¿Existe un morfismo de grupos no trivial de $U(15)$ en $\mathbb{Z}_6$?

$$f : U(15) \to \mathbb{Z}_6$$

$15 = 3\cdot 5 \implies U(15)$ no es cíclico

* teorema de órdenes:

$$|U(15)| = |\ker f| \times |\operatorname{Im} f|$$

$$|U(15)| = \varphi(15) = 15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$$

$$8 = |\ker f| \times |\operatorname{Im} f|$$

* $\operatorname{Im} f$ es un subgrupo de $\mathbb{Z}_6$

$\implies |\operatorname{Im} f| \mid |\mathbb{Z}_6|$ por el teorema de Lagrange

$\implies |\operatorname{Im} f| \mid 6$

* entonces: $\begin{cases} |\ker f| \times |\operatorname{Im} f| = 8 \implies |\operatorname{Im} f| \mid 8 \\ |\operatorname{Im} f| \mid 6 \end{cases}$

las posibilidades son: 1) $|\operatorname{Im} f| = 1 \implies f$ es el morfismo trivial

2) $|\operatorname{Im} f| = 2$

Veamos si podemos constrir un morfismo de grupos

$$f : U(15) \to \mathbb{Z}_6$$

tal que $|\operatorname{Im} f| = 2$

$\to$ para ver las posibilidades para $\operatorname{Im} f$ buscamos subgrupos de $\mathbb{Z}_6$ que tengan orden 2

$\mathbb{Z}_6$

g	$o(g)$
$\bar{0}$	1
$\bar{1}$	6
$\bar{2}$	3
$\bar{3}$	2
$\bar{4}$	3
$\bar{5}$	6

$o(\bar{3}) = 2$ y $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$

nuestro candidato a ser la $\mathrm{Im} f$ es $\{\bar{0}, \bar{3}\}$

$\longrightarrow$ $|\ker f| \times \underbrace{|\mathrm{Im} f|}_{=2} = 8 \Rightarrow |\ker f| = 4$

vamos a buscar un subgrupo de $U(15)$ que tenga orden 4

$U(15) = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}\}$

$15 = 3 \cdot 5$

$\bar{2}^2 = \bar{4}$

$\bar{2}^3 = \bar{8}$

$\bar{2}^4 = \overline{16} = \bar{1} \Rightarrow o(\bar{2}) = 4$

nuestro candidato a nucleo es $\langle \bar{2} \rangle = \overbrace{\{\bar{1}, \bar{2}, \bar{4}, \bar{8}\}}^{\ker f}$

entonces definimos: $f : U(15) \longrightarrow \mathbb{Z}_6$

$$\left.\begin{array}{l} f(\bar{1}) = \bar{0} \\ f(\bar{2}) = \bar{0} \\ f(\bar{4}) = \bar{0} \\ f(\bar{8}) = 0 \end{array}\right\} f(\bar{2}^k) = \bar{0} \quad \text{con } k \in \{1,2,3,4\}$$

$f(\bar{1} \cdot \bar{2}) = f(\bar{1}) + f(\bar{2})$

$\langle -\bar{2} \rangle = \{ \overset{=\overline{13}}{\overline{-2}}, \bar{4}, \overset{=\bar{7}}{\overline{-8}}, \overset{=\bar{3}}{\overline{16}} \}$

$\langle \overline{13} \rangle = \{ \overline{13}, \bar{4}, \bar{7}, \bar{1} \}$

$f(\bar{7}) = \bar{3}$ $\quad \bar{7} = -\bar{8}$

$f(\overline{11}) = \bar{3}$ $\quad \overline{11} = -\bar{4}$

$f(\overline{13}) = \bar{3}$ $\quad \overline{13} = -\bar{2}$

$f(\overline{14}) = \bar{3}$ $\quad \overline{14} = -\bar{1}$

$f(-(\bar{2}^k)) = \bar{3}$ con $k \in \{1,2,3,4\}$

vamos a verificar que es un morfismo de grupos

* $f(\bar{2}^k \cdot \bar{2}^j) = f(\bar{2}^k) + f(\bar{2}^j)$ ✓

$f(\bar{2}^k \cdot \bar{2}^j) = f(\underbrace{\bar{2}^{k+j}}_{\in \langle \bar{2} \rangle = \ker f}) = \bar{0}$

