





Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0).

Eres libre de compartir y redistribuir el contenido de esta obra en cualquier medio o formato, siempre y cuando des el crédito adecuado a los autores originales y no persigas fines comerciales.

# Álgebra II

Los Del DGIIM, losdeldgiim.github.io José Juan Urrutia Milán

## Índice general

1.	Grupos: definición, generalidades y ejemplos	5
	1.1. Grupos diédricos	12

Álgebra II Índice general

En Álgebra I el objeto principal de estudio fueron los anillos conmutativos, conjuntos en los que teníamos definidas dos operaciones, una usualmente denotada con notación aditiva y otra con notación multiplicativa.

Posteriormente, el estudio se centró en los dominios de integridad (DI), anillos conmutativos donde teníamos más propiedades con las que manejar nuestros elementos (como la tan característica propiedad cancelativa). Después, el objeto de estudio fueron los dominios euclídeos (DE), donde ya podíamos realizar un estudio sobre la divisibilidad de los elementos del conjunto.

Finalmente, nos centramos en los dominios de factorización única (DFU), donde realizamos una breve introducción a la irreducibilidad de los polinomios.

En esta asignatura el principal objeto de estudio serán los grupos, conjuntos en los que hay definida una sola operación que entendemos por "buena<sup>1</sup>". Por tanto, los grupos serán estructuras menos restrictivas que los anillos conmutativos, aunque su estudio no será menos interesante.

<sup>&</sup>lt;sup>1</sup>La operación cumplirá ciertas propiedades deseables.

## 1. Grupos: definición, generalidades y ejemplos

Comenzamos realizando la primera definición necesaria para entender el concepto de grupo, que es entender qué es una operación dentro de un conjunto.

**Definición 1.1** (Operación binaria). Sea G un conjunto, una operación binaria en G es una aplicación

$$\begin{array}{cccc} *: & G \times G & \longrightarrow & G \\ & (a,b) & \longmapsto & a*b \end{array}$$

Ejemplo. Ejemplos de operaciones binarias sobre conjuntos que ya conocemos son:

- 1. La suma y el producto de números en  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ .
- 2. Dado un conjunto X, los operadores  $\cap$  y  $\cup$  son operaciones binarias sobre el conjunto  $\mathcal{P}(X)$ .

**Definición 1.2** (Grupo). Un grupo es una tripleta (G, \*, e) donde G es un conjunto no vacío, \* es una operación binaria en G y e es un elemento destacado de G de forma que se verifica:

i) La propiedad asociativa de \*:

$$(x*y)*z = x*(y*z) \quad \forall x, y, z \in G$$

ii) La existencia de un elemento neutro (el elemento destacado de G):

$$\exists e \in G \mid e * x = x \qquad \forall x \in G$$

iii) La existencia de un elemento simétrico para cada elemento de G:

$$\forall x \in G \quad \exists x' \in G \mid x' * x = e$$

Si además se cumple:

iv) La propiedad conmutativa de \*:

$$x * y = y * x \quad \forall x, y \in G$$

Entonces, diremos que (G, \*, e) es un grupo conmutativo o abeliano.

**Notación.** Para una mayor comodidad a la hora de manejar grupos, introducimos las siguientes notaciones:

- 1. Cuando dado un conjunto no vacío G sepamos por el contexto a qué grupo (G, \*, e) nos estamos refiriendo, indicaremos simplemente G (o en algunos casos (G, \*), para hacer énfasis en la operación binaria) para referirnos al grupo (G, \*, e).
- 2. En algunos casos, usaremos (por comodidad) la notación multiplicativa de los grupos. De esta forma, dado un grupo  $(G, \cdot, 1)$ , en ciertos casos notaremos la operación binaria  $\cdot$  simplemente por yuxtaposición:

$$x \cdot y = xy \qquad \forall x, y \in G$$

Además, nos referiremos al elemento neutro como "uno" y al simétrico de cada elemento como "inverso", sustituyendo la notación de x' por la de  $x^{-1}$ .

3. Otra notación que también usaremos (aunque de forma menos frecuente que la multiplicativa) será la aditiva. Dado un grupo (G, +, 0), nos referiremos al elemento neutro como "cero" y al simétrico de cada elemento como "opuesto", sustituyendo la notación de x' por la de -x.

