Herstein Algebra Moderna Resuelto

Humberto Alonso Villegas 21 de enero de 2014

1. Teoría de Conjuntos

Ejemplo 1.- Sea s
 un conjunto cualquiera y definamos en S por a b
 para $a,b\in S$ si y solo si a = b. Hemos definido claramente, así, una relación de equivalencia sobre S. En

2. Teoría de Grupos

2.1. Definición de Grupo

Definición 2.1. Un conjunto no vacio de elementos G se dice que forma un grupo si en G esta definida una operación binaria, llamada producto y denotada por (\cdot) tal que:

- 1. $\forall a,b \in G \in G \ a \cdot b \in G$
- $\textit{2.} \ \forall \ a,b,c \in G, \ a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- 3. $\exists e \in G : \forall a \in G, e \cdot a = a \cdot e = a$
- 4. $\forall \ a \in G \ \exists \ a^{-1} \in G : a \cdot a^{-1} = e$

Definición 2.2. Un Grupo se dice que es abeliano (o conmutativo) si \forall $a,b \in G$ $a \cdot b = b \cdot a$

2.2. Algunos ejemplos de Grupo

Ejemplo 1.- Supongamos que $G = \mathbb{Z}$, con $a \cdot b$, para $a, b \in G$, definida como la suma usual entre enteros, es decir, con $a\Delta b = a + b$. Demostrar que G es un grupo abeliano infinito en el que 0 juega el papel de e y -a el de a^{-1} G es un grupo \iff cumple lo siguiente.

- 1. \forall a,b \in $G \in G$ a·b \in G
- 2. $\forall a,b,c \in G, a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- 3. $\exists e \in G : \forall a \in G, e \cdot a = a \cdot e = a$
- 4. $\forall a \in G \; \exists \; a^{-1} \in G : a \cdot a^{-1} = e$

 $Demostraci\'{o}n.$:

- 1.- Sean $a,b \in G$, $a \cdot b \in G \iff a+b \in \mathbb{Z} \iff a,b \in \mathbb{Z}$
- **2.-** Sean $a,b,c \in G$, $\Rightarrow a,b,c \in G$, $\Rightarrow a \cdot (b \cdot c) = a + (b + c) = (a + b) + c = (a \cdot b) \cdot c$ $\Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- **3.-** Sea a \in G, \exists e \in G : e·a = a·e = a \forall a \in G \iff \exists w \in \mathbb{Z} : w·a = a·w = a \forall a \in \mathbb{Z} (1 cumple)
- **4.-** Sea a $\in \mathbb{Z}$, $\exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e \iff \exists a^{-1} \in \mathbb{Z} : a + a^{-1} = a^{-1} + a = 1$ (cumple -a)

De esto se tiene que G es un grupo, ahora veamos que G es grupo abeliano

Sea
$$a,b \in G \Rightarrow a,b \in \mathbb{Z}, a \cdot b = b \cdot a \iff a+b=b+a$$

2.- Supongamos que G consiste en los números reales 1 y -1 con la multiplicación entre números reales como operación. G es entonces un grupo abeliano de orden 2.

Demostraci'on.:

Es claro que el orden de G es 2

1, 3, 4:

 $1\cdot 1=1\in G,\ 1\cdot (-1)=(-1)\cdot 1=-1\in G,\ (-1)\cdot (-1)=1$... tenemos que \forall a,b \in G, a b \in G, \forall a \in G \exists $a^{-1}\in G$: a \in e, \exists e in G: \forall a \in G a e = a. Además lo anterior muestra que G es conmutativo

2.- Sean a,b,c en G, \Rightarrow a,b,c $\in \mathbb{R}$ \therefore a·(b·c) = (a·b)·c

.

3.- Sea $G = S_3$, el grupo de todas las aplicaciones biyectivas del conjunto $A = x_1, x_2, x_3$ sobre si mismo, con el producto, la composición. G es un grupo de orden 6.

Demostraci'on.:

 $\varphi_e := G \to G$ donde:

 $\varphi_e(x_1) = x_1$

 $\varphi_e(x_2) = x_2$

 $\varphi_e(x_3) = x_3$

 $\varphi_1 := G \to G$ donde:

 $\varphi_1(x_1) = x_1$

 $\varphi_1(x_2) = x_3$

 $\varphi_1(x_3) = x_2$

 $\varphi_2 := G \to G$ donde:

 $\varphi_2(x_1) = x_3$

 $\varphi_2(x_2) = x_2$

 $\varphi_2(x_3) = x_1$

 $\varphi_3 := G \to G$ donde:

 $\varphi_3(x_1) = x_2$

 $\varphi_3(x_2) = x_1$

 $\varphi_3(x_3) = x_3$

 $\varphi_4 := G \to G$ donde:

 $\varphi_4(x_1)=x_2$

 $\varphi_4(x_2) = x_3$

 $\varphi_4(x_3) = x_1$

 $\varphi_5 := G \to G$ donde:

 $\varphi_5(x_1) = x_3$

$$\varphi_5(x_2) = x_1$$
$$\varphi_5(x_3) = x_2$$

- **1.-**: Sean φ_a y $\varphi_b \in G$ y $\varphi_C = \varphi_a \circ \varphi_b$, sabemos que φ_a y φ_b son aplicaciones biyectivas de A en A, $\therefore \varphi_C$ también es una aplicación biyectiva de A en A $\therefore \varphi_C \in G$
- **2.-** Veamos que $\varphi_a \circ (\varphi_b \circ \varphi_c) = (\varphi_a \circ \varphi_b) \circ \varphi_c \ \forall \ \varphi_a, \varphi_b, \varphi_c \in G$ Omitiremos cuando alguna φ es φ_e , pues es claro que se cumple.

