A New Way to Look at Homomorphisms

A thesis

submitted in partial fulfilment

of the requirements for the Degree

of

Master of Science

at the

University of Waikato

by

Yue Guo

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

University of Waikato

2013

Acknowledgements

Firstly, I would like to express my greatest appreciation to my supervisor, Dr. Ian Hawthorn (from the University of Waikato), without whom I cannot complete my thesis. His effective suggestion, continuous encouragement and endless patience help me throughout writing of this paper the whole time. I hardly find any better words to show my gratitude, so please allow me to just use a simple old Chinese saying (according to Confucius, the first and the best teacher in China):
It is the greatest benefit for myself to learn from a straight, forgiving and knowledgeable teacher.

友直，友谅，友多闻，益矣。(孔子)

Last but not the least, I also want to thank my parents, who support and always believe in me. My gratitude is not only for when they treated me well, but also for when they treated me tough, because now I am so glad that they do not spoil me. They are my first teachers and will be forever.

感谢父母，养育之恩大于天。

Abstract

This thesis is about arbitrary functions between groups. We look at two way to measure how close an arbitrary function is to being a homomorphism. We first look at an action of the group on functions in which homomorphisms are invariant. We also look at distributors, structures which are similar to commutators and which are trivial for a homomorphism. This leads to a rich and interesting theory and gives us a new way to look at homomorphisms and new tools to try to build homomorphisms from arbitrary functions. We demonstrate the applicability of these tools by constructing several alternate proofs of the Schur-Zassenhaus theorem.

Contents

Chapter 1

Introduction

Definition 1.1 *(Homomorphism)*

If there are two finite groups G and H, then a group homomorphism is a function $f : G \to H$ such that

$$f(xy) = f(x)f(y), \forall\ x \text{ and } y \in G.$$

From this definition, we can deduce that $\forall\ x \in G$,

$$\begin{aligned} f(1) &= 1 \\ \text{and } f(x^{-1}) &= f(x)^{-1}. \end{aligned}$$

For an arbitrary function between groups, it is not necessary that all group structure must be preserved, and the function is a homomorphism if it is (from the definition). In group theory, many theorems can be proved by showing the existence of (at least one) homomorphism from a set of functions with a certain type, but sometimes it is really hard to find or build one. Because most of time, a function between groups may preserve group structure for a subgroup of it, but not for the whole group. (Also it might not preserve any group structure at all in some cases.) So we need to find the link from an arbitrary function to a related homomorphism. That is the reason why we define "f-distributor" and "conjugation of functions" in this particular paper.

Let G and H be finite groups, and $f : G \to H$ is a function from G to H.

Then the f-distributor of x and y is defined as

$$[x,y]_f := f(y)^{-1}f(x)^{-1}f(xy), \forall\ x \text{ and } y \in G. \text{ (from definition 2.1 on page 3)}$$

And the conjugate of the function f under x ($\in G$) is define as

$$f^x(y) := f(x)^{-1}f(xy), \forall\ y \in G. \text{ (from definition 3.1 on page 17)}$$

Such like commutators and normal conjugations of a group, which can describe how close a group is to be commutative, these distributors and conjugation of any function show how "close" the function is to be a homomorphism. Then a homomorphism can be redefined by using them.

A function $f : G \to H$ is a group homomorphism

$\Leftrightarrow$ $[x,y]_f = 1, \forall\ x \text{ and } y \in G$ (Theorem 2.1 on page 4)

$\Leftrightarrow$ $f^a = f, \forall\ a \in G.$ (Theorem 3.2 on page 18)

There are three different kinds of methods to prove the existence of homomorphism by using our new notation:

(1). Since the conjugation of a function between groups is an action **if and only if** the function preserve identity, then look at the set of all identity preserving functions between certain groups. If we can show there must be a function (which is not the trivial homomorphism) with orbit-size 1 under this action, then that is the homomorphism which we want. (e.g. Cauchy Theorem and Schur-Zassenhaus Theorem for G/H solvable)

(2). Look at all orbits under the action, and see how they partition the function set. Then try to "average" all orbits to establish a homomorphism. (e.g. to prove that the transfer map is a homomorphism)

(3). We can also build a new function with "average" all these distributors from the original function. When the image of the function is abelian, we can prove that the new function is a homomorphism by using distributor identities. (e.g. Schur-Zassenhaus Theorem for H abelian)

Chapter 2

Distributors

2.1 Definition of Distributors

If G and H are finite groups, and $f : G \to H$ is a function from G to H, then generally $f(xy) = f(x)f(y)$ is not always true for all x and y in G, unless this function is a homomorphism. Then a tool to measure the extent of which the function f fails to be a homomorphism is required. In other words, we want to measure whether a function f is nearly a homomorphism or far away.

We can get the idea from the way that commutators describe how near a group is to abelian.

Definition 2.1 *Let G and H be finite groups, and $f : G \to H$ is a function from G to H. Then the f-distributor of x and y is defined as*

$$[x, y]_f := f(y)^{-1} f(x)^{-1} f(xy), \forall \ x \ and \ y \in G.$$

Similarly as the definition of commutator subgroup, we can define the f-distributor of a group.

Definition 2.2 *Let G and H be finite groups, and $f : G \to H$ is a function from G to H. Then the f-distributor of group G is defined as*

$$[G, G]_f := \Big\langle [x, y]_f : \forall \ x \ and \ y \in G \Big\rangle.$$

Let X and Y be two subgroups of group G $(X, Y \leqslant G)$. then the f-distributor of X and Y is defined as

$$[X, Y]_f := \Big\langle [x, y]_f : \forall\ x \in X \text{ and } \forall\ y \in Y \Big\rangle.$$

Since we want the f-distributor to describe how close the function f is to being a homomorphism, then the condition of f-distributor for function f being a homomorphism need to be considered.

Theorem 2.1 *A function $f : G \to H$ is a group homomorphism*
iff *$[x, y]_f = 1$ for all x and y in group G.*

Proof. $[x, y]_f = 1, \forall\ x$ and $y \in G$

$\Leftrightarrow$ $f(y)^{-1}f(x)^{-1}f(xy) = 1, \forall\ x$ and $y \in G$

(by the definition of f-distributor)

$\Leftrightarrow$ $f(xy) = f(x)f(y), \forall\ x$ and $y \in G$

(left product $f(x)f(y)$ on both sides)

$\Leftrightarrow$ f is a homomorphism in group G.

(by the definition of homomorphism)

□

By the definition of distributors, we know that distributors have similar form as commutators. So there should be some links between them. We will show that by considering the following examples.

Example 2.2 *Consider the function $(-1) : G \to G$ defined by*
$(-1) : x \mapsto x^{-1}, \forall\ x \in G$. Then $\forall\ x$ and $y \in G$, the (-1)-distributor is

$$\begin{aligned}
[x, y]_{-1} &= \Big(y^{-1}\Big)^{-1}\Big(x^{-1}\Big)^{-1}(xy)^{-1} && \textit{(by the definition of } f\textit{-distributor)} \\
&= yxy^{-1}x^{-1} \\
&= [y^{-1}, x^{-1}] && \textit{(by the definition of commutator)} \\
&= [x^{-1}, y^{-1}]^{-1}. && (\ [a, b]^{-1} = [b, a], \forall\ a \text{ and } b \in G)
\end{aligned}$$

In other word, the (-1)-distributor of two elements is the inverse of their inverses' commutator.

Then because the group G is closed under inverse,

$$\begin{aligned}
[G,G]_{-1} &= \Big\langle [x,y]_{-1} : \forall\ x \text{ and } y \in G \Big\rangle \\
&= \Big\langle [x^{-1},y^{-1}]^{-1} : \forall\ x \text{ and } y \in G \Big\rangle \\
&= \Big\langle [x,y] : \forall\ x \text{ and } y \in G \Big\rangle \\
&= G'.
\end{aligned}$$

Then the (-1)-distributor of a group is the same as its derived group. This result is not surprising, because we have that (-1) is a group homomorphism ***if and only if*** *the group is commutative from undergraduate studying of group theory. So we can get the following result:*

$$\begin{array}{c}
(-1)(x) = x^{-1}\ (\forall\ x \in G) \\
\text{is a homomorphism} \Leftrightarrow \text{Group } G \text{ is abelian} \\
\Updownarrow \qquad\qquad\qquad \Updownarrow \\
[G,G]_{-1} = 1 \quad \Longleftrightarrow \quad [G,G] = 1
\end{array}$$

Figure 1

Here is another example about distributors linking to commutators.

Example 2.3 *Consider the function $(2) : G \to G$ defined by $(2) : x \mapsto x^2, \forall\ x \in G$. Then $\forall\ x$ and $y \in G$, the (2)-distributor is*

$$\begin{aligned}
[x,y]_2 &= \Big(y^2\Big)^{-1}\Big(x^2\Big)^{-1}(xy)^2 \qquad \textit{(by the definition of } f\textit{-distributor)} \\
&= (yy)^{-1}(xx)^{-1}(xyxy) \\
&= y^{-1}y^{-1}x^{-1}(x^{-1}x)yxy \\
&= y^{-1}(y^{-1}x^{-1})y(xy) \\
&= y^{-1}(xy)^{-1}y(xy) \\
&= [y,xy]. \qquad\qquad \textit{(by the definition of commutator)}
\end{aligned}$$

Because the group G must be closed under product,

$$[G,G]_2 = \Big\langle [y,xy] : \forall\ x \text{ and } y \in G \Big\rangle \subseteq G'.$$

We can also show that $G' \subseteq [G,G]_2$. From

$$\forall\ a \text{ and } b \in G,\ [a,b] = [a,(ba^{-1})a] \in [G,G]_2$$

Then $[G,G]_2 = G'$. So the (2)-distributor of a group is also the same as its derived group. This is not surprising neither, because (2) is a group homomorphism ***if and only if*** *the group is commutative. Then similarly as last example:*

$$\begin{array}{c} (2)(x) = x^2\ (\forall\ x \in G) \\ \text{is a homomorphism} \Leftrightarrow \text{Group } G \text{ is abelian} \\ \Updownarrow \qquad\qquad\qquad \Updownarrow \\ [G,G]_2 = 1 \qquad \Longleftrightarrow \qquad [G,G] = 1 \end{array}$$

Figure 2

Last two examples show that the condition for function (-1) and (2) being homomorphisms still holds by using distributor to argue it:

$$\begin{array}{ll} & (-1) \text{ and } (2) \text{ are homomorphisms} \\ \Leftrightarrow & (-1)\text{-distributor and } (2)\text{-distributor are } 1 \\ \Leftrightarrow & \text{derived group } G' \text{ is trivial} \\ \Leftrightarrow & \text{group } G \text{ is abelian.} \end{array}$$

2.2 Some Properties of Distributors

In this section, we will discuss some properties about distributors which may be needed later.

Proposition 2.4 *If f is a function from group G to group H, then*

$$f(xy) = f(x)f(y)[x,y]_f \ ,\forall \ x \text{ and } y \in G.$$

Proof. $[x,y]_f = f(y)^{-1}f(x)^{-1}f(xy)$, $\forall$ x and $y \in G$

(by the definition of distributor)

$\Rightarrow$ $f(x)^{-1}f(xy) = f(y)[x,y]_f \ ,\forall$ x and $y \in G$

(by left product $f(y)$ on both sides)

$\Rightarrow$ $f(xy) = f(x)f(y)[x,y]_f \ ,\forall$ x and $y \in G$.

(by left product $f(x)$ on both sides)

□

This shows that any function f should map a product of two elements to the product of their image right product their f-distributor. So that the distributor is the link between the image of product and the product of images for a non-homomorphism function.

We already know that distributors are like commutators. Since commutator identities play a key role in the theory of commutators, there should be something like that for distributors. We call these "distributor identities".

Theorem 2.5 *If f is a function from group G to group H, then*

$$[x,y]_f^{f(z)} = [y,z]_f[x,yz]_f[xy,z]_f^{-1}, \forall \ x \ \& \ y \ \& \ z \in G.$$

Proof. we will prove it by using last proposition.

$$f(xyz) = f(xy)f(z)[xy,z]_f = f(x)f(yz)[x,yz]_f \ ,\forall \ x \ \& \ y \ \& \ z \in G$$

$$\Big(\text{two different way to expand } f(xyz)\Big)$$

$\Rightarrow$ $f(x)f(y)[x,y]_f f(z)[xy,z]_f = f(x)f(y)f(z)[y,z]_f[x,yz]_f$,

$$\forall \ x \ \& \ y \ \& \ z \in G$$

$$\Big(\text{expand } f(xy) \text{ and } f(yz)\Big)$$

$$\Rightarrow\ f(z)^{-1}[x,y]_f f(z)[xy,z]_f = [y,z]_f[x,yz]_f\ ,\forall\ x\ \&\ y\ \&\ z \in G$$

$$\text{(by left product } \Big(f(x)f(y)f(z)\Big)^{-1} \text{ on both sides)}$$

$$\Rightarrow\ [x,y]_f^{f(z)} = [y,z]_f[x,yz]_f[xy,z]_f^{-1}, \forall\ x\ \&\ y\ \&\ z \in G.$$

$$\text{(by right product } [xy,z]^{-1} \text{ on both sides)}$$

□

There are other properties about distributor which need to be discussed following.

Proposition 2.6 *If f is a function from group G to H, then*

(a). $[x,1]_f = f(1)^{-1},\ \forall\ x \in G$;

(b). $[1,x]_f = \Big(f(1)^{-1}\Big)^{f(x)},\ \forall\ x \in G$;

(c). $f\Big(x^{-1}\Big) = f(1)\Big[x^{-1},x\Big]_f^{-1}\ f(x)^{-1},\ \forall\ x \in G$;

(d). $f\Big(x^{-1}\Big) = f(x)^{-1}f(1)\Big[x,x^{-1}\Big]_f^{-1},\ \forall\ x \in G$;

(e). $\Big[x^{-1},x\Big]_f = f(x)^{-1}\Big[x,x^{-1}\Big]_f\ f(x)^{f(1)},\ \forall\ x \in G.$

Proof. $(a).[x,1]_f = f(1)^{-1}f(x)^{-1}f(x1), \forall\ x \in G$

$$\text{(from the definition of distributor)}$$

$$\Rightarrow [x,1]_f = f(1)^{-1}f(x)^{-1}f(x), \forall\ x \in G$$

$$\Rightarrow [x,1]_f = f(1)^{-1}, \forall\ x \in G.$$

$(b).[1,x]_f = f(x)^{-1}f(1)^{-1}f(1x), \forall\ x \in G$

$$\text{(from the definition of distributor)}$$

$$\Rightarrow [1,x]_f = f(x)^{-1}f(1)^{-1}f(x), \forall\ x \in G$$

$$\Rightarrow [1,x]_f = \Big(f(1)^{-1}\Big)^{f(x)}, \forall\ x \in G.$$

$(c).\Big[x^{-1},x\Big]_f = f(x)^{-1}f\Big(x^{-1}\Big)^{-1}f(1), \forall\ x \in G$

$$\text{(from the definition of distributor)}$$

$$\Rightarrow f\Big(x^{-1}\Big)^{-1} = f(x)\Big[x^{-1},x\Big]_f\ f(1)^{-1}, \forall\ x \in G$$

$$\text{(left product } f(x) \text{ and right product } f(1)^{-1} \text{ on both sides)}$$

$$\Rightarrow f\Big(x^{-1}\Big) = f(1)\Big[x^{-1},x\Big]_f^{-1}\ f(x)^{-1}, \forall\ x \in G.$$

(take the inverses on both sides)

$$(d).\Big[x,x^{-1}\Big]_f = f\Big(x^{-1}\Big)^{-1} f(x)^{-1} f(1), \forall\ x \in G$$

(from the definition of distributor)

$$\Rightarrow f\Big(x^{-1}\Big)^{-1} = \Big[x,x^{-1}\Big]_f\ f(1)^{-1} f(x), \forall\ x \in G$$

(right product $f(1)^{-1}f(x)$ on both sides)

$$\Rightarrow f\Big(x^{-1}\Big) = f(x)^{-1} f(1)\Big[x,x^{-1}\Big]_f^{-1}, \forall\ x \in G.$$

(take the inverses on both sides)

$$(e).f\Big(x^{-1}\Big) = f(1)\Big[x^{-1},x\Big]_f^{-1}\ f(x)^{-1} = f(x)^{-1} f(1)\Big[x,x^{-1}\Big]_f^{-1},$$

$$\forall\ x \in G$$

$$\Big(\text{from } (c) \text{ and } (d)\Big)$$

$$\Rightarrow \Big[x^{-1},x\Big]_f^{-1} = f(1)^{-1} f(x)^{-1} f(1)\Big[x,x^{-1}\Big]_f^{-1}\ f(x), \forall\ x \in G$$

(left product $f(1)^{-1}$ and right product $f(x)$ on both sides)

$$\Rightarrow \Big[x^{-1},x\Big]_f = f(x)^{-1}\Big[x,x^{-1}\Big]_f\ f(1)^{-1} f(x) f(1), \forall\ x \in G$$

(take the inverses on both sides)

$$\Rightarrow \Big[x^{-1},x\Big]_f = f(x)^{-1}\Big[x,x^{-1}\Big]_f\ f(x)^{f(1)}, \forall\ x \in G.$$

□

Not like commutator, we cannot find the relation between these two distributors if we swap the two elements in them. But from last proposition (e), we see the connection between them if these two elements are inverses to each other.

Then we will use the distributor identities to prove that the distributor of a group is normal in the generated group of the image.

