Problem set 1

1) S does become a group with the given binary operation.

<u>Identity</u>: $a * 0 = a + 0 + a \cdot 0 = a$

$0 * a = 0 + a + 0 \cdot a = a.$

Thus, 0 is the identity for the given binary operation.

<u>Inverses</u>: Given $a \in S$, we want to find some $x \in S$ such that $a * x = 0$.

$a * x = a + x + ax = a + x(1+a)$

So, if $a * x = 0$, we must have $x = \frac{-a}{1+a}$.

We verify that $\left(\frac{-a}{1+a}\right)$ is the inverse of a:

$$a * \left(\frac{-a}{1+a}\right) = a + \left(\frac{-a}{1+a}\right) + \frac{a(-a)}{1+a}$$

$$= \frac{a(1+a) - a - a^2}{(1+a)} = 0.$$

$$\left(\frac{-a}{1+a}\right) * a = \left(\frac{-a}{1+a}\right) + a + \frac{(-a)a}{1+a} = 0$$

[Note: $\left(\frac{-a}{1+a}\right)$ is defined as $a \neq -1$.]

We need to ensure that $\frac{-a}{1+a} \in S$ if $a \in S$.

Suppose $\frac{-a}{1+a}$ (which is in $\mathbb{R}$) is not in S.

Then $\frac{-a}{1+a} = -1$, i.e. $a = a+1$.

which is not possible.

Thus, every element $a \in S$ has an inverse in S.

<u>Associativity</u> We want to show that if $a, b, c \in S$, then $(a*b)*c = a*(b*c)$.

$a*b = a+b+ab$

$(a*b)*c = (a+b+ab) + c + (a+b+ab)c$

$= a+b+c+ab+bc+ca+abc.$

$b*c = b+c+bc$

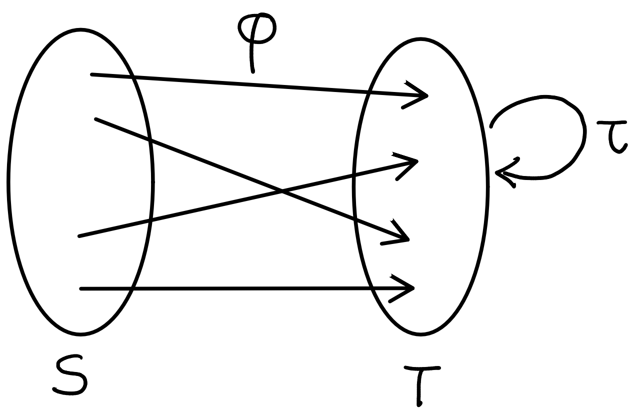
$a*(b*c) = a+(b+c+bc) + a(b+c+bc)$

$= a+b+c+ab+bc+ca+abc.$

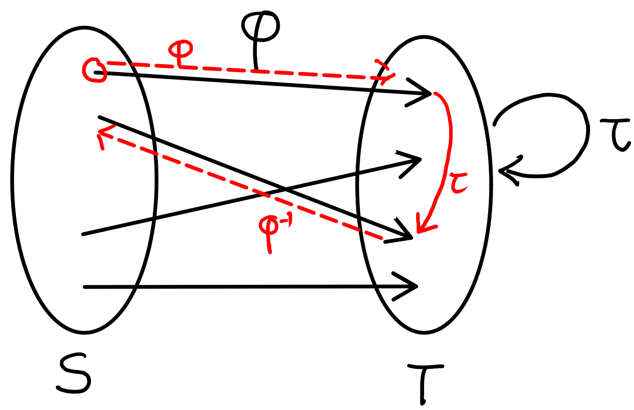
Thus, $(a*b)*c = a*(b*c)$

Thus, we see that S is a group under the given binary operation.

2) Let $\varphi : S \to T$ be a 1-1 correspondence.



Let $\tau \in \mathrm{Perm}(T)$. Thus, τ is a 1-1 correspondence from T to itself.