$$arphi_1 \circ (arphi_1 \circ arphi_1) = arphi_1 \circ arphi_e = arphi_1 \ (arphi_1 \circ arphi_1) \circ arphi_1 = arphi_e \circ arphi_1 = arphi_1$$

$$\varphi_2 \circ (\varphi_2 \circ \varphi_2) = \varphi_2 \circ \varphi_e = \varphi_2$$
 $(\varphi_2 \circ \varphi_2) \circ \varphi_2 = \varphi_e \circ \varphi_2 = \varphi_2$

$$\varphi_3 \circ (\varphi_3 \circ \varphi_3) = \varphi_3 \circ \varphi_e = \varphi_3 (\varphi_3 \circ \varphi_3) \circ \varphi_3 = \varphi_e \circ \varphi_3 = \varphi_3$$

$$\varphi_4 \circ (\varphi_4 \circ \varphi_4) = \varphi_4 \circ \varphi_5 = \varphi_e$$
$$(\varphi_4 \circ \varphi_4) \circ \varphi_4 = \varphi_5 \circ \varphi_4 = \varphi_e$$

$$\varphi_5 \circ (\varphi_5 \circ \varphi_5) = \varphi_5 \circ \varphi_4 = \varphi_e
(\varphi_5 \circ \varphi_5) \circ \varphi_5 = \varphi_4 \circ \varphi_5 = \varphi_e$$

$$\varphi_1 \circ (\varphi_2 \circ \varphi_2) = \varphi_1 \circ \varphi_e = \varphi_1 (\varphi_1 \circ \varphi_2) \circ \varphi_2 = \varphi_4 \circ \varphi_2 = \varphi_1$$

$$\varphi_1 \circ (\varphi_3 \circ \varphi_3) = \varphi_1 \circ \varphi_e = \varphi_1 (\varphi_1 \circ \varphi_3) \circ \varphi_3 = \varphi_5 \circ \varphi_3 = \varphi_1$$

$$\varphi_1 \circ (\varphi_4 \circ \varphi_4) = \varphi_1 \circ \varphi_5 = \varphi_3 (\varphi_1 \circ \varphi_4) \circ \varphi_4 = \varphi_2 \circ \varphi_4 = \varphi_3$$

$$arphi_1 \circ (arphi_5 \circ arphi_5) = arphi_1 \circ arphi_4 = arphi_2 \ (arphi_1 \circ arphi_5) \circ arphi_5 = arphi_3 \circ arphi_5 = arphi_2$$

$$arphi_2 \circ (arphi_1 \circ arphi_1) = arphi_2 \circ arphi_e = arphi_2 \ (arphi_2 \circ arphi_1) \circ arphi_1 = arphi_5 \circ arphi_1 = arphi_2$$

$$\varphi_2 \circ (\varphi_3 \circ \varphi_3) = \varphi_2 \circ \varphi_e = \varphi_2
(\varphi_2 \circ \varphi_3) \circ \varphi_3 = \varphi_4 \circ \varphi_3 = \varphi_2$$

$$\varphi_2 \circ (\varphi_4 \circ \varphi_4) = \varphi_2 \circ \varphi_5 = \varphi_1 (\varphi_2 \circ \varphi_4) \circ \varphi_4 = \varphi_3 \circ \varphi_4 = \varphi_1$$

$$arphi_2 \circ (arphi_5 \circ arphi_5) = arphi_2 \circ arphi_4 = arphi_3 \ (arphi_2 \circ arphi_5) \circ arphi_5 = arphi_1 \circ arphi_5 = arphi_3$$

$$\varphi_3 \circ (\varphi_1 \circ \varphi_1) = \varphi_3 \circ \varphi_e = \varphi_3
(\varphi_3 \circ \varphi_1) \circ \varphi_1 = \varphi_4 \circ \varphi_1 = \varphi_3$$

$$\varphi_3 \circ (\varphi_2 \circ \varphi_2) = \varphi_3 \circ \varphi_e = \varphi_3
(\varphi_3 \circ \varphi_2) \circ \varphi_2 = \varphi_5 \circ \varphi_2 = \varphi_3$$

$$\varphi_3 \circ (\varphi_4 \circ \varphi_4) = \varphi_3 \circ \varphi_5 = \varphi_2 (\varphi_3 \circ \varphi_4) \circ \varphi_4 = \varphi_1 \circ \varphi_4 = \varphi_2$$

$$\varphi_3 \circ (\varphi_5 \circ \varphi_5) = \varphi_3 \circ \varphi_4 = \varphi_1 (\varphi_3 \circ \varphi_5) \circ \varphi_5 = \varphi_2 \circ \varphi_5 = \varphi_1$$

$$\varphi_4 \circ (\varphi_1 \circ \varphi_1) = \varphi_4 \circ \varphi_e = \varphi_4 (\varphi_4 \circ \varphi_1) \circ \varphi_1 = \varphi_3 \circ \varphi_1 = \varphi_4$$

$$arphi_4 \circ (arphi_3 \circ arphi_3) = arphi_4 \circ arphi_e = arphi_4 \ (arphi_4 \circ arphi_3) \circ arphi_3 = arphi_2 \circ arphi_3 = arphi_4$$

$$\varphi_4 \circ (\varphi_2 \circ \varphi_2) = \varphi_4 \circ \varphi_e = \varphi_4 (\varphi_4 \circ \varphi_2) \circ \varphi_2 = \varphi_1 \circ \varphi_2 = \varphi_4$$

$$\varphi_4 \circ (\varphi_5 \circ \varphi_5) = \varphi_4 \circ \varphi_4 = \varphi_5
(\varphi_4 \circ \varphi_5) \circ \varphi_5 = \varphi_e \circ \varphi_5 = \varphi_5$$

$$arphi_5 \circ (arphi_1 \circ arphi_1) = arphi_4 \circ arphi_e = arphi_5 \ (arphi_5 \circ arphi_1) \circ arphi_1 = arphi_2 \circ arphi_1 = arphi_5$$

$$\varphi_5 \circ (\varphi_3 \circ \varphi_3) = \varphi_5 \circ \varphi_e = \varphi_5
(\varphi_5 \circ \varphi_3) \circ \varphi_3 = \varphi_1 \circ \varphi_3 = \varphi_5$$

$$arphi_5 \circ (arphi_2 \circ arphi_2) = arphi_5 \circ arphi_e = arphi_5 \ (arphi_5 \circ arphi_2) \circ arphi_2 = arphi_3 \circ arphi_2 = arphi_5$$

$$arphi_5 \circ (arphi_4 \circ arphi_4) = arphi_5 \circ arphi_5 = arphi_4 \ (arphi_5 \circ arphi_4) \circ arphi_4 = arphi_e \circ arphi_4 = arphi_4$$

$$arphi_1 \circ (arphi_1 \circ arphi_2) = arphi_1 \circ arphi_4 = arphi_2 \ (arphi_1 \circ arphi_1) \circ arphi_2 = arphi_e \circ arphi_2 = arphi_2$$

$$arphi_1 \circ (arphi_1 \circ arphi_3) = arphi_1 \circ arphi_5 = arphi_3 \ (arphi_1 \circ arphi_1) \circ arphi_3 = arphi_e \circ arphi_3 = arphi_3$$

$$arphi_1 \circ (arphi_1 \circ arphi_4) = arphi_1 \circ arphi_2 = arphi_4 \ (arphi_1 \circ arphi_1) \circ arphi_4 = arphi_e \circ arphi_4 = arphi_4$$

$$arphi_1 \circ (arphi_1 \circ arphi_5) = arphi_1 \circ arphi_3 = arphi_5 \ (arphi_1 \circ arphi_1) \circ arphi_5 = arphi_e \circ arphi_5 = arphi_5$$

