Juan Menduiña

Trabajo Práctico N° 5.1:
Estructuras Algebraicas - Teoría de Grupos.

Ejercicio 1.

Determinar cuáles de las siguientes operaciones están bien definidas sobre el conjunto A dado. Analizar las propiedades en los casos afirmativos:

(a) $A= \mathbb{N}$, $a*b= 3ab$.

Esta operación está bien definida sobre el conjunto A dado, ya que, para cada a, b ∈ A, 3ab ∈ A.

<u>Conmutatividad:</u> La operación * en A es conmutativa porque se cumple que, para cada a, b ∈ A, a*b= b*a. En particular, 3ab= 3ba.

<u>Asociatividad:</u> La operación * en A es asociativa porque se cumple que, para cada a, b, c ∈ A, (a*b)*c= a*(b*c). En particular, 3 (3ab) c= 3a (3bc) ⟺ 9abc= 9abc.

<u>Elemento neutro:</u> No existe un elemento e ∈ A tal que, para todo a ∈ A, se cumple que a*e= e*a= a. En particular, 3ae= 3ea= a ⟺ 3e= $\frac{a}{a}$ ⟺ 3e= 1 ⟺ e= $\frac{1}{3}$ ∉ A.

<u>Inversos:</u> Un elemento a ∈ A tiene inverso si existe a´ ∈ A tal que a*a´= a´*a= e. En particular, no existe elemento neutro, por lo que no existen inversos.

(b) $A= \mathbb{Z}$, $a*b= \frac{a+b}{3+ab}$.

Esta operación no está bien definida sobre el conjunto A dado, ya que no se cumple que, para cada a, b ∈ A, $\frac{a+b}{3+ab}$ ∉ A.

(c) $A= \mathbb{R}$, $x*y= x + y - xy$.

Esta operación está bien definida sobre el conjunto A dado, ya que, para cada x, y ∈ A, x + y - xy ∈ A.

<u>Conmutatividad:</u> La operación * en A es conmutativa porque se cumple que, para cada x, y ∈ A, x*y= y*x. En particular, x + y - xy= y + x - yx.

<u>Asociatividad:</u> La operación * en A es asociativa porque se cumple que, para cada x, y, z ∈ A, (x*y)*z= x*(y*z). En particular, (x + y - xy) + z - (x + y - xy) z= x + (y + z - yz) - x (y + z - yz) ⟺ x + y - xy + z - xz - yz + xyz= x + y + z - yz - xy - xz + xyz.

Elemento neutro: Existe un elemento e ∈ A tal que, para todo x ∈ A, se cumple que x*e= e*x= x. En particular, x + e - xe= e + x - ex= x ⟺ e - xe= x - x ⟺ e (1 - x)= 0 ⟺ e= $\frac{0}{1-x}$ ⟺ e= 0 ∈ A.

Inversos: Un elemento x ∈ A tiene inverso si existe x´ ∈ A tal que x*x´= x´*x= e. En particular, x + x´ - xx´= x´ + x - x´x= 0 ⟺ x´ - xx´= -x ⟺ x´ (1 - x)= -x ⟺ x´= $\frac{-x}{1-x}$, por lo que existe inverso para todo x ∈ A \ {1}, ya que x´= $\frac{-x}{1-x}$ ∈ A.

(d) *A= {0, 1, 2, 3},*

*	***0***	***1***	***2***	***3***
0	*0*	*0*	*0*	*0*
1	*0*	*1*	*2*	*3*
2	*1*	*2*	*0*	*2*
3	*2*	*3*	*1*	*1*

Esta operación está bien definida sobre el conjunto A dado, ya que, para cada a, b ∈ A, a*b ∈ A.

Conmutatividad: La operación * en A no es conmutativa porque no se cumple que, para cada a, b ∈ A, a*b= b*a. En particular, 0*2≠ 2*0 ⟺ 0≠ 1.

Asociatividad: La operación * en A no es asociativa porque no se cumple que, para cada a, b, c ∈ A, (a*b)*c= a*(b*c). En particular, para a= 2, b= 3, c= 2, (2*3)*2≠ 2*(3*2) ⟺ 2*2≠ 2*1 ⟺ 0≠ 2.

Elemento neutro: Existe un elemento e ∈ A tal que, para todo a ∈ A, se cumple que a*e= e*a= a. En particular, 1 es el elemento neutro ∈ A, ya que 0*1= 1*0= 0, 1*1= 1*1= 1, 2*1= 1*2= 2, 3*1= 1*3= 3.

Inversos: Un elemento a ∈ A tiene inverso si existe a´ ∈ A tal que a*a´= a´*a= e. En particular, esto sólo se cumple para 1 (cuyo inverso es 1 ∈ A) y 3 (cuyo inverso es 3 ∈ A), ya que 1*1=1*1= 1 y 3*3= 3*3= 1, por lo que no existe inverso para todo a ∈ A.

Ejercicio 2.

Demostrar que:

(a) *Dado M= {m ∈ ℕ: m > 0}, (M, +) es un semigrupo pero no es un monoide.*

Cerradura: Para cada a, b ∈ M, a + b ∈ M.

Asociatividad La operación + en M es asociativa porque se cumple que, para cada a, b, c ∈ M, (a + b) + c= a + (b + c) (por asociatividad en ℕ).

