Grupos finitos

Notas de clase de
Eugenio Miranda Palacios
para el curso 2010/2011
Adaptadas por Manuel Bullejos
para el curso 2020/2021

Índice

1. Definición de grupo

Primeros conceptos

Definición 1.1. Un *grupo* es una cuádrupla $(G, 1, \cdot, ()^{-1})$ donde G es un conjunto, $\cdot : G \times G \to G$ es una ley de composición (operación binaria), $1 \in G$ es un elemento y $()^{-1} : G \to G$ es una operación unaria (aplicación). Satisfaciendo tres axiomas:

- *Asociatividad:* Para cualesquiera $x, y, z \in G$ se satisface $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- *Elemento neutro:* El elemento $1 \in G$ es neutro para el producto, esto es, $\forall x \in G, 1 \cdot x = x$.
- *Elemento inverso:* Para todo $x \in G$, el elemento $x^{-1} \in G$ es inverso de x, esto es, $x^{-1} \cdot x = 1$.

Un grupo G se llama *conmutativo* o *abeliano* si además cumple:

- *Conmutatividad:* Para todo par de elementos $x, y \in G$ se verifica $x \cdot y = y \cdot x$.

Llamamos *orden del grupo* al cardinal del conjunto G. Lo representamos por $|G|$. Cuando el conjunto G es finito diremos que G *es un grupo finito*.

Por abuso de lenguaje es costumbre referirse al grupo $(G, 1, \cdot, ()^{-1})$ como el grupo G, es decir que la operación se sobreentiende.

Notación. Normalmente escribiremos la operación de un grupo en *notación multiplicativa* por yuxtaposición, es decir sin un símbolo especial:

- El producto de x e y se denota como xy.
- El elemento neutro 1 también y se llama unidad.

Cuando el grupo es abeliano usaremos a veces la *notación aditiva*:

- El compuesto de x e y se denota por $x + y$.
- El elemento neutro se denota por 0 y se llama cero.
- La operación $()^{-1}$ se denota $-$, de manera que $-x + x = 0$ y al elemento $-x$ se le llama *opuesto de* x.

Resumimos esto en la siguiente tabla:

Grupo multiplicativo		Grupo aditivo	
$a \cdot b$, ab	Multiplicación	$a + b$	Adición
1	Identidad, Uno	0	Cero
a^{-1}	Inverso	$-a$	Opuesto
a^n	Potencia de a	na	Múltiplo de a
ab^{-1}	Cociente	$a - b$	Diferencia

La tabla de Cayley

Definición 1.2. Sea $G = \{g_1, g_2, \ldots, g_n\}$ un grupo finito con $g_1 = 1$. La *tabla de Cayley*, *tabla de multiplicación* o *tabla de grupo* de G es la matriz $n \times n$ cuya entrada (i, j) es el elemento $g_i g_j$.

Para un grupo finito, la tabla de grupo contiene en cierto sentido toda la información sobre el grupo. Sin embargo es un objeto computacionalmente inmanejable ya que su tamaño es el cuadrado del orden del grupo y visualmente no es un objeto muy útil para determinar propiedades del grupo. Parte del desarrollo de la teoría de grupos (en particular de la teoría de grupos finitos) tiene como objetivo mostrar una visión más conceptual de la estructura interna de grupos.

1.1. Primeros ejemplos

Ejemplo 1.1. El conjunto $\mathbb{Z}$ de los enteros, el conjunto $\mathbb{Q}$ de los racionales y el conjunto $\mathbb{R}$ de los números reales son grupos para la operación suma.

En todos estos casos, el neutro es el número 0 y el inverso de a es el número $-a$.

Ejemplo 1.2. El conjunto de los enteros con la multiplicación ordinaria no es un grupo.

El neutro es el número 1, pero hay enteros que no tienen inverso.

Por ejemplo, no existe ningún *entero* b tal que $5b = 1$.

Ejemplo 1.3. El subconjunto $\{1,\ -1,\ i,\ -i\}$ de los números complejos es un grupo para la multiplicación ordinaria.

El inverso de -1 es él mismo.

El inverso de i es $-i$ y viceversa.

Como este es un grupo finito, podemos escribir su tabla de Cayley que sería:

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

Ejemplo 1.4. El conjunto $\mathbb{Q}^+$ de los racionales positivos es un grupo bajo multiplicación ordinaria.—pause

El inverso de a es $1/a = a^{-1}$.

Ejemplo 1.5. El conjunto S de los números irracionales positivos junto con el 1 satisface las tres propiedades de la definición de grupo. Pero no es un grupo.

Por ejemplo, $\sqrt{2} \cdot \sqrt{2} = 2$, así que S no es cerrado para la multiplicación.

Ejemplo 1.6. El conjunto $\mathcal{M}_{2\times 2}(\mathbb{R})$ de todas las matrices 2×2 de números reales es un grupo para la suma de matrices.

La identidad es

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

El inverso de

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

es

$$\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

Ejemplo 1.7. El conjunto $\mathbb{Z}_n$ para $n \geq 1$ es un grupo para la suma módulo n.

Para todo $j \neq 0$ de $\mathbb{Z}_n$ el inverso de j es $n - j$.

Ejemplo 1.8. El conjunto $\mathbb{R}^\times$ de los números reales no nulos es un grupo bajo multiplicación ordinaria.

El neutro es el número 1.

El inverso de a es $1/a$.

Ejemplo 1.9. El conjunto

$$GL_2(\mathbb{R}) = GL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad | \quad a, b, c, d \in \mathbb{R},\ ad - bc \neq 0 \right\}$$

de las matrices 2×2 con elementos reales y determinante no nulo es un grupo no abeliano para la multiplicación de matrices.

El neutro es la matriz identidad y para el inverso

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

Este es un grupo no abeliano muy importante que se llama *grupo lineal general* de matrices 2×2 sobre $\mathbb{R}$.

Ejemplo 1.10. El conjunto de todas las matrices 2×2 de números reales no es un grupo bajo multiplicación.

No existe inverso para las matrices de determinante 0.

Ejemplo 1.11. Sabemos que un entero a tiene inverso multiplicativo módulo n si y sólo si $\mathrm{m.\,c.\,d.}(a, n) = 1$.

Para todo natural $n > 1$ definimos

$$U(n) = U(\mathbb{Z}_n) = \mathbb{Z}_n^\times = \{[a] \in \mathbb{Z}_n \mid \mathrm{m.\,c.\,d.}(a, n) = 1\}.$$

El conjunto $U(n)$ es un grupo para la multiplicación módulo n.

Para $n = 10$ tenemos $U(n) = \{1,\ 3,\ 7,\ 9\}$. La tabla de Cayley para $U(10)$ es

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	7
9	9	7	3	1

Si n es primo, $U(n) = \{1, 2, \ldots, n - 1\}$

Según Weber (*Lehrbuch der Algebra*, 1899) los grupos $U(n)$ son los ejemplos mas importantes de grupos abelianos finitos.

