[Büten Zar]
B.Sz

Comentarios

Büten Zar

FB

Letra

Ejercicio 1

Ejercicio 2

Ejercicio 3

Ejercicio 4

Ejercicio 5

Ejercicio 6

Ejercicio 7

Ejercicio 8

Ejercicio 9

Ejercicio 10

Ejercicio 1 Menu [Büten Zar] B.Sz

① El neutro de G es único.

Demostración:

Sean e_1 y e_2 neutros, es decir: ⓘ $a * e_1 = e_1 * a = a \quad \forall a \in G$

ⓘⓘ $a * e_2 = e_2 * a = a \quad \forall a \in G$.

en ⓘ uso en particular $a = e_2$ y obtengo $e_2 * e_1 = e_1 * e_2 = e_2$

en ⓘⓘ uso en particular $a = e_1$ y obtengo $e_1 * e_2 = e_2 * e_1 = e_1$

Por transitiva de la igualdad, $e_1 = e_1$.

② El inverso de $g \in G$ es único.

Demostración:

Sean g' y g'' los inversos de g, es decir: ⓘ $g * g' = g' * g = e$

ⓘⓘ $g * g'' = g'' * g = e$

$$\Rightarrow \quad g * g' = g * g''$$

utilizo la propiedad cancelativa por la izq.

$$g' = g''$$

(3) $(ab)^{-1} = b^{-1}a^{-1} \quad \forall\, a,b \in G$

Demostración:

asociativa

$$(ab)^{-1}.(a.b) = (a.b).(ab)^{-1} = e \qquad \text{sea } c = (ab)^{-1}$$

$$(c.a).b = a.(b.c) = e$$

$$\begin{cases} (c.a).b = e \Rightarrow c.a = b^{-1} \\ a(b.c) = e \Rightarrow b.c = a^{-1} \end{cases}$$

Entonces $\underbrace{ca.bc}_{e} = b^{-1}.a^{-1} \Rightarrow c = b^{-1}a^{-1} \quad \forall\, a,b \in G$

(4) Si $x.g = xh \Rightarrow g = h$

Demostración:

Por (H) $xg = xh \Rightarrow x^{-1}xg = x^{-1}xh \Rightarrow \overbrace{(x^{-1}.x)}^{e}g = \overbrace{(x^{-1}x)}^{e}h \Rightarrow g = h$

(5) Si $gx = hx \Rightarrow g = h$

Demostración:

Por (H) $gx = hx \Rightarrow (gx)x^{-1} = (hx)x^{-1} \overset{\text{asociativa}}{\Rightarrow} g(xx^{-1}) = h(xx^{-1}) \Rightarrow g.e = h.e$

$\Rightarrow g = h$

6) $(ab)^{-1} = a^{-1}.b^{-1} \quad \forall a,b \in G \iff G$ es abeliano $(a.b = b.a)$

Demostración:

$(\Rightarrow)$ (H) $(ab)^{-1} = a^{-1}b^{-1} \quad \forall a,b \in G$ (T) $a.b = b.a$

$$\left.\begin{array}{ll} \text{por } \underline{\text{prop 3}} & (ab)^{-1} = b^{-1}.a^{-1} \\ \text{por (H)} & (ab)^{-1} = a^{-1}.b^{-1} \end{array}\right\} \Rightarrow b^{-1}.a^{-1} = a^{-1}.b^{-1} \Rightarrow G \text{ es abeliano.}$$

$(\Leftarrow)$ (H) G es abeliano (T) $(ab)^{-1} = a^{-1}b^{-1} \quad \forall a,b \in G$

$$\left.\begin{array}{ll} \text{por prop 3} & (ab)^{-1} = b^{-1}.a^{-1} \\ & G \text{ es abeliano} \end{array}\right\} \Rightarrow b^{-1}.a^{-1} = a^{-1}.b^{-1} = (ab)^{-1}$$

7) $(ab)^2 = a^2b^2$ para todo $a,b \in G \iff G$ es abeliano.

Demostración:

$$(ab)^2 = a^2.b^2 \iff (ab)(ab) = a.a.b.b \overset{\text{asociativa}}{\iff} a(ba)b = a(ab)b$$

$$\underset{\text{opero}}{\overset{\text{prop 4 y 5}}{\iff}} ba = ab$$

8) Si $(ab)^3 = e_G \quad \forall a,b \in G \Longrightarrow (ba)^3 = e_G$

Demostración:

$$(ab).(ab).(ab) = e_G \iff a^{-1}.(a.b).(a.b).(a.b) = a^{-1}.e_G \iff (a^{-1}.a).b.(a.b).(a.b) = a^{-1}$$

$$\iff e.b.(a.b).(a.b).a = a^{-1}.a \iff (b.a).(b.a).(b.a) = e_G \iff (b.a)^3 = e_G$$

9 $(a^n)^{-1} = (a^{-1})^n \quad \forall a \in G \,, n \in \mathbb{N}$

Demostración: Por IC.

Paso base: $n=1$

$$a^{-1} = a^{-1}$$

Paso inductivo:

H $n = h$

$$(a^h)^{-1} = (a^{-1})^h$$

T $n = h+1$

$$(a^{h+1})^{-1} = (a^{-1})^{h+1}$$

Demostración:

$$(a^{h+1})^{-1} = (a^{-1})^{h+1} \iff (a^1 . a^h)^{-1} = (a^{-1})^h . a^{-1} \overset{\text{prop } 3}{\iff} (a^h)^{-1} \underbrace{(a^1)^{-1}}_{a^{-1} \text{ paso base}} = (a^{-1})^h . a^{-1}$$

$$\overset{\text{cancelativa}}{\iff} (a^h)^{-1} = (a^{-1})^h$$

Menu

Ejercicio 2 : Investigar si los siguientes conjuntos con las respectivas operaciones que se definen son grupos:

① El conjunto $M_{nxn}(\mathbb{R})$ y la operación es el producto usual de matrices $A * B = A.B$

i) Cierre, se cumple

ii) Asociativa : $\forall a, b, c \in G \qquad (A * B) * C = A * (B * C)$

iii) "Neutro" : $\exists$ la matriz ID $\quad I.A = A.I = A \quad \forall A \in G$

iv) "Inverso" : $\forall A \; \exists \; A^{-1}$, Falso, solo $\exists \; A^{-1}$ si $\det(A) \neq 0$

No es un grupo.

