Q41 Chap 3.

Known group G is $G = \mathbb{R}^*$, the group of non-zero real numbers under mult.

ie. $e = 1$, $x^{-1} = \frac{1}{x}$

Consider $H = \{ a + b\sqrt{2} : a, b \in \mathbb{Q}$, a, b not both zero $\}$

Clearly $H \subset G$ $\qquad \hookrightarrow a + b\sqrt{2} \neq 0$

remember $\sqrt{2} \notin \mathbb{Q}$

Prove, using Prop 3.30, that H is a subgroup of $\mathbb{R}^*$.

1. $e = 1 \in H$, since $1 = 1 + 0\sqrt{2}$
   ie $a = 1$, $b = 0$

2. Closure. We need to prove that $\forall\, h_1, h_2 \in H \;\; h_1 h_2 \in H$.

$a, b, c, d \in \mathbb{Q}$

So let $a + b\sqrt{2}$, $c + d\sqrt{2} \in H$

$0 \neq (a + b\sqrt{2})(c + d\sqrt{2}) \quad \overset{?}{\in} H.$

$= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd$

$$= \underbrace{\frac{(ac+2bd)}{}}_{\in \mathbb{Q}\,\checkmark} + \underbrace{\frac{(ad+bc)}{}}_{\in \mathbb{Q}\,\checkmark}\sqrt{2} \in H \checkmark$$

and $(ac+2bd)$ and $(ad+bc)$ are not both zero since RHS. $\neq 0$

3. Existence (in H) of all inverses.

Consider an element $a+b\sqrt{2} \in H$.

Q? Is $(a+b\sqrt{2})^{-1} \in H$??

$$(a+b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} \cdot \frac{(a-b\sqrt{2})}{(a-b\sqrt{2})}$$

$$= \frac{a-b\sqrt{2}}{a^2-2b^2}$$

$$= \underbrace{\frac{a}{a^2-2b^2}}_{\in \mathbb{Q}\,\checkmark} + \underbrace{\frac{-b}{a^2-2b^2}}_{\in \mathbb{Q}\,\checkmark}\sqrt{2} \in H.$$

So by Prop 3.30 H is a subgroup $\mathbb{R}^*$.

all congruences classes modulo 12

$\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$

Q6 Recall.

$$U(12) = \{ a \in \mathbb{Z}_{12} : \gcd(a,12) = 1 \}.$$

$$= \{ 1, \quad 5, 7, 11 \}$$

$\gcd(0,12) = \underline{12}$, $\gcd(3,12) = 3$

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$$5 \cdot 11 \equiv 5(-1)$$
$$\equiv -5$$
$$\equiv 7$$

$\underline{\underline{U(12)}}$

When filling out Cayley tables

- every row and column contains each element once and only once
- Remember $11 \equiv -1 \mod 12$, $7 \equiv -5 \mod 12$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$U(8)$

Do we regard $U(12)$, $U(8)$ as having a different group structure? Might they have the same group structure?

Because the Cayley tables have the same structure, after the mapping

$$\begin{aligned}\phi: U(12) &\longrightarrow U(8)\\ 1 &\longmapsto 1\\ 5 &\longmapsto 3\\ 7 &\longmapsto 5\\ 11 &\longmapsto 7\end{aligned}$$

~~so~~ $U(12)$ "turns into" $U(8)$

ϕ is an example of an isomorphism.

Do all groups of order 4 have this structure?

Consider $\mathbb{Z}_4, +$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4$

same as $U(8)$?

But in $U(8)$, all elements are self-inverse. In $\mathbb{Z}_4$ this is not so

$-2 \equiv 2$, $-1 \equiv 3$

$-3 \equiv 1$

$-0 \equiv 0$

For this reason $\mathbb{Z}_4$ has a different group structure to $U(8)$, $U(12)$.

$\boxed{\text{Q48}}$ A theoretical, general question.

Let G be a group.

$$Z(G) = \{\boxed{x} \in G : \boxed{\forall g \in G \quad xg = gx}\}$$

called the centre of G.

Zentrum German for centre.

Now if G is Abelian, $\underline{Z(G) = G}$

But for a non-Abelian group G the centre is an interesting subset, all the special elements x that commute with all elements in G.

