Álgebra Moderna: Tarea 1.1

Tomás Ricardo Basile Álvarez
316617194

25 de septiembre de 2020

a) Determina cuales de las siguientes operaciones binarias son asociativas y cuales no. Justifica tu respuesta:

(a1): La operación $\star$ sobre $\mathbb{Z}$ definida por $a \star b := a - b$

No es asociativa pues si $a, b, c \in \mathbb{Z}$, tenemos que:

$$\begin{aligned} a \star (b \star c) &= a \star (b - c) \quad \text{Por la definición de } \star \\ &= a - (b - c) \quad \text{Por la definición de } \star \\ &= a - b + c \end{aligned}$$

Mientras que por otro lado se tiene:

$$\begin{aligned} (a \star b) \star c &= (a - b) \star c \quad \text{Por la definición de } \star \\ &= (a - b) - c \quad \text{Por la definición de } \star \\ &= a - b - c \end{aligned}$$

Con esto vemos que $a \star (b \star c)$ es en general distinto a $(a \star b) \star c$ pues para $a, b, c \in \mathbb{Z}$, generalemente $a - b + c$ es distinto a $a - b - c$.

(a2) La operación $\star$ sobre los $\mathbb{R}$ definida por $a \star b := a + b + ab$

Sí es asociativa, pues si $a, b, c \in \mathbb{Z}$, por un lado tenemos que:

$$\begin{aligned} a \star (b \star c) &= a \star (b + c + bc) \text{ Por la definición de } \star \\ &= a + (b + c + bc) + a(b + c + bc) \text{ Por la definición de } \star \\ &= a + b + c + bc + ab + ac + abc \text{ Realizando las operaciones en los enteros} \end{aligned}$$

Pero por otro lado, si colocamos asociamos de manera distinta tenemos:

$$\begin{aligned} (a \star b) \star c &= (a + b + ab) \star c \text{ Por la definición de } \star \\ &= (a + b + ab) + c + (a + b + ab)c \text{ Por la definición de } \star \\ &= a + b + ab + c + ac + bc + abc \text{ Haciendo las operaciones de enteros} \\ &= a + b + c + bc + ab + ac + abc \text{ Reordenando las sumas} \end{aligned}$$

Vemos que los resultados para $a \star (b \star c)$ y para $(a \star b) \star c$ son iguales y por tanto, la operación es asociativa.

(a3) La operación $\star$ sobre los $\mathbb{Z} \times \mathbb{Z}$ definida por:

$$(a, b) \star (c, d) := (ad + bc, bd)$$

Primero tomamos tres elementos del grupo que sean $(a_1, b_1), (a_2, b_2), (a_3, b_3)$ para $a_1, a_2, a_3, b_1, b_2, b_3$ enteros. Por un lado tenemos:

$$\begin{aligned}(a_1, b_1) \star ((a_2, b_2) \star (a_3, b_3)) &= (a_1, b_1) \star (a_2 b_3 + b_2 a_3, b_2 b_3) \ \text{ por def de } \star \\ &= (a_1(b_2 b_3) + b_1(a_2 b_3 + b_2 a_3), b_1(b_2 b_3)) \ \text{ por def de } \star \\ &= (a_1 b_2 b_3 + a_2 b_1 b_3 + a_3 b_1 b_2 \ , \ b_1 b_2 b_3) \ \text{ Operamos los enteros}\end{aligned}$$

Por otro lado, si asociamos de otra forma, tenemos:

$$\begin{aligned}((a_1, b_1) \star (a_2, b_2)) \star (a_3, b_3) &= (a_1 b_2 + b_1 a_2 \ , \ b_1 b_2) \star (a_3, b_3) \ \text{ por def de } \star \\ &= ((a_1 b_2 + b_1 a_2) b_3 + (b_1 b_2) a_3 \ , \ (b_1 b_2) b_3) \ \text{ por def de } \star \\ &= (a_1 b_2 b_3 + a_2 b_1 b_3 + a_3 b_1 b_2 \ , \ b_1 b_2 b_3) \ \text{ Operamos los enteros}\end{aligned}$$

Podemos ver que ambas operaciones tienen el mismo resultado, por lo tanto concluimos que $\star$ es una operación asociativa.

b) Determina cuales de los siguientes conjuntos son grupos bajo la suma y cuales no. Justifica tu respuesta.

(b1): $A \subset \mathbb{Q}$, con $A := \{x \in \mathbb{Q} \mid \text{el valor absoluto de } x \text{ es menor que } 1\ \}$.

