h^{-1}h' \in D_U \implies (1,h^{-1}h') \in U$. Now,

$$(g^{-1}h)(g'h') = (g^{-1}g', h^{-1}h') \in U \text{ and } (1,h^{-1}h') \in U.$$

Therefore,

$$(1,h^{-1}h')^{-1}(g^{-1}g',h^{-1}h') = (g^{-1}g',1) \in U \implies g^{-1}g' \in B_U.$$

Hence, $gB_U = g'B_U$, i.e., $\varphi_U$ is well-defined.

Now, suppose $\phi_U(hD_U) = \phi_U(h'D_U)$. Since $hh'^{-1} \in D_U$, there exist $g, g' \in G$ such that $(g,h),(g',h') \in U$. Thus, we have $gB_U = g'B_U \implies g^{-1}g' \in B_U \implies (g^{-1}g',1) \in U$.

Now, $(g,h)(g^{-1}g',1) = (g',hh') \in U$ and $(g',h') \in U$. Therefore, $(g'^{-1},h'^{-1})(g',hh') = (1,h'^{-1}hh') \in U \implies h'^{-1}h \in D_U$.

Hence, $hD_U = h'D_U$, i.e., $\phi_U$ is well-defined.

Clearly, $\varphi_U \circ \phi_U(hD_U) = \varphi_U(gB_U)$ where $(g,h) \in U$ and so equals $h'D_U$ where $(g,h') \in U$.

Now, $(g,h)^{-1}(g,h') = (1,h^{-1}h') \in U \implies h^{-1}h' \in D_U \implies hD_U = h'D_U$.

Hence, $\varphi_U \circ \phi_U = \mathrm{Id}_{C_U/D_U}$. Similarly, $\phi_U \circ \varphi_U = \mathrm{Id}_{A_U/B_U}$.

Hence, $\varphi_U$ is a bijection. We will show it is a homomorphism.

Now, let $\varphi_U(gB_U) = h'D_U$, $\varphi_U(g'B_U) = hD_U$ and $\varphi_U(g'gB_U) = h''D_U$.

Then, $(g,h),(g',h'),(gg',h'') \in U$.

Consider $(g,h)(g',h')(gg',hh')^{-1}$. We have

$(g,h)(g',h')(gg',hh')^{-1} = (1,hh'(h'')^{-1}) \in U \implies hh'(h'')^{-1} \in D_U \implies hh' = h'' \mod D_U$,

Thus, $\varphi_U(gB_U) \cdot \varphi_U(g'B_U) = \varphi_U(gg'B_U)$.

Therefore, $\varphi_U$ is an isomorphism.

$\square$

**Theorem 1.2.3.** *Define $\alpha : \mathcal{S} \to \mathcal{T}$ by $\alpha(u) = (A_U/B_U, C_U/D_U, \varphi_U)$, and $\beta : \mathcal{T} \to \mathcal{S}$ by $\beta(A/B, C/D, \varphi) = U_\varphi$. The map $\alpha$ is a bijection with inverse $\beta$.*

*Proof.* Recall that

$$A_U = \{g \in G : (g,h) \in U \text{ for some } h \in H\},$$

$$B_U = \{g \in G : (g,1) \in U\},$$

$$C_U = \{h \in H : (g,h) \in U \text{ for some } g \in G\},$$

$$D_U = \{h \in H : (1,h) \in U\},$$

$$U_\varphi = \{(g,h) \in G \times H : \varphi(gB) = hD\},$$

$$\varphi_U \colon A_U/B_U \xrightarrow{\sim} C_U/D_U.$$

Consider $\beta\alpha(V) = \beta(A_V/B_V, C_V/D_V, \varphi_V) = U_{\varphi_V}$. Now, $U_{\varphi_V} = \{(g,h) : \varphi_V(gB_V) = hD_V\}$.

Let $(v_1, v_2) \in V$. Then, $\varphi_V(v_1 B_V) = v_2 D_V$, so $(v_1, v_2) \in U_{\varphi_V}$, so $V \subseteq U_{\varphi_V}$.

Conversely, let $(v_1, v_2) \in U_{\varphi_V}$, i.e., $\varphi_V(v_1 B_V) = v_2 D_V$. Then $v_1 \in A_V$ and $v_2 \in C_V$, i.e., there exist $t, t'$ such that $(v_1, t), (t', v_2) \in V$.

Now, this implies $\varphi_V(v_1 B_V) = tD_V$ and $\varphi_V(t' B_V) = v_2 D_V$. Therefore, $v_2 \equiv t \mod D_V$ and $t' \equiv v_1 \mod B_V$, since $\varphi_V$ is an isomorphism.

It follows that $v_2 t^{-1} \in D_V$ and $t' v_1^{-1} \in B_V$, so $(1, v_2 t^{-1}), (t' v_1^{-1}, 1) \in V$, by definition of $D_V$ and $B_V$.

We want to show that $(v_1, v_2) \in V$; this is clear because $(v_1, v_2) = (1, v_2 t^{-1})(v_1, t)$, both of which are in $V$. Hence, $(v_1, v_2) \in V$. Thus, $V \subseteq U_{\varphi_V}$, and therefore $V = U_{\varphi_V}$.

Hence, $\beta\alpha(V) = V$, i.e., $\beta\alpha = \mathrm{Id}_{\mathcal{S}}$.

Now, consider $\alpha\beta(A/B, C/D, \varphi) = \alpha(U_\varphi) = (A_{U_\varphi}/B_{U_\varphi}, C_{U_\varphi}/D_{U_\varphi}, \varphi_{U_\varphi}) = (A_U/B_U, C_U/D_U, \varphi_U)$.

By definition, we have:

$$
\begin{aligned}
A_U &= \{g \in G : (g, h') \in U \text{ for some } h' \in H\} \\
&= \{g \in G : \varphi(gB) = h'D \text{ for some } h' \in H\}, \\
B' &= \{g \in G : (g, 1) \in U_\varphi\} = \{g \in G : \varphi(gB) = D\}, \\
C' &= \{h \in H : (g', h) \in U_\varphi \text{ for some } g' \in G\} = \{h \in H : \varphi(g'B) = hD \text{ for some } g' \in G\}, \\
D' &= \{h \in H : (1, h) \in U_\varphi\} = \{h \in H : \varphi(B) = hD\}, \\
U_\varphi &= \{(g, h) \in A \times C : \varphi(gB) = hD\}.
\end{aligned}
$$

**Claim:** The following equalities hold:

- $\underline{A = A'}$: Let $a' \in A'$, then $(a', h') \in U_\varphi$ for some $h' \in H$, which implies $(a', h') \in A \times C \implies a' \in A$, so $A' \subseteq A$.

  Conversely, if $a \in A$, then $aB \in A/B$ and $\varphi(aB) = cD$ for some $c \in C$, so $(a, c) \in U_\varphi \implies a \in A'$, hence $A \subseteq A'$.

- $\underline{B = B'}$: Let $b' \in B'$, then $(b', 1) \in U_\varphi \implies \varphi(b'B) = D \implies b'B = B \implies b' \in B$.

  Conversely, if $b \in B$, then $\varphi(bB) = D \implies b \in B'$.

- $\underline{C = C'}$: Let $c' \in C'$, then $(g', c') \in U_\varphi$ for some $g' \in G$, so $(g', c') \in A \times C \implies c' \in C$, hence $C' \subseteq C$.

  Conversely, if $c \in C$, then $cD \in C/D$, and $\bar{\varphi}(cD) = aB$ for some $a \in A$, so $(a, c) \in U_\varphi \implies c \in C'$, hence $C \subseteq C'$.

- $\underline{D = D'}$: Let $d' \in D'$, then $(1, d') \in U_\varphi \implies \varphi(B) = d'D \implies d'D = D \implies d' \in D$.

  Conversely, if $d \in D$, then $\bar{\varphi}(dD) = B \implies d \in D'$.