$$\varphi_1 \circ (\varphi_2 \circ \varphi_1) = \varphi_1 \circ \varphi_5 = \varphi_3
(\varphi_1 \circ \varphi_2) \circ \varphi_1 = \varphi_4 \circ \varphi_1 = \varphi_3$$

$$\varphi_1 \circ (\varphi_3 \circ \varphi_1) = \varphi_1 \circ \varphi_4 = \varphi_2$$

$$(\varphi_1\circ\varphi_3)\circ\varphi_1=\varphi_5\circ\varphi_1=\varphi_2$$

$$arphi_1 \circ (arphi_4 \circ arphi_1) = arphi_1 \circ arphi_3 = arphi_5 \ (arphi_1 \circ arphi_4) \circ arphi_1 = arphi_2 \circ arphi_1 = arphi_5$$

$$\varphi_1 \circ (\varphi_5 \circ \varphi_1) = \varphi_1 \circ \varphi_2 = \varphi_4 (\varphi_1 \circ \varphi_5) \circ \varphi_1 = \varphi_3 \circ \varphi_1 = \varphi_4$$

$$arphi_2 \circ (arphi_2 \circ arphi_1) = arphi_2 \circ arphi_5 = arphi_1 \ (arphi_2 \circ arphi_2) \circ arphi_1 = arphi_e \circ arphi_1 = arphi_1$$

$$\varphi_2 \circ (\varphi_2 \circ \varphi_3) = \varphi_2 \circ \varphi_4 = \varphi_3
(\varphi_2 \circ \varphi_2) \circ \varphi_3 = \varphi_e \circ \varphi_3 = \varphi_3$$

$$\varphi_2 \circ (\varphi_2 \circ \varphi_4) = \varphi_2 \circ \varphi_3 = \varphi_4 (\varphi_2 \circ \varphi_2) \circ \varphi_4 = \varphi_e \circ \varphi_4 = \varphi_4$$

$$arphi_2 \circ (arphi_2 \circ arphi_5) = arphi_2 \circ arphi_1 = arphi_5 \ (arphi_2 \circ arphi_2) \circ arphi_5 = arphi_e \circ arphi_5 = arphi_5$$

$$\varphi_2 \circ (\varphi_1 \circ \varphi_2) = \varphi_2 \circ \varphi_4 = \varphi_3 (\varphi_2 \circ \varphi_1) \circ \varphi_2 = \varphi_5 \circ \varphi_2 = \varphi_3$$

$$\varphi_2 \circ (\varphi_3 \circ \varphi_2) = \varphi_2 \circ \varphi_5 = \varphi_1 (\varphi_2 \circ \varphi_3) \circ \varphi_2 = \varphi_4 \circ \varphi_2 = \varphi_1$$

$$arphi_2 \circ (arphi_4 \circ arphi_2) = arphi_2 \circ arphi_1 = arphi_5 \ (arphi_2 \circ arphi_4) \circ arphi_2 = arphi_3 \circ arphi_2 = arphi_5$$

$$arphi_2 \circ (arphi_5 \circ arphi_2) = arphi_2 \circ arphi_3 = arphi_4 \ (arphi_2 \circ arphi_5) \circ arphi_2 = arphi_1 \circ arphi_2 = arphi_4$$

$$\varphi_3 \circ (\varphi_3 \circ \varphi_1) = \varphi_3 \circ \varphi_4 = \varphi_1
(\varphi_3 \circ \varphi_3) \circ \varphi_1 = \varphi_e \circ \varphi_1 = \varphi_1$$

$$\varphi_3 \circ (\varphi_3 \circ \varphi_2) = \varphi_3 \circ \varphi_5 = \varphi_2
(\varphi_3 \circ \varphi_3) \circ \varphi_2 = \varphi_e \circ \varphi_2 = \varphi_2$$

$$arphi_3 \circ (arphi_3 \circ arphi_4) = arphi_3 \circ arphi_1 = arphi_4 \ (arphi_3 \circ arphi_3) \circ arphi_4 = arphi_e \circ arphi_4 = arphi_4$$

$$arphi_3 \circ (arphi_3 \circ arphi_5) = arphi_3 \circ arphi_2 = arphi_5 \ (arphi_3 \circ arphi_3) \circ arphi_5 = arphi_e \circ arphi_5 = arphi_5$$

$$arphi_3 \circ (arphi_1 \circ arphi_3) = arphi_3 \circ arphi_5 = arphi_2 \ (arphi_3 \circ arphi_1) \circ arphi_3 = arphi_4 \circ arphi_3 = arphi_2$$

$$\varphi_3 \circ (\varphi_2 \circ \varphi_3) = \varphi_3 \circ \varphi_4 = \varphi_1
(\varphi_3 \circ \varphi_2) \circ \varphi_3 = \varphi_5 \circ \varphi_3 = \varphi_1$$

$$\varphi_3 \circ (\varphi_4 \circ \varphi_3) = \varphi_3 \circ \varphi_2 = \varphi_5 (\varphi_3 \circ \varphi_4) \circ \varphi_3 = \varphi_1 \circ \varphi_3 = \varphi_5$$

$$\varphi_3 \circ (\varphi_5 \circ \varphi_3) = \varphi_3 \circ \varphi_1 = \varphi_4 (\varphi_3 \circ \varphi_5) \circ \varphi_3 = \varphi_2 \circ \varphi_3 = \varphi_4$$

$$\varphi_4 \circ (\varphi_4 \circ \varphi_1) = \varphi_4 \circ \varphi_3 = \varphi_2
(\varphi_4 \circ \varphi_4) \circ \varphi_1 = \varphi_5 \circ \varphi_1 = \varphi_2$$

$$\varphi_4 \circ (\varphi_4 \circ \varphi_2) = \varphi_4 \circ \varphi_1 = \varphi_3 (\varphi_4 \circ \varphi_4) \circ \varphi_2 = \varphi_5 \circ \varphi_2 = \varphi_3$$

$$\varphi_4 \circ (\varphi_4 \circ \varphi_3) = \varphi_4 \circ \varphi_2 = \varphi_1 (\varphi_4 \circ \varphi_4) \circ \varphi_3 = \varphi_5 \circ \varphi_3 = \varphi_1$$

$$\varphi_4 \circ (\varphi_4 \circ \varphi_5) = \varphi_4 \circ \varphi_e = \varphi_4
(\varphi_4 \circ \varphi_4) \circ \varphi_5 = \varphi_5 \circ \varphi_5 = \varphi_4$$

