Recall

$\phi : G \to G'$ - group homomorphism w/ kernel H

$$aH = Ha = \phi^{-1}(\{\phi(a)\})$$

Definition

Let $H \leq G$ w/ kernel H
Then H is a **normal subgroup** of G, denoted

$$H \trianglelefteq G$$

iff $\forall a \in G \quad aH = Ha$

Theorem

Let $\phi : G \to G'$ be a group homomorphism w/ kernel H

Then the cosets of H in G form a group, called the

coset / factor group, denoted G/H

wrt the operation defined by

$$aH \cdot bH = a \cdot bH$$

Moreover, the map $\mu : \underset{\{aH \mid a \in G\}}{\overset{\shortparallel}{G/H}} \to \phi(G)$

where $\phi(G) \leq G'$,
defined by $\mu(aH) = \phi(a)$, is isomorphic

<u>Proof</u>

1) $\forall aH, bH \in G/H$, $\exists ! \, aH \cdot bH = a \cdot bH$

$a \cdot bH \in G/H$

bcs $\forall a, b \in G \quad \exists ! \, a \cdot b, \; a \cdot b \in G$

2) $\forall aH, bH, cH \in G/H$,

$$\begin{aligned}(aH \cdot bH) \cdot cH &= a \cdot bH \cdot cH = (a \cdot b) \cdot cH \\ &= (a \cdot b \cdot c)\, H \\ &= aH \cdot bcH\end{aligned}$$

$= aH \cdot (bH \cdot cH)$

associative ✓

3) $\exists' H = eH \in G/H \quad \forall aH \in G/H$

$eH \cdot aH = e\cdot aH = aH = aH \cdot eH$

identity ✓

4) $\forall aH \in G/H \quad \exists' a^{-1}H \in G/H$

$a^{-1}H \cdot aH = H = aH \cdot a^{-1}H$

inverses ✓

$\therefore$ G/H has group structure

Notice the map $\mu : G/H \to \phi(G)$

$\mu(aH) = \phi(a)$, $a \in G$ is a homomorphism

bcs

$(\forall aH, bH \in G/H)$ $\mu(aH \cdot bH) = \mu(a \cdot bH)$

$= \phi(ab)$

$= \phi(a) \cdot \phi(b)$

$= \mu(aH) \cdot \mu(bH)$

the kernel of μ is

$$\ker \mu = \{ aH \in G/H \mid \mu(aH) = e' = \phi(e) \}$$
$$= \{ aH \in G/H \mid a \in H = \ker \phi \}$$
$$= \{ H \}$$

hence μ is trivial 4

μ is injective

μ is also surjective

$\therefore$ μ is a bijective homomorphism

μ is an isomorphism

$$G/H \cong \phi(G)$$

where $\phi(G) \leq G'$

Example

Let $\phi: \overset{G}{\overset{\shortparallel}{\mathbb{Z}}} \to \overset{G' = \phi(G)}{\overset{\shortparallel}{\mathbb{Z}_n}}$ $\qquad \phi(m) = m \bmod n = r$

where $m = nk + r$

$k \in \mathbb{Z} \quad 0 \le r \le n$

Then ϕ is a group homomorphism w/ kernel $H = \langle n \rangle = n\mathbb{Z}$

By thm, $\mathbb{Z}/n\mathbb{Z}$ is a factor group whose elements are right/left cosets

$n\mathbb{Z}+0, \quad n\mathbb{Z}+1, \ldots, n\mathbb{Z}+(n-1)$

w/ identity being

$$n\mathbb{Z}+0 = n\mathbb{Z} = \langle n \rangle$$

the inverse of $n\mathbb{Z}+k$ is

$n\mathbb{Z}+(n-k)$

Moreover

$\mu : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ defined by

$\mu(n\mathbb{Z}+k) = k$ is an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$$

Theorem

Let $H \leq G$

The left (right) coset "multiplication" is well-defined iff

$$H \trianglelefteq G$$

Proof

$\Rightarrow$ Assume op on cosets defined by $aH \cdot bH = a \cdot bH$ for $a, b \in G$ is well-defined

G/H is a group, show $aH = Ha$ $a \in G$

Let $x \in aH$ then $xH = aH$

(by def. of left coset)

Since $aH \in G/H$ $\exists! a^{-1}H$, $a^{-1}H \in G/H$

Then $xH \cdot a^{-1}H = aH \cdot a^{-1}H = H$

so $xH \cdot a^{-1}H = x \cdot a^{-1}H = H$

$xa^{-1} \in H$, $xa^{-1} = h$, $h \in H$

then $x = ha \in Ha$

we can show $Ha \subseteq aH$

$\Leftarrow$ (is similar)

Theorem

Let $H \trianglelefteq G$

Then $\gamma : G \to G/H$ defined $\gamma(a) = aH$

is a homomorphism w/ kernel H

<u>Proof</u>

$\forall a, b \in G \qquad \gamma(a \cdot b) = a \cdot bH = aH \cdot bH$

$= \gamma(a) \cdot \gamma(b)$

$\therefore \gamma$ is a homomorphism

$$\begin{aligned} \ker \gamma &= \{ a \in G \mid \gamma(a) = H \} \\ &= \{ a \in G \mid aH \in H \} \\ &= H \end{aligned}$$

Overview

onto $\phi(G)$ homomorphism w/ ker. H

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "\gamma"'] & & \phi(G) \leq G' \\
& G/H \arrow[ur, "\mu"'] &
\end{tikzcd}$$

canonical homomorphism
$\gamma(a) = aH$

canonical isomorphism
$\mu(aH) = \phi(a)$

The Fundamental Homomorphism Theorem

Let $\phi : G \to G'$ be a group homomorphism w/ kernel H

Then $\phi(G) \leq G'$

4

$\mu : G/H \to \phi(G)$

def $\mu(aH) = \phi(a)$

is an isomorphism

$\gamma : G \to G/H$

$\gamma : G \to G/H$

def $\gamma(a) = aH$

is a homomorphism w/ kernel H

$\forall a \in G \quad \phi(a) = \mu(\gamma(a)) = (\mu \circ \gamma)(a)$

$\phi = \mu \circ \gamma$