② El conjunto $M_{nxn}(\mathbb{R})$ con la operación $A * B = AB + BA$

i) Cierre, se cumple

ii) Asociativa : $\forall A, B, C \in G \qquad (A * B) * C = A * (B * C)$

$$(AB + BA) * C = A * (BC + CB)$$

$$(AB + BA).C + C(AB + BA) = A(BC + CB) + (BC + CB)A$$

$$\cancel{ABC} + BAC + CAB + \cancel{CBA} = \cancel{ABC} + ACB + BCA + \cancel{CBA}$$

$$¿\; BAC + CAB = ACB + BCA \quad \forall A, B, C \in G \; ?$$

Falso, el producto de matrices no es conmutativo para todas las matrices.

No es un grupo.

③ El conjunto es $\mathbb{R}^2$ y la operación es : $(x_1, x_2) * (y_1, y_2) = (x_1 y_1 , x_2 y_1 + y_2)$

i) cierre, se cumple.

ii) Asociativa: $\forall\ x, y, z \quad [(x_1, x_2) * (y_1, y_2)] * (z_1, z_2) = (x_1, x_2) * [(y_1, y_2) * (z_1, z_2)]$

$$(x_1 y_1 , x_2 y_1 + y_2) * (z_1, z_2) = (x_1, x_2) * (y_1 z_1 , y_2 z_1 + z_2).$$

$$(x_1 y_1 z_1 , (x_2 y_1 + y_2) z_1 + z_2) = (x_1 y_1 z_1 , x_2 y_1 z_1 + (y_2 z_1 + z_2))$$

$$(x_1 y_1 z_1 , z_1 x_2 y_1 + z_1 y_2 + z_2) = (x_1 y_1 z_1 , x_2 y_1 z_1 + y_2 z_1 + z_2) \quad \text{ok} \checkmark$$

iii) Neutro: $\exists\ n \ / \ (x_1, x_2) * n = n * (x_1, x_2) = (x_1, x_2) \qquad \forall (x_1, x_2) \in \mathbb{R}^2$

$$\boxed{\exists\ n = (1,0)}$$

iv) "inverso o opuesto" $\forall (x_1, x_2) \in \mathbb{R}^2 \ \exists\ (x_1', x_2') \ / \quad (x_1, x_2) * (x_1', x_2') = (x_1', x_2') * (x_1, x_2) = (1,0)$

① $(x_1, x_2) * (x_1', x_2') = (x_1 x_1' , x_2 x_1' + x_2') = (1, 0)$

② $(x_1', x_2') * (x_1, x_2) = (x_1' x_1 , x_2' x_1 + x_2) = (1, 0)$

① $\begin{cases} x_1 x_1' = 1 \\ x_2 x_1' + x_2' = 0 \end{cases} \Rightarrow x_2' = -x_2 x_1' \Rightarrow \boxed{\dfrac{x_2'}{-x_2} = x_1'}$

② $\begin{cases} x_1' x_1 = 1 \\ x_2' x_1 + x_2 = 0 \end{cases} \Rightarrow x_2 = -x_2' x_1 \Rightarrow \boxed{-\dfrac{x_2}{x_1} = x_2'}$

tomo como contraejemplo el vector $(0,0)$, ese vector no tiene inverso.

$\Longrightarrow$ No es un grupo.

4) $G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in \mathbb{Z} \right\}$ y $*$ el producto matricial

i) Cierre, se cumple

ii) Asociativa: $\forall A, B, C \in G \quad (A*B)*C = A*(B*C)$ se cumple, prod mat ✓

iii) $\exists$ neutro: $\exists\, I \in G \,/\, I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A*I = I*A = A \quad \forall A \in G$

iv) $\exists$ inverso: El inverso existe siempre pues $\forall A \in G$ $Det(A) = 1$.

Vamos a verificar que el inverso $\in G$.

$$\left(\begin{array}{ccc|ccc} 1 & a & c & 1 & 0 & 0 \\ 0 & 1 & b & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|ccc} 1 & a & 0 & 1 & 0 & -c \\ 0 & 1 & 0 & 0 & 1 & -b \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \rightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -a & ab-c \\ 0 & 1 & 0 & 0 & 1 & -b \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$A^{-1} = \begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \in G$$

$(G; \cdot)$ es un grupo.

⑤ El conjunto es $\{a, b, c\}$ y la operación $*$

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

i) Cierre, se cumple.

ii) Asociativa:

$-\ (a*b)*c = a*(b*c)$

$b*c = a*a$

$a = a$

$-\ (c*b)*a = c*(b*a)$

$a*a = c*b$

$a = a$

$-\ (b*a)*c = b*(a*c)$

$b*c = b*c$

$-\ (c*a)*b = c*(a*b)$

$c*b = c*b$

$-\ (a*c)*b = a*(c*b)$

$c*b = c*b$

$-\ (b*c)*a = b*(c*a)$

$a*a = b*c$

$a = a$

cumple la asociativa.

iii) $\exists$ del neutro. $\exists\, a \in G \;/\; x*a = a*x = x \quad \forall x \in G$

a es el neutro de G

iv) $\exists$ del inverso: para a.

