Let $G$ be a group and $H \leq G$.

Define $G/H = \{aH : a \in G\}$, the set of left cosets of $H$ in $G$.

**Q:** Can we turn $G/H$ into a group? What could the operation be?

It would be natural to define

$$aH \cdot bH = (ab)H,$$

but does this make sense? For this operation to be well-defined, it should not depend on the coset representatives.
(i.e., if \(aH = a'H\) and \(bH = b'H\), then \(aH \cdot bH\) should be the same as \(a'H \cdot b'H\))

This would mean that \(\forall h \in H, \forall a \in G,\)
\[haH = hH \cdot aH = eH \cdot aH = eaH = aH\]
\[\Rightarrow ha \in aH, \forall a \in G, \forall h \in H\]
\[\Rightarrow Ha \subseteq aH, \forall a \in G.\]

By replacing \(a\) with \(a^{-1}\), we also deduce that \(Ha^{-1} \subseteq a^{-1}H, \forall a \in G,\) so
\[a(Ha^{-1})a \leq a(a^{-1}H)a \Rightarrow aH \subseteq Ha, \forall a \in G\]
\[\therefore aH = Ha \quad !!\]
Summary: To turn $G/H$ into a group with the operation $aH \cdot bH = abH$, we need every left coset of $H$ to also be a right coset!

Definition: A subgroup $H$ of a group $G$ is called **normal** if $aH = Ha \ \forall a \in G$. In this case we write $H \trianglelefteq G$.

Remarks:

(1) Not every subgroup of a group $G$ is normal (e.g., you show on A3 that the subgroup $\langle v \rangle \leq D_4$ is not normal.)
(2) If $G$ is Abelian, however, then every subgroup $H \leq G$ is normal.

(3) In §5 we proved that for $H \leq G$,
$$aH = Ha \quad \forall a \in G \iff aH a^{-1} = H \quad \forall a \in G.$$ 

i.e.,
$$H \leq G \iff aH a^{-1} = H \quad \forall a \in G$$

The following result is a modification of the above. In practice, we use this result to test if subgroups are normal.

**Theorem 6.1** [Normal Subgroup Test]

Let $G$ be a group and $H \leq G$. Then $H \leq G \iff xHx^{-1} = H \quad \forall x \in G.$
Proof: The forward direction holds by statement 6 of Proposition 5.1.

Now assume that $xHx^{-1} \subseteq H \ \forall x \in G$.

Fix $a \in G$. With $x = a$ we have $aHa^{-1} \subseteq H$, so $aH \subseteq Ha$. Likewise with $x = a^{-1}$ we have $a^{-1}Ha \subseteq H$, so $Ha \subseteq aH$. We conclude that $aH = Ha$, so $H \subseteq G$. 

Ex: If $H = \{ R \in D_n \mid R$ is a rotation $\}$, then $H \subseteq D_n$. Indeed, let $x \in D_n$ and $ReH$. If $x$ is a rotation, then so is $XRx^{-1}$, so $XRx^{-1} \in H$. If instead $x$ is a flip,
then \( xR^{-1}x^{-1} \) is a rotation \((A1)\).
Thus \( xHx^{-1} \subseteq H \) \( \forall x \in D_n \), so \( H \leq D_n \).

**Example:** \( A_n \leq S_n \). Indeed, let \( \sigma \in A_n \) and \( \tau \in S_n \).
If \( \tau \) is even then so is \( \tau^{-1} \) and hence
\( \tau \tau^{-1} \) is \((\text{even})(\text{even})(\text{even}) = \text{even}) \).
If \( \tau \) is odd then so is \( \tau^{-1} \) and hence
\( \tau \tau^{-1} \) is \((\text{odd})(\text{even})(\text{odd}) = (\text{odd})(\text{odd}) = \text{even} \).
Thus, \( \tau A_n \tau^{-1} \subseteq A_n \) \( \forall \tau \in S_n \), so \( A_n \leq S_n \).

**Theorem 6.2:** Let \( G \) be a group and \( H \leq G \). If \( |G:H| = 2 \) then \( H \leq G \).

**Proof:** Since \( |G:H| = 2 \), there are 2 left
cosets and 2 right cosets. Since the left cosets partition the group, they are $H$ and $\{g \in G : g \cdot H\}$. Likewise, the right cosets are $H$ and $\{g \in G : H \cdot g\}$.