Then $\varphi^{-1} \circ \tau \circ \varphi$ is a 1-1 correspondence from S to itself. (Composition of 1-1 correspondences is a 1-1 correspondence.)

So, we define a function $f : \mathrm{Perm}(T) \longrightarrow \mathrm{Perm}(S)$ defined by $f(\tau) = \varphi^{-1} \circ \tau \circ \varphi$.

<u>f is a group homomorphism</u>

To see this, we take $\tau_1, \tau_2 \in \mathrm{Perm}(T)$ and show that $f(\tau_1 \tau_2) = f(\tau_1) f(\tau_2)$

$$\begin{aligned} f(\tau_1) f(\tau_2) &= \varphi^{-1} \tau_1 \varphi \varphi^{-1} \tau_2 \varphi \\ &= \varphi^{-1} \tau_1 \tau_2 \varphi \qquad (\text{as } \varphi \varphi^{-1} = id_T) \\ &= f(\tau_1 \tau_2). \end{aligned}$$

<u>f is a 1-1 correspondence</u>

This can be proved in two ways:

<u>Proof 1</u>

Let us first show that f is a one-to-one function.

Suppose $f(\tau_1) = f(\tau_2)$ for $\tau_1, \tau_2 \in \mathrm{Perm}(T)$

Then $\varphi^{-1} \tau_1 \varphi = \varphi^{-1} \tau_2 \varphi$

So $\varphi(\varphi^{-1} \tau_1 \varphi) \varphi^{-1} = \varphi(\varphi^{-1} \tau_2 \varphi) \varphi^{-1}$

So $\tau_1 = \tau_2$.

Thus f is one-to-one.

Now, we show that f is onto.

Let $\sigma \in \mathrm{Perm}(S)$. We want to show that there exists some $\tau \in \mathrm{Perm}(T)$ such that $\varphi^{-1}\tau\varphi = \sigma$.

Rough work

$\varphi^{-1}\tau\varphi = \sigma$

$\varphi(\varphi^{-1}\tau\varphi)\varphi^{-1} = \varphi\sigma\varphi^{-1}$

$\tau = \varphi\sigma\varphi^{-1}$

Still need to verify that $f(\varphi\sigma\varphi^{-1}) = \sigma$

We choose $\tau = \varphi\sigma\varphi^{-1}$.
Observe that $\tau \in \mathrm{Perm}(T)$

$$f(\tau) = \varphi^{-1}(\varphi\sigma\varphi^{-1})\varphi = \sigma.$$

Thus, f is onto.
Thus f is a 1-1 correspondence.

<u>Proof 2</u> We define $g : \mathrm{Perm}(S) \to \mathrm{Perm}(T)$ by $g(\sigma) = \varphi \circ \sigma \circ \varphi^{-1}$

Then
$$f \circ g(\sigma) = \varphi^{-1} g(\sigma)\varphi = \varphi^{-1}(\varphi\sigma\varphi^{-1})\varphi = \sigma.$$

Thus, $f \circ g = id_{\mathrm{Perm}(S)}$

$$g \circ f(\tau) = \varphi\, f(\tau)\, \varphi^{-1} = \varphi(\varphi^{-1}\tau\varphi)\varphi^{-1} = \tau$$

Thus $g \circ f = id_{\mathrm{Perm}(T)}$

Thus g is the inverse function of f.
Thus f is a 1-1 correspondence (since only 1-1 correspondences have inverses).

Thus, f is a group isomorphism.

3) First we prove that <u>f is a group homomorphism</u>.

Let $g_1, g_2 \in G$

$$f(g_1 g_2) = h g_1 g_2 h^{-1} = h g_1 (h^{-1} h) g_2 h^{-1}$$
$$= (h g_1 h^{-1})(h g_2 h^{-1})$$
$$= f(g_1) \cdot f(g_2)$$

<u>f is a one-to-one function</u>

Suppose $f(g_1) = f(g_2)$.