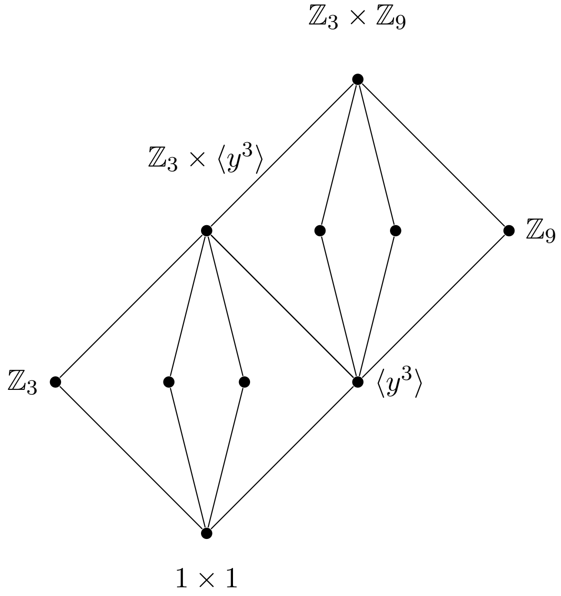
Hence, $\alpha\beta = \mathrm{Id}_{\mathcal{T}}$.

$\square$

*Example* 1.1. Let $G = \mathbb{Z}_3 = \langle x \rangle$ and $H = \mathbb{Z}_9 = \langle y \rangle$. Within $G \times H$, the six subgroups

$$1 \times 1, \quad 1 \times \langle y^3 \rangle, \quad 1 \times \mathbb{Z}_9, \quad \mathbb{Z}_3 \times 1, \quad \mathbb{Z}_3 \times \langle y^3 \rangle, \quad \text{and } \mathbb{Z}_3 \times \mathbb{Z}_9$$

arise from the trivial quotients. The group $\mathbb{Z}_3$ has only one nontrivial quotient, namely $\mathbb{Z}_3/1$, which is isomorphic to both $\mathbb{Z}_9/\langle y^3\rangle$ and $\langle y^3\rangle/1$ in $\mathbb{Z}_9$. Each of these corresponding pairs yields two subgroups, one for each of the two distinct automorphisms of $C_3$.




**Theorem 1.2.4** (Ribet's Lemma). *Let $H$ be a subgroup of $G_1 \times G_2 \times \cdots \times G_n$ such that $\mathrm{proj}_{ij}(H) = G_i \times G_j$ for every $i, j$. Assume that the groups $G_i$, with at most two exceptions, can be generated by commutators. Then $H = G_1 \times G_2 \times \cdots \times G_n$.*

*Proof.* We induct on $n$.

If $n = 2$, then $H$ is a subgroup of $G_1 \times G_2$ such that $\mathrm{proj}_{12}(H) = G_1 \times G_2$.

Since the projection map is the identity in this case, it follows that $H = G_1 \times G_2$.

Now suppose $n \geq 3$. Assume $G_1$ is generated by commutators. By the induction hypothesis, the projection $H \longrightarrow G_1 \times \cdots \times G_{n-1}$ is surjective. Thus, we only need to show that $H$ contains $G_1$, i.e., $G_1 \times \{e_1\} \times \cdots \times \{e_{n-1}\} \subseteq H$.

Since $G_1$ is generated by commutators, it suffices to prove that for any $x, y \in G_1$, the commutator $[x, y] \in H$.

We have $\mathrm{proj}_{1n}(H) = G_1 \times G_n$, so there exists $u \in G_1 \times \cdots \times G_{n-1}$ such that $(x, u, e_n) \in H$. As before, the induction hypothesis implies $H \twoheadrightarrow G_2 \times \cdots \times G_{n-1}$, thus there exists $v \in G_n$ such that $(y, e_1, \ldots, e_{n-1}, v) \in H$. Now,

$$(xyx^{-1}y^{-1}, e_1, \ldots, e_{n-1}, e_n) = (x, u, e_n)(y, e_1, \ldots, e_{n-1}, v)(x, u, e_n)^{-1}(y, e_1, \ldots, e_{n-1}, v)^{-1} \in H.$$

Since $H$ is a subgroup, this commutator lies in $H$. Thus, $[x, y] \in H$, and since such elements generate $G_1$, we conclude $G_1 \subseteq H$. Hence, $H = G_1 \times \cdots \times G_n$. □

We now apply these two theorems to obtain the following results:

**Proposition 1.2.1.** *Let $(N_i)_{i\in I}$ be a finite family of pairwise distinct normal subgroups of a group $G$. Suppose that the $G/N_i = \overline{G}_i$ are simple and at most two of them are abelian. Show that the map $G \to \prod_i \overline{G}_i$ is surjective.*

*Proof.* Suppose $|I| = 2$. Then, by hypothesis, we have $N_i \lhd G$ such that $\overline{G}_i$ are simple, $i = 1, 2$.

Consider $H = \text{image}(f) = \{(gN_1, gN_2) : g \in G\} \leq \overline{G}_1 \times \overline{G}_2$.

Now, we have $\pi_1 : G \to G/N_1$. We have $\pi_1(N_2) \lhd G/N_1 \implies \pi_1(N_2) = G/N_1$, since $G/N_1$ is simple. Similarly, $\pi_2(N_1) = G/N_2$, thus $f(N_1N_2) = G/N_1 \times G/N_2$.

In particular, $H = \text{Im}(f) \supseteq G/N_1 \times G/N_2$, i.e., $f$ is surjective.

Now, suppose $|I| = n > 2$. Let $\overline{G}_i'$ denote the commutator subgroup of $\overline{G}_i$. Since $\overline{G}_i' \lhd \overline{G}_i$ and $\overline{G}_i$ are simple, we must have either $\overline{G}_i' = \overline{G}_i$ or $\{e\}$. If $\overline{G}_i' = \{e\}$, then $\overline{G}_i$ is abelian, otherwise $\overline{G}_i' = \overline{G}_i$ implies that $\overline{G}_i$ is generated by commutators.

By hypothesis, at most two of $\overline{G}_i$ are abelian, thus, all $\overline{G}_i$ are generated by commutators with at most two exceptions.

As before, let $H = \text{image}(f) = \{(gN_1, gN_2, \ldots, gN_n) : g \in G\} \leq \prod_i \overline{G}_i$.

Consider now $\text{proj}_{i,j}(H) = \{(gN_i, gN_j) : g \in G\} = \overline{G}_i \times \overline{G}_j$,which follows from the case $|I| = 2$.

Hence, we may apply Ribet's lemma to conclude $H = \prod_i \overline{G}_i$.

Since $\text{image}(f) = \text{range}(f)$, we conclude that $f$ is surjective. This finishes the proof.

□

**Proposition 1.2.2.** *Let $f_i : G \to G_i$, $i = 1, 2$, be surjective homomorphisms such that $f = (f_1, f_2) : G \to G_1 \times G_2$ is not. Then there exists a nontrivial group $A$ with surjective homomorphisms $\rho_i : G_i \to A$ such that $\rho_1 \circ f_1 = \rho_2 \circ f_2$ on $G$.*

*Proof.* Consider $H = \text{Image}(f) = \{(f_1(g), f_2(g)) : g \in G\} \subsetneq G_1 \times G_2$. Note that the containment is strict as $f$ is not surjective.

Now, $\mathrm{proj}_i(H) = \{f_i(g) : g \in G\} = G_i$ since $f_i$ are surjective.

We apply Goursat's lemma to obtain $N_i \lhd G_i$ and $\varphi : G_1/N_1 \to G_2/N_2$ such that

$$H = H' := \{(g_1, g_2) : \varphi(g_1 N_1) = g_2 N_2\}.$$

Define $A := G_1/N_1 \cong G_2/N_2$.

Consider the homomorphisms

$$\rho_1 : G_1 \to A : g_1 \mapsto g_1 N_1$$
$$\rho_2 : G_2 \to A : g_2 \mapsto \varphi^{-1}(g_2 N_2).$$

Note that $\rho_i$ are surjective since they are projection maps and they are well-defined since $\varphi$ is an isomorphism.