$a*a = a*a = a$

para b

$b*c = c*b = a \qquad b^{-1} = c$

para c

$c*b = b*c = a \qquad c^{-1} = b$

$(\{a, b, c\}, *)$ es un grupo.

⑥ El conjunto es $\{a,b,c,d\}$ y la operación $*$ se define

$*$	a	b	c	d
a	a	b	c	d
b	b	c	a	a
c	c	a	b	b
d	d	a	b	c

¡Atención Sudoku!

i) Cierre, se cumple

ii) Asociativa: $\quad -\ (b*c)*d = b*(c*d)$

$$a*d = b*b$$

$$d = c \quad \times$$

$(\{a,b,c,d\}, *)$ no es un grupo. No cumple la asociativa.

⑦ El conjunto $\mathbb{Z}$ con la operación $*$: $a*b = ab - 2(a+b) + 6$

i) Cierre, se cumple.

ii) Asociativa, se cumple.

nota: el neutro y el inverso deben pertenecer al conjunto

iii) $\exists$ neutro. $\exists\, e \,/\, x*e = e*x = x \quad \forall x \in G$

$$x \circledast e = x.e - 2x - 2e + 6 = x$$

$$e(x-2) = 3x - 6$$

$$e = \frac{3x-6}{x-2} = 3 \qquad \boxed{e=3}$$

iv) $\exists$ inverso $\quad \forall x \in \mathbb{Z},\ \exists\, x^{-1} \,/\, x \circledast x^{-1} = x^{-1} \circledast x = 3$

$$x \circledast x^{-1} = x.x^{-1} - 2x - 2x^{-1} + 6 = 3$$

$$x^{-1}(x-2) = 2x - 3$$

$$x^{-1} = \frac{2x-3}{(x-2)}$$

cuando $x = 2$ no existe el inverso.

No es un grupo.

Ejercicio 3

Menu

Sea $G = \{e, a, b, c, d, f\}$ tal que $(G, \cdot)$ es un grupo. Completar la tabla de Cayley si se tiene la información parcial siguiente:

		2		4	5	
·	e	a	b	c	d	f
e	e	a	b	c	d	f
2 a	a	b	e	d	f	c
3 b	b	e	a	f	c	d
4 c	c	f	d	e	b	a
5 d	d	c	f	a	e	b
f	f	d	c	b	a	e

sudoku

tenemos que $a \circledast b = e \Rightarrow b \circledast a = e$

$- \; b \circledast f = d \Rightarrow (a \circledast b) \circledast f = a \circledast d$

$f = a \circledast d$

$- \; b \circledast c = f \Rightarrow (a \circledast b) \circledast c = a \circledast f$

$c = a \circledast f$

sudokú columna.

$f \circledast f = e$

$- \; f \circledast c = b \Rightarrow f \circ f \circ c = f \circ b$

$c = f \circ b$

$- \; f \circ b = c \Rightarrow f \circ \underbrace{b \circ a}_{e} = c \circ a \Rightarrow f = c \circ a$

$- \; f \circ d = a \Rightarrow \boxed{d = f \circ a} \Rightarrow \boxed{d \circ b = f}$

Columna 2-2 por sudoku puede solo ir b.

Columna 2-5 " " c

$- \; d \circ a = c \Rightarrow d = c \circ b$

Columna 4-4 por sudoku puede solo ir e

Columna 4-2 por sudoku " " " d

" 4-5 " " " a

" 5-5 " " e

" 5-3 " " c

" 3-3 " " a

Ejercicio 4

Menu

[Büten Zar]
B.Sz

① $G = (\mathbb{Z}, +)$ y $H = n\mathbb{Z}$ el conjunto de los enteros $\dot{n}$ (para $n \in \mathbb{Z}$ dado)

condición 1: $H \subset G$, $H \neq \emptyset$ ok ✓

condición 2: $\forall\ a, b \in H$ $(a+b) \in H$

$\dot{n} + \dot{n} = \dot{n} \rightarrow (a+b) \in H$ ok ✓

condición 3: $\forall\ a \in H \Rightarrow a^{-1} \in H$

Sea $a = n.q \Rightarrow a^{-1} = -n.q$ y $-n\,q \in H$.

condición 4: El neutro de $G \in H$

$e_G = 0$ y $0 = n.0 \Rightarrow 0 \in H$.

H es un subgrupo de G.

② $G = \mathbb{R} \setminus \{0\}$ con el producto y $H = \mathbb{R}^+$ el conjunto de los reales positivos.

condición 1: $H \subset G$, $H \neq \emptyset$

condición 2: El neutro de $G \in H$, $e_G = 1$ y $1 \in H$

condición 3: $\forall\ a, b \in H$ $(a.b) \in H$

Dos reales positivos multiplicados dan otro real positivo

condición 4: $\forall\ a \in H \Rightarrow a^{-1} \in H$

$\forall\ a$ real positivo $\exists\ a^{-1} = \frac{1}{a}$ real positivo. $\frac{1}{a} \in H$

H es un subgrupo de G.

