Math 4550
Homework 6
Solutions

1 (a) $\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}\}$

$H = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$

left cosets

$\bar{0} + H = \{\bar{0}, \bar{4}, \bar{8}\}$

$\bar{1} + H = \{\bar{1}, \bar{5}, \bar{9}\}$

$\bar{2} + H = \{\bar{2}, \bar{6}, \overline{10}\}$

$\bar{3} + H = \{\bar{3}, \bar{7}, \overline{11}\}$

right cosets

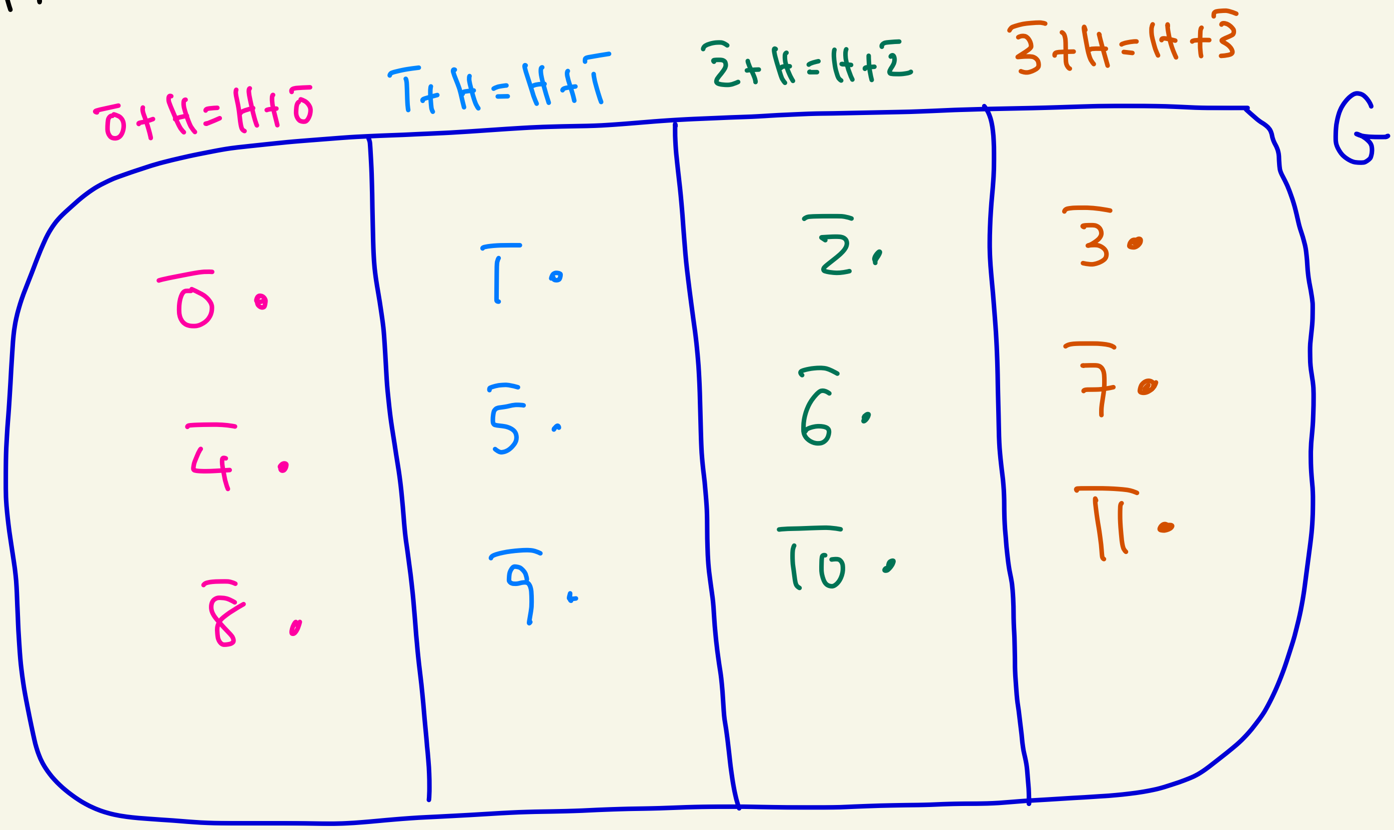
$H + \bar{0} = \{\bar{0}, \bar{4}, \bar{8}\}$

