First Isomorphism Theorem

Let $f : G \to H$ be a group homomorphism. The

- $K = \ker(f) := g \in G | f(g) = 1_H$ is a normal subgroup of G,
- $\mathrm{Im}(f)$ is a subgroup of H, and
- G/K is isomorphic to $\mathrm{Im}(f)$.

In fact, the isomorphism is given by

$$\bar{f} : G/K \to \mathrm{Im}(f), \quad \bar{f}(\bar{g}) = \bar{f}(gK) = f(g)$$

$\bar{f}$ is well defined

Let $\bar{g}_1, \bar{g}_2 \in G/K$, the statement is true iff

$$\forall \bar{g}_1, \bar{g}_2 \in G/K, \quad \bar{g}_1 = \bar{g}_2 \to \bar{f}(\bar{g}_1) = \bar{f}(\bar{g}_2)$$

The proof is given by

$$\begin{aligned} &\bar{g}_1 = \bar{g}_2 \implies g_1K = g_2K \implies g_1^{-1}g_2 \in K \\ \implies &f(g_1^{-1}g_2) = 1_H \implies f(g_1^{-1})f(g_2) = 1_H \\ \implies &f(g_1) = f(g_2) \end{aligned}$$

K is a subgroup of G

Identity

Since f is a homomorphism, $f(1_G) = 1_H$, therefore $1_G \in \ker(f)$

Inverse

To prove: $\forall k \in K, \ k^{-1} \in K$
Let $k \in K$, $f(kk^{-1}) = f(1_G) = 1_H = f(k)f(k^{-1}) = 1_H f(k^{-1})$
As $1_H = 1_H f(k^{-1})$,$f(k^{-1}) = 1_H$

Operation

To prove: $\forall k_1, k_2 \in K, \ k_1k_2 \in K$
Given any such k_1, k_2, since f is an isomorphism, we have

$$\begin{aligned} &f(k_1k_2) \\ =&f(k_1)f(k_2) \\ =&1_H1_H \\ =&1_H \end{aligned}$$

Therefore $k_1k_2 \in K$.

K is normal

By definition, K is a normal subgroup of G iff

$$\forall k \in K, g \in G, \quad gkg^{-1} \in K$$

Given any k, g, since f is an isomorphism, we have

$$\begin{aligned}
&f(gkg^{-1}) \\
=&f(g)f(k)f(g^{-1}) \\
=&f(k)
\end{aligned}$$

Therefore $gkg^{-1} \in K$.

$\mathrm{Im}(f)$ is a subgroup of H

Identity

Since G is a group, it has identity. Since f is a homomorphism, $f(1_G) = 1_H$. Therefore $1_H \in \mathrm{Im}(f)$

Inverse

To prove: $\forall h \in \mathrm{Im}(f), h^{-1} \in \mathrm{Im}(f)$
Let $h \in \mathrm{Im}(f)$, then $\exists g \in G$ s.t. $f(g) = h$ and because f is a homomorphism, $f(g^{-1}) = h^{-1}$

Operation

To prove: $\forall h_1, h_2 \in \mathrm{Im}(f),\ h_1h_2 \in \mathrm{Im}(f)$
Let $h_1 = f(g_1)$ and $h_2 = f(g_2)$, since f is an isomorphism,

$$h_1h_2 = f(g_1)f(g_2) = f(g_1g_2)$$

As shown above, there $\exists$ something $\in G$ that maps to h_1h_2 by f.

$\bar{f}$ is an homomorphism

What we need to prove to prove the statement is

$$\forall \bar{g}_1, \bar{g}_2 \in G/K, \quad \bar{f}(\bar{g}_1\bar{g}_2) = \bar{f}(\bar{g}_1)\bar{f}(\bar{g}_2)$$

The proof is given by

$$\begin{aligned}
&\bar{f}(\bar{g}_1\bar{g}_2) \\
=&\bar{f}((g_1K)(g_2K)) \\
=&\bar{f}((g_1g_2K)) \\
=&f(g_1g_2) \\
=&f(g_1)f(g) \\
=&\bar{f}(\bar{g}_1)\bar{f}(\bar{g}_2)
\end{aligned}$$

$\bar{f}$ is surjective

$\text{Im}(\bar{f}) = \{\bar{f}(\bar{g})|\bar{g} \in G/K\} = \{\bar{f}(gK)|g \in G\} = \{f(g)|g \in G\} = \text{Im}(f)$
If $h \in \text{Im}(f)$ then $h \in \text{Im}(\bar{f})$.

