TP 5 - Estructuras Algebraicas - Teoría de Grupos

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

Que una operación este bien definida para cierto conjunto A, significa que para cualquier $a, b \in A$ la aplicación de la operación entre los dos elementos, es decir, $a * b$ sea cerrada (el resultado este en el mismo conjunto).

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

La operación está bien definida, ya que no existe ningún $a, b \in \mathbb{N}$ tal que $3ab \notin \mathbb{N}$.

- Disclaimer: Si es que incluimos al 0 en el conjunto de los números naturales.

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

La operación NO está bien definida, ya que existen $a, b \in \mathbb{Z} : \frac{a+b}{3+ab} \notin \mathbb{Z}$

- Por ejemplo: Si $a = 1$ y $b = 2$

$$\frac{1+2}{3+2.1} = \frac{3}{5}$$

  - Sabemos que $\frac{3}{5} \notin \mathbb{Z}, \therefore *$ no está bien definida para el conjunto A.

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

La operación está bien definida, ya que no existe ningún $x, y \in \mathbb{R} : x + y - xy \notin \mathbb{R}$.

(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

La operación está bien definida, ya que no hay ningún elemento en A que haga que $a * b \notin A$.

▼ 2. Demostrar que:

(a) Dado $M = \{m \in \mathbb{N} : m > 0\}, (M, +)$ es un semigrupo pero no es un monoide

- $(M, +)$ es un semigrupo si está bien definido y si es asociativa.
- $(M, +)$ es un monoide si está bien definida, es asociativa y tiene neutro.

Suponiendo que el $+$ se refiere a la suma de dos números:

- Podemos ver que $(M, +)$ está bien definida, ya que para cualquier $a, b \in M$ se cumple que $a + b \in M$.
- También vemos que $(M, +)$ es asociativa, para cualquier $a, b, c \in M$ se cumple que $a + (b + c) = (a + b) + c$.
- Sabemos que el elemento neutro de los naturales es el 0, al excluirlo del conjunto M vamos a ver que no existe un $e \in M : a + e = a, \therefore M$ NO tiene elemento neutro, es decir, no es monoide.

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

Para que M sea un monoide, debe estar bien definida (cerrada), ser asociativa y contar con elemento neutro.

- Sabemos que M tiene un solo elemento, la operación $*$ está definida como $e * e = e$, vemos que el resultado, e, pertenece al conjunto M, por lo que está bien definida.
- Para que $(M, *)$ sea asociativa, hay que comprobar que para cualquier $a, b, c \in M$, se cumple que $(a * b) * c = a * (b * c)$, es decir, $(e * e) * e = e * (e * e)$.

$$(e * e) * e = e * e = e$$
$$e * (e * e) = e * e = e$$

  - Vemos que de ambas formas se obtiene e, por lo tanto, la operación es asociativa en el conjunto M.
- Para que e sea el elemento neutro de $(M, *)$, se tiene que cumplir que $e * e = e$, por el enunciado, vemos que eso se cumple, por lo tanto $(M, *)$ tiene como elemento neutro a e.

(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

Para que la operación $\cap$ en el conjunto $P(A)$ (conjunto de las partes de A) sea un monoide conmutativo, debe estar bien definida, ser asociativa, tener elemento neutro y ser conmutativa.

- Recordar que el conjunto de partes $P(A)$ está formado por todos los subconjuntos de A.
- Tomando $X, Y \in P(A)$, ambos son subconjuntos de A, entonces $X \cap Y$ también será subconjunto de A, por lo tanto, $\cap$ está bien definida para $P(A)$.
  - Incluso si $X = \{1\}$ e $Y = \{2, 3\}$, la intersección nos da $\emptyset$, pero $\emptyset \in P(A)$ (CONSULTAR).
- La $\cap$ es asociativa, para todos los $X, Y, Z \in P(A)$ se cumple que:

$$(X \cap Y) \cap Z = X \cap (Y \cap Z)$$

- El elemento neutro es un elemento del conjunto tal que $X, e \in P(A) : X \cap e = X$. En este caso, podemos ver que un candidato a elemento neutro es el propio A, ya que $X \cap A = X$ (y sabemos que A es único en su conjunto de partes). Por lo tanto, el elemento neutro para la $\cap$ en $P(A)$ es A.
- Sabemos que la $\cap$ es conmutativa, para cualquier $X, Y \in P(A)$, se cumple que:

$$X \cap Y = Y \cap X$$

- Por lo tanto, al demostrar que $P(A)$ con la operación $\cap$ está bien definida, posee un elemento neutro único, es asociativa y además es conmutativa, podemos decir que es un monoide conmutativo.

