Grupos I

Semigrupos y monoides.

Operaciones

Definición. *Una* **operación binaria interna** *en un conjunto X es una aplicación*

$$f : X \times X \to X$$

Para abreviar se dirá "operación" en lugar de "operación binaria interna", siempre que no haya riesgo de confusión. Cuando una aplicación f se considere como una operación en X, la imagen $f\big((x_1, x_2)\big)$ de cada par $(x_1, x_2) \in X \times X$ se escribe (según los casos) de alguna de las formas

$$x_1.x_2,\ x_1x_2,\ x_1 + x_2,\ x_1 * x_2,\ x_1 \circ x_2,\ \ldots$$

En las dos primeras se dice que la notación es **multiplicativa** y en la tercera se dice que la notación es **aditiva**.

Una operación $*$ en un conjunto X es **asociativa** si

$$x_1 * (x_2 * x_3) = (x_1 * x_2) * x_3, \quad \text{para todo } x_1, x_2, x_3 \in X$$

Una operación $*$ en un conjunto X es **conmutativa** si

$$x_1 * x_2 = x_2 * x_1, \quad \text{para todo } x_1, x_2 \in X$$

Cuando se usa notación aditiva, se supone que la operación es conmutativa y que, por tanto,

$$x_1 + x_2 = x_2 + x_1, \quad \text{para todo } x_1, x_2 \in X.$$

Una operación $*$ en un conjunto X posee **elemento unidad** (**elemento neutro**) si hay un elemento $e \in X$ que cumpla:

$$x * e = x = e * x, \quad \text{para todo } \ x \in X$$

Si la notación es aditiva, se dice *"elemento neutro"* y si es multiplicativa (o, en general, no aditiva) se dice *"elemento unidad"*. Nótese que en la definición se exige que e sea un elemento del conjunto X.

Proposición. *Si una operación $*$ en un conjunto X posee elemento unidad, entonces éste es único.*

Demostración. Suponer que $e, e' \in X$ cumplen

$$\begin{array}{lccccl} (\mathbf{1}) & e * x & = & x & = & x * e, \quad \text{para todo} \quad x \in X \\ (\mathbf{2}) & e' * x & = & x & = & x * e', \quad \text{para todo} \quad x \in X \end{array}$$

Poniendo en la igualdad **(1)** $x = e'$,

$$e * e' = e'$$

Poniendo en la igualdad **(2)** $x = e$,

$$e = e * e'$$

En consecuencia

$$e = e * e' = e' \ \blacksquare$$

Ejemplos

1. Las operaciones adición y multiplicación usuales en el conjunto $\mathbf{Z}$ de los enteros son asociativas y conmutativas. La adición posee elemento neutro: el número entero 0; la multiplicación posee elemento unidad: el número entero 1.
2. Consideremos el conjunto $\mathrm{M}_2(\mathbf{Z})$ de las matrices 2×2 sobre los enteros; en símbolos:

   $$\mathrm{M}_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \;\middle|\; a_{ij} \in \mathbf{Z};\ i, j \in \{1, 2\} \right\}$$

   Dadas

   $$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

   en $\mathrm{M}_2(\mathbf{Z})$, se define

   $$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

   y

   $$AB = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

   Obviamente, si $A, B \in \mathrm{M}_2(\mathbf{Z})$, entonces $A + B \in \mathrm{M}_2(\mathbf{Z})$ y $AB \in \mathrm{M}_2(\mathbf{Z})$. La adición en $\mathrm{M}_2(\mathbf{Z})$ es asociativa y conmutativa (compruébese); la multiplicación en $\mathrm{M}_2(\mathbf{Z})$ es asociativa (compruébese) pero no es conmutativa:

   $$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

La adición posee elemento neutro:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix};$$

la multiplicación posee elemento unidad:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

3. En el conjunto $\mathbf{Z}$ de los números enteros la operación

$$\begin{array}{ccc} \mathbf{Z}\times\mathbf{Z} & \to & \mathbf{Z} \\ (x,y) & \mapsto & x-y \end{array}$$

no es asociativa:

$$\begin{array}{rcccl} 8-(5-3) & = & 8-2 & = & 6 \\ (8-5)-3 & = & 3-3 & = & 0 \end{array}$$

ni conmutativa:

$$\begin{array}{rcl} 8-3 & = & 5 \\ 3-8 & = & -5 \end{array}$$

4. Sea X un conjunto. La unión y la intersección son operaciones en el conjunto $\mathcal{P}(X)$ de las partes de X. Si A, B son subconjuntos de X, entonces $A\cup B$ y $A\cap B$ son subconjuntos de X; por tanto las aplicaciones

$$\begin{array}{ccc} \mathcal{P}(X)\times\mathcal{P}(X) & \to & \mathcal{P}(X) \\ (A,B) & \mapsto & A\cup B \end{array} \quad \text{y} \quad \begin{array}{ccc} \mathcal{P}(X)\times\mathcal{P}(X) & \to & \mathcal{P}(X) \\ (A,B) & \mapsto & A\cap B \end{array}$$

son, efectivamente, operaciones en el conjunto $\mathcal{P}(X)$. Ambas operaciones son asociativas y conmutativas. La unión posee elemento neutro: $\varnothing$. ¿Posee la intersección elemento neutro?

5. Consideremos el conjunto $M(X)$ de todas las aplicaciones de un conjunto X en sí mismo:

$$M(X) = \{f \mid f : X \to X\}$$

Si f y g son aplicaciones de X en X, entonces la composición $f\circ g$ está definida y es también una aplicación de X en X. Queda así establecida una operación en el conjunto $M(X)$:

$$\begin{array}{ccc} M(X)\times M(X) & \to & M(X) \\ (f,g) & \mapsto & f\circ g \end{array}$$

Esta operación es asociativa, no es conmutativa (si $\mathrm{Card}(X)\geq 2$), y posee elemento unidad: la aplicación identidad de X en X, 1_X.

6. Denotemos por $B(X)$ el conjunto de todas las aplicaciones biyectivas de un conjunto X en sí mismo:

$$B(X) = \{f \mid f : X \to X, f \text{ biyectiva } \} = \{f \in M(X) \mid f \text{ biyectiva } \}$$

Si f y g son aplicaciones biyectivas de X en X, entonces la composición $f \circ g$ es también una aplicación biyectiva de X en X. Queda así definida una operación en el conjunto $B(X)$:

$$\begin{array}{ccc} B(X) \times B(X) & \to & B(X) \\ (f, g) & \mapsto & f \circ g \end{array}$$

Esta operación es asociativa, no es conmutativa (si $\text{Card}(X) \geq 3$), y posee elemento unidad: la aplicación identidad, 1_X, de X en X.

Semigrupos y monoides

Definición. *Un* **semigrupo** *es un par $S = (S, *)$ formado por un conjunto (no vacío) S y una operación $*$ en S asociativa.*

Definición. *Un* **semigrupo conmutativo** *o* **abeliano** *es un semigrupo en el que la operación es conmutativa.*

Definición. *Un* **monoide** *es un semigrupo $M = (M, *)$ con elemento unidad.*

Explícitamente:

Definición. *Un* **monoide** *es un par $M = (M, *)$ donde M es un conjunto y $*$ es una operación en M tales que:*

1 *$a * (b * c) = (a * b) * c$, para todo $a, b, c \in M$*

2 *Hay un elemento $e \in M$ tal que $a * e = a = e * a$ para todo $a \in M$*

Definición. *Un monoide $M = (M, *)$ en el que la operación es conmutativa:*

$$a * b = b * a, \text{para todo } a, b \in M,$$

se denomina **monoide conmutativo** *o* **abeliano**.

Ejemplos de monoides.

1 $(\mathbf{N}, +)$, el conjunto de los números naturales con la adición; el elemento neutro es el número natural 0.

2 $(\mathbf{N}, .)$, el conjunto de los números naturales con la multiplicación; el elemento unidad es el número natural 1.

3 $(\mathbf{Z}, +)$, el conjunto de los números enteros con la adición; el elemento neutro es el número entero 0.

4 $(\mathbf{Z}, .)$, el conjunto de los números enteros con la multiplicación; el elemento unidad es el número entero 1.

5 $\big(M(X),\circ\big)$, el conjunto de las aplicaciones de un conjunto X en sí mismo junto con la composición de aplicaciones como operación; el elemento unidad es la aplicación identidad 1_X de X en X.

6 $\big(B(X),\circ\big)$, el conjunto de las aplicaciones biyectivas de un conjunto X en sí mismo junto con la composición de aplicaciones como operación; el elemento unidad es la aplicación identidad 1_X de X en X.

7 Dados un conjunto X y una aplicación τ de X en X $\big[$es decir, $\tau \in M(X)\big]$, se definen las potencias de exponente natural de τ en la forma:

$$\begin{array}{l}\tau^0 = 1_X;\\ \tau^{n+1} = \tau^n \circ \tau, \quad (n \in \mathbf{N})\end{array}$$

De modo que

$$\begin{array}{l}\tau^0 = 1_X,\\ \tau^1 = \tau^0 \circ \tau = 1_X \circ \tau = \tau,\\ \tau^2 = \tau^1 \circ \tau = \tau \circ \tau,\\ \tau^3 = \tau^2 \circ \tau = (\tau \circ \tau) \circ \tau = \tau \circ \tau \circ \tau,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\end{array}$$

Por inducción se prueba que

$$\tau^n \circ \tau^m = \tau^{n+m}, \text{ para todo } n, m \in \mathbf{N}.$$

Pongamos $\langle\tau\rangle = \{\tau^n \mid n \in \mathbf{N}\}$. El par $\big(\langle\tau\rangle,\circ\big)$ es un monoide; el elemento unidad es $1_X = \tau^0$.

8 Dados un conjunto X y una aplicación biyectiva τ de X en X $\big[$es decir, $\tau \in B(X)\big]$, se definen las potencias de exponente entero de τ en la forma:

$$\begin{array}{ll}\tau^0 = 1_X,\\ \tau^{n+1} = \tau^n \circ \tau, & \text{si } n \in \mathbf{Z},\ n \geq 0\\ \tau^n = (\tau^{-1})^{-n}, & \text{si } n \in \mathbf{Z},\ n < 0\end{array}$$

[Obviamente, τ^{-1} denota la aplicación inversa de la aplicación biyectiva τ]. Se prueba que

$$\tau^n \circ \tau^m = \tau^{n+m}, \text{ para todo } n, m \in \mathbf{Z}.$$

Pongamos $\langle\tau\rangle = \{\tau^n \mid n \in \mathbf{Z}\}$. El par $\big(\langle\tau\rangle,\circ\big)$ es un monoide; el elemento unidad es $1_X = \tau^0$.