Ejemplo. Ejemplos de grupos que se usarán con frecuencia en la asignatura son:

- 1.  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  con su respectiva suma son grupos abelianos.
- 2.  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$ ,  $\mathbb{C}^*$  con su respectivo producto son grupos abelianos.

Notemos la importancia de eliminar el 0 de cada conjunto para que todo elemento tenga inverso, así como que  $\mathbb{Z}^*$  no es un grupo, ya que el inverso de cada elemento (para el producto al que estamos acostumbrados) no está dentro de  $\mathbb{Z}^*$ .

- 3.  $\{1,-1,i,-i\}\subseteq\mathbb{C}$  con el producto heredado¹ de  $\mathbb{C}$  también es un grupo abeliano.
- 4.  $(\mathcal{M}_2(\mathbb{R}), +)$  es un grupo abeliano.
- 5. El grupo lineal de orden 2 con coeficientes en  $\mathbb{R}$ :

$$GL_2(\mathbb{R}) = \{ M \in \mathcal{M}_2(\mathbb{R}) : det(M) \neq 0 \}$$

con el producto heredado de  $\mathcal{M}_2(\mathbb{R})$  es un grupo abeliano.

- 6.  $\mathbb{Z}_n$  con su suma es un grupo abeliano,  $\forall n \in \mathbb{N}$ .
- 7.  $U(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n \mid mcd(a, n) = 1\}$  con el producto es un grupo abeliano,  $\forall n \in \mathbb{N}$ .

<sup>&</sup>lt;sup>1</sup>Será común hablar de "operación heredada" cuando consideramos un subconjunto de un conjunto en el que ya hay definida una operación interna, haciendo referencia a la restricción en dominio y recorrido de dicha operación interna al subconjunto considerado.

8. Dado  $n \ge 1$ , consideramos:

$$\mu_n = \{\text{raíces complejas de } x^n - 1\} = \left\{ \xi_n = \cos \frac{2k\pi}{n} + i \operatorname{sen} \frac{2k\pi}{n} \right\}$$
$$= \left\{ 1, \xi, \xi^2, \dots, \xi^{n-1} : \xi = \cos \frac{2\pi}{n} + i \operatorname{sen} \frac{2\pi}{n} \right\}$$

Es un grupo abeliano con el producto heredado de  $\mathbb{C}$ .

9. Dado un cuerpo K, el grupo lineal especial de orden 2 sobre dicho cuerpo:

$$SL_2(\mathbb{K}) = \{ M \in \mathcal{M}_2(\mathbb{K}) : det(M) = 1 \}$$

Con el producto heredado de  $\mathcal{M}_2(\mathbb{K})$  es un grupo que no es conmutativo.

10. Sean  $(G, \Box, e), (H, \triangle, f)$  dos grupos, si consideramos sobre  $G \times H$  la operación binaria  $*: (G \times H) \times (G \times H) \to G \times H$  dada por:

$$(x, u) * (y, v) = (x \square y, u \triangle v) \qquad \forall (x, u), (y, v) \in G \times H$$

Entonces,  $G \times H$  es un grupo, al que llamaremos grupo directo de  $G \times H$ .

11. Si X es un conjunto no vacío y consideramos

$$S(X) = \{f : X \to X \mid f \text{ biyectiva}\} = Perm(X)$$

es un grupo no abeliano con la operación de composición de funciones o.

En el caso en el que X sea finito y tenga n elementos:  $X = \{x_1, x_2, \dots, x_n\}$ , notaremos:

$$S_n = S(X)$$

12. Sea (G, \*, e) un grupo y X un conjunto, consideramos el conjunto:

$$Apl(X,G) = G^X = \{f : X \to G \mid f \text{ aplicación}\}\$$

junto con la operación binaria  $*: G^X \times G^X \to G^X$  dada por:

$$(f * g)(x) = f(x) * g(x)$$
  $\forall x \in X, \forall f, g \in G^X$ 

Entonces,  $(G^X, *, g)$  es un grupo, con elemento neutro:

$$g(x) = e \qquad \forall x \in X$$

de esta forma, dada  $f \in G^X$ , la aplicación simétrica de f será:

$$f'(x) = (f(x))' \quad \forall x \in X$$

Casos a destacar son:

- a) Si  $X = \emptyset$ , entonces  $G^X = {\emptyset}$ .
- b) Si  $X = \{1, 2\}$ , entonces  $G^X$  se identifica con  $G \times G$ .

