Math 4550

Topic 6 - Normal subgroups and Factor groups

Def: Let G be a group and $H \leq G$. Let $g \in G$.

The left coset of H containing g is

$$gH = \{gh \mid h \in H\}$$

The right coset of H containing g is

$$Hg = \{hg \mid h \in H\}$$

The set of all left cosets is

$$\underbrace{G/H}_{\text{I read this as "G mod H"}} = \{gH \mid g \in G\}$$

Ex: $D_6 = \{1, r, r^2, s, sr, sr^2\}$

$H = \langle r \rangle = \{1, r, r^2\}$ $\boxed{r^3 = 1, s^2 = 1}$

left cosets:

$1H = \{1\cdot 1, 1\cdot r, 1\cdot r^2\} = \{1, r, r^2\} = H$

$rH = \{r\cdot 1, r\cdot r, r\cdot r^2\} = \{r, r^2, 1\} = H$

$r^2H = \{r^2\cdot 1, r^2\cdot r, r^2\cdot r^2\} = \{r^2, 1, r\} = H$

$sH = \{s\cdot 1, s\cdot r, s\cdot r^2\} = \{s, sr, sr^2\}$

$srH = \{sr\cdot 1, sr\cdot r, sr\cdot r^2\} = \{sr, sr^2, s\}$

$sr^2H = \{sr^2\cdot 1, sr^2\cdot r, sr^2\cdot r^2\} = \{sr^2, s, sr\}$

There are two left cosets:

$$\{1, r, r^2\} = H = rH = r^2H$$

$$\{s, sr, sr^2\} = sH = srH = sr^2H$$

right cosets:

$$H1 = \{1\cdot 1, r\cdot 1, r^2\cdot 1\} = \{1, r, r^2\}$$

$$Hr = \{1\cdot r, r\cdot r, r^2\cdot r\} = \{r, r^2, 1\}$$

$$Hr^2 = \{1\cdot r^2, r\cdot r^2, r^2 r^2\} = \{r^2, 1, r\}$$

$$Hs = \{1\cdot s, rs, r^2 s\} = \{s, sr^2, sr\}$$

$$rs = sr^{-1} = sr^{3-1} = sr^2$$
$$r^2 s = sr^{-2} = sr^{3-2} = sr$$

$$Hsr = \{1\cdot sr, rsr, r^2 sr\} = \{sr, s, sr^2\}$$

$$rsr = sr^{-1}r = s$$
$$r^2 sr = sr^{-2}r = sr^{-1} = sr^2$$

$$Hsr^2 = \{1\cdot sr^2, rsr^2, r^2sr^2\} = \{sr^2, sr, s\}$$

$$rsr^2 = sr^{-1}r^2 = sr$$
$$r^2sr^2 = sr^{-2}r^2 = s$$

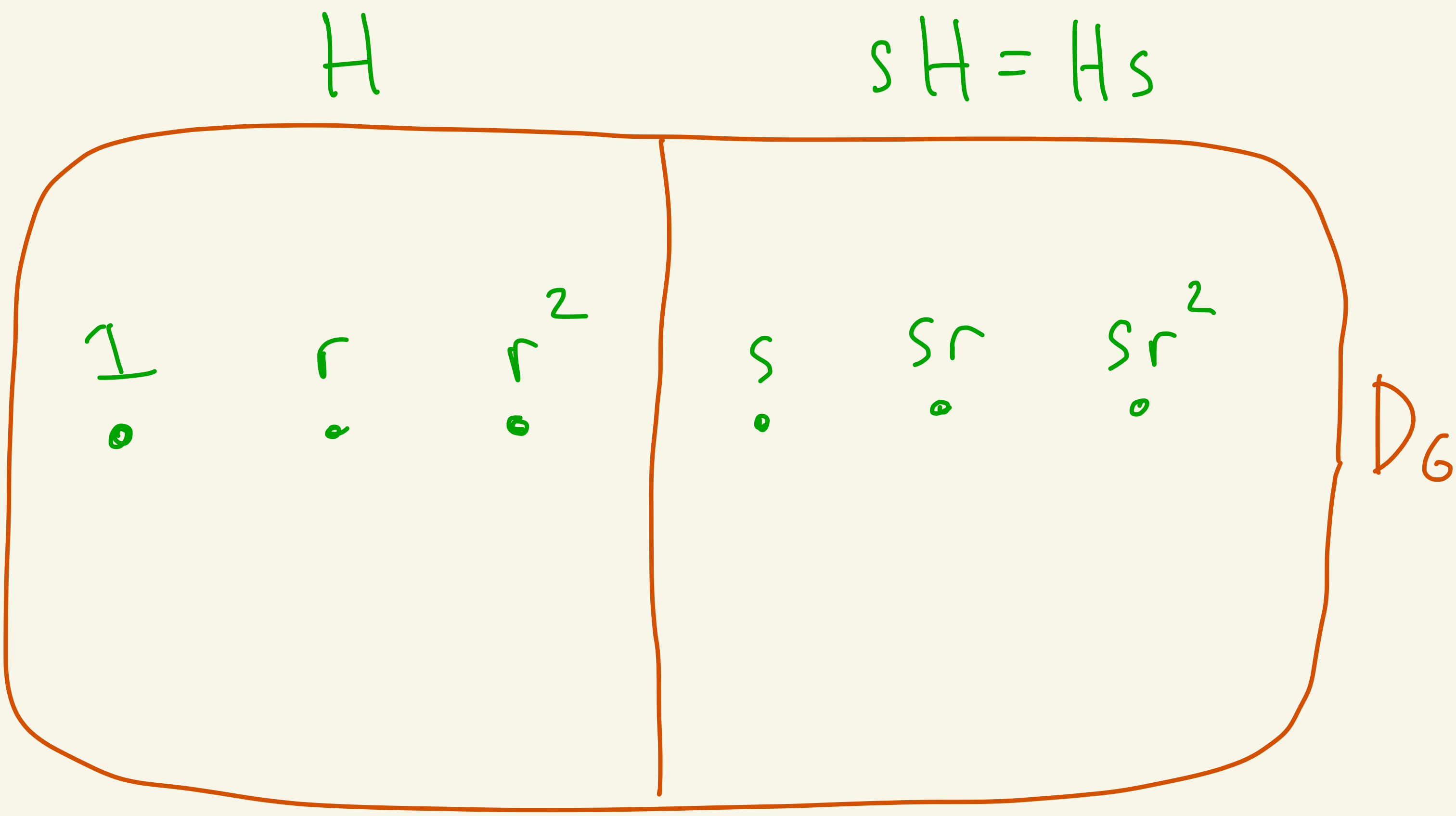
There are two right cosets:

$$\{1, r, r^2\} = H = Hr = Hr^2$$

$$\{s, sr, sr^2\} = Hs = Hsr = Hsr^2$$

In this case the left and right cosets are the same.

The group D_6 is partitioned by its left or its right cosets in the same way.
In this case



The set of left cosets is

$$D_6/H = \{H, sH\}$$

Theorem: Let G be a group and $H \leq G$. Let $a, b \in G$.

Then:

1. $a \in aH$
2. $aH = bH$ iff $b^{-1}a \in H$
3. $aH = bH$ iff $a \in bH$
4. $aH = bH$ iff $a = bh$ for some $h \in H$
5. The left cosets of G partion G.

   That is, $G = \bigcup_{g \in G} gH$

   and given any two left cosets aH and bH either $aH \cap bH = \phi$ or $aH = bH$.
6. If H is finite, then $|aH| = |H| = |Ha|$

Proof:

① $e \in H$ since $H \leq G$.

Thus, $a = ae \in aH$.

---

② ($\Rightarrow$) Suppose $aH = bH$

By part ① we know $a \in aH$.

Since $aH = bH$ this gives $a \in bH$.

Thus, $a = bh$ for some $h \in H$.

Thus, $b^{-1}a = h \in H$.

($\Leftarrow$) Suppose $b^{-1}a \in H$

Then $b^{-1}a = h$ for some $h \in H$.

Let's show $aH = bH$ by showing both $aH \subseteq bH$ and $bH \subseteq aH$.

Let $z \in aH$.

Then $z = ah_1$ where $h_1 \in H$.

So, $z = ah_1 = bhh_1 = b\underbrace{(hh_1)}_{\substack{\text{in } H \\ \text{since } H \leq G}} \in bH$

Thus, $aH \subseteq bH$.

Now suppose $w \in bH$.

Then $w = bh_2$ where $h_2 \in H$.

So, $w = bh_2 = ah^{-1}h_2 = a\underbrace{(h^{-1}h_2)}_{\text{in } H \text{ since } H \leq G} \in aH$

Thus, $bH \subseteq aH$.

Therefore $aH = bH$.

---

(3) HW

---

(4) HW

---

(5) Clearly $gH \subseteq G$ for any $g \in G$.

Thus,

$$G = \bigcup_{g \in G} \{g\} \subseteq \bigcup_{g \in G} gH \subseteq G.$$

So, $G = \bigcup_{g \in G} gH$.

Let aH and bH be two left cosets.
We want to show that either
$aH = bH$ or $aH \cap bH = \emptyset$.

We do this by showing that
$aH = bH$ iff $aH \cap bH \neq \emptyset$.

($\Rightarrow$) Suppose $aH = bH$.
Then, $aH \cap bH = \underbrace{aH \neq \emptyset}_{\text{since } a \in aH}$

($\Leftarrow$) Suppose $aH \cap bH \neq \emptyset$.
Then there exists $z \in aH \cap bH$.
Thus, $z = ah_1$ and $z = bh_2$ where
$h_1, h_2 \in H$.
Now let's show $aH = bH$.
Let $y \in aH$.
Then $y = ah_3$ where $h_3 \in H$.