▼ 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.

Esta demostración es tal cuál sacada de la teoría.

Por el enunciado, sabemos que:

- La operación $*$ en A es asociativa, o sea, $\forall x, y, z \in A : (x * y) * z = x * (y * z)$.
- Existe el elemento neutro en A para la operación $*$, es decir, $\forall x, e \in A : x * e = x$.
- Para la operación $* * a \in A$ tiene un inverso, es decir, existe un $b \in A$ tal que $a * b = b * a = e$.

Queremos demostrar que el inverso b es único, o sea, que no hay otro elemento $c \in A : a * c = c * a = e$.

- Supongamos que b y c son inversos de a, o sea:

$$a * b = b * a = e \quad y \quad a * c = c * a = e$$

- Sabemos que $b = b * e$, si sustituimos por $a * c$
  - Válido ya que $a * c = e$

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

  - Usamos la asociatividad

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

  - Reemplazamos $b * a = e$

$$b = e * c$$
$$b = c$$

- Demostramos que si b y c son inversos de a, entonces $b = c$. Por lo tanto, el inverso de un elemento, para una operación asociativa y con elemento neutro, es único.

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

CONSULTAR

Por el enunciado, sabemos que:

- S es un semigrupo con la operación $*$.
- R es una relación de congruencia sobre $(S, *)$.
- S/R es el conjunto cociente de S por R.
- $\circledast$ es la operación inducida por $*$ en S/R sobre las clases de equivalencia.

Para que $(S/R, \circledast)$ sea un semigrupo (semigrupo cociente) tiene que:

- Estar bien definida.
- Ser asociativa.

¿$(S/R, \circledast)$ está bien definida?

- Para dos clases de equivalencia $\bar{a}$ y $\bar{b}$ en S/R, la operación $\circledast$ se define como:

$$\bar{a} \circledast \bar{b} = \overline{a * b}$$

- Para que la operación este bien definida, o sea, que el resultado de $\overline{a} \circledast \overline{b} = \overline{a * b}$ no dependa de los representantes de las clases.
- Sea $a' \in \overline{a}$ y $b' \in \overline{b}$, es decir, $a' R a$ y $b' R b$.
- R es una relación de congruencia sobre $(S, *)$, lo que implica que la relación R es compatible con $*$, o sea que:

$$aRa' \quad y \quad bRb' \rightarrow a * bRa' * b'$$

- Entonces, si tomamos que $a' \in \overline{a}$ y $b' \in \overline{b}$:

$$\overline{a'} \circledast \overline{b'} = \overline{a' * b'} = \overline{a * b}$$

- Entonces, la operación $\circledast$ no depende de la elección de los representantes, o sea, que está bien definida.

¿$(S/R, \circledast)$ es asociativa?

- Para toda clase de equivalencia $\overline{a}, \overline{b}, \overline{c} \in S/R$ se tiene que dar que:

$$(\overline{a} \circledast \overline{b}) \circledast \overline{c} = \overline{a} \circledast (\overline{b} \circledast \overline{c})$$

- Analizando la igualdad:
  - Lado izquierdo:

$$(\overline{a} \circledast \overline{b}) \circledast \overline{c} = \overline{a * b} \circledast \overline{c} = \overline{(a * b) * c}$$

- Lado derecho:

$$\overline{a} \circledast (\overline{b} \circledast \overline{c}) = \overline{a} \circledast \overline{b * c} = \overline{a * (b * c)}$$

- Sabemos que $*$ es asociativa en S (por ser semigrupo). Por lo tanto tenemos:

$$\overline{(a * b) * c} = \overline{a * (b * c)}$$

- Lo que demuestra que $\circledast$ es asociativa para S/R.

Como $(S/R, \circledast)$ está bien definida y es asociativa, podemos decir que es un semigrupo.