9 Dado un conjunto X, el par $\big(\mathcal{P}(X),\cup\big)$ es un monoide; el elemento unidad es $\varnothing$. El par $\big(\mathcal{P}(X),\cap\big)$ es un monoide; el elemento unidad es X.

10 Consideremos el conjunto $\mathrm{M}_2(\mathbf{Z})$ de las matrices 2×2 sobre los enteros. El par $\big(\mathrm{M}_2(\mathbf{Z}),+\big)$ es un monoide. El par $\big(\mathrm{M}_2(\mathbf{Z}),.\big)$ es un monoide.

11 Consideremos el conjunto $\mathrm{M}_2(\mathbf{Q})$ de las matrices 2×2 sobre los racionales. El par $\big(\mathrm{M}_2(\mathbf{Q}),+\big)$ es un monoide. El par $\big(\mathrm{M}_2(\mathbf{Q}),.\big)$ es un monoide.

Ejemplos de semigrupos

1 Pongamos $\mathbf{N}^* = \{n \in \mathbf{N} \mid n \neq 0\} = \mathbf{N} - \{0\}$; el par $(\mathbf{N}^*, +)$ es un semigrupo (la suma de dos naturales no nulos es un natural no nulo) pero no es un monoide ¿por qué?.

2 El par $(\mathbf{N}^*, .)$ es un semigrupo ¿es un monoide?

3 Un entero n es **par** si hay un entero z tal que $n = 2z$. Sea P el conjunto de los enteros pares: $P = \{2z \mid z \in \mathbf{Z}\}$. El producto de dos enteros pares es un entero par: $(2z)(2z') = 2(2zz')$. El par $(P, .)$ es un semigrupo ¿Es $(P, .)$ un monoide?

4 La suma de dos enteros pares es un entero par: $2z + 2z' = 2(z + z')$. El par $(P, +)$ es un semigrupo. ¿Es $(P, +)$ un monoide?

Tablas

Las operaciones en conjuntos finitos se pueden representar mediante tablas de doble entrada en la forma que se indica. Sea $X = \{x_1, x_2, \ldots, x_i, \ldots, x_n\}$ un conjunto finito y supóngase definida una operación en X:

$$\begin{array}{ccc} X \times X & \to & X \\ (x_i, x_j) & \mapsto & x_i x_j \end{array}$$

– Se disponen los elementos de X, ordenados de alguna forma, como índices de entrada de las filas y de las columnas de una tabla bidimensional $n \times n$. Por convenio se disponen los elementos de X en el mismo orden como índices de columnas (de izquierda a derecha) y como índices de filas (de arriba abajo). El aspecto inicial de la tabla es:

	x_1	x_2	$\ldots$	x_j	$\ldots$	x_n
x_1						
x_2						
$\vdots$						
x_i						
$\vdots$						
x_n						

– Para cada $x_i \in X$ y cada $x_j \in X$ se pone el producto $x_i x_j$ en la intersección de la fila encabezada por x_i con la columna encabezada por x_j, según se ilustra a continuación:

	x_1	x_2	$\dots$	x_j	$\dots$	x_n
x_1	x_1x_1	x_1x_2	$\dots$	x_1x_j	$\dots$	x_1x_n
x_2	x_2x_1	x_2x_2	$\dots$	x_2x_j	$\dots$	x_2x_n
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
x_i	x_ix_1	x_ix_2	$\dots$	x_ix_j	$\dots$	x_ix_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_n	x_nx_1	x_nx_2	$\dots$	x_nx_j	$\dots$	x_nx_n

Ejemplo. Sea D un conjunto de dos elementos, digamos $D = \{r, s\}$. Consideremos el monoide $(M(D), \circ)$ de las aplicaciones de D en D con la operación de composición. Escribamos explícitamente los elementos del conjunto $M(D)$:

$$1_D = \begin{pmatrix} r & s \\ r & s \end{pmatrix} \quad \alpha = \begin{pmatrix} r & s \\ s & r \end{pmatrix} \quad \beta = \begin{pmatrix} r & s \\ r & r \end{pmatrix} \quad \gamma = \begin{pmatrix} r & s \\ s & s \end{pmatrix}$$

[Nota: No debe confundirse una expresión de entre las que aparecen en este ejemplo tal como

$$\alpha = \begin{pmatrix} r & s \\ s & r \end{pmatrix}$$

con una matriz (en el sentido del álgebra lineal). Mediante la notación aquí empleada se pretende representar la aplicación de D en D que aplica cada elemento de la fila superior en el correspondiente elemento de la fila inferior; esto es, la aplicación $\alpha : D \to D$ tal que $\alpha(r) = s$ y $\alpha(s) = r$.]

La tabla que representa la operación del monoide $M(D) = (M(D), \circ)$ es

	1_D	α	β	γ
1_D	1_D	α	β	γ
α	α	1_D	γ	β
β	β	β	β	β
γ	γ	γ	γ	γ

Las tablas se usarán con el fin de ilustrar explícitamente mediante ejemplos concretos durante el desarrollo de los temas sucesivos, diversas cuestiones y conceptos; especialmente en el caso de grupos finitos y anillos finitos. Pero debe notarse que el empleo de las tablas se hace únicamente con este fin ilustrativo. La pretensión de representar mediante tablas

las operaciones en conjuntos finitos con un número elevado de elementos es, humanamente, irrealizable: ¿Cómo y dónde escribir una tabla $n \times n$ cuando el entero n es muy grande?.

Ejercicio. Sea X un conjunto no vacío. Escojamos un elemento a en X. Consideremos el conjunto $F_a(X)$ de las aplicaciones de X en X que fijan el elemento a:

$$F_a(X) = \{f \in M(X) \mid f(a) = a\}$$

1 Probar que $(F_a(X), \circ)$ es un monoide (con la operación de composición).
2 Caso particular: suponer $X = \{a, b, c\}$.
  2.1 Escribir todos los elementos de $F_a(X)$.
  2.2 Confeccionar la tabla del monoide $(F_a(X), \circ)$.

Ejercicio. Sea X un conjunto de tres elementos, digamos $X = \{a, b, c\}$.
1 Escribir todos los elementos del conjunto $B(X)$ de las aplicaciones biyectivas de X en X.
2 Confeccionar la tabla del monoide $(B(X), \circ)$.

Ejercicio. Considérese el conjunto $R_4 = \{1, i, -1, -i\}$ de las raíces cuartas de la unidad en el conjunto $\mathbf{C}$ de los números complejos.
1 Comprobar que la multiplicación en $\mathbf{C}$ induce, por restricción, una operación en el conjunto R_4; es decir, comprobar que el producto de dos elementos cualesquiera de R_4 es un elemento de R_4.
2 Comprobar que el par $(R_4, .)$ es un monoide.
3 Confeccionar la tabla del monoide $(R_4, .)$.
4 ¿Es $(R_4, +)$ un monoide? Justifica la respuesta. (Aquí "+" denota la adición de números complejos).

Unidades de los monoides

Definición. *Un elemento u de un monoide $M = (M, *)$ es* **una unidad** *si hay un elemento $v \in M$ tal que*

$$u * v = e = v * u,$$

donde e es **el** *elemento unidad de M.*

Debe ponerse especial atención con el fin de no confundir **el** elemento unidad, e, de un monoide M con **una** unidad de M. Dado que en todo monoide M se verifica $e * e = e$, el elemento unidad de M es una unidad de M.

Ejemplos.

1 En el monoide $(\mathbf{N}, +)$ el elemento unidad es el número natural 0; por tanto 0 es una unidad. Si $m \in \mathbf{N}$ es una unidad, entonces hay un $n \in \mathbf{N}$ tal que $m + n = 0$. La única posibilidad es $m = n = 0$. En consecuencia 0 es la unica unidad en este monoide.

2 En el monoide $(\mathbf{N},\ .)$ el elemento unidad es el número natural 1; por tanto 1 es una unidad. Si $m \in \mathbf{N}$ es una unidad, entonces hay un $n \in \mathbf{N}$ tal que $mn = 1$. La única posibilidad es $m = n = 1$. En consecuencia 1 es la unica unidad en este monoide.

3 En el monoide $(\mathbf{Z}, +)$ el elemento unidad es el entero 0. Para todo $m \in \mathbf{Z}$ hay un elemento $n \in \mathbf{Z}$ tal que $m + n = 0$ (tomar $n = -m$). En consecuencia todo entero es una unidad en el monoide $(\mathbf{Z}, +)$.

4 En el monoide $(\mathbf{Z},\ .)$ el elemento unidad es 1; por tanto 1 es una unidad. Además, dado que $(-1)(-1) = 1$, resulta que -1 es también una unidad. Si $u \in \mathbf{Z}$ es una unidad, entonces hay un $v \in \mathbf{Z}$ tal que $uv = 1$, tomando valores absolutos, $|u|\,|v| = |uv| = |1| = 1$, de donde se deduce (por **2**) que debe ser $u = v = 1$ ó $u = v = -1$. En consecuencia las unidades del monoide $(\mathbf{Z},\ .)$ son, exactamente, 1 y -1.

Ejercicios.

1 Dado un conjunto X, describir las unidades del monoide $(M(X), \circ)$.
2 Dado un conjunto X, describir las unidades del monoide $(B(X), \circ)$.
3 Describir las unidades del monoide $(\mathrm{M}_2(\mathbf{Q}), +)$.
4 Describir las unidades del monoide $(\mathrm{M}_2(\mathbf{Q}),\ .)$.

Proposición. *Si u es una unidad de un monoide $M = (M, *)$, entonces hay un único elemento $v \in M$ tal que*

$$u * v = e = v * u$$

Demostración.

- Existencia: Por ser u una unidad
- Unicidad: Suponer que v y v' son elementos de M tales que

$$u * v = e = v * u \ \text{ y } \ u * v' = e = v' * u$$

Entonces

$$v = v * e = v * (u * v') = (v * u) * v' = e * v' = v' \ \blacksquare$$

Notaciones multiplicativa y aditiva.