13. El grupo más pequeño que se puede considerar es el único grupo válido sobre un conjunto unitario  $X = \{e\}$ . Es decir, el grupo (X, \*, e) con  $X = \{e\}$  y  $*: X \times X \to X$  dada por:

$$e * e = e$$
  $e \in X$ 

A este grupo (independientemente de cual sea el conjunto X, ya que todos tendrán la misma<sup>2</sup> estructura) lo llamaremos grupo trivial.

#### **Propiedades**

Aunque estas propiedades parezcan ya conocidas y familiares (por ejemplo para el caso  $(\mathbb{Z}, +, 0)$ ), es una buena observación darnos cuenta de que son válidas para **cualquier grupo** que consideremos, por raros y difíciles que sean sus elementos y operación interna.

**Proposición 1.1.** Sea (G, \*, e) un grupo, destacamos sus primeras propiedades:

- $i) \ x * x' = e \ \forall x \in G.$
- $ii) \ x * e = x \ \forall x \in G.$
- iii) El elemento neutro de \* es único. Simbólicamente:

$$\exists_1 e \in G \mid e * x = x \qquad \forall x \in G$$

iv) Fijado  $x \in G$ , el simétrico de x es único. Simbólicamente:

$$\forall x \in G \quad \exists_1 x' \in G \mid x' * x = e$$

Demostración. Demostramos cada una a partir de la anterior:

i) En primer lugar, observemos que:

$$x' * (x * x') = (x' * x) * x' = e * x' = x'$$
(1.1)

Ahora:

$$x * x' = e * (x * x') = ((x')' * x') * (x * x') = (x')' * (x' * (x * x')) \stackrel{(*)}{=} (x')' * x' = e$$

Donde en (\*) hemos usado (1.1).

ii) Usando i) en (\*):

$$x * e = x * (x' * x) = (x * x') * x \stackrel{(*)}{=} e * x = x$$

iii) Sea  $f \in G$  de forma que  $f * x = x \ \forall x \in G$ , entonces:

$$f = f * e \stackrel{(*)}{=} e$$

Donde en (\*) hemos usado ii).

<sup>&</sup>lt;sup>2</sup>Concepto que luego formalizaremos.

iv) Dado  $x \in G$ , sea  $x'' \in G$  de forma que x'' \* x = x, entonces:

$$x'' = x'' * e \stackrel{(*)}{=} x'' * (x * x') = (x'' * x) * x' = e * x' = x'$$

Donde en (\*) hemos usado i).

**Notación.** A partir de ahora, dado un grupo (G, \*, e), comenzaremos a usar (por comodidad) la notación multiplicativa de los grupos:

$$xy = x * y \qquad \forall x, y \in G$$

Y denotando a x' (el elemento simétrico de x) por  $x^{-1}$ .

**Proposición 1.2.** En un grupo G se verifica la propiedad cancelativa (tanto a la izquierda como a la derecha):

$$\forall x, y, z \in G: \begin{cases} xy = xz \Longrightarrow y = z \\ xy = zy \Longrightarrow x = z \end{cases}$$

Demostración. Para la primera, supongamos que xy = xz:

$$y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$$

Ahora, para la segunda, supongamos que xy = zy y la demostración es la misma que la anterior pero en el otro sentido y tomando  $e = yy^{-1}$ .

$$x = xe = x(yy^{-1}) = (xy)y^{-1} = (zy)y^{-1} = z(yy^{-1}) = z$$

Proposición 1.3. Sea G un grupo, entones:

1.  $e^{-1} = e$ .

2. 
$$(x^{-1})^{-1} = x, \forall x \in G$$
.

3. 
$$(xy)^{-1} = y^{-1}x^{-1}, \forall x, y \in G.$$

Demostración. Cada caso se demuestra observando sencillamente que:

1. ee = e.

2. 
$$xx^{-1} = e$$
.

3. 
$$(y^{-1}x^{-1})(xy) = y^{-1}x^{-1}xy = y^{-1}ey = e$$
.

**Proposición 1.4.** Sea G un conjunto no vacío con una operación binaria \* asociativa, son equivalentes:

i) G es un grupo.

П

П

ii) Para cada par de elementos  $a, b \in G$ , las ecuaciones<sup>3</sup>:

$$aX = b$$
  $Xa = b$ 

Tienen solución en G, es decir:  $\exists c, d \in G \mid ac = b \land da = b$ .

