Comments to practice Problems

① straight forward:

- calculate $\text{ord}(10)$ in $\mathbb{Z}_{12}$ $= \frac{12}{\gcd(10,12)} = \frac{12}{2} = 6$
- " $\text{ord}(12)$ in $\mathbb{Z}_{16}$ $= \frac{16}{\gcd(12,16)} = \frac{16}{4} = 4$

$\text{ord}(10,12) = \text{lcm}(6,4) = 12$

② ⓐ $\Phi: x \to nx$ homom. !

$\Phi(x+y) = n(x+y) = nx + ny = \Phi(x) + \Phi(y)$

$\Longrightarrow$ homom.

ⓑ For which n is it an isom?

Recall. isom. = homom. ✓ which is one-to-one and onto.

group operation is preserved! (we checked this in part (a)!)

one-to-one: $\Phi(nx) = 0$ must imply $x = 0 \mod 10$

Try: $n = 2$:

$\phi(5) = 2 \cdot 5 = 10 = 0 \mod 10$

$5 \neq 0 \mod 10$

conclusion: not hom. isomorphism for $n = 2$.

Try: $n = 3$:

$1 \to 3$
$2 \to 6$
$3 \to 9$
$4 \to 12 = 2 \mod 10$
$5 \to 15 = 5 \mod 10$
$6 \to 18 = 8 \mod 10$
$7 \to 21 = 1 \mod 10$
$8 \to 24 = 4 \mod 10$
$9 \to 27 = 7 \mod 10$

$\Rightarrow$ for $n = 3$ map is 1-1.

not efficient method!

observation: $n=2$: $\gcd(2,10)=2>1$

$n=3$: $\gcd(3,10)=1$

<u>claim:</u> The map: $\phi: x \to nx \mod 10$ is an isom. $\Longleftrightarrow \gcd(n,10)=1$

proof $\gcd(n,10)=d>1$

$$\Rightarrow \frac{10}{d} \mapsto \frac{n\cdot 10}{d} = 10\cdot\frac{n}{d} = 0 \mod 10$$

$\frac{10}{d} \neq 0 \mod 10$ for $d>1$.

($\frac{n}{d}$ ↑ integer because $d \mid n$)

$\Rightarrow \Phi$ <u>not</u> $\mapsto$

if $\gcd(n, 10) = 1$

$\Rightarrow \exists\ s, t$ s.t. $sn + t \cdot 10 = 1$

hence if $\Phi(x) = 0 \mod 10$

$\Vert$

$nx = 0 \mod 10$

$\Rightarrow \quad snx = 0 \mod 10$

$\Rightarrow \quad snx + t \cdot 10 \cdot x = 0 \mod 10$

$\Rightarrow \quad \underbrace{(sn + t \cdot 10)}_{=1} x = 0 \mod 10$

$x = 0 \mod 10.$

elementary solution

more elegant solution:

If $\gcd(n, 10) = 1 \Rightarrow n \in U(10)$

$\Rightarrow$ there exists inverse $s \in U(10)$

i.e. $sn \equiv 1 \mod 10$

hence: If $nx \equiv 0 \mod 10$

$\Rightarrow \underbrace{sn}_{\equiv 1 \mod 10} x \equiv s0 \equiv 0 \mod 10$

$\Rightarrow x \equiv 0 \mod 10$

(3)

(a) true: $|\mathbb{Z}_n| = n$ for any n

(b) true: have shown: $|G| = p$

$\Rightarrow G \cong \mathbb{Z}_p$ abelian

(c) not true: $G = D_p$ dihedral group

$|D_p| = 2p$

not abelian

(d) not true:

If $a \in G \Rightarrow \text{ord}(a) \mid |G|$

(4) similar to midterm problem. 8 ✗ 44

⑤ similar to midterm problem

⑥ homework problem:

Chew $\Phi = \{(e,k),\ k \in K\}$

⑦ ⓐ $2a = 2(2,1) = (4,2) = (0,0)$ in $\mathbb{Z}_4 \oplus \mathbb{Z}_2$

$|\mathbb{Z}_4 \oplus \mathbb{Z}_2| = 4 \cdot 2$

$\Rightarrow |\langle a \rangle| = 2$

$\Rightarrow |G/\langle a \rangle| = \frac{|G|}{|\langle a \rangle|} = \frac{4 \cdot 2}{2} = 4$

ⓑ have seen: $|G| = 4 \Rightarrow G = \mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

need to calculate $\text{ord}(g\langle a \rangle)$ in $G/\langle a \rangle$.

quickest method:

check whether $2b \in \langle a \rangle$ for all $b \in G$!

proof. $2b = 2(i,j) = (2i, 2j) = (2i, 0)$

$i \in \mathbb{Z}_4$, $j \in \mathbb{Z}_2$, $2j \in \mathbb{Z}_2$ ↑

result: if $b = (1,0) \Rightarrow 2(1,0) = (2,0) \notin \langle a \rangle$

$3(1,0) = (3,0) \notin \langle a \rangle$

$4(1,0) = (0,0) \in \langle a \rangle$

$\Rightarrow b^j \langle a \rangle = \langle a \rangle \iff 4 \mid j$

$\Rightarrow b\langle a \rangle$ has order 4 in $G/\langle a \rangle$

$\Rightarrow G/\langle a \rangle \cong \mathbb{Z}_4$.

(8) Sol. $U(8) \not\cong U(5)$

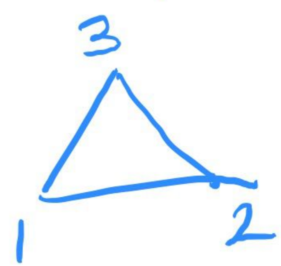
Question: Is $S_3 \cong D_3$?

S_3 ← symmetric group

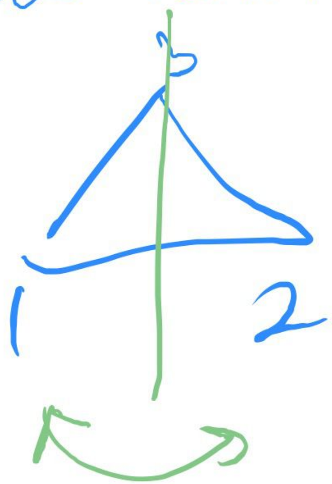
D_3 ← dihedral group.

$|S_3| = 6 = |D_3|$

try to find an isom.



If $a \in D_3 \longrightarrow \pi_a \in S_3$ permutation of corners e.g. a = reflection at vertical axis



$\to$ permutation $\begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{matrix} = (12)$

observe: $\Phi : a \to \pi_a$ is 1-1

and Φ is a hom.

$\Rightarrow$ Φ is an isom.

$\Rightarrow$ $S_3 \cong D_3$.