Ejemplo 1.12. El conjunto $\{0,\ 1,\ 2,\ 3\}$ no es un grupo bajo multiplicación módulo 4.

Las clases 1 y 3 tienen inverso, pero las clase 0 y 2 no lo tienen.

Ejemplo 1.13. El conjunto $\mathbb{Z}$ no es un grupo para la resta, porque la operación no es asociativa.

Ejemplo 1.14. Para todo entero $n \geq 1$ el conjunto de todas las raíces n-ésimas de la unidad

$$\mu_n = \left\{ \cos\left(\frac{2\pi k}{n}\right) + i \operatorname{sen}\left(\frac{2\pi k}{n}\right) \ \mid \ k = 0, 1, 2, \ldots, n-1 \right\},$$

(es decir, todas las raíces complejas del polinomio $x^n - 1$) es un grupo para la multiplicación.

Ejemplo 1.15. El conjunto

$$\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in \mathbb{R}\}$$

es un grupo para la suma por componentes definida por

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

Ejemplo 1.16. Par un punto fijo $(a, b) \in \mathbb{R}^2$ definimos una aplicación $T_{a,b} : \mathbb{R}^2 \to \mathbb{R}^2$ como $T_{a,b}(x, y) = (x + a, y + b)$.

El conjunto $G = \{T_{a,b} \mid a, b \in \mathbb{R}\}$ es un grupo para la composición de aplicaciones.

Un cálculo directo muestra que $T_{a,b} \cdot T_{c,d} = T_{a+c,b+d}$.

De esta fórmula se deduce que G es cerrado para la operación, que el neutro es $T_{0,0}$, que el inverso de $T_{a,b}$ es $T_{-a,-b}$ y que el grupo G es abeliano.

La composición de aplicaciones siempre es asociativa.

Los elementos de G se llaman *traslaciones*.

Ejemplo 1.17. El conjunto de todas las matrices 2×2 de determinante 1 con elementos en $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{Z}_p$ (con p primo) es un grupo no abeliano para la multiplicación de matrices, que se llama *grupo lineal especial* y se representa por $SL_2(F) = SL(2, F)$ donde $F = \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{Z}_p$ respectivamente.

En este caso la fórmula del inverso es bastante sencilla:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Sumario de ejemplos

Grupo	Operación	Neutro	Elemento	Inverso	Abeliano
$\mathbb{Z}$	Suma	0	k	$-k$	Sí
$\mathbb{Q}^+$	Producto	1	m/n	n/m	Sí
$\mathbb{Z}_n$	Suma mod n	0	$[k]$	$[n-k]$	Sí
$\mathbb{R}^\times$	Producto	1	x	$1/x$	Sí
$GL(2, F)$	Producto	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$	$\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$	No
$U(n)$	Prod. mod n	1	k, $(k, n) = 1$	x, $xk \equiv 1 \pmod{n}$	Sí
$\mathbb{R}^n$	Suma comp.	$(0, 0, \ldots, 0)$	$(a_1, a_2, \ldots, a_n)$	$(-a_1, -a_2, \ldots, -a_n)$	Sí
$SL(2, F)$	Producto	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$	$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$	No

1.2. Propiedades elementales

En la definición usual de grupo se exige que la unidad y el inverso sean biláteros e incluso que sean únicos. Pero todo esto puede deducirse de la definición dada:

Proposición 1.3 (Reglas de cálculo)**.** *Sea G un grupo con unidad* 1*.*

1. *Para todo elemento $x \in G$ se verifica $xx^{-1} = 1$.*
2. *Para todo elemento $x \in G$ se verifica $x1 = x$.*
3. *La unidad de un grupo es única.*
4. *El inverso de cualquier elemento es único.*
5. *(*Propiedad cancelativa*): Para $x, y, z \in G$,*
$$xy = xz \Rightarrow y = z \qquad yx = zx \Rightarrow y = z.$$
6. $1^{-1} = 1$.
7. *Para todo elemento $x \in G$ se verifica $(x^{-1})^{-1} = x$.*
8. *Para cualesquiera $x, y \in G$ se verifica $(xy)^{-1} = y^{-1}x^{-1}$.*
9. *Para cualesquiera $x, y \in G$ existen únicos $u, v \in G$ tales que $xu = y$ y $vx = y$.*

Demostración. 1. Calculamos:
$$x^{-1}(xx^{-1}) = (x^{-1}x)x^{-1} = 1x^{-1} = x^{-1}.$$
Multiplicamos ambos miembros por la izquierda por $(x^{-1})^{-1}$:
$$xx^{-1} = 1(xx^{-1}) = (x^{-1})^{-1}(x^{-1}(xx^{-1})) = (x^{-1})^{-1}x^{-1} = 1.$$

2. Calculamos utilizando el apartado anterior:
$$x1 = x(x^{-1}x) = (xx^{-1})x = 1x = x.$$

3. Sean $1, f \in G$ dos unidades. Entonces $1 = 1f = f$

4. Sean x', x^{-1} dos inversos para $x \in G$. Entonces
$$x' = x'1 = x'(xx^{-1}) = (x'x)x^{-1} = 1x^{-1} = x^{-1}.$$

5. Sea $xy = xz$. Multiplicamos ambos miembros por x^{-1} por la izquierda: $y = 1y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = 1z = z$. Igual por el otro lado.

6. De la misma definición: $1 \cdot 1 = 1$, luego $1 = 1^{-1}$.

7. Como hemos visto antes, $xx^{-1} = 1$, luego de la misma definición de inverso obtenemos que $(x^{-1})^{-1} = x$.

8. Un simple cálculo: $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = 1$, luego $(xy)^{-1} = y^{-1}x^{-1}$.

9. Otro simple cálculo muestra que $u = x^{-1}y$ y $v = yx^{-1}$ verifican las condiciones pedidas y son los únicos que las verifican.

□

Las propiedad asociativa garantiza que en un cálculo podemos introducir paréntesis arbitrariamente: Sean $x_1, \dots x_n \in G$. Definimos por recurrencia: $\prod_{i=1}^{n} x_i = (\prod_{i=1}^{n-1} x_i)x_n$.

Proposición 1.4 (Ley asociativa general)**.** *Sea G un grupo Para cualesquiera enteros $m > n > 0$ sean $x_1, \dots x_m \in G$. Se verifica*

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

De la misma forma, cuando se verifica la propiedad conmutativa podemos multiplicar los elementos en cualquier orden:

Proposición 1.5 (Ley conmutativa general)**.** *Sea G un grupo abeliano, sean $x_1, \dots, x_n \in G$ y sea σ una permutación del conjunto $\{1, \dots, n\}$. Se verifica:*

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{n} x_{\sigma(i)}$$

Potencias o múltiplos.