Since $ah_1 = z = bh_2$ we have that $a = bh_2h_1^{-1}$.

Thus, $y = ah_3 = b\underbrace{h_2h_1^{-1}h_3}_{\text{in } H} \in bH$

So, $aH \subseteq bH$.

Suppose $x \in bH$.

Then $x = bh_4$ where $h_4 \in H$.

Since $ah_1 = bh_2$ we have $b = ah_1h_2^{-1}$

Thus,

$$x = bh_4 = a\underbrace{h_1h_2^{-1}h_4}_{\text{in } H} \in aH$$

So, $bH \subseteq aH$.

Hence $aH = bH$.

---

(6) HW

$\boxed{\diagup\diagup\diagup}$

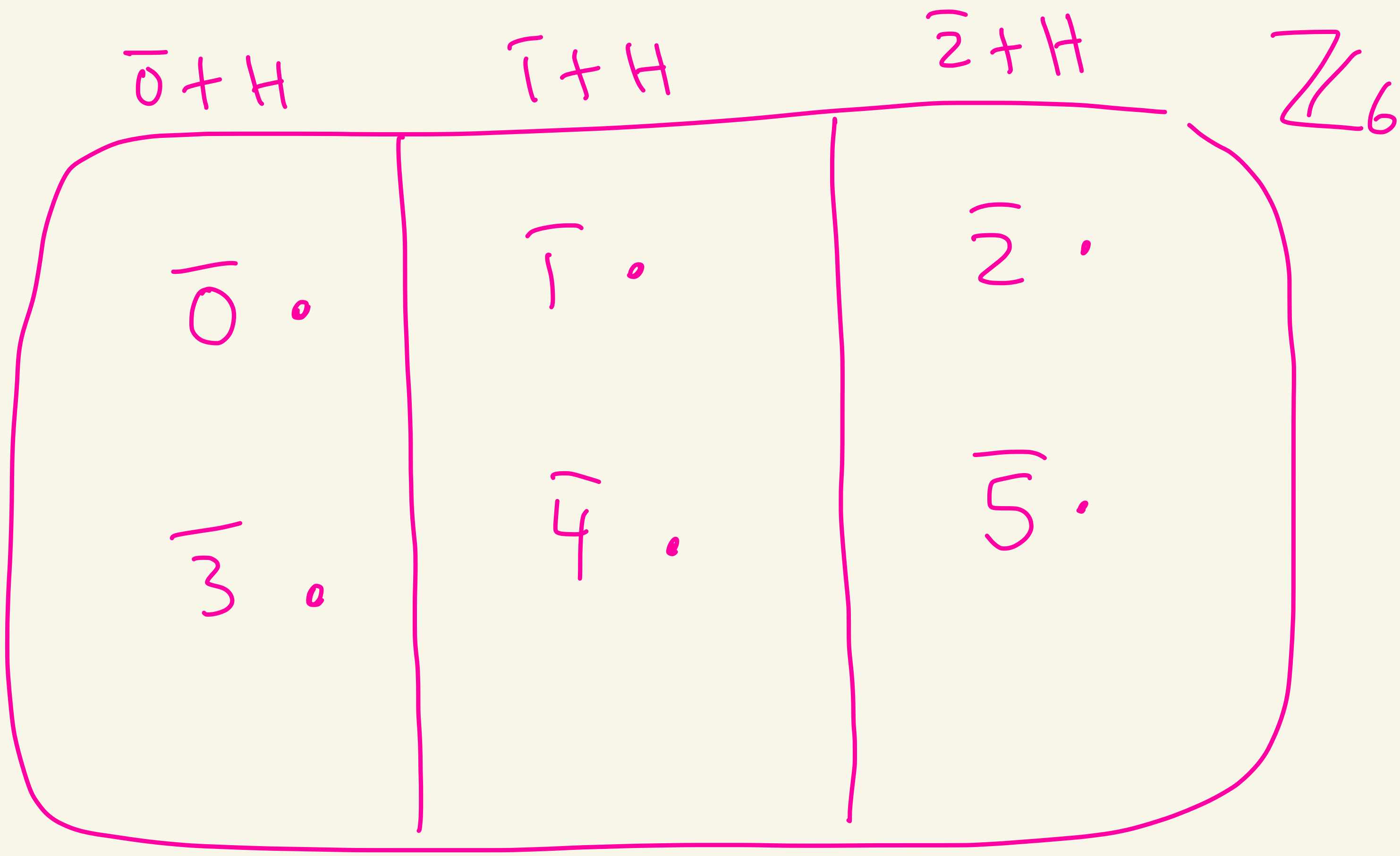
Ex: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$H = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$

$\bar{0} + H = \{\bar{0}, \bar{3}\} = \bar{3} + H$

$\bar{1} + H = \{\bar{1}, \bar{4}\} = \bar{4} + H$

$\bar{2} + H = \{\bar{2}, \bar{5}\} = \bar{5} + H$



The set of left cosets is

$\mathbb{Z}_6/H = \{\bar{0} + H, \bar{1} + H, \bar{2} + H\}$

Lagrange's theorem

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

---

proof:

Let $g_1H, g_2H, \ldots, g_rH$ be the distinct left cosets that partition G.

