1.1. Grupos

- Se llama **Grupo** a un par $(G, *)$, donde G es un conjunto no vacío y $*$ es una operación interna en G que verifica las siguientes propiedades:

  g_1 Propiedad **asociativa**: $(a * b) * c = a * (b * c)$ para todos $a, b, c \in G$

  g_2 Existencia de **elemento neutro**: $\exists\, e \in G$ tal que $e * a = a$ para todo $a \in G$.

  g_3 Existencia de **inverso u opuesto** de cada elemento:
  $\forall\, a \in G$ existe $a' \in G$ tal que $a' * a = e$.

- Se dice que $(G, *)$ es un **grupo abeliano** si además se verifica la siguiente propiedad:

  g_4 Propiedad **conmutativa**: $a * b = b * a$ para todos $a, b \in G$

Si el conjunto G es finito, se llama **orden** del grupo $(G, *)$ al cardinal de G, y se nota por $|G|$. Si el conjunto G es infinito se dice que el **orden** de $(G, *)$ es infinito. Si $(G, *)$ es un grupo finito, la operación $*$ se puede describir mediante una tabla, denominada **Tabla de Cayley** del grupo.

Lemas

1. Si $*$ es operación interna asociativa en G, entonces $\forall a, b, c, d \in G$, $(a*b)*(c*d) = (a*(b*c))*d$
2. Si $(G, *)$ es grupo con neutro $e \in G$, entonces $\forall\, a \in G$ tal que $a * a = a$ se verifica que $a = e$.

Teorema 1: Inverso y neutro por la derecha

Sea $(G, *)$ grupo con elemento neutro $e \in G$, entonces:

1. Para todos $a, a' \in G$ tales que $a' * a = e$ se verifica que $a * a' = e$.
2. Para todo $a \in G$ se verifica que $a * e = a$.

Teorema 2: Unicidad del neutro y del inverso

1. En todo grupo $(G, *)$ el elemento neutro es único
2. En todo grupo $(G, *)$ el inverso de cada elemento es único.

Notaciones

Si no existe ambigüedad en la operación, el grupo $(G, *)$ se notará simplemente G. Sean $a, b \in G$:

G	en un grupo general	en un grupo abeliano
operar a con b	$a * b,\ a \cdot b,\ a \odot b,\ a \otimes b,\ ab,\ \cdots$	$a + b$
elemento neutro	$e,\ e_G,\ 1,\ 1_G,\ z,\ z_G$	$0,\ 0_G$
inverso u opuesto de a	$a',\ a^{-1}$ (**inverso**)	$-a$ (**opuesto**)
potencia $0 \in \mathbb{Z}$ del elemento $a \in G$	$a^0 = e$	$0a = z$
potencia $1 \in \mathbb{Z}$ del elemento $a \in G$	$a^1 = a$	$1a = a$
potencia $n \in \mathbb{Z}$ para $n \geq 2$	$a^n = a * a^{n-1}$	$na = a + (n-1)a$
potencia $-1 \in \mathbb{Z}$ del elemento $a \in G$	a^{-1}	$-a$
potencia $-n \in \mathbb{Z}$ para $n \geq 2$	$a^{-n} = (a^{-1})^n$	$(-n)a = n(-a)$

Propiedades cancelativas

Sea $(G, *)$ un grupo, $\forall\, a, b, x \in G$

- Si $x * a = x * b$ entonces $a = b$
- Si $a * x = b * x$ entonces $a = b$

Grupo de congruencias y grupo de unidades, módulo n: $(\mathbb{Z}_n, +_n)$ y $(\mathbb{U}_n, \cdot_n)$

Dado $n \in \mathbb{N}$, se define en $\mathbb{Z}$ la relación de equivalencia **congruencia módulo** n:

$$a \equiv_n b \Leftrightarrow n|(b-a)$$

El conjunto cociente $\mathbb{Z}/\equiv_n$ se nota $\mathbb{Z}_n$ y para cada $a \in \mathbb{Z}$ su clase es $[a]_n = \{x \in \mathbb{Z} : x \equiv_n a\} \in \mathbb{Z}_n$.