Definición 1.6 (Potencias)**.** Dado un grupo G (con notación multiplicativa) y un elemento $x \in G$ definimos las potencias de x de forma recursiva como sigue:

- $x^0 = 1$,
- supuesto definido x^n, entonces $x^{n+1} = x^n x$.

Las siguientes propiedades tienen una demostración fácil por inducción.

Proposición 1.7. *Para un grupo G, dos elemetos $x, y \in G$ y naturales $n, m \in \mathbb{N}$ se cumplen:*

1. $(x^n)^m = x^{nm} = (x^m)^n$.
2. $x^n x^m = x^{n+m}$.

3. *Si* $xy = yx$, *entonces* $(xy)^n = x^n y^n$.

Definición 1.8 (Múltiplos)**.** Dado un grupo abeliano G (con notación aditiva) y un elemento $x \in G$ definimos los múltiplos de x de forma recursiva como sigue:

- $0x = 0$,
- supuesto definido nx, entonces $(n+1)x = nx + x$.

Las siguientes propiedades tienen una demostración fácil por inducción.

Proposición 1.9. *Para un grupo abeliano* G, *dos elemetos* $x, y \in G$ *y naturales* $n, m \in \mathbb{N}$ *se cumplen:*

1. $n(mx) = (nm)x = m(nx)$.
2. $nx + mx = (n+m)x$.
3. $n(x+y) = nx + ny$.

Definición 1.10 (Orden de un elemento)**.** Dado un elemento $x \in G$ de un grupo (en notación multiplicativa) diremos que el orden de x es n si n es el menor entero positivo tal que $x^n = 1$ (en notación aditiva $nx = 0$). Si para todo entero positivo n se tiene que $x^n \neq 1$ ($nx \neq 0$ en notación aditiva), diremos que el orden de x es infinito.

Denotaremos al orden de x como $|x|$ o bien como $o(x)$.

Ejemplo 1.18. Los órdenes de los elementos del grupo

$$U(7) = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

son:

$$o(1) = 1,\ o(2) = 3,\ o(3) = 6,\ o(4) = 3,\ o(5) = 6,\ o(6) = 2.$$

Ejemplo 1.19. Los órdenes de los elementos del grupo $\mu_4 = \{1, -1, i, -i\}$ son:

$$o(1) = 1,\ o(-1) = 2,\ o(i) = 4,\ o(-i) = 4.$$

Ejemplo 1.20. En el grupo aditivo $\mathbb{Z}_6$ los órdenes de los elementos son:

$$o(0) = 1,\ o(1) = 6,\ o(2) = 3,\ o(3) = 2,\ o(4) = 3,\ o(5) = 6.$$

Observación 1.1. Observar que en los ejemplos anteriores el orden de un elemento es siempre un divisor del orden del grupo. Probaremos esta propiedad más adelante.

Observación 1.2. Observar también que el orden de un producto de dos elementos no tienen porqué estar relacionado con el orden de los elementos. Si x e y son dos elementos de un grupo, puede ocurrir, si x e y no conmutan, que tanto x como y tengan orden finito y sin embargo xy tenga orden infinito.

Proposición 1.11. *Sea* x *un elemento de un grupo* G *de orden* $|x| = n$ *y sea* k *un entero positivo talque* $x^k = 1$. *Entonces* k *es múltiplo de* n.

Demostración. Bastará con dividir k entre n, si el resultado es $k = nq + r$, con r el resto de la división, tendríamos $1 = x^k = x^{nq}x^r = x^r$ pero por ser n el menor entero positivo talque $x^n = 1$ y ser $r < n$ ha de ser $r = 0$ y por tanto k es múltiplo de n. □

1.3. Grupos simétricos

Sea X un conjunto arbitrario.

Definición 1.12. Una *permutación* del conjunto X es cualquier aplicación biyectiva $\sigma : X \to X$.

El conjunto de todas las permutaciones del conjunto X forman un grupo con la operación composición de aplicaciones, neutro la identidad en X e inversos las aplicaciones inversas. Llamaremos a este grupo *grupo simétrico sobre el conjunto* X y lo denotaremos por S_X.

Nos interesa sobre todo el caso en que el conjunto X es finito y en particular el caso en que $X = \mathbf{n} = \{1, 2, \ldots, n\}$. Al grupo simétrico sobre este conjunto lo denotaremos simplemente como S_n y tiene orden $n!$.

Hay dos notaciones para designar los elementos de S_n.

Primera notación:
Cualquier elemento $\sigma \in S_n$ está definido por el conjunto de imágenes de los elementos de $\mathbf{n}$. Podemos determinar σ mediante una matriz $2 \times n$:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ i_1 & i_2 & \ldots & i_{n-1} & i_n \end{pmatrix}$$

donde la primera fila son los elementos ordenados de $\mathbf{n}$ y para cada elemento de la segunda fila tomamos $i_k = \sigma(k)$ (la imagen de k bajo la aplicación σ).

Definición 1.13. La anterior matriz se llama *matriz de la permutación* σ.

Las matrices de permutación constituyen una notación un poco pesada, pero son muy útiles para calcular productos de permutaciones:

Ejemplo 1.21. Sean

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

entonces

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Ejemplo 1.22. Sean ahora

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Entonces

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Lema 1.14. *Para $n \geq 3$, el grupo S_n no es conmutativo.*

Con esta notación, para calcular la inversa de una permutación bastará con intercambiar las filas y reordenar. Por ejemplo

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}, \qquad \tau^{-1} = \begin{pmatrix} 3 & 5 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

Segunda notación.

Una segunda notación más compacta para las permutaciones es como productos de ciclos disjuntos:

Definición 1.15. Un *ciclo de longitud* m es una permutación representada por una sucesión $\sigma = (i_1\ i_2\ \ldots\ i_m)$ donde los i_k son enteros positivos todos distintos y menores o iguales a n.

La permutación σ está definida por $\sigma(i_k) = i_{k+1}$ para $k = 1, 2, \ldots, m-1$, $\sigma(i_m) = i_1$ y $\sigma(j) = j$ para todo $j \neq i_k$, $k = 1, 2, \ldots, m$.

Ejemplo 1.23. El ciclo (1234) es la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Observación 1.3. No toda permutación es un ciclo, por ejemplo la permutación τ en el Ejemplo 1.21 no es un ciclo.

Observación 1.4. Vamos a abusar del lenguaje de la siguiente forma.

Muchas veces en lugar de denotar a un ciclo genérico de longitud m como $\sigma = (i_1 i_2,\ \ldots i_m)$ lo escribiremos simplemente como $\sigma = (12\ \ldots\ m)$, de manera que esta n-tupla puede indicar tanto un ciclo genérico como el ciclo concreto.

Por ejemplo usaremos (123) para representar la permutación que lleva el 1 en el 2, el 2 en el 3 y el 3 en el 1, pero también para representar una permutación genérica de longitud tres $(i_1 i_2 i_3)$.

Sin embargo (132) sólo indicara esa permutación concreta.

