Assignment 2.

Question 1.

Show that $2\mathbb{Z}_8 = \{2\bar{k} \mid \bar{k} \in \mathbb{Z}_8\}$ is a subgroup of $\mathbb{Z}_8$.

Q1 $\mathbb{Z}_8$ is the quotient set (all equivalence classes)

$|\mathbb{Z}_8| = 8$ $\quad \mathbb{Z}_8 = \{[1], [2], \ldots [7]\}$

$2\mathbb{Z}_8 = \{[0], [2], [4], [6]\}$

$(2\mathbb{Z}_8, +) \longleftarrow$ ($\mathbb{Z}_8$ is abelian, so use $+$ as binary operator)

$$2\mathbb{Z}_8 = \left\{ \begin{array}{l} [0] = \{\ldots -16, -8, 0, 8, 16 \ldots\}, \\ [2] = \{\ldots -14, -6, 2, 10, 18 \ldots\}, \\ [4] = \{\ldots -12, -4, 4, 12, 20 \ldots\}, \\ [6] = \{\ldots -10, -2, 6, 14, 22 \ldots\} \end{array} \right\}$$

$2\mathbb{Z}_8$ partions even numbers $\in \mathbb{Z}$

can use

Proposition 5.3. *Let $(G, *)$ be a group and let H be a non–empty subset of G. Then $(H, *|_{H\times H})$, where $*|_{H\times H}$ denotes the restriction of $*$ to $H \times H$, is a subgroup of $(G, *)$ if and only if $xy^{-1} \in H$ whenever $x, y \in H$.*

consider $2\mathbb{Z}_8$ as H and $\mathbb{Z}_8$ as G

- by the definition of $2\mathbb{Z}_8$, it is not empty
- suppose $x, y \in 2\mathbb{Z}_8$

  then $\exists a, b \in \mathbb{Z}$, such that $x = [2a]$, $y = [2b]$

  since $a - b \in \mathbb{Z}$

  then $[2(a-b)] \in 2\mathbb{Z}_8$

  $= [2a - 2b]$

  $= [2a] - [2b] = x - y$

  $\therefore x - y \in 2\mathbb{Z}_8$

  and since $-y$ is the inverse of x, then $xy^{-1} \in \mathbb{Z}_8$, and this is a subgroup by the prop 5.3.

Q2

Question 2.

Let $\varphi : G \to H$ a homomorphism of groups.

Show that φ is injective if and only if $\ker \varphi = \{e_G\}$.

($\Rightarrow$) Assume φ is injective, then since φ is a homomorphism then $\varphi(e_G) = e_H$. Since φ is injective then only one element in

($\Leftarrow$) Assume $\ker \varphi = \{e_G\}$

take $x, y \in G$

s.t. $\varphi(x) = \varphi(y)$

$\varphi(x) *_H \varphi(y)^{-1} = e_H$

$\varphi(x *_G y^{-1}) = e_H$ (property of homomorphisms)

$x *_G y^{-1} \in \ker \varphi$

but by the assumption $\ker \varphi = \{e_G\}$

then $x *_G y^{-1} = e_G$

$\therefore$ $x = y$

And this fulfils the definition

injectivity $:= \forall x, x' \in X \mid f(x) = f(x') \Rightarrow x = x'$

Question 3.

An *automorphism* of the group G is an isomorphism $\varphi : G \to G$. Put

$$\mathrm{Aut}(G) := \{\varphi : G \to G \,|\, \varphi \text{ is an isomorphism}\}$$

(a) Show that $\mathrm{Aut}(G)$ is a subgroup of $S(G)$, the group of invertible functions from the set underlying G to itself with the binary operation given by composition of functions.

(b) Given $g \in G$ show that

$$\varphi_g : G \longrightarrow G,\ x \longmapsto gxg^{-1}$$

is an automorphism. It is called the *inner automorphism* defined by g.

Q3a) need to show: $\mathrm{Aut}(G) \leqslant S(G)$

use $S(G) := \{f : G \to G \,|\, f \text{ is invertible}\}$

Note that $\mathrm{id}_G : G \to G$, $g \mapsto g$ $\quad e \in S(G)$

Because id_G is invertible and because $\forall g \in S(G)$, $g \circ \mathrm{id}_G = g$

Now, using the subgroup criteria (5.2):

take $g, g' \in G$

① $\mathrm{id}_G(g\,g') = \mathrm{id}_G\,\mathrm{id}_G$, so this a homomorphism,
It being invertible means it's an isomorphism.
So, $\mathrm{id}_G \in \mathrm{Aut}(G)$

② for any $g \in \mathrm{Aut}(G)$, the inverse of g is in $\mathrm{Aut}(G)$, simply because every isomorphism is invertible.

③ $\mathrm{Aut}(G)$ is closed under composition, since the composition of two isomorphisms is again an isomorphism

$\therefore\ \mathrm{Aut}(G) \leqslant S(G)$

Q3 b)

To show φ_g is an automorphism, we must show it is an isomorphism.

Firstly, φ_g must be shown to be a homomorphism.

$\forall x, y \in G$

$$\begin{aligned}\varphi_g(xy) &= gxyg^{-1} \\ &= gx \cdot e \cdot yg^{-1} \quad (\text{since } G \text{ is a group, } e \in G) \\ &= gxg^{-1} \cdot gyg^{-1} \\ &= \varphi_g(x) \cdot \varphi_g(y)\end{aligned}$$

Then this is a homomorphism

Let $\psi_g = \varphi_g : G \to G$

$$x \to g^{-1} x g$$

$$\left.\begin{aligned}\psi(xy) &= g^{-1} x y g \\ &= g^{-1} x g \cdot g^{-1} y g \\ &= \psi(x) \cdot \psi(y)\end{aligned}\right\} \text{ then } \psi \text{ is also a homomorphism}$$

$\forall x \in G$

$$\psi(\varphi(x)) = id_G(x) = x$$

$\therefore$ because of definition 4.12 then this is an isomorphism