So $h g_1 h^{-1} = h g_2 h^{-1}$

$\Rightarrow h^{-1}(h g_1 h^{-1}) h = h^{-1}(h g_2 h^{-1}) h$

$\Rightarrow g_1 = g_2$

Thus f is a one-to-one function.

<u>f is an onto function</u>

Let $g \in G$. We want to find some g' such that $f(g') = g$, i.e. $h g' h^{-1} = g$

$h g' h^{-1} = g$
$\iff g' = h^{-1} g h$
Try this out.

We take $g' = h^{-1} g h$.

Then $f(g') = h (h^{-1} g h) h^{-1}$
$= g$.

Thus, f is onto.

(Also see solution of Problem 2).

4) Compute the multiplication table for this set.

$5 \cdot 5 \equiv 25 \mod 40$ | $15 \cdot 5 \equiv 35 \mod 40$

$5 \cdot 15 \equiv 75 \equiv 35 \mod 40$ | $15 \cdot 15 \equiv 25 \mod 40$

$5 \cdot 25 \equiv 125 \equiv 5 \mod 40$ | $15 \cdot 25 \equiv 15 \mod 40$

$5 \cdot 35 \equiv 175 \equiv 15 \mod 40$ | $15 \cdot 35 \equiv 5 \mod 40$

$25 \cdot 5 \equiv 5 \mod 40$ | $35 \cdot 5 \equiv 15 \mod 40$

$25 \cdot 15 \equiv 15 \mod 40$ | $35 \cdot 15 \equiv 5 \mod 40$

$25 \cdot 25 \equiv 25 \mod 40$ | $35 \cdot 25 \equiv 35 \mod 40$

$25 \cdot 35 \equiv 35 \mod 40$ | $35 \cdot 35 \equiv 25 \mod 40$

Thus, we see that this set is closed under multiplication.

Also, we see that $x \cdot 25 \equiv x \mod 40$ for any $x \in \{5, 15, 25, 35\}$.
Thus, 25 is the identity.

Also, for any $x \in \{5, 15, 25, 35\}$,
$x^2 \equiv 25 \mod 40$.
Thus, every element has an inverse. In fact, every element is its own inverse.

The binary operation is associative since multiplication modulo 40 is associative.

5) Let $x, y \in G$. We want to show that $xy = yx$.

We know that $(xy)^{-1} = y^{-1}x^{-1}$.
(Indeed $(xy)\cdot(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1$.)

However, we are given that $(xy)^{-1} = x^{-1}y^{-1}$
(taking $a=x$, $b=y$).
So $y^{-1}x^{-1} = x^{-1}y^{-1}$.

Taking inverses of both sides, we get
$(x^{-1})^{-1}(y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1}$

So $xy = yx$.
Thus, G is abelian.

6) We use the Euclidean algorithm to compute the gcd of 37 and 20.

$$\begin{aligned}
37 &= 20\cdot 1 + \underline{17} \\
20 &= 17\cdot 1 + \underline{3} \\
17 &= 3\cdot 5 + \underline{2} \\
3 &= 2\cdot 1 + \underline{1} \\
2 &= 1\cdot 2 + 0
\end{aligned}
\qquad
\begin{aligned}
17 &= 37 - 20\cdot 1 \\
3 &= 20 - 17 = 20\cdot 2 - 37 \\
2 &= (37 - 20\cdot 1) - (20\cdot 2 - 37)\cdot 5 \\
&= 37\cdot 6 - 20\cdot 11 \\
1 &= (20\cdot 2 - 37) - (37\cdot 6 - 20\cdot 11) \\
&= 20\cdot 13 - 37\cdot 7
\end{aligned}$$

gcd(37,20)

Thus, $20\cdot 13 - 37\cdot 7 = 1$.
So, $20\cdot \underline{13} \equiv 1 \mod 37$

7) We use the Euclidean algorithm to find the gcd of 31 and 101.