Observación 1.5. Notemos también que cada ciclo de longitud m puede ser representado de m formas distintas, dependiendo del por que valor empezamos, así por ejemplo:

$$(123\ \ldots\ n-1\ n) = (23\ \ldots\ n-1\ n\ 1) = \cdots = (n\ 12\ \ldots\ n-1).$$

El número de ciclos de longitud m en S_n, está dado por la fórmula:

$$\frac{V_m^n}{m} = \frac{n!}{m \cdot (n-m)!}.$$

Definición 1.16. Llamaremos transposición a un ciclo de longitud 2.

Observación 1.6. El único ciclo de longitud 1 es la identidad y como ciclo puede ser representado de n formas distintas: $(1) = (2) = \ldots = (n)$.

Observación 1.7. En general el producto de dos ciclos no tiene porqué ser un ciclo y tampoco es conmutativo.

Definición 1.17. Dos ciclos $\sigma = (i_1\ i_2,\ \dots\ i_m)$ y $\tau = (j_1\ j_2\ \dots\ j_s)$ se llaman *disjuntos* si para todo par de índices k, ℓ se tiene $i_k \neq j_\ell$.

El siguiente lema tiene una demostración elemental.

Lema 1.18. *El producto de ciclos disjuntos es conmutativo.*

La siguiente proposición muestra la importancia de los ciclos disjuntos.

Proposición 1.19. *Toda permutación se descompone de manera única (salvo orden e identidades) como producto de ciclos disjuntos.*

Demostración. La demostración de esta proposición es algoritmica, en el sentido de que facilita un algoritmo para obtener la descomposición en ciclos disjuntos de una permutación.

Sea $\sigma \in S_n$, consideramos la sucesión $1, \sigma(1), \sigma^2(1), \dots$ Esta sucesión no puede ser infinita y por tanto han de existir índices i, k tales que $\sigma^{i+k}(1) = \sigma^i(1)$, que implica que $\sigma^k(1) = 1$.

Tomemos k el menor índice con esta propiedad y consideremos el ciclo $\gamma_1 = (1\sigma(1)\sigma^2(1)\dots\ \sigma^{k-1}(1))$.

Claramente σ y γ_1 actúan de igual forma sobre el conjunto

$$J_1 = \{1, \sigma(1), \sigma^2(1), \dots,\ \sigma^{k-1}(1)\},$$

i.e. $\sigma(x) = \gamma_1(x)$ para todo índice $x \in J_1$.

Tomemos ahora i el menor índice que no esté en J_1 y repitamos el proceso, esto es, consideremos la sucesión $j, \sigma(j), \sigma^2(j), \dots$ y tomemos r el menor índice tal que $\sigma^r(j) = j$, consideremos el ciclo $\gamma_2 = (j\sigma(j)\sigma^2(j)\dots\ \sigma^{r-1}(j))$ y el conjunto

$$J_2 = \{j, \sigma(j), \sigma^2(j), \dots,\ \sigma^{r-1}(j)\}.$$

Claramente γ_1 y γ_2 son disjuntas y el producto $\gamma_1\gamma_2$ actúa de igual forma que σ sobre el conjunto $J_1 \cup J_2$, esto es $\sigma(x) = \gamma_1\gamma_2(x), \forall x \in J_1 \cup J_2$.

Notemos que si $\sigma(1) = 1$ entonces $\gamma_1 = (1)$ y podemos no tener en cuenta este ciclo ya que es la identidad.

Tomaríamos ahora el menor índice que no esté en la unión $J_1 \cup J_2$ y repetíríamos el proceso hasta completar todos los índices de $\mathbf{n}$.

Para probar la unicidad supongamos $\sigma = \gamma_1 \cdots \gamma_r = \beta_1 \cdots \beta_s$ dos descomposiciones en ciclos disjuntos.

Supongamos que $\sigma(1) \neq 1$ y que $\gamma_1 = (1\ \sigma(1)\ \sigma^2(1)\ \dots\ \sigma^{k-1}(1))$ como anteriormente.

Como también estamos suponiendo $\sigma = \beta_1 \cdots \beta_s$ el índice 1 tiene que aparecer en alguno de los β, supongamos que aparece en el primero, en este caso $\sigma(1) = \beta_1(1)$ lo que implica $\sigma^i(1) = \beta_1^i(1)$, en particular $\beta_1^{k-1} = 1$ y

$$\beta_1 = (1\ \beta_1(1)\ \beta_1^2(1)\ \dots\ \beta_1^{k-1}(1)) = (1\ \sigma(1)\ \sigma^2(1)\ \dots\ \sigma^{k-1}(1)) = \gamma_1.$$

Tomamos ahora el primer índice que no esté J_1 y procedamos de igual forma hasta que cubramos todos los índices que mueve σ. □

La expresión de una permutación como producto de ciclos disjuntos permite apreciar fácilmente a primera vista las propiedades mas sencillas de las permutaciones:

Proposición 1.20 (Ruffini, 1799)**.**

1. *El orden de todo ciclo* $\gamma = (i_1,\ i_2,\ \ldots,\ i_m)$ *es igual a la longitud* m*.*
2. *Sea* $\sigma = \gamma_1\gamma_2\ldots\gamma_t$ *un producto de ciclos disjuntos de longitudes respectivas* $m_1,\ldots,m_t$*. El orden de la permutación* σ *es* $\mathrm{m.c.m.}(m_1,\ldots,m_t)$*.*
3. *Sea* $\gamma = (i_1,\ i_2,\ \ldots,\ i_{m-1},\ i_m)$ *un ciclo de longitud* m*. Entonces* $\gamma^{-1} = (i_m,\ i_{m-1},\ \ldots,\ i_2,\ i_1)$ *también es un ciclo de longitud* m*.*
4. *Sea* $\sigma = \gamma_1\gamma_2\ldots\gamma_t$ *un producto de ciclos disjuntos de longitudes respectivas* $m_1,\ldots,m_t$*. Entonces* $\sigma^{-1} = \gamma_1^{-1}\gamma_2^{-1}\ldots\gamma_t^{-1}$*.*

Demostración. Las demostraciones de 1,3 y 4 son inmediata.

Podemos hacer la demostración de 2 por inducción sobre t. Veamos solo como sería el primer paso de la inducción, esto es, para $t = 2$. Supongamos entonces $\sigma = \gamma_1\gamma_2$ y llamemos $m = m.c.m(m_1, m_2)$. Existiran entonces enteros a y b tales que $m = m_1a = m_2b$. Entonces

$$\sigma^m = (\gamma_1\gamma_2)^m = \gamma_1^m\gamma_2^m = (\gamma_1^{m_1})^a(\gamma_2^{m_2})^b = 1.$$

Por otro lado si $\sigma^k = \gamma_1^k\gamma_2^k = 1$, entonces $\gamma_1^k = \gamma_2^{-k}$, pero como son ciclos disjuntos, ha de ser $\gamma_1^k = \gamma_2^{-k} = 1$ y por tanto también $\gamma_2^k = 1$. Utilizamos ahora la Proposición 1.11 para deducir que k es multiplo de m_1 y de m_2 y por tanto de m, así $m \leq k$. De esta forma m es el menor entero positivo talque $\sigma^m = 1$.