En las consideraciones teóricas se usa, por convenio, notación multiplicativa para representar la operación en un semigrupo, en un monoide o, más adelante, en un grupo. Posteriormente, al estudiar la teoría de anillos (y cuerpos), nos encontraremos en situaciones análogas a lo que ocurre en $\mathbf{Z}$, en $\mathbf{Q}$, en $\mathrm{M}_2(\mathbf{Q})$, etc; esto es, estructuras algebraicas en las que conviven dos operaciones; una de tipo aditivo y otra multiplicativo. Según que la operación se exprese en forma multiplicativa o en forma aditiva se usan, por costumbre, terminologías y convenios específicos que pasamos a comentar, pues conviene que el lector se familiarice con ellas:

– **Notación multiplicativa**. La operación en un monoide M se expresa en la forma

$$\begin{array}{ccc} M\times M & \to & M \\ (a,b) & \mapsto & a.b \end{array} \qquad \text{o bien} \qquad \begin{array}{ccc} M\times M & \to & M \\ (a,b) & \mapsto & a\times b \end{array}$$

En este caso se suele omitir el punto "." o el aspa "×"y se escribe simplemente $a.b = ab$ ó $a \times b = ab$, si no hay posible ambigüedad. En una expresión de la forma $ab = a.b = a\times b$ se dice que a y b son los **factores** y que ab es el **producto**, y la operación se denomina, genéricamente, **multiplicación**. El elemento unidad se escribe 1 en lugar de e; pero no debe confundirse con el número entero 1. Los axiomas de la definición de monoide se expresan:

1. La operación es asociativa:

$$a(bc) = (ab)c, \text{ para todo } a, b, c \in M.$$

2. Hay un elemento, denotado 1, en M tal que

$$a1 = a = 1a, \text{ para todo } a \in M.$$

– **Notación aditiva**. La operación en un monoide M se expresa en la forma

$$\begin{array}{ccc} M\times M & \to & M \\ (a,b) & \mapsto & a+b \end{array}$$

Se dice que a y b son los **sumandos** y que $a + b$ es la **suma**, y la operación se denomina, de modo genérico, **adición**. El elemento unidad se escribe 0 y se denomina el elemento **neutro** o el **cero** del monoide M; pero no debe confundirse con el número entero 0. En este caso los axiomas de la definición de monoide se expresan:

1. La operación es asociativa:

$$a + (b + c) = (a + b) + c, \text{ para todo } a, b, c \in M.$$

2. Hay un elemento, denotado 0, en M tal que

$$a + 0 = a = 0 + a, \text{ para todo } a \in M.$$

Si la notación utilizada es aditiva, entonces se supone que el monoide M es abeliano, es decir, se supone que

$$a + b = b + a, \quad \text{para todo} \quad a, b \in M.$$

(Atención, esto no elimina la posibilidad de que el monoide sea conmutativo y se utilice notación multiplicativa.)

Definición.

- *Sea u una unidad de un monoide multiplicativo $M = (M, .)$. El único elemento $v \in M$ tal que*

$$uv = 1 = vu$$

se denomina el **inverso** *de u y se escribe $v = u^{-1}$.*

- *Sea u una unidad de un monoide aditivo $M = (M, +)$. El único elemento $v \in M$ tal que*

$$u + v = 0 = v + u$$

se denomina el **opuesto** *de u y se escribe $v = -u$.*

Propiedades de las unidades

Proposición. *Sea $M = (M, .)$ un monoide.*

1 *Si u y v son unidades de M, entonces uv es una unidad de M y*

$$(uv)^{-1} = v^{-1}u^{-1}$$

2 *Si u es una unidad de M, entonces u^{-1} es una unidad de M y*

$$(u^{-1})^{-1} = u$$

3 *El elemento unidad 1 de M es una unidad y*

$$1^{-1} = 1$$

Demostración.

1

$$(uv)(v^{-1}u^{-1}) = 1 = (v^{-1}u^{-1})(uv)$$

2

$$uu^{-1} = 1 = u^{-1}u$$

3

$$1 \times 1 = 1 \quad \blacksquare$$

Se denota por $\mathbf{U}(M)$ el conjunto de las unidades de un monoide M. Así

$$\mathbf{U}(M) = \{u \in M \mid \text{existe } v \in M, uv = 1 = vu\}$$

Esto es, dado $u \in M$, se tiene

$$u \in \mathbf{U}(M) \iff \text{hay un } v \in M \text{ tal que } uv = 1 = vu$$

Notas y ejemplos

1 $\mathbf{U}(\mathbf{N},+)=\{0\}$

2 $\mathbf{U}(\mathbf{N},.)=\{1\}$

3 $\mathbf{U}(\mathbf{Z},+)=\mathbf{Z}$

4 $\mathbf{U}(\mathbf{Z},.)=\{1,-1\}$

5 Para un conjunto X cualquiera

$$\mathbf{U}\big(M(X)\big)=B(X);$$

es decir, las unidades del monoide $M(X)$ de las aplicaciones de X en X son exactamente las aplicaciones biyectivas de X en X.

6 En el monoide multiplicativo $\mathrm{M}_2(\mathbf{Q})$ consideremos las matrices

$$A=\begin{pmatrix}2&3\\1&2\end{pmatrix}\ \text{ y }\ B=\begin{pmatrix}3&11\\1&4\end{pmatrix}$$

Se verifica $\det(A)\neq 0$ y $\det(B)\neq 0$, por tanto

$$A,B\in\mathbf{U}\big(\mathrm{M}_2(\mathbf{Q})\big).$$

Se comprueba fácilmente que

$$A^{-1}=\begin{pmatrix}2&-3\\-1&2\end{pmatrix},B^{-1}=\begin{pmatrix}4&-11\\-1&3\end{pmatrix}$$

Compruébese que

$$(AB)^{-1}=B^{-1}A^{-1}$$

pero que

$$(AB)^{-1}\neq A^{-1}B^{-1}$$

Nota. Se prueba en álgebra lineal que $\mathbf{U}(M_2(\mathbf{Q}))=\mathrm{GL}_2(\mathbf{Q})$, donde $\mathrm{GL}_2(\mathbf{Q})$ denota el conjunto de las matrices 2×2 con coeficientes en $\mathbf{Q}$ y de determinante distinto de 0.

Submonoides

Definición. *Un subconjunto S de un monoide $M=(M,.)$ es un* **submonoide** *de M si cumple las dos condiciones siguientes:*

(1) *para todo s_1,s_2 elementos de S, su producto s_1s_2 también es un elemento de S; y*

(2) *el elemento unidad 1 del monoide M pertenece a S.*

En el caso aditivo, $M=(M,+)$, la definición anterior se escribe

(1) para todo s_1,s_2 elementos de S, su suma s_1+s_2 también es un elemento de S; y

(2) el elemento neutro 0 del monoide M pertenece a S.

Si S es un submonoide de un monoide $M = (M, .)$, entonces, por **(1)**, queda definida una operación en S:

$$\begin{array}{ccc} S \times S & \to & S \\ (s_1, s_2) & \mapsto & s_1 s_2 \end{array}$$

que se denomina **la restricción de la operación en M a S.**

Proposición. *Sea S un submonoide de un monoide $M = (M, .)$. El conjunto S junto con la restricción de la operación en M a S es un monoide.*

Demostración. Es elemental y se deja como ejercicio.

Ejemplos.

1 El conjunto $\mathbf{N}$ de los números naturales es un submonoide del monoide aditivo $(\mathbf{Z}, +)$ de los números enteros. ¿Es $\mathbf{N}$ un submonoide del monoide multiplicativo $(\mathbf{Z}, .)$ de los enteros?

2 Sea X un conjunto. El conjunto $B(X)$ de las aplicaciones biyectivas de X en X es un submonoide del monoide $(M(X), \circ)$ de las aplicaciones de X en X.

3 El conjunto $\mathbf{U}(M)$ de las unidades de cualquier monoide M es un submonoide de M.

4 Sea τ una aplicación de un conjunto X en sí mismo. El conjunto

$$\langle \tau \rangle = \{\tau^n \mid n \in \mathbf{N}\}$$

es un submonoide del monoide $(M(S), \circ)$.

5 Sea τ una aplicación biyectiva de un conjunto X en sí mismo. El conjunto

$$\langle \tau \rangle = \{\tau^n \mid n \in \mathbf{Z}\}$$

es un submonoide del monoide $(B(S), \circ)$.

6 Sea a un elemento dado de un conjunto X. En el monoide $M(X)$ consideremos el conjunto $M_a(X)$ de las aplicaciones de X en X que fijan a:

$$M_a(X) = \{f \mid f : X \to X, f(a) = a\} = \{f \in \mathrm{M}(X) \mid f(a) = a\}$$

El conjunto $M_a(X)$ es un submonoide de $M(X)$.

7 Considérese el conjunto $\mathrm{GL}_2(\mathbf{Q})$ de las matrices 2×2 sobre los racionales y de determinante distinto de cero; esto es,

$$\mathrm{GL}_2(\mathbf{Q}) = \{A \in \mathrm{M}_2(\mathbf{Q}) \mid \det(A) \neq 0\}$$

El conjunto $\mathrm{GL}_2(\mathbf{Q})$ es un submonoide del monoide multiplicativo $(\mathrm{M}_2(\mathbf{Q}), .)$ de las matrices 2×2 sobre $\mathbf{Q}$.

8 El conjunto $\mathbf{U}(M)$ de las unidades de un monoide M es un submonoide de M.

Ejercicios.

1 Sea S un subconjunto de un conjunto X. Consideremos el conjunto $M_S(X)$ de las aplicaciones de X en X que aplican todo elemento de S en S; esto es,

$$M_S(X) = \{f \in M(X) \mid f(S) \subseteq S\} = \{f \in M(X) \mid f(s) \in S, \text{ para todo } s \in S\}.$$

Probar que $M_S(X)$ es submonoide del monoide $(M(X), \circ)$

2 Sea a un elemento de un conjunto X. Consideremos el conjunto $V_A(X)$ de las aplicaciones de X en X que mueven a; esto es,

$$V_a(X) = \{f \in M(X) \mid f(a) \neq a\}.$$

¿Es $V_a(X)$ submonoide del monoide $(M(X), \circ)$? Justifica la respuesta.

Grupos

El concepto de grupo y ejemplos elementales

Definición. *Un* **grupo** *es un par $G = (G, .)$ donde G es un conjunto y "." es una operación en G :*

$$\begin{array}{ccc} G \times G & \to & G \\ (a, b) & \mapsto & a.b \end{array}$$

tales que se cumplan las condiciones siguientes (los axiomas de grupo):

1. La operación es asociativa

$$a.(b.c) = (a.b).c, \text{ para todo } a, b, c \in G \ .$$

2. Hay un elemento $e \in G$ tal que

$$a.e = a = e.a, \text{ para todo } a \in G \ .$$

3. Para cada $a \in G$ hay un elemento $a' \in G$ tal que

$$a.a' = e = a'.a \ .$$

Notas y ejemplos

1 Si $G = (G, .)$ es un grupo, entonces, por los axiomas **1** y **2**, G es un monoide y, por el axcioma **3**, todo elemento de este monoide G es una unidad; esto es, $\mathbf{U}(G) = G$. Recíprocamente, si $M = (M, .)$ es un monoide en el que todo elemento es una unidad [$\mathbf{U}(M) = M$], entonces $(M, .)$ es un grupo.