**Claim:** $\rho_1 \circ f_1(g) = \rho_2 \circ f_2(g)\ \forall g \in G$.

Let $g \in G$ be arbitrary. Then, $\rho_1 \circ f_1(g) = \rho_1(f_1(g)) = f_1(g)N_1$.

Similarly, $\rho_2 \circ f_2(g) = \varphi^{-1}(f_2(g)N_2)$.

Now, $(f_1(g), f_2(g)) \in H$ and $H = H' \implies (f_1(g), f_2(g)) \in H'$.

Thus, $\varphi(f_1(g)N_1) = f_2(g)N_2 \implies f_1(g)N_1 = \varphi^{-1}(f_2(g)N_2)$.

This proves the claim and we are done. □

## 1.3 Burnside's and Alperin's Theorems

Let $S, K$ be subgroups of $G$ such that $S \subset K$. Two elements (or subsets) of $H$ are said to ***fuse*** in $K$ if they are $K$-conjugate.

We extend the notion of normality: if $X \subset G$ and $H$ is a subgroup of $G$, then we say $X$ is ***H-normal*** if $H \subset N_G(X)$, that is, if $hXh^{-1} = X$ for all $h \in H$.

**Proposition 1.3.1.** *Let $S$ be a $p$-Sylow subgroup of $G$ and $(A_i, B_i)_{i \in I}$ be two families of $S$-normal subsets of $S$. Let $g \in G$ be such that $gA_ig^{-1} = B_i$ for every $i$. Then, there exists $n \in N_G(S)$ such that $nA_in^{-1} = B_i$ for every $i$.*

*Proof.* Consider $N_A = \bigcap_{i\in I} N_G(A_i)$ and $N_B = \bigcap_{i\in I} N_G(B_i)$. Since $gA_ig^{-1} = B_i$ for every $i$, we have $gN_Ag^{-1} = N_B$. Moreover, $S$-normality of $A_i$ and $B_i$ implies that $S \subset N_A \cap N_B$. In particular, we have $gSg^{-1} \subset N_B$. Now, the groups $S$ and $gSg^{-1}$ are both $p$-Sylow subgroups of $N_B$, hence there exists $z \in N_B$ with $zSz^{-1} = gSg^{-1}$. Thus, $n = z^{-1}g \in N_G(S)$ and we have $nA_in^{-1} = z^{-1}gA_ig^{-1}z = z^{-1}B_iz = B_i$ for every $i$, as required. □

**Corollary 1.3.0.1.** *If two normal subgroups of $S$ are conjugate in $G$, then they are conjugate in $N_G(S)$.*

**Theorem 1.3.1** (Burnside)**.** *Let $X, Y \subset Z(S)$ be subsets of the center of $S$. Let $g \in G$ be such that $gXg^{-1} = Y$. Then, there exists $n \in N_G(S)$ such that $nxn^{-1} = gxg^{-1}$ for every $x \in X$. In particular, $nXn^{-1} = Y$.*

*Proof.* We apply the previous theorem with indexing set $I = X, A_x = \{x\}, B_x = \{gxg^{-1}\}$. Since $A_x, B_x \subset Z(S)$, they are $S$-normal. Hence, there exists $n \in N_G(S)$ such that $nxn^{-1} = gxg^{-1}$ for every $x \in X$. □

**Corollary 1.3.1.1.** *Let $x, y \in Z(S)$, If $x$ and $y$ are conjugate in $G$, then they are conjugate in $N_G(S)$.*

We call two elements $x, y \in S$ ***locally conjugate*** if there exists a subgroup $U \leq S$ such that $x$ and $y$ are conjugate in $N_G(U)$.

**Lemma 1.3.1.** *Let $A \subseteq S$ and $g \in G$ such that $g^nAg^{-1} := A^g \subseteq S$. Then there exist an integer $n \geq 1$, subgroups $U_1, U_2, \ldots, U_n$ of $S$ and $g_1, g_2, \ldots, g_n \in G$ such that:*

*i)* $g = g_1g_2\ldots g_n$.

*ii)* $g \in N_G(U_i)$ *for* $1 \leq i \leq n$.

*iii)* $A^{g_1g_2\cdots g_{i-1}} \subset U_i$ *for* $1 \leq i \leq n$

*Proof.* Let $T \leq S$ such that $T = \langle A\rangle$. We induct on $[S : T]$.

If $[S : T] = 1$, then $T = S$ and $g^{-1}Sg = S$, i.e., $g \in N_G(S)$. We may take $n = 1$, $g = g_1$ and $S = U_1$.

Suppose $[S : T] > 1$ i.e., $T \neq S$. Then $T \leq S$ and $N_S(T) = T_1 \neq T$. $T_1$ is a $p$-subgroup of $N_G(T)$, since it is contained in $S$. We choose a $p$-Sylow subgroup $\Sigma \subset N_G(T)$ containing $T_1$.

Then $\exists u \in G$ such that $u^{-1}\Sigma u = \Sigma^u \subset S$.

Now, let $V = g^{-1}Tg = T^g$. We have $V \subset S$ as $T \subset S$, since $g^{-1}Ag = S$. Now, $g^{-1}\Sigma g = \Sigma^g$ is a $p$-Sylow subgroup of $N_G(V) = g^{-1}N_G(T)g = N_G(T)^g$. Since $N_S(V)$ is a $p$-subgroup of $N_{G(V)}$ and so $\exists w \in N_G(V)$ such that $w^{-1}N_S(V)w \subset g^{-1}\Sigma g = \Sigma^g$. Set $v = u^{-1}gw^{-1} \implies g = uvw$.

We have $T_1^u \subseteq \Sigma^u \subseteq S$ as $T \subseteq \Sigma$. Since $[S : T_1] < [S : T]$, we apply the induction hypothesis to obtain subgroups $U_1, U_2, \ldots, U_m$ of $S$ and $u_i \in N_G(U_i)$ with $u = u_1u_2\ldots u_m$ and $T_1^{u_1u_2\ldots u_{i-1}} \subset U_i$ for $1 \leq i \leq m$.

Set $T_2 = N_S(V)$ and $T_3 = T_2^{v^{-1}} = T_2^{wg^{-1}u}$. We have $T_2^w \subseteq \Sigma^g$, thus, $T_3 = T_2^{wg^{-1}u} = (wg^{-1}u)^{-1}T_2(wg^{-1}u) = u^{-1}g(w^{-1}T_2w)g^{-1}u \subset u^{-1}g(\Sigma^g)g^{-1}u = \Sigma^{gg^{-1}u} = \Sigma^u$.

The group $T_3 \subseteq S$ and $T_3^v = T_2 \subseteq S$. Since $[S : T_3] < [S : T]$, we apply the induction hypothesis to obtain subgroups $V_1, V_2, \ldots, V_s$ of $S$ and $v_j \in N_G(V_j)$ with $v = v_1v_2\ldots v_r$ and $T^{v_1v_2\ldots v_{i-1}} \subset V_j$ for $1 \leq j \leq r$.

**Claim:** The subgroups $U_1, U_2, \ldots, U_m, V_1, V_2, \ldots, V_r$ of $S$ and the factorization $g = u_1u_2\ldots u_mv_1v_2\ldots v_rw$ satisfy the required properties.

Consider $u_i \in N_G(U_i)$, $v_j \in N_G(V_j)$, $w \in N_G(V)$ and $T^{u_1u_2\ldots u_{i-1}} \subset U_i$ for $1 \leq i \leq m$ since $T \subseteq T_1$. We now need to check that $T^{u_1u_2\ldots u_mv_1v_2\ldots v_{j-1}} \subseteq V_j$ for $1 \leq j \leq r$.