□

Definición 1.21. La Proposición 1.19 nos permite definir el *tipo* o *estructura de ciclos* de una permutación de la siguiente forma. Supongamos que $\sigma = \gamma_1\gamma_2\ldots\gamma_r$ es una descomposición en ciclos disjuntos (ninguno de ellos la identidad). Llamemos m_i a la longitud del ciclo γ_i y supongamos $m_1 \leq m_2 \leq \ldots \leq m_r$. El tipo de σ será la sucesión $m_1, m_2, \cdots, m_r$.

Definimos el tipo de la idetidad como 1.

Ejemplo 1.24. Por ejemplo, si $\sigma = (12)(345)(567)$, el tipo de σ será $2, 3, 3$.

Observación 1.8. En la siguiente tabla mostramos para $n \leq 5$ los distintos tipos y un representante de cada uno de ellos.

n	Tipo	Representante
1	1	1
2	1	1
	2	(12)
3	1	1
	2	(12)
	3	(123)
4	1	1
	2	(12)
	2,2	(12)(34)
	3	(123)
	4	(1234)
5	1	1
	2	(12)
	2,2	(12)(34)
	3	(123)
	2,3	(12)(345)
	4	(1234)
	5	(12345)

Definición 1.22. Dos permutaciones $\sigma, \tau \in S_n$ se llaman *conjugadas en* S_n si existe una $\rho \in S_n$ tal que $\tau = \rho\sigma\rho^{-1}$.

Observación 1.9. Claramente, *ser conjugadas* es una relación de equivalencia, que divide al grupo de permutaciones en clases de cojugación.

Proposición 1.23. *Si* $(12\dots r)$ *es un ciclo cualquiera, para cualquier permutación* ρ *se tiene*

$$\rho(12,\dots r)\rho^{-1} = (\rho(1)\rho(2)\dots\rho(r)).$$

En particular los conjugados de un ciclo de longitud r *son ciclos de longitud* r*. Tambien es cierto el recíproco, esto es, dos ciclos de la misma longitud siempre son conjugados. De manera que:*

Dos ciclos son conjugados si, y solo si, tienen la misma longitud.

Demostración. Para probar la igualdad aplicaremos ambos términos de la igualdad a un índice cualquiera j. Como ρ es una biyección, podremos poner $j = \rho(i)$, para un único i. Distinguimos los siguientes casos:

- $1 \leq i < r$. En este caso

$$(\rho(12,\dots r)\rho^{-1})(\rho(i)) = \rho(12,\dots r)(i) = \rho(i{+}1) = (\rho(1)\rho(2)\dots\rho(r))(\rho(i)).$$

- $i = r$. En este caso

$$(\rho(12,\dots r)\rho^{-1})(\rho(r)) = \rho(12,\dots r)(r) = \rho(1) = (\rho(1)\rho(2)\dots\rho(r))(\rho(r)).$$

- $r < i$. En este caso

$$(\rho(12,\dots r)\rho^{-1})(\rho(i)) = \rho(12,\dots r)(i) = \rho(i) = (\rho(1)\rho(2)\dots\rho(r))(\rho(i)).$$

Finalmente, si tenemos otro ciclo $(i_1 i_2 \dots\ i_r)$ de longitud r, bastará tomar como ρ una permutación que cumpla $\rho(j) = i_j, j = 1, 2, \dots, r$, para tener

$$\rho(12\dots\ r) = (\rho(1)\rho(2)\dots\rho(r)) = (i_1 i_2 \dots\ i_r).$$

□

Corolario 1.24. *Dos permutaciones son conjugadas en S_n si y sólo si tienen el mismo tipo.*

Demostración. Bastará con tener en cuenta que el conjugado de un producto es el producto de los conjugados, i.e.

$$\rho(\sigma_1\sigma_2\dots\sigma_m)\rho^{-1} = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1})\dots(\rho\sigma_m\rho^{-1}).$$

□

Definición 1.25. Todo ciclo de (i, j) longitud 2 se llama *transposición*

Al igual que los ciclos, las transposiciones también *generan* S_n, como mostramos en la siguiente

Proposición 1.26. *Toda permutación se descompone como producto de transposiciones.*

Demostración. Como toda permutación descompone como producto de ciclos, para demostrar esta proposición bastará con que probemos que todo ciclo descompone como producto de transposiciones.

Es fácil de comprobar que

$$(123\dots\ r) = (12)(23)\dots(r-1\ r) = (1r)(1\ r-1)\dots(12).$$

Y por tanto tenemos al menos dos formas de expresar un ciclo de longitud r como producto de transposiciones. □

Observación 1.10. La descomposición de una permutación como producto de transposiciones no es única: Por ejemplo:

$$(1, 2, 3) = (1, 2)(2, 3) = (1, 3)(1, 2).$$

De hecho ni siquiera el número de transposiciones es único: Por ejemplo:

$$(2, 3) = (1, 2)(2, 3)(1, 3)$$

o

$$(1, 2, 3, 4, 5) = (4, 5)(3, 5)(2, 5)(1, 5) = (4, 5)(2, 5)(1, 2)(2, 5)(2, 3)(1, 3)$$

Pero en cualquier descomposición, el número de transposiciones que aparecen siempre es de la misma paridad.

Definición 1.27 (La signatura y la paridad)**.**

Dada una permutación $\sigma \in S_n$, con descomposición en ciclos disjuntos $\sigma = \gamma_1\gamma_2\dots\gamma_r$, definimos

$$N(\sigma) = \sum_{i=1}^{r}(long(\gamma_i) - 1),$$

y definimos la signatura de σ como

$$sg(\sigma) = (-1)^{N(\sigma)}.$$

Diremos que σ es par si $sg(\sigma) = 1$ y en caso contrario diremos que es impar.

Observación 1.11. Todo ciclo de longitud par es impar y todo ciclo de longitud impar es par. Así:

- La identidad es par,
- toda transposición es impar y
- todo ciclo de longitud tres es par.

Lema 1.28. *Sea σ una permutación cualquiera y τ una transposición. Etonces $sg(\tau\sigma) = -sg(\sigma)$.*

Demostración. Notemos $\tau = (12)$ y supongamos $\sigma = \gamma_1\gamma_2\dots\gamma_r$ la descomposición en ciclos disjuntos. Entonces 1 y 2 pueden aparecer o no en alguna de las γ, que podemos suponer son las primeras ya que el orden es irrelevante. Distinguimos los siguientes casos:

Caso 1.- 1 y 2 no aparece en ningún γ.

Caso 2.- 1 y 2 aparecen consecutivamente en un mismo ciclo, $\gamma_1 = (123\dots\ r)$.