Elemento neutro: No existe un elemento e ∈ M tal que, para todo m ∈ M, se cumple que m + e= e + m= m. En particular, 0 es el elemento neutro ∈ ℕ pero ∉ M.

Por lo tanto, queda demostrado que (M, +) es un semigrupo pero no es un monoide.

(b) *El conjunto de un solo elemento M= {e} con la operación definida por e*e= e es un monoide.*

Cerradura: Para cada a, b ∈ M, a*b ∈ M. En particular, considerando que e es el único elemento posible, e*e= e ∈ M.

Asociatividad: La operación * en M es asociativa porque se cumple que, para cada a, b, c ∈ M, (a*b)*c= a*(b*c). En particular, considerando que e es el único elemento posible, (e*e)*e= e*(e*e) ⟺ e*e= e*e ⟺ e= e.

Elemento neutro: Existe un elemento e ∈ M tal que, para todo a ∈ M, se cumple que a*e= e*a= a. En particular, considerando que e es el único elemento posible, e es el elemento neutro ∈ M, ya que e*e= e*e= e.

Por lo tanto, queda demostrado que (M, *) es un monoide.

(c) *Dado un conjunto no vacío A, el conjunto de las partes de A, P (A), con la operación intersección de conjuntos es un monoide conmutativo.*

Cerradura: Para cada X, Y ∈ P (A), X ∩ Y ∈ P (A).

Asociatividad: La operación ∩ en P (A) es asociativa porque se cumple que, para cada X, Y, Z ∈ P (A), (X ∩ Y) ∩ Z= X ∩ (Y ∩ Z) (por asociatividad de ∩ en conjuntos).

Elemento neutro: Existe un elemento E ∈ P (A) tal que, para todo X ∈ P (A), se cumple que X ∩ E= E ∩ X= X. En particular, A es el elemento neutro ∈ P (A), ya que X ∩ A= A ∩ X= X.

Conmutatividad: La operación ∩ en P (A) es conmutativa porque se cumple que, para cada X, Y ∈ P (A), X ∩ Y= Y ∩ X (por conmutatividad de ∩ en conjuntos).

Por lo tanto, queda demostrado que (M, *) es un monoide conmutativo.

Ejercicio 3.

Demostrar que, si, para una operación asociativa $*$ en A, existe un elemento neutro e y un elemento del conjunto, a, tiene inverso, entonces, éste es único.

Se supone que b y c son dos inversos de a en A, lo que significa que:

a*b= b*a= e.
a*c= c*a= e.

Se quiere probar que b= c.

Se considera el siguiente producto:

b= b*e.

Sustituyendo e por a*c, se tiene:

b= b*(a*c).

Usando la propiedad asociativa, se tiene:

b= (b*a)*c.

Usando que b es un inverso de a, se tiene:

b= e*c.

Usando la propiedad del neutro, se tiene:

b= c.

Por lo tanto, queda demostrado que, cuando la operación es asociativa y existe un elemento neutro, el inverso de a es único.

Ejercicio 4.

Sea R una relación de congruencia sobre un semigrupo (S, ∗), demostrar que (S/R, ⊗) (el conjunto cociente y la operación inducida por ∗ sobre las clases de equivalencia) es un semigrupo llamado Semigrupo Cociente.

Dado que R es una relación de congruencia sobre un semigrupo (S, *), se tiene que:

- R es una relación de equivalencia, es decir, es reflexiva, simétrica y transitiva; y
- Si aRb y cRd, entonces, (a*c)R(b*d).

Se define el conjunto cociente S/R como el conjunto de clases de equivalencia de S bajo la relación R como:

S/R= {[a]: a ∈ S}, donde [a]= {x ∈ S: xRa} es la clase de equivalencia de a bajo R.

Para cada [a], [b] ∈ S/R, se define la operación ⊗ en S/R como:

[a] ⊗ [b]= [a*b].

Esto es posible porque R es una relación de congruencia y, por lo tanto, la clase de equivalencia de a*b depende sólo de las clases de equivalencia de a y b, independientemente de los representantes que se elijan en cada clase.

<u>Cerradura:</u> Para que la operación ⊗ sea cerrada en S/R, se necesita que el resultado de [a] ⊗ [b] sólo dependa de las clases de equivalencia de a y b, y no de los representantes específicos seleccionados de estas clases. Es decir, si se toman otros elementos c ∈ [a] y d ∈ [b] tales que cRa y dRb, se quiere que [a*b]= [c*d]. Dado que R es una relación de congruencia, si aRc y bRd, entonces, (a*b)R(c*d), lo que implica que [a*b]= [c*d].

<u>Asociatividad:</u> Como (S, *) es un semigrupo, se sabe que la operación * en S es asociativa, es decir, se cumple que, para cada a, b, c ∈ S, (a*b)*c= a*(b*c). La operación ⊗ en S/R es asociativa porque se cumple que, para cada [a], [b], [c] ∈ S/R, ([a] ⊗ [b]) ⊗ [c]= [a] ⊗ ([b] ⊗ [c]) ⟺ [a*b] ⊗ [c]= [a] ⊗ [b*c] ⟺ [(a*b)*c]= [a*(b*c)] (por ser (S, *) un semigrupo).

Por lo tanto, queda demostrado que (S/R, ⊗) es un semigrupo (Semigrupo Cociente).

Ejercicio 5.