$$\varphi_4 \circ (\varphi_1 \circ \varphi_4) = \varphi_4 \circ \varphi_2 = \varphi_1 (\varphi_4 \circ \varphi_1) \circ \varphi_4 = \varphi_3 \circ \varphi_4 = \varphi_1$$

$$\varphi_4 \circ (\varphi_2 \circ \varphi_4) = \varphi_4 \circ \varphi_3 = \varphi_2$$

$$(\varphi_4 \circ \varphi_2) \circ \varphi_4 = \varphi_1 \circ \varphi_4 = \varphi_2$$

$$\varphi_4 \circ (\varphi_3 \circ \varphi_4) = \varphi_4 \circ \varphi_1 = \varphi_3 (\varphi_4 \circ \varphi_3) \circ \varphi_4 = \varphi_2 \circ \varphi_4 = \varphi_3$$

$$\varphi_4 \circ (\varphi_5 \circ \varphi_4) = \varphi_4 \circ \varphi_e = \varphi_4 (\varphi_4 \circ \varphi_5) \circ \varphi_4 = \varphi_e \circ \varphi_4 = \varphi_4$$

$$\varphi_5 \circ (\varphi_5 \circ \varphi_1) = \varphi_5 \circ \varphi_2 = \varphi_3
(\varphi_5 \circ \varphi_5) \circ \varphi_1 = \varphi_4 \circ \varphi_1 = \varphi_3$$

$$arphi_5 \circ (arphi_5 \circ arphi_2) = arphi_5 \circ arphi_3 = arphi_1 \ (arphi_5 \circ arphi_5) \circ arphi_2 = arphi_4 \circ arphi_2 = arphi_1$$

$$arphi_5 \circ (arphi_5 \circ arphi_3) = arphi_5 \circ arphi_1 = arphi_2 \ (arphi_5 \circ arphi_5) \circ arphi_3 = arphi_4 \circ arphi_3 = arphi_2$$

$$\varphi_5 \circ (\varphi_5 \circ \varphi_4) = \varphi_5 \circ \varphi_e = \varphi_5
(\varphi_5 \circ \varphi_5) \circ \varphi_4 = \varphi_4 \circ \varphi_4 = \varphi_5$$

$$\varphi_5 \circ (\varphi_1 \circ \varphi_5) = \varphi_5 \circ \varphi_3 = \varphi_1 (\varphi_5 \circ \varphi_1) \circ \varphi_5 = \varphi_2 \circ \varphi_5 = \varphi_1$$

$$\varphi_5 \circ (\varphi_2 \circ \varphi_5) = \varphi_5 \circ \varphi_1 = \varphi_2
(\varphi_5 \circ \varphi_2) \circ \varphi_5 = \varphi_3 \circ \varphi_5 = \varphi_2$$

$$\varphi_5 \circ (\varphi_3 \circ \varphi_5) = \varphi_5 \circ \varphi_2 = \varphi_3 (\varphi_5 \circ \varphi_3) \circ \varphi_5 = \varphi_1 \circ \varphi_5 = \varphi_3$$

$$arphi_5 \circ (arphi_4 \circ arphi_5) = arphi_5 \circ arphi_e = arphi_5 \ (arphi_5 \circ arphi_4) \circ arphi_5 = arphi_e \circ arphi_5 = arphi_5$$

$$\varphi_1 \circ (\varphi_2 \circ \varphi_3) = \varphi_1 \circ \varphi_4 = \varphi_2 (\varphi_1 \circ \varphi_2) \circ \varphi_3 = \varphi_4 \circ \varphi_3 = \varphi_2$$

$$\varphi_1 \circ (\varphi_2 \circ \varphi_4) = \varphi_1 \circ \varphi_3 = \varphi_5 (\varphi_1 \circ \varphi_2) \circ \varphi_4 = \varphi_4 \circ \varphi_4 = \varphi_5$$

$$arphi_1 \circ (arphi_2 \circ arphi_5) = arphi_1 \circ arphi_1 = arphi_e \ (arphi_1 \circ arphi_2) \circ arphi_5 = arphi_4 \circ arphi_5 = arphi_e$$

$$arphi_1 \circ (arphi_3 \circ arphi_2) = arphi_1 \circ arphi_5 = arphi_3 \ (arphi_1 \circ arphi_3) \circ arphi_2 = arphi_5 \circ arphi_2 = arphi_3$$

$$\varphi_1 \circ (\varphi_3 \circ \varphi_4) = \varphi_1 \circ \varphi_1 = \varphi_e$$
$$(\varphi_1 \circ \varphi_3) \circ \varphi_4 = \varphi_5 \circ \varphi_4 = \varphi_e$$

$$arphi_1 \circ (arphi_3 \circ arphi_5) = arphi_1 \circ arphi_2 = arphi_4 \ (arphi_1 \circ arphi_3) \circ arphi_5 = arphi_5 \circ arphi_5 = arphi_4$$

$$\begin{array}{l} \varphi_1 \circ (\varphi_4 \circ \varphi_2) = \varphi_1 \circ \varphi_1 = \varphi_e \\ (\varphi_1 \circ \varphi_4) \circ \varphi_2 = \varphi_2 \circ \varphi_2 = \varphi_e \end{array}$$

$$\varphi_1 \circ (\varphi_4 \circ \varphi_3) = \varphi_1 \circ \varphi_2 = \varphi_4 (\varphi_1 \circ \varphi_4) \circ \varphi_3 = \varphi_2 \circ \varphi_3 = \varphi_4$$

$$\varphi_1 \circ (\varphi_4 \circ \varphi_5) = \varphi_1 \circ \varphi_e = \varphi_1
(\varphi_1 \circ \varphi_4) \circ \varphi_5 = \varphi_2 \circ \varphi_5 = \varphi_1$$

$$arphi_2 \circ (arphi_1 \circ arphi_3) = arphi_2 \circ arphi_5 = arphi_1 \ (arphi_2 \circ arphi_1) \circ arphi_3 = arphi_5 \circ arphi_3 = arphi_1$$

$$arphi_2 \circ (arphi_1 \circ arphi_4) = arphi_2 \circ arphi_2 = arphi_e \ (arphi_2 \circ arphi_1) \circ arphi_4 = arphi_5 \circ arphi_4 = arphi_e$$

$$arphi_2 \circ (arphi_1 \circ arphi_5) = arphi_2 \circ arphi_3 = arphi_4 \ (arphi_2 \circ arphi_1) \circ arphi_5 = arphi_5 \circ arphi_5 = arphi_4$$

$$\varphi_2 \circ (\varphi_3 \circ \varphi_1) = \varphi_2 \circ \varphi_4 = \varphi_3
(\varphi_2 \circ \varphi_3) \circ \varphi_1 = \varphi_4 \circ \varphi_1 = \varphi_3$$