Caso 3.- 1 y 2 aparecen no consecutivamente en una mismo ciclo

$$\gamma_1 = (1i_1\dots i_k 2j_1\dots j_s).$$

Caso 4.- 1 y 2 aparecen en ciclos distintos, $\gamma_1 = (1i_1\dots i_k)$ y $\gamma_2 = (2j_1\dots j_s)$.

Para calcular $sg(\tau\sigma)$ tenemos que calcular la descomposición en ciclos disjuntos de $\tau\sigma$, haremos esto dependiendo del caso en que estemos.

Caso 1.- En este caso (12) y las γ_i siguen siendo disjuntos, por lo que

$$\tau\sigma = (12)\gamma_1\gamma_2\dots\gamma_r$$

es su descomposición en ciclos disjuntos y por tanto $(\tau\sigma) = 1 + N(\sigma)$ y $sg(\tau\sigma) = -sg(\sigma)$.

Caso 2.- En este caso, la descomposición en ciclos disjuntos de $(12)(123\dots\ r)$ es $(12)(123\dots\ r) = (23,\dots\ r)$ de donde deducimos que $N(\tau\sigma) = N(\sigma) - 1$ y por tanto $sg(\tau\sigma) - sg(\sigma)$.

Caso 3.- En este caso, la descomposición en ciclos disjuntos de $(12)(1i_1 \dots i_k 2j_1 \dots j_s)$ es $(12)(1i_1 \dots i_k 2j_1 \dots j_s) = (1i_1 \dots i_k)(2j_1 \dots j_s)$ y tenemos

$$\begin{aligned} N(\tau\sigma) &= lg((1i_1 \dots i_k)) - 1 + lg((2j_1 \dots j_s)) - 1 + \sum_{j=2}^{r}(lg(\gamma_j) - 1) \\ &= k + s + \sum_{j=2}^{r}(lg(\gamma_j) - 1), \end{aligned}$$

por otro lado

$$\begin{aligned} N(\sigma) &= lg((1i_1 \dots i_k 2j_1 \dots j_s)) - 1 + \sum_{j=2}^{r}(lg(\gamma_j) - 1) \\ &= k + s + 1 + \sum_{j=2}^{r}(lg(\gamma_j) - 1) \\ &= N(\tau\sigma) + 1, \end{aligned}$$

de donde $sg(\tau\sigma) = -sg(\sigma)$.

Caso 4.- En este caso, si multiplicamos ambos términos de la igualdad

$$(12)(1i_1 \dots i_k 2j_1 \dots j_s) = (1i_1 \dots i_k)(2j_1 \dots j_s)$$

(obtenida en el Caso 2) por la izquierda por (12), obtenemos

$$(1i_1 \dots i_k 2j_1 \dots j_s) = (12)(1i_1 \dots i_k)(2j_1 \dots j_s),$$

de donde

$$\begin{aligned} N(\tau\sigma) &= lg(12) - 1 + lg((1i_1 \dots i_k)) - 1 + lg((2j_1 \dots j_s)) - 1 + \sum_{j=2}^{r}(lg(\gamma_j) - 1) \\ &= 1 + k + s + \sum_{j=2}^{r}(lg(\gamma_j) - 1) \\ &= 1 + N(\sigma) \end{aligned}$$

y tenemos $sg(\tau\sigma) = -sg(\sigma)$.

□

Corolario 1.29. *Una permutación es par (impar) si, y solo si, se descompone como un número par (impar) de transposiciones.*

Demostración. Si $\sigma = \tau_1 \dots \tau_r$ es una descomposición como producto de transposiciones de σ, basta considerar la igualdad $\sigma = \tau_1 \dots \tau_r 1$ y aplicar sucesivamente el Lema 1.28 para obtener $sg(\sigma) = (-1)^r sg(1) = (-1)^r$ y deducimos el corolario. □

Y como consecuencia inmediata del Corolario 1.29 anterior, tenemos

Corolario 1.30. *La signatura de un producto es el producto de las signaturas,* para todo producto de permutaciones.

1.4. Grupos diédricos

Una familia importante de ejemplos es la clase de grupos cuyos elementos son simetrías de objetos geométricos. La subclase mas sencilla es la correspondiente a figuras planas regulares.

Para cada $n \in \mathbb{Z},\ n \geq 3$ sea D_n el conjunto de simetrías de un n-gono regular, donde una simetría es cualquier movimiento rígido del plano (o *isometría*) que lleva el n-gono en sí mismo.

Por ejemplo, para $n = 3, 4, 5, 6$, etc. D_n sería el conjunto de simetrías del triangulo, cuadrado, pentágono, hexágono, etc.

Es fácil ver que:

- La composición de dos de tales movimientos también dejan fijo al n-gono.
- La identidad es uno de estos movimientos.
- Para cualquiera de los elementos de D_n la transformación inversa también pertenece a D_n.

Así que D_n es un grupo (más precisamente, un "*subgrupo*" del grupo euclídeo del plano).

Numeramos los vértices del n-gono de manera que los vértices 1 y 2 sean adyacentes. Cualquier isometría del plano queda determinada por la imagen de tres puntos no alineados. En nuestro caso, cualquier elemento de D_n está determinado por la imagen del centro del n-gono (que siempre es él mismo) y por las imágenes de los vértices 1 y 2.

Bajo cualquier elemento de D_n la imagen del vértice 1 es necesariamente uno de los otros n vértices, y la imagen del vértice 2 tiene que ser uno de los dos vértices adyacentes a la imagen del vértice 1.

Obtenemos así una cota para el orden de D_n: $|D_n| \leq 2n$.

Por otra parte, las n rotaciones $r_k,\ 0 \leq k < n$ alrededor del centro del n-gono y con ángulos $2k\pi/n$ radianes son todas distintas y llevan el n-gono en sí mismo, así que todas ellas pertenecen a D_n.

También pertenecen a D_n las n reflexiones en las rectas que pasan por el centro del n-gono y por cada uno de los vértices y de los puntos medios de las aristas.

En total hemos obtenido $2n$ elementos distintos de D_n, así que $|D_n| \geq 2n$.

Combinando con la desigualdad anterior vemos que $|D_n| = 2n$.

Ya que a lo largo del curso usaremos mucho los grupos diédricos como fuente de ejemplos, ahora fijaremos alguna notación y haremos algunos cálculos que simplificarán otros cálculos futuros y nos ayudarán a determinar D_n como un grupo abstracto (en lugar de volver al contexto geométrico cada vez que aparezca).

Fijamos un n-gono regular centrado en el origen en un XY-plano y numeramos los vértices consecutivamente desde 1 hasta n en sentido contrario a las agujas del reloj.

Sea r la rotación con centro en el origen y ángulo $2\pi/n$ radianes (en sentido contrario a las agujas del reloj).

Sea s la reflexión en el eje que pasa por el vértice 1 y el origen.