$$\begin{aligned} 101 &= 31\cdot 3 + 8 \\ 31 &= 8\cdot 3 + 7 \\ 8 &= 7\cdot 1 + \underset{\uparrow}{\underline{\underline{1}}} \\ 7 &= 1\cdot 7 + 0 \end{aligned}$$

gcd(101, 31)

$$\begin{aligned} 8 &= 101 - 31\cdot 3 \\ 7 &= 31 - (101 - 31\cdot 3)\cdot 3 = 31\cdot 10 - 101\cdot 3 \\ 1 &= (101 - 31\cdot 3) - (31\cdot 10 - 101\cdot 3) \\ &= 101\cdot 4 - 31\cdot 13 \end{aligned}$$

Thus $101\cdot \underline{\underline{4}} - 31\cdot \underline{\underline{13}} = 1$

8) We know that $|U(27)| = \varphi(27) = 3^3 - 3^2 = 18$.

So, we want to find an element of order 18.

We try out $\bar{2}$.

Powers of $\bar{2}$:

n	1	2	3	4	5	6	7	8	9
$\bar{2}^n$	2	4	8	16	5	10	20	13	26

$\text{ord}(\bar{2}) \mid 18$. So $\text{ord}(\bar{2}) = 1, 2, 3, 6, 9$ or 18.

The above table shows that $\text{ord}(\bar{2})$ is not $1, 2, 3, 6$ or 9. So $\text{ord}(\bar{2}) = 18$.

Thus $\langle \bar{2} \rangle = U(27)$ and so $U(27)$ is a cyclic group.

(If $\bar{2}$ had not worked, we would have tried other elements. If none had turned out to be a generator, we would have concluded that $U(27)$ is not cyclic.)

9) H is normal only if $\tau H \tau^{-1} \in H$.

Let $\sigma \in H$. Then, $\tau \sigma \tau^{-1} \in H$ if and only if $\tau \sigma \tau^{-1}(1) = 1$

So, we try to calculate $\tau \sigma \tau^{-1}(1)$.

Let $\tau^{-1}(1) = x$.
Then, $\tau \sigma \tau^{-1}(1) = \tau(\sigma(x))$

Is $\tau(\sigma(x)) = 1$?
$\tau(\sigma(x)) = 1 \iff \sigma(x) = \tau^{-1}(1) = x$

So, if $\sigma(x) \neq x$, we cannot have $\tau \sigma \tau^{-1} \in H$.

Thus, we see that H is <u>not</u> a normal subgroup. To show this, pick any $\sigma \in H$ and $x \in \{1, 2, \cdots n\}$ such that $\sigma(x) \neq x$. Then choose any $\tau \in S_n$ such that $\tau^{-1}(1) = x$. Then, above calculations show that $\tau \sigma \tau^{-1}$ will not be in H.

<u>Example</u> Take $n = 3$.
$\sigma = (2, 3)$. (so $x = 2$ will work. $\sigma(2) = 3$)
$\tau = (1, 2)$
Then $\tau \sigma \tau^{-1} = (1,2)(2,3)(1,2)$
$= (1, 3)$
This is not in H.
Thus H is not normal for a general n.

The above example works for any $n \geqslant 3$.
However, it will not work for $n = 2$.

In fact if $n = 2$, $S_2 = \{id, (1,2)\}$ and $H = \{id\}$ which is a normal subgroup of H_2.

10) In general $\mathbb{Z}/m\mathbb{Z}$ has a unique subgroup of order d for any d dividing m. It is generated by m/d.

Applying this, we see that as $20 \mid 100$, $\mathbb{Z}/100\mathbb{Z}$ does have a subgroup of order

20. It is the group $\langle \overline{5} \rangle$

11) $\operatorname{ord}(\overline{35}) = \dfrac{50}{\gcd(35, 50)} = \dfrac{50}{5} = 10$.

The generators of $\langle \overline{35} \rangle$ are of the form $x \cdot \overline{35}$ where $0 \leq x < 10$ and $\gcd(x, 10) = 1$.