$$arphi_2 \circ (arphi_3 \circ arphi_4) = arphi_2 \circ arphi_1 = arphi_5 \ (arphi_2 \circ arphi_3) \circ arphi_4 = arphi_4 \circ arphi_4 = arphi_5$$

$$\varphi_2 \circ (\varphi_3 \circ \varphi_5) = \varphi_2 \circ \varphi_2 = \varphi_e
(\varphi_2 \circ \varphi_3) \circ \varphi_5 = \varphi_4 \circ \varphi_5 = \varphi_e$$

$$arphi_2 \circ (arphi_4 \circ arphi_1) = arphi_2 \circ arphi_3 = arphi_4$$

$$(\varphi_2\circ\varphi_4)\circ\varphi_1=\varphi_3\circ\varphi_1=\varphi_4$$

$$arphi_2 \circ (arphi_4 \circ arphi_3) = arphi_2 \circ arphi_2 = arphi_e \ (arphi_2 \circ arphi_4) \circ arphi_3 = arphi_3 \circ arphi_3 = arphi_e$$

$$\varphi_2 \circ (\varphi_4 \circ \varphi_5) = \varphi_2 \circ \varphi_e = \varphi_2 (\varphi_2 \circ \varphi_4) \circ \varphi_5 = \varphi_3 \circ \varphi_5 = \varphi_2$$

$$\varphi_2 \circ (\varphi_5 \circ \varphi_1) = \varphi_2 \circ \varphi_2 = \varphi_e$$

$$(\varphi_2 \circ \varphi_5) \circ \varphi_1 = \varphi_1 \circ \varphi_1 = \varphi_e$$

$$\varphi_2 \circ (\varphi_5 \circ \varphi_3) = \varphi_2 \circ \varphi_1 = \varphi_5 (\varphi_2 \circ \varphi_5) \circ \varphi_3 = \varphi_1 \circ \varphi_3 = \varphi_5$$

$$\varphi_2 \circ (\varphi_5 \circ \varphi_4) = \varphi_2 \circ \varphi_e = \varphi_2 (\varphi_2 \circ \varphi_5) \circ \varphi_4 = \varphi_1 \circ \varphi_4 = \varphi_2$$

$$\varphi_3 \circ (\varphi_1 \circ \varphi_2) = \varphi_3 \circ \varphi_4 = \varphi_1 (\varphi_3 \circ \varphi_1) \circ \varphi_2 = \varphi_4 \circ \varphi_2 = \varphi_1$$

$$\varphi_3 \circ (\varphi_1 \circ \varphi_4) = \varphi_3 \circ \varphi_2 = \varphi_5
(\varphi_3 \circ \varphi_1) \circ \varphi_4 = \varphi_4 \circ \varphi_4 = \varphi_5$$

$$\varphi_3 \circ (\varphi_1 \circ \varphi_5) = \varphi_3 \circ \varphi_3 = \varphi_e
(\varphi_3 \circ \varphi_1) \circ \varphi_5 = \varphi_4 \circ \varphi_5 = \varphi_e$$

$$\varphi_3 \circ (\varphi_2 \circ \varphi_1) = \varphi_3 \circ \varphi_5 = \varphi_2$$

$$(\varphi_3 \circ \varphi_2) \circ \varphi_1 = \varphi_5 \circ \varphi_1 = \varphi_2$$

$$\varphi_3 \circ (\varphi_2 \circ \varphi_4) = \varphi_3 \circ \varphi_3 = \varphi_e (\varphi_3 \circ \varphi_2) \circ \varphi_4 = \varphi_5 \circ \varphi_4 = \varphi_e$$

$$\varphi_3 \circ (\varphi_2 \circ \varphi_5) = \varphi_3 \circ \varphi_1 = \varphi_4$$

$$(\varphi_3 \circ \varphi_2) \circ \varphi_5 = \varphi_5 \circ \varphi_5 = \varphi_4$$

$$\varphi_3 \circ (\varphi_4 \circ \varphi_1) = \varphi_3 \circ \varphi_3 = \varphi_e (\varphi_3 \circ \varphi_4) \circ \varphi_1 = \varphi_1 \circ \varphi_1 = \varphi_e$$

$$\varphi_3 \circ (\varphi_4 \circ \varphi_2) = \varphi_3 \circ \varphi_1 = \varphi_4 (\varphi_3 \circ \varphi_4) \circ \varphi_2 = \varphi_1 \circ \varphi_2 = \varphi_4$$

$$\varphi_3 \circ (\varphi_4 \circ \varphi_5) = \varphi_3 \circ \varphi_e = \varphi_3
(\varphi_3 \circ \varphi_4) \circ \varphi_5 = \varphi_1 \circ \varphi_5 = \varphi_3$$

$$arphi_3 \circ (arphi_5 \circ arphi_1) = arphi_3 \circ arphi_2 = arphi_5 \ (arphi_3 \circ arphi_5) \circ arphi_1 = arphi_2 \circ arphi_1 = arphi_5$$

$$arphi_3 \circ (arphi_5 \circ arphi_2) = arphi_3 \circ arphi_3 = arphi_e \ (arphi_3 \circ arphi_5) \circ arphi_2 = arphi_2 \circ arphi_2 = arphi_e$$

$$\varphi_{3} \circ (\varphi_{5} \circ \varphi_{4}) = \varphi_{3} \circ \varphi_{e} = \varphi_{3}$$

$$(\varphi_{3} \circ \varphi_{5}) \circ \varphi_{4} = \varphi_{2} \circ \varphi_{4} = \varphi_{3}$$

$$\varphi_{4} \circ (\varphi_{1} \circ \varphi_{2}) = \varphi_{4} \circ \varphi_{4} = \varphi_{5}$$

$$(\varphi_{4} \circ \varphi_{1}) \circ \varphi_{2} = \varphi_{3} \circ \varphi_{2} = \varphi_{5}$$

$$\varphi_{4} \circ (\varphi_{1} \circ \varphi_{3}) = \varphi_{4} \circ \varphi_{5} = \varphi_{e}$$

$$(\varphi_{4} \circ \varphi_{1}) \circ \varphi_{3} = \varphi_{3} \circ \varphi_{3} = \varphi_{2}$$

$$\varphi_{4} \circ (\varphi_{1} \circ \varphi_{5}) = \varphi_{4} \circ \varphi_{3} = \varphi_{2}$$

$$(\varphi_{4} \circ \varphi_{1}) \circ \varphi_{5} = \varphi_{3} \circ \varphi_{5} = \varphi_{2}$$

$$\varphi_{4} \circ (\varphi_{2} \circ \varphi_{1}) = \varphi_{4} \circ \varphi_{5} = \varphi_{e}$$

