(b) Sea G un grupo y $x, y \in G$ elementos de orden finito. Probar que si $xy = yx$ y $\text{mcd}(o(x), o(y)) = 1$, entonces $o(xy) = o(x)o(y)$.

$U(25) = U(5^2)$

$U(p^2)$ existe raíz primitiva módulo 25

G un grupo

$x, y \in G$ con orden finito

$o(x) = n \rightsquigarrow x^n = e_G$

$o(y) = m \rightsquigarrow y^m = e_G$

Queremos ver que

$$\left.\begin{array}{l} xy = yx \\ \text{mcd}(n, m) = 1 \\ \quad o(x) \quad o(y) \end{array}\right\} \Rightarrow o(xy) = o(x)o(y) = nm$$

* veamos que $(xy)^{nm} = e_G$

x e y conmutan

$$(xy)^{nm} = \underbrace{xy\,xy \cdots xy\,xy}_{nm \text{ veces}} = \underbrace{xx\cdots x}_{nm \text{ veces}}\underbrace{yy\cdots y}_{nm \text{ veces}}$$

$$= x^{nm} y^{nm}$$

$$= (x^n)^m (y^m)^n$$

$$= (e_G)^m (e_G)^n$$

$$= e_G$$

* veamos que nm es la menor potencia positiva de xy que nos da el neutro

tomemos $t \in \mathbb{Z}^+$ tal que $(xy)^t = e_G$

tenemos que ver que $nm \mid t$

como n y m son coprimos alcanza con ver que $n \mid t$ y $m \mid t$

$\rightarrow$ veamos que $n \mid t$

$(xy)^t = e_G$

$((xy)^t)^m = e_G^m$

$(xy)^{tm} = e_G$) $xy = yx$

$x^{tm} \underbrace{y^{tm}}_{(y^m)^t} = e_G$

$= e$

$x^{tm} = e_G \Rightarrow o(x) \mid tm$

$\Rightarrow n \mid tm$

$\Rightarrow n \mid t$ porque $mcd(n,m) = 1$

→ veamos $m \mid t$

$(xy)^t = e_G \Rightarrow ((xy)^t)^n = e_G^n$

$\Rightarrow (xy)^{tn} = e_G$

$\Rightarrow \underbrace{x^{tn}}_{=e_G} y^{tn} = e_G$

$\Rightarrow y^{tn} = e_G$

$\Rightarrow o(y) \mid tn$

$\Rightarrow m \mid tn$

$\Rightarrow m \mid t$ porque $mcd(m,n) = 1$

en conclusión

$n \mid t$

$m \mid t$

n y m coprimos

$\Rightarrow nm \mid t$

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.

$f: \mathbb{Z}_9 \longrightarrow D_3$

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

$\Rightarrow \mathbb{Z}_9$ es cíclico

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

$$f(\bar{a}) = f(\underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{a \text{ veces}}) = f(\bar{1}) \circ f(\bar{1}) \circ f(\bar{1}) \cdots \circ f(\bar{1})$$

$\uparrow$ f morfismo de grupos

→ ¿cuántas posibilidades hay para $f(\bar{1})$?

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

para definir $f(\bar{1})$ buscamos elementos en D_3 que tengan un orden que divide a 9

D_3

g	o(g)	
id	1	✓
r_1	3	✓
r_2	3	✓
s_1	2	X
s_2	2	X
s_3	2	X

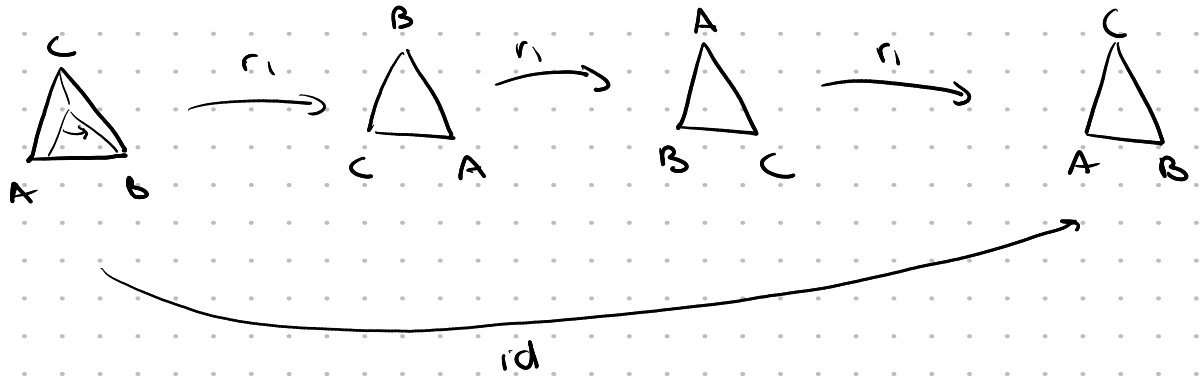
tenemos 3 posibilidades para $f(\bar{1})$