1. En $\mathbb{Z}_n$ se define $[a]_n +_n [b]_n = [a+b]_n$. Se verifica que $(\mathbb{Z}_n, +_n)$ es un grupo abeliano.
2. Sea $\mathbb{U}_n = \{[r]_n \in \mathbb{Z}_n : \text{ mcd}(r, n) = 1\}$. En $\mathbb{U}_n$ se define $[a]_n \cdot_n [b]_n = [ab]_n$. Se verifica que $(\mathbb{U}_n, \cdot_n)$ es un grupo abeliano, que se denomina **grupo de unidades** módulo n

Grupos $(\mathbb{Q}, +)$ y $(\mathbb{Q}^*, \cdot)$

En el conjunto $\mathbb{Z} \times \mathbb{N}$ se define la relación de equivalencia R_q: $(a, n) \sim_{\mathbb{Q}} (b, m) \Leftrightarrow am = bn$.
El conjunto cociente es: $\mathbb{Q} = (\mathbb{Z} \times \mathbb{N})/\sim_{\mathbb{Q}}$. Cada clase $[(a, n)] = \{(b, m) \in \mathbb{Z} \times \mathbb{N} : am = bn\} \in \mathbb{Q}$ se escribe: $[(a, n)] = \frac{a}{n} \in \mathbb{Q}$; si $n = 1$ se suele escribir simplemente: $[(a, 1)] = \frac{a}{1} = a \in \mathbb{Q}$.

1. En $\mathbb{Q}$ se define la operación suma $\frac{a}{n} + \frac{b}{m} = \frac{ma+nb}{mn}$.
   Se verifica que $(\mathbb{Q}, +)$ es grupo abeliano
2. Sea $\mathbb{Q}^* = \mathbb{Q} - \{0\}$. En $\mathbb{Q}^*$ se define $\frac{a}{n} \cdot \frac{b}{m} = \frac{ab}{mn}$.
   Se verifica que $(\mathbb{Q}^*, \cdot)$ es grupo abeliano

Grupos $(\mathbb{R}, +)$ y $(\mathbb{R}^*, \cdot)$

En el conjunto de todas las sucesiones de Cauchy con coeficientes racionales:
$S = \{(a_n)_{n\in\mathbb{N}} : (a_n)_{n\in\mathbb{N}}$ es sucesión de Cauchy y $\forall n \in \mathbb{N} \quad a_n \in \mathbb{Q}\}$ se define la relación de equivalencia: $(a_n)_{n\in\mathbb{N}} \sim_{\mathbb{R}} (b_n)_{n\in\mathbb{N}} \Leftrightarrow \text{lím}_{n\to\infty}(a_n - b_n) = 0$.
El conjunto cociente se denomina conjunto de números reales: $\mathbb{R} = S/\sim_{\mathbb{R}}$.

1. En $\mathbb{R}$ se define $[(a_n)_{n\in\mathbb{N}}] + [(b_n)_{n\in\mathbb{N}}] = [(a_n + b_n)_{n\in\mathbb{N}}]$.
   Se verifica que $(\mathbb{R}, +)$ es un grupo abeliano.
2. Sea $\mathbb{R}^* = \mathbb{R} - \{0\}$. En $\mathbb{R}^*$ se define $[(a_n)_{n\in\mathbb{N}}] \cdot [(b_n)_{n\in\mathbb{N}}] = [(a_n \cdot b_n)_{n\in\mathbb{N}}]$.
   Se verifica que $(\mathbb{R}^*, \cdot)$ es un grupo abeliano.