Consider $T^{gw^{-1}} = V^{w^{-1}} = V \subset N_S(V) = T_2$. Hence, $T \subset T_2^{wg^{-1}}$ and $T^u \subset T_2^{wg^{-1}u} = T_3$. Thus, we have $T^{u_1u_2\ldots u_mv_1v_2\ldots v_{j-1}} = T^{uv_1v_2\ldots v_{j-1}} \subset T_3^{v_1v_2\ldots v_{j-1}} \subset V_j$ for $1 \leq j \leq r$. This concludes the proof. $\square$

**Theorem 1.3.2** (Alperin)**.** *If $x$ and $y$ are conjugate in $G$, then there exists a sequence $a_0, a_1, \ldots, a_n \in S$ such that:*

1. *$a_0 = x$ and $a_n = y$.*
2. *$a_i$ is locally conjugate to $a_{i+1}$ for $1 \leq i \leq n-1$.*

*In particular, the local conjugacy classes of $S$ coincide with the conjugacy classes of $G$.*

*Proof.* Take $A = \{x\} \subset S$ and $g \in G$ such that $g^{-1}xg = y$. We have $A^g + \{g^{-1}xg\} = \{y\} \subset S$. Then, by the previous lemma, there exist subgroups $U_1, U_2, \ldots, U_n$ of $S$ and $g_1, g_2, \ldots, g_n \in G$ such that $g = g_1g_2\ldots g_n$ and $x^{g_1g_2\ldots g_{i-1}} \subset U_i$ for $1 \leq i \leq n$.

Define $a_0 = x,\ a_1 = x^{g_1},\ a_2 = x^{g_1 g_2}, \dots,\ a_n = x^{g_1 g_2 \cdots g_n} = x^g = y$. Now, $g \in N_G(U_i)$ for $1 \leq i \leq n \implies g_{i+1}^{-1} a_i g_{i+1} \in U_{i+1}$, whence we get each $a_i$ is locally conjugate to $a_{i+1}$. □

## 1.4 The Frattini Subgroup

Let $G$ be a finite group. The intersection of all maximal subgroups of $G$ is called the **Frattini subgroup** of $G$, and is denoted by $\Phi(G)$. It is a characteristic subgroup of $G$.

**Proposition 1.4.1.** *Let $S \leq G$ and $H = \langle S \rangle$. Then $\Phi(G) = H$ if and only if $H$ generates $G/\Phi(G)$.*

*Proof.* Suppose $H = G$. Then $H \cdot \Phi(G) = G \cdot \Phi(G) = G$. Conversely, if $G = H \cdot \Phi(G)$ and $H \neq G$, then there is a maximal $H' \supset H$, which implies $H' \supset \Phi(G)$, whence $G = H \cdot \Phi(G) \subset H' \implies H' = G$, a contradiction. □

*Remark* 1.2. This shows that elements of $\Phi(G)$ are non-generators of $G$; that is, if $S$ generates $G$, then so does $S \setminus (S \cap \Phi(G))$.

**Lemma 1.4.1.** *Let $G$ be a finite group. If $\Phi(G)$ is nilpotent, then $G$ is nilpotent.*

*Proof.* **Claim**: If for every prime $p \mid |G|$, there exists a unqiue $p$-Sylow subgroup, then $G$ is nilpotent.

Under the hypothesis, we know all Sylow subgroups of $G$ are normal and pairwise disjoint. Let $P_1, P_2, \dots, P_k$ be the distinct Sylow subgroups of $G$. Since $P_1 P_2 \dots P_k \subset G$ and $|G| = |P_1 P_2 \dots P_r|$, we get $G \cong P_1 \times P_2 \times \cdots \times P_k$, which is a direct product of $p$-groups. We also have $(P_1 P_2 \dots P_i) \cap P_{i+1} = 1$ for all $2 \leq i \leq k$, hence $G \cong P_1 \oplus P_2 \oplus \cdots \oplus P_k$. Therefore, $G$ is nilpotent, as it is a product of finitely many nilpotent groups. □

**Lemma 1.4.2** (Frattini Argument)**.** *Let $N \lhd G$, and let $P$ be a Sylow $p$-subgroup of $N$. Then $G = N_G(P)N$.*

*Proof.* Let $g \in G$. Now, $P \subset N \implies P^g \subset N^g = N$. Since $|P^g| = |P|$, we have that $P^g$ is a $p$-Sylow subgroupof $N$. Therefore, there exists $n \in \mathbb{N}$ such that $(P^g)^n = P$, i.e., $gn \in N_G(P)$, whence $g \in N_G(P)N$. This gives $G \subset N_G(P)N \implies G = N_G(P)N$

□

**Theorem 1.4.1.** *Let $G$ be finite. Then $\Phi(G)$ is nilpotent.*

*Proof.* We will show that for every prime $p \mid |G|$, there exists a unqiue $p$-Sylow subgroup, then the result follows by Lemma 1.4.1. Let $S$ be a $p$-Sylow subgroup of $Phi(G)$. We know $Phi(G) \lhd G$, thus by the Frattini argument, $G = N_G(S)\Phi(G)$. Using Proposition 1.4.1, we have $G = N_G(S)$, yielding $S \lhd G \implies S \lhd \Phi(G)$.

Hence, $S^l = S$ for all $l \in \Phi(G)$, i.e., $S$ is the unique $p$-Sylow subgroup. □

# Chapter 2

# The Transfer Homomorphism

We impose no restriction on the order of the groups we deal with. In particular, they may be infinite.

## 2.1 Properties of the Transfer

Let $G$ be a group and $H$ be a subgroup of $G$ of finite index. Let $X = G/H$ and $\varphi : X \to G$ be a section, i.e., $\pi \circ \varphi = \mathrm{id}_X$, where $\pi : G \to G/H$ is the natural projection.

**Claim:** $\varphi(gx) \equiv g\varphi(x) \mod H$.

*Proof.* Let $x = tH$. We will show that $gx$ is a coset containing $g\varphi(x)$. Now, $gx = gtH$ and $\pi \circ \varphi(tH) = tH$, i.e., $\varphi(tH) \in tH$, i.e., $\varphi(x) \in x$. This follows because: $\pi(z) = yH \implies zH = yH \implies z \in yH$. Therefore, $g\varphi(x) \in gx$, i.e., $gx$ is a coset containing $g\varphi(x)$. Hence, both $g\varphi(x)$ and $\varphi(gx)$ lie in the coset $gx$, i.e., $g\varphi(x) \equiv \varphi(gx) \mod H$. $\square$

Then, there exists a unique $h^{\varphi}_{gx} \in H$ such that

$$g\varphi(x) = \varphi(gx)\, h^{\varphi}_{gx}. \tag{2.1}$$

The uniqueness follows from the fact that:

$$g\varphi(x) \equiv \varphi(gx) \mod H \iff \varphi(gx)\varphi(x)^{-1}g^{-1} =: h^{\varphi}_{gx} \in H.$$

This $h^{\varphi}_{gx}$ is unique since it is determined by the fixed elements $g,\ \varphi(x),\ \varphi(gx)$. We define

$$\mathrm{Ver} : G \to H^{\mathrm{ab}} = H/D(H) : g \mapsto \prod_{x \in X} h^{\varphi}_{g,x} \mod D(H),$$

where $D(H)$ denotes the commutator subgroup $[H, H]$.

**Theorem 2.1.1.** $\mathrm{Ver} : G \to H^{\mathrm{ab}}$ *is a homomorphism and independent of the choice of section* $\varphi$.

*Proof.* Independence of $\varphi$: Suppose $\varphi'$ is another section, then $\pi \circ \varphi = \pi \circ \varphi' = \mathrm{id}$, therefore $\varphi(x)$ and $\varphi'(x)$ have the same image under $\pi$, i.e., $\varphi(x) \equiv \varphi'(x) \mod H$.

Hence, $\varphi'(x) = \varphi(x)\theta(x)$ where $\theta(x) \in H$.

Now, for $g \in G$, we have $g\varphi'(x) = g\varphi(x)\theta(x) = \varphi(gx)h^{\varphi}_{g,x}\theta(x) = \varphi'(gx)(\theta(gx))^{-1}h^{\varphi}_{g,x}\theta(x)$ since $\varphi(gx) = \varphi'(gx)(\theta(gx))^{-1}$.

Therefore, $h^{\varphi'}_{g,x} = (\theta(gx))^{-1}h^{\varphi}_{g,x}\theta(x)$.