So, the generators are $\overline{35}$, $3 \cdot \overline{35} = \overline{5}$, $7 \cdot \overline{35} = \overline{45}$ and $9 \cdot \overline{35} = \overline{15}$.

12) We know that the group is of the form $\langle \bar{d} \rangle$ where $\bar{d}$ is a divisor of 20.

So, the answer is $\langle \bar{1} \rangle$, $\langle \bar{2} \rangle$, $\langle \bar{4} \rangle$, $\langle \bar{5} \rangle$, $\langle \overline{10} \rangle$ or $\{0\} = \langle \overline{20} \rangle$. $\mathbb{Z}/20\mathbb{Z}$

We need to see if a generator of any of these groups is in $\langle \overline{12}, \overline{15} \rangle$.

$\overline{15} - \overline{12} = \bar{3}$.

$\bar{3}$ is a generator of $\mathbb{Z}/20\mathbb{Z}$ as $\gcd(3, 20) = 1$.

So $\langle \overline{12}, \overline{15} \rangle = \mathbb{Z}/20\mathbb{Z}$

Generators : $\bar{1}, \bar{3}, \bar{7}, \bar{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}$.
(all elements of the form $\bar{x}$ where $0 \le x < 20$ and $\gcd(x, 20) = 1$).

13) Part(1):
Clearly, $1_G \in N(H)$.
Let $g \in N(H)$. Then $gHg^{-1} = H$
So $g^{-1}(gHg^{-1})g = g^{-1}Hg$.

So $H = g^{-1}Hg$.
But this implies that $g^{-1} \in N(H)$.
So $N(H)$ is closed under inverses.

Let $g_1, g_2 \in N(H)$

Then $g_1g_2H(g_1g_2)^{-1} = g_1g_2Hg_2^{-1}g^{-1}$

$= g_1(g_2Hg_2^{-1})g_1^{-1}$

$= g_1Hg_1^{-1} = H.$

Thus $g_1g_2 \in N(H)$

Thus $N(H)$ is closed under products.
So $N(H)$ is a subgroup.

<u>Part (2)</u> For any $h \in H$, $hHh^{-1} = (hH)h^{-1}$
$= H \cdot h^{-1}$ (as $h \in H$)
$= H$ (as $h^{-1} \in H$).

So $h \in N(H)$
Thus H is a subgroup of $N(H)$.

For any $g \in N(H)$, $gHg^{-1} \subseteq H$.
So, by definition, H is a normal subgroup of $N(H)$.

14) As $|G| \geqslant 2$, there exists an element $x \in G$ such that $\operatorname{ord}(x) > 1$.
Let $\operatorname{ord}(x) = d$.
Let p be a prime number such that $p \mid d$. Let $r = d/p$
Then, $\operatorname{ord}(x^r) = \dfrac{d}{\gcd(r,d)} = \dfrac{d}{r} = p.$

15) Identity For any $s \in S$, $1 \cdot s = s \cdot 1$.
So, $1 \in C(S)$.

Inverses : Suppose $g \in C(S)$.
So for any $s \in S$, $gs = sg$.
So, $g^{-1}(gs)g^{-1} = g^{-1}(sg)g^{-1}$.
So $sg^{-1} = g^{-1}s$.
As this is true for any $s \in S$, we see that $g^{-1} \in C(S)$.

Products Let $g_1, g_2 \in C(S)$.

Then
$$\begin{aligned}
(g_1 g_2)s &= g_1(g_2 s) \\
&= g_1(s g_2) && (\text{as } g_2 \in C(S)) \\
&= (g_1 s) g_2 \\
&= (s g_1) g_2 && (\text{as } g_1 \in C(S)) \\
&= s(g_1 g_2)
\end{aligned}$$

So $g_1 g_2 \in C(S)$.
Thus, $C(S)$ is closed under products.

Thus, $C(S)$ is a subgroup of G.