From the theorem,

$$|g_1H| = |g_2H| = \cdots = |g_rH| = |H|$$

Thus,

$$\begin{aligned} |G| &= |g_1H| + |g_2H| + \cdots + |g_rH| \\ &= |H| + |H| + \cdots + |H| \\ &= r|H| \end{aligned}$$

∎

Corollary: If G is a group and $|G| = p$ where p is prime, then G is cyclic.

---

proof: Since p is prime, $p \geq 2$.

Thus, there exists $x \in G$ where $x \neq e$.

Consider $H = \langle x \rangle$.

Since $x \neq e$, we know $e, x \in H$ and that $|H| \geq 2$.

By Lagrange, $|H|$ divides $|G| = p$.

The only divisors of p are 1 and p because p is prime.

Thus, $|H| = p$.

Therefore $H = G$.

Thus, $G = \langle x \rangle$ is cyclic

$\blacksquare$

Theorem: Let G be a finite group. If $x \in G$, then the order of x divides $|G|$.

Proof: Let $H = \langle x \rangle$.

Then, $H = \{e, x, x^2, \dots, x^{m-1}\}$ where m is the order of x.

So, $|H| = m$.

By Lagrange's theorem, $|H|$ divides $|G|$.

So, m divides $|G|$. $\blacksquare$

<u>Def:</u> Let G be a group and $H \leq G$. We say that H is <u>normal</u> if $gH = Hg$ for all $g \in G$.

We write $H \trianglelefteq G$ to mean that H is a normal subgroup of G.

<u>Ex:</u> $D_6 = \{1, r, r^2, s, sr, sr^2\}$

$H = \langle r \rangle = \{1, r, r^2\}$

previously we saw that:

<u>left cosets</u>

$\{1, r, r^2\} = H = rH = r^2H$

$\{s, sr, sr^2\} = sH = srH = sr^2H$

<u>right cosets</u>

$\{1, r, r^2\} = H = Hr = Hr^2$

$\{s, sr, sr^2\} = Hs = Hsr = Hsr^2$

Thus, $H \trianglelefteq D_6$

__Ex:__ $D_6 = \{1, r, r^2, s, sr, sr^2\}$

$H = \langle s \rangle = \{1, s\}$

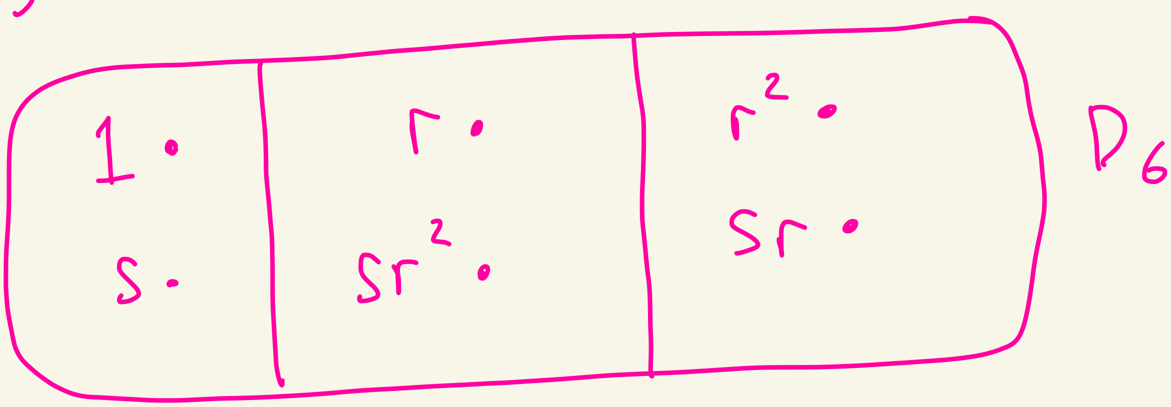
left cosets

$H = \boxed{\{1, s\}} = sH$

$rH = \{r, rs\} = \{r, sr^{-1}\} = \boxed{\{r, sr^2\}} = sr^2H$

$r^2H = \{r^2, r^2s\} = \boxed{\{r^2, sr\}} = sr\,H$

So, the left cosets partition D_6 as follows:



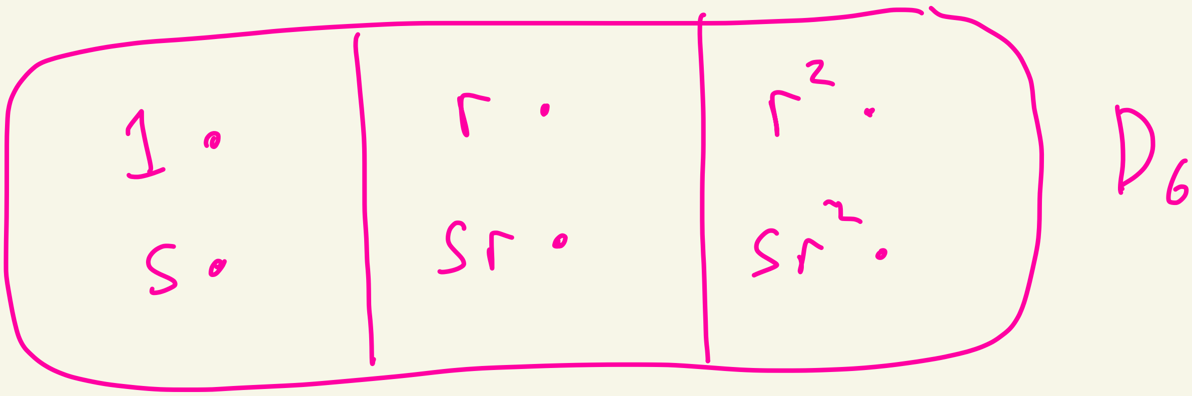
__right cosets__

$H = \{1, s\} = Hs$

$Hr = \{r, sr\} = Hsr$

$Hr^2 = \{r^2, sr^2\} = Hsr^2$

The right cosets partition D_6 as follows:



The left and right cosets are not the same. Thus, H is not a normal subgroup of D_6.

Theorem: If G is an abelian group, then all of it's subgroups are normal.

proof: Let G be an abelian group.

Let $H \leq G$ and $g \in G$.

Then,

$$gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg.$$

Thus, $H \trianglelefteq G$. $\blacksquare$

Ex: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ is abelian.

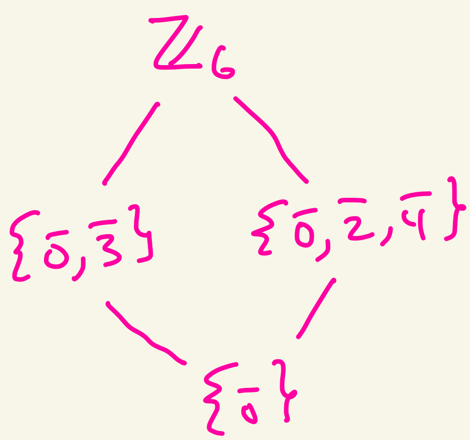
All subgroups of $\mathbb{Z}_6$ are normal.

$\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{1} \rangle = \langle \bar{5} \rangle = \mathbb{Z}_6$

$\langle \bar{2} \rangle = \langle \bar{4} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$

$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$



Theorem: Let G be a group and $H \leq G$. Then the following are equivalent.

① H is normal.
② $gHg^{-1} \subseteq H$ for all $g \in G$
③ $gHg^{-1} = H$ for all $g \in G$

Here $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$

---

proof:

(① ⇒ ②) Assume H is normal, that is $gH = Hg$ for all $g \in G$

Fix some $g \in G$.
Let $x \in gHg^{-1}$.
Then $x = ghg^{-1}$ for some $h \in H$.
Since $gh \in gH$ and $gH = Hg$ there exists h_1 where $gh = h_1 g$.
Then, $x = ghg^{-1} = h_1 g g^{-1} = h_1 \in H$.
So, $gHg^{-1} \subseteq H$.

(② ⇒ ③) Assume $xHx^{-1} \subseteq H$ for all $x \in G$.
We must show that $H \subseteq xHx^{-1}$ for all $x \in G$.
Let $g \in G$ be fixed.
Let's show $H \subseteq gHg^{-1}$.
Let $h \in H$.

Then, $g^{-1}hg = g^{-1}h(g^{-1})^{-1} \in H$ ← by assumption with $x = g^{-1}$

Thus, $g^{-1}hg = h_2$ where $h_2 \in H$.

Then, $h = gh_2g^{-1} \in gHg^{-1}$.

Thus, $H \subseteq gHg^{-1}$.

(3 ⇒ 1) Suppose $xHx^{-1} = H$ for all $x \in G$.

Let g be fixed.

Let $x \in gH$.

Then, $x = gh$ where $h \in H$.

assumption with $x = g$

By assumption $ghg^{-1} \in H$ and so $ghg^{-1} = h_3$ where $h_3 \in H$

Thus, $x = gh = h_3 g \in Hg$.

So, $gH \subseteq Hg$.

Similarly let $y \in Hg$.

Then $y = h'g$ for some $h' \in H$.

And $g^{-1}h'g = g^{-1}h(g^{-1})^{-1} \in H$ ← assumption with $x = g^{-1}$

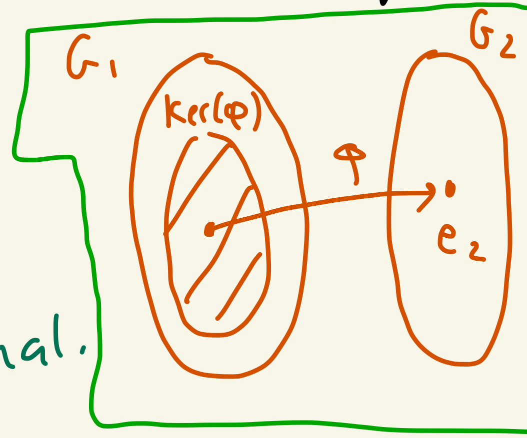
So, $g^{-1}h'g = h_4$ for some $h_4 \in H$.