Analizar si las siguientes son estructuras de grupo:

(a) *(ℤ, +), los enteros con la suma usual.*

Cerradura: Para cada a, b ∈ ℤ, a + b ∈ ℤ.

Asociatividad: La operación + en ℤ es asociativa porque se cumple que, para cada a, b, c ∈ ℤ, (a + b) + c= a + (b + c).

Elemento neutro: Existe un elemento e ∈ ℤ tal que, para todo a ∈ ℤ, se cumple que a + e= e + a= a. En particular, 0 es el elemento neutro ∈ ℤ, ya que a + 0= 0 + a= a ⟺ a= a= a.

Inversos: Un elemento a ∈ ℤ tiene inverso si existe a´ ∈ ℤ tal que a + a´= a´ + a= e. En particular, a + (-a)= (-a) + a= 0 ⟺ a - a= -a + a= 0 ⟺ 0= 0= 0, por lo que existe inverso para todo a ∈ ℤ, ya que -a ∈ ℤ.

Por lo tanto, (ℤ, +) es un grupo, ya que satisface cerradura, asociatividad, elemento neutro e inversos.

(b) *(ℤ, *), los enteros con el producto usual.*

Cerradura: Para cada a, b ∈ ℤ, a*b ∈ ℤ.

Asociatividad: La operación * en ℤ es asociativa porque se cumple que, para cada a, b, c ∈ ℤ, (a*b)*c= a*(b*c).

Elemento neutro: Existe un elemento e ∈ ℤ tal que, para todo a ∈ ℤ, se cumple que a*e= e*a= a. En particular, 1 es el elemento neutro ∈ ℤ, ya que a*1= 1*a= a ⟺ a= a= a.

Inversos: Un elemento a ∈ ℤ tiene inverso si existe a´ ∈ ℤ tal que a*a´= a´*a= e. En particular, esto sólo se cumple para 1 (cuyo inverso es 1 ∈ ℤ) y -1 (cuyo inverso es -1 ∈ ℤ), ya que 1*1=1*1= 1 y (-1) (-1)= (-1) (-1)= 1, por lo que no existe inverso para todo a ∈ ℤ.

Por lo tanto, (ℤ, +) no es un grupo, ya que satisface cerradura, asociatividad y elemento neutro, pero no satisface inversos.

(c) *($\mathbb{R}^2$, +), los pares ordenados de reales con la suma usual.*

Cerradura: Para cada (a_1, b_1), (a_2, b_2) ∈ $\mathbb{R}^2$, (a_1, b_1) + (a_2, b_2)= (a_1+a_2, b_1+b_2) ∈ $\mathbb{R}^2$.

Asociatividad: La operación + en $\mathbb{R}^2$ es asociativa porque se cumple que, para cada (a_1, b_1), (a_2, b_2), (a_3, b_3) ∈ $\mathbb{R}^2$, [(a_1, b_1) + (a_2, b_2)] + (a_3, b_3)= (a_1, b_1) + [(a_2, b_2) + $(a_3,$

b_3)]. En particular, (a_1+a_2, b_1+b_2) + (a_3, b_3)= (a_1, b_1) + (a_2+a_3, b_2+b_3) ⟺ (a_1+a_2+a_3, b_1+b_2+b_3)= (a_1+a_2+a_3, b_1+b_2+b_3).

Elemento neutro: Existe un elemento (e_1, e_2) ∈ $\mathbb{R}^2$ tal que, para todo (a, b) ∈ $\mathbb{R}^2$, se cumple que (a, b) + (e_1, e_2)= (e_1, e_2) + (a, b)= (a, b). En particular, (0, 0) es el elemento neutro ∈ $\mathbb{R}^2$, ya que (a, b) + (0, 0)= (0, 0) + (a, b)= (a, b) ⟺ (a+0, b+0)= (0+a, 0+b)= (a, b) ⟺ (a, b)= (a, b)= (a, b).

Inversos: Un elemento (a, b) ∈ $\mathbb{R}^2$ tiene inverso si existe (a´, b´) ∈ $\mathbb{R}^2$ tal que (a, b) + (a´, b´)= (a´, b´) + (a, b)= (e_1, e_2). En particular, (a, b) + (-a, -b)= (-a, -b) + (a, b)= (0, 0) ⟺ (a-b, b-b)= (-a+a, -b+b)= (0, 0) ⟺ (0, 0)= (0, 0)= (0, 0), por lo que existe inverso para todo (a, b) ∈ $\mathbb{R}^2$, ya que (-a, -b) ∈ $\mathbb{R}^2$.

Por lo tanto, ($\mathbb{R}^2$, +) es un grupo, ya que satisface cerradura, asociatividad, elemento neutro e inversos.

(d) *(M_{2x2}, +), las matrices de 2x2 con la suma usual de matrices.*

Cerradura: Para cada A, B ∈ M_{2x2}, A + B ∈ M_{2x2}. En particular, para A= $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ ∈ M_{2x2}, B= $\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ ∈ M_{2x2}, con cualesquiera a_{ij}, b_{ij} ∈ ℝ, i, j= 1, 2, A + B= $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ + $\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$= $\begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$, por lo que A + B ∈ M_{2x2}.