Theorem 2.7 *If $f : G \to H$ is any function for groups, then*

$$[G,G]_f \trianglelefteq \Big\langle f(G) \Big\rangle \leqslant H.$$

Proof. From Theorem 2.5 on page 7 about distributor identities, it is clear that the distributor of a group is closed under conjugation by elements of the image of f. Then it is normal in $\Big\langle f(G) \Big\rangle$, because $\forall\ x, y, a, b \in G$,

(From Proposition 2.4 on page 7, we have $f(a)f(b) = f(ab)[a,b]_f^{-1}$)

$$\begin{aligned}
[x,y]_f^{f(a)f(b)} &= [x,y]_f^{f(ab)[a,b]_f^{-1}} \\
&= \Big([x,y]_f^{f(ab)}\Big)^{[a,b]_f^{-1}} \\
&= [a,b]_f[y,ab]_f[x,yab]_f[xy,ab]_f^{-1}[a,b]_f^{-1} \\
&\in [G,G]_f\ ;
\end{aligned}$$

and $\Big($From Proposition 2.6 (a) and (d) on page 8, we have

$f(a)^{-1} = f(a^{-1})[a,a^{-1}]_f[a,1]_f\Big)$

$$\begin{aligned}
[x,y]_f^{f(a)^{-1}} &= [x,y]_f^{f(a^{-1})[a,a^{-1}]_f[a,1]_f} \\
&= \Big([x,y]_f^{f(a^{-1})}\Big)^{[a,a^{-1}]_f[a,1]_f} \\
&= [a,1]_f^{-1}[a,a^{-1}]_f^{-1}[y,a^{-1}]_f[x,ya^{-1}]_f[xy,a^{-1}]_f^{-1}[a,a^{-1}]_f[a,1]_f \\
&\in [G,G]_f\ .
\end{aligned}$$

□

Now we will get the distributors of a composition function.

Theorem 2.8 *If $g : G \to H$ and $f : H \to K$ are two arbitrary functions, and G & H & K are groups. Let the composition of f and g be defined as*

$$f \circ g(x) := f\Big(g(x)\Big), \forall\ x \in G.$$

$$\text{Then} \qquad [x,y]_{f\circ g} = \Big[g(x),g(y)\Big]_f\ f\Big([x,y]_g\Big)\Big[g(x)g(y),[x,y]_g\Big]_f\ ,$$
$$\forall\ x \text{ and } y \in \text{group } G.$$

$$\text{In particular, } [x,y]_{f\circ g} = f\Big([x,y]_g\Big) \qquad \text{when } f \text{ is a homomorphism,}$$

$$\text{and} \qquad [x,y]_{f\circ g} = \Big[g(x),g(y)\Big]_f \text{ when } g \text{ is a homomorphism.}$$

Proof. $\forall\ x$ and $y \in G$, $f \circ g(xy) = (f \circ g)(xy) = f\Big(g(xy)\Big)$

$$\begin{aligned}
&\Rightarrow \Big(f \circ g(x)\Big)\Big(f \circ g)(y)\Big)[x,y]_{f\circ g} \\
&= f\Big(g(x)g(y)[x,y]_g\Big) \qquad \Big(\text{two different way to expand } f \circ g(xy)
\end{aligned}$$

$$\text{by using Proposition 2.4 from page 7}\Big)$$

$$\begin{aligned}
&= f\Big(g(x)g(y)\Big)\ f\Big([x,y]_g\Big)\Big[g(x)g(y),[x,y]_g\Big]_f \\
&= f\Big(g(x)\Big)\ f\Big(g(y)\Big)\Big[g(x),g(y)\Big]_f\ f\Big([x,y]_g\Big)\Big[g(x)g(y),[x,y]_g\Big]_f \\
&= \Big(f\circ g(x)\Big)\Big(f\circ g(y)\Big)\Big[g(x),g(y)\Big]_f\ f\Big([x,y]_g\Big)\Big[g(x)g(y),[x,y]_g\Big]_f \\
\Rightarrow [x,y]_{f\circ g} &= \Big[g(x),g(y)\Big]_f\ f\Big([x,y]_g\Big)\Big[g(x)g(y),[x,y]_g\Big]_f\ .
\end{aligned}$$

$$\text{(left product } \Big(f\circ g(x)\ f\circ g(y)\Big)^{-1} \text{ on both sides)}$$

When f is a homomorphism, $[a,b]_f = 1,\ \forall\ a$ and $b \in H$. So

$$\begin{aligned}
[x,y]_{f\circ g} &= \Big[g(x),g(y)\Big]_f\ f\Big([x,y]_g\Big)\Big[g(x)g(y),[x,y]_g\Big]_f \\
&= 1\ f\Big([x,y]_g\Big)\ 1 \\
&= f\Big([x,y]_g\Big).
\end{aligned}$$

When g is a homomorphism, $[a,b]_g = 1,\ \forall\ a$ and $b \in G$. So

$$\begin{aligned}
[x,y]_{f\circ g} &= \Big[g(x),g(y)\Big]_f\ f\Big([x,y]_g\Big)\Big[g(x)g(y),[x,y]_g\Big]_f \\
&= \Big[g(x),g(y)\Big]_f\ f(1)\Big[g(x)g(y),1\Big]_f \\
&= \Big[g(x),g(y)\Big]_f\ \Big(f(1)(f(1)^{-1}\Big) \quad \text{(from Proposition 2.6 (a) on page 8)} \\
&= \Big[g(x),g(y)\Big]_f\ .
\end{aligned}$$

□

Proposition 2.9 *Assume that G and H are finite groups. If there is a function $f : G \to H$, then $[G,G]_f$ is the unique minimal normal subgroup of $\Big\langle f(G)\Big\rangle$, for which composition of f with the natural map onto the quotient group $\Big\langle f(G)\Big\rangle\Big/[G,G]_f$ is a group homomorphism.*

Proof. Let π be the projection from $\Big\langle f(G)\Big\rangle$ onto the the quotient group $\Big\langle f(G)\Big\rangle\Big/[G,G]_f$. From last theorem and the fact that π is a natural homomorphism, we have

$$\forall\ x \text{ and } y \in G, [x,y]_{\pi\circ f} = \pi([x,y]_f) = 1 \ \ (\text{ because } [x,y]_f \in [G,G]_f = 1).$$

So that $\pi \circ f$ is a homomorphism, from Theorem 2.1 on page 4.

Now we only need to show that $[G,G]_f$ is minimal with this property. Assume that $N \trianglelefteq \Big\langle f(G) \Big\rangle$ and that the composition of f with the natural homomorphism $\pi_1 : H \to H/N$ is a homomorphism. Again from last theorem,

$$\forall\ x \text{ and } y \in G, \quad \pi_1([x,y]_f) = [x,y]_{\pi_1 \circ f} = 1.$$

So that $[x,y]_f \in N$. Then $[G,G]_f \leqslant N$. Hence $[G,G]_f$ is the minimal subgroup with this property. □

Furthermore, if there is a function θ from $\Big\langle f(G) \Big\rangle$ to a group K with $\theta \circ f$ being a homomorphism from G to K, then there exists a homomorphism α from $\Big\langle f(G) \Big\rangle \Big/ [G,G]_f$ to K with $\theta = \alpha \circ \pi$ (π is the natural homomorphism claimed in last proposition).

Here is the distributors of a product function.

Theorem 2.10 *If f_1 and f_2 are two arbitrary functions from group G to group H, then function*

$$f_1 * f_2(x) := f_1(x) f_2(x), \forall\ x \in G$$

is a product of these two functions, and $f_1 * f_2 : G \to H$ satisfies

$$[x,y]_{f_1 * f_2} = \Big(\Big[f_2(x)^{-1}, f_1(y) \Big] [x,y]_{f_1} \Big)^{f_2(x) f_2(y)} [x,y]_{f_2}\ , \forall\ x \text{ and } y \in G.$$

It follows that

$$[x,y]_{f_1 * f_2} = \Big(\Big[f_2(x)^{-1}, f_1(y) \Big] [x,y]_{f_1} \Big)^{f_2(xy)}, \text{ if } f_2 \text{ is a group homomorphism;}$$
$$[x,y]_{f_1 * f_2} = \Big[f_1(y), f_2(x) \Big]^{f_2(y)} [x,y]_{f_2}\ , \qquad \text{if } f_1 \text{ is a group homomorphism.}$$

Proof. $\forall\ x$ and $y \in G$,

$$\begin{aligned}
[x,y]_{f_1 * f_2} &= \Big(f_1 * f_2(y) \Big)^{-1} \Big(f_1 * f_2(x) \Big)^{-1} \Big(f_1 * f_2(xy) \Big) \\
&\qquad\qquad \text{(from the definition of distributor)} \\
&= \Big(f_1(y) f_2(y) \Big)^{-1} \Big(f_1(x) f_2(x) \Big)^{-1} \Big(f_1(xy) f_2(xy) \Big) \\
&= f_2(y)^{-1} f_1(y)^{-1} f_2(x)^{-1} f_1(x)^{-1} f_1(xy) f_2(xy)
\end{aligned}$$

$$= f_2(y)^{-1}f_1(y)^{-1}f_2(x)^{-1}f_1(x)^{-1}\Big(f_1(x)f_1(y)[x,y]_{f_1}\Big)\Big(f_2(x)f_2(y)[x,y]_{f_2}\Big)$$

(from Proposition 2.4 on page 7)

$$= f_2(y)^{-1}f_1(y)^{-1}f_2(x)^{-1}f_1(y)[x,y]_{f_1}\ f_2(x)f_2(y)[x,y]_{f_2}\ \cdots\cdots\cdots\bigstar$$

$$= f_2(y)^{-1}f_2(x)^{-1}\Big(f_2(x)f_1(y)^{-1}f_2(x)^{-1}f_1(y)\Big)[x,y]_{f_1}\ f_2(x)f_2(y)[x,y]_{f_2}$$

$$= f_2(y)^{-1}f_2(x)^{-1}\Big[f_2(x)^{-1},f_1(y)\Big][x,y]_{f_1}\ f_2(x)f_2(y)[x,y]_{f_2}$$

$$= \Big(\Big[f_2(x)^{-1},f_1(y)\Big][x,y]_{f_1}\Big)^{f_2(x)f_2(y)}[x,y]_{f_2}$$

It is obvious that, when f_2 is a group homomorphism

$$[x,y]_{f_1*f_2} = \Big(\Big[f_2(x)^{-1},f_1(y)\Big][x,y]_{f_1}\Big)^{f_2(x)f_2(y)}[x,y]_{f_2}$$

$$= \Big(\Big[f_2(x)^{-1},f_1(y)\Big][x,y]_{f_1}\Big)^{f_2(x)f_2(y)}\ 1 \text{ (from Theorem 2.1 on page 4)}$$

$$= \Big(\Big[f_2(x)^{-1},f_1(y)\Big][x,y]_{f_1}\Big)^{f_2(xy)};$$

(from definition of homomorphism)

and when f_1 is a group homomorphism

$$[x,y]_{f_1*f_2} = f_2(y)^{-1}f_1(y)^{-1}f_2(x)^{-1}f_1(y)[x,y]_{f_1}\ f_2(x)f_2(y)[x,y]_{f_2}$$

$$\Big(\text{from } (\bigstar)\Big)$$

$$= f_2(y)^{-1}f_1(y)^{-1}f_2(x)^{-1}f_1(y)f_2(x)f_2(y)[x,y]_{f_2}$$

(from Theorem 2.1 on page 4)

$$= f_2(y)^{-1}\Big[f_1(y),f_2(x)\Big]f_2(y)[x,y]_{f_2}$$

$$= \Big[f_1(y),f_2(x)\Big]^{f_2(y)}[x,y]_{f_2}\ .$$

□

Theorem 2.11 *If f_i $(i = 1,\cdots,n)$ are arbitrary functions from group G to an **abelian** group H, then function*

$$F(x) := \prod_{i=1}^{n} f_i(x), \forall\ x \in G$$

*is a product function from group G to the **abelian** group H, which satisfies*

$$[x,y]_F = \prod_{i=1}^{n}[x,y]_{f_i}\ , \forall\ x \text{ and } y \in G.$$

Proof. Firstly, we need to prove case $n = 2$:

when H is adelian, $\forall\ x$ and $y \in G$,

$$[x,y]_{f_1 * f_2} = \Big(\Big[f_2(x)^{-1}, f_1(y)\Big][x,y]_{f_1}\Big)^{f_2(x)f_2(y)}[x,y]_{f_2}$$

(from last theorem)

$$= \Big(1\ [x,y]_{f_1}\Big)^{f_2(x)f_2(y)}[x,y]_{f_2}$$

$$= [x,y]_{f_1}[x,y]_{f_2}\ .$$

For case $n \geqslant 2$, we can prove it by induction (it is quite similar as proof above). So

$$[x,y]_{\prod_{i=1}^{n} f_i(x)} = \prod_{i=1}^{n}[x,y]_{f_i}\ .$$

□

2.3 Right Distributors

Just as that we have two different definitions for commutators, we can define another type of distributor. In this case we will call it the "right distributors". Comparing to this, the "original" distributors defined before can be considered as the "left distributors".

Let G and H be finite groups, and $f : G \to H$ is a function from G to H. Then the right f-distributor of x and y is defined as

$$[x, y]_{(f)} := f(xy)f(y)^{-1}f(x)^{-1}, \forall \text{ } x \text{ and } y \in G.$$

And the right f-distributor of group G is defined as

$$[G, G]_{(f)} := \Big\langle [x, y]_{(f)} : \forall x, y \in G \Big\rangle.$$

Then we can find the relation between these two kinds of distributors:

$$\begin{aligned}
\forall \text{ } x \text{ and } y \in G, [x, y]_f &= f(y)^{-1}f(x)^{-1}f(xy) \\
&= f(y)^{-1}f(x)^{-1}f(xy)\Big(f(y)^{-1}f(x)^{-1}f(x)f(y)\Big) \\
&= f(y)^{-1}f(x)^{-1}\Big(f(xy)f(y)^{-1}f(x)^{-1}\Big)f(x)f(y) \\
&= f(y)^{-1}f(x)^{-1}[x, y]_{(f)}f(x)f(y) \\
&= [x, y]_{(f)}^{f(x)f(y)}.
\end{aligned}$$

Here is the list of properties for right distributors, which can be proved from left distributors:

$[x, y]_{(-1)} = [y, x] = [x, y]^{-1}, \forall \text{ } x \text{ and } y \in G;$

$[x, y]_{(2)} = [y^{-1}x^{-1}, x^{-1}], \forall \text{ } x \text{ and } y \in G;$

$f(xy) = [x, y]_{(f)} \text{ } f(x)f(y), \forall \text{ } x \text{ and } y \in G;$

$[y, z]_{(f)}^{f(x)^{-1}} = [x, yz]_{(f)}^{-1}[xy, z]_{(f)}[x, y]_{(f)}, \forall \text{ } x, y, z \in G;$

$[x, 1]_{(f)} = \Big(f(1)^{-1}\Big)^{f(x)^{-1}}, \forall \text{ } x \in G;$

$[1, x]_{(f)} = f(1)^{-1}, \forall \text{ } x \in G;$

$f\Big(x^{-1}\Big) = \Big[x^{-1}, x\Big]_{(f)}^{-1} f(1)f(x)^{-1}, \forall \text{ } x \in G;$

$f\Big(x^{-1}\Big) = f(x)^{-1}\Big[x^{-1}, x\Big]_{(f)}^{-1} f(1), \forall \text{ } x \in G;$

$\Big[x, x^{-1}\Big]_{(f)} = f(x)^{f(1)^{-1}}[x^{-1}, x]_{(f)} \text{ } f(x)^{-1}, \forall \text{ } x \in G.$

As similarly as left distributors, we can also prove that:

$\forall\ x$ and $y \in G$,

$$[x,y]_{(f\circ g)} = \Big[[x,y]_{(g)}, g(x)g(y)\Big]_{(f)}\ f\Big([x,y]_{(g)}\Big)\Big[g(x),g(y)\Big]_{(f)}^{-1};$$

$$[x,y]_{(f_1 * f_2)} = [x,y]_{(f_1)}\Big([x,y]_{(f_2)}\Big[f_2(x)^{-1}, f_1(y)\Big]\Big)^{\Big(f_1(x)f_1(y)\Big)}.$$

From Theorem 2.7 on page 9, we know that the distributor of group G must be normal in the generated group of the image. So from last equation, we have

$$[G,G]_{(f)} = [G,G]_f.$$

Then all properties of left distributor group still hold for right distributor group. For right distributors of any two elements, most properties change a little bit, but there is no big difference between them. So we will use left distributors in this paper.

Chapter 3

Conjugation of Functions

3.1 Definition of Conjugation of Functions

From last chapter, it shows that the f-distributor of any function f between two groups can be considered as the "commutator" of the function f. We know that for the general commutator of two elements in a group, it can be linked to the conjugation of these two elements. Then it is natural to ask this following question: can we define the "conjugation" for any function?

Definition 3.1 *Let G and H be finite groups. If $f : G \to H$ is a function, and $\mathbf{a} \in G$ is a fixed element. Then define a new function $f^{\mathbf{a}} : G \to H$ by*

$$f^{\mathbf{a}}(x) := f(\mathbf{a})^{-1} f(\mathbf{a}x), \forall\ x \in G.$$

We call this the conjugate of the function f under $\mathbf{a}$.

For commutator and conjugation of any two elements x and y in a group G, we have

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

So there should be some connection between f-distributor and the conjugation of f for the same function f. Then we can use them to redefine each other.

Proposition 3.1 *If $f : G \to H$ is a function for groups, then*

$$\begin{aligned} [a,x]_f &= f(x)^{-1}f^a(x), \\ f^a(x) &= f(x)[a,x]_f \ , \\ \textit{and} \ \ f(x) &= f^a(x)[a,x]_f^{-1}, \ \ \forall \ a \ \textit{and} \ x \in G. \end{aligned}$$

Proof.

$\forall$ a and $x \in G$, $[a,x]_f = f(x)^{-1}f(a)^{-1}f(ax)$

(from the definition of distributor)

$$= f(x)^{-1}\Big(f(a)^{-1}f(ax)\Big)$$

$= f(x)^{-1}f^a(x)$ (from the definition of conjugation)

$\Rightarrow \quad [a,x]_f = f(x)^{-1}f^a(x);$

$\Rightarrow \quad f^a(x) = f(x)[a,x]_f;$ (left product $f(x)$ on both sides)

$\Rightarrow \quad f(x) = f^a(x)[a,x]_f^{-1}.$ (right product $[a,x]_f^{-1}$ on both sides)

□

By using the definitions above, we can define homomorphism by using the conjugation of functions.