$\bar{f}$ is injective

Let $\bar{g}_1, \bar{g}_2 \in G/K$, the proof is given by

$$\begin{aligned}
&\bar{f}(\bar{g}_1) = \bar{f}(\bar{g}_2) \\
\Longrightarrow\ &\bar{f}(\bar{g}_1^{-1})\bar{f}(\bar{g}_1) = \bar{f}(\bar{g}_1^{-1})\bar{f}(\bar{g}_2) \\
\Longrightarrow\ &\bar{f}(\bar{g}_1^{-1})\bar{f}(\bar{g}_2) = 1 \\
\Longrightarrow\ &f(g^{-1}g) = 1 \\
\Longrightarrow\ &g^{-1}g \in K \\
\Longrightarrow\ &g_1K = g_2K \\
\Longrightarrow\ &\bar{g}_1 = \bar{g}_2
\end{aligned}$$

Second Isomorphism Theorem

If $N \trianglelefteq G$ and $S \leq G$, then

1. $N \cap S \trianglelefteq S$
2. $NS = \{ns|n \in N, s \in S\} \leq G$
3. $S/_{N \cap S} \cong NS/_{N} = SN/_{N}$

$N \cap S$ is a subgroup of S

Since both N and S are subgroups of G, $1 \in N$ and $1 \in S$, therefore $1 \in N \cap S$.

$\forall x_1, x_2 \in N \cap S$,

- Since $x_1, x_2 \in N$ and N is a group, $x_1x_2 \in N$
- Since $x_1, x_2 \in S$ and S is a group, $x_1x_2 \in S$

Therefore $x_1x_2 \in N \cap S$

$N \cap S$ is normal

$\forall x \in N \cap S$, $\forall s \in S$

- Since $x \in N$ and $N \trianglelefteq G$ and $s \in G$, $sxs^{-1} \in N$
- Since $x \in S$, and S is a group, $sxs^{-1} \in S$

Therefore $sxs^{-1} \in N \cap S$

NS is a subset of G

$\forall n \in N, s \in S$, since both $n, s \in G$ and G is a group, $ns \in G$

NS is a group

Obviously, $1_{NS} = 1_N 1_S \in NS$.
Let $x_1, x_2 \in NS$, then exists $n_1 s_1 = x_1$ and $n_2 s_2 = x_2$. Thus $x_1 x_2 = n_1 s_1 n_2 s_2$.
Since $N \trianglelefteq G$, any $n \in N$ has some $n' \in N$ such that $gng^{-1} = n'$, for all $g \in G$ as well as $s \in S \leq G$.
So let $n_2 = s_1^{-1} n_2' s_1$, we get $x_1 x_2 = n_1 n_2' s_1 s_2 \in NS$

N is a normal subgroup of NS

Because $N \trianglelefteq G$ and $NS \leq G$

$S/N \cap S$ is isomorphic to NS/N

Let $f : S \to NS/N$ be $f(s) = sN$. Then

$$\begin{aligned}\ker(f) =& \{s \in S | f(s) = 1_{NS/N}\} \\ =& \{s \in S | sN = N\} \\ =& \{s \in S | s \in N\} \\ =& S \cap N\end{aligned}$$

The statement is true by first isomorphism theorem.

Third Isomorphism Theorem

If $N \triangleleft M \triangleleft G$ and $N \triangleleft G$, Then $M/N \triangleleft G/N$ and

$$ {}^{G/N}\!\big/_{M/N} \cong {}^{G}\!\big/_{M} $$

This can be proved by first isomorphism theorem and

$$\phi : {}^{G}\!\big/_{N} \to {}^{G}\!\big/_{M}, \ \phi(gN) = gM$$

ϕ is well defined

It equivalent to:

$$\forall g_1, g_2 \in G, g_1 N = g_2 N \implies \phi(g_1 N) = \phi(g_2 N)$$

The proof is given by

$$g_1 N = g_2 N \implies g_1^{-1} g_2 \in N \implies g_1^{-1} g_2 \in M \implies \phi(g_1 N) = \phi(g_2 N)$$

${}^{M}\!\diagup_{N}$ is a normal subset of ${}^{G}\!\diagup_{N}$

It is true iff:

$$\forall\ mN \in {}^{M}\!\diagup_{N},\ gN \in {}^{G}\!\diagup_{N}, (gN)(mN)(gN)^{-1} \in {}^{M}\!\diagup_{N}$$

$(gN)(mN)(gN)^{-1} = (gmg^{-1})N$, as $M \triangleleft G$, $gmg^{-1} \in M$. So $gmg^{-1}N \in {}^{N}\!\diagup_{M}$

${}^{M}\!\diagup_{N}$ is the kernel of ϕ

$$\begin{aligned}\ker(\phi) &= \left\{ gN \in {}^{G}\!\diagup_{N} \,\middle|\, gM = M \right\} \\ &= \left\{ gN \in {}^{G}\!\diagup_{N} \,\middle|\, g \in M \right\} \\ &= {}^{M}\!\diagup_{N}\end{aligned}$$

ϕ is surjective

By definition this is obvious. From this we have $\mathrm{Im}(\phi) = {}^{G}\!\diagup_{M}$

Fundamental Theorem of Finite Abelian Groups

Every finite abelian groups is isomorphic to a product of cyclic groups.