Prove $Z(G)$ is a subgroup of G.

<u>Use prop 3.30</u>

<u>Proof</u>:

1: $e \in Z(G)$? ✓

Let $g \in G$. $eg = g = g = ge$

from the definition of the group G.

2. Closure.

Let $\boxed{a, b \in Z(G)}$, $\boxed{Q?\ ab \in Z(G)?}$

Let $g \in G$

$$(ab)g = a(bg), \quad \text{by associativity}$$
$$= a(gb), \quad \text{since } b \in Z(G) \text{ i.e. } \forall g \in G\ bg = gb$$
$$= (ag)b, \quad \text{associativity.}$$
$$= (ga)b, \quad a \in Z(G)$$
$$= g(ab), \quad \text{by associativity}$$

$\Rightarrow ab \in Z(G)$ ✓

From now on, associativity always holds in groups, so we can adopt the convention of not including parentheses in triple/multi products.

$$abg = agb, \quad b \in Z(G)$$
$$= gab, \quad a \in Z(G)$$

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

3. For $\boxed{a \in Z(G)}$ Q? Is $a^{-1} \in Z(G)$?

Let $g \in G$ $\quad \underline{\forall g \in G}$ $ag = ga$

$$a^{-1}g = ((a^{-1}g)^{-1})^{-1}$$ ✓ by prop 3.20

$$= (g^{-1}(a^{-1})^{-1})^{-1}$$, by prop 3.19

$$= (g^{-1}a)^{-1}$$, prop 3.20

$$= (ag^{-1})^{-1}$$, $a \in Z(G)$

$$= (g^{-1})^{-1}a^{-1}$$, prop 3.19.

$$= ga^{-1}$$, prop 3.20.

$\Longrightarrow a^{-1} \in Z(G)$

So by Prop 3.30 $Z(G)$ is a subgroup of G. $\triangle$

Consider $D_3 = \{id, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$

$Z(D_3) = \{id\}$, the trivial subgroup

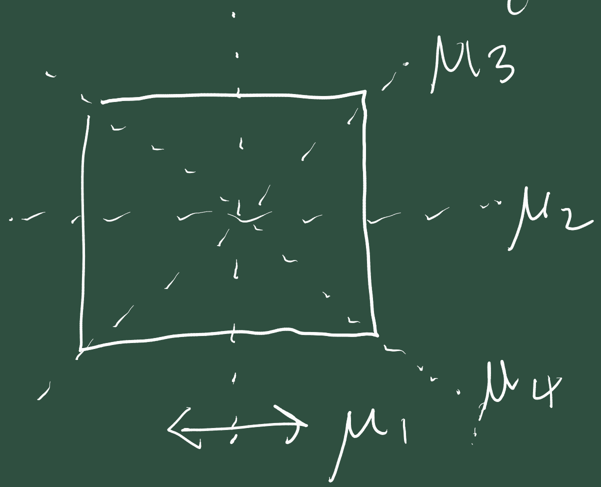
is $\rho_1 \in Z(D_3)$? $\quad \rho_1 \circ \mu_2 = \mu_1$

No $\quad \mu_2 \circ \rho_1 = \mu_3$

Consider D_4, a group of order 8.