Asociatividad: La operación + en M_{2x2} es asociativa porque se cumple que, para cada A, B, C ∈ M_{2x2}, (A + B) + C= A + (B + C). En particular, para A= $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, B= $\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$, C= $\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$ ∈ M_{2x2}, con cualesquiera a_{ij}, b_{ij}, c_{ij} ∈ ℝ, i, j= 1, 2,
(A + B) + C= A + (B + C) ⟺
$(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}) + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + (\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$ ⟺
$\begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11}+c_{11} & b_{12}+c_{12} \\ b_{21}+c_{21} & b_{22}+c_{22} \end{pmatrix}$ ⟺
$\begin{pmatrix} a_{11}+b_{11}+c_{11} & a_{12}+b_{12}+c_{12} \\ a_{21}+b_{21}+c_{21} & a_{22}+b_{22}+c_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11}+c_{11} & a_{12}+b_{12}+c_{12} \\ a_{21}+b_{21}+c_{21} & a_{22}+b_{22}+c_{22} \end{pmatrix}$.

Elemento neutro: Existe un elemento E ∈ M_{2x2} tal que, para todo A ∈ M_{2x2}, se cumple que A + E= E + A= A. En particular, $0_{M_{2x2}}$= $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ es el elemento neutro ∈ M_{2x2}, ya que, para A= $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ ∈ M_{2x2}, con cualesquiera a_{ij} ∈ ℝ, i, j= 1, 2,
A + $0_{M_{2x2}}$= $0_{M_{2x2}}$ + A= A ⟺
$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ ⟺
$\begin{pmatrix} a_{11}+0 & a_{12}+0 \\ a_{21}+0 & a_{22}+0 \end{pmatrix} = \begin{pmatrix} 0+a_{11} & 0+a_{12} \\ 0+a_{21} & 0+a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ ⟺
$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$.

Inversos: Un elemento A $\in M_{2x2}$ tiene inverso si existe A´ $\in M_{2x2}$ tal que A + A´= A´ + A= E. En particular, para A= $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_{2x2}$, con cualesquiera $a_{ij} \in \mathbb{R}$, i, j= 1, 2, A + (-A)= (-A) + A= $0_{M_{2x2}} \Leftrightarrow$
$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Leftrightarrow$
$\begin{pmatrix} a_{11} - a_{11} & a_{12} - a_{12} \\ a_{21} - a_{21} & a_{22} - a_{22} \end{pmatrix} = \begin{pmatrix} -a_{11} + a_{11} & -a_{12} + a_{12} \\ -a_{21} + a_{21} & -a_{22} + a_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Leftrightarrow$
$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, por lo que existe inverso para todo A $\in M_{2x2}$, ya que -A $\in M_{2x2}$.

Por lo tanto, ($\mathbb{R}^2$, +) es un grupo, ya que satisface cerradura, asociatividad, elemento neutro e inversos.

(e) *(P (A), ∪), A cualquier conjunto y P (A) indica el conjunto de partes de A.*

Cerradura: Para cada X, Y ∈ P (A), X ∪ Y ∈ P (A).

Asociatividad: La operación ∪ en P (A) es asociativa porque se cumple que, para cada X, Y, Z ∈ P (A), (X ∪ Y) ∪ Z= X ∪ (Y ∪ Z) (por asociatividad de ∪ en conjuntos).

Elemento neutro: Existe un elemento E ∈ P (A) tal que, para todo X ∈ P (A), se cumple que X ∪ E= E ∪ X= X. En particular, ∅ es el elemento neutro ∈ P (A), ya que X ∪ ∅= ∅ ∪ X= X ⇔ X= X= X.

Inversos: Un elemento X ∈ P (A) tiene inverso si existe X´ ∈ P (A) tal que X ∪ X´= X´ ∪ X= E. En particular, esto sólo se cumple para ∅ (cuyo inverso es ∅ ∈ P (A)), ya que ∅ ∪ ∅= ∅ ∪ ∅= ∅ ⇔ ∅= ∅= ∅, por lo que no existe inverso para todo X ∈ P (A).

Por lo tanto, (P (A), ∪) no es un grupo, ya que satisface cerradura, asociatividad y elemento neutro, pero no satisface inversos.

Ejercicio 6.

Probar que, en todo grupo, el único elemento idempotente es el neutro.

Dado un grupo G con una operación *, se dice que un elemento e ∈ G es idempotente si cumple que:

$e*e= e$.

Se quiere probar que el único elemento idempotente es el elemento neutro.

Sea G un grupo con elemento neutro e, es decir, e ∈ G tal que, para todo a ∈ G, se cumple que $a*e= e*a= a$.

Se supone que a ∈ G es un elemento idempotente, es decir, cumple que:

$a*a= a$.

Se quiere probar que $a= e$, el elemento neutro.

Pre-multiplicando a ambos lados de la ecuación anterior por el inverso de a (en un grupo, cada elemento tiene inverso), se tiene:

$a'*(a*a)= a'*a$.

Usando la propiedad asociativa (en un grupo, la operación es asociativa), se tiene:

$(a'*a)*a= a'*a$.

Usando la propiedad de inversos (en un grupo, cada elemento tiene inverso), se tiene:

$e*a= e$.

Usando la propiedad del elemento neutro (en un grupo, existe elemento neutro para la operación), se tiene:

$a= e$.

Por lo tanto, queda demostrado que, en todo grupo, el único elemento idempotente es el neutro.

Ejercicio 7.

Mostrar que, en todo grupo, vale la propiedad cancelativa.