2 Por el punto **1** anterior todo grupo es un monoide. Por tanto se pueden aplicar a cualquier grupo todas las consideraciones vistas previamente para los monoides. En particular, el elemento e que aparece en el axioma **2** de la definición de grupo es único y se denomina el **elemento unidad** del grupo [**elemento neutro** en el caso de notación aditiva]; para cada elemento a en un grupo G, el elemento a' que se menciona en el axioma **3** de la definición de grupo es único, se denomina el **inverso** de A [con notación aditiva, **opuesto**] y se denota a^{-1} [con notación aditiva, $-a$].

3

Definición. *Dos elementos a y b de un grupo* **conmutan** *si $a * b = b * a$. Un grupo G es* **conmutativo** *o* **abeliano** *si todo par de elementos de él conmutan. Si el conjunto G es finito, entonces se dice que el grupo G es* **finito** *y se denota por $|G|$ el número de elementos de G; en otro caso se dice que el grupo G es* **infinito** *y se pone $|G| = \infty$.*

Propiedades inmediatas.

En todo grupo se cumplen las siguientes propiedades elementales, derivadas directamente de la definición de grupo:

Proposición. *Sea $G = (G, .)$ un grupo.*

4. *Si e, e' son elementos de G tales que*

$$a.e = a = e.a, \text{ para todo } a \in G,$$

y

$$a.e' = a = e'.a, \text{ para todo } a \in G,$$

entonces $e' = e$. En consecuencia, el elemento e del axioma **2** *de la definición de grupo es único; se dice que e es el* **elemento unidad** *del grupo G, y se pone, habitualmente, $e = 1$ si se utiliza notación multiplicativa; [se pone $e = 0$ si la notación es aditiva, en cuyo caso 0 se denomina el elemento* **neutro** *o* **cero** *del grupo].*

5. *Sea a un elemento de G, si a', a'' son elementos de G tales que*

$$a.a' = e = a'.a,$$

y

$$a.a'' = e = a''.a,$$

entonces $a' = a''$. En consecuencia, dado $a \in G$, el elemento a' del axioma **3** *de la definición de grupo es único; se dice que a' es el* **elemento inverso** *de a y se pone, habitualmente, $a' = a^{-1}$ si la notación es multiplicativa; [si la notación usada es aditiva entonces se escribe $a' = -a$ y se dice que $-a$ es el* **opuesto** *de a].*

6. *$1^{-1} = 1$; [$-0 = 0$, en caso de notación aditiva].*

7. *Para todo $a \in G$ se tiene $(a^{-1})^{-1} = a$; [$-(-a) = a$ para notación aditiva].*

8. *Para todo $a, b \in G$ se tiene $(a.b)^{-1} = b^{-1}.a^{-1}$; [$-(a + b) = -a + (-b) = -a - b$ en caso de notación aditiva (nótese que en este caso se supone que el grupo G es conmutativo)].*

9. *Sean a, b, c elementos de G,*
si $a.b = a.c$, entonces $b = c$;
si $b.a = c.a$, entonces $b = c$.

10. *Dados $a, b \in G$,*
hay un único elemento $x \in G$ que cumpla $a.x = b$, y

hay un único elemento $y \in G$ que cumpla $y.a = b$.

Demostración. Se exponen las demostraciones de las propiedades utilizando notación multiplicativa.

4. Se tiene
$$e = e.e' = e'.$$

5. Se tiene
$$a' = a'.e = a'.(a.a'') = (a'.a).a'' = e.a'' = a''.$$

6. Como $1.1 = 1$, el inverso de 1 es 1.

7. De $a.a^{-1} = 1 = a^{-1}.a$ se sigue que el inverso de a^{-1} es a.

8. Dado que
$$(a.b).(b^{-1}.a^{-1}) = a.(b.b^{-1}).a^{-1} = a.1.a^{-1} = a.a^{-1} = 1$$
y
$$(b^{-1}.a^{-1}).(a.b) = b^{-1}.(a^{-1}.a).b = b^{-1}.1.b = b^{-1}.b = 1,$$
se sigue que el inverso de $a.b$ es $b^{-1}.a^{-1}$.

9. Si $a.b = a.c$, entonces $a^{-1}.(a.b) = a^{-1}.(a.c)$, de donde $(a^{-1}.a).b = (a^{-1}.a).c$; esto es $1.b = 1.c$ y, finalmente, $b = c$. Se prueba analogamente la otra propiedad multiplicando (a derecha) los dos miembros de la igualdad $b.a = c.a$ por el inverso de a.

10. Existencia: Tomar $x = a^{-1}.b$ (respectivamente, $y = b.a^{-1}$). Unicidad: es consecuencia de la propiedad **9.**

Ejercicio. Cada elemento a en un grupo G determina las aplicaciones

$$\begin{array}{rcccc} f_a & : & G & \to & G \\ & & x & \mapsto & f_a(x) = ax \end{array} \qquad \Big| \qquad \begin{array}{rcccc} c_a & : & G & \to & G \\ & & x & \mapsto & c_a(x) = xa \end{array}$$

Probar:

- **a.** Si a, b son elementos de G, entonces $f_a \circ f_b = f_{ab}$ y $c_a \circ c_b = c_{ba}$.
- **b.** $f_1 = 1_G$ (la aplicación identidad de G en G) y $c_1 = 1_G$.
- **c.** Como consecuencia de los apartados **a.** y **b.**, para cada $a \in G$ la aplicación f_a es una biyección de G en G, y la aplicación c_a es una biyección de G en G.
- **d.** Interpretar el apartado **c.** en términos de las filas y las columnas de la tabla de la operación del grupo G.

Ejemplos

Se exponen a continuación numerosos ejemplos de grupos concretos, el estudiante novato deberá considerarlos con detenimiento al objeto de ir adquiriendo el dominio de los conceptos más abstractos. Algunos de estos ejemplos se utilizarán posteriormente a fin de ilustrar los nuevos conceptos que se vayan introduciendo. Se hace un énfasis especial en la "tabla del grupo" como una forma de escribir explícitamente o representar la operación del grupo; obviamente, tal representación de la operación sólo es factible (humanamente) en los casos de grupos finitos de orden pequeño.

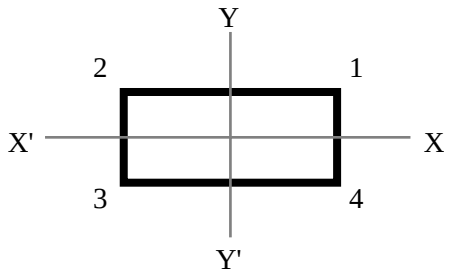
En todos los ejemplos tratados el estudiante debe poner especial atención en comprender cabalmente los dos ingredientes que intervienen en la construcción o definición de un grupo $G = (G, *)$:

- el conjunto G soporte del grupo, y
- la operación (binaria interna) $*$ definida en el conjunto G.

Para, a continuación, comprobar si se cumplen (o no) los "axiomas de grupo".

1. El grupo de las isometrías de un rectángulo.

Consideremos en un plano un rectángulo que no sea un cuadrado (esto es, que tenga dos lados de longitudes distintas). Las isometrías del plano que fijan el rectángulo (globalmente, no necesariamente punto a punto) son:



- La identidad: 1
- La simetría axial con respecto al eje X–X': h
- La simetría axial con respecto al eje Y–Y': v
- La simetría central con respecto al centro del rectángulo: s

La composición de dos isometrías del plano que fijan el rectángulo es a su vez una isometría que fija el rectángulo; se tiene así un conjunto $G = \{1, h, v, s\}$ y una operación (binaria interna) en él:

$$\begin{array}{ccc} G \times G & \to & G \\ (f, g) & \mapsto & f \circ g \end{array}$$

El conjunto G con esta operación es un grupo (el **grupo de las isometrías del rectángulo**); se muestra a la derecha la tabla que representa la operación. Este grupo se conoce usualmente con el nombre de **grupo de Klein** y se denota por K_4. El grupo K_4 es conmutativo y se tiene $|K_4| = 4$. (La conmutatividad se manifiesta en la simetría de la tabla con respecto a la diagonal "principal").

	1	h	v	s
1	1	h	v	s
h	h	1	s	v
v	v	s	1	h
s	s	v	h	1

2. Los grupos de raíces n-ésimas de la unidad.

Para cada entero positivo n consideremos el conjunto R_n de los números complejos z tales que $z^n = 1$. Por ejemplo:

$R_1 = \{1\}$.

$R_2 = \{1, -1\}$.

$$R_3 = \left\{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\right\}.$$

$R_4 = \{1, i, -1, -i\}$.

En general

$$R_n = \{\cos(2k\pi/n) + i\,\mathrm{sen}(2k\pi/n) \mid k \in \mathbf{Z},\ 0 \leq k < n\}, \quad (n = 1, 2, 3, \ldots).$$

Fijado n, si z_1 y z_2 pertenecen a R_n, entonces $(z_1 z_2)^n = z_1^n z_2^n = 1$, con lo que $z_1 z_2 \in R_n$; esto permite restringir la multiplicación en el cuerpo $\mathbf{C}$ de los complejos al subconjunto R_n:

$$\begin{array}{ccc} R_n \times R_n & \to & R_n \\ (z_1, z_2) & \mapsto & z_1 z_2 \end{array}$$

El conjunto R_n equipado con esta operación es un grupo conmutativo (compruébese), llamado el **grupo de las raíces n-ésimas de la unidad** en el cuerpo $\mathbf{C}$ de los números complejos.

En la tabla adjunta se representa la operación en el grupo

$$R_3 = \left\{1, \frac{-1+i\sqrt{3}}{2} = \alpha, \frac{-1-i\sqrt{3}}{2} = \beta\right\}$$

de las raíces cúbicas de la unidad.