▼ 5. Analizar si las siguientes son estructuras de grupo

Para que una operación en cierto conjunto tenga estructura de grupo, debe:

- Estar bien definida (cerrada).
- Ser asociativa.
- Tener elemento neutro.
- Cada elemento del conjunto debe tener un inverso.

(a) $(\mathbb{Z}, +)$, los enteros con la suma usual

- La suma de dos enteros es un entero, o sea, para todo $a, b \in \mathbb{Z}$ se cumple que $a + b \in \mathbb{Z}$.
- La suma de dos enteros es asociativa, es decir, para todo $a, b, c \in \mathbb{Z}$ se cumple que $(a + b) + c = a + (b + c)$.
- El elemento neutro para la suma en los números enteros es el 0 (y es único), ya que para cualquier $a \in \mathbb{Z}$ se cumple que $a + 0 = a$.
- Para cualquier $a \in \mathbb{Z}$, su inverso es $-a$, porque $a + (-a) = 0$.
- Por lo tanto $(\mathbb{Z}, +)$ tiene estructura de grupo.

(b) $(\mathbb{Z}, \cdot)$, los enteros con el producto usual

- El producto de dos enteros es un entero, o sea, para todo $a, b \in \mathbb{Z}$ se cumple que $a \cdot b \in \mathbb{Z}$.
- El producto entre dos enteros es asociativo, para todo $a, b, c \in \mathbb{Z}$ se cumple que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- El elemento neutro para el producto en los números enteros es el 1 (y es único), ya que para cualquier $a \in \mathbb{Z}$ se cumple que $a \cdot 1 = a$.
- No todos los enteros tienen inverso en la multiplicación. Solo 1 y -1 tienen inversos, ya que $1 \cdot 1 = 1$ y $-1 \cdot -1 = 1$, pero los demás enteros no tienen inverso para la multiplicación.
- Por lo tanto $(\mathbb{Z}, +)$ NO tiene estructura de grupo porque no todos los elementos tienen inverso.

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

- La suma de dos pares ordenados de números reales es otro par ordenado de números reales. Si $(x_1, y_2), (x_2, y_2) \in \mathbb{R}^2$ entonces se cumple que $(x_1 + x_2, y_1 + y_2) \in \mathbb{R}^2$.
- La suma de pares ordenados es asociativa. Para todo $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$:

  $((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = (x_1 + x_2, y_1 + y_2) + (x_3, y_3) = (x_1 + x_2 + x_3, y_1 + y_2 + y_3)$
  $(x_1, y_1) + ((x_2, y_2) + (x_3, y_3)) = (x_1, y_1) + (x_2 + x_3, y_2 + y_3) = (x_1 + x_2 + x_3, y_1 + y_2 + y_3)$
- El par $(0, 0)$ es el elemento neutro (y es único) para la suma de los pares ordenados del conjunto $\mathbb{R}^2$, ya que para cualquier $(x, y) \in \mathbb{R}^2$ se cumple que $(x, y) + (0, 0) = (x, y)$.
- Para cualquier $(x, y) \in \mathbb{R}^2$, su inverso es $(-x, -y)$, ya que $(x, y) + (-x, -y) = (0, 0)$.
- Por lo tanto $(\mathbb{R}^2, +)$ tiene estructura de grupo.

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

- La suma de dos matrices 2×2 es otra matrix 2×2.
- La suma de matrices es asociativa, para $A, B, C \in M_{2x2}$ se cumple que $(A + B) + C = A + (B + C)$.
- La matriz nula $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ es el elemento neutro para la suma de matrices 2×2, ya que para cualquier $A \in M_{2x2}$ se cumple que $A + 0 = A$.
- Para cualquier matriz $A \in M_{2x2}$: $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ su inverso es $-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ porque $A + (-A) = 0$.
- Por lo tanto $(M_{2x2}, +)$ tiene estructura de grupo.