Theorem 3.2 *A function $f : G \to H$ is a group homomorphism*
iff *$f^a = f$, $\forall$ $a \in G$.*

Proof. It is obvious from last proposition.

$f^a = f, \forall \ a \in G \Leftrightarrow f^a(x) = f(x), \forall \ x \in G$, for all a in G

$\Leftrightarrow f(x)[a,x]_f = f(x), \forall$ a and $x \in G$

$\Leftrightarrow [a,x]_f = 1, \forall$ a and $x \in G$

(left product $f(a)^{-1}$ on both sides)

$\Leftrightarrow$ f is a homomorphism. (from Theorem 2.1 on page 4)

This can also be proved by only using definitions of conjugation and homomorphism. □

Example 3.3 *Consider a function defined as* $(-1) : x \to x^{-1}$, $\forall x \in G$. *Then* $\forall\ x$ *and* $y \in G$,

$$\begin{aligned}(-1)^a(x) &= a(ax)^{-1} \\ &= ax^{-1}a^{-1} \\ &= \left(x^{-1}\right)^{a^{-1}}.\end{aligned}$$

So the conjugate of (-1) *under* a *maps* x *to the conjugate of* x^{-1} *under* a^{-1}.

$$\begin{aligned}\textit{Then } (-1) \textit{ is a homomorphism} &\Leftrightarrow (-1)^a = (-1), \forall\ a \in G \\ &\Leftrightarrow (-1)^a(x) = (-1)(x), \forall\ a \textit{ and } x \in G \\ &\Leftrightarrow \left(x^{-1}\right)^{a^{-1}} = x^{-1}, \forall\ a \textit{ and } x \in G \\ &\Leftrightarrow x^{a^{-1}} = x, \forall\ a \textit{ and } x \in G \\ &\Leftrightarrow x^a = x, \forall\ a \textit{ and } x \in G \\ &\Leftrightarrow [x, a] = [a, x] = 1, \forall\ a \textit{ and } x \in G \\ &\Leftrightarrow \textit{Group } G \textit{ is abelian.}\end{aligned}$$

Then from Figure 1 on page 5, we have:

$$\begin{array}{c} (-1)(x) = x^{-1}\ (\forall\ x \in G) \\ \textit{is a homomorphism} \Leftrightarrow \textit{Group } G \textit{ is abelian} \\ \Updownarrow \qquad\qquad \Updownarrow \\ [G, G]_{-1} = 1 \iff [G, G] = 1 \\ \Updownarrow \qquad\qquad \Updownarrow \\ (-1)^a = (-1), \forall\ a \in G \Leftrightarrow x^a = x, \forall\ a \textit{ and } x \in G \end{array}$$

Figure 3

Example 3.4 *Consider a function defined as* $(2) : x \to x^2$, $\forall x \in G$. *Then*

$\forall\ x\ and\ y \in G,$

$$\begin{aligned}(2)^a(x) &= a^{-1}a^{-1}axax \\ &= a^{-1}xax \\ &= x^a x.\end{aligned}$$

So the conjugate of (2) *under* a *maps* x *to the conjugate of* x *under a right product itself.*

Then (2) *is a homomorphism* $\Leftrightarrow (2)^a = (2), \forall\ a \in G$

$\Leftrightarrow (2)^a(x) = (-2)(x), \forall\ a\ and\ x \in G$

$\Leftrightarrow x^a x = x^2, \forall\ a\ and\ x \in G$

$\Leftrightarrow x^a = x, \forall\ a\ and\ x \in G$

$\Leftrightarrow$ *Group* G *is abelian.*

Then from Figure 2 on page 6, we have:

$(2)(x) = x^2\ (\forall\ x \in G)$

is a homomorphism $\Leftrightarrow$ *Group* G *is abelian*

$$\begin{array}{ccc} \Updownarrow & & \Updownarrow \\ [G,G]_2 = 1 & \Longleftrightarrow & [G,G] = 1 \\ \Updownarrow & & \Updownarrow \\ (2)^a = (2), \forall\ a \in G & \Leftrightarrow & x^a = x, \forall\ a\ and\ x \in G \end{array}$$

Figure 4

So we get the same result as in Chapter 2.

In the next section, there are some other properties about conjugation of functions which need to be discussed.

3.2 Some Properties of Function Conjugation

Here are some very important and useful properties for conjugations of functions.

Proposition 3.5 *If f is a function from group G to group H, then*

$$f(xy) = f(x)f^x(y) \ , \forall \ x \ \textit{and} \ y \in G.$$

Proof. It is obvious from the definition of conjugation of function (on page 17), by left product $f(x)$ on both sides. But it also can be proved by using distributor.

$$\begin{aligned} \forall \ x \text{ and } y \in G, \ f(xy) &= f(x)f(y)[x,y]_f \qquad \text{(from Proposition 2.4 on page 7)} \\ &= f(x)\Big(f(y)[x,y]_f\Big) \\ &= f(x)f^x(y). \qquad \text{(from Proposition 3.1 on page 17)} \end{aligned}$$

□

We also want to look at the distributor of a function conjugation.

Proposition 3.6 *If f is a function from group G to group H, then*

$$[y,z]_{f^x} = [x,z]_f^{-1}[xy,z]_f \ , \ \forall \ x,y,z \in G.$$

Proof. $\forall \ x,y,z \in G$,

$$\begin{aligned} [x,z]_f^{-1}[xy,z]_f &= \Big(f(z)^{-1}f(x)^{-1}f(xz)\Big)^{-1}\Big(f(z)^{-1}f(xy)^{-1}f(xyz)\Big) \\ &\qquad \text{(from definition of distributor)} \\ &= f(xz)^{-1}f(x)f(z)f(z)^{-1}f(xy)^{-1}f(xyz) \\ &= \Big(f(x)^{-1}f(xz)\Big)^{-1}f(xy)^{-1}f(x)f(x)^{-1}f(xyz) \\ &= f^x(z)^{-1}\Big(f(x)^{-1}f(xy)\Big)^{-1}f^x(yz) \\ &\qquad \text{(from definition of conjugation)} \\ &= f^x(z)^{-1}f^x(y)^{-1}f^x(yz) \qquad \text{(from definition of conjugation)} \\ &= [y,z]_{f^x} \ . \qquad \text{(from definition of distributor)} \end{aligned}$$

□

Theorem 3.7 *$f : G \to H$ is a function for groups, then*

$$\left(f^a\right)^b = f^{ab},\ \forall\ a \text{ and } b \in G.$$

Proof. $\forall\ x, a, b \in G$

$$\begin{aligned}
\left(f^a\right)^b(x) &= f^a(x)[b, x]_{f^a} && \text{(from Proposition 3.1 on page 17)} \\
&= f^a(x)[a, x]_f^{-1}[ab, x]_f && \text{(from last proposition)} \\
&= \left(f^a(x)[a, x]_f^{-1}\right)[ab, x]_f \\
&= f(x)[ab, x]_f && \text{(from Proposition 3.1 on page 17)} \\
&= f^{ab}(x) && \text{(from Proposition 3.1 on page 17)} \\
\Rightarrow \left(f^a\right)^b &= f^{ab}, \forall\ a \text{ and } b \in G.
\end{aligned}$$

Or we can prove it without using any theorems and propositions, by simply expanding the conjugation of functions by definition:

$$\begin{aligned}
\left(f^a\right)^b(x) &= f^a(b)^{-1} f^a(bx) && \text{(from the definition of conjugation)} \\
&= \left(f(a)^{-1} f(ab)\right)^{-1} \left(f(a)^{-1} f(abx)\right) \\
& && \text{(from the definition of conjugation)} \\
&= f(ab)^{-1} f(a) f(a)^{-1} f(abx) \\
&= f(ab)^{-1} f(abx) \\
&= f^{ab}(x). && \text{(from the definition of conjugation)}
\end{aligned}$$

□

So the conjugate of a conjugate is the conjugate of the product.

Then from the definition of action, if we want the conjugation of functions to be an action, we also need $f^1 = f$.

Theorem 3.8 *$f : G \to H$ is a function for groups, then*

$$f^1(x) = f(1)^{-1} f(x), \forall\ x \in G.$$

$$\textit{Also}\quad f(1) = 1 \Leftrightarrow f^1(x) = f(x), \forall\ x \in G.$$

Proof.

$$\begin{aligned} \forall\, x \in G, f^1(x) &= f(1)^{-1} f(1x) \qquad \text{(from the definition of conjugation)} \\ &= f(1)^{-1} f(x). \end{aligned}$$

But we can also use distributors to prove this equation.

$$\begin{aligned} f^1(x) &= f(x)[1,x]_f && \text{(from Proposition 3.1 on page 17)} \\ &= f(x)\Big(f(1)^{-1}\Big)^{f(x)} && \text{(from Proposition 2.6 (b) on page 8)} \\ &= f(x)f(x)^{-1}f(1)^{-1}f(x) \\ &= f(1)^{-1}f(x). \end{aligned}$$

Then obviously we can have

$$\begin{aligned} f^1(x) = f(x) &\Leftrightarrow f(1)^{-1}f(x) = f(x) && \text{(from equation above)} \\ &\Leftrightarrow f(1)^{-1} = f(x)f(x)^{-1} && \text{(right product } f(x)^{-1} \text{ on both sides)} \\ &\Leftrightarrow f(1)^{-1} = 1 \\ &\Leftrightarrow f(1) = 1. && \text{(take inverses on both sides)} \end{aligned}$$

□

From last two theorems, we can conclude that conjugations of functions can be a action **if and only if** $f(1) = 1$. We will discuss it later in next section.

Now we look at the conjugation of a composition function and a product function. (We need to use these theorems a lot in following chapters.)

Theorem 3.9 *If $g : G \to H$ and $f : H \to K$ are two arbitrary functions, and G, H, K are groups.*

$$\begin{aligned} &\textit{Then} && (f \circ g)^a &&= f^{g(a)} \circ g^a, \forall\ a \in G. \\ &\textit{Moreover,} && (f \circ g)^a &&= f \circ g^a \quad \textit{when } f \textit{ is a homomorphism} \\ &\textit{and} && (f \circ g)^a &&= f^{g(a)} \circ g \quad \textit{when } g \textit{ is a homomorphism.} \end{aligned}$$

Proof. $\forall\ x$ and $a \in G$,

$$
\begin{aligned}
(f\circ g)^a(x) &= \Big(f\circ g(x)\Big)[a,x]_{f\circ g} \qquad \text{(from Proposition 3.1 on page 17)}\\
&= f\Big(g(x)\Big)\ \Big[g(a),g(x)\Big]_f\ f\Big([a,x]_g\Big)\Big[g(a)g(x),[a,x]_g\Big]_f\\
&\qquad\qquad \text{(from Theorem 2.8 on page10)}\\
&= f^{g(a)}\Big(g(x)\Big)\ \ f^{g(a)g(x)}\Big([a,x]_g\Big)\\
&\qquad\qquad \text{(from Proposition 3.1 on page 17)}\\
&= f^{g(a)}\Big(g(x)\Big)\ \ (f^{g(a)})^{g(x)}\Big([a,x]_g\Big)\\
&\qquad\qquad \text{(from Theorem 3.7 at page 22)}\\
&= f^{g(a)}\Big(g(x)\Big)\ f^{g(a)}\Big(g(x)\Big)^{-1}\ f^{g(a)}\Big(g(x)[a,x]_g\Big)\\
&\qquad\qquad \text{(from the definition of conjugation)}\\
&= 1\ f^{g(a)}\Big(g^a(x)\Big) \qquad \text{(from the definition of conjugation)}\\
&= \Big(f^{g(a)}\circ g^a\Big)(x)\\
\Rightarrow (f\circ g)^a &= f^{g(a)}\circ g^a.
\end{aligned}
$$

Or we can prove it without using any theorems and propositions, by simply expanding the conjugation of functions by definition:

$$
\begin{aligned}
\Big(f^{g(a)}\circ g^a\Big)(x) &= f^{g(a)}\Big(g^a(x)\Big)\\
&= f^{g(a)}\Big(g(a)^{-1}g(ax)\Big)\\
&= f\Big(g(a)\Big)^{-1}f\Big(g(a)g(a)^{-1}g(ax)\Big)\\
&= f\Big(g(a)\Big)^{-1}f\Big(g(ax)\Big)\\
&= \Big(f\circ g(a)\Big)^{-1}\Big(f\circ g(ax)\Big)\\
&= (f\circ g)^a(x).
\end{aligned}
$$

Then from Theorem 3.2 at page 18, it is clear that

$$
\begin{aligned}
f \text{ is a homomorphism} \Rightarrow f^{g(a)} = f \ \ &\Rightarrow\ \ (f\circ g)^a = f\circ g^a\ ;\\
g \text{ is a homomorphism} \Rightarrow \ \ g^a = g \ \ &\Rightarrow\ \ (f\circ g)^a = f^{g(a)}\circ g\ .
\end{aligned}
$$

But we can also prove that by applying distributors:

when f is a homomorphism

$$
\begin{aligned}
(f\circ g)^a(x) &= f\circ g(x)\ [a,x]_{f\circ g} \qquad \text{(from Proposition 3.1 on page 17)}\\
&= f\Big(g(x)\Big)f\Big([a,x]_g\Big) \qquad \text{(from Theorem 2.8 on page 10)}
\end{aligned}
$$

$$= f\Big(g(x)[a,x]_g\Big) \qquad \text{(from the definition of homomorphism)}$$
$$= f\Big(g^a(x)\Big) \qquad \text{(from Proposition 3.1 on page 17)}$$
$$= \Big(f \circ g^a\Big)(x);$$

when g is a homomorphism

$$(f \circ g)^a(x) = f \circ g(x)\ [a,x]_{f\circ g}$$
$$= f\Big(g(x)\Big)\Big[g(a), g(x)\Big]_f \qquad \text{(from Theorem 2.8 on page 10)}$$
$$= f^{g(a)}\Big(g(x)\Big) \qquad \text{(from Proposition 3.1 on page 17)}$$
$$= \Big(f^{g(a)} \circ g\Big)(x).$$

□

Theorem 3.10 *If f_1 and f_2 are two arbitrary functions from group G to group H, then*

$$(f_1 * f_2)^a(x) = \Big(f_1^a(x)\Big)^{f_2(a)} f_2^a(x).$$

Proof. Look back (★) from Theorem 2.10 on page 13, we have $\forall\ a$ and $x \in G$,

$$[a,x]_{f_1*f_2} = f_2(x)^{-1}f_1(x)^{-1}f_2(a)^{-1}f_1(x)[a,x]_{f_1}\ f_2(a)f_2(x)[a,x]_{f_2}$$
$$= \Big(f_1(x)f_2(x)\Big)^{-1}f_2(a)^{-1}\Big(f_1(x)[a,x]_{f_1}\Big)f_2(a)\Big(f_2(x)[a,x]_{f_2}\Big)$$
$$= \Big(f_1 * f_2(x)\Big)^{-1}\Big(f_2(a)^{-1}f_1^a(x)f_2(a)\Big)f_2^a(x)$$
$$\text{(from Proposition 3.1 on page 17)}$$
$$= \Big(f_1 * f_2(x)\Big)^{-1}\Big(f_1^a(x)\Big)^{f_2(a)}f_2^a(x)$$

$$\Rightarrow \Big(f_1 * f_2(x)\Big)[a,x]_{f_1*f_2} = \Big(f_1^a(x)\Big)^{f_2(a)}f_2^a(x)$$
$$\text{(left product } f_1 * f_2(x) \text{ on both sides)}$$
$$\Rightarrow \qquad (f_1 * f_2)^a(x) = \Big(f_1^a(x)\Big)^{f_2(a)}f_2^a(x).$$
$$\text{(from Proposition 3.1 on page 17)}$$

We can also prove that from definitions:

$$(f_1 * f_2)^a(x) = \Big(f_1 * f_2(a)\Big)^{-1}\Big(f_1 * f_2(ax)\Big)$$
$$= \Big(f_1(a)f_2(a)\Big)^{-1}\Big(f_1(ax)f_2(ax)\Big)$$
$$= f_2(a)^{-1}\Big(f_1(a)^{-1}f_1(ax)\Big)f_2(ax)$$

$$
\begin{aligned}
&= f_2(a)^{-1} f_1^a(x) f_2(ax) \\
&= \Big(f_2(a)^{-1} f_1^a(x) f_2(a)\Big)\Big(f_2(a)^{-1} f_2(ax)\Big) \\
&= \Big(f_1^a(x)\Big)^{f_2(a)} f_2^a(x).
\end{aligned}
$$

□

Proposition 3.11 *Let $f_1 : G \to J$ and $f_2 : G \to K$ are two arbitrary functions for group G, and J and K are two subgroups of a group H with $[J, K] = 1$. Then*

$$(f_1 * f_2)^a = f_1^a * f_2^a, \forall\ a \in G.$$

Proof. $\forall\ a$ and $x \in G$, $f_1^a(x) \in J$ and $f_2(a) \in K$. Since $[J, K] = 1$, then

$$f_1^a(x) f_2(a) = f_2(a) f_1^a(x).$$

$$
\begin{aligned}
\text{So } \Big(f_1^a(x)\Big)^{f_2(a)} &= f_2(a)^{-1} f_1^a(x) f_2(a) \\
&= f_2(a)^{-1} f_2(a) f_1^a(x) \\
&= 1\ f_1^a(x) \\
&= f_1^a(x).
\end{aligned}
$$

From last theorem, we have

$$
\begin{aligned}
\Big(f_1 * f_2\Big)^a(x) &= \Big(f_1^a(x)\Big)^{f_2(a)} f_2^a(x) \\
&= f_1^a(x) f_2^a(x).
\end{aligned}
$$

□

Theorem 3.12 *If f_i $(i = 1, \cdots, n)$ are arbitrary functions from group G to an **abelian** group H, then function*

$$F(x) = \prod_{i=1}^{n} f_i(x)$$

*is a product function from group G to the **abelian** group H, and*

$$F^a(x) = \prod_{i=1}^{n} f_i^a(x).$$

Proof. For the case when $n = 2$, this follows the last proposition, because H abelian implies $[H, H] = 1$. For the case $n \geqslant 2$, this can be proved by induction.