Dado un grupo G con una operación *, la propiedad cancelativa establece que:

- Por la izquierda: Si a*b= a*c, entonces, b= c, para cada a, b, c ∈ G.
- Por la derecha: Si b*a= c*a, entonces, b= c, para cada a, b, c ∈ G.

Por la izquierda:

Se supone que, en el grupo G, se cumple que:

a*b= a*c, para algunos a, b, c ∈ G.

Se quiere probar que b= c.

Pre-multiplicando a ambos lados de la ecuación anterior por el inverso de a (en un grupo, cada elemento tiene inverso), se tiene:

a´*(a*b)= a´*(a*c).

Usando la propiedad asociativa (en un grupo, la operación es asociativa), se tiene:

(a´*a)*b= (a´*a)*c.

Usando la propiedad de inversos (en un grupo, cada elemento tiene inverso), se tiene:

e*b= e*c.

Usando la propiedad del elemento neutro (en un grupo, existe elemento neutro para la operación), se tiene:

b= c.

Por lo tanto, queda demostrado que, si a*b= a*c, entonces, b= c, para cada a, b, c ∈ G.

Por la derecha:

Se supone que, en el grupo G, se cumple que:

b*a= c*a, para algunos a, b, c ∈ G.

Se quiere probar que b= c.

Post-multiplicando a ambos lados de la ecuación anterior por el inverso de a (en un grupo, cada elemento tiene su inverso), se tiene:

(b*a)*a´= (c*a)*a´.

Usando la propiedad asociativa (en un grupo, la operación es asociativa), se tiene:

b*(a*a´)= c*(a*a´).

Usando la propiedad de inversos (en un grupo, cada elemento tiene inverso), se tiene:

b*e= c*e.

Usando la propiedad del elemento neutro (en un grupo, existe elemento neutro para la operación), se tiene:

b= c.

Por lo tanto, queda demostrado que, si b*a= c*a, entonces, b= c, para cada a, b, c $\in$ G.

Por lo tanto, queda demostrado que, en todo grupo, vale la propiedad cancelativa.

Ejercicio 8.

*Sea (G, *) un grupo tal que todo elemento es su propio inverso, probar que G es abeliano.*

Dado que, en (G, *), todo elemento es su propio inverso, para todo a ∈ G, se cumple que:

a*a= e.

Se quiere probar que la operación * en G es conmutativa, es decir, que se cumple que, para cada a, b ∈ G, a*b= b*a.

Se considera el siguiente producto:

(a*b)*(a*b).

Usando que todo elemento en (G, *) es su propio inverso, se tiene:

(a*b)*(a*b)= e.

Usando la propiedad asociativa (en un grupo, la operación es asociativa), se tiene:

a*(b*a)*b= e.

Pre-multiplicando por el inverso de a (a´= a) y post-multiplicando por el inverso de b (b´= b) a ambos lados de la ecuación (en un grupo, cada elemento tiene su inverso), se tiene:

a*a*(b*a)*b*b= a*e*b.

Usando la propiedad de inversos (en un grupo, cada elemento tiene inverso), se tiene:

e*(b*a)*e= a*e*b.

Usando la propiedad del elemento neutro (en un grupo, existe elemento neutro para la operación), se tiene:

b*a= a*b.

Por lo tanto, queda demostrado que, dado (G, *) un grupo tal que todo elemento es su propio inverso, G es abeliano.

Ejercicio 9.

*Dado un grupo (G, *), probar que G es abeliano si y sólo si, para cualquier x, y en G, vale que* $(x * y)^2 = x^2 * y^2$.

Dado un grupo (G, *), si G es abeliano, entonces, para cada x, y ∈ G, x*y= y*x, lo que implica que $(x * y)^2$= (x*y)*(x*y)= x*(y*x)*y (por asociatividad)= x*(x*y)*y (por conmutatividad)= (x*x)*(y*y) (por asociatividad)= $x^2 * y^2$. Por lo tanto, dado un grupo (G, *), si G es abeliano, entonces, para cada x, y ∈ G, $(x * y)^2 = x^2 * y^2$.

Dado un grupo (G, *), si, para cada x, y ∈ G, $(x * y)^2 = x^2 * y^2$, entonces, (x*y)*(x*y)= $x^2 * y^2$, lo que implica que x´*(x*y)*(x*y)*y´= x´*(x*x)*(y*y)*y´ (pre-multiplicando por x´ y post-multiplicando por y´) ⟺ (x´*x)*(y*x)*(y*y´)= (x´*x)*(x*y)*(y*y´) (por asociatividad) ⟺ e*(y*x)*e= e*(x*y)*e (por inversos) ⟺ y*x= x*y (por elemento neutro). Por lo tanto, dado un grupo (G, *), si, para cada x, y ∈ G, $(x * y)^2 = x^2 * y^2$, entonces, G es abeliano.

Por lo tanto, queda demostrado que, dado un grupo (G, *), G es abeliano si y sólo si, para cada x, y ∈ G, $(x * y)^2 = x^2 * y^2$.

Ejercicio 10.

*Dados los grupos (G, *) y (F, ⊓), se define, en el conjunto GxF, la ley ∘ tal que (x, y)∘(z, t)= (x*z, y⊓t). Probar que (GxF, ∘) es Grupo (Grupo Producto).*

Cerradura: Para cada (x, y), (z, t) ∈ GxF, (x*z, y⊓t) ∈ GxF, ya que x*z ∈ G y y⊓t ∈ F (por (G, *) y (F, ⊓) grupos).