Since $\{x : x \in G/H\} = \{gx : x \in G/H\}$, we have

$$\prod_{x \in X} h^{\varphi'}_{g,x} \equiv \prod_{x \in X} (\theta(gx))^{-1}h^{\varphi}_{g,x}\theta(x) = \prod_{x \in X} h^{\varphi}_{g,x} \mod D(H).$$

This proves independence.

Homomorphism: For $g' \in G$, we have $gg'\varphi(x) = g\varphi(g'x)h^{\varphi}_{g',x} = \varphi(gg'x)h^{\varphi}_{g,g'x}h^{\varphi}_{g,x}$.

Therefore, $h^{\varphi}_{gg',x} = h^{\varphi}_{g,g'x}h^{\varphi}_{g',x}$ and $\prod_x h^{\varphi}_{gg',x} = \mathrm{Ver}(g)$ as $\{x : x \in G/H\} = \{g'x : x \in G/H\}$.

Hence, $\prod_x h^{\varphi}_{gg',x} = \prod_x h^{\varphi}_{g,g'x} \cdot \prod_x h^{\varphi}_{g',x} \implies \mathrm{Ver}(gg') = \mathrm{Ver}(g) \cdot \mathrm{Ver}(g')$ $\square$

**Theorem 2.1.2.** *Let* $n = (G : H)$ *and let* $i : H^{\mathrm{ab}} \to G^{\mathrm{ab}}$ *be the map deduced from the injection* $H \hookrightarrow G$. *The composite map* $G \xrightarrow{\mathrm{Ver}} H^{\mathrm{ab}} \xrightarrow{i} G^{\mathrm{ab}}$ *is* $g \mapsto g^n$.

*Proof.* We have $g\varphi(x) = \varphi(gx)h^{\varphi}_{g,x}$. Thus, $\prod_x g\varphi(x) = \prod_x \varphi(gx)h^{\varphi}_{g,x}$.

Since $G^{\mathrm{ab}}$ is abelian, we have

$$\begin{aligned}\left(\prod_x g\right)\left(\prod_x \varphi(x)\right) &= \left(\prod_x \varphi(gx)\right)\left(\prod_x h_{g,x}^{\varphi}\right) \mod D(G)\\ \implies g^n \prod_x \varphi(x) &= \prod_x \varphi(gx)\cdot \mathrm{Ver}(g) \mod D(G)\\ \implies g^n &= \mathrm{Ver}(g) \mod D(H)\end{aligned}$$

Note that $\prod_x \varphi(x) = \prod_x \varphi(gx)$ since as $x$ runs over $X,$ so does $gx$.

$\square$

**Corollary 2.1.2.1.** *If $G$ is abelian, then* $\mathrm{Ver}(g) = g^n$ *for all $g \in G$.*

*Proof.* If $G$ is abelian, then $G^{\mathrm{ab}} = G$, and from the above theorem, $\mathrm{Ver}(g) = g^n$ for all $g \in G^{\mathrm{ab}} = G$.

$\square$

**Theorem 2.1.3** (Functionality)**.** *If $\sigma : (G, H) \to (G', H')$ is a homomorphism which induces a bijection $\widetilde{\sigma} : G/H \to G'/H'$, then the following diagram commutes:*

$$\begin{array}{ccc} G^{\mathrm{ab}} & \xrightarrow{\sigma} & G'^{\,\mathrm{ab}} \\ \big\downarrow{\scriptstyle \mathrm{Ver}} & & \big\downarrow{\scriptstyle \mathrm{Ver}} \\ H^{\mathrm{ab}} & \xrightarrow{\sigma} & H'^{\,\mathrm{ab}} \end{array}$$

*Proof.* We set $X = G/H$ and $X' = G'/H'$. Thus, $\widetilde{\sigma}$ is a bijection $X \to X'$.

**Claim:** If $\varphi : X \to G$ is a section of $G \to X$, then $\varphi' : X' \to X \to G \to G'$ is a section of $G' \to X'$.

Note $\varphi' = \sigma \circ \varphi \circ \widetilde{\sigma}^{-1}$ and we have to show that $\widetilde{\sigma}' \circ \varphi = \mathrm{id}_{X'}$.

Consider:

$$\begin{array}{ccc} G & \xrightarrow{\sigma} & G' \\ {\scriptstyle\widetilde{\sigma}}\big\uparrow & & {\scriptstyle\widetilde{\sigma}'}\big\uparrow \\ X & \xrightarrow{\pi} & X' \end{array} \implies \pi' \circ \sigma = \widetilde{\sigma}' \circ \pi$$

Now, we have $\pi' \circ \varphi' = \pi' \circ \sigma \circ \varphi \circ \widetilde{\sigma}^{-1} = \widetilde{\sigma} \circ \pi \circ \varphi \circ \widetilde{\sigma}^{-1} = \widetilde{\sigma}\widetilde{\sigma}^{-1} = \mathrm{id}_{X'}$. This proves the claim.

We fix an arbitrary $g \in G$ and set $\sigma(g) = g' \in G'$.

**Claim:** For all $x \in X$, the image of $h^{\varphi}_{g,x}$ in $H'$ is $h^{\varphi'}_{g',x'}$.

**Proof:** We need to prove that $\sigma(h^{\varphi}_{g,x}) = h^{\varphi'}_{g',x'}$.

While defining transfer, we had the equation:

$$g\varphi(x) = \varphi(gx)h^{\varphi}_{g,x} \tag{A}$$

Applying $\sigma$ to (A) gives us:

$$\sigma(g) \cdot \sigma(\varphi(x)) = \sigma(\varphi(gx)) \cdot \sigma(h^{\varphi}_{g,x})$$

$$g'\varphi'(\widetilde{\sigma}(x)) = \varphi'(\widetilde{\sigma}(gx)) \cdot \sigma(h^{\varphi}_{g,x}) \tag{B}$$

as $\varphi' = \sigma \circ \varphi \circ \widetilde{\sigma}^{-1}$.

Applying (A) with $\varphi'$ and $g'$ gives us

$$g'\varphi'(x') = \varphi'(g'x')h^{\varphi'}_{g',x'} \tag{C}$$

where $x' = \widetilde{\sigma}(x)$. Now, $g'x' = g'\widetilde{\sigma}(x)$. Therefore, (B) implies

$$g'\varphi'(x') = \varphi'(\widetilde{\sigma}(gx)) = \sigma(h^{\varphi}_{g,x}) \tag{B'}$$

**Subclaim:** $\varphi'(\widetilde{\sigma}(gx)) = \varphi'(g'x')$.

Let $x = g_2H$, then $g'x' = g'\widetilde{\sigma}(g_2H) = \sigma(gg_2H) = \sigma(g)\sigma(g_2)H' = g'g_2'H' = \sigma(gg_2)H' = \widetilde{\sigma}(gg_2H) = \widetilde{\sigma}(gx)$ Then, (B') and (C) imply

$$\varphi'(\widetilde{\sigma}(gx))\sigma(h^{\varphi'}_{g'x'}) = \varphi'(g'x')h^{\varphi'}_{g'x'} \implies \sigma(h^{\varphi}_{g,x}) = h^{\varphi'}_{g',x'}$$

Then, $\text{Ver}(g') = \prod_{x' \in X'} h^{\varphi'}_{g',x'} = \prod_{\widetilde{\sigma}(x) \in X'} \sigma(h^{\varphi}_{g,x}) = \sigma(\prod_{x \in X} h^{\varphi}_{g,x}) = \sigma(\text{Ver}(g))$ since $\widetilde{\sigma}$ is a bijection, i.e., as $x$ runs over $X$, $x'$ runs over $X'$.

$\square$

**Proposition 2.1.1.** *The image of the homomorphism* $\text{Ver} : G^{\text{ab}} \to H^{\text{ab}}$ *is contained in the set of elements of* $H^{\text{ab}}$ *fixed under conjugation by* $N_G(H)$.

*Proof.* We take $G = G'$, $H = H'$ and $\sigma : G \to G$ as $\sigma(g) = zgz^{-1}$ where $z \in N_G(H)$.

