§6 – Quotients & Normal Subgroups

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

Define $\boxed{G/H = \{aH : a \in G\}}$, 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 $\forall h \in H$, $\forall a \in G$,

$$haH = hH \cdot aH$$
$$= eH \cdot aH = eaH = aH$$
$$\Rightarrow ha \in aH \quad \forall a \in G, \forall h \in H$$
$$\Rightarrow Ha \subseteq aH \quad \forall a \in G.$$

By replacing a with a^{-1}, we also deduce that $Ha^{-1} \subseteq a^{-1}H$ $\forall a \in G$, so

$$a(Ha^{-1})a \subseteq a(a^{-1}H)a \Rightarrow aH \subseteq Ha \quad \forall a \in G$$

$$\therefore aH = Ha \quad !!$$

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 $H \leq G$,

$$aH = Ha \quad \forall a \in G \iff aHa^{-1} = H \quad \forall a \in G.$$

i.e., $\boxed{H \trianglelefteq G \iff aHa^{-1} = H \quad \forall a \in G}$

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

$$H \trianglelefteq G \iff xHx^{-1} \subseteq H \quad \forall x \in G.$$

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 $H \trianglelefteq G$. ■

Ex: If $H = \{R \in D_n \mid R \text{ is a rotation}\}$, then $H \trianglelefteq D_n$. Indeed, let $x \in D_n$ and $R \in H$. If x is a rotation, then so is xRx^{-1}, so $xRx^{-1} \in H$. If instead x is a flip, then $xRx^{-1} = R^{-1}$ is a rotation (A1).

Thus $xHx^{-1} \subseteq H$ $\forall x \in D_n$, so $H \trianglelefteq D_n$.

Ex: $A_n \trianglelefteq S_n$. Indeed, let $\sigma \in A_n$ and $\tau \in S_n$.

If τ is even then so is τ^{-1} and hence

$\tau\sigma\tau^{-1}$ is (even)(even)(even) = even.

If τ is odd then so is τ^{-1} and hence

$\tau\sigma\tau^{-1}$ is $(\text{odd})\underbrace{(\text{even})(\text{odd})}_{\text{odd}} = (\text{odd})(\text{odd}) = \text{even}$

Thus, $\tau A_n \tau^{-1} \subseteq A_n$ $\forall \tau \in S_n$, so $A_n \trianglelefteq S_n$.

Theorem 6.2: Let G be a group and $H \leq G$. If $|G:H| = 2$ then $H \trianglelefteq G$.

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 $\{g \in G : g \notin H\}$. Likewise, the right cosets are H and $\{g \in G : g \notin H\}$.

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

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

Remark: Given $H \trianglelefteq G$, 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 $h' \in H$: $\boxed{ah = h'a}$

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

$$\boxed{Z(G) = \{a \in G \mid ab = ba \ \ \forall b \in G\}}$$

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

Actually, $Z(G) \trianglelefteq G$! 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

$$\boxed{aH \cdot bH = abH}$$

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 $a = a'h_1$ and $b = b'h_2$ for some $h_1, h_2 \in H$.

We have $aH \cdot bH = abH$

$$= a'h_1 b' \underline{h_2 H}$$

$$= a'\underbrace{h_1 b'}_{= b'h_3 \text{ for some } h_3 \in H} H$$

$$= a'b'\underbrace{h_3 H}_{= H}$$

$$= a'b'H = a'H \cdot b'H.$$

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

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

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

$$\boxed{\left|G/H\right| = |G:H| = \frac{|G|}{|H|}} \quad \text{(Lagrange)}$$

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 $a + 3\mathbb{Z} = \{a + 3k \;:\; k \in \mathbb{Z}\}$

$$= \{b \in \mathbb{Z} \;:\; 3 \mid b - a\} = [a] \quad !$$

$\therefore$ 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, $\boxed{\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.}$

Ex: Consider $\langle R_{90} \rangle = \{e, R_{90}, R_{180}, R_{270}\} \trianglelefteq D_4$.

The quotient group has order

$$|D_4/\langle R_{90}\rangle| = \frac{|D_4|}{|\langle R_{90}\rangle|} = \frac{8}{4} = 2.$$

The elements are $\langle R_{90}\rangle$ and $\underline{V}\langle R_{90}\rangle = \{V, H, D, D'\}$.

could use any flip here.

The Cayley table for $D_4/\langle R_{90}\rangle$ is

	$\langle R_{90}\rangle$	$V\langle R_{90}\rangle$
$\langle R_{90}\rangle$	$\langle R_{90}\rangle$	$V\langle R_{90}\rangle$
$V\langle R_{90}\rangle$	$V\langle R_{90}\rangle$	$\langle R_{90}\rangle$

The cool thing is that we can see the Cayley table for $D_4/\langle R_{90}\rangle$ in the Cayley table for D_4!

	e	R_{90}	R_{180}	R_{270}	H	V	D	D'
e	e	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	e	D'	D	H	V
R_{180}	R_{180}	R_{270}	e	R_{90}	V	H	D'	D
R_{270}	R_{270}	e	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	e	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	e	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	e	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	e

Ex: Recall that $K = \{e, R_{180}\} = Z(D_4) \trianglelefteq D_4$.

The quotient group has order

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

The elements: $K = \{e, R_{180}\}$, $R_{90}K = \{R_{90}, R_{270}\}$

$HK = \{H, V\}$, $DK = \{D, D'\}$

Cayley table:

	K	$R_{90}K$	HK	DK
K	K	$R_{90}K$	HK	DK
$R_{90}K$	$R_{90}K$	K	DK	HK
HK	HK	DK	K	$R_{90}K$
DK	DK	HK	$R_{90}K$	K

By rearranging the table for D_4, we can once again see the structure of the quotient.

	e	R_{180}	R_{90}	R_{270}	H	V	D	D'
e	e	R_{180}	R_{90}	R_{270}	H	V	D	D'
R_{180}	R_{180}	e	R_{270}	R_{90}	V	H	D'	D
R_{90}	R_{90}	R_{270}	R_{90}	e	D'	D	H	V
R_{270}	R_{270}	R_{90}	e	R_{180}	D	D'	V	H
H	H	V	D	D'	e	R_{180}	R_{90}	R_{270}
V	V	H	D'	D	R_{180}	e	R_{270}	R_{90}
D	D	D'	V	H	R_{270}	R_{90}	e	R_{180}
D'	D'	D	H	V	R_{90}	R_{270}	R_{180}	e

Exercise: Let G be a group and $H \trianglelefteq G$.

(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 $G/Z(G) = \{g^k Z(G) : k \in \mathbb{Z}\}$. Thus, given $a, b \in G$, we can write $a = g^i z_1$

and $b = g^j z_2$ for some $i, j \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$

But then $ab = g^i z_1 g^j z_2$

$$= g^i g^j z_2 z_1 \qquad (z_1, z_2 \in Z(G))$$

$$= g^j g^i z_1 z_2$$

$$= g^j z_2 g^i z_1 \qquad (z_2 \in Z(G))$$

$$= ba.$$

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

$$y^q = e \implies (y\langle x \rangle)^q = \langle x \rangle$$

$$\implies p = |y\langle x \rangle| \text{ divides } q$$

(Can't happen as p, q are prime and $p \neq q$)

$\therefore |y^q| = p.$ ■