Demostración. Demostramos las dos implicaciones:

- $i) \Rightarrow ii)$  Tomando  $c = a^{-1}b, d = ba^{-1} \in G$  se tiene.
- $(ii) \Rightarrow i)$  Basta demostrar que  $\exists e \in G \text{ con } ex = x \ \forall x \in G \text{ y que fijado } x \in G$ , entonces  $\exists x' \in G \text{ con } x'x = e$ :
  - 1. Dado  $a \in G$ , sabemos que la ecuación Xa = a tiene solución, por lo que existe  $e \in G$  de forma que ea = a.

Por otra parte, dado cualquier  $b \in G$ , sabemos que la ecuación aX = b tiene solución, por lo que existirá un  $x_b \in G$  de forma que  $ax_b = b$ . Finalmente:

$$eb = e(ax_b) = (ea)x_b = ax_b = b$$
  $\forall b \in G$ 

2. Fijado  $x \in G$ , sabemos que la ecuación Xx = e tiene solución, por lo que existe  $x' \in G$  de forma que x'x = e, para cualquier  $x \in G$ .

**Proposición 1.5** (Ley asociativa general). Sea G un grupo,  $\forall x, y \in G$ ,  $\forall m, n > 0$  con m > n > 0, se tiene que:

$$\left(\prod_{i=1}^{m} x_i\right) \left(\prod_{i=m+n}^{n} x_i\right) = \prod_{i=1}^{n} x_i$$

 $\square$ 

Definición 1.3 (Potencia). Podemos definir:

$$x^{n} = \begin{cases} \prod_{i=1}^{n} x & n > 0\\ e & n = 0\\ (x^{-1})^{-n} & n < 0 \end{cases}$$

Proposición 1.6.

$$x^{n+m} = x^n \cdot x^m$$

**Definición 1.4.** Sea G un grupo, si tiene un número finito de elementos, diremos que es un grupo finito. Al número de elementos de G se le llama "orden del grupo", que notaremos con |G|. Si G no fuera finito, se le llama grupo infinito.

**Definición 1.5** (Tabla de Cayley). En un grupo finito  $G = \{x_1, x_2, \ldots, x_n\}$ , se llama tabla de Cayley (o de multiplicar) a la matriz  $n \times n$  de forma que su entrada (i, j) es  $x_i x_j$ .

 $<sup>^3\</sup>mathrm{Donde}$ hemos usado X para denotar la incógnita y que no se confunda con un elemento de G.

**Ejemplo.** Si  $G = \{0, 1\}$ , podemos definir:

$$\begin{pmatrix} *_1 & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} *_2 & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Si  $G = \{0, 1, 2\}$ :

$$\begin{pmatrix}
 & 0 & 1 & 2 \\
0 & 0 & 1 & 2 \\
1 & 1 & 2 & 0 \\
2 & 2 & 0 & 1
\end{pmatrix} \qquad
\begin{pmatrix}
 & 0 & 1 & 2 & 3 \\
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2
\end{pmatrix} \qquad
\begin{pmatrix}
 & 0 & 1 & 2 & 3 \\
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 0 & 3 & 2 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 2 & 1 & 0
\end{pmatrix}$$

Que tienen en particular:

- Simétricas (en caso de ser grupos abelianos).
- Todos los elementos aparecen en todas las filas o columnas (porque si no estaríamos diciendo que las ecuaciones aX = b, Xa = b no tendrían solución)
- Tiene que haber un elemento que actúe de neutro, es decir, mantenga igual el encabezado en una fila o columna.

**Definición 1.6** (Orden de un elemento). Sea G un grupo, el orden de un elemento  $x \in G$  es el menor entero positivo<sup>4</sup> n (en caso de existir) que verifica:  $x^n = 1$ .

Si no existe dicho n, se dice que el orden es infinito.

Escribiremos:

$$O(x) = ord(x) = n$$

Observación. Sea m de forma que  $x^m = 1$ , entonces n|m.