Here is another proof by using properties of distributors:

$$\begin{aligned} F^a(x) &= F(x)[a,x]_F && \text{(from Proposition 3.1 on page 17)} \\ &= \prod_{i=1}^{n} \underbrace{f_i(x)}_{\in H} \prod_{i=1}^{n} \underbrace{[a,x]_{f_i}}_{\in H} && \text{(from Theorem 2.11 on page 13)} \\ &= \prod_{i=1}^{n} \left(f_i(x)[a,x]_{f_i} \right) \\ &= \prod_{i=1}^{n} f_i^a(x). && \text{(from Proposition 3.1 on page 17)} \end{aligned}$$

□

Proposition 3.13 *$f : G \to H$ is a function for groups, then*

$$f^a(1) = 1, \forall\ a \in G.$$

Proof.

$$\begin{aligned} \forall\ a \in G, f^a(1) &= f(a)^{-1} f(a1) && \text{(from the definition of conjugation)} \\ &= f(a)^{-1} f(a) \\ &= 1. \end{aligned}$$

But we can also use distributors to prove this equation.

$$\begin{aligned} f^a(1) &= f(1)[a,1]_f && \text{(from Proposition 3.1 on page 17)} \\ &= f(1)f(1)^{-1} && \text{(from Proposition 2.6 on page 8)} \\ &= 1. \end{aligned}$$

□

From last proposition, it is clear that any conjugations of functions must map the identity to an identity, even when the function f has $f(1) \neq 1$. This property shows that when conjugation of functions is an action, the orbits will partition the set of identity preserving functions.

In this section, all properties of conjugation of functions can be proved in two different way: simply expanding by definition of function conjugation, and using properties of distributors. Because of that, we can also define the conjugation of functions at the first, and then use properties of function conjugation to prove distributors' properties. It will not change these results.

3.3 Cauchy Theorem

In this section, we will use the conjugation of functions to prove Cauchy Theorem. The idea is from Reference [2].

Lemma 3.14 *Let*

$$\zeta := \{f : G \to H,\ f \text{ is identity preserving}\}.$$

Then the map

$$f \mapsto f^{a^{-1}} \quad (\forall\ f \in \zeta \text{ and } \forall\ a \in G)$$

is a group action of G *on set* ζ*.Also*

$$Orb_G(f) = \{f^a : \forall\ a \in G\}.$$

Proof. Recall the definition of group action:
If G is a group and ζ is a set, then a (left) group action of G on ζ is a function

$$G \times \zeta \to \zeta, \quad (a, f) \to a \cdot f$$

that satisfies the following:

$$\text{Associativity: } (ab) \cdot f = a \cdot (b \cdot f);$$

$$\text{Identity:} \quad 1 \cdot f = f.$$

In this case, $a \cdot f = f^{a^{-1}}$. Then

$$\begin{aligned} a \cdot (b \cdot f) = \left(f^{b^{-1}}\right)^{a^{-1}} &= f^{b^{-1}a^{-1}} \qquad \text{(from Theorem 3.7 on page 22)} \\ = f^{(ab)^{-1}} &= (ab) \cdot f\ . \end{aligned}$$

Identity also holds from Theorem 3.8 on page 22, therefore this is a group action.

Then from the definition of orbit, we have

$$\begin{aligned} \mathrm{Orb}_G(f) &= \{f^{a^{-1}} : \forall\ a \in G\} \\ &= \{f^a : \forall\ a \in G\}. \quad \text{(because } G \text{ is a group)} \end{aligned}$$

□

Lemma 3.15 *Consider the conjugation action on the set*

$$\zeta = \{f : G \to H,\ f \text{ is identity preserving}\}.$$

For some function $f \in \zeta$, if $|Orb_G(f)| = 1$, then function f must be a group homomorphism.

Proof. For $a = 1\ (\in G)$, $f^a = f^1 = f$ (from Theorem 3.8 on page 22)
$\Rightarrow f \in \mathrm{Orb}_G(f),\ \forall\ f \in \zeta.$

$\therefore\ |\mathrm{Orb}_G(f)| = 1 \Rightarrow \mathrm{Orb}_G(f) = \{f\}$
$\Rightarrow f^a = f,\ \forall\ a \in G$
$\Rightarrow f$ is a homomorphism. (from Theorem 3.2 on page 18)

□

Hence we can use this lemma to give a new proof of Cauchy Theorem.

Theorem 3.16 *(Cauchy Theorem)*
Let G be a finite group. For a prime number p, if p divides the order of G ($p \Big| |G|$), then G must have an element of order p.

Proof. Let ζ be a set of functions, defining it as

$$\zeta := \{\text{functions from } \mathbf{Z}_p \text{ to } G, \text{ which preserve identity}\}.$$

Then $\forall\ f \in \zeta$, $f : \mathbf{Z}_p \to G$ with $f(1) = 1$.

Clearly $|\zeta| = |G|^{p-1}$. Because $p \Big| |G|$, then definitely $p \Big| |\zeta|$.

From Lemma 3.14, we can let $\mathbf{Z}_p$ act on ζ by using conjugation of functions. So

$$\mathrm{Orb}_{\mathbf{Z}_p}(f) = \{f^a : \forall\ a \in \mathbf{Z}_p\}.$$

Then from Orbit-Stabilizer Theorem and Lagrange's Theorem, we have

$$|\mathrm{Orb}_{\mathbf{Z}_p}(f)| \Big| |\mathbf{Z}_p| = p.$$

Because p is a prime, the size of $|\mathrm{Orb}_{\mathbf{Z}_p}(f)|$ is 1 or p.

Assume that there are m orbits with size p, and n orbits with size 1 (Clearly m and n are integers which are not smaller than zero). Clearly these orbits partition the set ζ, and ζ is the union of disjoint orbits. Then

$$|\zeta| = \sum_{f \in \zeta} |\mathrm{Orb}_{\mathbf{Z}_p}(f)| = mp + n.$$

$$\begin{aligned} \therefore p \Big| |\zeta| &\Rightarrow p \Big| mp + n \\ &\Rightarrow p \Big| n. \end{aligned}$$

Then we have that the integer n is either a multiple of p or zero.

Now we need to discuss the number n ($n \geqslant 0$).

Firstly $n \neq 0$, because there is a trivial homomorphism $f_0(a) = 1$ ($\forall\ a \in \mathbf{Z}_p$) for any group G and any prime p, and it is clear that f_0 is a homomorphism with orbit size 1. Then definitely $n \geqslant 1$.

Secondly $n \neq 1$. If $n = 1$, then from $p \Big| n$, we must have $p = 1$, which is a contradiction to the fact that p is prime. So we have $n \geqslant 2$.

Next from last lemma, because there are more than one functions with orbit-size 1, there are at least two functions which are homomorphisms (apparently one of them is the trivial homomorphism). So definitely we have a non-trivial homomorphism in ζ.

Let f be a non-trivial homomorphism in ζ, then $\exists\ g \in G$ with $g \neq 1$ such that $f(x) = g$ (for some $x \in \mathbf{Z}_p$). Then

$$\begin{aligned} g^p &= [f(x)]^p \\ &= f(x^p) \quad \text{(because } f \text{ is a homomorphism)} \\ &= f(1) \quad (x \in \mathbf{Z}_p \Rightarrow x^p = 1) \\ &= 1. \end{aligned}$$

So there must be a non-identity element g in group G with order of prime p. □

The idea is that: there are many theorems in group theory which may be expressed as finding a homomorphism of a certain type. There will be more examples of using conjugation of functions to prove theorems later.

3.4 Right Conjugation of Functions

Just as right distributors, we can also define "right conjugation of functions".

Let G and H be finite groups. If $f : G \to H$ is a function, and $\mathbf{a} \in G$ is a fixed element. Then define a new function $f^{(\mathbf{a})} : G \to H$ by

$$f^{(\mathbf{a})}(x) := f(x\mathbf{a})f(\mathbf{a})^{-1}, \forall\ x \in G.$$

We call this the right conjugate of the function f under $\mathbf{a}$.

Then we have:

$f^{(a)}(x) = [x, a]_{(f)}f(x), \forall\ a$ and $x \in G$;

$f(xy) = f^{(y)}(x)f(y), \forall\ x$ and $y \in G$;

$(-1)^{(a)}(x) = (x^{-1})^a, \forall\ a$ and $x \in G$;

$(2)^{(a)}(x) = xx^{a^{-1}}, \forall\ a$ and $x \in G$;

$(f_1 * f_2)^{(a)}(x) = f_1^{(a)}(x)\Big(f_2^{(a)}(x)\Big)^{f_1(a)^{-1}}, \forall\ a$ and $x \in G$.

The most important part is:

$\Big(f^{(a)}\Big)^{(b)} = f^{(ba)}, \forall\ a$ and $b \in G$;

and $f^{(1)}(x) = f(x)f(1)^{-1}, \forall\ x \in G$.

Then let

$$\zeta := \{f : G \to H,\ f \text{ is identity preserving}\}.$$

Then the map

$$f \mapsto f^{(a)}\ \ (\forall\ f \in \zeta \text{ and } \forall\ a \in G)$$

is a group action of G on set ζ.

Similarly as what we have done to distributors, we will use left conjugation of functions in this paper.

Chapter 4

Transfer Maps

4.1 Old Definition of Transfer

The transfer map is one specific kind of homomorphism, which is also "one of the basic techniques of finite group theory" (from Reference [4], page 285). It has wide applications, especially for some insolvable groups.

Definition 4.1 *If H is a subgroup of finite index n in a group G, then the transfer is the function from G to the abelianization H (H/H'), defined by*

$$\tau(g) = \prod_{i=1}^{n} h_i H',$$

where $X = \{x_1, \ldots, x_n\}$ is a right transversal of H in G and $h_i \in H$ with $x_i g = h_i x_{\sigma(i)}$.

What's more, σ is a permutation of $\{1, \ldots, n\}$. In other words, $\sigma \in S_n$. Then for each $g \in G$, there are elements $y_1, y_2, \ldots, y_m$ of right transversal X and positive integers $n_1, n_2, \ldots, n_m$ (all depending on g and $m \leqslant n$) such that the transfer

$$\tau(g) = \prod_{j=1}^{m} (y_j g^{n_j} y_j^{-1}) H'$$

with $y_j g^{n_j} y_j^{-1} \in H$ and $\Sigma_{j=1}^{m} n_j = n$.

On Reference [4] page 285-286 (10.1.1) and Reference [5] page 194-195 (Theorem 7.45), there are proofs to show the transfer is a homomorphism.

That is to say, for every group G, we definitely can find a homomorphism from it to the abelianization of it's subgroup, which has finite index in G. But we can also prove it by conjugation of functions in next section.

4.2 New Definition of Transfer

If we have a subgroup $H \leqslant G$ with finite right transversal $X = \{x_1, \ldots, x_n\}$, and looking at cosets $\{Hx_i\}$ $(i = 1, \ldots, n)$, this gives a map from G to H. Then each $g \in G$ is of the form as $g = hx_i$, for some $h \in H$ and i.

Define a map by $\theta : g \mapsto h$, then θ is not a homomorphism. It is clear that from any right transversal, there is exact one element which belong to subgroup H. Without loss of generality, let $x_1 = 1$.

Combine this map with the natural homomorphism $\pi : H \to H/H' = A$ (Clearly A is a abelian group), then $f = \pi \circ \theta$.

Lemma 4.1 *It is true that*

$$\begin{aligned} \theta(hg) &= h\theta(g); \\ \theta(h) &= h, \qquad \forall\ g \in G \text{ and } \forall\ h \in H. \end{aligned}$$

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

Assume that $g = h_0 x_i$ ($h_0 \in H$ and $x_i \in X$), then $\theta(g) = h_0$.

$$\begin{aligned} \therefore \theta(hg) &= \theta\Big(h(h_0 x_i)\Big) \\ &= \theta\Big((hh_0)x_i\Big) \\ &= hh_0 \qquad \text{(because } hh_0 \in H\text{)} \\ &= h\theta(g); \end{aligned}$$

$$\begin{aligned} \text{and } \theta(h) &= \theta(h1) \\ &= \theta(hx_1) \\ &= h. \end{aligned}$$

□

Lemma 4.2 $\theta^h = \theta, \forall\ h \in H$.

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

$$\begin{aligned} \theta^h(g) &= \theta(h)^{-1}\theta(hg) \qquad \text{(from the definition of conjugation)} \\ &= h^{-1}\Big(h\theta(g)\Big) \qquad\qquad\qquad\qquad \text{(from last lemma)} \end{aligned}$$

$$= \theta(g)$$
$$\Rightarrow \theta^h = \theta.$$

□

Lemma 4.3 *$f^h = f, \forall\ h \in H$.*

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

$$\begin{aligned} f^h(g) &= (\pi \circ \theta)^h(g) \\ &= \left(\pi^{\theta(h)} \circ \theta^h\right)(g) \quad \text{(from Theorem 3.9 on page 23)} \\ &= \left(\pi \circ \theta^h\right)(g) \qquad \text{(because } \pi \text{ is a homomorphism)} \\ &= \pi \circ \theta(g) \qquad\qquad\qquad \text{(from last lemma)} \\ &= f(g) \end{aligned}$$
$$\Rightarrow f^h = f.$$

□

Then we have

$$\begin{aligned} f^h = f, \forall\ h \in H \quad &\Rightarrow \quad f^1 = f \quad \text{(because } 1 \in H) \\ &\Rightarrow \quad f(1) = 1. \text{(from Theorem 3.8 on page 22)} \end{aligned}$$

So from Lemma 3.14 on page 29, the conjugation of f under inverses in G is a group action. Then we need to look at the orbits.

Theorem 4.4 *$\forall\ x \in G$, if $x = hx_i$ for some $h \in H$ and $x_i \in X$, then*

$$f^x = f^{x_i}.$$

Proof.
$$\begin{aligned} f^x &= f^{hx_i} \\ &= \left(f^h\right)^{x_i} \quad \text{(from Theorem 3.7 on page 22)} \\ &= f^{x_i}. \end{aligned}$$

□

We can double check last theorem by expanding the conjugation of functions:

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

$$\begin{aligned} f^h(g) &= f(h)^{-1} f(hg) \qquad \text{(from the definition of conjugation)} \\ &= \Big(\pi \circ \theta(h)\Big)^{-1} \Big(\pi \circ \theta(hg)\Big) \\ &= \pi(h)^{-1}\pi(h)\ \pi\Big(\theta(g)\Big) \qquad \text{(from Lemma 4.1 on page 35)} \\ &= 1\ \pi \circ \theta(g) \\ &= f(g). \end{aligned}$$

Then let $x = hx_i \in G$,

$$\begin{aligned} f^x(g) &= f^{hx_i}(g) \\ &= f(hx_i)^{-1} f(hx_i g) \qquad \text{(from the definition of conjugation)} \\ &= \Big(\pi \circ \theta(hx_i)\Big)^{-1} \Big(\pi \circ \theta(hx_i g)\Big) \\ &= \Big(\pi(h)\ \pi \circ \theta(x_i)\Big)^{-1} \Big(\pi(h)\ \pi \circ \theta(x_i g)\Big) \\ &\qquad\qquad \text{(from Lemma 4.1 on page 35)} \\ &= \pi \circ \theta(x_i)^{-1}\ \pi(h)^{-1}\pi(h)\ \pi \circ \theta(x_i g) \\ &= \pi \circ \theta(x_i)^{-1}\ 1\ \pi \circ \theta(x_i g) \\ &= f(x_i)^{-1} f(x_i g) \\ &= f^{x_i}(g). \end{aligned}$$

$$\begin{aligned} \text{So}\ \ \mathrm{Orb}_G(f) &= \{f^x : \forall\ x \in G\} \\ &= \{f^{x_i} : \forall\ x_i \in X\} \\ &= \mathrm{Orb}_X(f). \end{aligned}$$

Then we just need to check what $\mathrm{Orb}_X(f)$ is.

Lemma 4.5 $\theta(x_i) = 1, \forall\ x_i \in X$.

Proof. $\forall\ x_i \in X,\ \theta(x_i) = \theta(1x_i) = 1.$ □

Lemma 4.6

$$\begin{aligned} \theta^{x_i}(g) &= \theta(x_i g) \\ &= x_i g x_{\sigma(i)}^{-1} \in H, \qquad \forall\ x_i \in X\ \textit{and}\ \forall\ g \in G. \end{aligned}$$

Proof. $\forall\ x_i \in X$ and $\forall\ g \in G$,

$$\begin{aligned}
\theta^{x_i}(g) &= \theta(x_i)^{-1}\theta(x_i g) \qquad \text{(from the definition of conjugation)} \\
&= 1^{-1}\theta(x_i g) \qquad\qquad\qquad\qquad \text{(from last lemma)} \\
&= \theta(x_i g) \\
&= \theta(x_i g x_{\sigma(i)}^{-1} x_{\sigma(i)}) \quad \text{where } x_i g x_{\sigma(i)}^{-1} \in H \\
&= x_i g x_{\sigma(i)}^{-1}.
\end{aligned}$$

□

Lemma 4.7 $f^{x_i}(g) = x_i g x_{\sigma(i)}^{-1} H' \qquad \forall\ x_i \in X$ *and* $\forall\ g \in G$.

Proof. $\forall\ x_i \in X$,

$$\begin{aligned}
f^{x_i}(g) &= (\pi \circ \theta)^{x_i}(g) \\
&= \left(\pi^{\theta(x_i)} \circ \theta^{x_i}\right)(g) \quad \text{(from Theorem 3.9 on page 23)} \\
&= \left(\pi \circ \theta^{x_i}\right)(g) \qquad \text{(because } \pi \text{ is a homomorphism)} \\
&= \pi\left(\theta^{x_i}(g)\right) \\
&= \pi(x_i g x_{\sigma(i)}^{-1}) \qquad\qquad \text{(from last lemma)} \\
&= (x_i g x_{\sigma(i)}^{-1})H'.
\end{aligned}$$

□

Theorem 4.8

$$\tau(g) = \prod_{i=1}^{n} f^{x_i}(g),\ \forall\ g \in G$$

is the transfer map.

