Factor/Quotient Groups

Def. Let H be a normal subgroup of a group G (i.e. $gH = Hg$, for any $g \in G$).

We define G/H (called "$G\ mod\ H$") to be the set of distinct cosets of H in G.

$$\boldsymbol{G/H = \{a_1H, a_2H, \ldots\}}$$

We define the product of two elements (i.e. cosets) of G/H by:

$$(xH)(yH) = \left\{(xh_1)(yh_2) \mid h_1, h_2 \in H\right\} = xyH$$

G/H is a group with this multiplication and is called a **factor group** or **quotient group**.

First, let's show if H is a normal subgroup of G then

$$(xH)(yH) = \left\{(xh_1)(yh_2) \mid h_1, h_2 \in H\right\} \text{ is equal to } xyH.$$

$(xh_1)(yh_2) = x(h_1y)h_2,$ because multiplication is associative.

Since H is normal i.e. $yH = Hy$ for all $y \in G$, there is an $h_3 \in H$ such that $h_1y = yh_3$.

So $(xh_1)(yh_2) = x(h_1y)h_2$

$$= x(yh_3)h_2$$

$$= xy(h_3h_2) \in xyH.$$

Let's show G/H is a group.

0) We just saw that it's closed under multiplication.
1) The multiplication is associative because the group multiplication in G is associative.

   $$(aH)(bHcH) = (aH)(bcH) = (abc)H$$

   $$(aHbH)(cH) = (abH)(cH) = (abc)H.$$

2) The identity element is the coset $eH = H$.
3) Given aH, $a^{-1}H$ is the inverse element (coset) in G/H since

   $$(aH)(a^{-1}H) = (aa^{-1})H = eH = H.$$

Ex. Let $G = \mathbb{Z}$ and $H = 4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8 \dots\}$. Identify the elements of $G/H = \mathbb{Z}/4\mathbb{Z}$.

Since G is abelian, H is a normal subgroup of G.

The factor group $\mathbb{Z}/4\mathbb{Z}$ is the set of cosets of $H = 4\mathbb{Z}$ in $G = \mathbb{Z}$.

That is, the elements of G/H are:

$$0 + 4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8 \dots\}$$

$$1 + 4\mathbb{Z} = \{\dots, -7, -3, 1, 5, 9 \dots\}$$

$$2 + 4\mathbb{Z} = \{\dots, -6, -2, 2, 6, 10 \dots\}$$

$$3 + 4\mathbb{Z} = \{\dots, -5, -1, 3, 7, 11 \dots\}.$$

If we want to "multiply" two elements, say $2 + 4\mathbb{Z}$ and $3 + 4\mathbb{Z}$, we do it by:

$$(2 + 4\mathbb{Z})(3 + 4\mathbb{Z}) = (2 + 3) + 4\mathbb{Z} = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}.$$

Ex. What is the identity element of $\mathbb{Z}/4\mathbb{Z}$? What is the inverse element of $3 + 4\mathbb{Z}$?

Any element of $\mathbb{Z}/4\mathbb{Z}$ looks like the set $m + 4\mathbb{Z}$,

where $m = 0, 1, 2$, or 3.

The identity element of $\mathbb{Z}/4\mathbb{Z}$ is just $4\mathbb{Z}$ since:

$$(4\mathbb{Z})(m + 4\mathbb{Z}) = (0 + m) + 4\mathbb{Z} = m + 4\mathbb{Z}.$$

To find the inverse of $3 + 4\mathbb{Z}$ we want the coset $m + 4\mathbb{Z}$ such that:

$$(m + 4\mathbb{Z})(3 + 4\mathbb{Z}) = 4\mathbb{Z}$$

$$(3 + m) + 4\mathbb{Z} = 4\mathbb{Z}.$$

So we need $3 + m = 0 \ mod \ 4$ or $m = 1$,

so $1 + 4\mathbb{Z}$ is the inverse element of $3 + 4\mathbb{Z}$.

Notice $\mathbb{Z}/4\mathbb{Z}$ looks a lot like $\mathbb{Z}_4$.

In fact there's a simple isomorphism from $\mathbb{Z}/4\mathbb{Z}$ onto $\mathbb{Z}_4$.

$$\phi: \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}_4 \text{ by } \phi(m + 4\mathbb{Z}) = m.$$

By similar reasoning $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$, for any $n \in \mathbb{Z}^+$.