If $a \in H$, then $aH = H = Ha$

If $a \in H$, then $aH = \{g \in G : g \cdot H\} = Ha$. ■

**Remark:** Given $H \triangleleft G$, we can think of the elements of $H$ as "almost commuting" with each $a \in G$. That is, we can move $a$ to the other side of a product $ah$ ($h \in H$), but it may come at the cost of replacing $h$ with
some other \( h' \in H \): \( ah = h'a \)

In some special cases it will turn out that \( h = h' \).

**Ex:** Recall from Quiz 2 that the centre of a group \( G \) is defined as

\[
Z(G) = \{ a \in G \mid ab = ba \; \forall b \in G \}
\]

There you also proved that \( Z(G) \leq G \).

Actually, \( Z(G) \leq G \)! Indeed, if \( a \in Z(G) \) and \( b \in G \), then \( bab^{-1} = bb^{-1}a = a \in Z(G) \).

**Theorem 6.3** Let \( G \) be a group and
$H \trianglelefteq G$. Then $G/H = \{aH : a \in G\}$ is a group under the operation

$aH \cdot bH = abH$

**Proof:**

**[Well-defined]** Let's make sure that our operation doesn't depend on our choice of coset representative. [i.e., if $aH = a'H$ & $bH = b'H$ then $aH \cdot bH = a'H \cdot b'H$.]

Suppose $aH = a'H$ and $bH = b'H$.

Then $a = a'h_i$ and $b = b'h_2$ for some $h_i, h_2 \in H$.

We have $aH \cdot bH = abH = a'h_i b'h_2 H$
Thus, the operation is well-defined.

[**Associativity**] This follows from associativity of the operation in $G$.

[**Identity**] Note that $eH \cdot aH = eaH = aH$

$aH \cdot eH = aeH = aH$

Thus, $eH = H$ is the identity of $G/H$.

[**Inverses**] $aH \cdot a^{-1}H = aa^{-1}H = H$
Thus, \((aH)^{-1} = a^{-1}H\).

By the arguments above, \(G/H\) is a group.

**Note:** If \(H \trianglelefteq G\), we call the group \(G/H\) the quotient group of \(G\) by \(H\) (or sometimes "\(G \mod H\)"). The order of \(G/H\) is \(|G:H|\) (\# of left cosets).

If \(G\) is finite, then

\[
\left| \frac{G}{H} \right| = |G:H| = \frac{|G|}{|H|} \quad \text{(Lagrange)}
\]

**Ex:** Consider \(G = \mathbb{Z}\) and \(H = 3\mathbb{Z}\).

We have that
\[ \mathbb{Z}/3\mathbb{Z} = \{ a + 3\mathbb{Z} : a \in \mathbb{Z} \} = \{ 0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z} \} \]

But \( a + 3\mathbb{Z} = \{ a + 3k : k \in \mathbb{Z} \} = \{ b \in \mathbb{Z} : 3 \mid (b-a) \} = [a] \]

\( \therefore \) The elements of \( \mathbb{Z}/3\mathbb{Z} \) and \( \mathbb{Z}/3 \) are the same!

So is the operation: \( (a + 3\mathbb{Z})(b + 3\mathbb{Z}) = (a+b) + 3\mathbb{Z} \)

\[ [a] + [b] = [a+b] \]

Thus, \( \mathbb{Z}/3\mathbb{Z} \) and \( \mathbb{Z}/3 \) are the same group!

We've been working with quotients all along!

Remark: There is nothing special here about \( n=3 \).

In general, \( \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n \).
**Ex:** Consider \(<R_{90}> = \{ e, R_{90}, R_{180}, R_{270} \} \triangleq D_4\).

The quotient group has order

\[
\left| \frac{D_4}{<R_{90}>} \right| = \frac{|D_4|}{|<R_{90}>|} = \frac{8}{4} = 2.
\]

The elements are \(<R_{90}>\) and \(V<\overline{R_{90}}> = \{ V, H, D, D' \}\).

The Cayley table for \(D_4/<R_{90}>\) is

\[
\begin{array}{c|cc}
\langle R_{90} \rangle & \langle \overline{R_{90}} \rangle & V<\overline{R_{90}}> \\
\hline
\langle \overline{R_{90}} \rangle & \langle \overline{R_{90}} \rangle & \langle V<\overline{R_{90}}> \rangle \\
V<\overline{R_{90}}> & V<\overline{R_{90}}> & \langle \overline{R_{90}} \rangle \\
\end{array}
\]

The cool thing is that we can see the Cayley table for \(D_4/<R_{90}>\) in the Cayley table for \(D_4\)!
**Ex:** Recall that $K = \{e, R_{180}\} = Z(D_4) \triangleleft D_4$.