Proof.

$\forall\ g \in G$,

$$\begin{aligned}
\prod_{i=1}^{n} f^{x_i}(g) &= \prod_{i=1}^{n} (x_i g x_{\sigma(i)}^{-1})H' \quad \text{(from last lemma where } x_i g x_{\sigma(i)}^{-1} \in H) \\
&= \prod_{i=1}^{n} h_i H' \\
&= \tau(g)
\end{aligned}$$

So $\tau(g)$ is the transfer. □

Theorem 4.9 *If H is a subgroup of finite index in a group G, then the transfer $\tau : G \to H/H'$ is a homomorphism whose definition is independent of the choice of right transversal of H in G.*

Proof.

$$\begin{aligned}
\forall\, x \in G, \quad \tau^x &= \prod_{i=1}^{n} \left(f^{x_i}\right)^x && \text{(from Theorem 3.12 on page 26)} \\
&= \prod_{i=1}^{n} f^{x_i x} && \text{(from Theorem 3.7 on page 22)} \\
&= \prod_{i=1}^{n} f^{h_i x_{\sigma(i)}} && \text{(for some } h_i x_{\sigma(i)} = x_i x\text{)} \\
&= \prod_{i=1}^{n} f^{x_{\sigma(i)}} && \text{(from Theorem 4.4 on page 36)} \\
&= \prod_{i=1}^{n} f^{x_i} && \text{(because } \sigma \text{ is a permutation)} \\
&= \tau. && \text{(from last theorem)}
\end{aligned}$$

So from Theorem 3.2 on page 18, the transfer map τ is a homomorphism. □

Then from the discussion in last section, for each $g \in G$

$$\tau(g) = \prod f^{y_j}(g^{n_j}),$$

with $y_j g^{n_j} y_j^{-1} \in H \quad (y_j \in X)$ and $\Sigma n_j = n$.

4.3 Some Applications of Transfer Maps

From last section, we know that the transfer map is a homomorphism from every group G to H/H', with H being any subgroup of finite index in G. There are many theorems which need to be proved by finding the transfer map for a certain type of groups (mostly use the case of $\tau(g) = g^n, \forall\ g \in G$). So in this section, we will discuss the condition for $\tau(g) = g^n$ $(\forall\ g \in G)$, and then show some theorems for example from Reference [3] and [5].

Lemma 4.10 *Let H be a subgroup of finite index n in G, and for some $g \in G$ there are elements y_j of right transversal X and positive integers n_j $(j = 1, 2, \ldots, m)$ with $y_j g^{n_j} y_j^{-1} \in H$ and $\Sigma n_j = n$. If*

$$\textit{for each } n_j,\ [g^{n_j}, y_j^{-1}] \in H' \textit{ and } g^{n_j} \in N_G(H') \Rightarrow \tau(g) = g^n H'.$$

Furthermore, when H is abelian $(H' = 1)$, y_j and n_j $(j = 1, 2, \ldots, m)$ are selected like above. Then for some $g \in G$, if

$$\forall\ j,\ [g^{n_j}, y_j] = 1 \Rightarrow \tau(g) = g^n.$$

Proof. For all $g \in G$, there are elements y_j of right transversal X and positive integers n_j $(j = 1, 2, \ldots, m)$ with $y_j g^{n_j} y_j^{-1} \in H$ and $\Sigma n_j = n$. Then $\forall\ j$

$$\begin{aligned} f^{y_j}(g^{n_j}) &= y_j g^{n_j} y_j^{-1} H' \\ &= g^{n_j}\left((g^{n_j})^{-1} y_j g^{n_j} y_j^{-1}\right) H' \\ &= g^{n_j}[g^{n_j}, y_j^{-1}] H' \end{aligned}$$

$$[g^{n_j}, y_j^{-1}] \in H' \Rightarrow [g^{n_j}, y_j^{-1}] H' = H'.$$

$$\begin{aligned} \therefore \tau(g) &= \prod f^{y_j}(g^{n_j}) \\ &= \prod g^{n_j} H' \\ &= \left(\prod g^{n_j}\right) H' \quad (g^{n_j} \in N_G(H') \Rightarrow H' g^{n_j} = g^{n_j} H') \\ &= g^n H'. \end{aligned}$$

Now look at the case of abelian H $(H' = 1)$:

$$\begin{aligned} N_G(1) = G & \\ \text{and } [g^{n_j}, y_j] = 1 \quad &\Rightarrow \quad (g^{n_j})^{-1} y_j^{-1} g^{n_j} y_j = 1 \\ &\Rightarrow \quad y_j^{-1} g^{n_j} = g^{n_j} y_j^{-1} \\ &\Rightarrow \quad 1 = (g^{n_j})^{-1} y_j g^{n_j} y_j^{-1} \\ &\Rightarrow \quad [g^{n_j}, y_j^{-1}] = 1 \in H' \\ &\Rightarrow \quad \tau(g) = g^n H' = g^n. \end{aligned}$$

□

Next two theorems are from Reference [5], page 196-197 (Theorem 7.47-50).

Theorem 4.11 *If H is an abelian subgroup of finite index n in a group G and if $H \leqslant Z(G)$, then $\tau(g) = g^n, \forall g \in G$. Furthermore, if a group G has a subgroup H of finite index n with $H \leqslant Z(G)$, then the function $g \mapsto g^n$ for all $g \in G$ is a homomorphism.*

Proof. Look at the transfer map $\tau(g) = \prod f^{y_j}(g^{n_j})$, with $y_j g^{n_j} y_j^{-1} \in H$ $(y_j \in X$ and $\Sigma n_j = n)$.

Because $H \leqslant Z(G)$, then $[H, G] = 1$.

$$\begin{aligned} \therefore [y_j g^{n_j} y_j^{-1}, y_j] = 1 \quad &\Rightarrow \quad [y_j g^{n_j} y_j^{-1}, y_j y_j y_j^{-1}] = 1 \\ &\Rightarrow \quad y_j [g^{n_j}, y_j] y_j^{-1} = 1 \\ &\Rightarrow \quad [g^{n_j}, y_j] = 1 \\ &\Rightarrow \quad \tau(g) = g^n \qquad \text{(from last lemma)} \end{aligned}$$

Then, if a group G has a subgroup H of finite index n with $H \leqslant Z(G)$, the function $g \mapsto g^n$ for all $g \in G$ is the transfer from G to H. Because we already prove that any transfer is a homomorphism in Theorem 3.15 at the end of the last section, in this case the transfer $g \mapsto g^n$ for all $g \in G$ must be a homomorphism. □

According to Rotman in Reference [5], by using transfer, this is the easiest way to prove that function $\tau(g) = g^n \quad (\forall\ g \in G)$ is a homomorphism when group G has a subgroup of finite index n.

Theorem 4.12 *(Burnside Normal Complement Theorem)*
Let G be a finite group and let H be an abelian Sylow subgroup contained in the center of its normalizer: $H \leqslant Z(N_G(H))$. Then H has a normal complement K.

Proof. Let $|H| = m$ and $[G : H] = n$. Because H is a Sylow subgroup, then $|H|$ and $[G : H]$ are relatively prime. So there are some integers k and l such that $km + ln = 1$.

Look at the transfer homomorphism $\tau(g) = \prod f^{y_j}(g^{n_j})$, with $y_j g^{n_j} y_j^{-1} \in H$ ($y_j \in X$ and $\Sigma n_j = n$).

Assume that $K = \mathrm{Ker}(\tau)$, then from First Isomorphism Theorem, we get

$$G/K \cong \mathrm{Im}(\tau) \leqslant H \text{ and } K \trianglelefteq G.$$

So

$$G = K\ \mathrm{Im}(\tau) \subseteq KH.$$

Because $KH \subseteq G$, $KH = G$. Then to prove that K is a normal complement of H in G, we need to show that $H \cap K = 1$.

$\forall\ x \in H$, then $x^m = 1$. Now look at the transfer $\tau(x) = \prod f^{y_j}(x^{n_j})$, with $y_j x^{n_j} y_j^{-1} \in H$. Because H is abelian, $H \leqslant C_G(H)$. So

$$y_j H y_j^{-1} \leqslant y_j C_G(H) y_j^{-1} = C_G(y_j H y_j^{-1}).$$

Since $x \in H$, $x^{n_j} \in H$. Hence

$$y_j H y_j^{-1} \leqslant C_G(y_j H y_j^{-1}) \leqslant C_G(y_j x^{n_j} y_j^{-1}).$$

$y_j x^{n_j} y_j^{-1} \in H$, so $C_G(H) \leqslant C_G(y_j x^{n_j} y_j^{-1})$. Then $H \leqslant C_G(y_j x^{n_j} y_j^{-1})$.

Because $C_G(y_j x^{n_j} y_j^{-1}) \leqslant G$ and H is a Sylow subgroup in G, then H and $y_j H y_j^{-1}$ are two Sylow subgroups in $C_G(y_j x^{n_j} y_j^{-1})$. Then

$$\exists\ c \in C_G(y_j x^{n_j} y_j^{-1}) \text{ such that } c^{-1} H c = y_j H y_j^{-1}.$$

So $H^{y_j^{-1}c} = H$. Therefore $y_j^{-1}c \in N_G(H)$.

Because $H \leqslant Z(N_G(H))$, then $[H, N_G(H)] = 1$. So$[x^{n_j}, y_j^{-1}c] = 1$.

$$\begin{aligned}
c \in C_G(y_j x^{n_j} y_j^{-1}) &\Rightarrow [y_j x^{n_j} y_j^{-1}, c] = 1 \\
&\Rightarrow [y_j x^{n_j} y_j^{-1}, y_j y_j^{-1} c y_j y_j^{-1}] = 1 \\
&\Rightarrow y_j [x^{n_j}, y_j^{-1} c y_j] y_j^{-1} = 1 \\
&\Rightarrow [x^{n_j}, y_j^{-1} c y_j] = 1 \\
&\Rightarrow [x^{n_j}, y_j][x^{n_j}, y_j^{-1}c]^{y_j} = 1 \quad \text{(commutator identities)} \\
&\Rightarrow [x^{n_j}, y_j] = 1 \\
&\Rightarrow \tau(x) = x^n, \forall\ x \in H. \qquad \text{(from Lemma 4.10)}
\end{aligned}$$

If $x \in K = \mathrm{Ker}(\tau)$ also, then $x^n = 1$. So

$$\begin{aligned}
x \in H \cap K \Rightarrow \quad x &= x^{km+ln} &&= x^{km}x^{ln} \\
&= (x^m)^k (x^n)^l = 1.
\end{aligned}$$

Then $H \cap K = 1$.

So K is a normal complement of H in G. □

Here is the last application of transfer in this paper, from Reference [3], page 250 (Theorem 3.4).

Theorem 4.13 *(Focal Subgroup Theorem)*
If P is a Sylow p-subgroup of G, then the focal subgroup

$$Foc_G(P) := \left\langle x^{-1}x^u | x \in P, u \in G, \text{ and } x^u \in P \right\rangle \text{ equal to } P \cap G'.$$

Proof. It is clear that

$$P' \leqslant \mathrm{Foc}_G(P) \leqslant P \cap G' \text{ and } \mathrm{Foc}_G(P) \trianglelefteq P,$$

so $P/\mathrm{Foc}_G(P) \leqslant P/P'$ and $P/\mathrm{Foc}_G(P)$ is abelian.

Assume that $|P| = m$ and $[G : P] = n$. Because that P is a Sylow subgroup of G, then $\gcd(m, n) = 1$. So there are some integers k and l such that $km + ln = 1$. Then

$$\forall\ x \in P,\ x^{ln} = x^{1-km} = x\Big((x^m)^k\Big)^{-1} = x.$$

Let τ be the transfer from G to $P/\mathrm{Foc}_G(P)$, then

$$\tau(g) = \prod f^{y_j}(g^{n_j}),$$

with $y_j g^{n_j} y_j^{-1} \in P$ and $\Sigma n_j = n$.

$\forall\ x \in P$, $x^{n_j} \in P$, then

$$[x^{n_j}, y_j^{-1}] = (x^{n_j})^{-1} y_j x^{n_j} y_j^{-1} \in \mathrm{Foc}_G(P),$$

and

$$\mathrm{Foc}_G(P) \trianglelefteq P \Rightarrow P \subset N_G\Big(\mathrm{Foc}_G(P)\Big)$$

So

$$\forall\ x \in P,\ \tau(x) = x^n \mathrm{Foc}_G(P). \quad \text{(from Lemma 4.10)}$$

Then

$$\tau(x^l) = x^{ln}\mathrm{Foc}_G(P) = x\mathrm{Foc}_G(P).$$

So the transfer τ is surjective $\Big(\mathrm{Im}(\tau) = P/\mathrm{Foc}_G(P)\Big)$.

Let $K = \mathrm{Ker}(\tau)$. Then from First Isomorphism Theorem,

$$G/K \cong P/\mathrm{Foc}_G(P). \text{ So } G = PK.$$

Because τ maps G to a abelian subgroup, then $G' \leqslant K$. So

$$\mathrm{Foc}_G(P) \leqslant P \cap G' \leqslant P \cap K \text{ and } P \cap K \trianglelefteq P.$$

Then from Second Isomorphism Theorem,

$$G/K = PK/K \cong P/(P \cap K).$$

So

$$P/(P \cap K) \cong P/\mathrm{Foc}_G(P) \Rightarrow |P \cap K| = |Foc_G(P)|.$$

Then

$$P \cap K = P \cap G' = \mathrm{Foc}_G(P).$$

□

Chapter 5

Schur-Zassenhaus Theorem

5.1 Hall Subgroups

Definition 5.1 *If π is a set of primes, a subgroup H of G is called an S_π-subgroup of G provided H is a π-group and $|G : H|$ is divisible by no primes in π. Such a subgroup is also called a Hall subgroup of G.*

Specially if $\pi = \{p\}$, then H is simply a Sylow p-subgroup of G.

Definition 5.2 *If H is an S_π-subgroup of G and H possesses a complement K in G, then $|K| = |G : H|$ and $|H| = |G : K|$. So K is an $S_{\pi'}$-subgroup of G. It is clear that $G = HK$ and $H \cap K = 1$, so each is a complement of each other.*

Unlike Sylow p-subgroups which always exist (from Sylow Theorem), the existence of Hall π-subgroups is more complex. We will discuss the theorems about that question in the following sections.

5.2 Old Proof for Schur-Zassenhaus Theorem

This whole section is all about some standard proofs for Schur-Zassenhaus Theorem, from Reference [1], [3] and [5].

Theorem 5.1 *(**Schur-Zassenhaus Theorem** for Abelian Case Part 1: Existence)*

Let H be an abelian normal S_π-subgroup of a finite group G, then G possesses an $S_{\pi'}$-subgroup K which is a complement to H in G.

Proof. See from Reference [3], page 221-222.

Because H is a normal S_π-subgroup of a finite group G, we can assume that $|H| = n$ and $|\overline{G}| = |G/H| = m$ (m and $n \in \mathbf{Z}^+$). Then it is clear that $\gcd(m, n) = 1$ and $|G| = mn$.

Now let $\{x_i : 1 \leqslant i \leqslant m\}$ be a set of left coset representatives of H in G. If $\bar{x_i}$ is the image of x_i in G, then they are all distinct.

So to be convenient, we will use letters α, β, γ for the elements of $\overline{G}$, and x_α means the element x_i with the property $\bar{x_i} = \alpha$. Then apparently the associative law must hold:

$$(x_\alpha x_\beta)x_\gamma = x_\alpha(x_\beta x_\gamma).$$

Our aim is to replace each x_α by another suitable coset representative y_α, which satisfy

$$y_\beta y_\gamma = y_{\beta\gamma} \ (\forall\ \beta \text{ and } \gamma \in \overline{G}).$$

Then y_α will form a group with order m, so this must be an $S_{\pi'}$-subgroup of G.

In this notation, $x_\alpha x_\beta$ and $x_{\alpha\beta}$ must determine the same coset of H in G. So we have

$$x_\alpha x_\beta = x_{\alpha\beta} f(\alpha, \beta), \quad f(\alpha, \beta) \in H.$$

Then function f is recognized as a 2-cocycle from G to abelian H.