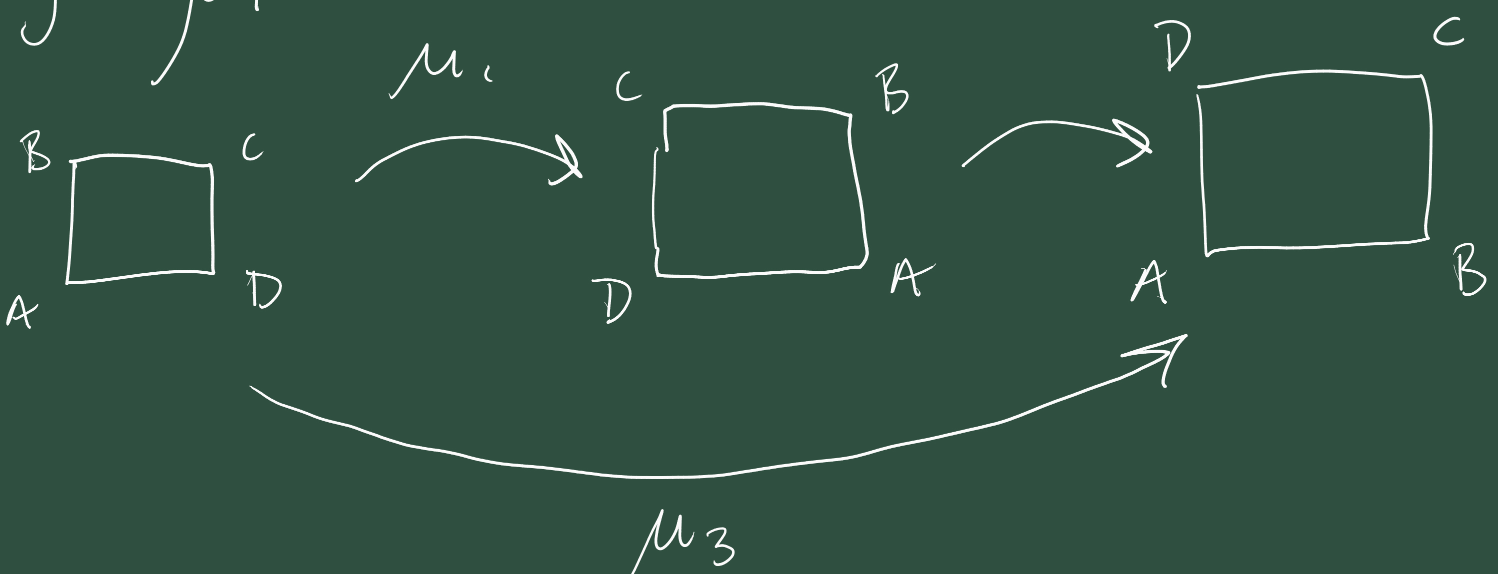
$$D_4 = \{e, \rho, \rho^2, \rho^3, \mu_1, \mu_2, \mu_3, \mu_4\}$$

ρ " rot by $\frac{\pi}{2}$ radians clockwise.