(e) $(P(A), \cup)$, A cualquier conjunto y $P(A)$ indica el conjunto de partes de A

- La unión de dos subconjuntos de A es un subconjunto de A.
- La unión de conjuntos para $P(A)$ es asociativa. Para $X, Y, Z \subseteq A$, se cumple:

$$(X \cup Y) \cup Z = X \cup (Y \cup Z)$$

- El conjunto $\emptyset$ es el elemento neutro para la $\cup$ en $P(A)$, ya que $X \cup \emptyset = X$, para todo $X \subseteq A$.
- Se debe cumplir que para todo $X \subseteq A$ tenga un inverso, $Y \subseteq A$ tal que $X \cup Y = \emptyset$
  - Esto no se cumple, salvo que $X = \emptyset$.
  - Para todos los subconjuntos de A (que no sean $\emptyset$), la unión con otro subconjunto siempre tendrá al menos un elemento.
  - Por lo tanto, no existe un inverso para todos los $X \in P(A)$.
- Por lo tanto $(P(A), \cup)$ NO tiene estructura de grupo ya que no todos los subconjuntos tienen un inverso.

▼ 6. Probar que en todo Grupo el único elemento idempotente es el neutro

Sea G un grupo cualquiera.

- Un elemento $a \in G$ es idempotente si $a \cdot a = a$, o sea, $a^2 = a$.

Sea $e \in G$ un elemento neutro de G, es decir $a \in G, e \cdot a = a \cdot e = a$.

Supongamos que $a \in G$ es idempotente, o sea que $a \cdot a = a$. Queremos probar que $a = e$.

- La ecuación que define la idempotencia es $a \cdot a = a$.
- Como G es un grupo, todo elemento $a \in G$ tiene un inverso, tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.
  - Siendo e el elemento neutro en G.
- Multiplicamos a^{-1} en ambos lados de la ecuación.

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

- Al ser G un grupo es asociativa, entonces:

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

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

$$e \cdot a = e$$

- Como e es el elemento neutro, $e \cdot a = e$, pero tenemos que $e = a$

$$a = e$$

Por lo tanto, demostramos que si a es idempotente en un grupo, entonces $a = e$, por lo que el elemento idempotente en un grupo es el elemento neutro.

▼ 7. Mostrar que en todo grupo vale la propiedad cancelativa

La propiedad cancelativa dice que si los elementos a, b, c pertenecen a un grupo G y se tiene que

$$a * b = a * c \quad o \quad b * a = c * a$$

- Se puede cancelar a en ambos lados, y teniendo:

$$b = c$$

Sabemos que un grupo G está bien definido, es asociativo, tiene elemento neutro único y todos sus elementos tienen inverso.

Queremos probar que si $a * b = a * c$ entonces $b = c$

- Multiplicamos a^{-1} en ambos lados de la igualdad.

Ahora vamos a probar que si $b * a = c * a$ entonces $b = c$

- Multiplicamos a^{-1} en ambos lados de la ecuación.

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

- Asociatividad:

$$(a^{-1} * a) * b = (a^{-1} * a) * c$$

- $a^{-1} * a = e$ (elemento neutro)

$$e * b = e * c$$

- Como e es el elemento neutro en G

$$b = c$$

- Entonces, la cancelación se cumple por la ecuación izquierda, o sea la $a * b = a * c$

$$(b * a) * a^{-1} = (c * a) * a^{-1}$$

- Asociatividad:

$$b * (a * a^{-1}) = c * (a * a^{-1})$$

- $a * a^{-1} = e$ (elemento neutro)

$$b * e = c * e$$

- Como e es el elemento neutro en el grupo G

$$b = c$$

- Podemos ver que la cancelación se cumple en la ecuación derecha.

Por lo tanto, demostramos que la propiedad cancelativa se cumple para todo grupo.

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

Por el enunciado, sabemos que:

- G es un grupo, o sea que está bien definido, es asociativo, tiene elemento neutro único y todo elemento del grupo tiene inverso.
- Cada elemento es su propio inverso, para todo $a \in G : a * a = e$.

Queremos probar que G es abeliano, es decir, que sea conmutativo.

Sean $a, b \in G : a * a = e \land b * b = e$, queremos llegar a que $a * b = b * a$.

- Como cada elemento es su propio inverso, podemos decir que:
  - $a * b$ es su propio inverso.

$$(a * b) * (a * b) = e$$

- Asociatividad:

$$((a * b) * a) * b = e \rightarrow (a * (b * a)) * b = e$$

- Como $b * a$ es un elemento de G y todo elemento es su propio inverso:

$$a * (b * a) = b$$

- Multiplicamos a en ambos lados de la ecuación:

$$a * (a * (b * a)) = a * b$$

- Asociatividad:

$$(a * a) * (b * a) = a * b$$

- e$e = a * a$

$$e * (b * a) = a * b \rightarrow b * a = a * b$$

Se demostró que para cualquiera de los elementos de G, se cumple la conmutatividad. Por lo tanto, el grupo $(G, *)$ es abeliano.