Ex. Let $G = \mathbb{R}$ be a (abelian) group under addition and let $c \in \mathbb{R}^+$.

The cyclic subgroup $H =< c >$ of $\mathbb{R}$ contains:

$$\{\ldots - 3c, -2c, -c, 0, c, 2c, 3c, \ldots\}.$$

Describe the elements of G/H.

Every coset of H, mH where $m \in \mathbb{R}$ is:

$$\{\ldots - 3c + m, -2c + m, -c + m, m, m + c, m + 2c, m + 3c, \ldots\}$$

Notice that if m_1 and m_2 differ by an integer multiple of c you get the same coset.

For example if $c = \pi, \quad m_1 = \frac{1}{2}, \quad m_2 = \frac{1}{2} + 2\pi$:

$$H = \{\ldots - 3\pi, -2\pi, -\pi,\ 0,\ \pi,\ 2\pi,\ 3\pi, \ldots\}$$

$$m_1H = \{\ldots, -3\,\pi + \tfrac{1}{2},\ -2\pi + \tfrac{1}{2},\ -\pi + \tfrac{1}{2},\ \tfrac{1}{2},\ \pi + \tfrac{1}{2},\ 2\pi + \tfrac{1}{2}, \ldots\}$$

$$m_2H = \{\ldots, -3\,\pi + \left(\tfrac{1}{2} + 2\pi\right), -2\pi + \left(\tfrac{1}{2} + 2\pi\right), -\pi + \left(\tfrac{1}{2} + 2\pi\right), \left(\tfrac{1}{2} + 2\pi\right), \ldots\}$$

$$= \left\{\ldots, -\pi + \tfrac{1}{2},\ \tfrac{1}{2},\ \pi + \tfrac{1}{2},\ 2\pi + \tfrac{1}{2}, \ldots\right\} = m_1H.$$

So the group $G/H = \mathbb{R}/< c >$ is the set of cosets of the form $m + c\mathbb{Z}$, where $0 \leq m < c$. This group is isomorphic to:

$\mathbb{R}_c = \{\text{real numbers modulo c}\}$. That is, two real numbers are the same if their difference is an integer multiple of c (analogous to $\mathbb{Z}_n$). So 0.5 and $0.5 + 3\pi$ are the same in $\mathbb{R}_\pi$.

The isomorphism is:

$$\phi: \mathbb{R}/< c > \to \mathbb{R}_c \quad \text{by } \phi(m + c\mathbb{Z}) = m;\ \ 0 \leq m < c.$$

Ex. Find the order of the factor group $(\mathbb{Z}_2 \times \mathbb{Z}_4)/ < (1,1) >$.

The order of G/H is the number of cosets of H in G. If G is a finite group we saw that this number was $\frac{|G|}{|H|}$.

In this case $G = \mathbb{Z}_2 \times \mathbb{Z}_4$ so $|G| = (2)(4) = 8$.

The order of $< (1,1) >$ is the order of $(1,1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_4$.

1 is order 2 in $\mathbb{Z}_2$, and 1 is order 4 in $\mathbb{Z}_4$. The $LCM(2,4) = 4$, so

$< (1,1) >$ is order 4. Thus $|(\mathbb{Z}_2 \times \mathbb{Z}_4)/ < (1,1) >| = \frac{8}{4} = 2$.

Ex. Find the order of $(1,7)+< (1,3) >$ in the factor group $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/ < (1,3) >$.

$H =< (1,3) >= \{(1,3), (2,6), (3,9), (0,0)\}$

So what we want to know is the smallest k so that

$((1,7)+< (1,3) >)^k =< (1,3) >$. That is the same as finding the smallest k so that $(1,7)^k$ is any of the elements of

$$< 1,3 >= \{(1,3), (2,6), (3,9), (0,0)\}.$$

$(1,7)^2 = (1,7) + (1,7) = (2,2)$ (since $7 + 7 = 2 \ mod\ 12$)

$(1,7)^3 = (1,7) + (1,7) + (1,7) = (3,9) \in < (1,3) >$

So $(1,7)+< (1,3) >$ has order 3 in $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/ < (1,3) >$.

Theorem: Let H be a normal subgroup of G.

Then $\phi: G \to G/H$ by $\phi(x) = xH$ is a homomorphism with H as kernel.