Asociatividad: La operación ∘ en GxF es asociativa porque se cumple que, para cada (x, y), (z, t), (u, v) ∈ GxF, ((x, y)∘(z, t))∘(u, v)= (x, y)∘((z, t)∘(u, v)). En particular, (x*z, y⊓t)∘(u, v)= (x, y)∘(z*u, t⊓v) ⟺ ((x*z)*u, (y⊓t)⊓v)= (x*(z*u), y⊓(t⊓v)) (por * y ⊓ asociativas en G y F, respectivamente).

Elemento neutro: Existe un elemento (e_1, e_2) ∈ GxF tal que, para todo (x, y) ∈ GxF, se cumple que (x, y)∘(e_1, e_2)= (e_1, e_2)∘(x, y)= (x, y). En particular, (e_G, e_F) es el elemento neutro ∈ GxF (e_G y e_F elementos neutros de G y F, respectivamente), ya que (x*e_G, y⊓ e_F)= (e_G*x, e_F ⊓y)= (x, y) ⟺ (x, y)= (x, y)= (x, y).

Inversos: Un elemento (x, y) ∈ GxF tiene inverso si existe (x´, y´) ∈ GxF tal que (x, y)∘(x´, y´)= (x´, y´)∘(x, y)= (e_1, e_2). En particular, dado que existe inverso x´ ∈ G (y´ ∈ F) para cada x ∈ G (y ∈ F) (por (G, *) y (F, ⊓) grupos), (x, y)∘(x´, y´)= (x´, y´)∘(x, y)= (e_G, e_F) ⟺ (x*x´, y⊓y´)= (x´*x, y´⊓y)= (e_G, e_F) ⟺ (e_G, e_F)= (e_G, e_F)= (e_G, e_F), por lo que existe inverso para todo (x, y) ∈ GxF, ya que (x´, y´) ∈ GxF.

Por lo tanto, queda demostrado que (GxF, ∘) es un grupo (Grupo Producto), ya que satisface cerradura, asociatividad, elemento neutro e inversos.

Ejercicio 11.

Estudiar si son subgrupos de los grupos indicados:

(a) *Los enteros pares de ($\mathbb{Z}$, +).*

$\mathbb{Z}_2$= {x ∈ $\mathbb{Z}$: x= 2k, k ∈ $\mathbb{Z}$}.
$\mathbb{Z}_2 \subset \mathbb{Z}$.

Cerradura: Para cada a, b ∈ $\mathbb{Z}_2$, a + b ∈ $\mathbb{Z}_2$. En particular, para a= 2m y b= 2n, con cualesquiera m, n ∈ $\mathbb{Z}$, a + b= 2m + 2n= 2 (m + n), con m + n ∈ $\mathbb{Z}$, por lo que a + b ∈ $\mathbb{Z}_2$.

Asociatividad: La operación + en $\mathbb{Z}_2$ es asociativa porque se hereda del grupo original ($\mathbb{Z}$, +).

Elemento neutro: El elemento neutro de + en $\mathbb{Z}$ también existe en $\mathbb{Z}_2$. En particular, 0 ∈ $\mathbb{Z}_2$, ya que 0= 2 * 0, con k= 0 ∈ $\mathbb{Z}$.

Inversos: Un elemento a ∈ $\mathbb{Z}_2$ tiene inverso si existe a´ ∈ $\mathbb{Z}_2$ tal que a + a´= a´ + a= e. En particular, para a= 2k ∈ $\mathbb{Z}_2$, con cualquier k ∈ $\mathbb{Z}$, su inverso en $\mathbb{Z}$ es a´= -a= -2k= 2 (-k), con -k ∈ $\mathbb{Z}$, por lo que existe inverso para todo a ∈ $\mathbb{Z}_2$, ya que a´ ∈ $\mathbb{Z}_2$.

Por lo tanto, ($\mathbb{Z}_2$, +) es un subgrupo del grupo ($\mathbb{Z}$, +), ya que satisface cerradura, elemento neutro e inversos.

(b) *Las matrices simétricas de 2x2.*

S_{2x2}= {$\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}$: a_{ij} ∈ $\mathbb{R}$, i, j= 1, 2}.
$S_{2x2} \subset M_{2x2}$.

Cerradura: Para cada A, B ∈ S_{2x2}, A + B ∈ S_{2x2}. En particular, para A= $\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}$, B= $\begin{pmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{pmatrix}$ ∈ S_{2x2}, con cualesquiera a_{ij}, b_{ij} ∈ $\mathbb{R}$, i, j= 1, 2, A + B= $\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}$ + $\begin{pmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{pmatrix}$= $\begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{12}+b_{12} & a_{22}+b_{22} \end{pmatrix}$, por lo que A + B ∈ S_{2x2}.

Asociatividad: La operación + en S_{2x2} es asociativa porque se hereda del grupo original (M_{2x2}, +).

Elemento neutro: El elemento neutro de + en M_{2x2} también existe en S_{2x2}. En particular, $0_{M_{2x2}}$= $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ∈ S_{2x2}, ya que a_{12}= a_{21}= 0.