**Claim:** $\sigma$ induces $\widetilde{\sigma} : G^{\mathrm{ab}} \to G^{\mathrm{ab}}$.

This is true because for any $[x, y] \in D(G)$, we have

$$\sigma[x, y] = [\sigma(x), \sigma(y)] = [zxz^{-1}, zyz^{-1}] = [x, y],$$

i.e., $\sigma(D(G)) \subset D(G)$, and $\widetilde{\sigma}(gG') = \sigma(g)H'$.

We also know that $\mathrm{Ver} : G \to H^{\mathrm{ab}}$ induces a $\widetilde{\mathrm{Ver}} : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$, since $\mathrm{Ver}(G') \subseteq H'$ which is $\mathrm{Ver}(gG') = \mathrm{Ver}(g)H'$.

Now, we have $G \xrightarrow{\sigma} G \xrightarrow{\pi} G^{\mathrm{ab}} \xrightarrow{\widetilde{\mathrm{Ver}}} H^{\mathrm{ab}}$.

This maps $g \mapsto zgz^{-1} \mapsto (zgz^{-1})G' \mapsto \widetilde{\mathrm{Ver}}(zgz^{-1})H'$.

Let us call this map $f$, i.e., $f(g) = \mathrm{Ver}(\sigma(g))H' = \widetilde{\mathrm{Ver}}(\sigma(g)G') = \widetilde{\mathrm{Ver}}(\widetilde{\sigma}(gG'))$.

Now, by the commutative diagram, $f(g) = \widetilde{\sigma}(\widetilde{\mathrm{Ver}}(gG'))$.

$$\begin{tikzcd}
G^{\mathrm{ab}} \arrow[r, "\widetilde{\sigma}"] \arrow[d, "\widetilde{\mathrm{Ver}}"] & G'^{\,\mathrm{ab}} \arrow[d, "\widetilde{\mathrm{Ver}}"] \\
H^{\mathrm{ab}} \arrow[r, "\widetilde{\sigma}"] & H'^{\,\mathrm{ab}}
\end{tikzcd}$$

We have $\mathrm{Ver}(g) = \prod_{x \in X} h^{\varphi}_{g,x} \mod H' \implies \widetilde{\mathrm{Ver}}(gG') = \prod_{x \in X} h^{\varphi}_{g,x} H'$.

Thus,

$$\begin{aligned}
\widetilde{\sigma}(\widetilde{\mathrm{Ver}}(gG')) &= \widetilde{\sigma}\left(\prod_x h^{\varphi}_{g,x} H'\right) = \sigma\left(\prod_x h^{\varphi}_{g,x}\right) H' \\
&= \left(\prod_x \sigma(h^{\varphi}_{g,x})\right) H' = \left(\prod_x z h^{\varphi}_{g,x} z^{-1}\right) H' \\
&= \left(z \ \mathrm{Ver}(g)\, z^{-1}\right) H' = \widetilde{\sigma}(\widetilde{\mathrm{Ver}}(g)).
\end{aligned}$$

$\square$

## 2.2 Computing the Transfer

Let $H$ be a subgroup of $G$ of finite index $n$ and $X = G/H$. Let $g \in G$ and let $C_g = \langle g \rangle$ be the cyclic group genereated by $g$. Then, $C_g$ decomposes $X$ into orbits $\mathcal{O}_\alpha$, i.e., $X = \bigsqcup_\alpha \mathcal{O}_\alpha$, where $\bigsqcup$ denotes disjoint union.

We set $|\mathcal{O}_\alpha| := f_\alpha$ and $x_\alpha \in \mathcal{O}_\alpha$, i.e., $\mathcal{O}_\alpha = \{x_\alpha, \ldots, g^{f_\alpha - 1}x_\alpha\}$ and $g^{f_\alpha}x_\alpha = x_\alpha$.

Let $z_\alpha \in G$ be a representative of $x_\alpha$, i.e., $z_\alpha H = x_\alpha$ (equivalently, $\pi(z_\alpha) = x_\alpha$). Then, we have

$$g^{f_\alpha}x_\alpha = x_\alpha \implies g^{f_\alpha}z_\alpha H = z_\alpha H \implies g^{f_\alpha}z_\alpha = z_\alpha h_\alpha$$

for some $h_\alpha \in H$.

**Theorem 2.2.1** (Transfer Evaluation Lemma). $\mathrm{Ver}(g) = \prod_\alpha h_\alpha = \prod_\alpha z_\alpha^{-1} g^{f_\alpha} z_\alpha \mod D(H)$.

*Proof.* Since Ver is independent of the choice of section, we choose a convenient section:

$$\varphi(g^i x_\alpha) := g^i z_\alpha \text{ for } i = 0, 1, \ldots, f_\alpha - 1.$$

Here we fix an orbit $\mathcal{O}_\alpha$ by fixing $x_\alpha$ and so we will later product over all such $\alpha$ to cover $X = \bigsqcup_\alpha \mathcal{O}_\alpha$.

For $i \neq f_\alpha - 1$, we have $g\varphi(g^i x_\alpha) = g^{i+1}z_\alpha = \varphi(g^{i+1}x_\alpha) = \varphi(g \cdot g^i x_\alpha)$, i.e., $\forall x \neq g^{f_\alpha - 1}x_\alpha$, we have $g\varphi(x) = \varphi(gx)$.

When $x = g^{f_\alpha - 1}x_\alpha$, then

$$\begin{aligned} g\varphi(x) &= g\varphi(g^{f_\alpha - 1}x_\alpha) = gg^{f_\alpha - 1}z_\alpha \\ &= g^{f_\alpha}z_\alpha = z_\alpha h_\alpha = \varphi(gx)\, h_\alpha \end{aligned}$$

Hence, $h_{\varphi,g,x} = h_\alpha$. $\mathrm{Ver}(\varphi) = \prod_\alpha h_{\varphi,g,\alpha} = \prod_\alpha h_\alpha \mod D(H)$.

By definition, $h_\alpha = z_\alpha^{-1} g^{f_\alpha} z_\alpha$, so

$$\mathrm{Ver}(\varphi) = \prod_\alpha z_\alpha^{-1} g^{f_\alpha} z_\alpha \mod D(H).$$

□

**Proposition 2.2.1.** *Let $\varphi : H \to A$ be a homomorphism of $H$ into an abelian group $A$. Suppose $\varphi(h) = \varphi(h')$ whenever $h, h' \in H$ are conjugate in $G$. Then,*

$$\varphi(\mathrm{Ver}(h)) = \varphi(h)^n \quad \forall h \in H \quad [\textit{where } n = (G : H)]$$

*Proof.* We have

$$\begin{aligned}\varphi(\mathrm{Ver}(h)) = \varphi\left(\prod_\alpha z_\alpha^{-1} h^{f_\alpha} z_\alpha\right) = \varphi\left(\prod_\alpha h^{f_\alpha}\right) \\ = \prod_\alpha \varphi(h)^{f_\alpha} = \varphi(h)^n, \text{ since } \sum_\alpha f_\alpha = |X| = n\end{aligned}$$

□

**Corollary 2.2.1.1.** *Let $\mathcal{C}$ be a subgroup of $H$ having the following property: if $c \in \mathcal{C}$ and $h \in H$ are $G$-conjugate, then they are equal. Then,* $\mathrm{Ver}(c) = c^n \mod D(H)$ $\forall c \in \mathcal{C}$.

*Proof.* We know that $\mathrm{Ver}(c) = \prod_\alpha h_\alpha$, where $h_\alpha = z_\alpha^{-1} g^{f_\alpha} z_\alpha$, as before. Now, $h_\alpha$ and $c^{f_\alpha}$are $G$-conjugate, hence equal. Hence, $\mathrm{Ver}(c) = c^n \mod D(H)$. □

**Corollary 2.2.1.2.** *Assume that if two elements of $H$ are conjugate in $G$, they are equal. Then*

1. $\mathrm{Ver}(h) = h^n$ $\forall h \in H$ *where* $n = (G : H)$.
2. *Assume $|H|$ and $(G : H)$ are relatively prime. Let* $N = \ker(G \xrightarrow{\mathrm{Ver}} H)$, *then $N$ is a normal complement of $H$; that is, $G = N \ltimes H$.*

*Proof.* 1. **Claim:** $H$ is abelian: take any $h, h' \in H$. We have $hh'h^{-1}h'^{-1} = (hh'h^{-1})h'^{-1} = h'h'^{-1} = 1$, by hypothesis, whence, the claim follows. Applying corollary 2.2.1.2 we get $\mathrm{Ver}(h) = h^n$ $\forall h \in H$ where $n = (G : H)$.