Proof:

Let $x, y \in G$, then $\phi(xy) = xyH = (xH)(yH)$ (Since H is normal)

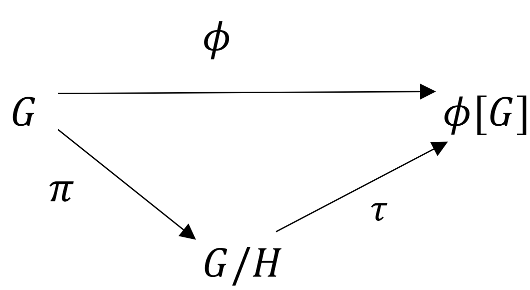
$= \phi(x)\phi(y)$.

H is the identity element in G/H.

$\phi(x) = xH = H$ if, and only if, $x \in H$.

So H is the kernel of ϕ.

The Fundamental Homomorphism Theorem: Let $\phi: G \to G'$ be a group homomorphism with kernel H. Then $\phi[G]$ is a group, and $\tau: G/H \to \phi[G]$ given by $\tau(gH) = \phi(g)$ is an ismorphism. If $\pi: G \to G/H$ is the homomorphism given by $\pi(g) = gH$, then $\phi(g) = \tau\pi(g)$ for each $g \in G$.



Another way to think about this theorem is that if we can find $\phi: G \to G'$, a homomorphism onto G', and $H = \ker(\phi)$, then G' is isomorphic to G/H (written $G' \cong G/H$).

Ex. Classify the group $(\mathbb{Z}_8 \times \mathbb{Z}_4)/ (\{0\} \times \mathbb{Z}_4)$

$\pi: \mathbb{Z}_8 \times \mathbb{Z}_4 \to \mathbb{Z}_8$ given by $\pi(x, y) = x$ is a homomorphism of $\mathbb{Z}_8 \times \mathbb{Z}_4$ onto $\mathbb{Z}_8$ with kernel $\{0\} \times \mathbb{Z}_4$.

By the fundamental homomorphism theorem we conclude that $(\mathbb{Z}_8 \times \mathbb{Z}_4)/ (\{0\} \times \mathbb{Z}_4)$ is isomorphic to $\mathbb{Z}_8$.

Ex. Show S_n/ A_n is isomorphic to $\mathbb{Z}_2$.

$\phi: S_n \to \mathbb{Z}_2$, by $\phi(\sigma) = 0$ if σ is even (i.e. in A_n)

$= 1$ if σ is odd

is a homomorphism of S_n onto $\mathbb{Z}_2$.

The kernel of ϕ is A_n so $S_n/ A_n \cong \mathbb{Z}_2$ by the fundamental homomorphism theorem.

Theorem (Equivalent characterizations of Normal Subgroups): The following 3 conditions are equivalent.

1) $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
2) $gHg^{-1} = H$ for all $g \in G$.
3) $gH = Hg$ for all $g \in G$.

Proof: $1 \Rightarrow 2$. Assume $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

Thus $gHg^{-1} = \{ghg^{-1} | \ h \in H\} \subseteq H$ for all $g \in G$.

Now let's show $gHg^{-1} \supseteq H$ for all $g \in G$.
Let $h \in H$. Replacing g by g^{-1} in $ghg^{-1} \in H$
we get: $g^{-1}h(g^{-1})^{-1} = g^{-1}hg = h_1 \in H$.
Thus, $h = gh_1g^{-1} \in gHg^{-1}$ so $gHg^{-1} \supseteq H$.

Thus, $gHg^{-1} = H$.

$2 \Rightarrow 3$ $\quad gHg^{-1} = H \Rightarrow gH = Hg$ for all $g \in G$.

$3 \Rightarrow 1$ $\quad$ Suppose $gH = Hg$ for all $g \in G$. Then, $gh = h_1g$, so $ghg^{-1} = h_1 \in H$ for all $g \in G$ and all $h \in H$.

Def. An isomorphism $\phi: G \to G$ of a group with itself is an **automorphism**. The automorphism $i_g: G \to G$ by $i_g(x) = gxg^{-1}$ for all $x \in G$ is the **inner automorphism** of G by g. Performing i_g on x is called **conjugation** of x by g.

Thus, H is a normal subgroup of G if H is invariant under all inner automorphisms of G.