$H + \bar{1} = \{\bar{1}, \bar{5}, \bar{9}\}$

$H + \bar{2} = \{\bar{2}, \bar{6}, \overline{10}\}$

$H + \bar{3} = \{\bar{3}, \bar{7}, \overline{11}\}$

The left and right cosets are the same.
The subgroup H is normal.



$\boxed{1(b)}$ $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

Recall:
$r^4 = 1,\ s^2 = 1$
$r^k s = s r^{-k}$
$= s r^{4-k}$

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

left cosets

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

$rH = \{r, r^3\}$

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

$srH = \{sr, sr^3\}$

right cosets

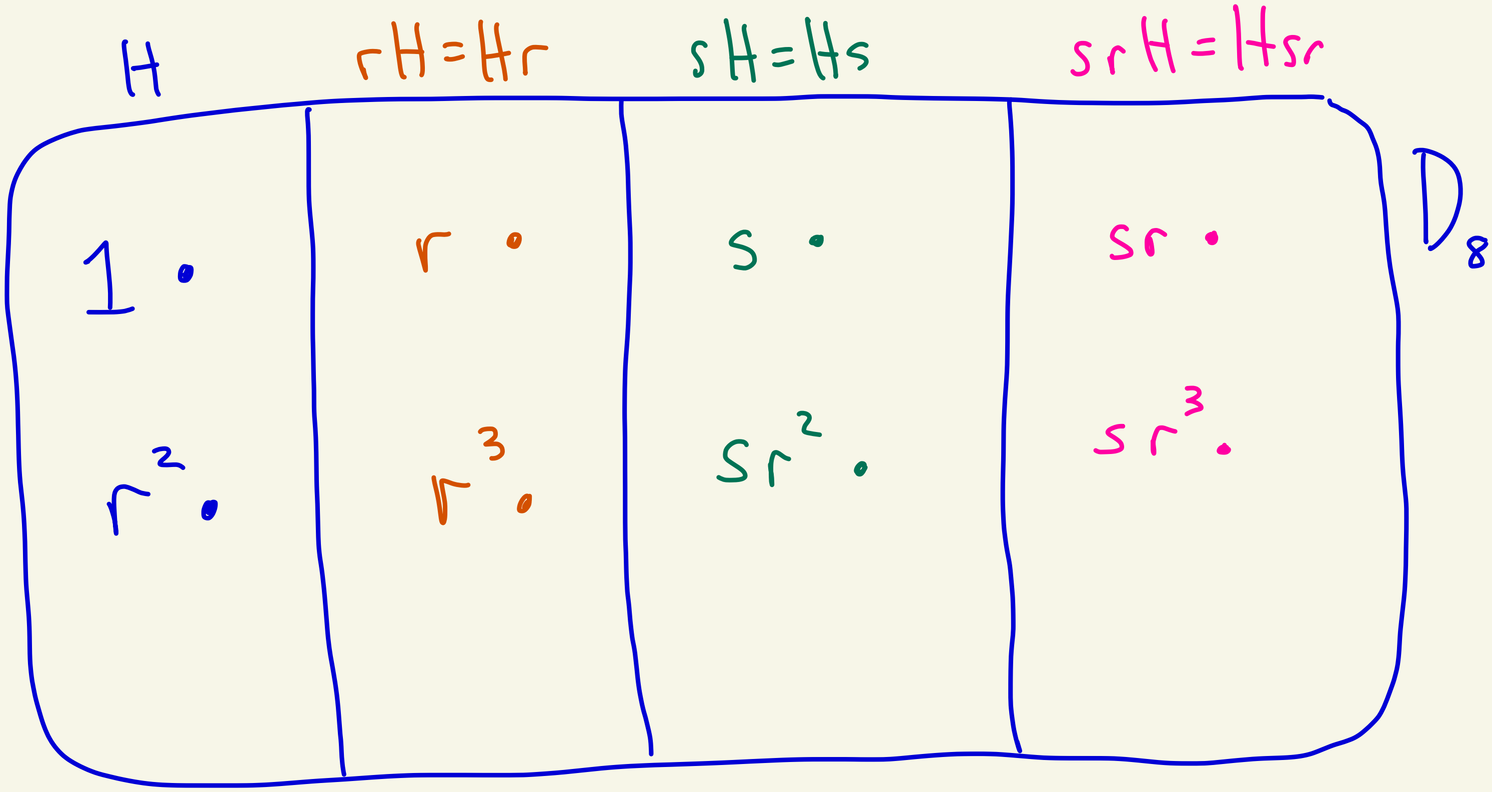
$H = \{1, r^2\}$

$Hr = \{r, r^3\}$

$Hs = \{s, r^2 s\} = \{s, sr^{-2}\} = \{s, sr^2\}$

$Hsr = \{sr, r^2 sr\} = \{sr, sr^{-2} r\}$
$= \{sr, sr^{-1}\} = \{sr, sr^3\}$

The left and right cosets are the same.
Thus H is a normal subgroup of D_8.



1 (c)

Recall:

$r^4 = 1, \; s^2 = 1$

$r^k s = s r^{-k}$
$= s r^{4-k}$

$D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

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

left cosets

$H = \{1, s\}$

$rH = \{r, rs\} = \{r, sr^{-1}\} = \{r, sr^3\}$

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

$r^3H = \{r^3, r^3s\} = \{r^3, sr^{-3}\} = \{r^3, sr\}$

right cosets

$H = \{1, s\}$

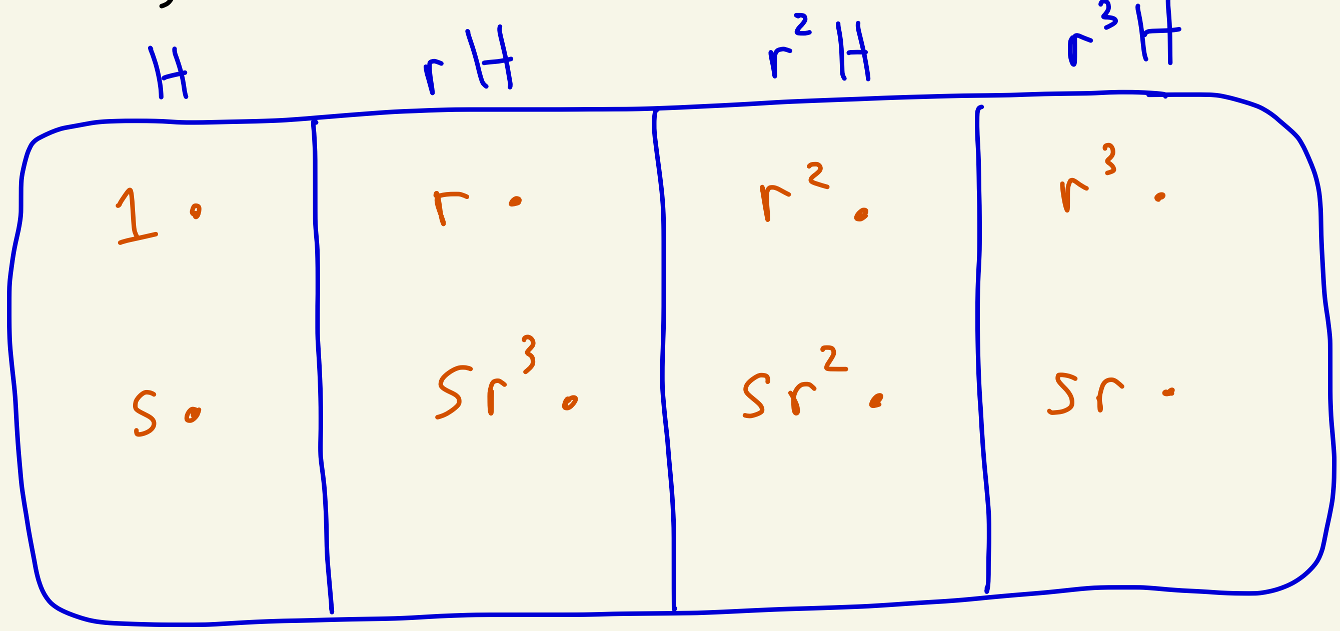
$Hr = \{r, sr\}$

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

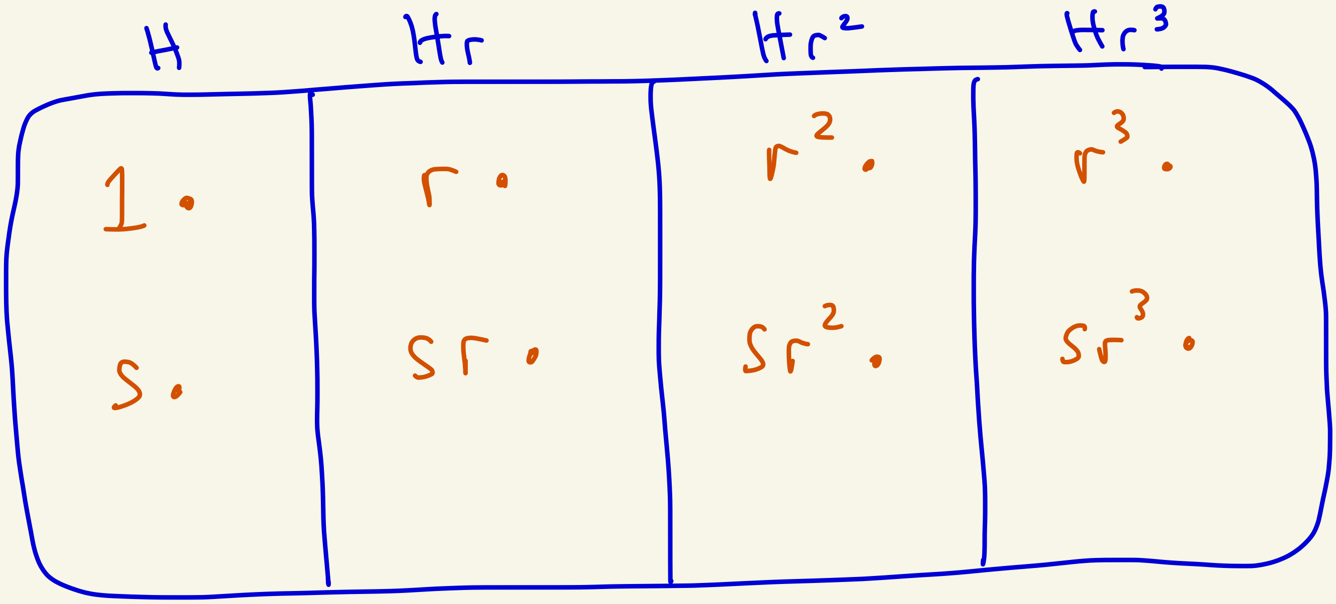
$Hr^3 = \{r^3, sr^3\}$

The left and right cosets differ so H is not normal.