Lema 1.31. *1.* $1,\ r,\ \ldots,\ r^{n-1}$ *son todas distintas y* $r^n = 1$*, así que* $o(r) = n$*.*

2. $s^2 = 1$*, es decir que* $o(s) = 2$*.*

3. $s \neq r^i$ *para todo* i*.*

4. $sr^i \neq sr^j$ *para todo* $0 \leq i, j \leq n-1$ *con* $i \neq j$*, así que*

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

es decir, cada elemento se puede escribir de forma única *como* $s^k r^j$ *para algún* $k = 0, 1$ *y* $0 \leq j \leq n-1$*.*

5. $rs = sr^{-1}$*. En particular* r *y* s *no conmutan, así que* D_n *no es abeliano.*

6. $r^i s = sr^{-i}$ *para todo* $0 \leq i \leq n$*. Esto indica como conmuta* s *con las potencias de* r*.*

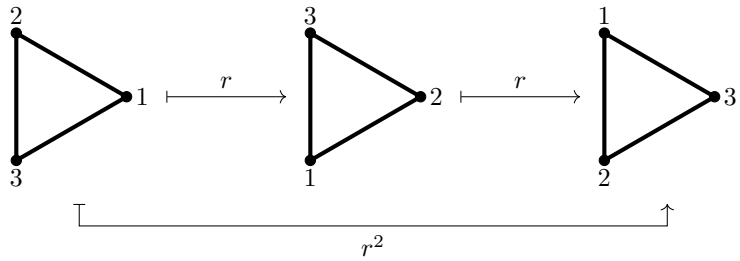
Observamos ahora que la tabla completa de multiplicación de D_n puede escribirse en términos sólo de r y s, es decir, todos los elementos de D_n tienen una representación única de la forma $s^k r^i$, $k = 0, 1$ y $0 \leq 1 \leq n-1$, y cualquier producto de dos elementos en esta forma puede reducirse a la misma forma usando sólo las "relaciones" 1,2 y 6 (reduciendo todos los cálculos módulo n). Por ejemplo, si $n = 12$,

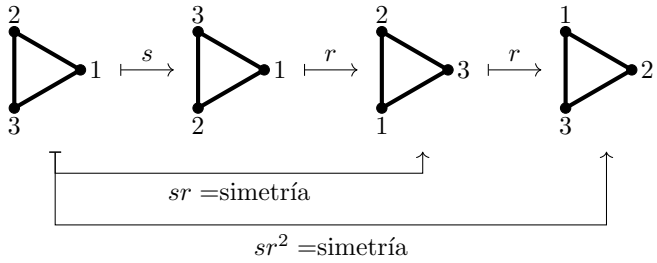
$$(sr^9)(sr^6) = s(r^9 s)r^6 = s(sr^{-9})r^6 = s^2 r^{-9+6} = r^{-3} = r^9$$

Observación 1.12. Aunque aún no hemos hablado de presentaciones, digamos que dar una presentación de un grupo es básicamente dar los datos necesarios para reconstruir totalmente el grupo. El Lema 1.31 nos permite dar una presentación de D_n como

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

Ejemplo 1.25. Por ejemplo para $n = 3$, D_3 tiene seis elementos, la identidad, un giro r de 120 grados, en el sentido contrario a las agujas del reloj, su cuadrado r^2 que será un giro de 240 grados y tres simetrías que se pueden obtener tomando s la simetría respecto al eje que pasa por el vértice 1 y el centro del triangulo y componiendo s con r y con r^2.





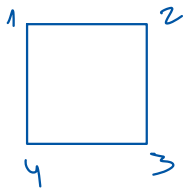
Notar ahora que cada movimiento está determinado por como actúa sobre los vértices. Así por ejemplo:

- la rotación r actúa $1 \mapsto 2 \mapsto 3 \mapsto 1$ y por tanto la vamos a denotar como $r = (123)$,
- la simetría s actúa $1 \mapsto 1, 2 \mapsto 3 \mapsto 2$ y la denotaremos como $s = (23)$,
- de forma análoga $r^2 = (132)$,
- $sr = (13)$,
- $sr^2 = (12)$.

Con está notación

$$\begin{aligned} D_3 = &\quad \langle r, s;\ r^3 = 1,\ s^2 = 1,\ rs = sr^{-1} \rangle \\ = &\quad \{1, r, r^2, s, sr, sr^2\} \\ = &\quad \{1, (123), (132), (23), (13), (12)\} \end{aligned}$$

$D_3 \cong S_3$



$D_4 = \{1, p, p^2, p^3, \tau, p\tau, p^2\tau, p^3\tau\}$

giros — simetrías

$D_4 = \langle p, \tau ;\ p^4 = 1,\ \tau^2 = 1,\ \tau p = p^{-1}\tau \rangle$

$D_4 \subsetneq S_4$

1.5. Producto directo

Sean $(H, *)$ y $(K, \diamond)$ dos grupos y sea $H \times K$ el conjunto producto cartesiano de H y K. Definimos una operación binaria en $H \times K$ de la siguiente forma:

$$(h, k) \cdot (h_1, k_1) = (h * h_1, k \diamond k_1)$$

Lema 1.32. *El par $(H \times K, \cdot)$ es un grupo*

Demostración. Hay que efectuar tres comprobaciones:

Asociatividad Para cualesquiera $(h, k), (h_1, k_1), (h_2, k_2) \in H \times K$ calculamos:

$$\begin{aligned}((h, k) \cdot (h_1, k_1)) \cdot (h_2, k_2) &= (h * h_1, k \diamond k_1) \cdot (h_2, k_2) \\ &= ((h * h_1) * h_2, (k \diamond k_1) \diamond k_2)) = (h * (h * h_1), k \diamond (k_1 \diamond k_2)) \\ &= (h, k_1) \cdot (h_1 * h_2, k_1 \diamond k_2) = (h, k) \cdot ((h_1, k_1) \cdot (h_2, k_2))\end{aligned}$$

Existencia de neutro Sea e el elemento neutro de H y sea f el elemento neutro de K. Para cualquier $(h, k) \in H \times K$ calculamos:

$$(e, f) \cdot (h, k) = (e * h, f \diamond k) = (h, k)$$

Existencia de inverso Sea $(h, k) \in H \times K$ arbitrario y sean h' el inverso de h en H y k' el inverso de k en K. Calculamos:

$$(h', k') \cdot (h, k) = (h' * h, k' \diamond k) = (e, f)$$

□

En particular si tomamos $H = K = \mathbb{R}$, el producto $\mathbb{R} \times \mathbb{R}$ es el grupo aditivo de los vectores del plano.

Otro grupo producto interesante es $\mathbb{Z}_2 \times \mathbb{Z}_2$. Es un grupo de orden cuatro para el que todo elemento verifica que $2a = 0$, esto es, todo elemento no nulo tiene orden 2. Este es un grupo de orden 4 que no tiene elementos de orden 4.