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

G es abeliano → Para cualquier $x, y \in G$: $(x * y)^2 = x^2 * y^2$

- Que G sea abeliano significa que:
  - Está bien definido.
  - Es asociativo.
  - Tiene elemento neutro único.
  - Cada elemento tiene un inverso.
  - Es conmutativo.
- Queremos llegar a que $(x * y)^2 = x^2 * y^2$

$$(x * y)^2 = (x * y) * (x * y)$$

- Asociatividad:

$$x * (y * x) * y$$

- Conmutatividad:

$$x * (x * y) * y$$

- Asociatividad:

$$(x * x) * (y * y) = x^2 * y^2$$

Si $x, y \in G$: $(x * y)^2 = x^2 * y^2$ → G es abeliano.

- Queremos probar que $x * y = y * x$
- Vamos a partir de:

$$(x * y)^2 = x^2 * y^2 \rightarrow (x * y) * (x * y) = (x * x) * (y * y)$$

- Asociatividad:

$$x * (y * x) * y = x * x * y * y$$

- Cancelamos las x e y de los costados de cada igualdad:

$$y * x = x * y$$

- Demostramos la conmutatividad en G, por lo tanto, es abeliano.

Se probó que G es abeliano **si y sólo si** para cualquier $x, y \in G : (x * y)^2 = x^2 * y^2$.

▼ 10. Dados los Grupos $(G, *)$ y $(F, \diamond)$ se define en el conjunto $G \times F$ la ley $\cdot$ tal que $(x, y) \cdot (z, t) = (x * z, y \diamond t)$. Probar que $(G \times F, \cdot)$ es Grupo (Grupo Producto)

Sabemos que $(G, *)$ y $(F, \diamond)$ son grupos.

- Están bien definidos.
- Son asociativos.
- Tienen elemento neutro único.
- Cada elemento tiene inverso.

Queremos demostrar que $(G \times F, \cdot)$ es un grupo (grupo producto), donde $\cdot$ se define como:

$$(x, y) \cdot (z, t) = (x * z, y \diamond t)$$

¿Está bien definida?

- Sabemos que para cualquier $x, z \in G$ la operación $x * z \in G$.
- De forma trivial para $(F, \diamond)$, donde para cualquier $y, t \in F$ la operación $y \diamond t \in F$.
- Por lo tanto, para cualquier $(x, y), (z, t) \in G \times F$ el resultado $(x * z, y \diamond t) \in G \times F$.
- Entonces, podemos decir que la operación $\cdot$ está bien definida para el conjunto $G \times F$.

¿Es asociativo?

- Para todo $x, z, w \in G$ se cumple que $(x * z) * w = x * (z * w)$ y para todo $y, t, s \in F$ se cumple que $(y \diamond t) \diamond s = y \diamond (t \diamond s)$
- Para cualquier $(x, y), (z, t), (w, s) \in G \times F$

$$((x, y) \cdot (z, t)) \cdot (w, s) = (x * z, y \diamond t) \cdot (w, s) = ((x * z) * w, (y \diamond t) \diamond s)$$
$$(x, y) \cdot ((z, t) \cdot (w, s)) = (x, y) \cdot (z * w, t \diamond s) = (x * (z * w), y \diamond (t \diamond s))$$

- Como $(G, *)$ y $(F, \diamond)$ son asociativos:

$$(x * z) * w = x * (z * w)$$
$$(y \diamond t) \diamond s = y \diamond (t \diamond s)$$

- Entonces, $(G \times F, \cdot)$ es asociativo.

¿Tiene elemento neutro?

- $(G, *)$ tiene elemento neutro, e_G, tal que para todo $x \in G : x * e_G = x$.
- $(F, \diamond)$ también tiene elemento neutro, e_F, tal que para todo $y \in F : y \diamond e_F = y$.
- Sea el par $(e_G, e_F) \in G \times F$:

$$(x, y) \cdot (e_G, e_F) = (x * e_G, y \diamond e_F) = (x, y)$$

- Por lo tanto, $(G \times F, \cdot)$ tiene como elemento neutro a (e_G, e_F).

