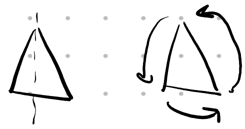
Segundo parcial 2023 (segundo semestre)

Ejercicio 5. El número de homomorfismos que existen de $\mathbb{Z}_9$ (los enteros módulo 9) a $D_3 = \{id, r_1, r_2, s_1, s_2, s_3\}$ (el grupo dihedral de orden 6), es:

(A) 0. (B) 1. (C) 2. (D) 3.



$f: \mathbb{Z}_9 \to D_3$ homomorfismo de grupo

* $\mathbb{Z}_9$ cíclico?

$\mathbb{Z}_9 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\}$ con la suma.

hay algún elemento de orden 9?

$o(\bar{1}) = 9$

$\mathbb{Z}_9 = \langle \bar{1} \rangle$

entonces para definir un morfismo de grupos $f: \mathbb{Z}_9 \to D_3$ alcanza con dar $f(\bar{1})$

sea $a \in \mathbb{Z}_9$

como $\mathbb{Z}_9 = \langle \bar{1} \rangle$ existe $n \in \mathbb{Z}$ tal que $a = \bar{1}^n = \underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{n \text{ veces}}$

entonces $f(a) = f(\bar{1}^n) = f(\bar{1} + \bar{1} + \dots + \bar{1}) = f(\bar{1}) \circ f(\bar{1}) \circ \dots \circ f(\bar{1}) = f(\bar{1})^n$

f morfismo de grupos: $f(x+y) = f(x) \circ f(y)$

* posibilidades para $f(\bar{1})$

$\boxed{o(f(x)) \mid o(x)}$

$o(\bar{1}) = 9$

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

$f(\bar{1})$ es un elemento de D_3 cuyo orden divide a 9

D_3

g	$o(g)$	
id	1	✓
r_1	3	✓
r_2	3	✓
s_1	2	X

entonces tenemos tres posibilidades:

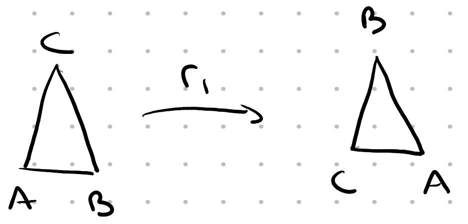
* $f(\bar{1}) = id$ (morfismo trivial)