No es un grupo bajo la suma ya que para empezar, la suma en este conjunto no es cerrada. Consideramos como ejemplo los racionales 0,7 y 0,8 que claramente son racionales y tienen valor absoluto menor que 1 por lo que pertenecen a A. Luego, su suma es $0{,}7 + 0{,}8 = 1{,}5$ que es un racional pero su valor absoluto es mayor que 1 por lo que no pertenece a A. Entonces, como la operación no es cerrada, A no es un grupo bajo la suma.

(b2) $A \subset \mathbb{Q}$, con $A := \{x \in \mathbb{Q} | \text{ el valor absoluto de } x \text{ es mayor o igual que } 1\}$.

No es un grupo, pues la suma no es cerrada en A. Consideramos los racionales -2 y 1,5. Estos elementos pertenecen a A pues claramente son racionales y sus valores absolutos son respectivamente 2, 1,5 , que son mayores que 1. Sin embargo, si realizamos su suma obtenemos $-2 + 1{,}5 = -0{,}5$ y este resultado no se encuentra en A, pues a pesar de ser un racional, su valor absoluto es menor que 1.

(b3) : $A \subset \mathbb{Q}$, con $A := \{a \in \mathbb{Q} \,|x = \frac{p}{1}, x = \frac{p}{2}$ ó $x = \frac{p}{3}$ para $p \in \mathbb{Z}\}$

No es un grupo, pues la suma no es cerrada en A. Consideramos $\frac{1}{2}$ y $\frac{1}{3}$, estos números son claramente elementos de A, pues tienen respectivamente la forma $\frac{p}{2}, \frac{p}{3}$ para $p = 1 \in \mathbb{Z}$. Sin embargo, si realizamos la suma, obtenemos $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$ que no es un elemento de A. Esto porque $\frac{5}{6}$ ya está escrito en su mínima expresión y por tanto no puede escribirse como la división de dos enteros con un denominador menor a 6 (y para que pertenezca al conjunto habría que escribirlo como una división de dos enteros con el denominador igual a $1, 2$ ó 3).

c) Sea $G := \{a + b\sqrt{2} \in \mathbb{R}|a, b \in \mathbb{Q}\}$

(c1) Probar que G es un grupo bajo la suma.

1) Cerradura: Sea $a_1 + b_1\sqrt{2} \in G$, $a_2 + b_2\sqrt{2} \in G$, para lo cual $a_1, b_1, a_2, b_2 \in \mathbb{Q}$. La suma de estos elementos es: $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$. Y por la cerradura de la suma en $\mathbb{Q}$ tenemos que: $a_1 + a_2 \in \mathbb{Q},\ b_1 + b_2 \in \mathbb{Q}$. Entonces $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$ tiene la forma que debe de tener para pertenecer a G.

2) Asociatividad: En este caso, como $+$ es una operación asociativa en $\mathbb{R}$ y claramente $G \subset \mathbb{R}$, entonces la suma sigue siendo asociativa en G como se menciona en la observación 1.4 de las notas de clase 1.

3) Neutro: El neutro es el número real 0. Primero vemos que $0 \in G$, pues $0 = 0 + 0\sqrt{2}$ y este elemento tiene la forma que pide el conjunto G con $a = b = 0$. Además, efectivamente es el neutro de G pues para todo $a+b\sqrt{2} \in G$ tenemos que $(a+b\sqrt{2})+0 = a+b\sqrt{2}$ y que $0 + (a + b\sqrt{2}) = a + b\sqrt{2}$.

4) Inverso: Sea $a + b\sqrt{2} \in G$, para lo cual $a, b \in \mathbb{Q}$. Este elemento tiene como inverso a $-a + (-b)\sqrt{2}$, que pertenece a G porque $-a, -b \in \mathbb{Q}$ y realmente es el inverso porque: $(a + b\sqrt{2}) + (-a + (-b)\sqrt{2}) = (a - a) + (b - b)\sqrt{2} = 0$ y $(-a + (-b)\sqrt{2}) + (a + b\sqrt{2}) = (-a + a) + (-b + b)\sqrt{2} = 0$.

(c2) Probar que $G/\{0\}$ es un grupo bajo el producto.