The quotient group has order

$$|D_4/K| = \frac{|D_4|}{|K|} = \frac{8}{4} = 2.$$

The elements: $K = \{e, R_{180}\}$, $R_{90}K = \{R_{90}, R_{270}\}$, $HK = \{H, V\}$, $DK = \{D, D'\}$. 

<table>
<thead>
<tr>
<th>$e$</th>
<th>$R_{90}$</th>
<th>$R_{180}$</th>
<th>$R_{270}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H$</td>
<td>$D$</td>
<td>$V$</td>
<td>$D'$</td>
</tr>
<tr>
<td>$V$</td>
<td>$D'$</td>
<td>$H$</td>
<td>$D$</td>
</tr>
<tr>
<td>$D$</td>
<td>$V$</td>
<td>$D'$</td>
<td>$H$</td>
</tr>
<tr>
<td>$D'$</td>
<td>$H$</td>
<td>$D$</td>
<td>$V$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$H$</th>
<th>$V$</th>
<th>$D$</th>
<th>$D'$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H$</td>
<td>$V$</td>
<td>$D$</td>
<td>$D'$</td>
</tr>
<tr>
<td>$V$</td>
<td>$H$</td>
<td>$D'$</td>
<td>$D$</td>
</tr>
<tr>
<td>$D$</td>
<td>$D'$</td>
<td>$V$</td>
<td>$H$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$e$</th>
<th>$R_{90}$</th>
<th>$R_{180}$</th>
<th>$R_{270}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H$</td>
<td>$V$</td>
<td>$D$</td>
<td>$D'$</td>
</tr>
<tr>
<td>$V$</td>
<td>$H$</td>
<td>$D'$</td>
<td>$D$</td>
</tr>
<tr>
<td>$D$</td>
<td>$V$</td>
<td>$D'$</td>
<td>$H$</td>
</tr>
<tr>
<td>$D'$</td>
<td>$H$</td>
<td>$D$</td>
<td>$V$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$e$</th>
<th>$R_{180}$</th>
<th>$R_{90}$</th>
<th>$R_{270}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H$</td>
<td>$D$</td>
<td>$V$</td>
<td>$D'$</td>
</tr>
<tr>
<td>$V$</td>
<td>$D'$</td>
<td>$H$</td>
<td>$D$</td>
</tr>
<tr>
<td>$D$</td>
<td>$V$</td>
<td>$D'$</td>
<td>$H$</td>
</tr>
<tr>
<td>$D'$</td>
<td>$H$</td>
<td>$D$</td>
<td>$V$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$R_{90}$</th>
<th>$R_{180}$</th>
<th>$R_{270}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_{90}$</td>
<td>$R_{180}$</td>
<td>$R_{270}$</td>
</tr>
<tr>
<td>$R_{180}$</td>
<td>$R_{270}$</td>
<td>$e$</td>
</tr>
<tr>
<td>$R_{270}$</td>
<td>$e$</td>
<td>$R_{90}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$R_{180}$</th>
<th>$R_{90}$</th>
<th>$R_{270}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_{180}$</td>
<td>$R_{90}$</td>
<td>$R_{270}$</td>
</tr>
<tr>
<td>$R_{90}$</td>
<td>$R_{180}$</td>
<td>$e$</td>
</tr>
<tr>
<td>$R_{270}$</td>
<td>$e$</td>
<td>$R_{90}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$R_{270}$</th>
<th>$R_{90}$</th>
<th>$R_{180}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_{270}$</td>
<td>$R_{90}$</td>
<td>$R_{180}$</td>
</tr>
<tr>
<td>$R_{90}$</td>
<td>$R_{180}$</td>
<td>$R_{270}$</td>
</tr>
<tr>
<td>$e$</td>
<td>$R_{90}$</td>
<td>$R_{180}$</td>
</tr>
</tbody>
</table>
**Cayley table:**