③ $G = GL_2(\mathbb{R})$ (Matrices invertibles 2x2 con coeficientes reales) con el producto usual de matrices y $H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_{2x2}(\mathbb{R}) : a.c \neq 0 \right\}$

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2x2}(\mathbb{R}) \ / \ ad - bc \neq 0 \right\}$$

Condición 1 : $H \subset G$, $H \neq \emptyset$ ok ✓

condición 2 : El neutro de $G \in H$

$$e_G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad y \quad e_G \in H$$

condición 3 : $\forall A, B \in H \ . \ A.B \in H$

$$A = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \quad B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

$$A.B = \begin{pmatrix} a'a & a'b + b'c \\ 0 & cc' \end{pmatrix} \in H \qquad \begin{array}{l} a.c \neq 0 \\ a'.c' \neq 0 \end{array}$$

$aa'cc' \neq 0$ ok ✓

condición 4 : $\forall A \in H \Longrightarrow A^{-1} \in H$

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ 0 & c & 0 & 1 \end{array} \right) = \left(\begin{array}{cc|cc} a & b & 1 & 0 \\ 0 & 1 & 0 & 1/c \end{array} \right)$$

$$A^{-1} = \begin{pmatrix} 1/a & -b/a.c \\ 0 & 1/c \end{pmatrix} \quad \left(\begin{array}{cc|cc} a & 0 & 1 & -b/c \\ 0 & 1 & 0 & 1/c \end{array} \right) = \left(\begin{array}{cc|cc} 1 & 0 & 1/a & -\frac{b}{a.c} \\ 0 & 1 & 0 & 1/c \end{array} \right)$$

por $A \in H$ se tiene que $\left. \begin{array}{l} a \neq 0 \\ c \neq 0 \end{array} \right\} a.c \neq 0 \Rightarrow \frac{1}{a.c} \neq 0 \qquad A^{-1} \in H$

H es un subgrupo de G

4) $G = GL_2(\mathbb{R})$ y $H = \{ M \in G : \det(M) = 1 \}$ (Supongo operacion . usual mat)

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{R}) \;\middle/\; ad - bc \neq 0 \right\}$$

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{R}) \;\middle|\; ad - bc = 1 \right\}$$

Condición 1: $H \subset G$, $H \neq \emptyset$ ok ✓

condición 2: El neutro de $G \in H$

$$e_G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \det(e_G) = 1 \implies e_G \in H$$

condición 3: $\forall A, B \in H$, $A.B \in H$

$$\det(A) = 1 \quad \det(B) = 1 \qquad \det(A.B) = \det(A).\det(B) = 1$$

$$\implies A.B \in H$$

condición 4: $\forall A \in H$, $\exists A^{-1}$ en G y $A^{-1} \in H$

$\forall A \in H \; \exists A^{-1}$ pues $\det(A) \neq 1$

$$\det(A^{-1}) = \frac{1}{\det(A)} = 1 \implies A^{-1} \in H$$

H es un subgrupo de G

(5) $G = \mathbb{Q}^+$ con el producto y $H = \left\{ \frac{a}{b} \in \mathbb{Q} : a \equiv 0 \pmod 7 ,\ MCD(b,7) = 1 \right\}$

condición 1: $H \subset \mathbb{Q}^+$, $H \neq \emptyset$

condición 2: El neutro de $G \in H$

$e_G = \frac{1}{1}$ ¿$1 \equiv 0 \pmod 7$? NO!!

No se cumple la condición 2, entonces H no es un subgrupo de G

(6) $G = D_3$ el grupo diedral y $H = \{id, r, r^2 s, s\}$ (r es una rotación y s una simetría axial)

$D_3 = \{$ "movimientos del plano que transforman al triángulo es sí mismo $\}$

Condición 1: $H \subset G$, $H \neq \emptyset$ ok ✓

Condición 2: El neutro de $G \in H$, La transformación $Id \in H$ ok

$e_G = ID$

Condición 3: $\forall\ a, b \in H$, $a \circ b \in H$

$(Id \circ a) \in H \quad \forall a \in H$

$(r \circ s) = s'$ y $s' \notin H$

no se cumple la condición 3, H no es subgrupo de G.

[Büten Zar]
B.Sz

(7) $G = S_3$ el grupo de permutaciones $(S_3, \circ)$ y $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$

condición 1: $H \subset G$, $H \neq \emptyset$ OK ✓

condición 2: El neutro de G. $e_G \in H$

$$e_G = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \in H$$

condición 3: $\forall g, f \in H$, $g \circ f \in H$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{ok}$$

operar con el neutro es trival, se cumple cond 3.

condición 4: $\forall g \in H$, $g^{-1} \in H$

se cumple. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = Id$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = Id$$

H es un subgrupo de G.

8 $G = S_3$ y $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$

$(S_3, \circ)$

Condición 1: $H \subset G$, $H \neq \emptyset$ ok ✓

Condición 2: El neutro de G, $e_G \in H$

$$e_G = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \in H$$

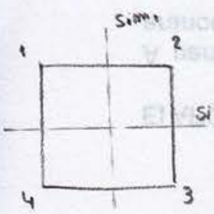
Condición 3: $\forall g, f \in H$, $g \circ f \in H$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H$$

La condición 3 no se cumple, entonces H no es un subgrupo de G.

9 $G = S_4$ y $H = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \underset{sim_1}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \underset{sim_2}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}} \right\}$

$(S_4, \circ)$



condición 1: $H \subset G$, $H \neq \emptyset$ ok ✓

Condición 2: El neutro de G, $e_G \in H$ $\quad e_G = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \in H$

Condición 3: $\forall f, g \in H$ $\quad f \circ g \in H$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$S_2 \circ S_1 = S_1 \circ S_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = S_3$$

$S_3 \circ S_2 = S_1$ $\quad$ Se cumple.

Condición 4: $\forall f \in H$, $f^{-1} \in H$

$S_1 \circ S_1 = ID$ $\quad ID \circ ID = ID$

$S_2 \circ S_2 = ID$

$S_3 \circ S_3 = ID$

H es un subgrupo de G.

Ejercicio 5

Sean H_1 y H_2 dos subgrupos de un grupo G.