$f(\underbrace{\bar{2}^k}_{\in \langle \bar{2} \rangle = \ker f}) + f(\bar{2}^j) = \bar{0} + \bar{0} = \bar{0}$

* $f(\bar{7} \times \overline{11}) \overset{?}{=} f(\bar{7}) + f(\overline{11})$ ✓

$f(\bar{7} \times \overline{11}) = f(\overline{77}) = f(\bar{2}) = \bar{0}$

$f(\bar{7}) + f(\overline{11}) = \bar{3} + \bar{3} = \bar{0}$

* $f(-\bar{2}^k \times (-\bar{2}^j)) = f(-\bar{2}^k) + f(-\bar{2}^j)$ ✓

$f(-\bar{2}^k \times (-\bar{2}^j)) = f(\bar{2}^{k+j}) = \bar{0}$

$f(-\bar{2}^k) + f(-\bar{2}^j) = \bar{3} + \bar{3} = \bar{0}$

* $f(\bar{2} \times \bar{7}) = f(\bar{2}) + f(\bar{7})$ ✓

$f(\bar{2} \times \bar{7}) = f(\overline{14}) = \bar{3}$

$f(\bar{2}) + f(\bar{7}) = \bar{0} + \bar{3} = \bar{3}$

$f(\bar{4} \times \bar{7}) = f(\bar{4}) + f(\bar{7})$

Ejercicio 3. Para los siguientes grupos G, K, determinar si existen homomorfismos $f : G \to K$ no triviales. En caso afirmativo dar un ejemplo, justificando que es un homomorfismo.

a. Para un primo impar p, $G = \mathbb{Z}_p$ el grupo de enteros módulo p y $K = S_{p-1}$ el grupo de permuataciones de $p-1$ elementos.

b. $G = \mathbb{Z}_{100}$ el grupo de enteros módulo 100, y $K = \mathrm{U}(101)$ el grupo de invertibles módulo 101.

c. $G = U(12)$ el grupo de invertibles módulo 12 y $\mathbb{Z}_4$ el grupo de enteros módulo 4.

a) p primo impar

$f : \mathbb{Z}_p \longrightarrow S_{p-1}$ morfismo de grupos.

* teorema de ordenes:

$|\mathbb{Z}_p| = |\ker f| |\mathrm{Im} f| \Rightarrow |\mathrm{Im} f| \,\big|\, |\mathbb{Z}_p| \Rightarrow |\mathrm{Im} f| \,\big|\, p$

* $\operatorname{Im} f$ es un subgrupo de S_{p-1}

$\Rightarrow |\operatorname{Im} f| \mid |S_{p-1}| \Rightarrow |\operatorname{Im} f| \mid (p-1)!$

* tenemos $\left.\begin{array}{l} |\operatorname{Im} f| \mid p \\ |\operatorname{Im} f| \mid (p-1)! \\ \operatorname{mcd}(p, (p-1)!) = 1 \end{array}\right\} \Rightarrow |\operatorname{Im} f| = 1$

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

b) morfismo de grupos $f: \mathbb{Z}_{100} \to U(101)$

* $|\mathbb{Z}_{100}| = 100$

$|U(101)| = \varphi(101) = 100$

* $\mathbb{Z}_{100}$ es cíclico? si

$\mathbb{Z}_{100} = \langle \bar{1} \rangle$

* para definir $f: \mathbb{Z}_{100} \to U(101)$ tenemos que dar $f(\bar{1})$

$o(f(\bar{1})) \mid o(\bar{1})$

$\Rightarrow o(f(\bar{1})) \mid 100$

$\left.\begin{array}{l} y \in U(101) \\ o(y) = |\langle y \rangle| \\ |\langle y \rangle| \mid |U(101)| \end{array}\right\} \Rightarrow o(y) \mid |U(101)| \Rightarrow o(y) \mid 100$

el orden de cualquier elemento de $U(101)$ divide a 100

por ejemplo podemos tomar $f(\bar{1}) = \bar{2}$

$f: \mathbb{Z}_{100} \to U(101)$

$f(\bar{1}^k) \underset{\uparrow}{=} f(\bar{1})^k = \bar{2}^k$

morfismo de grupos