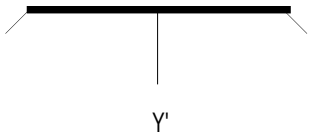
	1	α	β
1	1	α	β
α	α	β	1
β	β	1	α

En la tabla adjunta se representa la operación en el grupo $R_4 = \{1, i, -1, -i\}$ de las raíces cuartas de la unidad

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

3. El grupo de las isometrías de un cuadrado.

Consideremos un cuadrado en un plano. Las isometrías del plano que fijan el cuadrado son:



– La simetría axial con respecto al eje X–X': h
– La simetría axial con respecto al eje Y–Y': v
– La simetría axial con respecto al eje 1–3: d_1
– La simetría axial con respecto al eje 2–4: d_2

Pongamos $D_4 = \{1, g_1, g_2, g_3, h, v, d_1, d_2\}$; el conjunto D_4 junto con la operación de composición de transformaciones es un grupo: el **grupo diédrico** de grado 4. Se expone seguidamente la tabla de este grupo:

	1	g_1	g_2	g_3	h	v	d_1	d_2
1	1	g_1	g_2	g_3	h	v	d_1	d_2
g_1	g_1	g_2	g_3	1	d_1	d_2	v	h
g_2	g_2	g_3	1	g_1	v	h	d_2	d_1
g_3	g_3	1	g_1	g_2	d_2	d_1	h	v
h	h	d_2	v	d_1	1	g_2	g_3	g_1
v	v	d_1	h	d_2	g_2	1	g_1	g_3
d_1	d_1	h	d_2	v	g_1	g_3	1	g_2
d_2	d_2	v	d_1	h	g_3	g_1	g_2	1

4. Los grupos de permutaciones.

Para cada entero positivo n pongamos $I_n = \{i \in \mathbf{Z} \mid 1 \leq i \leq n\}$, y sea S_n el conjunto de las aplicaciones biyectivas de I_n en sí mismo:

$$S_n = \{\alpha \mid \alpha : I_n \to I_n,\ \alpha \text{ biyectiva}\}.$$

Si α, β son aplicaciones biyectivas de I_n en sí mismo, entonces la composición $\alpha \circ \beta$ es también una aplicación biyectiva de I_n en I_n; por tanto queda definida una operación (binaria interna) en el conjunto S_n:

$$\begin{array}{ccc} S_n \times S_n & \to & S_n \\ (\alpha, \beta) & \mapsto & \alpha \circ \beta \end{array}$$

donde

$$(\alpha \circ \beta)(i) = \alpha(\beta(i)),\ (i \in I_n).$$

El par $S_n = (S_n, \circ)$ es un grupo (compruébese), llamado el **grupo de las permutaciones** del conjunto I_n o el **grupo simétrico de grado** n. Se tiene $|S_n| = n!$. Examinemos con algún detalle el grupo S_3: hay exactamente $3! = 6$ permutaciones de I_3 que son:

$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\gamma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \gamma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \gamma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

La tabla del grupo simétrico S_3 es como sigue:

	1	α_1	α_2	γ_1	γ_2	γ_3
1	1	α_1	α_2	γ_1	γ_2	γ_3
α_1	α_1	α_2	1	γ_3	γ_1	γ_2
α_2	α_2	1	α_1	γ_2	γ_3	γ_1
γ_1	γ_1	γ_2	γ_3	1	α_1	α_2
γ_2	γ_2	γ_3	γ_1	α_2	1	α_1
γ_3	γ_3	γ_1	γ_2	α_1	α_2	1

Es fácil comprobar que los grupos S_1 y S_2 son conmutativos, mientras que S_n no es conmutativo si $n \geq 3$.

5. Los grupos lineales.

Sea k un cuerpo conmutativo (por ejemplo, el cuerpo $\mathbf{Q}$ de los números racionales ó cualquiera de los cuerpos $\mathbf{Z}_p$ con p primo) y sea n un entero positivo. Se denota $\mathrm{M}_n(k)$ el conjunto de las matrices cuadrdas $n \times n$ con coeficientes en k. Se denota $\mathrm{GL}_n(k)$ el conjunto de las matrices cuadradas $n \times n$ con coeficientes en k y de determinante distinto de cero (matrices regulares):

$$\mathrm{GL}_n(k) = \{A \in \mathrm{M}_n(k) \mid \det(A) \neq 0\}.$$

Dado que $\det(AB) = \det(A)\det(B)$, y que en todo cuerpo el producto de dos elementos no nulos es no nulo, la multiplicación en $\mathrm{M}_n(k)$ define (por restricción) una operación (binaria interna) en el conjunto $\mathrm{GL}_n(k)$:

$$\begin{array}{ccc} \mathrm{GL}_n(k) \times \mathrm{GL}_n(k) & \to & \mathrm{GL}_n(k) \\ (A, B) & \mapsto & AB \end{array}$$

El conjunto $\mathrm{GL}_n(k)$ equipado con esta operación es un grupo denominado el **grupo lineal de grado n sobre k.**

6. Los grupos aditivos de los anillos.

En todo anillo $A = (A,\ +,\ .)$ el par $(A, +)$ es (por definición de anillo) un grupo, denominado el **grupo aditivo del anillo** A. Ejemplos de tales grupos son

$(\mathbf{Z}, +)$, el grupo aditivo de los enteros;
$(\mathbf{Q}, +)$, el grupo aditivo de los racionales;
$(\mathbf{R}, +)$, el grupo aditivo de los reales;
$(\mathbf{C}, +)$, el grupo aditivo de los complejos;
$(\mathbf{Z}_m, +)$ para un entero $m \geq 0$, el grupo aditivo de los enteros módulo m. En la tabla adjunta se representa la operación del grupo aditivo del anillo $\mathbf{Z}_4$:

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

7. Los grupos de las unidades de los anillos.

En todo anillo $A = (A,\ +,\ .)$ el par $(\mathbf{U}(A), .)$, formado por el conjunto de las unidades del anillo A y la operación de multiplicación, es un grupo, denominado el **grupo de las unidades del anillo** A. Ejemplos de tales grupos son

$(\mathbf{U}(\mathbf{Z}),\ .) = (\{1, -1\}, .)$,
$(\mathbf{U}(\mathbf{Q}),\ .)$, el grupo multiplicativo de los racionales no nulos;
$(\mathbf{U}(\mathbf{R}),\ .)$, el grupo multiplicativo de los reales no nulos;
$(\mathbf{U}(\mathbf{C}),\ .)$, el grupo multiplicativo de los complejos no nulos;
$(\mathbf{U}(\mathbf{Z}_m),\ .)$ para un entero $m \geq 2$, el grupo multiplicativo de las unidades del anillo de los enteros módulo m.

Para $m = 12$, se tiene $\mathbf{U}(\mathbf{Z}_{12}) = \{1, 5, 7, 11\}$; en la tabla siguiente se representa la operación en el grupo multiplicativo $\mathbf{U}(\mathbf{Z}_{12})$:

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Para $m = 5$, se tiene $\mathbf{U}(\mathbf{Z}_5) = \{1, 2, 3, 4\}$; en la tabla siguiente se representa la operación en el grupo multiplicativo $\mathbf{U}(\mathbf{Z}_5)$:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Potencias y múltiplos

Definición. *Sea $G = (G, .)$ un grupo. Para cada elemento $a \in G$ y cada entero $n \in \mathbf{Z}$ la*

potencia de base a y exponente n, *denotada* a^n, *es*

$$a^n \begin{cases} = 1, & \text{si } n = 0, \\ = aa^{n-1}, & \text{si } n > 0, \\ = (a^{-1})^{-n}, & \text{si } n < 0. \end{cases}$$

Ejemplos

1 Si a es un elemento de un grupo multiplicativo G, entonces:

$$a^0 = 1,\ a^1 = a,\ a^2 = aa,\ a^3 = aaa,\ a^4 = aaaa,\ \ldots$$

$$a^{-1} = (a^{-1})^1,\ a^{-2} = (a^{-1})^2 = a^{-1}a^{-1},\ a^{-3} = (a^{-1})^3 = a^{-1}a^{-1}a^{-1},\ \ldots$$

2 Las potencias de i en el grupo R_4 de las raíces cuartas de la unidad son:

$$i^0 = 1,\ i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1,\ i^5 = i,\ i^6 = -1,\ i^7 = -i,\ \ldots$$

$$i^{-1} = -i,\ i^{-2} = -1,\ i^{-3} = i,\ i^{-4} = 1,\ i^{-5} = -i,\ \ldots$$

3 Sea

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Q}),$$

para todo entero n se tiene

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Ejercicio. Calcular potencias de diversos elementos de los grupos considerados en los ejemplos.

Proposición. *Para cualquier elemento a en un grupo G y enteros n, m arbitrarios se tienen:*

1. $a^n a^m = a^{n+m}$,
2. $(a^n)^m = a^{nm}$,
3. *Si b es un elemento de G que conmute con a, entonces* $(ab)^n = a^n b^n$.

Ejemplo. Sea k un cuerpo conmutativo ($k = \mathbf{Q}$, $k = \mathbf{Z}_2$, ...). Las matrices

$$a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{y} \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

tienen determinante 1 y -1, respectivamente; por consiguiente a y b pertenecen al grupo $\mathrm{GL}_2(k)$, y se cumplen las siguientes relaciones:

$$ab = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix},\ ba = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}.$$

Dado que $1 \neq 0$ en cualquier cuerpo, se tiene $ab \neq ba$. Además:

$$(ab)^2 = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} \quad \text{y} \quad a^2b^2 = \begin{pmatrix} 1 & 1 \\ 3 & 4 \end{pmatrix}.$$

Dado que $1 \neq 2$ en cualquier cuerpo (¿por qué?), se concluye que

$$(ab)^2 \neq a^2b^2.$$

Notación aditiva: múltiplos enteros.

Sea $G = (G, +)$ un grupo aditivo (y, por tanto, abeliano de acuerdo con el convenio establecido), se definen los **múltiplos enteros** na, $(n \in \mathbf{Z})$, de un elemento a de G en la forma:

$$na \begin{cases} = 0, & \text{si } n = 0, \\ = a + (n-1)a, & \text{si } n > 0, \\ = (-n)(-a), & \text{si } n < 0. \end{cases}$$

Proposición. *Para elementos cualesquiera a, b en un grupo aditivo G y enteros n, m arbitrarios se tienen:*

1. $(na) + (ma) = (n + m)a$,
2. $m(na) = (mn)a$,
3. $n(a + b) = (na) + (nb)$.

Subgrupos

Definición. *Un subconjunto H de un grupo G es un* **subgrupo** *de G si*

1. *la unidad de G pertenece a H; esto es, $1 \in H$;*
2. *el producto (en G) de todo par de elementos de H pertenece a H; esto es, para todo u, v, si $u, v \in H$, entonces $uv \in H$; y*
3. *el inverso (en G) de todo elemento de H pertenece a H; esto es, para todo u, si $u \in H$, entonces $u^{-1} \in H$.*

Ejemplos.

1. Los conjuntos $\{1\}$, $\{1, h\}$, $\{1, v\}$, $\{1, s\}$ y K_4 son (todos los) subgrupos del grupo de K_4 de las isometrías del rectángulo.
2. Los conjuntos $\{1\}$, $\{1, -1\}$ y R_4 son (todos los) subgrupos del grupo R_4 de las raíces cuartas de la unidad.
3. Los conjuntos $\{1\}$, $\{1, \gamma_1\}$, $\{1, \gamma_2\}$, $\{1, \gamma_3\}$, $\{1, \alpha_1, \alpha_2\}$ y S_3 son (todos los) subgrupos del grupo simétrico de grado 3: S_3.
4. Para cualquier entero positivo n y cualquier cuerpo (conmutativo) k, el conjunto

$$\mathrm{SL}_n(k) = \{A \in \mathrm{M}_n(k) \mid \det(A) = 1\}$$

es un subgrupo del grupo $\mathrm{GL}_n(k)$, llamado el **grupo lineal especial** (de grado n sobre el cuerpo k).