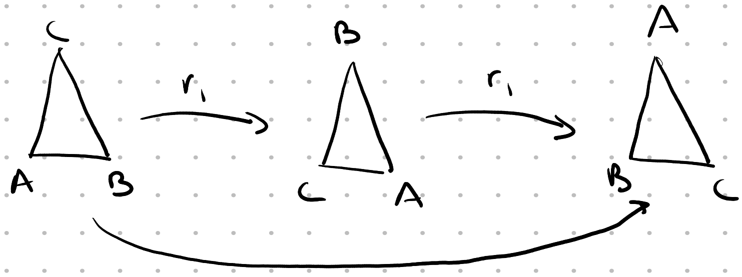
* $f(\bar{1}) = r_1$

* $f(\bar{1}) = r_2$

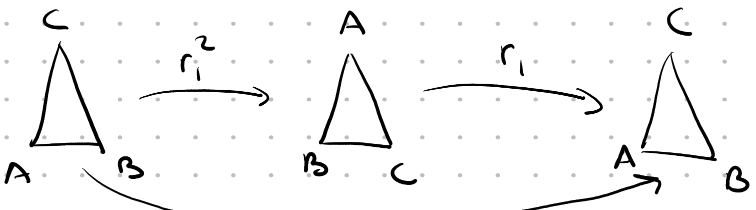
s_2	2	X
s_3	2	X

$\Rightarrow$ hay 3 morfismos de grupos de $\mathbb{Z}_4$ en D_3



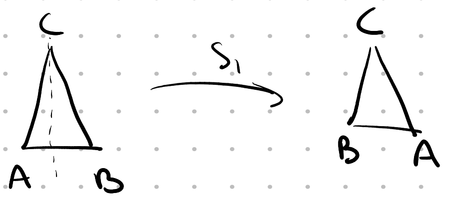


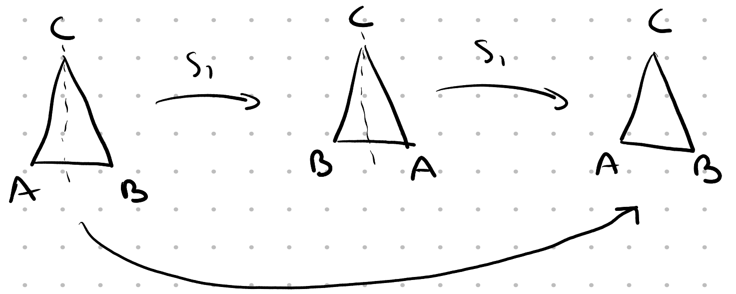
$r_1^2 = r_1 \circ r_1 \neq id$



$o(r_1) = 3$

$r_1^3 = r_1 \circ r_1 \circ r_1 = id$





$o(s_1) = 2$

$s_1^2 = s_1 \circ s_1 = id$

Ejercicio 6. Determinar exactamente cuáles de los siguientes enteros $\{13, 21, 48, 53\}$ son solución a la ecuación $7^x \equiv 1 \pmod 9$.

(A) $x = 21$ y $x = 48$.

(B) $x = 13$ y $x = 48$.

(C) $x = 21$ y $x = 53$.

(D) $x = 21$, $x = 48$ y $x = 53$.

Forma 1:

$7^x \equiv 1 \pmod 9 \rightsquigarrow \bar{7}^x = \bar{1}$ en $U(9)$

$\Leftrightarrow o(\bar{7}) \mid x$

$a^{o(a)} = e$

$a^n = e \Leftrightarrow o(a) \mid n$

vamos a buscar el orden de $\bar{7}$ en $U(9)$

$7^2 \equiv 49 \equiv 4 \pmod 9 \rightsquigarrow \bar{7}^2 = \bar{4}$

$7^3 \equiv 7^2 \cdot 7 \equiv 4 \cdot 7 \equiv 28 \equiv 1 \pmod 9 \rightsquigarrow \bar{7}^3 \equiv \bar{1}$

entonces $o(\bar{7}) = 3$

$7^x \equiv 1 \pmod 9 \Leftrightarrow \bar{7}^x = \bar{1}$ en $U(9)$

$\Leftrightarrow o(\bar{7}) \mid x$

$\Leftrightarrow 3 \mid x$

entonces $x = 21$, $x = 48$ son solución

<u>Forma 2</u>

* calculamos $7^{13} \pmod 9$

como 9 y 7 son coprimos podemos aplicar el teorema de Euler

$\varphi(9) = 9\left(1 - \frac{1}{3}\right) = 9 \cdot \frac{2}{3} = 6$

$9 = 3^2$

teorema de Euler: $7^6 \equiv 1 \pmod 9$

$13 = 6 \cdot 2 + 1$

$7^{13} \equiv 7^{6 \cdot 2 + 1} \equiv \underbrace{(7^6)^2}_{\equiv 1} \cdot 7 \equiv 7 \pmod 9 \Rightarrow x = 13$ no es solución

* $7^{21} \pmod 9$

teorema de Euler: $7^6 \equiv 1 \pmod 9$

$21 = 6 \cdot 3 + 3$

$7^{21} \equiv 7^{6 \cdot 3 + 3} \equiv \underbrace{(7^6)^3}_{\equiv 1} 7^3 \equiv 7^3 \equiv 7^2 \cdot 7 \equiv 4 \cdot 7 \equiv 28 \equiv 1 \pmod 9$

$\Rightarrow x = 21$ es solución

- **Pregunta 2:** (15 puntos)

1) (5 puntos) Demostrar que si $f : G \to H$ es un homomorfismo de grupos entonces su kernel es un subgrupo normal de G.
2) (10 puntos) Demostrar que si N es un subgrupo normal de G entonces:
   a. G/N es un grupo.
   b. El mapa $\pi : G \to G/N$, definido $\pi(g) = gN$, es un homomorfismo sobreyectivo.
   c. El kernel de π es N.