Demostración.

$$m = nq + r \qquad 0 \leqslant r < n$$
  
$$1 = x^m = x^{nq}x^r = x^r \Longrightarrow r = 0$$

**Ejemplo.** Observemos que si G es un grupo (entendiendo que cuando quitamos el 0 es notación aditiva y si no es multiplicativa):

1. 
$$O(x) = 1 \iff x = 1$$
.

$$2. \ O(x) = O(x^{-1}) \ \forall x \in G.$$

3. Si cogemos  $x \neq 0$  en  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ :  $O(x) = +\infty$ .

4. Si cogemos  $x \neq 0$  en  $\mathbb{C}$ : O(i) = 4.

5. En 
$$\mathbb{Z}_9$$
:  $O(\overline{6}) = 3$ .

<sup>4</sup>Entendemos estrictamente mayor que 0.

6. En  $\mathbb{Z}_7^* \subset U(\mathbb{Z}_7)$ :

$$O(\overline{2}) = 3$$

$$O(\overline{3}) = 6$$

**Ejercicio.** Consideramos  $(\mathbb{Z}, *)$  con a \* b = a + b + 1, un grupo abeliano.

Demostración. Demostramos cada una de las propiedades de la definición de grupo abeliano:

Asociativa:

$$(a * b) * c = (a + b + 1) * c = a + b + c + 2$$
  $\forall a, b, c \in \mathbb{Z}$ 

■  $-1 \in \mathbb{Z}$  es el elemento neutro:

$$a + x + 1 = a \Longrightarrow x = -1$$

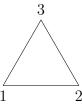
• Fijado x, el simétrico de x será:

$$x * x^{-1} = -1 \Longrightarrow a^{-1} = -a - 2$$

• Es un grupo abeliano a partir de la conmutatividad de  $(\mathbb{Z}, +)$ .

### 1.1. Grupos diédricos

**Ejemplo.** Vienen de la geometría, de considerar las isometrías de polígonos regulares que dejan fija la figura en el plano.



- 1. Dado un triángulo rectángulo con centro en el origen de vértices  $\{1, 2, 3\}$ , isometrías que dejan fija la figura son:
  - Identidad, id.
  - Rotación que lleva 1 en 2 y 2 en 3 (girar  $\frac{2\pi}{3}$ ):

$$r_1 = (1 \ 2 \ 3)$$

 $\blacksquare$ Rotación que lleva 3 en 2 y 2 en 1 (girar  $\frac{4\pi}{3}$ ):

$$r_2 = (1 \ 3 \ 2)$$

Simetrías axiales son por cada una de las rectas de las mediatrices de los lados:

$$s_1 = (1 \ 2)$$
  
 $s_2 = (1 \ 3) = sr$   
 $s_3 = (2 \ 3) = sr^2$ 

- 2. Pensando en el cuadrado:
  - Rotaciones:
    - Identidad.
    - $\frac{\pi}{2}$ :  $(1\ 2\ 3\ 4) = r$ .
    - $\pi$ : (1 3) (2 4) =  $r^2$  (1 y 3 se intercambian y luego los otros).
    - $\frac{3\pi}{2}$ :  $(1\ 4\ 3\ 2) = r^3$ .
    - $r^4 = 1$  (la identidad).
  - Simetrías:
    - Las mediatrices (2):

$$s = s_1 = (1\ 2)\ (3\ 4)$$
  $s_2 = (1\ 4)\ (2\ 3)$ 

• Unir dos vértices opuestos (2).

$$s_3 = (2 \ 4)$$
  $s_4 = (1 \ 3)$ 

Se cumple que  $s_i^2 = 1$ .

Se verifica que  $sr \neq rs$ , pero sí se cumple  $sr = r^3s$ .

$$(1 \ 4) \ (2 \ 3) = r^2.$$
  
 $(1 \ 3) = r^3 s$   
 $(2 \ 4) = rs$ 

Si ahora pensamos en la tabla de  $D_4$  (Hacer mirando la prop 1.7):

$$\begin{pmatrix} & 1 & r & r^2 & r^3 & s & sr & sr^2 & sr^3 \\ 1 & 1 & r & r^2 & r^3 & s & sr & sr^2 & sr^3 \\ r & r & r^2 & r^3 & 1 & sr^3 & s & sr & sr^2 \\ r^2 & r^2 & r^3 & 1 & r & sr^2 & sr^3 & s & sr \\ r^3 & r^3 & 1 & r & r^2 & sr & sr^2 & sr^3 & s \\ s & s & sr & sr^2 & sr^3 & 1 & r & r^2 & r^3 \\ sr & sr & sr^2 & sr^3 & s & r^3 & 1 & r & r^2 \\ sr^2 & sr^2 & sr^3 & s & sr & r^2 & r^3 & 1 & r \\ sr^3 & sr^3 & s & sr & sr^2 & r & r^2 & r^3 & 1 \end{pmatrix}$$

Para  $D_n$  en forma general:

**Definición 1.7** (Grupos diédricos  $D_n$ ). Consideramos  $D_n$ , las isometrías que dejan fijo un polígono regular de n lados. Tendremos, por tanto, 2n elementos:

• n rotaciones de ángulo  $\frac{2k\pi}{n}$  con  $k \in \{0, \dots, n-1\}$ .