2. **Claim:** $f : H \xrightarrow{i} G \xrightarrow{\mathrm{Ver}} H$ is an isomorphism.

   For injectivity, suppose $f(h_1) = f(h_2)$ whence $h_1^n = h_2^n$. This implies $(h_1h_2^{-1})^n = 1$, i.e., $|h_1h_2^{-1}|$ divides $n$. However, $h_1h_2^{-1} \in \ker f \subseteq H$, so $|h_1h_2^{-1}|$ divides $|H|$

   Since $|H|$ and $(G : H)$ are relatively prime, we have $|h_1h_2^{-1}| = 1$, i.e., $h_1 = h_2$.

   For surjectivity, we prove the following more general clam:

*Let $A$ be an abelian group of order $m$ and $\phi : A \to A : a \mapsto a^n$ such that $n$ and $m$ are relatively prime, then $\phi$ is surjective.*

Consider $a \in A$, then since $(n, m) = 1 \implies \exists x, y \in \mathbb{Z}$ s.t. $nx + my = 1$.

Thus, $a = a^{nx+my} = a^{nx} \cdot a^{my} = a^{nx} = (a^x)^n$ , since $|A| = m$.

Therefore, there exists a preimage $a^x \in A$ s.t. $\phi(a^x) = (a^x)^n = a$, which proves the lemma.

This gives surjectivity of $f$ and it is homomorphic since $f(h_1h_2) = (h_1h_2)^n = h_1^n h_2^n = f(h_1)f(h_2)$, whence the claim holds.

Now, $N \lhd G$ since it is a kernel of a homomorphism and $NH = G$ by the first isomorphism theorem, hence we need only show that $N \cap H = 1$,

but this is clear since for all $h \in N \cap H, \mathrm{Ver}(h) = h^n = 1 \implies h = 1$, by injectivity. Therefore, $G = N \ltimes H$.

□

**Corollary 2.2.1.3.** *Assume that $H \subset Z(G)$ and that $|H|$ and $(G : H)$ are relatively prime. Then, $G \cong H \times G/H$.*

*Proof.* By the previous corollary, we have $G = N \ltimes H$, but $H \subset Z(G)$. Hence, for all $g \in G$ and $h \in H$, we have$ghg^{-1} = gg^{-1}h = h \in H$, that is, $H \lhd G$, whence $G \cong H \times G/H$. □

**Theorem 2.2.2.** *Assume that $H$ is abelian and normal in $G$. Let $g \in G$ and $f$ be the smallest positive integer such that $g^f \in H$. Let $C_g = \langle g \rangle$ be the cyclic group genereated by $g$. Then,*

$$\mathrm{Ver}(g) = \prod_{\gamma \in G/C_gH} \gamma g^f \gamma^{-1}.$$

Note that such an $f$ exists because we may take $f = |G|$ to work for any $g$.

We will employ the Transfer Evaluation Lemma (Theorem 2.2.1) to prove this theorem.

*Proof.* Let $(\gamma_\alpha)_\alpha$ be a set of representatives of $G/C_gH$ and $x_\alpha$ be the image of $(\gamma_\alpha)^{-1}$ in $X = G/H$, i.e., $x_\alpha = (\gamma_\alpha)^{-1}H$. As earlier, we consider the action by left multiplication $C_g \curvearrowright X$, but since $H \lhd G, X$ is a group.

Let $(t_\beta)_\beta$ be a set of representatives of $G/H$, i.e., $x = \{t_\beta H\}_\beta$. Take arbitrary $\overline{t_\beta} \in X$, then its orbit is $\mathcal{O}(\overline{t_\beta}) = \{g^i t_\beta H : i \in \mathbb{Z}\} = \{t_\beta H, gt_\beta, g^2 t_\beta H, \ldots\} = C_g t_\beta H = C_g t_\beta$.

**Claim:** $X = \{\overline{t_\beta} H\}_\beta$

We seek conditions for when two orbits are equal: $\mathcal{O}(\overline{t_\beta}) = \mathcal{O}(\overline{t_{\beta'}}) \iff C_g \overline{t_\beta} = C_g \overline{t_{\beta'}} \iff C_g t_\beta H = C_g t_{\beta'} H \iff C_g H t_\beta = C_g H t_{\beta'}$, since $H \lhd C_g$.

Hence, we only have distinct orbits under $C_g \curvearrowright X$ if they are distinct right cosets of $C_g H$, thus it suffices to consider a right transversal of $C_g H$, which is $\{(\gamma_\alpha^{-1})_\alpha\}$, hence $X = \{\gamma_\alpha^{-1} H\}_\alpha$.

We recall that in Transfer Evaluation Lemma, $f$ was the size of $\mathcal{O}_\alpha$ and given by $g^f x_\alpha = x_\alpha$, i.e., $\overline{g^{f_\beta} t_\beta} = \overline{t_\beta}$. Now, since $X$ is a group, we may cancel $\overline{t_\beta}$ to obtain $\overline{g^{f_\beta}} = 1$, i.e., $g^{f_\beta} \in H$.

Hence, $f_\beta$ must be $f$ since $f$ is the smallest positive integer such that $g^f \in H$, by hypothesis.

Applying Theorem 2.2.1 with $z_\alpha = \gamma_\alpha^{-1}$, $f_\alpha = f$ and $h_\alpha = \gamma_\alpha g^f \gamma_\alpha^{-1}$ gives

$$\mathrm{Ver}(g) = \prod_\alpha \gamma_\alpha g^f \gamma_\alpha^{-1} = \prod_{\gamma \in G/C_g H} \gamma_\alpha g^f \gamma_\alpha^{-1}.$$

□

**Corollary 2.2.2.1.** *If* $h \in H$, *then* $\mathrm{Ver}(h) = \prod_{\gamma \in G/H} \gamma h^f \gamma^{-1}$.

*Proof.* In the theorem above, we take $g = h$ and $f = 1$, then $C_g H = \langle h \rangle H = H$, thus $G/C_g H = G/H$. Hence, for all $h \in H$, $\mathrm{Ver}(h) = \prod_{\gamma \in G/H} \gamma h^f \gamma^{-1}$. □

## 2.3 Applications of the Transfer map

### 2.3.1 Gauss Lemma

Let $p \neq 2$ be a prime, $G = \mathbb{F}_p^\times$ and $H = \{\pm 1\}$. Then, $(G : H) = \dfrac{p-1}{2}$.

Since $H$ is abelian, we have $\mathrm{Ver}(x) = x^{(G:H)} = x^{\frac{p-1}{2}}$, which is the ***Legendre symbol*** $\left(\frac{x}{p}\right)$, given by 1 if $x$ is a square (mod $p$) and $-1$ otherwise.

**Theorem 2.3.1** (Euler's Criterion)**.** $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \mod p$.

To compute this via the transfer map, we take a representative set $S$ of $X = G/H$, such as $S = \{1, 2, \ldots, (p-1)/2\}$.

For $x \in G, s \in S$, define $\varepsilon(x,s) := \pm 1$ as being 1 if $xs \in S$ and $-1$ if $xs \notin S$.

We use $\mathrm{Ver}(x) = \prod_s h_{x,s} \mod D(H)$.

Recall that $h_{x,s}$ above is the unique element of $H$ satisfying $xs \in Sh_{x,s}$ for a fixed but arbitrary $s \in S$.

Note that $h_{x,s} = \varepsilon(x,s)$, thus $\mathrm{Ver}(x) = \left(\frac{x}{p}\right) = \prod_{s\in S} \varepsilon(x,s)$

*Example* 2.1 (Computation of $\left(\frac{2}{p}\right)$). Let $m = \frac{(p-1)}{2}$, so $S = \{1, 2, \dots, m\}$.