Now look back at the associative law:

$$\begin{aligned}(x_\alpha x_\beta)x_\gamma &= x_{\alpha\beta}f(\alpha,\beta)x_\gamma \\ &= x_{\alpha\beta}x_\gamma f(\alpha,\beta)^{x_\gamma} \\ &= x_{\alpha\beta\gamma}f(\alpha\beta,\gamma)f(\alpha,\beta)^{x_\gamma} \\ \text{and}\quad x_\alpha(x_\beta x_\gamma) &= x_\alpha x_{\beta\gamma}f(\beta,\gamma) \\ &= x_{\alpha\beta\gamma}f(\alpha,\beta\gamma)f(\beta,\gamma)\end{aligned}$$

$$\begin{aligned}\therefore \qquad (x_\alpha x_\beta)x_\gamma &= x_\alpha(x_\beta x_\gamma) \\ \Leftrightarrow\ x_{\alpha\beta\gamma}f(\alpha\beta,\gamma)f(\alpha,\beta)^{x_\gamma} &= x_{\alpha\beta\gamma}f(\alpha,\beta\gamma)f(\beta,\gamma) \\ \Leftrightarrow \qquad f(\alpha\beta,\gamma)f(\alpha,\beta)^{x_\gamma} &= f(\alpha,\beta\gamma)f(\beta,\gamma)\end{aligned}$$

Then let

$$g(\delta)=\prod_{\alpha\in\overline{G}} f(\alpha,\delta),\ \forall\ \delta\in\overline{G}.$$

Because function f maps $G\times G$ to an abelian H, then

$$\begin{aligned}\prod_{\alpha\in\overline{G}}\Big(f(\alpha\beta,\gamma)f(\alpha,\beta)^{x_\gamma}\Big) &= \prod_{\alpha\in\overline{G}}\Big(f(\alpha,\beta\gamma)f(\beta,\gamma)\Big) \\ \prod_{\alpha\in\overline{G}} f(\alpha\beta,\gamma)\prod_{\alpha\in\overline{G}} f(\alpha,\beta)^{x_\gamma} &= \prod_{\alpha\in\overline{G}} f(\alpha,\beta\gamma)\prod_{\alpha\in\overline{G}} f(\beta,\gamma) \\ \prod_{\alpha\in\overline{G}} f(\alpha,\gamma)\Big(\prod_{\alpha\in\overline{G}} f(\alpha,\beta)\Big)^{x_\gamma} &= \Big(\prod_{\alpha\in\overline{G}} f(\alpha,\beta\gamma)\Big)f(\beta,\gamma)^{|\overline{G}|} \\ g(\gamma)g(\beta)^{x_\gamma} &= g(\beta\gamma)f(\beta,\gamma)^m\end{aligned}$$

$$\therefore g(\beta\gamma)=\Big(f(\beta,\gamma)^m\Big)^{-1}g(\beta)^{x_\gamma}g(\gamma).$$

Since $\gcd(m,n)=1$, then there is an integer r such that $rm\equiv 1 \pmod{n}$.

$$\begin{aligned}\text{Then}\quad g(\beta\gamma)^{-r} &= f(\beta,\gamma)^{rm}\Big(g(\beta)^{x_\gamma}\Big)^{-r}g(\gamma)^{-r} \\ &= f(\beta,\gamma)\Big(g(\beta)^{-r}\Big)^{x_\gamma}g(\gamma)^{-r}.\end{aligned}$$

If let

$$h(\delta)=g(\delta)^{-r},$$

then

$$h(\beta\gamma)=f(\beta,\gamma)h(\beta)^{x_\gamma}h(\gamma).$$

If we name

$$y_\alpha = x_\alpha h(\alpha),$$

$$\begin{aligned} \text{then } \ y_\beta y_\gamma &= x_\beta h(\beta) x_\gamma h(\gamma) \\ &= x_\beta x_\gamma h(\beta)^{x_\gamma} h(\gamma) \\ &= x_{\beta\gamma} f(\beta,\gamma) h(\beta)^{x_\gamma} h(\gamma) \\ &= x_{\beta\gamma} h(\beta\gamma) \\ &= y_{\beta\gamma}. \end{aligned}$$

So $\{y_\alpha : \forall\ \alpha \in \overline{G}\}$ is a subgroup required, which is a complement to H in G. □

Theorem 5.2 *(**Schur-Zassenhaus Theorem** for Abelian Case Part 2: Conjugation)*

If H is an abelian normal S_π-subgroup of a finite group G, then any two complements to H in G are conjugate.

Proof. The original proof is from Reference [3], page 223-224.

Since K and K_1 are two complements of H in G, then

$$G = HK = HK_1.$$

For any $x_1 \in K_1 \subseteq G$, $x_1 = xf(x)$, where $x \in K$ and $f(x)$ is a suitable element of H. In this case, x ranges over K as x_1 ranges over K_1. So if $y_1 \in K_1$, then $y_1 = yf(y)$ for some $y \in K$ and $f(y) \in H$.

Since K and K_1 are two subgroups in G, $x_1 y_1 \in K_1$ and $xy \in K$. Then

$$x_1 y_1 = xyf(xy), \text{ for some suitable } f(xy) \in H.$$

So

$$\begin{aligned} x_1 y_1 &= xf(x)yf(y) \\ &= xyf(x)^y f(y) \\ &= xyf(xy). \end{aligned}$$

Then

$$\forall\ x \text{ and } y \in K, f(xy) = f(x)^y f(y).$$

If $|H| = n$ and $|K| = |K_1| = m$ $(m, n \in \mathbf{Z}^+)$, then it is clear that $\gcd(m, n) = 1$ and $|G| = mn$. Then there exist some positive integers p and q such that $pm - qn = 1$. Then $\forall\ a \in H$,

$$\begin{aligned} a^{pm} &= a^{1+qn} = a^1 a^{qn} = a(a^n)^q \\ &= a(1^q) \quad (a \in H \text{ and } |H| = n \Rightarrow a^n = 1) \\ &= a. \end{aligned}$$

Next we will name the set $pK = \underbrace{K + K + \cdots + K}_{p}$ (p is the same positive integer as mentioned above), and it can be thought as going through the subgroup K p-times. Then $|pK| = pm$.

From the discussion above, we can get the formula:

$$\begin{aligned} \prod_{x \in pK} f(x) &= \prod_{x \in pK} f(xy) \\ &= \prod_{x \in pK} (f(x)^y f(y)) \\ &= \prod_{x \in pK} f(x)^y \prod_{x \in pK} f(y) \\ &= \left(\prod_{x \in pK} f(x) \right)^y f(y)^{pm} \\ &= y^{-1} \left(\prod_{x \in pK} f(x) \right) y f(y). \end{aligned}$$

Let

$$u = \prod_{x \in pK} f(x).$$

Then we need to rearrange the formula as:

$$\begin{aligned} y_1 &= y f(y) \\ &= \left(\prod_{x \in pK} f(x) \right)^{-1} y \left(\prod_{x \in pK} f(x) \right) \\ &= u^{-1} y u \\ &= y^u. \end{aligned}$$

Then it shows that $K_1 = K^u$.

So any two complements of a abelian normal Hall subgroup H in G must be conjugate to each other. □

The proof of next theorem is from Reference [1], an unpublished manuscript of Dr. Ian Hawthorn.

Theorem 5.3 *(**Schur-Zassenhaus Theorem** for General Case Part 1: Existence)*

Let H be a normal S_π-subgroup of G, then G possesses an $S_{\pi'}$-subgroup K which is a complement to H in G.

Proof. If $H = 1$, then G itself is an $S_{\pi'}$-subgroup which we want. And if $H = G$,then 1 is the complement. So this theorem is obvious true for trivial case. Then we just need to consider non-trivial case. We assume $H \neq 1$ and $H < G$ all the time in the following.

Now assume that the group-pair (G, H) is the minimal criminal, and the order of that is $\Big(|G|, |H|\Big)$. Then (G, H) is the smallest group-pair which satisfies the following condition: there is no such subgroup K of G which is a complement of a normal S_π-subgroup H in group G. It means that $K \leqslant G$ cannot exist with condition of $KH = G$ and $K \cap H = 1$, but any group-pair (G_1, H_1)which is smaller than (G, H) must have the complement for the normal Hall subgroup $H_1 \leqslant G_1$ (At least one group in group-pair must be smaller than the minimal criminal. In other words, $|H_1| < |H|$ or $|G_1| < |G|$. H_1 is a S_π-subgroup and $H_1 \trianglelefteq G_1 \Rightarrow \exists\ K_1$ with $K_1 H_1 = G_1$ and $K_1 \cap H_1 = 1$).

Let $p \Big| |H|$ (p is one prime in set π, $p \in \pi$), and $P \in Syl_p(H)$ (P is a Sylow p-subgroup in normal subgroup H). By definition of S_π-subgroup, $|H|$ and $|G : H|$ are co-prime $\Rightarrow |P|$ and $|G : P|$are relatively prime, so P is a Sylow p-subgroup in group G as well $\Big(P \in Syl_p(G)\Big)$.

Because the Sylow p-subgroup P is contained in H ($P \leq H$), then $N_G(P)H = G$ (By Frattini argument).

Step 1: $\Big(N_G(P) < G\Big)$ Sylow p-subgroup P is not normal in G, hence the normaliser of P is strict smaller than G.

Because H is a normal subgroup of G ($H \trianglelefteq G$) and a normaliser $N_G(P)$ is always normal in G $\Big(N_G(P) \trianglelefteq G\Big)$, then the intersection of these two is also normal in G $\Big((N_G(P) \cap H) \trianglelefteq G\Big)$. $N_G(P)$ is always a subgroup of G and $N_G(P) \cap H$ is always a subgroup of $N_G(P)$, then $\Big(N_G(P) \cap H\Big) \trianglelefteq N_G(P)$.

Because $N_G(P) \cap H$ is normal in $N_G(P)$ and the second isomorphism theorem, $G/H = N_G(P)H/H$ is isomorphic to $N_G(P)\Big/\Big(N_G(P) \cap H\Big)$. Since $|G : H|$ is prime to $|H|$, it follows that $\Big|N_G(P) : \Big(N_G(P) \cap H\Big)\Big|$ is prime to $|N_G(P) \cap H|$. Then $N_G(P) \cap H$ is a normal S_π-subgroup of $N_G(P)$.

So $N_G(P)$ is strict smaller than G and a normal S_π-subgroup $N_G(P) \cap H \trianglelefteq N_G(P)$. Then by induction, there is a subgroup $K \leq N_G(P)$ which is a complement to $N_G(P) \cap H$ in $N_G(P)$. Then $\Big(N_G(P) \cap H\Big)K = N_G(P)$ and $K \cap \Big(N_G(P) \cap H\Big) = 1$. So

$$\begin{aligned} K \cap H &= \Big(K \cap N_G(P)\Big) \cap H \quad (K \leq N_G(P) \Rightarrow K \cap N_G(P) = K) \\ &= K \cap \Big(N_G(P) \cap H\Big) \\ &= 1 \end{aligned}$$

and

$$\begin{aligned} KH &= K\Big(N_G(P) \cap H\Big)H \quad (\Big(N_G(P) \cap H\Big) \leqslant H \Rightarrow \Big(N_G(P) \cap H\Big)H = H) \\ &= N_G(P)H \\ &= G. \end{aligned}$$

So K is also a complement to H in G, which is a contradiction to the assumption.

Step 2:$P \trianglelefteq G$. In other words, Sylow p-subgroup P is also normal in G $\Big(N_G(P) = G\Big)$.

Firstly, assume $P \neq H$. Then the Sylow p-subgroup P is strict smaller than H ($P < H$). Then by induction, there must be a complement $N \leqslant G$ to P in G. It means that there is a subgroup N in G with $NP = G$ and $N \cap P = 1$.

It is clear that $1 < N \cap H \trianglelefteq N$. By the definition of Sylow p-subgroup, $|P|$ is prime to $|G : P| = |N|$. Similarly as the discussion in Step 1, $N \cap H$ is a S_π-subgroup of N.

Then by induction, there exists a subgroup $K \leqslant N$, which satisfies $N = K(N \cap H)$ and $K \cap (N \cap H) = 1$. So

$$\begin{aligned} K \cap H &= (K \cap N) \cap H \quad (K \leqslant N \Rightarrow K = K \cap N) \\ &= K \cap (N \cap H) \\ &= 1 \end{aligned}$$

and

$$\begin{aligned} KH &= K(N \cap H)H \quad \Big((N \cap H) \leqslant H \Rightarrow (N \cap H)H = H\Big) \\ &= NH \\ &\supset NP = G \end{aligned}$$

And it is obvious that $G \supset KH$, so $KH = G$. Then K is also a complement to H in G, which is also a contradiction to the assumption.

Secondly, assume $P = H$. The center of a p-group is nontrivial, and the center is always normal. So $1 \neq Z(P) \trianglelefteq P \trianglelefteq G$. Let $\bar{G} = G/Z(P)$ and $\bar{P} = P/Z(P)$. Then $\bar{P} \trianglelefteq \bar{G} < G$, and clearly $\bar{P}$ is a Sylow p-subgroup of $\bar{G}$. So $\bar{G}$ is strict smaller than G and $\bar{P} \in Syl_p(\bar{G})$. Then by induction, $\exists\ \bar{M}$ satisfies $\bar{M}\bar{P} = \bar{G}$ and $\bar{M} \cap \bar{P} = 1$. Let M be the pullback of $\bar{M}$ $\Big(\bar{M} = M/Z(P)\Big)$,

then $G = \bar{G}Z(P), P = \bar{P}Z(P)$ and $M = \bar{M}Z(P)$. So

$$\begin{aligned} M \cap P &= \left(\bar{M}Z(P)\right) \cap \left(\bar{P}Z(P)\right) \\ &= \left(\bar{M} \cap \bar{P}\right)Z(P) \\ &= Z(P) \quad (\text{because } \bar{M} \cap \bar{P} = 1) \end{aligned}$$

and

$$\begin{aligned} MP &= \bar{M}Z(P)\bar{P}Z(P) \\ &= \bar{M}\bar{P}Z(P) \quad \left(Z(P)\bar{P} = \bar{P}Z(P)\right) \\ &= \bar{G}Z(P) \\ &= G \end{aligned}$$

Checking out M, we have $M < G$ and $Z(P)$ is a Sylow p-subgroup of M. Then there exists $K \leqslant M$ with $KZ(P) = M$ and $K \cap Z(P) = 1$. K is a complement to $Z(P)$ in M. So

$$\begin{aligned} K \cap P &= (K \cap M) \cap P \quad (K \leqslant M \Rightarrow K = K \cap M) \\ &= K \cap (M \cap P) \\ &= K \cap Z(P) \\ &= 1 \end{aligned}$$

and

$$\begin{aligned} KP &= KZ(P)P \quad \left(Z(P) \trianglelefteq P \Rightarrow P = Z(P)P\right) \\ &= MP \\ &= G \end{aligned}$$

Because $P = H$, $K \cap H = 1$ and $KH = G$. Then K is also a complement to H in G, which is a contradiction as well.

Then the assumption for the minimal criminal of the group-pair (G, H) is wrong, so there is always a complement to normal Hall subgroup H in G. $\square$

Theorem 5.4 *(**Schur-Zassenhaus Theorem** for General Case Part 2: Conjugation)*

Let H be a normal S_π-subgroup of G. If either H or G/H is solvable, then any two complements of H in G are conjugate.

Proof. See from Reference [5] on page 190-191, Theorem 7.42.

Assume that $|H| = m$ and $|G/H| = n$. H is a normal S_π-subgroup of G, so m and n are co-prime $\Big(\gcd(m,n) = 1\Big)$. Let K_1 and K_2 be any two complements of H in G, then

$$K_1 \cong G/H \cong K_2.$$

Also , $K_iH = G$ and $H \cap K_i = 1$ hold for $i = 1$ and 2. What need to be proved is that K_1 and K_2 are conjugate in G.

Assume that group G is the minimal criminal, then G is the smallest group which satisfies the following condition: there are two complements of a normal Hall subgroup H in G which cannot be conjugate to each other in group G. But any group G_1 smaller than G must follow the condition: any two complements of a normal Hall subgroup H in G_1 are conjugate to each other in G_1. It means that if two subgroups are in G_1 with

$$K_iH = G_1 \text{ and } H \cap K_i = 1, \text{ for } i = 1 \text{ and } 2,$$

then $K_1 = K_2^g$ for some element $g \in G_1$.

Case 1: Assume that H is solvable, then $H' \lhd H$. It is easy to show that $H' \lhd G$.

Step 1: If $H' = 1$, then H is abelian. As be proved before, K_1 and K_2 must be conjugate in G, which contradict to the minimal criminal G.

Step 2: If

$$1 \lhd H' \lhd H,$$

then

$$1 < |G/H'| < |G|.$$

So $K_iH' < G \ \ (i = 1 \text{ and } 2)$, then $K_iH'/H' < G/H' \ \ (i = 1 \text{ and } 2)$.

Moreover, from Second Isomorphism Theorem,

$$K_iH'/H' \cong K_i/(K_i \cap H') = K_i \ \ (i = 1 \text{ and } 2),$$

because

$$K_i \cap H' \leqslant K_i \cap H = 1.$$

Because $H \trianglelefteq G$, $H/H' \trianglelefteq G/H'$ is always true obviously. Then it is clear that K_1H'/H' and K_2H'/H' are two complements of H/H' in G/H'. By induction, K_1H'/H' and K_2H'/H' must be conjugate in G/H', so there is a element $g \in G$ such that

$$\bar{g}^{-1}(K_1H'/H')\bar{g} = K_2H'/H' \text{ with } \bar{g} = gH' \in G/H'.$$

Therefore

$$g^{-1}K_1gH' = K_2H'.$$

Since $H' \trianglelefteq G$, then $H' \trianglelefteq K_2H'$. So $g^{-1}K_1g$ and K_2 are two complements of H' in K_2H'. Again by induction, $g^{-1}K_1g$ and K_2 are conjugate in K_2H', hence obviously K_1 and K_2 are conjugate in G, which contradict to the minimal criminal G too.

Case 2: Assume that G/H is solvable, then there is a minimal normal subgroup $M/H(> H)$ of G/H. Moreover, M/H must be a p-group, because it is a minimal normal subgroup of a solvable group.

Step 1: If $H < M = G$, then G/H is a p-group. Because $K_1 \cong G/H \cong K_2$, then K_1 and K_2 are p-groups. Since $|G/H|$ and $|H|$ are co-prime, so G/H is a Sylow p-subgroup of G. Because $K_1 \cong G/H \cong K_2$, then K_1 and K_2 are also Sylow p-subgroups of G. Then K_1 and K_2 are conjugate in G, which also contradict to the minimal criminal.

Step 2: Finally, we assume that $M < G$. It is clear that

$$M \cap K_i \quad (i = 1 \text{ and } 2)$$

are complements of H in M, because :

(1) $(M \cap K_i)H = M \cap K_iH$ (Dedekind Law and $H < M$)
$= M \cap G$
$= M$;

and

(2) $(M \cap K_i) \cap H = M \cap (K_i \cap H) = M \cap 1$
$= 1$.

By induction, $M \cap K_1$ and $M \cap K_2$ are conjugate in M, so there is at least one element $x \in M$ satisfied that

$$\begin{aligned} M \cap K_2 &= (M \cap K_1)^x = M^x \cap K_1^x \\ &= M \cap K_1^x. \end{aligned}$$

Then let $K_3 = K_1^x$. It is obvious that K_3 is also a complement of H in G, because :
Assume that K is a complement of H in G (with $KH = G$ and $H \cap K = 1$), now we need to show that K^x ($\forall\ x \in G$) is also a complement of H in G;

(i) $H \cap K^x = H^x \cap K^x$ ($H \trianglelefteq G$, so $H = H^x$)
$= (H \cap K)^x$
$= 1^x$
$= 1$;

(ii) $K^xH = x^{-1}Kx H$
$= x^{-1}K(Hx)$ ($H \trianglelefteq G$, so $Hx = xH$)
$= (KH)^x$
$= G^x$
$= G$;

(iii) $|K^x| = |K|$, so $|K^x|$ and $|H|$ are co-prime.