Producto directo de grupos

Sean $(G_1, \oplus)$ y $(G_2, \odot)$ grupos. En el producto cartesiano $G_1 \times G_2$ se define la operación interna coordenada a coordenada: $\forall\ (a, b), (c, d) \in G_1 \times G_2, \quad (a, b) * (c, d) = (a \oplus c,\, b \odot d)$.
Entonces $(G_1 \times G_2, *)$ es un grupo, y se denomina **producto directo** de $(G_1, \oplus)$ y $(G_2, \odot)$.
Si $(G_1, \oplus)$ y $(G_2, \odot)$ son grupos abelianos, entonces su producto directo también es un grupo abeliano.

Grupos $(\mathbb{C}, +)$ **y** $(\mathbb{C}^*, \cdot)$

1. En $\mathbb{R} \times \mathbb{R}$ se define $(a, b) + (c, d) = (a + c, b + d)$.
   Se verifica que $(\mathbb{R} \times \mathbb{R}, +)$ es un grupo abeliano.
2. Sea $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ y $\mathbb{C}^* = \mathbb{C} - \{(0, 0)\}$. En $\mathbb{C}^*$ se define $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.
   Se verifica que $(\mathbb{C}^*, \cdot)$ es un grupo abeliano.

Notación para los elementos de $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, cuando en dicho conjunto se consideran las operaciones dadas: $(a, b) = a + bi \in \mathbb{C}$

Subgrupos

Sea $(G, *)$ un grupo y $H \subseteq G$. Se dice que H es **subgrupo** de $(G, *)$ si y sólo si $(H, *)$ es un grupo.
Para indicar que H es un subgrupo de $(G, *)$ se escribe $H \leq G$.
Un subgrupo $H \leq G$ se dice que es **subgrupo propio** de $(G, *)$ si $H \subset G$ y $H \neq G$. Se escribe $H < G$.
Sea e_G el elemento neutro de $(G, *)$, entonces $H_0 = \{e_G\} \leq G$ y se denomina **subgrupo trivial**.

Definición equivalente de subgrupo

Sea $(G, *)$ un grupo y $H \subseteq G$, entonces H es **subgrupo** de $(G, *)$ si y sólo si:

- $e_G \in H$, siendo $e_G \in G$ el elemento neutro del grupo $(G, *)$.
- La operación $*$ es interna en H: Para todos $a, b \in H$ se verifica que $a * b \in H$.
- Para todo $a \in H$ se verifica que $a^{-1} \in H$, siendo $a^{-1} \in G$ el inverso de a en G.

Caracterización 1 de subgrupo

Si $(G, *)$ es un grupo y $\emptyset \neq H \subseteq G$ entonces $H \leq G \Leftrightarrow \forall\, a, b \in H$ se verifica que $a * b^{-1} \in H$.

Caracterización 2 de subgrupo

Si $(G, *)$ es un grupo y $\emptyset \neq H \subseteq G$ entonces $H \leq G \Leftrightarrow \forall\, a, b \in H$ se verifica que $a^{-1} * b \in H$.

1.1. Problemas

1. Demostrar que sólo hay dos grupos esencialmente distintos de orden 4 y estudiar si existe algún grupo de orden 4 no abeliano. (No corroborar la asociatividad). Proceder del siguiente modo:

   Si $G = \{e, a, b, c\}$ es grupo y e es su elemento neutro, la tabla de Cayley será como la tabla que aparece anexa.

$*$	e	a	b	c
e	e	a	b	c
a	a	z		
b	b			
c	c			

   Dar la razón por la que $z \neq a \in G$.

   a) Si $z = e$ la tabla puede completarse de dos maneras para dar grupo. Encontrar estas dos tablas.

   b) Si $z = b$ entonces se puede completar la tabla de un solo modo para dar grupo. Encontrar dicha tabla.

   c) Si $z = c$ entonces se puede completar la tabla de un solo modo para dar grupo. Encontrar dicha tabla.

d) De las tablas obtenidas, sólo hay dos estructuras de grupo distintas. Determinar cuáles son y mostrar la manera de cambiar los nombres de los elementos para ver la coincidencia de tablas.