Then, $y = h'g = gh_4 \in gH$.

Thus, $Hg \subseteq gH$.

Therefore, $Hg = gH$ and H is normal. $\blacksquare$

Theorem: Let $\varphi : G_1 \to G_2$ be a homomorphism. Then, $\ker(\varphi) \trianglelefteq G_1$.



proof: We know $\ker(\varphi) \leq G_1$

Let's show that $\ker(\varphi)$ is normal.

Let $g \in G_1$ and $h \in \ker(\varphi)$.

Then,
$$\begin{aligned} \varphi(ghg^{-1}) &= \varphi(g)\varphi(h)\varphi(g^{-1}) \\ &= \varphi(g)\, e_2\, \varphi(g^{-1}) \\ &= \varphi(g)\varphi(g^{-1}) \\ &= \varphi(gg^{-1}) \\ &= \varphi(e_1) \\ &= e_2 \end{aligned}$$

since $h \in \ker(\varphi)$

So, $ghg^{-1} \in \ker(\varphi)$.

Thus, $g(\ker(\varphi))g^{-1} \subseteq \ker(\varphi)$

So, $\ker(\varphi)$ is normal. $\blacksquare$

Ex: Consider $GL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, \begin{matrix} a,b,c,d \in \mathbb{R} \\ ad-bc \neq 0 \end{matrix} \right\}$

Consider $\det : GL(2,\mathbb{R}) \longrightarrow \mathbb{R}^*$.

