Ejercicio 4

Determinar si existen homomorfismos no triviales $f : G \to K$ para cada grupo G y K.
En caso afirmativo dar un ejemplo, justificando que es un homomorfismo.

(a) $G = \mathbb{Z}_p$ con p primo y $K = S_{p-1}$.
(b) $G = U(p)$ con $p > 2$ primo, y $K = S_{p-2}$.
(c) $G = U(12)$ y $K = \mathbb{Z}_4$.

a) $f: \mathbb{Z}_p \to S_{p-1}$ morfismo de grupos no trivial? p primo

$|\mathbb{Z}_p| = p$

$|S_{p-1}| = (p-1)!$

$\Big\}$ $\text{mcd}(|\mathbb{Z}_p|, |S_{p-1}|) = 1 \Rightarrow$ el único morfismo $f: \mathbb{Z}_p \to S_{p-1}$ es el trivial

↳ $\begin{pmatrix} 1 & 2 & 3 & \cdots & p-1 \\ \uparrow & \uparrow & & & \uparrow \end{pmatrix}$

$p-1$ pos. $p-2$ pos. 1 pos.

$f: \mathbb{Z}_p \to S_{p-1}$

$\mathbb{Z}_p = \langle \bar{1} \rangle$

nos alcanza con dar $f(\bar{1})$

> $f: G \to K$ morfismo de grupos
> $g \in G$
> $\Rightarrow o(f(g)) \mid o(g)$

para definir $f(\bar{1})$ buscamos un elemento $g \in S_{p-1}$ tal que

$$o_{S_{p-1}}(g) \mid \underbrace{o_{\mathbb{Z}_p}(\bar{1})}_{p}$$

como p es primo hay dos posibilidades

① $o_{S_{p-1}}(g) = 1 \Rightarrow g = id$

entonces $f(\bar{1}) = id$

$\Rightarrow f$ es el morfismo trivial

$f(\bar{a}) = f(\bar{1} + \bar{1} + \bar{1} + \cdots + \bar{1})$
$= f(\bar{1}) \circ f(\bar{1}) \circ \cdots \circ f(\bar{1})$
$= id \circ id \circ \cdots \circ id$
$= id$

$\Big\}$ f es morfismo de grupos

② $o_{S_{p-1}}(g) = p$

absurdo porque $o_{S_{p-1}}(g) \mid (p-1)!$

entonces el único morfismo $f: \mathbb{Z}_p \to S_{p-1}$ es el trivial

---

$f: G \to K$ morfismo de grupos

Ejercicio 2. Sea $\varphi : G_1 \to G_2$ un homomorfismo de grupos finitos.

a. Sea $g \in G_1$. Probar que $o(\varphi(g))$ divide a $\mathrm{mcd}(|G_1|, |G_2|)$.

b. Probar que si $|G_1|$ y $|G_2|$ son coprimos, entonces φ es trivial.

c. Supongamos que φ es un isomorfismo de grupos. Sea $g \in G_1$. Probar que el orden de g en G_1 es igual al orden de $\varphi(g)$ en G_2.

d. Probar que $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$ no son isomorfos.

b) p primo, $p>2$

$f: U(p) \longrightarrow S_{p-2}$ morfismo de grupos no trivial?

* $U(p)$ es cíclico?

p primo $\Rightarrow$ existe raíz primitiva modulo p

$\Rightarrow U(p)$ es cíclico

$\Rightarrow U(p) = \langle \bar{g} \rangle$ para algún $\bar{g} \in U(p)$

para definir $f: U(p) \to S_{p-2}$ alcanza con definir $f(\bar{g})$

sea $\bar{k} \in U(p)$ $\quad f(\bar{k}) = f(\bar{g}^n)$ para algún n

$= f(\bar{g}) \circ f(\bar{g}) \circ \cdots \circ f(\bar{g})$

$= f(\bar{g})^n$

* queremos definir $f(\bar{g})$:

$f(\bar{g})$ tiene que verificar

$\mathbb{Z}_p = \{\overset{\times}{\bar{0}}, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$

$U(p) = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$

$$o_{S_{p-2}}(f(\bar{g})) \mid \underbrace{o_{U(p)}(\bar{g})}_{|U(p)| = \varphi(p) = p-1}$$

p primo $\Rightarrow p-1$ es par

$p>2 \quad \Rightarrow 2 \mid p-1$

existe algún elemento en S_{p-2} que tenga orden 2?