① $\ker(f) = \{h \in G \text{ tq } f(h) = e_H\}$

para ver que $\ker(f)$ es un subgrupo normal queremos ver que

$$g \ker(f) g^{-1} = \ker(f) \quad \text{para todo } g \in G$$

$$g \ker(f) = \ker(f) g$$

alcanza con ver que $g \ker(f) g^{-1} \subset \ker(f)$ para todo $g \in G$

fijamos $g \in G$

sea ghg^{-1} con $h \in \ker(f)$

queremos ver que $ghg^{-1} \in \ker(f)$

es decir queremos ver que $f(ghg^{-1}) = e_H$

$$f(ghg^{-1}) \underset{\substack{\uparrow \\ f \text{ morfismo} \\ \text{de grupos}}}{=} f(g) f(h) f(g^{-1}) \underset{\substack{\uparrow \\ h \in \ker(f)}}{=} f(g) e_H f(g^{-1}) = f(g) f(g^{-1})$$

$$\underset{f \text{ morfismo de grupos}}{=} f(gg^{-1})$$

$$= f(e_G)$$

$$\underset{\substack{\uparrow \\ f \text{ morfismo} \\ \text{de grupos}}}{=} e_H$$

entonces $f(ghg^{-1}) = e_H$

$\Rightarrow ghg^{-1} \in \ker(f)$

entonces $g \ker(f) g^{-1} \subset \ker(f)$

$\Rightarrow \ker(f)$ es un subgrupo normal de G

② N subgrupo normal de G

Queremos probar que $G/_N$ es un grupo

i) definimos la operación: $(aN)(bN) = \underset{\uparrow}{(ab)}N$

operación de G

ii) la operación está bien definida

$$(aN)(bN) \underset{\uparrow}{=} (xy)N$$

$x \in aN$

$y \in bN$

tenemos que probar que $\begin{cases} xN = aN \\ yN = bN \end{cases} \Rightarrow (xy)N = (ab)N$

vamos a probar $(xy)N = (ab)N$

veamos que $ab \in (xy)N$

$ab = xyn$ para algún n

* $xN = aN$

$\Rightarrow a \in xN$

$\Rightarrow a = xm$ para algún $m \in N$

* $yN = bN$

$\Rightarrow b \in yN$

$\Rightarrow b = ym'$ para algún $m' \in N$

entonces: $ab = x\overbrace{my}^{\in Ny = yN}m'$

$my \in Ny$

como N es subgrupo normal: $Ny = yN$

entonces $my \in yN$

$\Rightarrow my = ym''$ para algún $m'' \in N$

$ab = xyn$

entonces: $ab = xmym' = xy\overbrace{m''m}^{\in N}{}^{\in N}$ $m''m \in N$ porque $m'' \in N$ y $m \in N$

conclusión $ab \in (xy)N$

$$\Rightarrow (ab)N = (xy)N$$

y obtenemos que la operación está bien definida

$$(aN)(bN) = (ab)N$$

iii) la operación tiene neutro

$$\underbrace{(aN)(xN)}_{(ax)N} = aN$$

producto de G

$$e_{G/N} = e_G N$$

$$(aN)(e_G N) = (ae_G)N = aN \checkmark$$

iv) la operación es asociativa

$$((aN)(bN))(cN) = (aN)((bN)(cN))$$

$$\begin{aligned}((aN)(bN))(cN) &= ((ab)N)(cN)\\ &= ((ab)c)N\\ &= (a(bc))N\\ &= (aN)((bc)N)\\ &= (aN)((bN)(cN))\end{aligned}$$

v) tiene inversos

$$(aN)^{-1} = a^{-1}N$$

$$(aN)(a^{-1}N) = (aa^{-1})N = e_G N = e_{G/N}$$