Factor Groups

Definition

Let $H \lhd G$. The set of all cosets of H, denoted G/H and often referred to as G modulo H, is given by:

$$G/H = \{gH \mid g \in G\}$$

Theorem

Let $H \lhd G$:

$$(aH)(bH) = (ab)H$$

is a binary operation on G/H.

Proof

Assume $a_1, a_2, b \in G$
Assume $a_1 H = a_2 H$

$a_1 H, a_2 H, bH \in G/H$
$(a_1 H)(bH) = (a_1 b)H$
$(a_2 H)(bH) = (a_2 b)H$
$a_1 b, a_2 b \in G$
So $(a_1 b)H, (a_2 b)H \in G/H$
Therefore the operation is closed.

$a_1^{-1} a_2 \in H$
$\exists\, h \in H, a_1^{-1} a_2 = h$
$(a_1 b)^{-1}(a_2 b) = b^{-1}(a_1^{-1} a_2)b = b^{-1} h b$
But $H \lhd G$
So $b^{-1} h b \in H$
$(a_1 b)H = (a_2 b)H$
Therefore the operation is well-defined.

Therefore the operation is a binary operation.

Theorem

Let $H \lhd G$:

G/H is a group

G/H is called a factor or quotient group.

Proof

Assume $a, b, c \in G$

$(aH)(bH) = (ab)H$ is a well-defined and closed operation.

$[(aH)(bH)](cH) = [(ab)H](cH) = [(ab)c]H = [a(bc)]H = (aH)[(bc)H] = (aH)[(bH)(cH)]$
$\therefore G/H$ is associative under the operation.

$H(aH) = (eH)(aH) = (ea)H = aH$
$(aH)H = (aH)(eH) = (ae)H = aH$
$\therefore G/H$ has identity H

$a^{-1} \in G$
$(a^{-1}H)(aH) = (a^{-1}a)H = eH = H$
$(aH)(a^{-1}H) = (aa^{-1})H = eH = H$
$\therefore G/H$ is closed under inverses.

$\therefore G/H$ is a group under the operation.

Theorem

Let $\phi : G \to G'$ be a homomorphism of groups and $K = \ker(\phi)$:

$$G/K \simeq \phi[G]$$

Proof

Let $\mu : G/K \to \phi[G]$ be defined by $\mu(aK) = \phi(a)$
By previous theorem, μ is well-defined

Assume $\mu(aK) = \mu(bK)$
$\phi(a) = \phi(b)$
$\phi(a)^{-1}\phi(b) = e'$
$\phi(a^{-1})\phi(b) = e'$
$\phi(a^{-1}b) = e'$
$a^{-1}b \in K$
$aK = bK$
$\therefore \mu$ is one-to-one.

Assume $g' \in \phi[G]$
$\exists\, g \in G, \phi(g) = g'$ $gK \in G/K$
$\mu(gK) = \phi(g) = g'$
$\therefore \mu$ is onto and is thus a bijection.

$\mu((aK)(bK)) = \mu((ab)K) = \phi(ab) = \phi(a)\phi(b) = \mu(aK)\mu(bK)$
$\therefore \mu$ is a homomorphism and thus an isomorphism

$\therefore G/K \simeq \phi[G]$

Example

$G = \mathbb{Z}_2 \times \mathbb{Z}_4$
$H = \langle(1,2)\rangle = \{(0,0), (1,2)\}$

Since G is abelian and $H \leq G$ we have $H \triangleleft G$

$|G| = 2 \cdot 4 = 8$
$|H| = 2$
$|G/H| = (G : H) = \frac{8}{2} = 4$

$(0,0)H = H$ $\qquad -(1,0) + (0,1) = (-1,1) = (1,1) \notin H$
$(1,0)H$ $\qquad -(1,0) + (1,1) = (0,1) \notin H$
$(0,1)H$ $\qquad -(0,1) + (1,1) = (1,0) \notin H$
$(1,1)H$