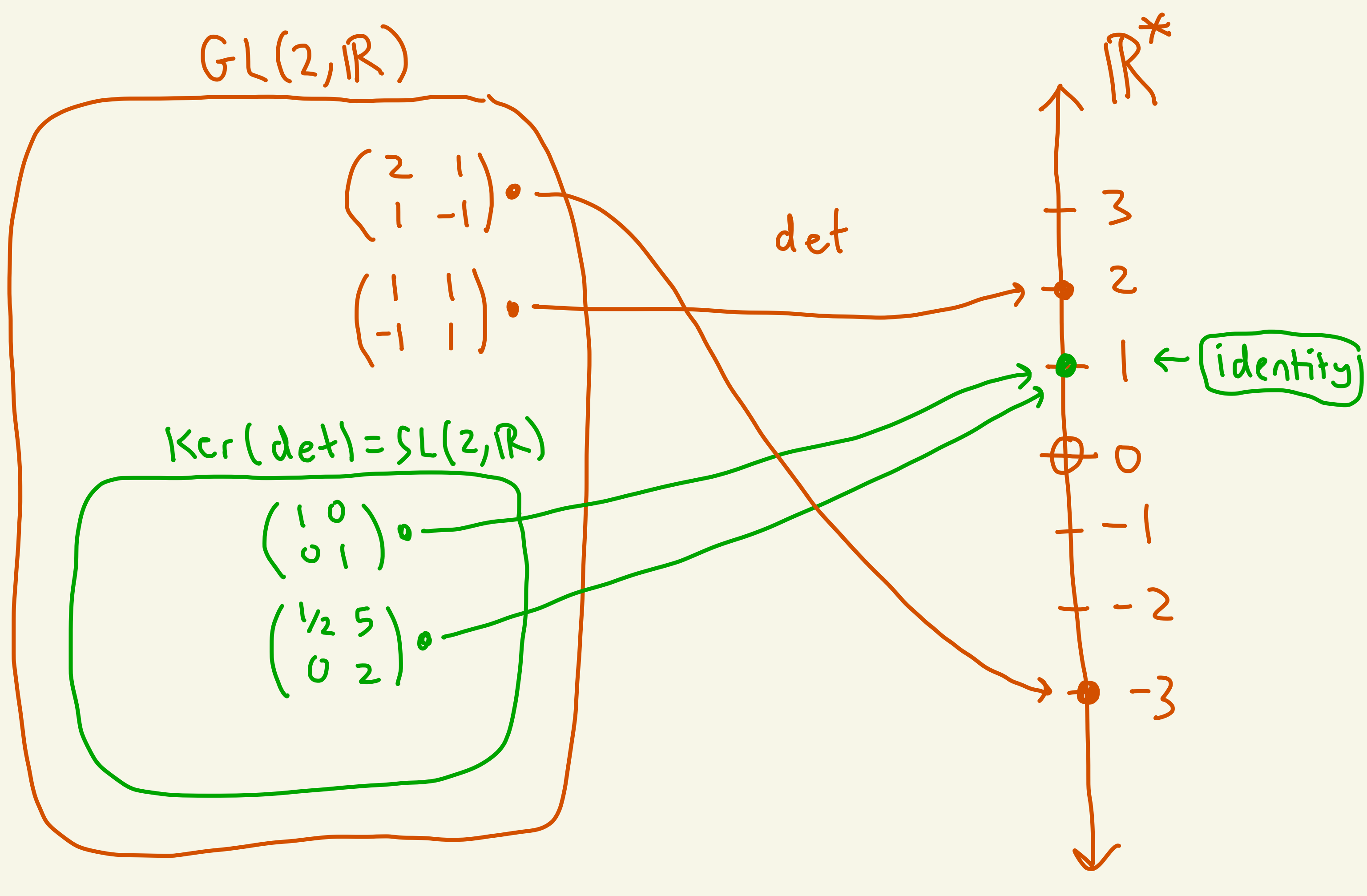
We know det is a homomorphism since

$$\det(AB) = \det(A)\det(B).$$

The kernel is

$$\operatorname{Ker}(\det) = \{ A \in GL(2,\mathbb{R}) \mid \det(A) = 1 \}$$
$$= SL(2,\mathbb{R})$$

Thus, $SL(2,\mathbb{R}) \trianglelefteq GL(2,\mathbb{R})$.



It turns out that if $H \trianglelefteq G$ then the set of left cosets can be made into a group using the operation $(aH)(bH) = (ab)H$.
Since there can be multiple ways to represent a left coset we must make sure this operation is well-defined.

__Theorem:__ Let G be a group and $H \leq G$.
The operation $(aH)(bH) = (ab)H$ on the set of left cosets G/H is well-defined if and only if H is normal.

__Proof:__
($\Leftarrow$) Suppose H is a normal subgroup of G.
Consider $a, b, c, d \in G$ where $aH = cH$ and $bH = dH$.
We must show that $(aH)(bH) = (ab)H$ is equal to $(cH)(dH) = (cd)H$.
Since $aH = cH$ we know $a \in cH$ and so $a = ch_1$ where $h_1 \in H$.
Similarly since $bH = dH$ we have $b = dh_2$ where $h_2 \in H$.
Then, $ab = ch_1dh_2$.

Since H is normal we know $Hd = dH$.
Thus since $h_1 d \in Hd$ we know $h_1 d \in dH$.
Hence $h_1 d = d h_3$ for some $h_3 \in H$.
Thus, $ab = c h_1 d h_2 = c d h_3 h_2 \in cdH$.
Since $ab \in cdH$ we know $abH = cdH$.

($\Leftarrow$) [Skip this direction in class since not used.]

Suppose the operation on left cosets is well-defined, that is if $aH = cH$ and $bH = dH$, then $abH = cdH$.

Let's show that H is normal.

Let $g \in G$ and $h \in H$.
Then, since $hH = eH$ we have

$$g^{-1}H = (eH)(g^{-1}H) \underset{\uparrow}{=} (hH)(g^{-1}H)$$

well-defined operation

$$= hg^{-1}H$$

Thus, $g^{-1}H = hg^{-1}H$.

So, $hg^{-1} \in g^{-1}H$.

Thus, $hg^{-1} = g^{-1}h_1$ where $h_1 \in H$.

So, $ghg^{-1} = h_1 \in H$.

We have shown that $ghg^{-1} \in H$ for any $g \in G$ and $h \in H$.

Hence H is normal. $\blacksquare$

Theorem: Let G be a group and $H \trianglelefteq G$.
Then, G/H is a group under the operation

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

The identity element is $eH = H$
The inverse of aH is $a^{-1}H$.

---

proof:

① Let $a, b \in G$. Then, $ab \in G$.
Thus, $(aH)(bH) = abH \in G/H$.
So, G/H is closed under the operation.

② Let $aH, bH, cH \in G/H$.

Then,

$$(aH)[(bH)(cH)] = [aH][bcH]$$

$$= a(bc)H$$

since G is associative

$$= (ab)cH$$

$$= [abH][cH]$$

$$= [(aH)(bH)](cH)$$

③ Given $aH \in G/H$ we have

$$(aH)(eH) = aeH = aH$$

$$(eH)(aH) = eaH = aH$$

④ Given $aH \in G/H$ we have

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

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

$\blacksquare$

Ex: $D_6 = \{1, r, r^2, s, sr, sr^2\}$

$H = \langle r \rangle = \{1, r, r^2\}$

Left cosets:

$H = \{1, r, r^2\} = rH = r^2H$

$sH = \{s, sr, sr^2\} = srH = sr^2H$

Previously we saw that $H \trianglelefteq D_6$.

So, $D_6/H = \{H, sH\}$ is a group with operation $(aH)(bH) = (ab)H$.

D_6/H	H	sH
H	H	sH
sH	sH	H

$H = 1H$ is the identity.