Inversos: Un elemento A ∈ S_{2x2} tiene inverso si existe A´ ∈ S_{2x2} tal que A + A´= A´ + A= E. En particular, para A= $\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}$ ∈ S_{2x2}, con cualesquiera a_{ij} ∈ $\mathbb{R}$, i, j= 1, 2, su inverso en M_{2x2} es A´= -A= $\begin{pmatrix} -a_{11} & -a_{12} \\ -a_{12} & -a_{22} \end{pmatrix}$, por lo que existe inverso para todo A $\in$ S_{2x2}, ya que A´ $\in S_{2x2}$.

Por lo tanto, (S_{2x2}, +) es un subgrupo del grupo (M_{2x2}, +), ya que satisface cerradura, elemento neutro e inversos.

<u>Ejercicio 12.</u>

*Demostrar que, si H y K son subgrupos de (G, *), entonces, H ∩ K es un subgrupo de (G, *).*

H ∩ K= {a ∈ G: a ∈ H ∧ a ∈ K}.
H ∩ K ⊂ G.

<u>Cerradura:</u> Para cada a, b ∈ H ∩ K, a*b ∈ H ∩ K, ya que a, b ∈ H, a, b ∈ K y a*b ∈ H, a*b ∈ K (por (H, *) y (K, *) subgrupos).

<u>Asociatividad:</u> La operación * en H ∩ K es asociativa porque se hereda del grupo original (G, *).

<u>Elemento neutro:</u> El elemento neutro de * en G también existe en H ∩ K. En particular, e ∈ H ∩ K, ya que e ∈ H y e ∈ K (por (H, *) y (K, *) subgrupos de G, con elemento neutro e).

<u>Inversos:</u> Un elemento a ∈ H ∩ K tiene inverso si existe a´ ∈ H ∩ K tal que a*a´= a´*a= e. En particular, para cada a ∈ H ∩ K, a ∈ H y a ∈ K y, además, a´ ∈ H y a´ ∈ K (por (H, *) y (K, *) subgrupos), por lo que existe inverso para todo a ∈ H ∩ K, ya que a´ ∈ H ∩ K.

Por lo tanto, queda demostrado que (H ∩ K, *) es un subgrupo del grupo (G, *), ya que satisface cerradura, elemento neutro e inversos.

Ejercicio 13.

*Sea (G, *) un grupo, sea $a \in G$ y sea H un subgrupo de G. Demostrar que el conjunto aHa^{+1}= {$a*h*a^{-1}$: $h \in H$} es un subgrupo de G.*

aHa^{+1}= {$a*h*a^{-1}$: $h \in H$}.
$aHa^{+1} \subset G$.

Elemento neutro: El elemento neutro de * en G también existe en aHa^{+1}. En particular, $e \in aHa^{+1}$, ya que $e \in H$ (por (H, *) subgrupo de G, con elemento neutro e), lo que implica que aea^{-1}= aa^{-1} (por (G, *) grupo)= e (por (G, *) grupo).

Asociatividad: La operación * en aHa^{+1} es asociativa porque se hereda del grupo original (G, *).

Cerradura: Para cada x, $y \in aHa^{+1}$, $x*y \in aHa^{+1}$. En particular, para x= $ah_1a^{-1} \in aHa^{+1}$ e y= $ah_2a^{-1} \in aHa^{+1}$, con cualesquiera h_1, $h_2 \in H$, x*y= $(ah_1a^{-1})*(ah_2a^{-1})$= $ah_1(a^{-1}a)h_2a^{-1}$ (por asociatividad)= $ah_1eh_2a^{-1}$ (por (G, *) grupo)= $ah_1h_2a^{-1}$ (por elemento neutro), con $h_1*h_2 \in H$ (por (H, *) subgrupo), por lo que $x*y \in aHa^{+1}$.

Inversos: Un elemento $x \in aHa^{+1}$ tiene inverso si existe $x' \in aHa^{+1}$ tal que $x*x'= x'*x$= e. En particular, para x= $aha^{-1} \in aHa^{+1}$, con cualquier $h \in H$, su inverso en G es x'= $(aha^{-1})^{-1}$= $(a^{-1})^{-1}h^{-1}a^{-1}$= $ah^{-1}a^{-1}$ (por (G, *) grupo), con $h^{-1} \in H$ (por (H, *) subgrupo), por lo que existe inverso para todo $x \in aHa^{+1}$, ya que $x' \in aHa^{+1}$.

Por lo tanto, queda demostrado que el conjunto aHa^{+1}= {$a*h*a^{-1}$: $h \in H$} es un subgrupo de G, ya que satisface cerradura, elemento neutro e inversos.

Ejercicio 14.

Probar que todo grupo cíclico es abeliano.

Sea (G, *) un grupo cíclico con generador g ∈ G, es decir:

G= $\langle g \rangle$= $\{g^n$: n ∈ $\mathbb{Z}\}$.

Esto significa que cualquier elemento de G se puede expresar como una potencia de g.

Se quiere probar que la operación * en G es conmutativa, es decir, que se cumple que, para cada a, b ∈ G, a*b= b*a.

Sean a, b ∈ G. Dado que G es cíclico, se tiene:

a= g^n, con n ∈ $\mathbb{Z}$.
b= g^m, con m ∈ $\mathbb{Z}$.

Considerando las operaciones a*b y b*a, se tiene:

a*b= $g^n * g^m$= g^{n+m}.
b*a= $g^m * g^n$= g^{m+n}.