Es útil la siguiente caracterización de los subgrupos de un grupo cualquiera:

Proposición. *Un subconjunto H de un grupo G es un subgrupo de G si, y sólo si, se cumplen las dos propiedades siguientes*

1. *$H \neq \emptyset$ y*
2. *para todo $u, v \in H$ se tiene que $uv^{-1} \in H$.*

Demostración. Sea H un subgrupo de un grupo G; dado que $1 \in H$, se tiene $H \neq \emptyset$; si u, v son elementos de H, entonces v^{-1} pertenece a H y, por tanto, $uv^{-1} \in H$. Reciprocamente, sea H un subconjunto no vacío de un grupo G tal que para todo $u, v \in H$, $uv^{-1} \in H$; por ser $H \neq \emptyset$ hay, al menos, un elemento $x \in H$, por tanto $1 = xx^{-1} \in H$; si $u \in H$, entonces $u^{-1} = 1.u^{-1} \in H$; finalmente, si $u, v \in H$, entonces se tendrá $u, v^{-1} \in H$, de donde $uv = u(v^{-1})^{-1} \in H$.

Ejercicio. Escribir la definición de subgrupo y el enunciado de la proposición anterior utilizando notación aditiva.

Nótese que para cualquier grupo G, los conjuntos $\{1\}$ y G son subgrupos de G.

Sea H un subgrupo de un grupo G. La operación en G

$$\begin{array}{ccc} G \times G & \to & G \\ (a, b) & \mapsto & a.b \end{array}$$

se restringe a una operación en el subconjunto H en la forma

$$\begin{array}{ccc} H \times H & \to & H \\ (u, v) & \mapsto & u.v \ ; \end{array}$$

y H (con esta operación) es un grupo (¿por qué?). Por consiguiente, todo subgrupo de un grupo es asimismo un grupo.

Estructura de los subgrupos de Z

Es posible describir todos los subgrupos del grupo aditivo $\mathbf{Z} = (\mathbf{Z}, +)$ de los enteros: Si m es un entero, entonces el conjunto

$$(m) = m\mathbf{Z} = \{mz \mid z \in \mathbf{Z}\}$$

es un subgrupo de $\mathbf{Z}$ (La demostración de esta afirmación es sencilla y se deja como ejercico). Recíprocamente:

Proposición. *Si H es un subgrupo del grupo aditivo $\mathbf{Z}$ de los enteros, entonces hay un único entero $m \geq 0$ tal que $H = m\mathbf{Z}$. Si $H = \{0\}$, entonces $m = 0$; si $H \neq \{0\}$, entonces m es el menor entero positivo en H.*

Demostración. Suponer $H \neq \{0\}$, de modo que hay elementos no nulos en H, sea $h \in H, h \neq 0$; dado que H es un subgrupo de $\mathbf{Z}$, se tendrá que el opuesto $-h$ de h pertenece a H; en consecuencia hay enteros positivos en H; sea m el menor entero positivo en H y veamos que $H = m\mathbf{Z}$. Obviamente, $m\mathbf{Z} \subseteq H$ (¿por qué?). Veamos la otra inclusión: Si h es cualquier elemento de H, entonces (por la propiedad de la división) hay enteros q, r tales que

$$h = mq + r, \quad \text{y} \quad 0 \leq r < m.$$

Dado que $h, mq \in H$, se tiene que $r \in H$; como m es (por elección) el menor entero positivo en H, debe ser $r = 0$, de donde $h = mq \in m\mathbf{Z}$. Esto prueba que $H \subseteq m\mathbf{Z}$. en consecuencia, $H = m\mathbf{Z}$. Finalmente, si m, n son enteros no negativos tales que $m\mathbf{Z} = n\mathbf{Z}$, entonces debe ser $m = n$ (¿demostración?).

Notas.

- Un subconjunto H de $\mathbf{Z}$ es un subgrupo del grupo aditivo $\mathbf{Z}$ si, y sólo si, H es un ideal del anillo $\mathbf{Z}$; es decir, los subgrupos de $\mathbf{Z}$ son exactamente los ideales del anillo $\mathbf{Z}$.
- Hay una biyección entre el conjunto $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$ de los números naturales y el conjunto $\mathcal{S}(\mathbf{Z})$ de los subgrupos del grupo aditivo $\mathbf{Z} = (\mathbf{Z}, +)$ de los enteros:

$$\begin{array}{ccccc} \varphi & : & \mathbf{N} & \to & \{H \mid H \text{ subgrupo de } \mathbf{Z}\} \\ & & m & \mapsto & \varphi(m) = m\mathbf{Z} \end{array}$$

  ¿Por qué es la aplicación φ inyectiva? ¿Por qué es suprayectiva? Como se verá, esta biyección φ establece un *"isomorfismo"* entre el conjunto ordenado $(\mathbf{N}, |)$ de los

números naturales con la relación "divide a" y el conjunto ordenado $(\mathcal{S}(\mathbf{Z}), \subseteq)$ de los subgrupos de $\mathbf{Z}$ con la relación de inclusión.

Definición. *Un entero a es* **múltiplo** *de un entero d si hay un entero b tal que $a = db$; en este caso también se dice que d es* **divisor** *de a.*

Dados dos enteros d y a, la relación "d es divisor de a" se escribe $d \,|\, a$; y la relación "d no es divisor de a" se escribe $d \not| \, a$. El conjunto de todos los múltiplos de un entero dado m es el conjunto

$$m\mathbf{Z} = (m) = \{mz \mid z \in \mathbf{Z}\}$$

Por tanto la relación "d es divisor de a", equivalente a la relación "a es múltiplo de d", se puede espresar $a \in d\mathbf{Z}$. Nótese que el conjunto de los múltiplos de 0 es $0\mathbf{Z} = \{0\}$ y que el conjunto $m\mathbf{Z}$ de los múltiplos de un entero $m \neq 0$ es infinito. Todo divisor de un entero $a \neq 0$ está comprendido entre $-|a|$ y $|a|$; por tanto el conjunto de todos los divisores de un entero $a \neq 0$ es finito.

Ejemplos.

1 Los números enteros 6, 18, -24, 740740734 son múltiplos de 6. Se tiene
$6 = 6 \times 1 \in 6\mathbf{Z}$
$18 = 6 \times 3 \in 6\mathbf{Z}$
$-24 = 6 \times (-4) \in 6\mathbf{Z}$
$740740734 = 6 \times 123456789 \in 6\mathbf{Z}$
El entero 20 no es múltiplo de 6.

2 Los números enteros -2, 3, 4, -6 y 12 son divisores de 12. El entero 8 no es divisor de 12.
$-2 \,|\, 12, \quad 3 \,|\, 12, \quad 4 \,|\, 12, \quad -6 \,|\, 12, \quad 12 \,|\, 12, \quad 8 \not| \, 12.$

3 Se tiene

$$1 \,|\, 7, \quad 7 \,|\, 7, \quad -1 \,|\, 7, \quad \text{y} \quad -7 \,|\, 7;$$

y si un entero d es un divisor de 7 entonces $d = 1$, ó $d = 7$, ó $d = -1$ ó $d = -7$. Por tanto el conjunto de todos los divisores de 7 es $\{1, 7, -1, -7\}$

4 El conjunto de todos los divisores de 12 es

$$\{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$$

Proposición. *Sean m y n números enteros. Son equivalentes:*
(1.) *n es múltiplo de m*
(2.) $m \,|\, n$
(3.) $n \in m\mathbf{Z}$
(4.) $n\mathbf{Z} \subseteq m\mathbf{Z}$

Demostración. Es sencilla y se deja como ejercicio.

Dados dos subgrupos $a\mathbf{Z}$ y $b\mathbf{Z}$ del grupo aditivo $\mathbf{Z} = (\mathbf{Z}, +)$ de los enteros, pongamos

$$a\mathbf{Z} + b\mathbf{Z} = \{ax + by \mid x, y \in \mathbf{Z}\}$$

de modo que $a\mathbf{Z} + b\mathbf{Z}$ es el conjunto de todos los enteros que se pueden expresar como suma de un elemento de $a\mathbf{Z}$ y de un elemento de $b\mathbf{Z}$. Por ejemplo, poniendo $a = 12$ y $4b = 8$,

$$12\mathbf{Z} + 8\mathbf{Z} = \{12x + 8y \mid x, y \in \mathbf{Z}\} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$$

Proposición. *Sean $a\mathbf{Z}$ y $b\mathbf{Z}$ subgrupos del grupo aditivo de los enteros. Se cumplen las siguientes propieaddes:*

1. $a\mathbf{Z} + b\mathbf{Z}$ *es un subgrupo de* $\mathbf{Z}$.
2. $a\mathbf{Z} \subseteq a\mathbf{Z} + b\mathbf{Z} \quad y \quad b\mathbf{Z} \subseteq a\mathbf{Z} + b\mathbf{Z}$
3. *Si $c\mathbf{Z}$ es un subgrupo de $\mathbf{Z}$ tal que $a\mathbf{Z} \subseteq c\mathbf{Z} \quad y \quad b\mathbf{Z} \subseteq c\mathbf{Z}$, entonces*

$$a\mathbf{Z} + b\mathbf{Z} \subseteq c\mathbf{Z}$$

Demostración.