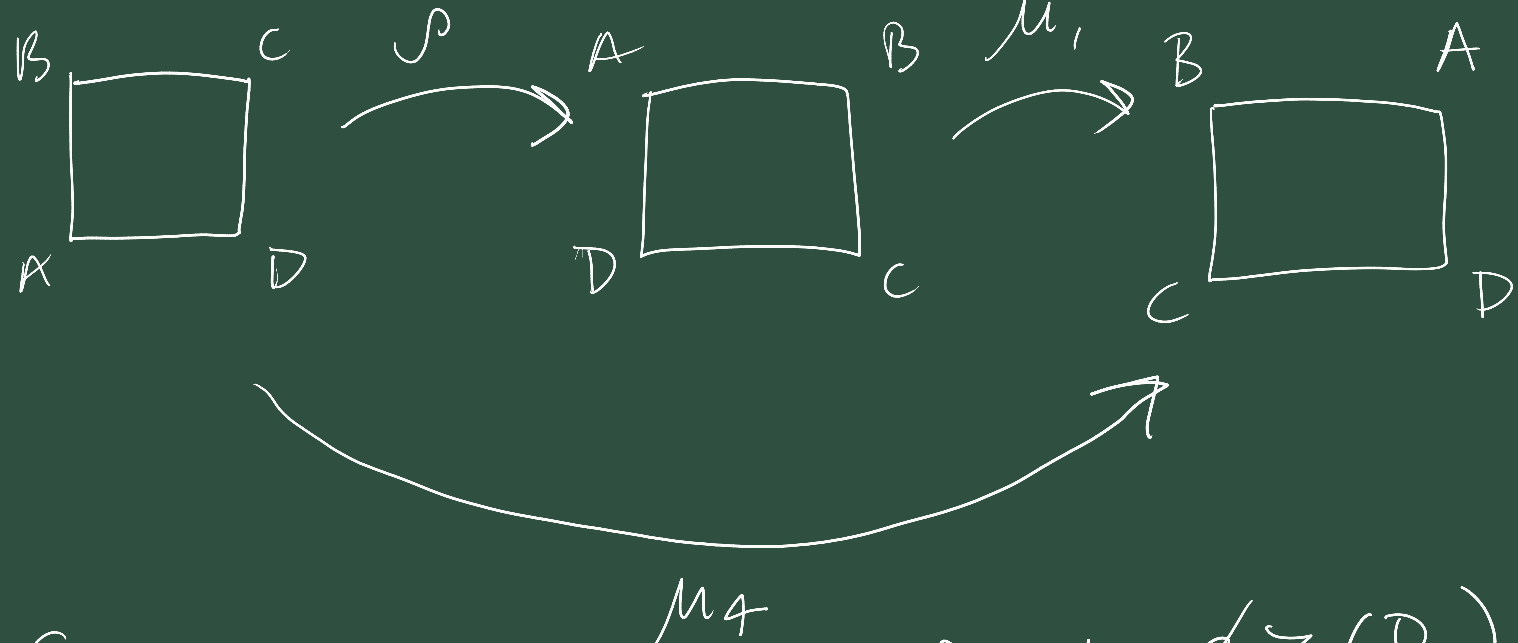


$$Z(D_4) = \{e, \rho^2\}$$

$\rho \circ \mu_1$



But $\mu_1 \circ \rho$



So $\rho \circ \mu_1 \neq \mu_1 \circ \rho \Rightarrow \rho, \mu_1 \notin Z(D_4)$

The same can be said of any other reflection $\mu_2, \mu_3, \mu_4 \notin Z(D_4)$

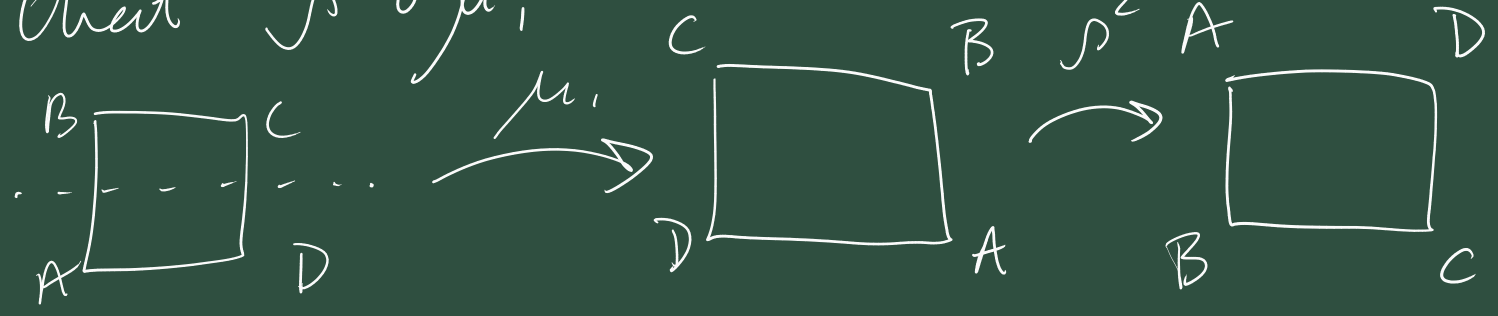
The same can also be discovered about $\rho^3 \notin Z(D_4)$