Let's see the two partitions created by drawing them.



partition of D_8 by the left cosets of H



partition of D_8 by the right cosets of H

2

(a) From problem 1 we got that

$$\mathbb{Z}_{12}/H = \{\bar{0}+H, \bar{1}+H, \bar{2}+H, \bar{3}+H\}$$

where

$$\bar{0}+H = \{\bar{0},\bar{4},\bar{8}\} = \bar{4}+H = \bar{8}+H$$
$$\bar{1}+H = \{\bar{1},\bar{5},\bar{9}\} = \bar{5}+H = \bar{9}+H$$
$$\bar{2}+H = \{\bar{2},\bar{6},\overline{10}\} = \bar{6}+H = \overline{10}+H$$
$$\bar{3}+H = \{\bar{3},\bar{7},\overline{11}\} = \bar{7}+H = \overline{11}+H$$

The identity element is $\bar{0}+H$.

(b)

$$(\bar{2}+H)+(\bar{3}+H) = \bar{5}+H = \boxed{\bar{1}+H}$$

Since

$$(\bar{1}+H)+(\bar{3}+H) = \bar{4}+H = \bar{0}+H \leftarrow$$

$\bar{0}+H$ is the identity element

the inverse of $\bar{3}+H$ is $\bar{1}+H$.

$\boxed{\text{(c)}}$

<u>order of $\bar{1}+H$</u>

$\bar{1}+H \neq \bar{0}+H$

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

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

$(\bar{1}+H)+(\bar{1}+H)+(\bar{1}+H)+(\bar{1}+H) = \bar{4}+H = \bar{0}+H \leftarrow$ identity element

Thus, $\bar{1}+H$ has order 4.

<u>order of $\bar{2}+H$</u>

$\bar{2}+H \neq \bar{0}+H$

$(\bar{2}+H)+(\bar{2}+H) = \bar{4}+H = \bar{0}+H \leftarrow$ identity element

Thus, $\bar{2}+H$ has order 2.

$\boxed{\text{(d)}}$

Since $\mathbb{Z}_{12}$ is abelian, from a problem in this HW set, $\mathbb{Z}_{12}/H$ is abelian.

From part (c) we have that

$\langle \bar{1}+H \rangle = \{\bar{1}+H, \bar{2}+H, \bar{3}+H, \bar{4}+H\} = \mathbb{Z}_{12}/H.$

Thus, $\mathbb{Z}_{12}/H$ is cyclic with $\bar{1}+H$ as a generator.

3

(a) From problem 1 we get that

$$D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$
$$H = \langle r^2 \rangle = \{1, r^2\}$$

<u>left cosets</u>:

$$H = \{1, r^2\} = r^2 H$$
$$rH = \{r, r^3\} = r^3 H$$
$$sH = \{s, sr^2\} = sr^2 H$$
$$srH = \{sr, sr^3\} = sr^3 H$$

So,

$$D_8/H = \{H, rH, sH, srH\}$$

The identity element is $H = 1H$.

(b)

$$(rH)(sH) = rsH = sr^{-1}H = sr^3 H = srH$$

$$(srH)(srH) = (sr)(sr)H = ssr^{-1}r = s^2 H = 1H = H$$

(c)

Since

$$(rH)(rH) = r^2H = H$$

We know that

$$(rH)^{-1} = rH$$

Since

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

we know that

$$(sH)^{-1} = H.$$

(d)

$H \leftarrow$ identity

H has order 1

$sH \neq H$

$(sH)(sH) = s^2H = H \leftarrow$ identity

So, sH has order 2

identity

$rH \neq H$

$(rH)(rH) = r^2H = H$

So, rH has order 2

see part (b)

$srH \neq H$

$(srH)(srH) = srsrH = H$

identity

So, srH has order 2

$\boxed{(e)}$

From (d) there are no elements of D_8/H that have order 4.

So no element will generate all of $D_8/H = \{H, rH, sH, srH\}$

Thus, D_8/H is not cyclic.