1. Sean $ax_1 + by_1, ax_2 + by_2$ elementos de $a\mathbf{Z} + b\mathbf{Z}$ con $ax_1, ax_2 \in a\mathbf{Z}$ y $by_1, by_2 \in b\mathbf{Z}$. Se cumple

   $$(ax_1 + by_1) + (ax_2 + by_2) = (ax_1 + ax_2) + (by_1 + by_2) \in a\mathbf{Z} + b\mathbf{Z}$$

   Además,

   $$0 = a \times 0 + b \times 0 \in a\mathbf{Z} + b\mathbf{Z}$$

   Finalmente, si $ax + by$ es un elemento de $a\mathbf{Z} + b\mathbf{Z}$, con $ax \in a\mathbf{Z}$ y $bx \in b\mathbf{Z}$, entonces

   $$-(ax + by) = -ax - by \in a\mathbf{Z} + b\mathbf{Z}$$

   En consecuencia $a\mathbf{Z} + b\mathbf{Z}$ es un subgrupo de $\mathbf{Z}$.
2. La relación $ax = ax + b0 \in a\mathbf{Z} + b\mathbf{Z}$, válida para todo $x \in \mathbf{Z}$, prueba que $a\mathbf{Z} \subseteq a\mathbf{Z} + b\mathbf{Z}$. Análogamente se prueba $b\mathbf{Z} \subseteq a\mathbf{Z} + b\mathbf{Z}$
3. Demostración trivial. ∎

Definición. *Dados dos subgrupos $a\mathbf{Z}$ y $b\mathbf{Z}$ del grupo aditivo $\mathbf{Z}$ de los enteros, el subgrupo*

$$a\mathbf{Z} + b\mathbf{Z} = \{ax + by \mid x, y \in \mathbf{Z}\}$$

se denomina la **suma de los subgrupos** *$a\mathbf{Z}$ y $b\mathbf{Z}$.*

Dados dos enteros a y b hay un único entero $d \geq 0$ tal que

$$a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$$

El subgrupo suma, $d\mathbf{Z}$, es el menor subgrupo de $\mathbf{Z}$ que contiene a los subgrupos $a\mathbf{Z}$ y $b\mathbf{Z}$. Con mayor detalle:

1. $d\mathbf{Z}$ es un subgrupo de $\mathbf{Z}$
2. $a\mathbf{Z} \subseteq d\mathbf{Z}$ y $b\mathbf{Z} \subseteq d\mathbf{Z}$
3. Si $c\mathbf{Z}$ es un subgrupo de $\mathbf{Z}$ y $a\mathbf{Z} \subseteq c\mathbf{Z}$ y $b\mathbf{Z} \subseteq c\mathbf{Z}$, entonces $d\mathbf{Z} \subseteq c\mathbf{Z}$.

Ha quedado probado que dados dos enteros a y b hay un único entero $d \geq 0$ que cumpla las dos propieaddes siguientes:

(a) $d \,|\, a$ y $d \,|\, b$, y
(b) si c es un entero y $c \,|\, a$ y $c \,|\, b$, entonces $c \,|\, d$.

Se dice que d es el **máximo común divisor** de a y b.

Subgrupo engendrado por un subconjunto.

Una propiedad simple pero especialmente importante es que la intersección de cualquier colección de subgrupos de un grupo G es un subgrupo de G:

Proposición. *Sea $(H_i)_{i\in I}$ una familia de subgrupos de un grupo G, entonces el conjunto $\bigcap_{i\in I} H_i$ es un subgrupo de G.*

Demostración. Trivial y se deja como ejercicio.

La intersección $H = \bigcap_{i\in I} H_i$ de una familia $(H_i)_{i\in I}$ de subgrupos de un grupo G posee entonces las siguientes propiedades:

- H es un subgrupo de G,
- $H \subseteq H_i$, para todo $i \in I$, y
- si K es un subgrupo de G y $K \subseteq H_i$, para todo $i \in I$, entonces $K \subseteq H$.

Es decir, la intersección H de la familia $(H_i)_{i\in I}$ es el mayor subgrupo de G contenido en cada uno de los miembros H_i de la familia dada.

Por otra parte, sea X un subconjunto de un grupo G; consideremos la colección $\mathcal{F}(X)$ de los subgrupos H de G tales que $X \subseteq H$:

$$\mathcal{F}(X) = \big\{H \mid H \text{ subgrupode } G,\ X \subseteq H\big\}.$$

La intersección $\langle X\rangle = \bigcap_{H\in\mathcal{F}(X)} H$ de la familia $\mathcal{F}(X)$ cumple las siguientes propiedades:

- $\langle X\rangle$ es un subgrupo de G,
- $X \subseteq \langle X\rangle$, y
- si K es un subgrupo de G y $X \subseteq K$, entonces $\langle X\rangle \subseteq K$.

Es decir, $\langle X\rangle$ es el menor subgrupo de G que contiene a X. Se dice que $\langle X\rangle$ es el **subgrupo de G engendrado por el subconjunto** X de G. ¿Cómo son los elementos del subgrupo $\langle X\rangle$? Dado que $X \subseteq \langle X\rangle$, todo elemento $x \in X$ pertenece a $\langle X\rangle$; además, puesto que $\langle X\rangle$ es un (sub)grupo, deberán pertenecer a él todos los inversos x^{-1} (en el grupo G) de

los elementos $x \in X$, y todos los productos (finitos) cuyos factores sean elementos de X o inversos de elementos de X; por tanto deberá tenerse

$$x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_r}^{\varepsilon_r} \in \langle X \rangle, \text{ para todo } x_{\alpha_i} \in X; \text{ para todo } \varepsilon_i \in \{1, -1\}; \ i = 1, \dots, r; \ r \in \mathbf{N}.$$

Ahora bien, el conjunto de todos los productos anteriores es un subgrupo de G que contiene a X (¿demostración?); en consecuencia

$$\langle X \rangle = \{x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_r}^{\varepsilon_r} \mid x_{\alpha_i} \in X; \ \varepsilon_i \in \{1, -1\}; \ i = 1, \dots, r; \ r \in \mathbf{N}\}.$$

Si X es un subconjunto finito de un grupo G, digamos $X = \{x_1, x_2, \dots, x_n\}$, entonces se usará la notación $\langle x_1, x_2, \dots, x_n \rangle$ en lugar de $\langle \{x_1, x_2, \dots, x_n\} \rangle$.

Ejemplos.

1 En el grupo K_4 de las isometrías de un rectángulo se tienen:

$$\langle h \rangle = \{1, h\};$$

$$\langle v, h \rangle = K_4;$$

$$\langle v, s \rangle = K_4.$$

Probar que si X es un subconjunto de K_4 y $\langle X \rangle = K_4$, entonces X posee, al menos, dos elementos.

2 Para el grupo R_4 de las raíces cuartas de la unidad se tiene

$$\langle -1 \rangle = \{1, -1\};$$

$$R_4 = \langle i \rangle = \langle -i \rangle.$$

3 En el grupo simétrico de grado 3: S_3, se cumplen:

$$\langle \gamma_1 \rangle = \{1, \gamma_1\};$$

$$\langle \alpha_2 \rangle = \{1, \alpha_1, \alpha_2\};$$

$$\langle \alpha_1, \alpha_2 \rangle = \{1, \alpha_1, \alpha_2\};$$

$$\langle \gamma_1, \gamma_2, \gamma_3 \rangle = S_3.$$

Grupos Cíclicos.

Una clase particularmente simple e importante de grupos está constituida por los grupos que poseen un sistema generador formado por un único elemento; estudiemos con algún detalle estos grupos.

Definición. *Un grupo G es* **cíclico** *si hay un elemento $a \in G$ tal que $G = \langle a \rangle$. En este caso se dice que a es un* **generador** *de G.*

Si G es un grupo cíclico con generador a, entonces $G = \{a^n \mid n \in \mathbf{Z}\}$; esto es, todo elemento de G es una potencia de a y, por tanto, el grupo G es abeliano. Si el grupo G es aditivo, entonces $G = \{na \mid n \in \mathbf{Z}\}$.

Ejemplos.

1. El grupo R_4 de las raíces cuartas de la unidad es cíclico con i como generador. También $-i$ es un generador de R_4. En general, para todo entero positivo n, el grupo R_n de las raíces n-ésimas de la unidad es cíclico y cualquier raíz primitiva n-ésima de la unidad es un generador de R_n.
2. El grupo (aditivo) $\mathbf{Z}$ es cíclico con 1 como generador, -1 es también un generador de $\mathbf{Z}$. Cualquier subgrupo $m\mathbf{Z}$ de $\mathbf{Z}$ es cíclico con m como generador.
3. El grupo de Klein K_4 no es cíclico.
4. El grupo diédrico de grado 4, D_4, no es cíclico (porque no es abeliano).

Sea G un grupo cíclico con generador a: $G = \langle a \rangle$; la aplicación $p_a : \mathbf{Z} \to G$, tal que $p_a(n) = a^n$, $(n \in \mathbf{Z})$, es suprayectiva. Al considerar las potencias de a se presenta una alternativa:

1: existen enteros i, j, $i \neq j$, tales que $a^i = a^j$ (esto es, p_a no es inyectiva); ó bien,
2: $a^i \neq a^j$, para todo $i, j \in \mathbf{Z}$, $i \neq j$ (esto es, p_a es inyectiva y, por tanto, biyectiva).

Estudiemos separadamente estas dos posibilidades.

Caso 1: Si existen enteros i, j distintos (digamos $i > j$) tales que $a^i = a^j$, entonces $a^{i-j} = 1$; por tanto hay algún entero $m > 0$ tal que $a^m = 1$. Sea n el menor entero positivo que cumpla $a^n = 1$, entonces las potencias $a^0 = 1$, $a^1 = a$, $a^2, \ldots$, a^{n-1} son distintas dos a dos: pues si r, s son enteros, $0 \leq r \leq s \leq n-1$, tales que $a^s = a^r$, entonces $a^{s-r} = 1$ y $s - r < n$, luego debe ser $s - r = 0$, esto es, $s = r$. Además, si a^i es un elemento de $G = \langle a \rangle$, poniendo $i = nq + r$ con $q, r \in \mathbf{Z}$ y $0 \leq r < n$, resulta $a^i = a^{nq+r} = (a^n)^q a^r = a^r$. En consecuencia $G = \langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$, y estos elementos son distintos dos a dos. En este caso se dice que el **orden** de a es n y se pone $o(a) = n$.

Caso 2: Si $a^i \neq a^j$ siempre que $i \neq j$, entonces la aplicación suprayectiva p_a es, además, inyectiva; por tanto p_a es biyectiva, y el grupo cíclico G es infinito. En este caso se dice que el **orden** de a es infinito y se pone $o(a) = \infty$.

Ejemplos.

1. Considerar la matriz
$$C = \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Q}).$$
Se tienen
$$C^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ C^3 = \begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix} \text{ y } C^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Por tanto C es de orden finito: $o(C) = 4$ y se tiene

$$\langle C\rangle = \{I_2, C, C^2, C^3\}.$$

2. La matriz

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Q})$$

es de orden infinito ya que, para todo entero n,

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Ejercicio. Considerar en el grupo $\mathrm{GL}_2(\mathbf{Q})$ las matrices

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ y } B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

Calcular los órdenes $o(A)$, $o(B)$ y $o(AB)$.

Proposición. *Sea $G = \langle a\rangle$ un grupo cíclico finito de orden n. Un elemento a^j de G es un generador de G si, y sólo si,* $\mathrm{mcd}(n, j) = 1$*; (esto es, si, y sólo si, los enteros n y j son primos entre sí).*

Demostración. Suponer que j es un entero tal que a^j es un generador de G; entonces hay un entero s tal que

$$a = (a^j)^s = a^{js};$$

multiplicando por el inverso de a, a^{-1}, queda

$$a^{js-1} = 1$$

Por tanto n (el orden de a) es un divisor del entero $js - 1$, con lo que hay un entero t que cumple

$$nt = js - 1$$

de donde se concluye que los enteros n y j son primos entre sí.