$(H)(sH) = 1 \cdot sH = sH$

$(sH)(sH) = s^2H = 1H = H$

$(H)(H) = (1H)(1H) = H$

$(sH)(H) = (sH)(1H) = sH$

The powers of sH are:

sH

$(sH)(sH) = s^2H = 1H = H$

Thus, $D_6/H = \langle sH \rangle$ is cyclic.

Since $|D_6/H| = 2$ we know $D_6/H \cong \mathbb{Z}_2$.

Ex: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ is abelian

$H = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$ is a normal subgroup

left cosets:

$\bar{0} + H = \{\bar{0}, \bar{3}\} = \bar{3} + H$

$\bar{1} + H = \{\bar{1}, \bar{4}\} = \bar{4} + H$

$\bar{2} + H = \{\bar{2}, \bar{5}\} = \bar{5} + H$

$$\boxed{\mathbb{Z}_6/H = \{\bar{0}+H, \bar{1}+H, \bar{2}+H\}}$$

this is a group with operation

$(\bar{a}+H) + (\bar{b}+H) = (\bar{a}+\bar{b}) + H$

identity: $\bar{0}+H$

Here's the group table.

$\mathbb{Z}_6/H$	$\bar{0}+H$	$\bar{1}+H$	$\bar{2}+H$
$\bar{0}+H$	$\bar{0}+H$	$\bar{1}+H$	$\bar{2}+H$
$\bar{1}+H$	$\bar{1}+H$	$\bar{2}+H$	$\bar{0}+H$
$\bar{2}+H$	$\bar{2}+H$	$\bar{0}+H$	$\bar{1}+H$

some example calculations

$(\bar{0}+H) + (\bar{2}+H) = (\bar{0}+\bar{2}) + H = \bar{2}+H$

$(\bar{1}+H) + (\bar{1}+H) = (\bar{1}+\bar{1}) + H = \bar{2}+H$

$(\bar{1}+H) + (\bar{2}+H) = \bar{3}+H = \bar{0}+H$

$(\bar{2}+H) + (\bar{2}+H) = \bar{4}+H = \bar{1}+H$

Note that the "powers" of $\bar{1}+H$ are:

$\bar{1}+H$

$(\bar{1}+H)+(\bar{1}+H)=\bar{2}+H$

$(\bar{1}+H)+(\bar{1}+H)+(\bar{1}+H)=\bar{3}+H=\bar{0}+H$

Thus, $\mathbb{Z}_6/H=\langle \bar{1}+H\rangle$ is cyclic.

Since $|\mathbb{Z}_6/H|=3$ we have $\mathbb{Z}_6/H\cong\mathbb{Z}_3$.

Ex: Consider

$G = \mathbb{Z}_4 \times \mathbb{Z}_2 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{2},\bar{0}), (\bar{2},\bar{1}), (\bar{3},\bar{0}), (\bar{3},\bar{1})\}$

$H = \langle(\bar{2},\bar{0})\rangle = \{(\bar{2},\bar{0}), (\bar{0},\bar{0})\}$.

G is abelian, thus $H \trianglelefteq G$.

The left cosets are

$(\bar{0},\bar{0}) + H = \{(\bar{0},\bar{0}), (\bar{2},\bar{0})\}$
$(\bar{1},\bar{0}) + H = \{(\bar{1},\bar{0}), (\bar{3},\bar{0})\}$
$(\bar{0},\bar{1}) + H = \{(\bar{0},\bar{1}), (\bar{2},\bar{1})\}$
$(\bar{1},\bar{1}) + H = \{(\bar{1},\bar{1}), (\bar{3},\bar{1})\}$

So,
$\mathbb{Z}_4 \times \mathbb{Z}_2 / H = \{(\bar{0},\bar{0})+H, (\bar{1},\bar{0})+H, (\bar{0},\bar{1})+H, (\bar{1},\bar{1})+H\}$

has order 4. With identity $(\bar{0},\bar{0})+H$.

Is $\mathbb{Z}_4 \times \mathbb{Z}_2 / H$ cyclic?

Let's check the orders.

$(\bar{0},\bar{0})+H$

order 1

$(\bar{1},\bar{0})+H$

$[(\bar{1},\bar{0})+H] + [(\bar{1},\bar{0})+H] = (\bar{2},\bar{0})+H = (\bar{0},\bar{0})+H$

order 2.

$(\bar{0},\bar{1})+H$

$[(\bar{0},\bar{1})+H]+[(\bar{0},\bar{1})+H]=(\bar{0},\bar{2})+H=(\bar{0},\bar{0})+H$

order 2.

$(\bar{1},\bar{1})+H$

$[(\bar{1},\bar{1})+H]+[(\bar{1},\bar{1})+H]=(\bar{2},\bar{2})+H=(\bar{2},\bar{0})+H=(\bar{0},\bar{0})+H$

order 2.

So, $\mathbb{Z}_4\times\mathbb{Z}_2/H$ is not cyclic.

It is abelian (by HW) since $\mathbb{Z}_4\times\mathbb{Z}_2$ is abelian.