④

(a) $G = \mathbb{Z}_3 \times \mathbb{Z}_3 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2}),$
$(\bar{2},\bar{0}), (\bar{2},\bar{1}), (\bar{2},\bar{2})\}$

$$H = \langle (\bar{0},\bar{1}) \rangle = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2})\}$$

left cosets:

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

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

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

So,

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

The identity element is $(\bar{0},\bar{0}) + H$

(b)

$$[(\bar{1},\bar{2}) + H] + [(\bar{1},\bar{1}) + H] = (\bar{2},\bar{3}) + H \overset{\text{mod } 3}{=} (\bar{2},\bar{0}) + H$$

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

$\boxed{(c)}$

Note that
$$(\bar{1},\bar{2})+H = (\bar{1},\bar{0})+H \leftarrow \boxed{\text{from part (a)}}$$

So we can instead find the inverse of $(\bar{1},\bar{0})+H$.

We have that:
$$[(\bar{1},\bar{0})+H]+[(\bar{2},\bar{0})+H] = (\bar{3},\bar{0})+H = (\bar{0},\bar{0})+H$$

mod 3

Thus, the inverse of $(\bar{1},\bar{2})+H = (\bar{1},\bar{0})+H$ is $(\bar{2},\bar{0})+H$.

Now let's look at $(\bar{2},\bar{2})+H$.

From part (a) we get
$$(\bar{2},\bar{2})+H = (\bar{2},\bar{0})+H$$

And above we found that the inverse of $(\bar{2},\bar{0})+H$ is $(\bar{1},\bar{0})+H$.

$\boxed{(d)}$

$(\bar{0},\bar{0})+H$ is the identity so it has order 1.

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

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

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

these are not the identity

$(\bar{1},\bar{0})+H$ is the identity so it has order 3

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

$[(\bar{2},\bar{0})+H]+[(\bar{2},\bar{0})+H]=(\bar{4},\bar{0})+H=(\bar{1},\bar{0})+H$

$[(\bar{2},\bar{0})+H]+[(\bar{2},\bar{0})+H]+[(\bar{2},\bar{0})+H]=(\bar{6},\bar{0})+H=(\bar{0},\bar{0})+H$

not the identity

$(\bar{2},\bar{0})+H$ is the identity so it has order 3

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

$\boxed{\text{(e)}}$ $G/H = \{(\bar{0},\bar{0})+H, (\bar{1},\bar{0})+H, (\bar{2},\bar{0})+H\}$

Thus, G/H has size 3.

The generators are the elements of order 3. There are two of them:

$$\left.\begin{array}{l}(\bar{1},\bar{0})+H \\ (\bar{2},\bar{0})+H\end{array}\right\} \text{both of these generate } G/H$$

So, G/H is cyclic.

$\boxed{5(a)}$ Let e be the identity element of G.

($\Rightarrow$) Suppose that $aH = bH$.

Since $H \leq G$ we know that $e \in H$.

Thus, $a = ae \in aH$.

recall that $xH = \{xh \mid h \in H\}$

Since $aH = bH$ and $a \in aH$ we know that $a \in bH$.

($\Leftarrow$) Suppose that $a \in bH$.

Thus, $a = bh$ where $h \in H$.

Let's show that $aH = bH$.

First we show that $aH \subseteq bH$.

Let $c \in aH$.

Then, $c = ah_1$ where $h_1 \in H$.

Thus,

$$c = ah_1 = bhh_1 = b(\underbrace{hh_1}) \in bH$$

this is in H because $H \leq G$ and so H is closed under the group operation

Hence $c \in bH$.

Therefore, $aH \subseteq bH$.

Now we show that $bH \subseteq aH$

Let $d \in bH$.

Then, $d = bh_2$ where $h_2 \in H$.