Then K_3 holds all properties discussed above as the same as K_1. So

$$M \cap K_2 = M \cap K_3 = J.$$

Obviously $J \lhd K_i$ for $i = 2$ and 3. (Because if $J = K_i$ for i is 2 or 3, then $M = G$, which is wrong.) It follows that

$$K_i \leqslant N_G(J) \ \ (i = 2 \text{ and } 3).$$

Now look at $N_G(J)/J$. Because for $i = 2$ and 3,

$$\begin{aligned}
(K_i/J)(J(N_G(J) \cap H)/J) &= (K_i J(N_G(J) \cap H))/J \\
&= (K_i(N_G(J) \cap H))/J \quad (\text{because } J < K_i) \\
&= (N_G(J) \cap K_i H))/J \quad \Big(\text{Dedekind Law and} \\
&\qquad\qquad\qquad\qquad K_i \leqslant N_G(J)\Big) \\
&= (N_G(J) \cap G)/J \\
&= (N_G(J))/J \qquad\qquad \Big(N_G(J) \leqslant G\Big)
\end{aligned}$$

and

$$\begin{aligned}
(J(N_G(J) \cap H)/J) \cap (K_i/J) &= ((J(N_G(J) \cap H) \cap K_i)/J \\
&= J(N_G(J) \cap H \cap K_i)/J \quad \Big(\text{Dedekind Law} \\
&\qquad\qquad\qquad\qquad \text{and } J \leqslant N_G(J)\Big) \\
&= J/J \qquad\qquad\qquad\qquad (H \cap K_i = 1) \\
&= 1
\end{aligned}$$

Then K_2/J and K_3/J are complements of $J(N_G(J) \cap H)/J$ in $N_G(J)/J$.

By induction, K_2/J and K_3/J are conjugate in $N_G(J)/J$. Then there must be a element $\bar{y} = Jy$ in $N_G(J)/J$ $\Big(\text{with } y \in N_G(J) \subset G\Big)$ which satisfies

$$\begin{aligned}
K_2/J &= \bar{y}^{-1}(K_3/J)\bar{y} \\
&= (y^{-1}K_3 y)/J \\
&= K_1^{xy}/J.
\end{aligned}$$

It follows that $K_2 = K_1^{xy}$ and clearly $xy \in G$. Then apparently K_1 and K_2 are conjugate in G, which still contradict to the minimal criminal.

Then the assumption for the minimal criminal of the group G is wrong, so any two complements of a normal Hall subgroup H in G must be conjugate to each other. □

See from Reference [4] on page 255. Since at least one of $|G/H|$ and $|H|$ must be odd (from the definition of Hall subgroups), the Feit-Thompson Theorem implies that either G/H or H must be solvable for any group G. Then last theorem also can be expressed as:
Let H be a normal S_π-subgroup of G, then any two complements of H in G are conjugate.

5.3 S-Z Theorem Proved by Function Conjugation

Here is a new proof for Schur-Zassenhaus theorem (when G/H is solvable) by using conjugation of functions. This idea is from Reference [1].

Theorem 5.5 *(**Schur-Zassenhaus Theorem** for G/H solvable)*

Let H be a normal S_π-subgroup of G. If G/H is solvable, then:

(a). G possesses an $S_{\pi'}$-subgroup K which is a complement to H in G;

(b). any two complements of H in G are conjugate.

Proof. Let $|H| = n$ and $|G/H| = m$, then definitely $\gcd(m, n) = 1$ from the definition of Hall subgroup.

Because H is a normal subgroup of group G, then there is a natural homomorphism π from G to the quotient group G/H with $\pi(g) = gH$ ($\forall\ g \in G$).

Let $\bar{G} = G/H$, then consider the set of functions

$$\zeta := \{f : \bar{G} \to G, \text{ transversal functions with } \pi\Big(f(\bar{g})\Big) = \bar{g},\ \forall\ \bar{g} \in \bar{G},$$
$$\text{which are identity preserving}\}.$$

Clearly $f(\bar{1}) = 1$ ($\forall\ f \in \zeta$) and $|\zeta| = |H|^{|\overline{G}|-1} = n^{m-1}$.

If $\bar{K}$ is a subgroup of $\bar{G}$ ($\bar{K} \leqslant \bar{G}$), then define the function set for this subgroup as

$$\zeta_{\overline{K}} := \{f \in \zeta : f^{\bar{k}} = f, \forall\ \bar{k} \in \overline{K}\}.$$

Now we need to choose some subgroups $\overline{K}$ with the following properties:

(1). $\bar{K} \trianglelefteq \trianglelefteq \overline{G}$;

(2). $\zeta_{\overline{K}} \neq \varnothing$;

(3). $\forall\ f$ and $g \in \zeta_{\overline{K}}$, then $\exists\ h \in H$ such that $g(\bar{k}) = f(\bar{k})^h$ for all $\bar{k}$ in $\overline{K}$.

Note that for any solvable group $\overline{G}$ there must be at least one subgroup $\overline{K}$ satisfying above properties, because $\bar{1}$ always has these properties.

$$(\bar{1} \trianglelefteq \overline{G};$$
$$\forall\ f \in \zeta, f^{\bar{1}} = f \Rightarrow \zeta_{\bar{1}} = \zeta \neq \varnothing;$$
$$f(\bar{1}) = 1 = g(\bar{1})^h, \forall\ h \in H \text{ and } \forall\ f \text{ and } g \in \zeta.)$$

Then we can suppose that $\overline{K}$ is a maximal subgroup of this type.

If $\overline{G}$ has these properties (as $\overline{K} = \overline{G}$), then it is finished here. Otherwise we assume that $\overline{K} \lneqq \overline{G}$. Since $\overline{G}$ is solvable, then there is a subgroup $\overline{M}$ of $\overline{G}$ satisfying that $\overline{K} \lhd \overline{M} \trianglelefteq \lhd \overline{G}$ and the order of composition factor $\overline{M}/\overline{K}$ is a prime p (clearly $p \Big| m$ and $\gcd(p, n) = 1$).

Let $\overline{P} \in \mathrm{Syl}_p(\overline{M})$, then $\overline{M} = \overline{P}\ \overline{K}$. And $\overline{P} \nsubseteq \overline{K}$.

Look at the action of $\overline{P}$ on $\zeta_{\overline{K}}$.

$$\forall\ f \in \zeta_{\overline{K}} \text{ and } \forall\ \bar{a} \in \overline{P},\ \bar{a} : f \mapsto f^{\bar{a}^{-1}} = f^{\bar{b}} \text{ with } \bar{b} = \bar{a}^{-1}.$$

It is easy to show that $\overline{P}$ partition $\zeta_{\overline{K}}$:

$$\begin{aligned} \forall\ \bar{a} \in \overline{P} \text{ and } \forall\ \bar{k} \in \overline{K},\ (f^{\bar{a}})^{\bar{k}} &= f^{\bar{a}\bar{k}} \\ &= f^{\bar{k}'\bar{a}} \\ &\quad (\overline{K} \lhd \overline{M} \Rightarrow \bar{a}\bar{k} = \bar{k}'\bar{a},\ \text{for some } \bar{k}' \in \overline{K}) \\ &= (f^{\bar{k}'})^{\bar{a}} \\ &= f^{\bar{a}}. \end{aligned}$$

Then we have

$$\sum_{f \in \zeta_{\overline{K}}} |\mathrm{Orb}_{\overline{P}}(f)| = |\zeta_{\overline{K}}|.$$

And $|\mathrm{Orb}_{\overline{P}}(f)|$ is either a power of p or 1.

Assume that there are q functions in $\zeta_{\overline{K}}$ with orbit-size 1 (maybe $q = 0$). Then from last formula we have $|\zeta_{\overline{K}}| = q + rp$ (r is a integer). But also

$|\zeta_{\overline{K}}| = \#$ of homomorphisms from $\overline{K}$ to G in ζ)(# of functions from $\overline{G}\backslash\overline{K}$ to G in ζ)

$= AB$.

From property (3), A (# of homomorphisms from $\overline{K}$ to G in ζ) is a factor of n, because they are all conjugate in H. And

B (# of functions from $\overline{G}\backslash\overline{K}$ to G in ζ) $= |H|^{|\overline{G}|-|\overline{K}|} = n^{m-|\overline{K}|}$.

Apparently both of them should be prime to p, so $|\zeta_{\overline{K}}|$ should not be a multiple of p.

Then $q \neq 0$, otherwise $|\zeta_{\overline{K}}| = rp$, which is a contradiction. So there must be at least one function which has orbit-size 1, naming it function f. Then $\forall\ \bar{a} \in \overline{P}, f^{\bar{a}} = f$.

$$\begin{aligned}
\therefore \forall\ \bar{m} \in \overline{M}, f^{\bar{m}} &= f^{\bar{a}\bar{k}} \quad (\overline{M} = \overline{P}\ \overline{K} \Rightarrow \exists\ \bar{a} \in \overline{P} \text{ and } \exists\ \bar{k} \in \overline{K} \text{ s.t. } \bar{m} = \bar{a}\bar{k}) \\
&= (f^{\bar{a}})^{\bar{k}} \\
&= f^{\bar{a}} \\
&= f
\end{aligned}$$

$\Rightarrow f \in \zeta_{\overline{M}}$

$\Rightarrow \zeta_{\overline{M}} \neq \varnothing$.

Now we just need to show that $\forall\ f$ and $g \in \zeta_{\overline{M}}, \exists\ h \in H$ such that $g(\bar{m}) = f(\bar{m})^h$.

Firstly $\forall\ f \in \zeta_{\overline{M}}$ and $\forall\ h \in H$, let $F(\bar{x}) = f(\bar{x})^h,\ \forall\ \bar{x} \in \overline{G}$

$$\begin{aligned}
\Rightarrow \forall\ \bar{m} \in \overline{M},\quad F^{\bar{m}}(\bar{x}) = F(\bar{m})^{-1}F(\bar{m}\bar{x}) &\quad = (f(\bar{m})^h)^{-1}f(\bar{m}\bar{x})^h \\
= (f(\bar{m})^{-1}f(\bar{m}\bar{x}))^h &\quad = (f^{\bar{m}}(\bar{x}))^h \\
= f(\bar{x})^h &\quad = F(\bar{x})
\end{aligned}$$

$\Rightarrow F \in \zeta_{\overline{M}}$.

$$\begin{aligned}
\text{Then } \forall\ f \text{ and } g \in \zeta_{\overline{M}} &\Rightarrow f \text{ and } g \in \zeta_{\overline{K}} \\
&\Rightarrow \exists\ h \in H \text{ s.t. } g(\bar{k}) = f(\bar{k})^h\ \ \forall\ \bar{k} \in \overline{K}. \\
\text{If } F(\bar{x}) = f(\bar{x})^h,\ \forall\ \bar{x} \in \overline{G} &\Rightarrow g(\bar{k}) = F(\bar{k})\ \ \forall\ \bar{k} \in \overline{K} \\
&\Rightarrow g(\overline{K}) = F(\overline{K}) = K \text{ and } F(\overline{M}) = f(\overline{M})^h
\end{aligned}$$

Assume that $F(\overline{P}) = P, g(\overline{P}) = P'$ and $F(\overline{M}) = M, g(\overline{M}) = M'$. Because F and g are two homomorphisms in $\overline{M}$, then $M = PK, M' = P'K$ and $P \in \mathrm{Syl}_p(M), P' \in \mathrm{Syl}_p(M')$.

$$\begin{aligned}
\forall\ \bar{a} \in \overline{P},\quad \pi\Big(F(\bar{a})^{-1}g(\bar{a})\Big) &= \pi\Big(F(\bar{a})\Big)^{-1}\ \pi\Big(g(\bar{a})\Big) \\
&= \bar{a}^{-1}\bar{a} \\
&= \bar{1}
\end{aligned}$$

$\Rightarrow F(\bar{a})^{-1}g(\bar{a}) \in H$

$\overline{K} \lhd \overline{M} \Rightarrow K \lhd M$ and $K \lhd M'$

$$\Rightarrow M \leqslant N_G(K) \text{ and } M' \leqslant N_G(K)$$
$$\Rightarrow F(\bar{a})^{-1} g(\bar{a}) \in N_G(K)$$
$$\Rightarrow F(\bar{a})^{-1} g(\bar{a}) \in N_H(K)$$

Let $L = N_H(K)$ $\Rightarrow g(\bar{a}) \in F(\bar{a})L$
$\Rightarrow P' \subseteq PL$
$\Rightarrow P' \in \mathrm{Syl}_p(PL)$ and $P \in \mathrm{Syl}_p(PL)$ (because $|L| \Big| |H|$)
$\Rightarrow \exists\ h' \in L \leqslant H$ such that $P' = P^{h'}$

Also $h' \in L = N_H(K) \Rightarrow K^{h'} = K$
$\Rightarrow M' = M^{h'}$
$\Rightarrow h_0 = hh' \in H$ s.t. $g(\overline{M}) = f(\overline{M})^{h_0}$
$\Rightarrow \forall\ \bar{m} \in \overline{M}, \exists\ \bar{m'} \in \overline{M}$ s.t. $g(\bar{m}) = f(\bar{m'})^{h_0}$

$$\pi\Big(g(\bar{m})\Big) = \pi\Big(f(\bar{m'})^{h_0}\Big)$$
$$\Rightarrow\ \bar{m} = \pi(h_0)^{-1}\pi(f(\bar{m'}))\pi(h_0)$$
$$= \bar{1}^{-1}\bar{m'}\bar{1}$$
$$= \bar{m'}$$
$$\Rightarrow \forall\ \bar{m} \in \overline{M}, g(\bar{m}) = f(\bar{m})^{h_0}.$$

Then $\zeta_{\overline{M}}$ holds all three properties which are discussed before, and $\overline{M}$ is bigger than the maximal $\overline{K}$ assumed above. Hence it is a contradiction. So $\zeta_{\overline{G}}$ must satisfy all these properties. Then it is obviously true for both existence and uniqueness under conjugation. $\square$

5.4 S-Z Theorem Proved by Distributors

Here is another way to look at the proof for Schur-Zassenhaus theorem (abelian case) by using distributors, from Reference [1] and [2].

Theorem 5.6 *(**Schur-Zassenhaus Theorem** for Abelian Case Part 1: Existence)*

Let H be an abelian normal S_π-subgroup of a finite group G, then G possesses an $S_{\pi'}$-subgroup K which is a complement to H in G.

Proof. Because H is a normal subgroup of group G, then there is a natural homomorphism π from G to the quotient group G/H with $\pi(g) = gH, \forall\, g \in G$.

Let $\overline{G} = G/H$, then consider the set of functions

$\zeta := \{f : \bar{G} \to G$, transversal functions with $\pi \circ f(\bar{x}) = \bar{x},\ \forall\ \bar{x} \in \bar{G}$,
which are identity preserving$\}$.

So we have following properties:

(1). $\forall f \in \zeta$, $\forall\ \bar{a}$ and $\bar{x} \in \overline{G}$,

$$\begin{aligned}
\pi \circ f^{\bar{a}}(\bar{x}) &= \pi\Big(f(\bar{a})^{-1} f(\bar{a}\bar{x})\Big) \\
&= \Big(\pi \circ f(\bar{a})\Big)^{-1}\Big(\pi \circ f(\bar{a}\bar{x})\Big) \text{ (because } \pi \text{ is a homomorphism)} \\
&= \bar{a}^{-1}(\bar{a}\bar{x}) \\
&= \bar{x}.
\end{aligned}$$

So $f^{\bar{a}} \in \zeta$ too.

(2). $\forall f \in \zeta$, $\forall\ \bar{a}$ and $\bar{x} \in \overline{G}$,

$$\begin{aligned}
\pi[\bar{a}, \bar{x}]_f &= \pi\Big(f(\bar{x})^{-1} f(\bar{a})^{-1} f(\bar{a}\bar{x})\Big) \\
&= \Big(\pi \circ f(\bar{x})\Big)^{-1}\Big(\pi \circ f(\bar{a})\Big)^{-1}\Big(\pi \circ f(\bar{a}\bar{x})\Big) \\
&= \bar{x}^{-1}\bar{a}^{-1}(\bar{a}\bar{x}) \\
&= \bar{x}^{-1}\bar{1}\bar{x} \\
&= \bar{x}^{-1}\bar{x} \\
&= \bar{1}.
\end{aligned}$$

So $[\bar{a}, \bar{x}]_f \in H$.

It is clear that any f-distributor of group $\overline{G}$ belong to the abelian group H. So $[\bar{a}, \bar{x}]_f[\bar{b}, \bar{y}]_f = [\bar{b}, \bar{y}]_f[\bar{a}, \bar{x}]_f$ $(\forall\ \bar{a}, \bar{b}, \bar{x}, \bar{y} \in \overline{G})$, and it is true for anyone in $\overline{G}$. It means that the order does not matter for a product of f-distributors in this particular case.

(3). Let $|H| = n$ and $|\overline{G}| = m$ $(m, n \in \mathbf{Z}^+)$, then it is clear that $\gcd(m, n) = 1$ and $|G| = mn$. So there exist some positive integers k and l such that $km - ln = 1$. Then $\forall a \in H$,

$$\begin{aligned} a^{km} &= a^{1+ln} \\ &= a^1 a^{ln} \\ &= a(a^n)^l \\ &= a(1^l) \quad (a \in H \text{ and } |H| = n \Rightarrow a^n = 1) \\ &= a. \end{aligned}$$

Next we will name the set $k\overline{G} = \underbrace{\overline{G} + \overline{G} + \cdots + \overline{G}}_{k}$ (k is the same positive integer as mentioned above), and it can be thought as going through the quotient group $\overline{G}$ k-times. Then $|k\overline{G}| = km$.

Now look at the function

$$\bar{\bar{f}}(\bar{x}) := f(\bar{x}) \prod_{\bar{a} \in k\overline{G}} [\bar{a}, \bar{x}]_f \ , \forall\ f \in \zeta.$$

If

$$F(\bar{x}) = \prod_{\bar{a} \in k\overline{G}} [\bar{a}, \bar{x}]_f \ ,$$

then

$$\bar{\bar{f}} = f * F$$

and F is a function from $\overline{G}$ to abelian group H.