Recíprocamente, suponer que $\mathrm{mcd}(n, j) = 1$; por la propiedad de Bezout hay enteros u y v tales

$$nu + jv = 1$$

Se tiene entonces

$$a = a^1 = a^{nu+jv} = (a^n)^u (a^j)^v = (a^j)^v$$

Por tanto, para todo $i \in \mathbf{Z}$,

$$a^i = (a^j)^{vi}$$

con lo que $G = \langle a^j\rangle$. ∎

Clases Módulo un Subgrupo. El Teorema de Lagrange.

Un subgrupo H de un grupo $G = (G, .)$ determina en el conjunto G las relaciones $\mathcal{R}_i$ y $\mathcal{R}_d$ definidas en la forma siguiente: cualesquiera que sean $a, b \in G$, pondremos

$a\mathcal{R}_i b$ si, y sólo si, $a^{-1}b \in H$, y
$a\mathcal{R}_d b$ si, y sólo si, $ab^{-1} \in H$.

Veamos que $\mathcal{R}_i$ es una relación de equivalencia en G:

- Para todo $a \in G$ se tiene: $a^{-1}a = 1 \in H$, por tanto $a\mathcal{R}_i a$.
- Si $a, b \in G$ cumplen $a\mathcal{R}_i b$, entonces $a^{-1}b \in H$ y, como el inverso de cualquier elemento de H pertenece a H, se obtiene $b^{-1}a \in H = (a^{-1}b)^{-1} \in H$; esto es, $b\mathcal{R}_i a$.
- Si $a, b, c \in G$ cumplen $a\mathcal{R}_i b$ y $b\mathcal{R}_i c$, entonces $a^{-1}b \in H$ y $b^{-1}c \in H$; dado que el producto de dos elementos de H pertenece a H, se obtiene $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$; esto es, $a\mathcal{R}_i c$.

Ejercicio. Probar que $\mathcal{R}_d$ es una relación de equivalencia en G.

Sea H un subgrupo de un grupo G y sea a un elemento de G ¿Cómo es la clase de equivalencia de a respecto de la relación de equivalencia $\mathcal{R}_i$ determinada por H en G? Para que un elemento x de G pertenezca a la clase $[a]_{\mathcal{R}_i}$ de a es necesario y suficiente que $a\mathcal{R}_i x$ que, a su vez, equivale a $a^{-1}x \in H$. En consecuencia,

$$x \in [a]_{\mathcal{R}_i} \text{ si, y sólo si, } x = ah \text{ para algún } h \in H;$$

por tanto

$$[a]_{\mathcal{R}_i} = \{ah \mid h \in H\}.$$

Se tiene así una descripción explícita de los elementos de las clases de equivalencia en G módulo $\mathcal{R}_i$.

Ejercicio. Probar que

$$[a]_{\mathcal{R}_d} = \{ha \mid h \in H\}.$$

Notación. Para cualquier subconjunto S de un grupo G y para cualquier elemento $a \in G$, se pone

$$aS = \{as \mid s \in S\} \text{ y } Sa = \{sa \mid s \in S\}.$$

Definición. *Sea H un subgrupo de un grupo G y sea a un elemento de G. La clase de equivalencia $[a]_{\mathcal{R}_i} = aH$ de a con respecto a la relación de equivalencia $\mathcal{R}_i$ se denomina la* **clase a izquierda de** a **módulo** H. *La clase de equivalencia $[a]_{\mathcal{R}_d} = Ha$ de a con respecto a la relación de equivalencia $\mathcal{R}_d$ se denomina la* **clase a derecha de** a **módulo** H.

Se denota G/H al conjunto cociente $G/\mathcal{R}_i$, de modo que $G/H = \{aH \mid a \in G\}$, el conjunto de las distintas clases a izquierda (en G) módulo (el subgrupo) H. Se denota $H\backslash G$ al conjunto cociente $G/\mathcal{R}_d$, de modo que $H\backslash G = \{Ha \mid a \in G\}$, el conjunto de las

distintas clases a derecha (en G) módulo (el subgrupo) H. Nótese que para cualesquiera $a, b \in G$ se tiene:

$$aH = bH \iff a^{-1}b \in H \iff b^{-1}a \in H,$$

y

$$Ha = Hb \iff ba^{-1} \in H \iff ab^{-1} \in H.$$

Ejemplo. En el grupo simétrico de grado 3, S_3, consideremos el subgrupo $H = \{1, \alpha_1, \alpha_2\}$.

Las clases a izquierda módulo H:	Las clases a derecha módulo H:
$1H = \{1, \alpha_1, \alpha_2\} = \alpha_1 H = \alpha_2 H$	$H1 = \{1, \alpha_1, \alpha_2\} = H\alpha_1 = H\alpha_2$
$\gamma_1 H = \{\gamma_1, \gamma_2, \gamma_3\} = \gamma_2 H = \gamma_3 H$	$H\gamma_1 = \{\gamma_1, \gamma_2, \gamma_3\} = H\gamma_2 = H\gamma_3$

Como se puede observar, en éste grupo y para el subgrupo dado H, cada clase a izquierda coincide con su correspondiente clase a derecha: $aH = Ha$ para todo $a \in S_3$. Por consiguiente, en este caso, $\mathcal{R}_i = \mathcal{R}_d$.

Ejemplo. En el grupo simétrico de grado 3, S_3, consideremos ahora el subgrupo $K = \{1, \gamma_1\}$.

Las clases a izquierda módulo K:	Las clases a derecha módulo K:
$1K = \{1, \gamma_1\} = \gamma_1 K$	$K1 = \{1, \gamma_1\} = K\gamma_1$
$\alpha_2 K = \{\gamma_2, \alpha_2\} = \gamma_2 K$	$K\alpha_2 = \{\gamma_2, \alpha_1\} = K\gamma_1$
$\alpha_3 K = \{\gamma_3, \alpha_1\} = \gamma_1 K$	$K\alpha_3 = \{\gamma_3, \alpha_2\} = K\gamma_2$

En este caso se tiene $\gamma_2 K \neq K\gamma_2$, y $\gamma_3 K \neq K\gamma_3$.

Sea H un subgrupo de un grupo G y sea a un elemento de G. La aplicación

$$\begin{array}{rccc} \tau_a^i & : & H & \to & aH \\ & & h & \mapsto & ah \end{array}$$

es biyectiva (demostración trivial); por tanto H es finito si, y sólo si, la clase a izquierda $aH, a \in G$, es finita y, en este caso, el número de elementos $|H|$ de H coincide con el número de elementos $|aH|$ de cualquier clase a izquierda en G módulo H: $|H| = |aH|\,,\ (a \in G)$. En consecuencia, todas las clases a izquierda módulo H poseen el mismo cardinal, que coincide con el cardinal del subgrupo H:

$$|aH| = |bH| = \ldots = |H|\,, \quad (a, b, \ldots \in G).$$

Ejercicio. Considerando la aplicación

$$\begin{array}{rccc} \tau_a^d & : & H & \to & Ha \\ & & h & \mapsto & ha \end{array}$$

concluir que todas las clases a derecha módulo el subgrupo H poseen el mismo cardinal, que coincide con el cardinal de H.

Como se ha visto la relación $\mathcal{R}_i$ determinada en un grupo G por un subgrupo H es de equivalencia, por tanto G es la unión disjunta de las distintas clases a izquierda módulo H:

$$G = \bigcup_{a \in G} aH \quad \text{(unión disjunta)} .$$

Analogamente, la relación $\mathcal{R}_d$ determinada en G por H, origina una partición de G en clases a derecha módulo H:

$$G = \bigcup_{a \in G} Ha \quad \text{(unión disjunta)} .$$

Ejercicio. Sea H un subgrupo de un grupo G. Consideremos el conjunto G/H de las clases a izquierda módulo H, y el conjunto $H\backslash G$ de las clases a derecha módulo H.

1. Probar que la aplicación
$$\begin{array}{ccc} G/H & \to & H\backslash G \\ aH & \mapsto & Ha^{-1} \end{array}$$
(está bien definida y) es biyectiva. Concluir que el cardinal del conjunto cociente G/H coincide con el cardinal del conjunto cociente $H\backslash G$:
$$|G/H| = |H\backslash G| .$$
2. Quizá pueda extrañar la forma de definir la aplicación en el apartado anterior de éste ejercicio ¿Qué ocurre si se pretende *definir* la aplicación en la forma
$$\begin{array}{ccc} G/H & \to & H\backslash G \\ aH & \mapsto & Ha \ ? \end{array}$$

Definición. *Sea H un subgrupo de un grupo G. El* **índice** *de H en G es el cardinal de G/H (que, según el ejercicio precedente, coincide con el cardinal de $H\backslash G$). Se pone*

$$|G : H| = |G/H| = |H\backslash G| .$$

Suponer que H es un subgrupo de un grupo finito G, entonces H es finito y el índice en G de H es también finito. Sea T un sistema completo de representantes de las clases a izquierda de H en G, de modo que si $T = \{t_1, t_2, \ldots, t_s\}$, entonces

$$G = t_1H \cup t_2H \cup \ldots \cup t_sH$$

y

$$t_iH \cap t_jH = \emptyset, \quad \text{si } i \neq j, \ \big(i, j \in \{1, 2, \ldots, s\}\big).$$

Por tanto,

$$|G| = |t_1H| + |t_2H| + \ldots + |t_sH| = |H| + |H| + \ldots + |H| = s\,|H|$$

Se ha probado así un resultado central en la teoría de grupos finitos:

Teorema (Lagrange)**.** *Si H es un subgrupo de un grupo finito G, entonces*

$$|G| = |G : H|\,|H|\,.$$

En particular:

Corolario. *Si H es un subgrupo de un grupo finito G, entonces el orden de H y el índice en G de H son divisores del orden de G.*

Si G es un grupo finito de orden primo p: $o(G) = p$, entonces los únicos subgrupos de G son $\{1\}$ y G; si a es un elemento de G, $a \neq 1$, entonces el subgrupo de G engendrado por a debe ser el propio G; esto es, $\langle a \rangle = G$. Por tanto G es cíclico (y, en particular, abeliano) y cualquier elemento de G distinto de la unidad es un generador de G.

Corolario. *Todo grupo finito G de orden primo es cíclico y cualquier elemento de G distinto de la unidad es un generador de G.*

Corolario. *Sea G un grupo finito, sea $n = |G|$. Para todo $a \in G$ se tiene $a^n = 1$.*

Demostración. Considerar el subgrupo de G engendrado por a.