2. Sean a y b elementos de un grupo $(G,\cdot)$. Demostrar que $ab^na^{-1}=(aba^{-1})^n$.

3. Demostrar que si $(G,\cdot)$ es un grupo con elemento neutro $e\in G$ y tal que para todo $a\in G$ se verifica que $a^2=e$, entonces $(G,\cdot)$ es abeliano.

4. Demostrar que si $(G,\cdot)$ es un grupo en el que para todo par de elementos $a,b\in G$ se verifica que $(ab)^2=a^2b^2$ entonces $(G,\cdot)$ es abeliano.

5. Demostrar que si $(G,\cdot)$ es un grupo finito de orden par entonces existe un elemento $a\in G$ distinto del neutro, que verifica que $a^2=e$.

6. Estudiar en cada caso si la operación $*$ dota al conjunto correspondiente de estructura de grupo. En caso afirmativo obtener el elemento neutro, el inverso de cada elemento e indicar si es abeliano.

   a) En $\mathbb{Z}$, $a*b=a-b$.

   b) En $G=\{2n+1:n\in\mathbb{Z}\}$ se define $*$ por: $a*b=a+b$

   c) En $G=\mathbb{R}-\{-1\}$, $a*b=a+b+ab$.

   d) $H=\{\begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix}:x,y,z\in\mathbb{R}\}$ con la operación:
   $$\begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix}\begin{pmatrix}1&x'&y'\\0&1&z'\\0&0&1\end{pmatrix}=\begin{pmatrix}1&x+x'&y+y'+xz'\\0&1&z+z'\\0&0&1\end{pmatrix}$$ (**Grupo de Heisenberg**).

7. Determinar cuales de los siguientes subconjuntos de $\mathbb{R}$ son subgrupos de $(\mathbb{R},+)$:

   a) $\mathbb{Q}^+=\{\frac{p}{q}\in\mathbb{Q}:\frac{p}{q}>0\}$

   b) $7\mathbb{Z}=\{7n:n\in\mathbb{Z}\}$

   c) $\pi\mathbb{Q}=\{\pi q:q\in\mathbb{Q}\}$

   d) $\{\pi^n:n\in\mathbb{Z}\}$

8. Demostrar que si H y K son subgrupos de un grupo abeliano $(G,*)$ entonces también es subgrupo de $(G,*)$ el conjunto $HK=\{h*k:h\in H,k\in K\}$

9. Sea $(G,*)$ un grupo y $a\in G$, se llama **centralizador de** a al subconjunto $C(a)=\{g\in G:g*a=a*g\}$ (elementos de G que conmutan con a). Demostrar que $C(a)$ es un subgrupo de G.

10. Sea $(G,*)$ un grupo, el conjunto $Z(G)=\{g\in G:x*g=g*x \text{ para todo } x\in G\}$ se denomina **centro de** G. Demostrar las siguientes proposiciones:

    a) $Z(G)\leq G$. b) $Z(G)=\bigcap_{a\in G}C(a)$. c) $a\in Z(G)\Leftrightarrow C(a)=G$

11. Sea $G=\{T_{a,b}:\mathbb{R}\to\mathbb{R},\ a,b\in\mathbb{R}$ con $a\neq 0,$ aplicaciones definidas por $T_{a,b}(r)=ar+b\}$. Se considera en G la operación composición de funciones.

    a) Demostrar que $(G,\circ)$ es un grupo. ¿Es grupo abeliano?

    b) Demostrar que $H=\{T_{a,b}\in G:a\in\mathbb{Q}\}$ es un subgrupo de G, ¿es $(H,\circ)$ abeliano?

    c) Demostrar que $K=\{T_{a,b}\in G:a=1\}$ es un subgrupo de G, ¿es $(K,\circ)$ abeliano?

    d) Sea $T_{a,b}\in G$ con $a\neq 1$, calcular el subgrupo $C(T_{a,b})=\{U\in G:U*T_{a,b}=T_{a,b}*U\}$.