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & p-2 \\ 1 & 2 & 4 & 3 & & p-2 \end{pmatrix} \in S_{p-2}$$

podemos definir $f(\bar{g}) = h$

c) $f: U(12) \longrightarrow \mathbb{Z}_4$

* $U(12)$ es cíclico? no

$12 = 2^2 \cdot 3$ $\Rightarrow$ no hay raíz primitiva modulo 12

hay raíz primitiva modulo n sii $n \to 2$, $n \to 4$, $n \to p^\alpha$ (p impar), $n \to 2p^\alpha$ (p impar)

* $|U(12)| = \varphi(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 12 \cdot \frac{1}{2}\,\frac{2}{3} = 4$

$U(12)$

g	$o(g)$
$\bar{1}$	1
$\bar{5}$	2
$\bar{7}$	2
$\bar{11}$	2

$\rightsquigarrow$ $o(g) \mid |U(12)| \Rightarrow o(g) \mid 4$ $\to$ $o(g)=1$ ← el neutro; $o(g)=2$; $o(g)=4$ ← no, porque no hay raíz primitiva

$\rightsquigarrow$ $\bar{5}^2 = \overline{25} = \bar{1}$ ← neutro

$\mathbb{Z}_4$

g	$o(g)$
$\bar{0}$	1
$\bar{1}$	4
$\bar{2}$	2
$\bar{3}$	4

$f(\bar{5}) = \bar{1}$

$\underbrace{o(f(\bar{5}))}_{4} \mid \underbrace{o(\bar{5})}_{2}$ X

$f: U(12) \to \mathbb{Z}_4$

* por el teorema de órdenes: $\underbrace{|U(12)|}_{=4} = |\ker f|\,|\mathrm{Im} f|$

tenemos las posibilidades:

① $|\ker f| = 4$

$|\mathrm{Im} f| = 1$

$\Rightarrow f$ es el morfismo trivial

② $|\ker f| = 1$

$|\mathrm{Im} f| = 4$ ↯ absurdo porque $\bar{1} \notin \mathrm{Im} f$

$\bar{3} \notin \mathrm{Im} f$

③ $|\ker f| = 2$

$|\mathrm{Im} f| = 2$

candidato a imágen: $\mathrm{Im} f = \{\bar{0}, \bar{2}\}$

candidato a nucleo: $\ker f = \{\bar{3}, \bar{5}\} = \langle \bar{5} \rangle$

$$f : U(12) \to \mathbb{Z}_4$$

$f(\bar{1}) = \bar{0}$ $\quad$ $f(\bar{7}) = \bar{2}$

$f(\bar{5}) = \bar{0}$ $\quad$ $f(\bar{11}) = \bar{2}$

veamos que f es un morfismo de grupos:

- $f(\bar{5} \cdot \bar{7}) \overset{?}{=} f(\bar{5}) + f(\bar{7})$ ✓

  $f(\bar{5} \cdot \bar{7}) = f(\bar{11}) = \bar{2}$

  $f(\bar{5}) + f(\bar{7}) = \bar{0} + \bar{2} = \bar{2}$

- $f(\bar{5} \cdot \bar{11}) \overset{?}{=} f(\bar{5}) + f(\bar{11})$ ✓

  $f(\bar{5} \cdot \bar{11}) = f(\bar{7}) = \bar{2}$

  $f(\bar{5}) + f(\bar{11}) = \bar{0} + \bar{2} = \bar{2}$

- $f(\bar{7} \cdot \bar{11}) \overset{?}{=} f(\bar{7}) + f(\bar{11})$ ✓

  $f(\bar{7} \cdot \bar{11}) = f(\bar{5}) = \bar{0}$

  $f(\bar{7}) + f(\bar{11}) = \bar{2} + \bar{2} = \bar{0}$

G un grupo finito y g un generador
$\Rightarrow$ G tiene $\varphi(|G|)$ generadores

Como g es un generador de G tenemos que $o(g) = |G|$ y además $G = \{g, g^2, \dots, g^{|G|}\}$.

Sea h otro generador de G
Entonces $o(h) = |G|$ y $h = g^n$ para algún $n \in \{1, \dots, |G|\}$

$$|G| = o(h) = o(g^n) = \frac{o(g)}{mcd(o(g), n)} = \frac{|G|}{mcd(o(g), n)}$$

entonces $|G| = \dfrac{|G|}{mcd(o(g), n)}$

por lo tanto $mcd(o(g), n) = 1$

Recíprocamente sea $h = g^n$ con $n \in \{1, \dots, |G|\}$ y $mcd(o(g), n) = 1$

$$o(h) = o(g^n) = \frac{o(g)}{mcd(o(g), n)} = \frac{|G|}{1} = |G|$$

(↑ $mcd(o(g), n)$ por la parte ...)

entonces h es generador

h generador $\iff$ $h = g^n$ con $n \in \{1, \dots, |G|\}$ y $mcd(o(g), n) = 1$

Luego, el conjunto de generadores de $|G|$ es

$$\{g^n : n \in \{1, \dots, |G|\} \text{ y } mcd(o(g), n) = 1\}$$

entonces la cantidad de generadores de $|G|$ es

$$\#\{g^n : n \in \{1 \dots |G|\} \text{ y } mcd(o(g), n) = 1\}$$

$$= \#\{n : n \in \{1 \dots |G|\} \text{ y } mcd(\underbrace{o(g)}_{= |G|}, n) = 1\}$$

$= \varphi(|G|)$