1 Probar que $H_1 \cap H_2$ es un subgrupo de G

condición 1 : $H_1 \cap H_2 \subset G$ y $H_1 \cap H_2 \neq \emptyset$ ok $e_G \in H_1 \cap H_2$

condición 2: $e_G \in H_1 \cap H_2$

$$\left.\begin{array}{l} H_1 \text{ es un subgrupo} \Rightarrow e_G \in H_1 \\ H_2 \text{ es un subgrupo} \Rightarrow e_G \in H_2 \end{array}\right\} \Rightarrow e_G \in H_1 \cap H_2$$

condición 3: $\forall\, x, y \in H_1 \cap H_2 \Rightarrow x * y \in H_1 \cap H_2$

$$\text{Si } x, y \in H_1 \cap H_2 \Rightarrow \left.\begin{array}{l} x, y \in H_1 \underset{(H)}{\Rightarrow} x * y \in H_1 \\ x, y \in H_2 \underset{(H)}{\Rightarrow} x * y \in H_2 \end{array}\right\} x * y \in H_1 \cap H_2$$

condición 4: $\forall\, x \in H_1 \cap H_2$, $x^{-1} \in H_1 \cap H_2$

$$\text{Si } x \in H_1 \cap H_2 \Rightarrow \left.\begin{array}{l} x \in H_1 \underset{(H)}{\Rightarrow} x^{-1} \in H_1 \\ x \in H_2 \underset{(H)}{\Rightarrow} x^{-1} \in H_2 \end{array}\right\} \Rightarrow x^{-1} \in H_1 \cap H_2$$

Queda demostrado $H_1 \cap H_2$ es un subgrupo de G.

2 ¿Es $H_1 \cup H_2$ necesariamente un subgrupo de G?

contraejemplo $G = (\mathbb{Z}, +)$, $H_1 = (\mathbb{Z}^{pares}, +)$, $H_2 (\mathbb{Z}^{5}, +)$

$$\left.\begin{array}{l} 4 \in H_1 \\ 5 \in H_2 \end{array}\right\} 4, 5 \in H_1 \cup H_2 \quad \text{pero} \quad 4 \oplus 5 = 9 \notin H_1 \cup H_2$$

$\Rightarrow H_1 \cup H_2$ no es subgrupo.

Ejercicio 6 Menu

[Büten Zar]
B.Sz

G es un grupo abeliano, probar que H es subgrupo de G:

① $\boxed{H = \{a \in G : a^2 = e_G\}}$

$(G,*)$ es abeliano, o sea, $a*b = b*a \quad \forall a,b \in G$

condición 1 : $H \subset G \,,\; H \neq \emptyset$

condición 2 : $e_G \in H$

$$e_G^2 = e_G \Rightarrow e_G \in H$$

condición 3 : $\forall\, x,y \in H \,,\; x \circledast y \in H$

$$\left.\begin{array}{l} x^2 = e_G \\ y^2 = e_G \end{array}\right\} \Rightarrow \underbrace{x^2}_{e_G}\underbrace{y^2}_{e_G} = x*\underbrace{x*y}*y \overset{(H)}{=} x\circledast y\circledast x\circledast y = (x\circledast y)^2 = e_G$$

$$\Rightarrow x \circledast y \in H$$

condición 4 : $\forall\, x \in H \,,\; x^{-1} \in H$

$$x \in H \Rightarrow x^2 = e_G \Rightarrow x \circledast x = e_G \Rightarrow e_G = x^{-1} \circledast x^{-1} = (x^{-1})^2$$

$$\Rightarrow x^{-1} \in H$$

Queda demostrado.

② $\boxed{H = \{ a^n \mid a \in G \}}$ donde n es un entero positivo dado

condición 1: $H \subset G$, $H \neq \emptyset$

condición 2: $e_G \in H$

$e_G^n \in H$ $\quad e_G^n = e_G$ ok ✓

condición 3: $\forall a, b \in H$, $a * b \in H$

$a \in H \Rightarrow a = x^n$ para algún $x \in G$

$b \in H \Rightarrow b = y^n$ para algún $y \in G$

$x, y \in G \Rightarrow (x \circledast y) \in G \Rightarrow (x \circledast y)^n \in H$

$(x \circledast y)^n = x \circledast y \circledast x \circledast y \ldots \underset{\text{Abeliano}}{=} x^n \circledast y^n = a \circledast b$

$\Rightarrow a \circledast b \in H$

condición 4: $\forall a \in H$, $a^{-1} \in H$

$a \in H \Rightarrow a = x^n$ para algún $x \in G$

$x \in G \Rightarrow x^{-1} \in G \Rightarrow (x^{-1})^n \in H$ y $(x^{-1})^n = (x^n)^{-1} = a^{-1}$

Queda demostrado.

Ejercicio 7

Menu

Escriba la tabla de multiplicación de $U(18)$. Hallar los órdenes de los elementos de $U(18)$

¿Es $U(18)$ cíclico?

Recordamos: $U(18) = \{$ clases de congruencia de $\mathbb{Z}$ mod 18 tales que $\exists$ inverso mod 18 $\}$

$\left(a \pmod{18} \text{ es invertible} \iff \text{MCD}(a, 18) = 1\right)$

$$U(18) = \{ 1 \pmod{18},\ 13 \pmod{18},\ 5 \pmod{18},\ 7 \pmod{18},\ 11 \pmod{18},\ 17 \pmod{18} \}$$

$\cdot$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{11}$	$\bar{13}$	$\bar{17}$
$\bar{1}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{11}$	$\bar{13}$	$\bar{17}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{17}$	$\bar{1}$	$\bar{11}$	$\bar{13}$
$\bar{7}$	$\bar{7}$	$\bar{17}$	$\bar{13}$	$\bar{5}$	$\bar{1}$	$\bar{11}$
$\bar{11}$	$\bar{11}$	$\bar{1}$	$\bar{5}$	$\bar{13}$	$\bar{17}$	$\bar{7}$
$\bar{13}$	$\bar{13}$	$\bar{11}$	$\bar{1}$	$\bar{17}$	$\bar{7}$	$\bar{5}$
$\bar{17}$	$\bar{17}$	$\bar{13}$	$\bar{11}$	$\bar{7}$	$\bar{5}$	$\bar{1}$

