

Herstein Algebra Moderna Resuelto

Humberto Alonso Villegas

20 de enero de 2014

1. Teoría de Conjuntos

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

- pensar como humano
- actuar como humano
- actuar racionalmente
- pensar racionalmente

2. Teoría de Grupos

2.1. Definición 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. $\forall a, b \in G \Rightarrow a \cdot b \in G$
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. $\forall a \in G \exists a^{-1} \in G : a \cdot a^{-1} = e$

Demostración. :

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 $a, b, c \in G, \Rightarrow a, b, c \in \mathbb{Z}, \Rightarrow a \cdot (b \cdot c) = a + (b + c) = (a + b) + c = (a \cdot b) \cdot c \Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3.- Sea $a \in G, \exists e \in G : e \cdot a = a \cdot e = a \forall a \in G \iff \exists w \in \mathbb{Z} : w \cdot a = a \cdot w = a \forall a \in \mathbb{Z}$ (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 $a, b \in G \Rightarrow a, b \in \mathbb{Z}, a \cdot b = b \cdot a \iff a + b = b + a \quad \square$

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.

Demostración. :

Es claro que el orden de G es 2

1, 3, 4:

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

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

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.

Demostración. :

$\varphi_e := G \rightarrow G$ donde:

$$\varphi_e(x_1) = x_1$$

$$\varphi_e(x_2) = x_2$$

$$\varphi_e(x_3) = x_3$$

$\varphi_1 := G \rightarrow G$ donde:

$$\varphi_1(x_1) = x_1$$

$$\varphi_1(x_2) = x_3$$

$$\varphi_1(x_3) = x_2$$

$\varphi_2 := G \rightarrow G$ donde:

$$\varphi_2(x_1) = x_3$$

$$\varphi_2(x_2) = x_2$$

$$\varphi_2(x_3) = x_1$$

$\varphi_3 := G \rightarrow G$ donde:

$$\varphi_3(x_1) = x_2$$

$$\varphi_3(x_2) = x_1$$

$$\varphi_3(x_3) = x_3$$

$\varphi_4 := G \rightarrow G$ donde:

$$\varphi_4(x_1) = x_2$$

$$\varphi_4(x_2) = x_3$$

$$\varphi_4(x_3) = x_1$$

$\varphi_5 := G \rightarrow G$ 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 $\varphi_a \circ (\varphi_b \circ \varphi_c) = (\varphi_a \circ \varphi_b) \circ \varphi_c \quad \forall \varphi_a, \varphi_b, \varphi_c \in G$
Omitiremos cuando alguna φ es φ_e , pues es claro que se cumple.

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

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

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

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

$$\begin{aligned}\varphi_5 \circ (\varphi_4 \circ \varphi_1) &= \varphi_5 \circ \varphi_3 = \varphi_1 \\ (\varphi_5 \circ \varphi_4) \circ \varphi_1 &= \varphi_e \circ \varphi_1 = \varphi_1\end{aligned}$$

$$\begin{aligned}\varphi_5 \circ (\varphi_4 \circ \varphi_2) &= \varphi_5 \circ \varphi_1 = \varphi_2 \\ (\varphi_5 \circ \varphi_4) \circ \varphi_2 &= \varphi_e \circ \varphi_2 = \varphi_2\end{aligned}$$

$$\begin{aligned}\varphi_5 \circ (\varphi_4 \circ \varphi_3) &= \varphi_5 \circ \varphi_2 = \varphi_3 \\ (\varphi_5 \circ \varphi_4) \circ \varphi_3 &= \varphi_e \circ \varphi_3 = \varphi_3\end{aligned}$$

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 $A, \therefore \exists \varphi_a^{-1} : \varphi_a \circ \varphi_a^{-1} = \varphi_I. \varphi_a^{-1}$ también es una aplicación biyectiva de A en $A, \therefore \varphi_a^{-1} \in G$ □

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

Demostración. :
Sea G un grupo

1. Sean $e_1, e_2 \in G : \forall a \in G \ e_1 \cdot a = a \cdot e_1 = a$ y $e_2 \cdot a = a \cdot e_2 = a$. 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 $a, a_1^{-1}, a_2^{-1} \in G : a \cdot a_1^{-1} = a_1^{-1} \cdot a = e$ y $a \cdot a_2^{-1} = a_2^{-1} \cdot a = e$. Ahora $a_1^{-1} = e \cdot a_1^{-1} \Rightarrow a_1^{-1} = (a_2^{-1} \cdot a) \cdot a_1^{-1} \Rightarrow$ como G es grupo $a_1^{-1} = a_2^{-1} \cdot (a \cdot a_1^{-1}) \Rightarrow a_1^{-1} = a_2^{-1} \cdot e$
 $\therefore a_1^{-1} = a_2^{-1}$

3. Sea $a \in G$ tenemos que $a \cdot a^{-1} = e$ 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 $a \cdot (a^{-1} \cdot (a^{-1})^{-1}) = ((a^{-1})^{-1} \cdot a^{-1}) \cdot (a^{-1})^{-1} \Rightarrow a \cdot e = e \cdot (a^{-1})^{-1} \therefore a = (a^{-1})^{-1}$

4. Sean $a, b \in G$
 $(a \cdot b)^{-1} \cdot (a \cdot b) = (a \cdot b) \cdot (a \cdot b)^{-1} = e \Rightarrow (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \iff (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = e \iff ((b^{-1} \cdot a^{-1}) \cdot a) \cdot b = a \cdot (b \cdot (b^{-1} \cdot a^{-1})) = e \iff (b^{-1} \cdot (a^{-1} \cdot a)) \cdot b = a \cdot ((b \cdot b^{-1}) \cdot a^{-1}) = e \iff (b^{-1} \cdot e) \cdot b = a \cdot (e \cdot a^{-1}) = e \iff b^{-1} \cdot b = a \cdot a^{-1} = e \iff e = e = e$ □

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

□

.