Dado que g^{n+m}= g^{m+n}, se tiene:

a*b= b*a.

Por lo tanto, queda demostrado que todo grupo cíclico es abeliano.

Ejercicio 15.

Sea G un grupo cíclico de orden n, si m es divisor de n, entonces, el elemento a^m y sus potencias generan un subgrupo.

Sea G un grupo cíclico de orden n con generador a $\in$ G, es decir:

G= $\langle a \rangle$= $\{a^x$: x $\in \mathbb{Z}$, 0 $\leq$ x $<$ n$\}$= $\{$e, a, a^2, … , $a^{n-1}\}$.

Esto implica que a^n= e, donde e es el elemento neutro de G.

Se supone que m es divisor de n, lo cual implica que existe un entero k tal que n= mk.

Se quiere probar que el elemento a^m y sus potencias generan un subgrupo de G.

Sea H el conjunto que contiene todas las potencias de a^m, es decir:

H= $\langle a^m \rangle$= $\{(a^m)^y$: y $\in \mathbb{Z}\}$
H= $\langle a^m \rangle$= $\{a^{my}$: y $\in \mathbb{Z}\}$.

Si a^{my}= e para algún y $\in \mathbb{Z}$, entonces, a^{my}= a^n= e, lo que implica que my es múltiplo de n y, como mk también lo es, se tiene:

my= mk
y= k.

Esto muestra que el menor entero positivo y para el cual a^{my}= e es y= k, por lo que el orden de a^m es k.

Entonces, H tiene, exactamente, k= $\frac{n}{m}$ ($<$ n) elementos:

H= $\langle a^m \rangle$= $\{a^{my}$: y $\in \mathbb{Z}$, 0 $\leq$ y $<$ k= $\frac{n}{m}$ $<$ n$\}$.
H $\subset$ G.

<u>Cerradura:</u> Para cada a, b $\in$ H, a*b $\in$ H. En particular, para a= a^{mx} $\in$ H y b= a^{my} $\in$ H, con cualesquiera x, y $\in \mathbb{Z}$, a*b= $a^{mx}*a^{my}$= a^{mx+my}= $a^{m(x+y)}$, con x + y $\in \mathbb{Z}$, por lo que a*b $\in$ H.

<u>Asociatividad:</u> La operación * en H es asociativa porque se hereda del grupo original (G, *).

<u>Elemento neutro:</u> El elemento neutro de * en G también existe en H. En particular, e $\in$ H, ya que a^{m*0}= a^0= e, con y= 0 $\in \mathbb{Z}$.

<u>Inversos:</u> Un elemento a $\in$ H tiene inverso si existe a´ $\in$ H tal que a*a´= a´*a= e. En particular, para a= a^{my} $\in$ H, con cualquier y $\in \mathbb{Z}$, su inverso en G es a´= $(a^{my})^{-1}$= a^{-my}= $a^{m(-y)}$, con -y $\in \mathbb{Z}$, por lo que existe inverso para todo a $\in$ H, ya que a´ $\in$ H.

Por lo tanto, queda demostrado que, dado un grupo cíclico G de orden n, si m es divisor de n, entonces, el elemento a^m y sus potencias generan un subgrupo de G, ya que el conjunto formado por estos elementos (H) satisface cerradura, elemento neutro e inversos.

Ejercicio 16.

*Sea (G, *) un grupo, sea a ∈ G y sea H un subgrupo de G. Si a, b ∈ G, probar que la relación dada por a≡ b (mod H) si a*b^{-1} ∈ H es una relación de equivalencia.*

$\equiv_H$ es reflexiva porque se cumple que, para todo a ∈ G, (a, a) ∈ $\equiv_H$. En particular, aa^{-1}= e ∈ H (por (H, *) subgrupo de G, con elemento neutro e), lo que implica que (a, a) ∈ $\equiv_H$.

$\equiv_H$ es simétrica porque se cumple que, para cada a, b ∈ G, si (a, b) ∈ $\equiv_H$, entonces, (b, a) ∈ $\equiv_H$. En particular, si ab^{-1} ∈ H, entonces, $(ab^{-1})^{-1}$ ∈ H (por (H, *) subgrupo) y es igual a $(b^{-1})^{-1}a^{-1}$= ba^{-1}, lo que implica que, si (a, b) ∈ $\equiv_H$, entonces, (b, a) ∈ $\equiv_H$.

$\equiv_H$ es transitiva porque se cumple que, para cada a, b, c ∈ G, si (a, b) ∈ $\equiv_H$ y (b, c) ∈ $\equiv_H$, entonces, (a, c) ∈ $\equiv_H$. En particular, si ab^{-1} ∈ H y bc^{-1} ∈ H, entonces, (ab^{-1})*(bc^{-1}) ∈ H (por cerradura) y es igual a a(b^{-1}b) c^{-1} (por asociatividad)= aec^{-1} (por inversos)= ac^{-1} (por elemento neutro), lo que implica que, si (a, b) ∈ $\equiv_H$ y (b, c) ∈ $\equiv_H$, entonces, (a, c) ∈ $\equiv_H$.

Por lo tanto, queda demostrado que la relación dada por a≡ b (mod H) si a*b^{-1} ∈ H es una relación de equivalencia, ya que es reflexiva, simétrica y transitiva.