$13 \equiv -5 \mod 18$

$\text{Ord}(\bar{1}) = 1$

Mirando tabla:

$\text{Ord}(\bar{7}) = 3$

$\text{ord}(\bar{11}) = 6$

$\text{ord}(\bar{13}) = 3$

$\text{ord}(\bar{17}) = 2$

$5^1 = 5 \mod 18$

$5^2 = 25 \equiv 7 \mod 18$

$5^3 \equiv 7.5 \equiv 17 \mod 18$

$5^4 \equiv 17.5 \equiv 13 \mod 18$

$5^5 \equiv 13.5 \equiv 11 \mod 18$

$5^6 \equiv 11.5 \equiv 1 \mod 18$

$\text{ord}(\bar{5}) = 6 = |U(18)|$

$\langle 5 \rangle = U(18)$

$U(18)$ es cíclico porque:

i) $|U(18)| = 6$ (es finito)

ii) $\langle \bar{5} \rangle = U(18)$

Ejercicio 8

Menu

(1) Sea G un grupo. Probar que si $a^n = e_G \Rightarrow \mathcal{O}(a) \mid n$

Por definición $\mathcal{O}(a) = m$ siendo m el mínimo natural que cumple $a^m = e_G$

Entonces $n \geq m$.

Entonces existen q y r / $n = mq + r$ con $r = 0$ o $r < m$

$$e_G = a^n = a^{mq+r} = (a^m)^q . a^r = e_G^q . a^r = a^r$$

$\Rightarrow a^r = e_G$

Pero m por def era el mínimo natural que cumplía $a^m = e_G$

Entonces $r > m$ ↯

Entonces $r = 0$ y $n = m.q \Rightarrow \mathcal{O}(a) \mid n$

(2) Sea G un grupo. Probar que si $a^n \neq e_G \Rightarrow \mathcal{O}(a) \nmid n$

Llamemosle m a $\mathcal{O}(a)$.

Si $m > n$ entonces queda demostrado

Si $m \leq n \Rightarrow n = mq + r$ $r < m$ o $r = 0$

$$a^n = a^{mq+r} = \underbrace{(a^m)^q}_{e_G} . a^r = a^r \Rightarrow a^n = a^r \Rightarrow n = r \Rightarrow r \neq 0$$

Si $n = r \Rightarrow m < r$ Abs!! $(r \neq 0)$

Por lo tanto m solo puede ser mayor que $\underline{n}$ y queda demostrado.

3 Sea G un grupo. Probar que $O(xy) = O(yx)$ $\forall x, y \in G$

Llamemosle $m = O(xy)$ y $n = O(yx)$.

por def: $\begin{cases} (xy)^m = e_G & xy \cdot xy \cdot xy \cdots = e_G \\ (yx)^n = e_G & yx \cdot yx \cdot yx \cdots = e_G \end{cases}$

$(yx)^n \overset{def}{=} y \cdot x \cdot y \cdot x \cdots\cdots y \cdot \cancel{x} = e_G$

$\iff$ Asociativa

$y \cdot (x \cdot y) \cdots (x \cdot y)\, x = e_G$

$\iff$ Def pot

$y \cdot (x \cdot y)^{n-1} \cdot x = e_G$

$\iff$ Inversos

$(x \cdot y)^{n-1} = y^{-1} \cdot x^{-1}$

$\iff$ Prop 3 Ej 1

$(x \cdot y)^{n-1} = (x \cdot y)^{-1}$

$\iff$ inverso

$(x \cdot y)^n = e_G = (yx)^n$

Lo mismo para $(xy)^m$

$$\left.\begin{cases} (xy)^n = (yx)^n = e_G \\ (xy)^m = (yx)^m = e_G \end{cases}\right\} \overset{def\ O}{\Rightarrow} \boxed{n = m}$$

4 Probar que si $a \in U(n) \Rightarrow o(a) \mid |U(n)|$

Demostración:

$$U(n) = \{ \overline{m} : \underset{MCD(m,n)=1}{0 \leq m \leq n} \}$$ clases de congruencia mod n

$$|U(n)| = \# U(n) = \varphi(n)$$ cantidad de elementos

por el corolario del teo de lagrange

$$\left.\begin{array}{l} o(a) \\ a \in U(n) \end{array}\right\} \Rightarrow o(a) \mid |U(n)| \Rightarrow o(a) \mid \varphi(n)$$

5 **a)** Hallar el resto de dividir 2^{20} entre 253

$$2^8 = 256 \equiv 3 \pmod{253}$$

$$2^{16} \equiv 9 \pmod{253}$$

$$2^4 \cdot 2^{16} \equiv 2^4 \cdot 9 \pmod{253}$$ $\Rightarrow$ el resto de dividir 2^{20} entre 253 es 144.

b) Sabiendo además que $2^{55} \equiv -45 \pmod{253}$, hallar el $o(2)$ en $U(253)$

$$\boxed{o(2) \mid \varphi(253)}$$

$$\varphi(253) = \varphi(11 \cdot 23) = \varphi(11) \cdot \varphi(23) = 220$$

$$o(2) \mid 220 = 2^2 \cdot 5 \cdot 11$$

o(2)	
1	×
2	×
4	×
5	×
10	×
11	×
20	× → parte (a)
22	×
44	×
55	× → dato
110	✓
220	✓

* $2^8 \equiv 3 \pmod{253}$ $\Rightarrow$ $2 \leq 2^r \leq 128$, $1 \leq r \leq 7$ $\quad 2^r \not\equiv 1 \pmod{253}$

* $a^n \neq e_G \Rightarrow o(a) \nmid n$

$2^{55} \not\equiv 1 \ (253) \Rightarrow o(2) \nmid 55$ → descarto el 11

$2^{20} \not\equiv 1 \ (253) \Rightarrow o(2) \nmid 20$ → descarto el 10

* $2^{22} \equiv 4 \cdot 144 \equiv 35 \cdot 2 \equiv 70 \ (253)$ → descarto el 22

* $2^{44} \not\equiv 1 \ (253)$ $\qquad 2^{110} \equiv 45^2 \equiv 1 \pmod{253}$

* $2^{220} \equiv 1 \pmod{253}$ F-E

$$\boxed{o(2) = 110}$$

Ejercicio 9

Considere un grupo cíclico finito G de orden n y generador g.