1) Cerradura: Sea $a_1 + b_1\sqrt{2} \in G$ y $a_2 + b_2\sqrt{2} \in G$, para lo cual $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. El producto de estos elementos es $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + a_2b_1\sqrt{2} + a_1b_2\sqrt{2} + 2b_1b_2 = (a_1a_2 + 2b_1b_2) + (a_2b_1 + a_1b_2)\sqrt{2}$
Y este elemento tiene la forma requerida por G porque como $a_1, b_1, a_2, b_2 \in \mathbb{Q}$, entonces los elementos $(a_1a_2 + 2b_1b_2) \in \mathbb{Q}$ y $(a_2b_1 + a_1b_2) \in \mathbb{Q}$ ya que son conseguidos con puros productos y sumas de racionales. Además, como $a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2}$ son distintos de 0 porque pertenecen a $G/\{0\}$ entonces su producto no es 0 y entonces el producto

pertenece a $G/\{0\}$.

2) Asociatividad: Como el producto es asociativo en $\mathbb{R}/\{0\}$ y el conjunto $G/\{0\}$ cumple claramente que $G/\{0\} \subset \mathbb{R}/\{0\}$. Entonces el producto es asociativo también en $G/\{0\}$ como se menciona en la obsevación 1.4 de las notas de clase 1.

3) Neutro: El neutro es el número real 1. Vemos que $1 \in G/\{0\}$ porque 1 se puede escribir como $1 + 0\sqrt{2}$ y así tiene la forma requerida por $G/\{0\}$.
Además, efectivamente es el neutro de $G/\{0\}$ porque $(a + b\sqrt{2}) \cdot 1 = 1 \cdot (a + b\sqrt{2}) = a + b\sqrt{2}$ porque 1 es el neutro de $\mathbb{R}$.

4) Inverso: Sea $a + b\sqrt{2} \in G$ distinto de 0, para lo cual $a, b \in \mathbb{Q}$ y no son ambos 0 a la vez, entonces visto como elemento de $\mathbb{R}/\{0\}$, tiene como inverso:

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 + 2b^2} = \left(\frac{a}{a^2 + 2b^2}\right) + \left(\frac{-b}{a^2 + 2b^2}\right)\sqrt{2}$$

Vemos que este elemento pertenece a $G/\{0\}$ porque ambas expresiones entre paréntesis existen (porque el denominador no se anula ya que al menos uno de los valores a, b es distinto de 0), son racionales (porque a, b son racionales y los productos y sumas son cerrados en $\mathbb{Q}$) y además, el inverso no es 0 porque por lo menos uno de los números $a, -b$ es distinto de 0, así que el resultado pertenece a $G/\{0\}$.

d) Sea G un grupo y $x \in G$. Definimos el orden de x como n el menor entero positivo tal que $x^n = 1$. Encontrar el orden de los siguientes elementos del grupo multiplicativo $\mathbb{Z}_{36}^*/\{\bar{0}\}$:

$$\bar{1}, \bar{5}, \overline{13}, \overline{17}, \overline{-1}, \overline{-13}$$

Primero notamos que el neutro en este grupo es $\bar{1}$ porque para todo $\bar{a} \in \mathbb{Z}_{36}^*/\{\bar{0}\}$ se tiene que $\bar{a}\bar{1} = \bar{1}\bar{a} = \overline{1 \cdot a} = \bar{a}$
a) $\bar{1}$: Como $(\bar{1})^1 = \bar{1}$ entonces el orden de $\bar{1}$ es 1.

b) $\bar{5}$: Calculamos sus potencias y cada que podemos, simplificamos el elemento sustituyéndolo por otro elemento de la misma clase de equivalencia pero que se encuentre entre 1 y 35 (es decir, lo sustituimos por su residuo al dividir por 36)

$$\begin{aligned}
\bar{5}^1 &= \bar{5} \\
\bar{5}^2 &= \overline{5 \cdot 5} = \overline{25} \\
\bar{5}^3 &= \bar{5} \cdot \bar{5}^2 = \bar{5} \cdot \overline{25} = \overline{5 \cdot 25} = \overline{125} = \overline{17} \\
\bar{5}^4 &= \bar{5}^1 \cdot \bar{5}^3 = \bar{5} \cdot \overline{17} = \overline{5 \cdot 17} = \overline{85} = \overline{13} \\
\bar{5}^5 &= \bar{5}^1 \cdot \bar{5}^4 = \bar{5} \cdot \overline{13} = \overline{5 \cdot 13} = \overline{65} = \overline{29} \\
\bar{5}^6 &= \bar{5}^1 \cdot \bar{5}^5 = \bar{5} \cdot \overline{29} = \overline{5 \cdot 29} = \overline{145} = \bar{1}
\end{aligned}$$