Firstly, from (2) we know that $\pi[\bar{a},\bar{x}]_f = \bar{1}$. Then

$$\begin{aligned}
\pi \circ \bar{\bar{f}}(\bar{x}) &= \pi\left(f(\bar{x}) \prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{x}]_f\right) \\
&= \pi \circ f(\bar{x}) \left(\prod_{\bar{a}\in k\overline{G}} \pi[\bar{a},\bar{x}]_f\right) \\
&= \pi \circ f(\bar{x}) \prod_{\bar{a}\in k\overline{G}} \bar{1} \\
&= \pi \circ f(\bar{x}) \\
&= \bar{x}.
\end{aligned}$$

So $\bar{\bar{f}} \in \zeta$.

Secondly, look at $\left(\bar{\bar{f}}\right)^{\bar{b}}(\bar{x}), \forall\ \bar{b} \in \overline{G}$. From (1), $\left(\bar{\bar{f}}\right)^{\bar{b}} \in \zeta$ is always true. Then we will show that $\bar{\bar{f}}$ is a homomorphism by expanding the conjugation of function. So

$$\begin{aligned}
\left(\bar{\bar{f}}\right)^{\bar{b}}(\bar{x}) &= (f * F)^{\bar{b}}(\bar{x}) \\
&= \left(f^{\bar{b}}(\bar{x})\right)^{F(\bar{b})} F^{\bar{b}}(\bar{x}) \\
&= F(\bar{b})^{-1} f^{\bar{b}}(\bar{x}) F(\bar{b}) F(\bar{b})^{-1} F(\bar{b}\bar{x}) \\
&= F(\bar{b})^{-1} f^{\bar{b}}(\bar{x}) F(\bar{b}\bar{x}).
\end{aligned}$$

Alternatively, we can also argue this as follows:

$$\begin{aligned}
\left(\bar{\bar{f}}\right)^{\bar{b}}(\bar{x}) &= \bar{\bar{f}}(\bar{b})^{-1} \bar{\bar{f}}(\bar{b}\bar{x}) \\
&= \left(f(\bar{b}) \prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}]_f\right)^{-1} \left(f(\bar{b}\bar{x}) \prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}\bar{x}]_f\right) \\
&= \left(\prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}]_f\right)^{-1} f(\bar{b})^{-1} f(\bar{b}\bar{x}) \prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}\bar{x}]_f \\
&= \left(\prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}]_f\right)^{-1} f(\bar{x}) f(\bar{x})^{-1} f(\bar{b})^{-1} f(\bar{b}\bar{x}) \prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}\bar{x}]_f \\
&= \left(\prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}]_f\right)^{-1} f(\bar{x}) [\bar{b},\bar{x}]_f \prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}\bar{x}]_f\ .
\end{aligned}$$

From the identity of distributors $[a,b]_f^{f(x)} = [b,x]_f[a,bx]_f[ab,x]_f^{-1}$, we get $[a,bx]_f = [b,x]_f^{-1}[a,b]_f^{f(x)}[ab,x]_f$. From (2) and (3),

$$\begin{aligned}
F(\bar{b}\bar{x}) &= \prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}\bar{x}]_f \\
&= \prod_{\bar{a}\in k\overline{G}} \left([\bar{b},\bar{x}]_f^{-1}[\bar{a},\bar{b}]_f^{f(\bar{x})}[\bar{a}\bar{b},\bar{x}]_f \right) \\
&= \left(\prod_{\bar{a}\in k\overline{G}} [\bar{b},\bar{x}]_f^{-1} \right) \left(\prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}]_f^{f(x)} \right) \prod_{\bar{a}\in k\overline{G}} [\bar{a}\bar{b},\bar{x}]_f \\
&= \left(\prod_{\bar{a}\in k\overline{G}} [\bar{b},\bar{x}]_f \right)^{-1} \left(\prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}]_f \right)^{f(\bar{x})} \prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{x}]_f \\
&= [\bar{b},\bar{x}]_f^{-1} f(\bar{x})^{-1} \left(\prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}] \right) f(\bar{x})F(\bar{x}) \\
&= [\bar{b},\bar{x}]_f^{-1} f(\bar{x})^{-1} F(\bar{b}) f(\bar{x})F(\bar{x}).
\end{aligned}$$

So

$$\begin{aligned}
\left(\bar{\bar{f}}\right)^{\bar{b}}(\bar{x}) &= F(\bar{b})^{-1} f^{\bar{b}}(\bar{x})[\bar{b},\bar{x}]_f^{-1} f(\bar{x})^{-1} F(\bar{b}) f(\bar{x})F(\bar{x}) \\
&= F(\bar{b})^{-1} f(\bar{x})[\bar{b},\bar{x}]_f[\bar{b},\bar{x}]_f^{-1} f(\bar{x})^{-1} F(\bar{b}) f(\bar{x})F(\bar{x}) \\
&= F(\bar{b})^{-1} f(\bar{x}) f(\bar{x})^{-1} F(\bar{b}) f(\bar{x})F(\bar{x}) \\
&= F(\bar{b})^{-1} F(\bar{b}) f(\bar{x})F(\bar{x}) \\
&= f(\bar{x})F(\bar{x}) \\
&= \bar{\bar{f}}(\bar{x}).
\end{aligned}$$

Or we can get this by using distributors:

$$\begin{aligned}
\left(\bar{\bar{f}}\right)^{\bar{b}}(\bar{x}) &= \left(\prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}]_f \right)^{-1} f(\bar{x})[\bar{b},\bar{x}]_f[\bar{b},\bar{x}]_f^{-1} \left(\prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{b}]_f \right)^{f(\bar{x})} \prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{x}]_f \\
&= f(\bar{x}) \prod_{\bar{a}\in k\overline{G}} [\bar{a},\bar{x}]_f \\
&= \bar{\bar{f}}(\bar{x}).
\end{aligned}$$

So, we proof that $\bar{\bar{f}}$ is a homomorphism from $\overline{G}$ to G and so $\mathrm{Im}(\bar{\bar{f}}) \leqslant G$.

Finally, we need to show that $\mathrm{Im}(\bar{\bar{f}})$ is a complement of H. In other words, we must prove: (i). $\mathrm{Im}(\bar{\bar{f}})H = G$; (ii). $\mathrm{Im}(\bar{\bar{f}}) \cap H = 1$.

(i). $\forall\ x \in G$, $\pi(x) = xH = \bar{x} \in \overline{G}$. So

$$\bar{\bar{f}}\Big(\pi(x)\Big) = \bar{\bar{f}}(\bar{x}) = a \in \mathrm{Im}(\bar{\bar{f}}).$$

Therefore

$$\begin{aligned} xH = \bar{x} \quad &= \pi\Big(\bar{\bar{f}}(\bar{x})\Big) \\ &= \pi(a) = \bar{a} \\ &= aH \\ \Rightarrow xh_1 &= ah_2, \exists\ h_1 \text{ and } h_2 \in H \\ \Rightarrow \quad x &= ah_2h_1^{-1}. \end{aligned}$$

Then $G \subseteq \mathrm{Im}(\bar{\bar{f}})H$. Hence it is obvious $\mathrm{Im}(\bar{\bar{f}})H \subseteq G$, then $G = \mathrm{Im}(\bar{\bar{f}})H$.

(ii). $\forall\ x \in \mathrm{Im}(\bar{\bar{f}}) \cap H$. Because $x \in H$, then

$$\begin{aligned} \pi(x) \ &= \ \bar{x} \ = xH \\ &= \ H = \bar{1}. \end{aligned}$$

And $x \in \mathrm{Im}(\bar{\bar{f}})$, so there exists a element $\bar{a} \in \overline{G}$ such that $x = \bar{\bar{f}}(\bar{a})$.

Then

$$\begin{aligned} \bar{a} \ &= \ \pi\Big(\bar{\bar{f}}(\bar{a})\Big) = \pi(x) \\ &= \ \bar{1}. \end{aligned}$$

So from $\bar{\bar{f}}$ is a homomorphism, we have

$$\begin{aligned} x \ &= \ \bar{\bar{f}}(\bar{a}) = \bar{\bar{f}}(\bar{1}) \\ &= \ 1. \end{aligned}$$

$$\therefore\ \mathrm{Im}(\bar{\bar{f}}) \cap H = 1.$$

So any abelian normal S_π-subgroup in G must have at least one complement in G. $\square$

Theorem 5.7 *(**Schur-Zassenhaus Theorem** for Abelian Case Part 2: Conjugation)*

If H is an abelian normal S_π-subgroup of a finite group G, then any two complements to H in G are conjugate.

Proof. Assume that $|H| = m$ and $|G/H| = n$. H is a normal S_π-subgroup of G, so m and n are co-prime ($\gcd(m, n) = 1$). Let K_1 and K_2 be any two complements of H in G, then $K_1 \cong G/H \cong K_2$. Also , $K_iH = G$ and $H \cap K_i = 1$ hold for $i = 1, 2$.

Then there are two homomorphisms $\bar{\bar{f}}_1$ and $\bar{\bar{f}}_2$ in ζ which satisfy that:

$$K_1 = \mathrm{Im}(\bar{\bar{f}}_1) \leqslant \langle \mathrm{Im}(f_1) \rangle \leqslant G = K_1H;$$

$$K_2 = \mathrm{Im}(\bar{\bar{f}}_2) \leqslant \langle \mathrm{Im}(f_2) \rangle \leqslant G = K_1H = \langle \mathrm{Im}(f_1) \rangle H.$$

What we need to do is to show that every two homomorphisms from function set ζ must be conjugate to each other.

Let $h(\bar{x}) = f_1(\bar{x})^{-1} f_2(\bar{x}), \forall\ \bar{x} \in \overline{G}$. Then

$$\begin{aligned} \pi\Big(h(\bar{x})\Big) &= \pi\Big(f_1(\bar{x})^{-1} f_2(\bar{x})\Big) \\ &= \pi\Big(f_1(\bar{x})\Big)^{-1}\ \pi\Big(f_2(\bar{x})\Big) \\ &= \bar{x}^{-1}\bar{x} \\ &= \bar{1}, \end{aligned}$$

$$\Rightarrow h(\bar{x}) \in H, \forall\ \bar{x} \in \overline{G}.$$

Then h is a function from $\overline{G}$ to H. So

$$\begin{aligned} h(\bar{x}) &= f_1(\bar{x})^{-1} f_2(\bar{x}) \\ \Rightarrow f_2(\bar{x}) &= f_1(\bar{x}) h(\bar{x}) \\ &= f_1 * h(\bar{x}). \end{aligned}$$

Then we can get the formula:

$$\begin{aligned}
[\bar{a},\bar{x}]_{f_2} &= [\bar{a},\bar{x}]_{f_1*h} \\
&= h(\bar{x})^{-1}f_1(\bar{x})^{-1}h(\bar{a})^{-1}f_1(\bar{x})[\bar{a},\bar{x}]_{f_1}h(\bar{a})h(\bar{x})[\bar{a},\bar{x}]_h \\
&= \underbrace{h(\bar{x})^{-1}}_{\in H}\underbrace{\Big(h(\bar{a})^{-1}\Big)^{f_1(\bar{x})}}_{\in H}\underbrace{[\bar{a},\bar{x}]_{f_1}}_{\in H}\underbrace{h(\bar{a})}_{\in H}\underbrace{h(\bar{x})}_{\in H}\underbrace{[\bar{a},\bar{x}]_h}_{\in H} \\
&= h(\bar{x})^{-1}h(\bar{x})\Big(h(\bar{a})^{-1}\Big)^{f_1(\bar{x})}h(\bar{a})[\bar{a},\bar{x}]_{f_1}[\bar{a},\bar{x}]_h \\
&= \Big(h(\bar{a})^{-1}\Big)^{f_1(\bar{x})}h(\bar{a})[\bar{a},\bar{x}]_{f_1}[\bar{a},\bar{x}]_h \\
&= \Big[f_1(\bar{x}),h(\bar{a})\Big][\bar{a},\bar{x}]_{f_1}[\bar{a},\bar{x}]_h\ .
\end{aligned}$$

Then

$$\begin{aligned}
\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_{f_2} &= \prod_{\bar{a}\in k\overline{G}}\Big(\Big[f_1(\bar{x}),h(\bar{a})\Big][a,x]_{f_1}[a,x]_h\Big) \\
&= \prod_{\bar{a}\in k\overline{G}}\Big[f_1(\bar{x}),h(\bar{a})\Big]\prod_{\bar{a}\in k\overline{G}}[a,x]_{f_1}\prod_{\bar{a}\in k\overline{G}}[a,x]_h \\
&= \left(\prod_{\bar{a}\in k\overline{G}}\Big(h(\bar{a})^{-1}\Big)^{f_1(\bar{x})}h(\bar{a})\right)\prod_{\bar{a}\in k\overline{G}}[a,x]_{f_1}\prod_{\bar{a}\in k\overline{G}}[a,x]_h \\
&= \left(\prod_{\bar{a}\in k\overline{G}}\Big(h(\bar{a})^{-1}\Big)^{f_1(\bar{x})}\right)\prod_{\bar{a}\in k\overline{G}}h(\bar{a})\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_{f_1}\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_h \\
&= \left(\prod_{\bar{a}\in k\overline{G}}h(\bar{a})^{-1}\right)^{f_1(\bar{x})}\prod_{\bar{a}\in k\overline{G}}h(\bar{a})\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_{f_1}\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_h \\
&= f_1(\bar{x})^{-1}\left(\prod_{\bar{a}\in k\overline{G}}h(\bar{a})^{-1}\right)f_1(\bar{x})\prod_{\bar{a}\in k\overline{G}}h(\bar{a})\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_{f_1}\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_h \\
&= f_1(\bar{x})^{-1}\left(\prod_{\bar{a}\in k\overline{G}}h(\bar{a})\right)^{-1}f_1(\bar{x})\prod_{\bar{a}\in k\overline{G}}h(\bar{a})\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_{f_1}\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_h \\
&= \left[f_1(\bar{x}),\prod_{\bar{a}\in k\overline{G}}h(\bar{a})\right]\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_{f_1}\prod_{\bar{a}\in k\overline{G}}[\bar{a},\bar{x}]_h.
\end{aligned}$$

Let

$$u=\prod_{\bar{a}\in k\overline{G}}h(\bar{a})\in H.$$

Then we have the formula as

$$F_2(\bar{x})=\Big[f_1(\bar{x}),u\Big]F_1(\bar{x})H(\bar{x}).$$

So

$$\begin{aligned}
\bar{\bar{f}}_2(\bar{x}) &= f_2(\bar{x})F_2(\bar{x}) \\
&= f_1 * h(\bar{x}) \left[f_1(\bar{x}), u\right] F_1(\bar{x})H(\bar{x}) \\
&= f_1(\bar{x}) \underbrace{h(\bar{x})}_{\in H} \underbrace{f_1(\bar{x})^{-1}u^{-1}f_1(\bar{x})}_{\in H} \underbrace{u}_{\in H} \underbrace{F_1(\bar{x})}_{\in H} \underbrace{H(\bar{x})}_{\in H} \\
&= f_1(\bar{x})f_1(\bar{x})^{-1}u^{-1}f_1(\bar{x})F_1(\bar{x})h(\bar{x})H(\bar{x})u \\
&= u^{-1}\bar{\bar{f}}_1(\bar{x})\bar{\bar{h}}(\bar{x})u \\
&= \left(\bar{\bar{f}}_1 * \bar{\bar{h}}(\bar{x})\right)^u
\end{aligned}$$

From the discussion above, we know that $\bar{\bar{h}}$ is a homomorphism from G/H to H. So $|\langle \mathrm{Im}(\bar{\bar{h}})\rangle| \Big| |G/H|$ and $|\langle \mathrm{Im}(\bar{\bar{h}})\rangle| \Big| |H|$. Because $\gcd(|G/H|, |H|) = 1$, then $|\langle \mathrm{Im}(\bar{\bar{h}})\rangle| = 1$. So apparently $\bar{\bar{h}}$ is the trivial homomorphism. Then $\bar{\bar{h}}(\bar{x}) = 1, \forall\ \bar{x} \in \overline{G}$.

So

$$\bar{\bar{f}}_2(\bar{x}) = u^{-1}\bar{\bar{f}}_1(\bar{x})u, \forall\ \bar{x} \in \overline{G}.$$

Then it shows that $K_2 = K_1^u$.

So any two complements of a abelian normal Hall subgroup H in G must be conjugate to each other. □

Similarly as the old proofs, we can prove the case of H solvable by induction.

Chapter 6

Conclusion

In the previous chapters, we found that "f-distributor" and "the conjugation of functions" as two measures of how close an arbitrary function between groups is to being a homomorphism. We use them to prove some well-known theorems in group theory, in several different methods.

Method 1. Consider the set of all identity preserving functions between certain groups. Let a group act on this function set by using function conjugation. Then an non-trivial function which has orbit-size 1, must be a homomorphism. (e.g. Theorem 3.16 on P.30 and Theorem 5.5 on P.59)

Method 2. Consider these orbits from above, then we can establish a homomorphism by averaging them. (e.g. Theorem 4.9 on P.39)

Method 3. When the image of the function is abelian, we can also construct a homomorphism by averaging all these distributors. (e.g. Theorem 5.6 on P.63)

Then it provides a possible way to look at some properties in group theory differently, which may lead to some interesting results.

Bibliography

[1] Ian Hawthorn, Unpublished manuscript.

[2] Ian Hawthorn and Yue Guo, *Arbitrary Functions in Group Theory*. Submitted to NZJM.

[3] Daniel Gorenstein, *Finite Group*. Chelsea, New York, 2nd Edition, 1980.

[4] Derek J.S. Robinson, *A Course in the Theory of Groups*. Springer-Verlag, New York, 2nd Edition, 1995.

[5] Joseph J. Rotman, *An Introduction to the Theory of Groups*. Springer-Verlag, New York, 4th Edition, 1995.