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

Demostración. :

1. Sean $a, b \in G$, $a \cdot b \in G \iff ab \in \mathbb{Z}^+$ con $a, b \in \mathbb{Z}^+$
2. Sean $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c \iff a(bc) = (ab)c$ con $a, b, c \in \mathbb{Z}^+$
3. $\exists e \in G : a \cdot e = e \cdot a = a \forall a \in G \iff \exists e \in \mathbb{Z}^+ : ae = ea = a \forall a \in \mathbb{Z}^+$ (el 1 cumple)
4. $\exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e \forall a \in G \iff \exists a^{-1} \in \mathbb{Z}^{-1} : a^{-1}a = aa^{-1} = e \forall a \in \mathbb{Z}^+$, pero $\nexists! a^{-1} \in \mathbb{Z}^+$ con estas propiedades

$\therefore G$ no es un Grupo

□

.

c) $G := \{ a_i : 0 \leq i \leq 6, a_i \cdot a_j = a_{i+j} \text{ si } i < j, a_i \cdot a_j = a_{i+j-7} \text{ si } i + j \geq 7 \}$, $a \cdot b = a + b$

Es claro que es Grupo, pues es otra manera de definir un $\mathbb{Z}_{[7]}$

d) $G := \{ x \in G : x = \frac{a}{b} \in G, a, b \in \mathbb{Q} \wedge b \text{ es impar} \}$

Demostración. :

1. Sean $a, b \in G$ $a \cdot b \in G$, con $a = \frac{a_1}{a_2}$ y $b = \frac{b_1}{b_2}$, $\iff \frac{a_1}{a_2} + \frac{b_1}{b_2} = c \in \mathbb{Q}$
 $\iff \frac{(a_1 b_2) + (b_1 a_2)}{a_2 b_2} = c \in G \iff ((a_1 b_2) + (b_1 a_2)), (a_2 b_2) \in G \wedge a_2 b_2$
 es impar, como $a_1, a_2, b_1, b_2 \in \mathbb{Z} \Rightarrow (a_1 b_2), (b_1 a_2) \in \mathbb{Z} \Rightarrow (a_1 b_2) + (b_1 a_2) \in \mathbb{Z}$, Ahora como a_2 y $b_2 \in G \wedge a_2, b_2$ son impares $\Rightarrow a_2 b_2$ es impar $\therefore c \in G$
2. Sean $a = \frac{a_1}{a_2}, b = \frac{b_1}{b_2}, c = \frac{c_1}{c_2} \in G$ $a \cdot (b \cdot c) = (a \cdot b) \cdot c \iff \frac{a_1}{a_2} + \frac{b_1}{b_2} + \frac{c_1}{c_2} = \frac{a_1}{a_2} + \frac{b_1}{b_2} + \frac{c_1}{c_2}$
 $\iff \frac{a_1}{a_2} + \frac{(b_1 c_2) + (c_1 b_2)}{b_2 c_2} = \frac{(a_1 b_2) + (b_1 a_2)}{a_2 b_2} + \frac{c_1}{c_2} \iff \frac{a_1(b_2 c_2) + ((b_1 c_2) + (c_1 b_2))a_2}{a_2(b_2 c_2)} =$
 $\frac{((a_1 b_2) + (b_1 a_2))c_2 + c_1(a_2 b_2)}{(a_2 b_2)c_2} \iff \frac{a_1 b_2 c_2 + b_1 c_2 a_2 + c_1 b_2 a_2}{a_2 b_2 c_2} = \frac{a_1 b_2 c_2 + b_1 a_2 c_2 + c_1 a_2 b_2}{a_2 b_2 c_2},$
 Sabemos que se cumple pues $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Z} - \{0\}$ y como a_2, b_2, c_2 son impares $\Rightarrow a_2 b_2 c_2$ es impar
3. Sea $a = \frac{a_1}{a_2} \in G \Rightarrow \exists e \in G : a \cdot e = e \cdot a = a \iff \exists e \in \mathbb{Q} : \frac{a_1}{a_2} + e = e + \frac{a_1}{a_2} = \frac{a_1}{a_2}, 0$ cumple y además $0 \in G$ pues $0 = \frac{0}{3} \in G$
4. Sea $a = \frac{a_1}{a_2} \in G \Rightarrow \exists a^{-1} \in G : a_1 \cdot a^{-1} = a^{-1} \cdot a_1 = e \iff \exists \frac{b_1}{b_2} \in \mathbb{Q} : \frac{a_1}{a_2} + \frac{b_1}{b_2} = \frac{b_1}{b_2} + \frac{a_1}{a_2} = e \wedge b_2$ es impar, $-\frac{a_1}{a_2}$ cumple

□