$$(\varphi_{4} \circ \varphi_{2}) \circ \varphi_{1} = \varphi_{1} \circ \varphi_{1} = \varphi_{6}$$

$$\varphi_{4} \circ (\varphi_{2} \circ \varphi_{3}) = \varphi_{4} \circ \varphi_{4} = \varphi_{5}$$

$$(\varphi_{4} \circ \varphi_{2}) \circ \varphi_{3} = \varphi_{1} \circ \varphi_{5} = \varphi_{3}$$

$$\varphi_{4} \circ (\varphi_{2} \circ \varphi_{3}) = \varphi_{4} \circ \varphi_{4} = \varphi_{5}$$

$$(\varphi_{4} \circ \varphi_{2}) \circ \varphi_{3} = \varphi_{1} \circ \varphi_{5} = \varphi_{3}$$

$$\varphi_{4} \circ (\varphi_{2} \circ \varphi_{5}) = \varphi_{4} \circ \varphi_{1} = \varphi_{3}$$

$$(\varphi_{4} \circ \varphi_{2}) \circ \varphi_{5} = \varphi_{1} \circ \varphi_{5} = \varphi_{6}$$

$$(\varphi_{4} \circ \varphi_{3}) \circ \varphi_{1} = \varphi_{2} \circ \varphi_{1} = \varphi_{5}$$

$$\varphi_{4} \circ (\varphi_{3} \circ \varphi_{1}) = \varphi_{4} \circ \varphi_{4} = \varphi_{5}$$

$$(\varphi_{4} \circ \varphi_{3}) \circ \varphi_{1} = \varphi_{2} \circ \varphi_{1} = \varphi_{5}$$

$$\varphi_{4} \circ (\varphi_{3} \circ \varphi_{1}) = \varphi_{4} \circ \varphi_{5} = \varphi_{e}$$

$$(\varphi_{4} \circ \varphi_{3}) \circ \varphi_{1} = \varphi_{2} \circ \varphi_{2} = \varphi_{e}$$

$$\varphi_{4} \circ (\varphi_{3} \circ \varphi_{5}) = \varphi_{4} \circ \varphi_{5} = \varphi_{e}$$

$$(\varphi_{4} \circ \varphi_{3}) \circ \varphi_{5} = \varphi_{2} \circ \varphi_{5} = \varphi_{1}$$

$$(\varphi_{4} \circ \varphi_{3}) \circ \varphi_{5} = \varphi_{2} \circ \varphi_{5} = \varphi_{1}$$

$$(\varphi_{4} \circ \varphi_{3}) \circ \varphi_{5} = \varphi_{2} \circ \varphi_{5} = \varphi_{1}$$

$$(\varphi_{4} \circ \varphi_{5}) \circ \varphi_{1} = \varphi_{e} \circ \varphi_{1} = \varphi_{1}$$

$$(\varphi_{4} \circ \varphi_{5}) \circ \varphi_{1} = \varphi_{e} \circ \varphi_{1} = \varphi_{1}$$

$$(\varphi_{4} \circ \varphi_{5}) \circ \varphi_{1} = \varphi_{e} \circ \varphi_{1} = \varphi_{1}$$

$$(\varphi_{4} \circ \varphi_{5}) \circ \varphi_{1} = \varphi_{e} \circ \varphi_{1} = \varphi_{1}$$

$$(\varphi_{4} \circ \varphi_{5}) \circ \varphi_{1} = \varphi_{e} \circ \varphi_{1} = \varphi_{1}$$

$$(\varphi_{4} \circ \varphi_{5}) \circ \varphi_{1} = \varphi_{e} \circ \varphi_{2} = \varphi_{2}$$

$$(\varphi_{4} \circ \varphi_{5}) \circ \varphi_{3} = \varphi_{4} \circ \varphi_{3} = \varphi_{3}$$

$$(\varphi_{5} \circ \varphi_{1}) \circ \varphi_{2} = \varphi_{2} \circ \varphi_{2} = \varphi_{2}$$

$$(\varphi_{5} \circ \varphi_{1}) \circ \varphi_{2} = \varphi_{2} \circ \varphi_{2} = \varphi_{2}$$

$$(\varphi_{5} \circ \varphi_{1}) \circ \varphi_{2} = \varphi_{5} \circ \varphi_{5} = \varphi_{4}$$

$$(\varphi_{5} \circ \varphi_{1}) \circ \varphi_{3} = \varphi_{5} \circ \varphi_{5} = \varphi_{4}$$

$$(\varphi_{5} \circ \varphi_{1}) \circ \varphi_{3} = \varphi_{5} \circ \varphi_{5} = \varphi_{4}$$

$$(\varphi_{5} \circ \varphi_{1}) \circ \varphi_{3} = \varphi_{5} \circ \varphi_{5} = \varphi_{4}$$

$$(\varphi_{5} \circ \varphi_{1}) \circ \varphi_{3} = \varphi_{5} \circ \varphi_{5} = \varphi_{4}$$

$$(\varphi_{5} \circ \varphi_{1}) \circ \varphi_{3} = \varphi_{5} \circ \varphi_{5} = \varphi_{4}$$

$$(\varphi_{5} \circ \varphi_{1}) \circ \varphi_{4} = \varphi_{5} \circ \varphi_{5} = \varphi_$$

 $arphi_5 \circ (arphi_2 \circ arphi_1) = arphi_5 \circ arphi_5 = arphi_4 \ (arphi_5 \circ arphi_2) \circ arphi_1 = arphi_3 \circ arphi_1 = arphi_4$

$$\varphi_5 \circ (\varphi_2 \circ \varphi_3) = \varphi_5 \circ \varphi_4 = \varphi_e$$

$$(\varphi_5 \circ \varphi_2) \circ \varphi_3 = \varphi_3 \circ \varphi_3 = \varphi_e$$

$$\varphi_5 \circ (\varphi_2 \circ \varphi_4) = \varphi_5 \circ \varphi_3 = \varphi_1$$

$$(\varphi_5 \circ \varphi_2) \circ \varphi_4 = \varphi_3 \circ \varphi_4 = \varphi_1$$

$$\varphi_5 \circ (\varphi_3 \circ \varphi_1) = \varphi_5 \circ \varphi_4 = \varphi_e$$

$$(\varphi_5 \circ \varphi_3) \circ \varphi_1 = \varphi_1 \circ \varphi_1 = \varphi_e$$

$$\varphi_5 \circ (\varphi_3 \circ \varphi_2) = \varphi_5 \circ \varphi_5 = \varphi_4$$

$$(\varphi_5 \circ \varphi_3) \circ \varphi_2 = \varphi_1 \circ \varphi_2 = \varphi_4$$