¿Cada elemento tiene su inverso?

- Para todo $x \in G$, existe un $x^{-1} \in G : x * x^{-1} = e_G$.
- Para todo $y \in F$, existe un $y^{-1} \in F : y * y^{-1} = e_F$.
- Para un elemento cualquiera $(x, y) \in G \times F$, definimos su inverso como $(x^{-1}, y^{-1}) \in G \times F$:

$$(x, y) \cdot (x^{-1}, y^{-1}) = (x * x^{-1}, y \diamond y^{-1}) = (e_G, e_F)$$

- Por lo tanto, cualquier elemento de $G \times F$ tiene su inverso.

Demostramos que:

- $(G \times F, \cdot)$ está bien definida (cerrada).
- $(G \times F, \cdot)$ es asociativa.
- $(G \times F, \cdot)$ tiene elemento neutro.
- Todos los elementos de $(G \times F, \cdot)$ tienen su inverso.

Por lo tanto, $(G \times F, \cdot)$ es un **grupo producto**.

▼ 11. Estudiar si son Subgrupos de los grupos indicados:

Para que un conjunto dado sea subgrupo de un grupo, debe cumplir con las propiedades de un grupo.

- La asociatividad no es necesaria, ya que se garantiza al estar trabajando con un grupo (lo mismo para la conmutatividad).
- Entonces, el análisis se resume en:
  - Ver si está bien definida (cerrada).
  - Ver si tiene elemento neutro único.
  - Ver si cada elemento tiene inverso.
    - Se puede resumir a comprobarlo en uno.

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

Partimos del grupo de los enteros y la operación suma (suponiendo que el $+$ hace referencia a la suma convencional).

Vamos a ver si el subconjunto de los números pares enteros con la suma es un subgrupo:

- Para todos los números pares, si sumamos un número par con otro número par, obtenemos como resultado un número par. Por lo tanto, los enteros pares para la suma están bien definidos.
- El elemento neutro en $(\mathbb{Z}, +)$ es el 0 y se repite para el subconjunto de los números enteros pares, ya que si sumamos un par cualquiera más 0, obtenemos ese número par.
- Para cada número entero par n, al estar en los $\mathbb{Z}$ tenemos a su inverso $-n$, de manera tal que si los sumamos obtenemos el neutro.

- Ejemplo: El inverso de 2 es -2, entonces $2 + (-2) = 0$.

Por lo tanto, los enteros pares son subgrupo de $(\mathbb{Z}, +)$.

(b) Las matrices simétricas de 2x2

Partimos del conjunto de todas las matrices cuadradas 2×2 con la operación de suma para las matrices (supongo porque no se específico nada 🐐).

Vamos a ver si las matrices simétricas 2×2 con la suma de matrices es un subgrupo. Recordar que las matrices simétricas 2×2 tiene la forma:

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}$$
$$a, b, c \in \mathbb{R}$$

- La suma de dos matrices simétricas 2×2 es una matriz simétrica 2×2. Si A y B son matrices simétricas:

$$A + B = \begin{pmatrix} a_1 & b_1 \\ b_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ b_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ b_1 + b_2 & d_1 + d_2 \end{pmatrix}$$

- El elemento neutro de las matrices simétricas 2×2 es la matriz cero, ya que si la sumamos a otra cualquier matriz simétrica 2×2 obtenemos esa matriz.
  - Claramente la matriz cero es simétrica y pertenece al conjunto.

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

- Para cada matriz simétrica 2×2 A, su inverso es otra matriz simétrica 2×2 $-A$, tal que la suma entre ambas nos da la matriz cero.

$$A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \quad -A = \begin{pmatrix} -a & -b \\ -b & -c \end{pmatrix}$$
$$A + (-A) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Demostramos que el subconjunto de las matrices simétricas 2×2 es un subgrupo del grupo de matrices 2×2.

▼ 12. Demostrar que si H y K son subgrupos de $(G, *)$ entonces $H \cap K$ es un subgrupo de $(G, *)$

Para demostrar que $H \cap K$ es subgrupo de $(G, *)$ debemos probar que:

- Está bien definida.
- Tiene elemento neutro.
- Cada elemento tiene su inverso.

¿Está bien definida?