Con lo que tenemos que el orden de 5 es 6.

c) $\overline{13}$: Realizamos el mismo procedimiento que en b):

$$\begin{aligned}
\overline{13}^1 &= \overline{13} \\
\overline{13}^2 &= \overline{13} \cdot \overline{13} = \overline{13 \cdot 13} = \overline{169} = \overline{25} \\
\overline{13}^3 &= \overline{13}^1 \cdot \overline{13}^2 = \overline{13} \cdot \overline{25} = \overline{13 \cdot 25} = \overline{325} = \overline{1}
\end{aligned}$$

Por lo que el orden de 13 es igual a 3.

d) $\overline{17}$: Realizamos el mismo procedimiento:

$$\begin{aligned}
\overline{17}^1 &= \overline{17} \\
\overline{17}^2 &= \overline{17} \cdot \overline{17} = \overline{17 \cdot 17} = \overline{289} = \overline{1}
\end{aligned}$$

Por lo que el orden de $\overline{17}$ es igual a 2.

e) $\overline{-1}$: Primero que nada, $\overline{-1} = \overline{35}$ porque $35, -1$ son congruente módulo 36 ya que $35 - (-1) = 36$, lo cuál es un múltiplo de 36. Ahora calculamos el orden de $\overline{35}$:

$$\begin{aligned}
\overline{35}^1 &= \overline{35} \\
\overline{35}^2 &= \overline{35} \cdot \overline{35} = \overline{35 \cdot 35} = \overline{1225} = \overline{1}
\end{aligned}$$

Por lo que el orden de $\overline{35} = \overline{-1}$ es 2.

f) $\overline{-13}$: Vemos que $\overline{-13} = \overline{-13 + 36} = \overline{23}$. Así que mejor calculamos el orden de $\overline{23}$:

$$\begin{aligned}
\overline{23}^1 &= \overline{23} \\
\overline{23}^2 &= \overline{23} \cdot \overline{23} = \overline{23 \cdot 23} = \overline{529} = \overline{25} \\
\overline{23}^3 &= \overline{23}^1 \cdot \overline{23}^2 = \overline{23} \cdot \overline{25} = \overline{23 \cdot 25} = \overline{575} = \overline{35} \\
\overline{23}^4 &= \overline{23} \cdot \overline{23}^3 = \overline{23} \cdot \overline{35} = \overline{23 \cdot 35} = \overline{805} = \overline{13} \\
\overline{23}^5 &= \overline{23} \cdot \overline{23}^4 = \overline{23} \cdot \overline{13} = \overline{23 \cdot 13} = \overline{299} = \overline{11} \\
\overline{23}^6 &= \overline{23} \cdot \overline{23}^5 = \overline{23} \cdot \overline{11} = \overline{23 \cdot 11} = \overline{253} = \overline{1}
\end{aligned}$$

Por lo que el orden de $\overline{23} = \overline{-13}$ es 6.

e) Sea G un grupo. Probar que si $x^2 = 1$ para todo $x \in G$, entonces G es abeliano.

Como para todo $x \in G$ se tiene que $x^2 = xx = 1$ y como los inversos son únicos, se puede ver que el inverso de x es x.

Sean $x, y \in G$ arbitrarios, entonces por cerradura se tiene que $xy \in G$.
Y como xy es elemento de G, xy es su propio inverso, entonces:

$$\begin{aligned}
&(xy)^{-1} = xy \\
\Rightarrow\ & y^{-1}x^{-1} = xy \quad \text{Por la proposición 2.3 d) de las notas de clase 2} \\
\Rightarrow\ & y^{-1}x^{-1}x = xyx \ \text{ Multiplicamos por x a la derecha} \\
\Rightarrow\ & y^{-1} = xyx \ \text{ porque } \ x^{-1}x = 1 \\
\Rightarrow\ & x^{-1}y^{-1} = x^{-1}xyx \ \text{ multiplicamos por } x^{-1} \text{ a la izquierda} \\
\Rightarrow\ & x^{-1}y^{-1} = yx \ \text{ porque } \ x^{-1}x = 1 \\
\Rightarrow\ & xy = yx
\end{aligned}$$

El último paso debido a lo discutido al inicio de que cada elemento es su propio inverso.
Entonces, para todo $x, y \in G$ se cumple que $xy = yx$ y por tanto el grupo es conmutativo.