① Probar que $g^k = g^m \iff k \equiv m \pmod{n}$

Demostración:

Vamos a ver que $O(g) = n$

$$\left.\begin{array}{l} |G| = n \text{ por letra} \\ g \text{ es generador de } G \end{array}\right\} \Longrightarrow O(g) = |G| = n$$

$$g^k = g^m \iff g^{k-m} = e_G \overset{\boxed{Ej\,8}}{\iff} O(g) \mid k-m \iff k \equiv m \pmod{n}$$

② Probar que si $mcd(m, n) = d$ y $n = d n' \Longrightarrow O(g^m) = n'$

$$O(g^m) = n' \iff (g^m)^{n'} = e_G \iff g^{m.n'} = e_G \overset{prop}{\iff} \underbrace{O(g)}_{|G|} \mid m.n'$$

$$\left.\begin{array}{l} n = n'.d \\ m = m'.d \\ MCD(m', n') = 1 \end{array}\right\} \Rightarrow n'.d \mid m'.d.n' \iff n' \mid m'.n' \quad ok$$

③

④

Ejercicio 10

Sea $a > 0$ y T el conjunto de las siguientes biyecciones de $\mathbb{R} \setminus \{0,1\}$ en sí mismo.

$$T = \left\{ \varphi_1(z) = z \ , \ \varphi_2(z) = \frac{1}{1-z} \ , \ \varphi_3(z) = \frac{z-1}{z} \ , \ \varphi_4(z) = \frac{a}{z} \ , \ \varphi_5(z) = 1 - z \ , \ \varphi_6(z) = \frac{z}{z-1} \right\}$$

① Si sabemos que $(T, \circ)$ es un grupo, hallar a.

Como $(T, \circ)$ es un grupo $\Rightarrow$ cumple propiedad de cierre.

$$\varphi_2 \circ \varphi_4 = \frac{1}{1 - \frac{a}{z}} = \frac{z}{z-a} \Longrightarrow a \text{ tiene que ser } 1.$$

$$\varphi_6(z) = \frac{z}{z-1}$$

② Escribir la tabla de composición de estas funciones

$\circ$	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_1	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_2	φ_2	φ_3	φ_1	φ_6	φ_4	φ_5
φ_3	φ_3	φ_1	φ_2	φ_5	φ_6	φ_4
φ_4	φ_4	φ_5	φ_6	φ_1	φ_2	φ_3
φ_5	φ_5	φ_6	φ_4	φ_3	φ_1	φ_2
φ_6	φ_6	φ_4	φ_5	φ_2	φ_3	φ_1

$$\varphi_2 \circ \varphi_3 = \frac{\left(\frac{1}{1-z}\right) - 1}{\left(\frac{1}{1-z}\right)} = 1 - 1 + z = z$$

③ Hallar el orden de cada elemento de T

$\mathcal{O}(\varphi_1) = 1$ $\quad$ $\mathcal{O}(\varphi_3) = 3$ $\quad$ $\mathcal{O}(\varphi_5) = 2$

$\mathcal{O}(\varphi_2) = 3$ $\quad$ $\mathcal{O}(\varphi_4) = 2$ $\quad$ $\mathcal{O}(\varphi_6) = 2$

Mirando tabla !!

(4) ¿ Es $(\{\varphi_1 , \varphi_4\} , \circ)$ un subgrupo de Γ ?

Condición 1 : $\{\varphi_1 , \varphi_4\} \subset \Gamma$ y $\neq \phi$

Condición 2 : $e_\Gamma \in \{\varphi_1 , \varphi_4\}$ $\quad e_\Gamma = \varphi_1$ ok

Condición 3 : $\forall\, a , b \in \{\varphi_1 , \varphi_4\}$ $\quad a \circ b \in \{\varphi_1 , \varphi_4\}$

Se cumple ✓

Condición 4 : $\forall\, a \in \{\varphi_1 , \varphi_4\}$, $a^{-1} \in \{\varphi_1 , \varphi_4\}$

$\varphi_1 \circ a = a \circ \varphi_1 = \varphi_1 \qquad a = \varphi_1$

$\varphi_4 \circ b = b \circ \varphi_4 = \varphi_1 \qquad b = \varphi_4$ — se ve la tabla.

Entonces $(\{\varphi_1 , \varphi_4\} , \circ)$ es subgrupo de Γ

Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Matemática Discreta 2
Curso 2012

Menu

PRÁCTICO 6: TEORÍA DE GRUPOS - CONCEPTOS BÁSICOS.

Ejercicio 1. Sea G un grupo. Probar las siguientes afirmaciones:

1. El neutro de G es único.
2. El inverso de $g \in G$ es único.
3. $(ab)^{-1} = b^{-1}a^{-1}$ para todo $a, b \in G$.
4. Si $xg = xh \Rightarrow g = h$.
5. Si $gx = hx \Rightarrow g = h$.
6. $(ab)^{-1} = a^{-1}b^{-1}$ para todo $a, b \in G \Leftrightarrow G$ es abeliano.
7. $(ab)^2 = a^2b^2$ para todo $a, b \in G \Leftrightarrow G$ es abeliano.
8. Si $(ab)^3 = e_G$ para todo $a, b \in G$ entonces $(ba)^3 = e_G$.
9. $(a^n)^{-1} = (a^{-1})^n$ para todo $a \in G$, $n \in \mathbb{N}$.