- Sean $a, b \in H \cap K$. Es decir:
  - $a, b \in H \land a, b \in K$
- Como H es subgrupo, está bien definido para $*$, es decir, $a * b \in H$.
- De manera trivial para K, al estar bien definido para $*$, $a * b \in K$.
- Entonces, como $a, b \in H \land a, b \in K$, podemos decir que $a * b \in H \cap K$, es decir, que está bien definida para $\cap$.

¿Tiene elemento neutro?

- Tanto H como K son subgrupos de $(G, *)$, por lo tanto ambos tiene el elemento neutro e de G.
- Como $e \in H \land e \in K$, se sigue que $e \in H \cap K$.
- Por lo tanto, $H \cap K$ contiene al elemento neutro.

¿Cada elemento tiene su inverso?

- Sea $a \in H \cap K$, es decir que $a \in H \land a \in K$.
- H es subgrupo, existe el inverso de a, $a^{-1} \in H$, tal que si $a * a^{-1} = e$.
- De manera trivial para K.
- Entonces, $a^{-1} \in H \cap K$.
- Para cada $a \in H \cap K$, existe su inverso $a^{-1} \in H \cap K$ tal que $a * a^{-1} = e$.

Se demostró que $H \cap K$ es cerrada, tiene neutro y cada elemento tiene su inverso, por lo tanto es subgrupo de $(G, *)$.

▼ 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.

Sabemos que H es subgrupo de G y que $a \in G$. Queremos probar que aHa^{+1} es subgrupo de G.

¿Está bien definida?

- Sea $x, y \in aHa^{+1}$, por su definición, existen $h_1, h_2 \in H$ tales que

$$x = a * h_1 * a^{-1} \quad y = a * h_2 * a^{-1}$$

- Vamos a probar que $x * y \in aHa^{+1}$

$$x * y = (a * h_1 * a^{-1}) * (a * h_2 * a^{-1})$$

- Asociatividad:

$$x * y = a * h_1 * (a^{-1} * a) * h_2 * a$$

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

$$x * y = a * h_1 * h_2 * a^{-1}$$

- Como H es subgrupo de G, está bien definida para la operación $*$, o sea que $h_1 * h_2 \in H$.

$$x * y = a * (h_1 * h_2) * a^{-1} \in aHa^{-1}$$

- Por lo tanto, el conjunto aHa^{+1} está bien definido.

¿Tiene elemento neutro?

- El subgrupo H tiene el elemento neutro e de G. Entonces, tomando $h = e \in H$

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

- Por lo tanto, $e \in aHa^{+1}$

¿Cada elemento tiene su inverso?

- Sea $x \in aHa^{+1}$, existe un $h \in H : x = a * h * a^{-1}$. Queremos probar que $x^{-1} \in aHa^{+1}$.
- Calculamos el inverso de x:

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

- Como H es un subgrupo, $h^{-1} \in H$. Por lo tanto $x^{-1} = a * h^{-1} * a^{-1} \in aHa^{+1}$.

Demostramos que aHa^{+1} está bien definida, contiene el elemento neutro de G y cada elemento tiene su inverso. Por lo tanto aHa^{+1} es subgrupo de G.

▼ 14. Probar que todo grupo cíclico es abeliano

Un grupo G es cíclico si existe un elemento $g \in G$ tal que todos los elementos de G pueden expresarse como potencias de g.

- Donde g es el generador del grupo, $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.

Sea $G = \langle g \rangle$ un grupo cíclico generado por g. Entonces, cada elemento de G puede escribirse como una potencia de g, para cualquier $a, b \in G$, existen $m, n \in \mathbb{Z}$ tales que:

$$a = g^m \quad b = g^n$$

Queremos llegar a que G es abeliano, es decir, $a * b = b * a$.

- Podemos expresar $a * b$ como:

$$a * b = g^m * g^n$$

- Por la propiedad de grupo, podemos decir que:

$$g^m * g^n = g^{m+n}$$

- Si lo pensamos del lado de $b * a$:

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

- La suma de enteros es conmutativa, por lo tanto:

$$g^{m+n} = g^{n+m}$$

- Entonces, podemos decir que:

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

- Por lo tanto, se cumple la conmutatividad para todos los elementos de G.