So,

$$d = bh_2 \underset{\substack{\uparrow \\ \boxed{\substack{a=bh \\ \text{gives} \\ ah^{-1}=b}}}}{=} ah^{-1}h_2 = a(h^{-1}h_2) \in aH$$

$h^{-1} \in H$ since $h \in H$ and $H \leq G$

$h^{-1}h_2 \in H$ since $h^{-1}, h_2 \in H$ which gives $h^{-1}h_2 \in H$ since $H \leq G$

Thus, $d \in aH$

So, $bH \subseteq aH$.

Since $aH \subseteq bH$ and $bH \subseteq aH$ we know that $aH = bH$.

$\blacksquare$

5(b) Just use part (a).

We have that

$aH = bH$

iff $a \in bH$ — from part (a)

iff $a = bh$ for some $h \in H$ — since $bH = \{bh \mid h \in H\}$

$\blacksquare$

5(c)

Define $f: H \to aH$ by $f(h) = ah$.
Let's show that f is one-to-one and onto.

<u>f is one-to-one:</u>

Suppose $f(h_1) = f(h_2)$.
Then, $ah_1 = ah_2$.
So, $a^{-1}ah_1 = a^{-1}ah_2$.
Thus, $h_1 = h_2$.
Hence f is one-to-one.

<u>f is onto:</u>

Let $x \in aH$.
Then, $x = ah$ for some $h \in H$.
And $f(h) = ah = x$
Thus, f is onto.

Since f is one-to-one and onto
we know that H and aH
have the same size.
That is, $|H| = |aH|$.

⑥ Let $|G| = pq$ where p and q are primes.

Let $H \leq G$.

By Lagranges theorem we know that
$|H|$ divides $|G|$.

Thus, $|H| = 1, p, q,$ or pq. ← since p and q are primes

Since $H \neq G$ we know $|H| \neq pq$.

Thus, $|H| = 1, p,$ or q.

If $|H| = 1$, then $H = \{e\}$.

Then $H = \langle e \rangle$ is cyclic.

If $|H| = p$, then by a theorem from class since p is prime we must have that H is cyclic.

If $|H| = q$, then by a theorem from class since q is prime we must have that H is cyclic.

In all three cases we have that H is cyclic.

$\boxed{//}$

7) Let $|G| = n$.

Suppose that $x \in G$.

Consider the subgroup

$$H = \langle x \rangle$$

generated by x.

Recall from class that the order of x is $|\langle x \rangle| = |H|$.

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

Thus, $n = |H| \cdot k$ for some integer $k \geq 1$

Hence,

$$x^n = x^{|H| \cdot k} = \left(x^{|H|}\right)^k = e^k = e$$

$|H|$ is the order of x

Thus, $x^n = e$

$\blacksquare$

8 (a) Suppose G is abelian.

Let $x, y \in G/H$.

Then, $x = aH$ and $y = bH$ for some $a, b \in G$.

So,

$$xy = (aH)(bH) = (ab)H = (ba)H = (bH)(aH) = yx$$

def of operation in G/H

since G is abelian

Hence $xy = yx$.

So, G/H is abelian. ▨

8 (b)

def of G/H operation

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

identity element of G/H

we know that $(aH)^{-1} = a^{-1}H$

8(c)

Let $k \in \mathbb{Z}$.

If $k=0$, then $(aH)^0 \overset{\text{def of } (aH)^0}{=} eH = a^0 H$

If $k \geq 1$, then

$$(aH)^k = \underbrace{(aH)(aH)\cdots(aH)}_{k \text{ times}} \overset{\text{def of } G/H \text{ operation}}{=} a^k H$$

If $k \leq -1$, then

$$(aH)^k = \underbrace{(aH)^{-1}(aH)^{-1}\cdots(aH)^{-1}}_{-k \text{ times}}$$

$$\overset{\text{part (b)}}{=} \underbrace{(a^{-1}H)(a^{-1}H)\cdots(a^{-1}H)}_{-k \text{ times}}$$

$$= (a^{-1})^{-k} H$$

$$= a^k H.$$

We have show that $(aH)^k = a^k H$ for all the cases of k.