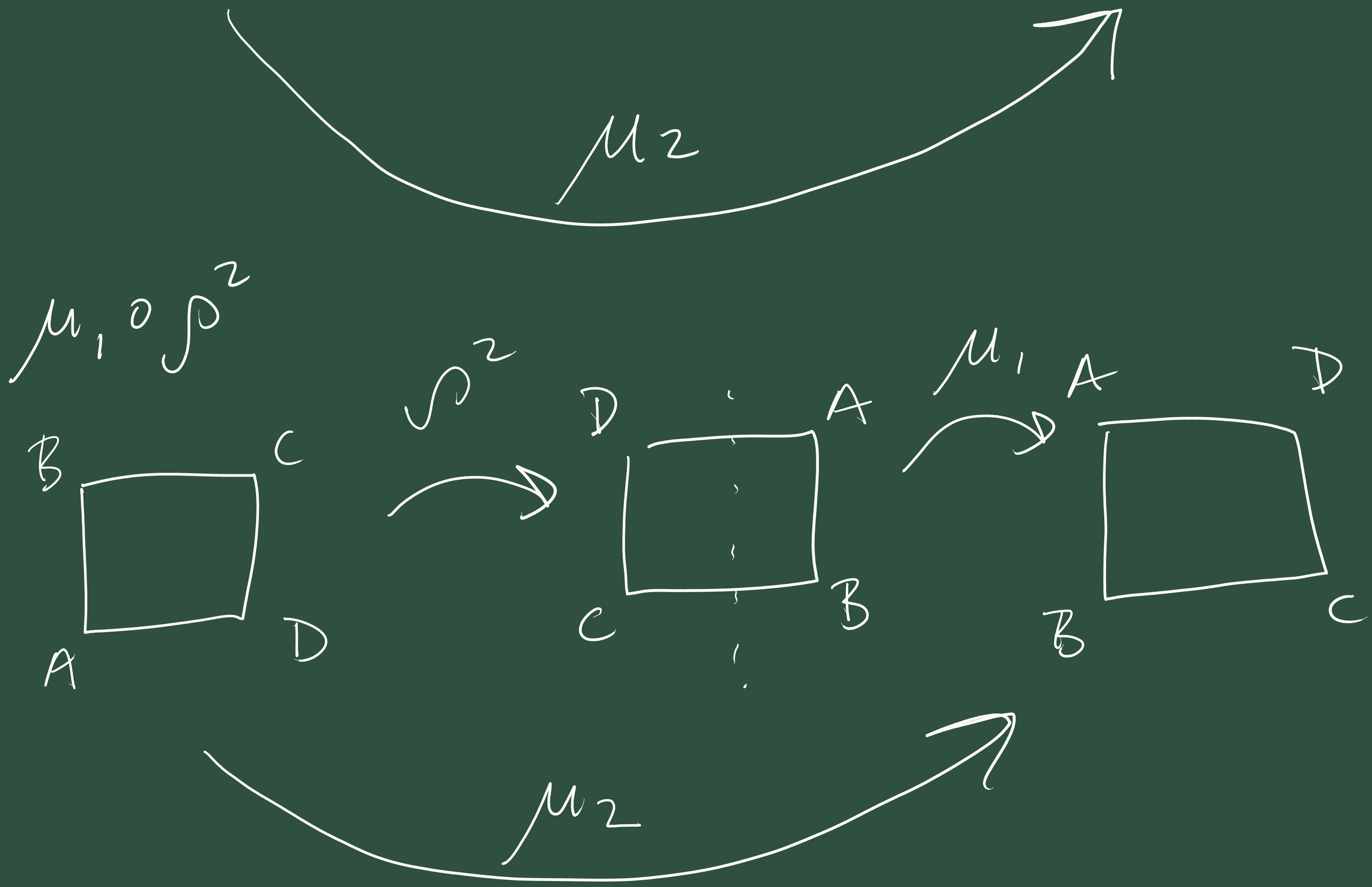
But ρ^2 is the half-turn rotation.

$$\rho^2 \circ \rho = \rho^3 = \rho \circ \rho^2$$

$$\rho^2 \circ \rho^3 = \rho = \rho^3 \circ \rho^2$$

Check $\rho^2 \circ \mu_1$





So $\rho^2 \circ \mu_1 = \mu_1 \circ \rho^2$

And also $\rho^2 \circ \mu_3 = \mu_3 \circ \rho^2$, $\rho^2 \circ \mu_2 = \mu_2 \circ \rho^2$

$\rho^2 \circ \mu_4 = \mu_4 \circ \rho^2$

Therefore $\rho^2 \in Z(D_4)$

In general

if ρ is any rotation about a centre point $\underline{c} \in \mathbb{R}^2$

and μ is any reflection in an axis through $\underline{c}$.

$$\boxed{\rho \circ \mu = \mu \circ \rho^{-1}}$$

For $\rho^2 \in D_4$, ρ^2 was the half-turn clockwise

$$(\rho^2)^{-1} = \rho^2.$$