If $s \in S$, we have $\varepsilon(2,s) = -1$ if and only if $m < 2s \leq 2m$, i.e.

$$\varepsilon(2,s) = -1 \iff m/2 < s \leq m \tag{1}$$

If $m$ is even, then the number of $s$ satisfying (1) is $m/2$, thus

$$\left(\frac{2}{p}\right) = \prod_{t=1}^{m} \varepsilon(2,t) = (-1)^{\frac{m}{2}}(1)^{\frac{m}{2}} = -1 \iff \frac{m}{2} \text{ is even} \iff \frac{p-1}{4} \text{ is even} \iff p \equiv 1 \mod 8$$

If $m$ is odd, then the number of $s$ satisfying (1) is $(m+1)/2$, thus

$$\left(\frac{2}{p}\right) = \prod_{t=1}^{m} \varepsilon(2,t) = (-1)^{\frac{m+1}{2}}(1)^{\frac{m-1}{2}} = 1 \iff \frac{m+1}{2} \text{is even} \iff \frac{p+1}{4} \text{ is even} \iff p \equiv -1 \mod 8$$

Therefore, we have $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 8$

Similarly, we have $\left(\frac{2}{p}\right) = -1$ if and only if $p \equiv \pm 3 \pmod 8$

### 2.3.2 Infinite and Finite Groups

**Proposition 2.3.1.** *If $G$ is a torsion-free group with a finite index subgroup $H$ isomorphic to $\mathbb{Z}$, then $G$ is isomorphic to $\mathbb{Z}$.*

*Proof.* We assume $H \lhd G$, without loss of generality, because otherwise we can replace $H$ by the intersection of its conjugates, i.e., $H' = \bigcap_{g\in G} gHg^{-1} = \mathrm{core}_G(H)$. We know that $H'$ is the largest normal subgroup of $G$ contained in $H$, and $H \cong \mathbb{Z}$, thus $H' \cong \mathbb{Z}$.

Consider the conjugation action of $G$ on $H$; this gives a corresponding group homomorphism $\varepsilon : G \to \mathrm{Aut}(H) = \{\pm 1\}$ .

Hence, we have two cases:

a.) $\varepsilon = 1$, i.e., $H \subseteq Z(G)$. Let $v : G \to H$ be the transfer map, then $v(h) = h^n$ for $h \in H$ since $H$ is abelian, where $n = (G : H)$. Now, consider $v|_H : H \to H$ sending $h \to h^n$.

Since $H \cong \mathbb{Z}$, $v|_H$ is injective as $h^n = h'^m \implies h = h'$.

Thus, $\ker(v|_H) = \ker(v) \cap H = \{1\}$. Let $N = \ker(v)$. Since $(G : H)$ is finite and $N \cap H = \{1\}$, $N$ must be finite, as $G/H \cong N$.

We must, then, have $N = \{1\}$ since $G$ is torsion-free, i.e., $\ker(\varepsilon) = \{1\}$. Hence, $G$ embeds into its subgroup $\mathbb{Z}$, i.e., $G = \mathbb{Z}$.

b.) $\varepsilon \neq 1$, let $G' = \ker \varepsilon = \{g \in G : \varepsilon(g) = 1\}$. Then, by case a), $G' \cong \mathbb{Z}$. Let $x \in G - G'$, then $\varepsilon(x) = -1$, so $\varepsilon(x^{-1}) = y^{-1}$. Now, $x^2 \in \ker \varepsilon = G'$ since $\varepsilon(x^2) = \varepsilon(x) \cdot \varepsilon(x^{-1}) = (-1) \cdot (-1) = 1$.

Now, $\varepsilon(x^2) = x^2$ and by definition $\varepsilon(x^2)(t) = xtx^{-1}$ $\forall t$, so $xx^{-1} = x^2 \implies x^4 = 1$, i.e., $x$ is a torsion element. This is a contradiction, since $G$ is torsion-free.

$\square$

**Theorem 2.3.2.** *Let $H$ be a $p$-Sylow subgroup of a finite group $G$ and let $\varphi : H \to A$ be a homomorphism with values in a finite abelian $p$-group $A$. Then:*

*i) $\varphi$ extends to a homomorphism of $G$ into $A$ if and only if for all $h, h' \in H$ conjugate in $G$, we have $\varphi(h) = \varphi(h')$.*

*ii) If an extension for $\varphi$ exists, it is unique and is given by $g \mapsto (\varphi(\mathrm{Ver}(g)))^{\frac{1}{n}}$, where $n = (G : H)$.*

*Proof.* i.) $\implies$: Suppose $\widetilde{\varphi}$ is an extension. Then for $h \in H$ and $g \in G$ with $ghg^{-1} \in H$, we have $\varphi(ghg^{-1}) = \widetilde{\varphi}(g)\varphi(h)\widetilde{\varphi}(g)^{-1} = \varphi(h)$, since $A$ is abelian.

$\impliedby$ Since $\gcd(n, p) = 1$ and $p$ divides $|A|$, $\varphi(\mathrm{Ver}(g))^n$ makes sense, since $\forall a \in A$, there exists $b \in A$ such that $b^n = a$. Now, by Proposition 2.2.1, $\varphi(\mathrm{Ver}(h)) = h^n$ for $h \in H$, hence $\widetilde{\varphi}(g) = \varphi(\mathrm{Ver}(g))^{\frac{1}{n}} \in A$ is a valid extension.

ii.) Let $\widetilde{\varphi}$ and $\widetilde{\varphi}'$ be two extensions and $B = \{g \in G : \widetilde{\varphi}(g) = \widetilde{\varphi}'(g)\}$. Clearly, $H \subseteq B$, and $B$ is a subgroup of $G$.

**Claim 1:** $B$ contains all $q$-Sylow subgroups, $q \neq p$.

Let $Q$ be an arbitrary $q$-Sylow subgroup. Take any $t \in Q$, then $|t| \bigm| q$, and $|\widetilde{\varphi}(t)|$ divides $p$, since $A$ is a $p$-group. Moreover, $|\widetilde{\varphi}(t)| \bigm| |t|$, by virtue of being a homomorphism, so $|\widetilde{\varphi}(t)| = 1$, i.e., $\widetilde{\varphi}(t) = 1$. Similarly, $\widetilde{\varphi}'(t) = 1$. Hence, $\forall t \in Q, \widetilde{\varphi}(t) = \widetilde{\varphi}'(t)$. Thus, $B$ contains all $q$-Sylow subgroups.

**Claim 2:** $B$ contains all $p$-Sylow subgroups.

Let $tH^{-1}t$ be an arbitrary $p$-Sylow subgroup. Take an arbitrary element $tht^{-1}$; consider $\widetilde{\varphi}(tht^{-1}) = \widetilde{\varphi}(t)\varphi(h)\varphi(t)^{-1} = \varphi(h) = \varphi'(h) = \widetilde{\varphi}'(tht^{-1})$, thus $tht^{-1} \in B$.

From these two claims, it follows that $B = G$, i.e, $\widetilde{\varphi} \equiv \widetilde{\varphi}'$.

$\square$

# References


Butler, Gregory and McKay, John (1983). "The transitive groups of degree up to eleven". In: *Communications in Algebra* 11.8, pp. 863–911. DOI: 10.1080/0092787830882.

Isaacs, I.M. (2008). *Finite Group Theory*. Graduate studies in mathematics. American Mathematical Society. ISBN: 9780821843444. URL: https://books.google.co.in/books?id=E9kOCgAAQBAJ.

Petrillo, Joseph (2009). "Goursat's Other Theorem". In: *The College Mathematics Journal* 40.2. Accessed 22 Oct. 2025, pp. 119–124. URL: http://www.jstor.org/stable/25653685.

Serre, J.P. (2016). *Finite Groups: An Introduction*. Surveys of modern mathematics. International Press. ISBN: 9781571463203. URL: https://books.google.co.in/books?id=hviGwQEACAAJ.