$\boxed{///}$

8 (d) Let G be cyclic.

Then, $G = \langle g \rangle$ for some $g \in G$.

Let's show that gH generates G/H.

Let $x \in G/H$.

Then $x = aH$ for some $a \in G$.

Since $a \in G$ and $G = \langle g \rangle$ we have that $a = g^k$ for some $k \in \mathbb{Z}$.

Therefore,

$$x = aH = g^k H \underset{\text{part (c)}}{=} (gH)^k$$

Hence, $G/H = \langle gH \rangle$.

So, G/H is cyclic.

$\boxed{///}$

9. Suppose that $H \trianglelefteq G$ and $K \trianglelefteq G$.

We showed that $H \cap K \leq G$ is HW 2.
So we just have to show that $H \cap K$ is normal.

Let $g \in G$ and $a \in H \cap K$.
We need to show that $gag^{-1} \in H \cap K$.

From class:
Let $N \leq G$.
Then N is normal iff $gng^{-1} \in N$ for all $n \in N$ and $g \in G$

Since $a \in H \cap K$ we know that $a \in H$ and $a \in K$.

Since $g \in G$ and $a \in H$ and H is normal we know that $gag^{-1} \in H$.

Since $g \in G$ and $a \in K$ and K is normal we know that $gag^{-1} \in K$.

Thus, $gag^{-1} \in H \cap K$.

Therefore, $H \cap K \trianglelefteq G$. $\blacksquare$

(10) $\varphi: G_1 \to G_2$ is a homomorphism.

Let e_1 and e_2 be the identity elements of G_1 and G_2 respectively.

Recall that
$$\ker(\varphi) = \{x \mid x \in G_1 \text{ and } \varphi(x) = e_2\}$$

From HW 4 we know that $\ker(\varphi)$ is a subgroup of G_1.

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

Let $H = \ker(\varphi)$.

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

We need to show that $ghg^{-1} \in H$.

From class: Let $H \leq G$. Then: H is normal iff $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$

Since $h \in H$ and $H = \ker(\varphi)$ we know that $\varphi(h) = e_2$

Thus,

since φ is a homomorphism

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

$= \varphi(e_1)$ HW 4

$= e_2$

Thus, $\varphi(ghg^{-1}) = e_2$.

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

Hence $\ker(\varphi) \trianglelefteq G_1$. $\blacksquare$

11 Let $H \leq G$ and G be finite.

From class, to show that $H \trianglelefteq G$ we can show that $gHg^{-1} = H$ for all $g \in G$ where

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

Let $g \in G$.

Let's show that $gHg^{-1} = H$.

Define $\varphi_g : H \to G$ by $\varphi_g(h) = ghg^{-1}$.

Note that φ_g is a homomorphism because

$$\begin{aligned}\varphi_g(h_1h_2) &= gh_1h_2g^{-1} \\ &= gh_1g^{-1}gh_2g^{-1} \\ &= \varphi_g(h_1)\varphi_g(h_2).\end{aligned}$$

Note that

$$\begin{aligned}\mathrm{im}(\varphi_g) &= \{\varphi_g(h) \mid h \in H\} \\ &= \{ghg^{-1} \mid h \in H\}\end{aligned}$$

$$= gHg^{-1}$$

Also note that φ_g is one-to-one because if $\varphi_g(a) = \varphi_g(b)$ then $gag^{-1} = gbg^{-1}$ and so $g^{-1}(gag^{-1})g = g^{-1}(gbg^{-1})g$ which gives $a = b$.

Also recall from HW 4 / class that $\mathrm{im}(\varphi_g) \leq G$.

Thus, $gHg^{-1} \leq G$.

Since φ_g is one-to-one we get that $|H| = |\mathrm{im}(\varphi_g)| = |gHg^{-1}|$.

Since H is the only subgroup of G of size $|H|$ and $gHg^{-1} \leq G$ we know that $H = gHg^{-1}$.

Thus, H is normal.