- $\bullet$  *n* simetrías axiales:
  - Si n es par tenemos:
    - $\circ$  n/2 respecto a las mediatrices.
    - $\circ$  n/2 respecto a unir vértices contrarios.
  - Si n es impar, tenemos n respecto a las mediatrices.

**Notación.** Dado  $D_n$ , notaremos por:

- r a la rotación de ángulo  $\frac{2\pi}{n}$ .
- s a la simetría que pasa por el origen de coordenadas y el vértice nombrado 1.

**Proposición 1.7.** Dado  $n \in \mathbb{N}$ , en  $D_n$  se cumple que:

- 1.  $1, r, r^2, \ldots, r^{n-1}$  son todos distintos y  $r^n = 1$ , es decir, O(r) = n.
- 2.  $s^2 = 1$ .
- 3.  $s \neq r^i \ \forall 0 \leqslant i \leqslant n-1 \ (ya \ que \ s \ fija \ el \ 1).$
- 4.  $sr^i$  con  $0 \le i \le n-1$  son simetrías en los ejes de simetrías  $(s_1, s_2, \ldots, s_n)$ , con  $sr^i \ne sr^j$ .
- 5.  $sr = r^{-1}s$ .
- 6.  $sr^i = r^{-i}s$ .

**Ejemplo.** En  $D_{12}$ :  $sr^9sr^6 = r^9$ 

**Definición 1.8** (Conjunto de generadores de un grupo). Un conjunto de generadores de un grupo G es un subconjunto  $S \subseteq G$  tal que todo elemento  $x \in G$  puede escribirse como producto finito de elementos de S y de sus inversos, notaremos:

$$G = \langle S \rangle$$

Si  $S = \{x_1, \dots, x_n\}$ , escribiremos:

$$G = \langle x_1, \dots, x_n \rangle$$

En cuyo caso, diremos que  ${\cal G}$  está generado por  ${\cal S}$  y podremos expresar:

$$x = s_1^{\gamma_1} \dots s_p^{\gamma_p} \qquad s_i \in S, \quad \gamma_i = \pm 1$$

**Ejemplo.** Veamos:

- 1.  $G = \langle x \rangle$ , en cuyo caso diremos que G es un grupo cíclico. Por ejemplo,  $\mathbb{Z} = \langle 1 \rangle$  (con notación aditiva).
- 2.  $D_n = \langle r, s \rangle$

**Proposición 1.8.** Si  $G = \langle S \rangle$  y existe un conjunto de relaciones  $R_1, R_2, \ldots, R_m$  (igualdades entre elementos de  $S \cup \{1\}$ ) tal que cualquier relación entre los elementos de S puede deducirse de estas, entonces, decimos que estos generadores y relaciones constituyen una presentación de G, notado:

$$G = \langle S/R_1, R_2, \dots, R_n \rangle$$

Ejemplo. Veamos que:

• En el diédrico  $D_n$ , tenemos que:

$$D_n = \langle r, s/rs = sr^{-1}, r^n = 1, s^2 = 1 \rangle$$

- $D_1 = \langle s, s^2 = 1 \rangle.$
- $D_2 = \langle r, s/r^2 = s^2 = 1, sr = rs \rangle$ .
- $C_n = \langle x/x^n = 1 \rangle$  es un grupo cíclico de orden n.
- $V^{\text{abs}} = \langle x, y/x^2 = 1, y^2 = 1, (xy)^2 = 1 \rangle$  es el grupo de Klein abstracto.
- $Q_2^{\text{abs}} = \langle x, y/x^4 = 1, y^2 = x^2, yxy^{-1} = x \rangle.$
- $\blacksquare$  Pensar cómo se relaciona  $Q_2^{\mathrm{abs}}$  con los cuaternios:

$$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$$

 $i \to j \to k$  en signo positivo.