$$(\varphi_5 \circ \varphi_3) \circ \varphi_2 = \varphi_1 \circ \varphi_2 = \varphi_4$$

$$\varphi_5 \circ (\varphi_3 \circ \varphi_4) = \varphi_5 \circ \varphi_1 = \varphi_2$$

$$(\varphi_5 \circ \varphi_3) \circ \varphi_4 = \varphi_1 \circ \varphi_4 = \varphi_2$$

$$(\varphi_5 \circ \varphi_3) \circ \varphi_4 = \varphi_1 \circ \varphi_4 = \varphi_2$$

$$(\varphi_5 \circ \varphi_4) \circ \varphi_1 = \varphi_e \circ \varphi_1 = \varphi_1$$

$$(\varphi_5 \circ \varphi_4) \circ \varphi_1 = \varphi_e \circ \varphi_1 = \varphi_2$$

$$(\varphi_5 \circ \varphi_4) \circ \varphi_2 = \varphi_e \circ \varphi_2 = \varphi_2$$

$$(\varphi_5 \circ \varphi_4) \circ \varphi_2 = \varphi_e \circ \varphi_2 = \varphi_3$$

$$(\varphi_5 \circ \varphi_4) \circ \varphi_3 = \varphi_6 \circ \varphi_3 = \varphi_3$$

$$(\varphi_5 \circ \varphi_4) \circ \varphi_3 = \varphi_6 \circ \varphi_3 = \varphi_3$$

- **3.-** Es claro que φ_e cumple $\forall \varphi_a \in G, \varphi_e \circ \varphi_a = \varphi_a \circ \varphi_e = a$ (con la composición como producto)
- **4.-** Sea $\varphi_a \in G$, $\therefore \varphi_a$ es una aplicación biyectiva de A en A, $\therefore \exists \varphi_a^{-1} : \varphi_a \circ \varphi_a^{-1} = \varphi_I$. φ_a^{-1} también es una aplicación biyectova de A en A, $\therefore \varphi_a^{-1} \in G$

2.3. Algunos lemas preliminares

Lema 2.1. Si G es un grupo, entonces:

1.
$$\exists ! \ e \in G : \forall \ a \in G \ a \cdot e = e \cdot a = a$$

2.
$$\forall a \in G \exists ! a^{-1} \in G : a \cdot a^{-1} = e$$

3.
$$\forall a \in G (a^{-1})^{-1} = a$$

4.
$$\forall a,b \in G \ (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

Demostraci'on.:

Sea G un grupo

- **1.** Sean e_1 , $e_2 \in G$: \forall a \in G $e_1 \cdot$ a = a· e_1 = a y $e_2 \cdot$ a = a· e_2 = a. Ahora e_1 = e_1 y $e_1 \cdot e_2 = e_1 \Rightarrow e_1 = e_1 \cdot e_2$, pero también se cumple que $e_1 \cdot e_2 = e_2$ \therefore $e_1 = e_2$
- **2.** Sean $\mathbf{a},a_1^{-1},\ a_2^{-1}\in G:\mathbf{a}\cdot a_1^{-1}=a_1^{-1}\cdot \mathbf{a}=\mathbf{e}$ y $\mathbf{a}\cdot a_2^{-1}=a_2^{-1}\cdot \mathbf{a}=\mathbf{e}$. Ahora

$$a_1^{-1}={\rm e\cdot}a_1^{-1}\Rightarrow a_1^{-1}=(a_2^{-1}\cdot{\rm a})\cdot a_1^{-1}\Rightarrow {\rm como}\; G$$
es grupo $a_1^{-1}=a_2^{-1}\cdot ({\rm a\cdot}a_1^{-1})\Rightarrow a_1^{-1}=a_2^{-1}\cdot {\rm e}$.: $a_1^{-1}=a_2^{-1}$

3. Sea a
$$\in G$$
 tenemos que a· a^{-1} = e y $a^{-1} \cdot (a^{-1})^{-1}$ = e \Rightarrow multiplicando por $(a^{-1})^{-1}$ tenemos: $(a \cdot a^{-1}) \cdot (a^{-1})^{-1} = (a^{-1})^{-1}$ y $(a^{-1})^{-1} \cdot (a^{-1} \cdot (a^{-1})^{-1})$ = $(a^{-1})^{-1} \Rightarrow (a \cdot a^{-1}) \cdot (a^{-1})^{-1} = (a^{-1})^{-1} \cdot (a^{-1} \cdot (a^{-1})^{-1}) \Rightarrow$ como G es grupo a· $(a^{-1} \cdot (a^{-1})^{-1}) = ((a^{-1})^{-1} \cdot a^{-1}) \cdot (a^{-1})^{-1} \Rightarrow$ a·e = e· $(a^{-1})^{-1} \therefore$ a = $(a^{-1})^{-1}$

4. Sean a,b $\in G$

$$(a \cdot b)^{-1} \cdot (a \cdot b) = (a \cdot b) \cdot (a \cdot b)^{-1} = e \Rightarrow (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \iff (b^{-1} \cdot a^{-1}) \cdot (a \cdot b)$$

$$= (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = e \iff ((b^{-1} \cdot a^{-1}) \cdot a) \cdot b = a \cdot (b \cdot (b^{-1} \cdot a^{-1})) = e \iff$$

$$(b^{-1} \cdot (a^{-1} \cdot a)) \cdot b = a \cdot ((b \cdot b^{-1}) \cdot a^{-1}) = e \iff (b^{-1} \cdot e) \cdot b = a \cdot (e \cdot a^{-1}) = e \iff$$

$$b^{-1} \cdot b = a \cdot a^{-1} = e \iff e = e = e$$

Lema 2.2. Dados a,b en el grupo $G \Rightarrow las$ ecuaciones $a \cdot x = b$ y $y \cdot a = b$ tienen soluciones únicas para x y y en G. En particular, las dos leyes de cancelación

- 1) $a \cdot u = a \cdot w \Rightarrow u = w$
- 2) $u \cdot a = w \cdot a \Rightarrow u = w$

.

 $Demostraci\'{o}n.$:

- 1) Sean a,b,c $\in G$: a·b = a·c $\Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c) \Rightarrow (a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$ $\Rightarrow e \cdot b = e \cdot c$ $\therefore b = c$
- 2) Sean a,b,c $\in G$: b·a = c·a \Rightarrow (b·a)· a^{-1} = (c·a)· a^{-1} \Rightarrow b·(a· a^{-1}) = c·(a· a^{-1}) \Rightarrow b·e = c·e \therefore b = c

.

Problemas.