Demostramos que en un grupo cíclico G, la operación es conmutativa para todos los elementos. Por lo tanto, todo grupo cíclico es abeliano.

▼ 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

Del enunciado tenemos que:

- G es cíclico orden n.
- m es divisor de n, o sea $n = m * k$
- a es el generador de G.

Queremos demostrar que las potencias de a^m generan un subgrupo de G.

- Por definición, $a^m \in G$ porque a es un generador de G, entonces sus potencias también están en G, por lo tanto $\langle a^m \rangle \subseteq G$.
- El orden de a es n, o sea, $a^n = e$, (elemento neutro). Queremos encontrar el orden de a^m.
  - Si m divide a n, o sea, $n = m * k$

$$(a^m)^k = a^{m \cdot k} = a^n = e$$

  - El orden de a^m es $k = \frac{n}{m}$. Es decir, $\langle a^m \rangle$ tiene k elementos.

$$\langle a^m \rangle = \{e, a^m, a^{2m}, ..., a^{(k-1)m}\}$$

- $\langle a^m \rangle$ es un conjunto formado por las potencias de a^m, por la propiedad de los grupos cíclicos, las potencias de un elemento generan un subgrupo. Vamos a ver si satisface las propiedades de un subgrupo:
  - Las potencias de a^m forman un conjunto cerrado bajo la operación del grupo, por lo tanto está bien definida.
  - El conjunto contiene el elemento neutro, ya que $(a^m)^0 = a^0 = e$.
  - G es un grupo, cada elemento en el tiene un inverso. Cada potencia de a^m tiene un inverso en $\langle a^m \rangle$, ya que para cada i, $(a^m)^{-i} = a^{-im}$.

El conjunto $\langle a^m \rangle = \{e, a^m, a^{2m}, ..., a^{(k-1)m}\}$, donde $k = \frac{n}{m}$, es un subgrupo de G generado por a^m.

- Por lo tanto, si m es un divisor de n, entonces a^m y sus potencias generan un subgrupo de G.

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

Para demostrar que la relación $a \equiv b \, mod(H)$, si $a * b^{-1} \in H$, es una relación de equivalencia hay que ver si cumple las tres propiedades.

¿Es reflexiva?

- La relación es reflexiva si para todo $a \in G$ se cumple que $a \equiv a \, mod(H)$.
- Debemos probar que, para todo $a \in G$, $a * a^{-1} \in H$.

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

- e es el neutro de G, y como H es subgrupo de G, entonces $e \in H$. Por lo tanto se cumple que para todo $a \in G$ que $a \equiv a \, mod(H)$.

¿Es simétrica?

- La relación es simétrica si, para todo $a, b \in G$, si $a \equiv b \, mod(H)$, entonces $b \equiv a \, mod(H)$. Es decir, probar que si $a * b^{-1} \in H$ entonces $b * a^{-1} \in H$.
- Sabemos que $a * b^{-1} \in H$, como H es un subgrupo de G, está bien definido y todo elemento tiene su inverso.
  - Si $h \in H$, entonces $h^{-1} \in H$

$$(a * b^{-1})^{-1} = (b^{-1})^{-1} * a^{-1} = b * a^{-1} \in H$$

- Lo que implica que $b \equiv a \, mod(H)$.

¿Es transitiva?

- La relación es transitiva si, para todo $a, b, c \in G$, si $a \equiv b \, mod(H)$ y $b \equiv c \, mod(H)$, entonces $a \equiv c \, mod(H)$. O sea, probar que si $a * b^{-1} \in H$ y $b * c^{-1} \in H$, entonces $a * c^{-1} \in H$.
- Sabemos que:

$$a * b^{-1} \in H$$
$$b * c^{-1} \in H$$

- Multiplicamos ambas expresiones:

$$(a * b^{-1}) * (b * c^{-1}) = a * (b^{-1} * b) * c = a * e * c^{-1} = a * c^{-1}$$

- Como H es un subgrupo de G y está bien definido, el producto de dos números de H pertenece a H.

$$a * c^{-1} \in H$$

- Entonces, se cumple que $a \equiv c \, mod(H)$.

Demostramos que la relación $a \equiv b \, mod(H)$ si $a * b^{-1} \in H$ cumple las propiedades de reflexividad, simetría y transitividad, por lo tanto, es una relación de equivalencia en G.