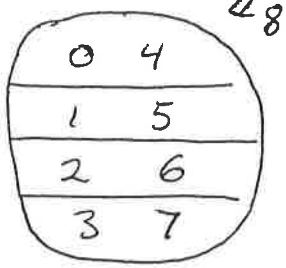
Section 14 Factor Groups

We have seen that the cosets of a subgroup $H \leq G$ sometime form a group. Such a group is called a <u>factor group</u>

As an example, consider the cosets of $H = \langle 4 \rangle = \{0, 4\}$ in the group $\mathbb{Z}_8$.

$$\begin{aligned} 0 + H &= \{0, 4\} = 4 + H \\ 1 + H &= \{1, 5\} = 5 + H \\ 2 + H &= \{2, 6\} = 6 + H \\ 3 + H &= \{3, 7\} = 7 + H \end{aligned}$$

$\mathbb{Z}_8$



The multiplication table of $\mathbb{Z}_8$ breaks up into blocks of cosets

	0	4	1	5	2	6	3	7
0	0	4	1	5	2	6	3	7
4	4	0	5	1	6	2	7	3
1	1	5	2	6	3	7	4	0
5	5	1	6	2	7	3	0	4
2	2	6	3	7	4	0	5	1
6	6	2	7	3	0	4	1	5
3	3	7	4	0	5	1	6	2
7	7	3	0	4	1	5	2	6

multiplication table for $\mathbb{Z}_8$

	0+H	1+H	2+H	3+H
0+H	0+H	1+H	2+H	3+H
1+H	1+H	2+H	3+H	0+H
2+H	2+H	3+H	0+H	1+H
3+H	3+H	0+H	1+H	2+H

multiplication table for the <u>factor group</u>

We are going to further explore this idea. We will need the following basic fact:

Suppose $H \leq G$. Then:

1. $aH = a'H \iff a = a'h$ for some $h \in H$
2. $Ha = Ha' \iff a = ha'$ for some $h \in H$

Not every subgroup $H \leq G$ will give rise to a factor group. H has to be a very special kind of subgroup. It must be what's called a <u>normal</u> subgroup.

> **Definition** A subgroup $H \leq G$ is a <u>normal subgroup</u> if $gH = Hg$ for every $g \in G$

Theorem Suppose H is a normal subgroup of G. Let $G/H = \{ aH \mid a \in G \}$ = set of cosets of H. Then there is a binary operation on G/H defined as $(aH)(bH) = (ab)H$ and G/H is a group under this operation. G/H is called a *factor group*

Proof First we must check that this operation makes sense. If $aH = a'H$ and $bH = b'H$, we must show $(aH)(bH) = (a'H)(b'H)$

i.e. $abH = a'b'H$

i.e. $ab = a'b'h$ for $h \in H$.

Now $aH = a'H$ means $a = a'h_0$ for $h_0 \in H$

And $bH = b'H$ means $b = b'h_1$ for $h_1 \in H$

And $b'H = Hb'$ means $b'h_2 = h_0 b'$ for $h_2 \in H$.

$Hb' = b'H$ means $h_0 b' = b'h_2$

Then $ab = a'h_0 b'h_1 = a'b'h_2 h_1 = a'b'h$.

for $h \in H$.

This means $(aH)(bH) = (a'H)(b'H)$
so the operation is well-defined.

Now we check group axioms.

$\mathcal{G}_1$ $$\big((aH)(bH)\big)cH = (abH)cH$$
$$= abcH$$
$$= (aH)(bcH)$$
$$= aH\big((bH)(cH)\big)$$

$\mathcal{G}_2$ The coset $eH = H$ is the identity because
$$(eH)(aH) = eaH = aH = (aH)(eH)$$

$\mathcal{G}_3$ The inverse of aH is $a^{-1}H$ because
$$(aH)(a^{-1}H) = aa^{-1}H = eH = (a^{-1}H)(aH).$$

$\blacksquare$

In short, if H is normal, then G/H is a group.

Notice that if G is abelian, every subgroup H is normal, for then $gH = Hg$

$\boxed{\text{Thus if } H \leq G \text{ and } G \text{ is abelian, then } G/H \text{ is always a group}}$

Example $\mathbb{Z}_{12} / \langle 3 \rangle$

Here are the cosets of $\langle 3 \rangle$:

	$\mathbb{Z}_{12}$			
$0+\langle 3 \rangle \rightsquigarrow$	0	3	6	9
$1+\langle 3 \rangle \rightsquigarrow$	1	4	7	10
$2+\langle 3 \rangle \rightsquigarrow$	2	5	8	11

Thus $\mathbb{Z}_{12} / \langle 3 \rangle = \{ 0+\langle 3 \rangle, \ 1+\langle 3 \rangle, \ 2+\langle 3 \rangle \}$

Here is the multiplication table. Notice that

$$\mathbb{Z}_{12} / \langle 3 \rangle \cong \mathbb{Z}_3$$

	$0+\langle 3 \rangle$	$1+\langle 3 \rangle$	$2+\langle 3 \rangle$
$0+\langle 3 \rangle$	$0+\langle 3 \rangle$	$1+\langle 3 \rangle$	$2+\langle 3 \rangle$
$1+\langle 3 \rangle$	$1+\langle 3 \rangle$	$2+\langle 3 \rangle$	$0+\langle 3 \rangle$
$2+\langle 3 \rangle$	$2+\langle 3 \rangle$	$0+\langle 3 \rangle$	$1+\langle 3 \rangle$

Example $(\mathbb{Z}_4 \times \mathbb{Z}_2) / \langle (2,0) \rangle$

Notice that $\langle (2,0) \rangle = \{ (0,0), (2,0) \}$.

Here are the cosets of $H = \langle (2,0) \rangle$

	$\mathbb{Z}_4 \times \mathbb{Z}_2$	
$(0,0)+H \to$	$(0,0)$	$(2,0)$
$(0,1)+H \to$	$(0,1)$	$(2,1)$
$(1,0)+H \to$	$(1,0)$	$(3,0)$
$(1,1)+H \to$	$(1,1)$	$(3,1)$

Here is the multiplication table. Notice that

$$(\mathbb{Z}_4 \times \mathbb{Z}_2) / \langle (2,0) \rangle \cong V$$

	$(0,0)+H$	$(0,1)+H$	$(1,0)+H$	$(1,1)+H$
$(0,0)+H$	$(0,0)+H$	$(0,1)+H$	$(1,0)+H$	$(1,1)+H$
$(0,1)+H$	$(0,1)+H$	$(0,0)+H$	$(1,1)+H$	$(1,0)+H$
$(1,0)+H$	$(1,0)+H$	$(1,1)+H$	$(0,0)+H$	$(0,1)+H$
$(1,1)+H$	$(1,1)+H$	$(1,0)+H$	$(0,1)+H$	$(0,0)+H$

How does all this tie in with homomorphisms?

Well, if $\varphi : G \to K$ is a homomorphism, then it turns out that $H = \mathrm{Ker}(\varphi)$ is a <u>normal subgroup of G</u>.

<u>Theorem</u> If $\varphi : G \to K$ then $H = \mathrm{Ker}(\varphi)$ is a normal subgroup.

<u>Proof</u>

We need to show $aH = Ha$ for any $a \in G$.

Idea: Show

1. $aH = \{ x \in G \mid \varphi(x) = \varphi(a) \}$ (then $aH = Ha$)
2. $Ha = \{ x \in G \mid \varphi(x) = \varphi(a) \}$