- 1. Determine, en cada caso uno de los siguientes casos, si el sistema descrito es o no grupo.
 - a) $G = \mathbb{Z}$, $a \cdot b = a b$

Demostración. :

- 1. Sean $a,b \in G$, $a \cdot b \in G \iff a \cdot b \in \mathbb{Z}$ con $a,b \in \mathbb{Z}$
- 2. Sean $a,b,c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c \iff a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{ con } a,b,c \in Z$
- 3. \exists e \in G : a·e = e·a = a \forall a \in G \iff \exists e \in Z : a-e = e-a = a \forall a \in Z(el 0 cumple)
- 4. $\exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e \ \forall \ a \in G \iff \exists a^{-1} \in \mathbb{Z} : a^{-1} \cdot a = a \cdot a^{-1} = e \ \forall \ a \in \mathbb{Z} (a \text{ cumple})$

.

b) $G = \mathbb{Z}^+$, $a \cdot b = ab$

Demostración. :

- 1. Sean $a,b \in G$, $a \cdot b \in G \iff ab \in \mathbb{Z}^+ \text{ con } a,b \in \mathbb{Z}^+$
- 2. Sean $a,b,c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c \iff a(bc) = (ab)c \text{ con } a,b,c \in \mathbb{Z}^+$
- 3. \exists e \in G : a·e = e·a = a \forall a \in G \iff \exists e \in \mathbb{Z}^+ : ae = ea = a \forall a \in \mathbb{Z}^+ (el 1 cumple)
- 4. $\exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e \ \forall \ a \in G \iff \exists a^{-1} \in \mathbb{Z}^{-1} : a^{-1}a = aa^{-1} = e \ \forall \ a \in \mathbb{Z}^+, \text{ pero } \exists! \ a^{-1} \in \mathbb{Z}^+ \text{ con estas propiedades}$
- \therefore G no es un Grupo

.

- c) G:= { $a_i: 0 \le i \le 6$, $a_i \cdot a_j = a_{i+j}$ si i < j, $a_i \cdot a_j = a_{i+j-7}$ si $i + j \ge 7$ }, $a \cdot b = a + b$ Es claro que es Grupo, pues es otra manera de definir un $\mathbb{Z}_{[7]}$
- d) $G := \{ x \in G : x = \frac{a}{b} \in G, a, b \in \mathbb{Q} \land b \text{ es impar } \}$

Demostración. :

- 1. Sean $a,b \in G$ $a \cdot b \in G$, con $a = \frac{a_1}{a_2}$ y $b = \frac{b_1}{b_2}$, $\iff \frac{a_1}{a_2} + \frac{b_1}{b_2} = c \in \mathbb{Q}$ $\iff \frac{(a_1b_2) + (b_1a_2)}{a_2b_2} = c \in G \iff ((a_1b_2) + (b_1a_2)), (a_2b_2) \in G \land a_2b_2$ es impar, como $a_1, a_2, b_1, b_2 \in \mathbb{Z} \Rightarrow (a_1b_2), (b_1a_2) \in \mathbb{Z} \Rightarrow (a_1b_2) + (b_1a_2)$ $\in \mathbb{Z}$, Ahora como a_2 y $b_2 \in G \land a_2$, b_2 son impares $\Rightarrow a_2b_2$ es impar \therefore $c \in G$
- $\begin{array}{l} \text{2. Sean } \mathbf{a} = \frac{a_1}{a_2}, \ \mathbf{b} = \frac{b_1}{b_2}, \ \mathbf{c} = \frac{c_1}{c_2} \in \mathbf{G} \ \mathbf{a} \cdot (\mathbf{b} \cdot \mathbf{c}) = (\mathbf{a} \cdot \mathbf{b}) \cdot \mathbf{c} \iff \frac{a_1}{a_2} + \frac{b_1}{b_2} + \frac{c_1}{c_2} = \\ \frac{a_1}{a_2} + \frac{b_1}{b_2} + \frac{c_1}{c_2} \iff \frac{a_1}{a_2} + \frac{(b_1c_2) + (c_1b_2)}{b_2c_2} = \frac{(a_1b_2) + (b_1a_2)}{a_2b_2} + \frac{c_1}{c_2} \iff \frac{a_1(b_2c_2) + ((b_1c_2) + (c_1b_2))a_2}{a_2(b_2c_2)} \\ = \frac{((a_1b_2) + (b_1a_2))c_2 + c_1(a_2b_2)}{(a_2b_2)c_2} \iff \frac{a_1b_2c_2 + b_1c_2a_2 + c_1b_2a_2}{a_2b_2c_2} = \frac{a_1b_2c_2 + b_1a_2c_2 + c_1a_2b_2}{a_2b_2c_2}, \\ \text{Sabemos que se cumple pues } a_1, \ a_2, \ b_1, \ b_2, \ c_1, \ c_2 \in \mathbb{Z} \{0\} \ \text{y como } a_2, \\ b_2, \ c_2 \ \text{son impares} \implies a_2b_2c_2 \ \text{es impar} \\ \end{array}$
- 3. Sea a = $\frac{a_1}{a_2} \in G \Rightarrow \exists$ e \in G : a·e = e·a = a $\iff \exists$ e \in \mathbb{Q} : $\frac{a_1}{a_2}$ + e = e + $\frac{a_1}{a_2}$ = $\frac{a_1}{a_2}$, 0 cumple y admás 0 \in G pues 0 = $\frac{0}{3}$ \in G
- 4. Sea $a = \frac{a_1}{a_2} \in G \Rightarrow \exists \ a^{-1} \in G : a_1 \cdot a^{-1} = a^{-1} \cdot a_1 = e \iff \exists \ \frac{b_1}{b_2} \in \mathbb{Q} : \frac{a_1}{a_2} + \frac{b_1}{b_2} = \frac{b_1}{b_2} + \frac{a_1}{a_2} = e \land b_2 \text{ es impar, } -\frac{a_1}{a_2} \text{ cumple}$

2. Si Ges un Grupo abeliano $\Rightarrow \forall$ a,
b $\in G$ y \forall n $\in \mathbb{N}$ (a·b)
^n = $a^n \cdot b^n$

Demostración. Sean a,b
$$\in G$$
 grupo abeliano y n $\in \mathbb{N}$ n = 2
$$(a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b) = a \cdot (b \cdot (a \cdot b)) = a \cdot (b \cdot (b \cdot a)) = a \cdot (b^2 \cdot a) = a \cdot (a \cdot b^2) = (a \cdot a) \cdot b^2 = a^2 \cdot b^2$$

suponemos que se cumple para n = i (a·b)^i = a^i \cdot b^i

$$\begin{array}{l} \mathbf{n} = \mathbf{i} {+} \mathbf{1} \\ \mathbf{Sean} \ \mathbf{a}, \mathbf{b} \in G \end{array} \qquad \Box$$