<table>
<thead>
<tr>
<th></th>
<th>K</th>
<th>$R_{q_0}K$</th>
<th>HK</th>
<th>DK</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>K</td>
<td>$R_{q_0}K$</td>
<td>HK</td>
<td>DK</td>
</tr>
<tr>
<td>$R_{q_0}K$</td>
<td>$R_{q_0}K$</td>
<td>K</td>
<td>DK</td>
<td>HK</td>
</tr>
<tr>
<td>HK</td>
<td>HK</td>
<td>DK</td>
<td>K</td>
<td>$R_{q_0}K$</td>
</tr>
<tr>
<td>DK</td>
<td>DK</td>
<td>HK</td>
<td>R_{q_0}K</td>
<td>K</td>
</tr>
</tbody>
</table>

By rearranging the table for $D_4$, we can once again see the structure of the quotient.
Exercise: Let $G$ be a group and $H \triangleleft G$.

(i) Prove that if $G$ is Abelian, so is $G/H$.

(ii) Prove that if $G$ is cyclic, so is $G/H$.

Not only are quotient groups interesting examples, they can tell us quite a bit about the parent group $G$.

Theorem 6.4: Let $G$ be a group. If $G/Z(G)$ is cyclic, then $G$ is Abelian.

Proof: Suppose that $G/Z(G) = \langle gZ(G) \rangle$ for some $g \in G$, so $G/Z(G) = \{g^kZ(G) : k \in \mathbb{Z} \}$. Thus, given $a, b \in G$, we can write $a = g^i z$. 
and \( b = g^j z_2 \) for some \( i, j \in \mathbb{Z} \) and \( z_1, z_2 \in Z(G) \)

But then \( ab = g^i z_1 g^j z_2 \)

\[
= g^i g^j z_1 z_2, \quad (z_1, z_2 \in Z(G))
\]

\[
= g^j g^i z_1 z_2, \quad (z_2 \in Z(G))
\]

\[
= g^j z_2 g^i z_1, \quad (z_2 \in Z(G))
\]

\[
= ba.
\]

Since \( ab = ba \) \( \forall a, b \in G \), \( G \) is Abelian.

**Exercise**: If \( |G| = pq \) where \( p, q \) are primes, then \( G \) is Abelian or \( Z(G) = \{e\} \).

**Theorem 6.5** \([Cauchy's Theorem for Abelian Groups]\)

Let \( G \) be a finite Abelian group. If \( p \)
is a prime and \( p \) divides \(|G|\), then \( G \) contains an element of order \( p \).

**Proof:** Clearly this holds when \( G \) has order 2. Proceeding by induction, suppose that the result holds for all groups of order \(< |G|\), and let \( p \) be a prime that divides \(|G|\).

First, note that \( G \) contains an element of prime order. Indeed, let \( x \in G \setminus \{e\} \). If \(|x| = m\), then \( m = nq \) for some prime \( q \). Hence

\[
|x^n| = \frac{|x|}{\gcd(|x|,n)} = \frac{nq}{\gcd(nq,n)} = q.
\]
So we may assume that $|x| = q$, $q$ prime.

If $q = p$ then we're done! So assume that $q \neq p$. Since $G$ is Abelian, $\langle x \rangle$ is normal and hence we can consider the quotient $G/\langle x \rangle$. This group has order $\frac{|G|}{q}$, and hence $p$ divides $|G/\langle x \rangle|$. By induction, there is an element $y \langle x \rangle \in G/\langle x \rangle$ of order $p$. Hence, $y^p \in \langle x \rangle = \{ e, x, x^2, \ldots, x^{q-1} \}$. Note that $y \neq e$ (else $|y\langle x \rangle| = 1$)

**Case I:** $y^p = e$.

In this case $|y|$ divides $p$, so $|y| = p$.
(as \( p \) prime and \( y \neq e \)).

Case II: \( y^p \neq e \)

Since \( |\langle x \rangle| = |x| = q \text{ (prime)} \), we have \( |y^p| = q \). We claim that \( |y^q| = p \). Indeed, \((y^p)^q = (y^q)^p = e\), so \( |y^q| \) divides \( p \) and hence \( |y^q| = 1 \) or \( p \). But if \( |y^q| = 1 \) then \( y^q = e \implies (y^{\langle x \rangle})^q = \langle x \rangle \)

\[ \implies p = |\langle x \rangle| \text{ divides } q \]

\( \implies |y^q| = p. \)

(Can’t happen as \( p,q \) are prime and \( p \neq q \).)