Ejercicio 2. Investigar si los siguientes conjuntos con las respectivas operaciones que se definen son grupos:

1. El conjunto $M_{n\times n}(\mathbb{R})$ y la operación es el producto usual de matrices: $A * B = AB$.
2. El conjunto $M_{n\times n}(\mathbb{R})$ con la operación: $A * B = AB + BA$.
3. El conjunto es $\mathbb{R}^2$ y la operación es: $(x_1, x_2) * (y_1, y_2) = (x_1y_1, x_2y_1 + y_2)$.
4. $G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$ y $*$ el producto matricial.
5. El conjunto es $\{a, b, c\}$ y la operación $*$ se define mediante la tabla:

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

6. El conjunto es $\{a, b, c, d\}$ y la operación $*$ se define mediante la tabla:

$*$	a	b	c	d
a	a	b	c	d
b	b	c	a	a
c	c	a	b	b
d	d	a	b	c

7. El conjunto $\mathbb{Z}$ con la operación $\otimes$ definida por : $a \otimes b = ab - 2(a + b) + 6$.

Ejercicio 3. Sea $G = \{e, a, b, c, d, f\}$ tal que $(G, \cdot)$ es un grupo. Completar la tabla de Cayley si se tiene la información parcial siguiente:

·	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a		e			
b	b			f		d
c	c				b	a
d	d					b
f	f			b		

Ejercicio 4. Para cada uno de los grupos G, investigar si H es un subgrupo de G:

1. $G = (\mathbb{Z}, +)$ y $H = n\mathbb{Z}$ el conjunto de los enteros múltiplos de n (para $n \in \mathbb{Z}$ dado).
2. $G = \mathbb{R}\backslash\{0\}$ con el producto y $H = \mathbb{R}^+$ el conjunto de los reales positivos.
3. $G = GL_2(\mathbb{R})$ (matrices invertibles 2×2 con coeficientes reales) con el producto usual de matrices y $H = \left\{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in M_{2\times 2}(\mathbb{R}) : ac \neq 0\right\}$.
4. $G = GL_2(\mathbb{R})$ y $H = \{M \in G : \det(M) = 1\}$.
5. $G = \mathbb{Q}^+$ con el producto y $H = \{\frac{a}{b} \in \mathbb{Q} : a \equiv 0 \pmod 7, \operatorname{mcd}(b, 7) = 1\}$.
6. $G = D_3$ el grupo diedral y $H = \{\mathrm{id}, r, r^2 s, r\}$ (r es una rotación y s una simetría axial).
7. $G = S_3$ el grupo de permutaciones y $H = \{\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)\}$.
8. $G = S_3$ y $H = \{\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)\}$.
9. $G = S_4$ y $H = \{\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{smallmatrix}\right)\}$.

Ejercicio 5. Sean H_1 y H_2 dos subgrupos de un grupo G.

1. Probar que $H_1 \cap H_2$ es un subgrupo de G.
2. ¿Es $H_1 \cup H_2$ necesariamente un subgrupo de G?

Ejercicio 6. Probar que si G es un grupo **abeliano** entonces H es un subgrupo de G para los siguientes casos:

1. $H = \{a \in G : a^2 = e_G\}$.
2. $H = \{a^n : a \in G\}$ donde n es un entero positivo dado.

Ejercicio 7. Escriba la tabla de multiplicación de $U(18)$. Hallar los órdenes de los elementos de $U(18)$. ¿Es $U(18)$ cíclico?

Ejercicio 8.

1. Sea G un grupo. Probar que si $a^n = e_G \Rightarrow o(a)|n$.
2. Sea G un grupo. Probar que si $a^n \neq e_G \Rightarrow o(a) \nmid n$
3. Sea G un grupo. Probar que $o(xy) = o(yx)$, $\forall\, x, y \in G$.
4. Probar que si $a \in U(n) \Rightarrow o(a)|\varphi(n)$.
5. a) Hallar el resto de dividir 2^{20} entre 253.
   b) Sabiendo además que $2^{55} \equiv -45 \pmod{253}$, hallar el orden de 2 en $U(253)$.

Ejercicio 9. Considere un grupo cíclico finito G de orden n y generador g.

1. Probar que $g^k = g^m$ si y solo si $k \equiv m \pmod{n}$
2. Probar que si $mcd(m,n) = d$ y $n = dn'$, entonces el orden de g^m es n'.
3. Probar que g^k es también un generador de G si y solo si $mcd(k,n) = 1$.
4. Usar la parte anterior para probar que G tiene $\varphi(n)$ generadores, donde φ es la indicatriz de Euler.

Ejercicio 10. Sea $a > 0$ y Γ el conjunto de las siguientes biyecciones de $\mathbb{R} \setminus \{0,1\}$ en sí mismo:

$$\varphi_1(z) = z, \quad \varphi_2(z) = \frac{1}{1-z}, \quad \varphi_3(z) = \frac{z-1}{z},$$
$$\varphi_4(z) = \frac{a}{z}, \quad \varphi_5(z) = 1-z, \quad \varphi_6(z) = \frac{z}{z-1}.$$

1. Si sabemos que $(\Gamma, \circ)$ es un grupo, hallar a.
2. Escribir la tabla de composición de estas funciones.
3. Hallar el orden de cada elemento de Γ.
4. ¿Es $(\{\varphi_1, \varphi_4\}, \circ)$ un subgrupo de Γ?