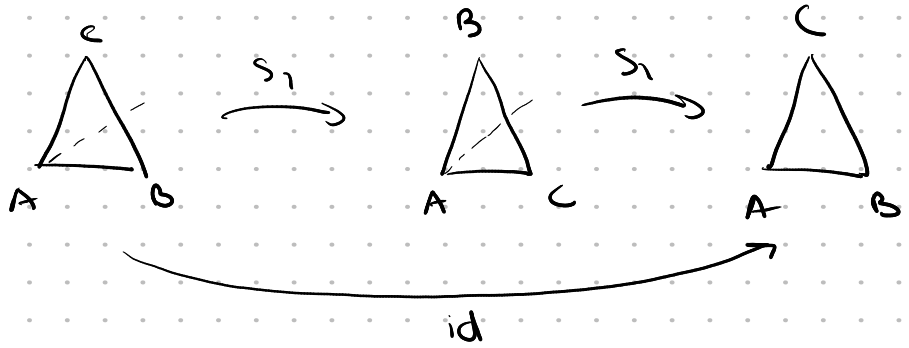
* $f(\bar{1}) = id$ ← morfismo trivial
* $f(\bar{1}) = r_1$
* $f(\bar{1}) = r_2$

hay 3 morfismos de grupos de $\mathbb{Z}_9$ en D_3

$f(\bar{1}) = r_1 \rightsquigarrow f(\bar{5}) = f(\bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1})$

$= f(\bar{1})^5 = r_1^5 = r_1^2 = r_2$





b) (6 puntos) Encuentre todos los homomorfismos $f : U(7) \to \mathbb{Z}_9$. Debe escribir cada homomorfismo explícitamente en la forma $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ f(1) & f(2) & f(3) & f(4) & f(5) & f(6) \end{pmatrix}$.

$U(7) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$U(7)$ cíclico?

2 es raíz primitiva modulo 7? no

$\varphi(7) = 6 = 2 \cdot 3$

2 es raíz primitiva modulo 7 $\iff$ $\begin{cases} \overline{2^2} = \bar{4} \neq 1 \pmod 7 \\ 2^3 = 8 \not\equiv 1 \pmod 7 \end{cases}$

3 es raíz primitiva modulo 7? sí

3 es raíz primitiva modulo 7 $\iff$ $\begin{cases} 3^2 \not\equiv 1 \pmod 7 \checkmark \\ 3^3 \not\equiv 1 \pmod 7 \checkmark \end{cases}$

$3^2 \equiv 9 \equiv 2 \pmod 7$

$3^3 \equiv 27 \equiv 6 \pmod 7$

entonces $U(7)$ es cíclico y $U(7) = \langle \bar{3} \rangle$

para dar un morfismo de grupos $f: U(7) \longrightarrow \mathbb{Z}_9$

alcanza con dar $f(\bar{3})$

→ posibilidades para $f(\bar{3})$?

$\mathbb{Z}_9$

g	$o(g)$
$\bar{0}$	1 ✓
$\bar{1}$	9
$\bar{2}$	9
$\bar{3}$	3 ✓
$\bar{4}$	9
$\bar{5}$	9
$\bar{6}$	3 ✓
$\bar{7}$	9
$\bar{8}$	9

$o_{U(7)}(\bar{3}) = 6$

entonces las posibilidades por $f(\bar{3})$ son

- $f(\bar{3}) = \bar{0}$
- $f(\bar{3}) = \bar{3}$
- $f(\bar{3}) = \bar{6}$

* $f: U(7) \to \mathbb{Z}_9$ dado por $f(\bar{3}) = \bar{0}$

$$f = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} \end{pmatrix}$$

* $f: U(7) \to \mathbb{Z}_9$ dado por $f(\bar{3}) = \bar{3}$

$$f = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{0} & \bar{6} & \bar{3} & \bar{3} & \bar{6} & \bar{0} \end{pmatrix}$$

$3^2 \equiv 9 \equiv 2 \pmod 7 \rightsquigarrow \bar{2} = \bar{3}^2$ en $U(7)$

$f(\bar{2}) = f(\bar{3} \cdot \bar{3}) = f(\bar{3}) + f(\bar{3}) = \bar{3} + \bar{3} = \bar{6}$

$3^3 \equiv 2 \cdot 3 \equiv 6 \pmod 7 \rightsquigarrow \bar{6} = \bar{3}^3$ en $U(7)$

$f(\bar{6}) = f(\bar{3} \cdot \bar{3} \cdot \bar{3}) = f(\bar{3}) + f(\bar{3}) + f(\bar{3}) = \bar{3} + \bar{3} + \bar{3} = \bar{0}$

$3^4 \equiv 6 \cdot 3 \equiv 4 \pmod 7 \rightsquigarrow \bar{4} = \bar{3}^4$ em $U(7)$

$$f(\bar{4}) = f(\bar{3}^4) = \bar{3}+\bar{3}+\bar{3}+\bar{3} = \bar{3}$$

* $f: U(7) \to \mathbb{Z}_9$ dado por $f(\bar{3}) = \bar{6}$

$$f = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{0} & \bar{3} & \bar{6} & & & \end{pmatrix}$$

$$f(\bar{2}) = f(\bar{3}^2) = f(\bar{3}) + f(\bar{3}) = \bar{6} + \bar{6} = \bar{3}$$