No ocurre lo mismo con $\mathbb{Z}_2 \times \mathbb{Z}_3$, los ordenes de los elementos de este grupo son:

$$o(0, 0) = 1,\ o(1, 0) = 2,\ o(0, 1) = o(0, 2) = 3,\ o(1, 1) = o(1, 2) = 6.$$

Por tanto este es un grupo de orden 6 que tiene dos elementos de orden 6.

En general, podemos calcular el orden de cualquier elemento de un producto directo cono se indica en la siguiente

Proposición 1.33. *El orden de un elemento $(x, y) \in H \times K$, de un producto de grupos, es el mínimo común múltiplo de los ordenes de sus componentes:*

$$o(x, y) = m.c.m.(o(x), o(y)).$$

Demostración. La demostración se deduce de los siguientes hechos, fáciles de probar:

- $(x, y)^n = (x^n, y^n)$ y
- $(x, y)^n = 1 \Leftrightarrow x^n = y^n = 1$, para cualquier entero positivo n.

□

1.6. Grupos de matrices

Sea F un cuerpo arbitrario. Llamamos $\mathcal{M}_n(F)$ al conjunto de todas las matrices cuadradas $n \times n$ con coeficientes en F. Este conjunto con la suma y producto usual, respecto es un anillo.

Nos interesa el grupo multiplicativo de este anillo. Lo representamos por $GL_n(F)$ y lo llamamos *grupo lineal general* de orden n de F. Sus elementos son las matrices cuadradas que tengan inverso. Es conocido el siguiente resultado:

Lema 1.34. *Para toda matriz $A \in \mathcal{M}_n(F)$ son equivalentes:*

1. *Existe $B \in \mathcal{M}_n(F)$ tal que $AB = I = BA$.*
2. $\det(A) \neq 0$.
3. *Las filas de A son linealmente independientes sobre F.*
4. *Las columnas de A son linealmente independientes sobre F.*

Sea $V = F^n$ un espacio vectorial de dimensión n sobre F. Para cada elección de una base $v_1, \ldots, v_n$ existe un isomorfismo $Aut(V) \cong GL_n(F)$, por lo que tendemos a identificar estos dos grupos, pero ¡cuidado! el isomorfismo no es canónico, sino que depende de la base.

Los grupos de matrices están íntimamente ligados a la Geometría.

Los grupos de matrices y los grupos simétricos se consideran como el espejo al que referir los grupos abstractos. Por ello son muy importantes los homomorfismos de un grupo abstracto G a un grupo de matrices $GL_n(F)$.

Tales homomorfismos se llaman *representaciones lineales* del grupo G y son objeto de estudio en el curso de Ampliación de álgebra.

Existen teoremas sobre grupos abstractos que actualmente sólo se saben demostrar a través de la teoría de representaciones.

Otra utilidad importante de los grupos de matrices es proveer ejemplos de grupos finitos.

Sea $\mathbb{F}$ un cuerpo finito con q elementos. Veamos cual es el orden de $GL_n(\mathbb{F})$:

Sea $A \in GL_n(\mathbb{F})$ arbitraria. Por el lema 1.34, la primera fila puede ser cualquier vector no nulo de $\mathbb{F}^n$, es decir que hay $q^n - 1$ posibilidades.

Una vez fijadas las primeras i filas, la $(i+1)$-ésima puede ser cualquier vector de $\mathbb{F}^n$ que no pertenezca al subespacio generado por las i primeras (que es de orden $\mathbb{F}^i$). Así que para esta fila tenemos $q^n - q^i$ posibilidades.

En total el número de matrices distintas de $GL_n(\mathbb{F})$ es

$$|GL_n(\mathbb{F})| = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}).$$

Por ejemplo:

- $|Gl_2(\mathbb{Z}_2)| = (2^2 - 1)(2^2 - 2) = 6$ y
- $|GL_3(\mathbb{Z}_2)| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$.

Otra familia de grupos de matrices interesante es la familia de *grupos lineales especiales*. Para un cuerpo F el conjunto

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}$$

tiene estructura de grupo con multiplicación la multiplicación de matrices. Más tarde probaremos que si $|\mathbb{F}| = q$ es finito entonces

$$|SL_n(\mathbb{F})| = \frac{1}{q-1}((q^n-1)(q^n-q)\dots(q^n-q^{n-1}))$$

Existen otros subgrupos (¡y grupos cocientes!) interesantes de $GL_n(F)$ como los grupos ortogonal y simpléctico (y los grupos proyectivos general y especial) y cada uno de ellos merece un estudio propio. Se conocen como *los grupos clásicos* y se les han dedicado varios libros. Para una primera aproximación, véase *Artin, Geometrical Algebra*

1.7. El grupo cuaternio

El grupo cuaternio se puede definir como un grupo de matrices. En el grupo $GL_2(\mathbb{C})$ consideramos las siguientes matrices:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix},\ j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ k = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

Es fácil comprobar que el conjunto

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

es cerrado para el producto con 1 como neutro y con inverso de -1 el mismo y del resto sus opuestos, así que forma un grupo de orden ocho llamado *grupo de los cuaternios*.

La tabla de multiplicación puede escribirse a partir de los productos

$$i \cdot i = -1,\ j \cdot j = -1,\ i \cdot j = k,\ j \cdot i = -k$$

y sería

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Claramente Q_2 *no es abeliano*.

Además una presentación estaría dada por:

$$Q_2 = \langle i, j;\ i^4 = 1,\ j^2 = i^2,\ ji = i^{-1}j \rangle.$$

Referencias

[1] A. Clark, *Elementos de Álgebra abstracta*, Alhambra (1970)

[2] D. S. Dummit & R. M. Foote, *Abstract Algebra*, Wiley (2004)

[3] J. B. Fraleigh, *Álgebra abstracta*, Addison-Wesley Iberoamericana (1987)

[4] J. A. Gallian, *Contemporary Abstract Algebra 6th ed.*, Houghton-Mifflin (2006)

[5] A.C.Hibbard, K.M. Levasseur, *Exploring Abstract Algebra with Mathematica*, Springer (1999)

[6] N. Jacobson, *Basic Algebra (2 vol.)* Freeman (1985)

[7] A. Jones, S. Morris & K. P, *Abstract Algebra and Famous Impossibilities*, Springer-Verlag New York (1994)

[8] A.I. Kostrikin, *Introducción al álgebra* McGraw-Hill (1992)

[9] S. Lang, *Algebra, 3rd edition*, Addison-Wesley (1997)

[10] W. Paulsen *Abstract Algebra, An interactive Approach*, CRC Press (2009)

[11] J. J. Rotman, *Advanced Modern Algebra*, Prentice Hall (2002)

[12] J. J. Rotman, *Galois Theory*, Universitext, Springer-Verlag New York (1990)

[13] I. Stewart, *Galois theory*, Chapman Hall (1973)

[14] J. Swallow, *Exploratory Galois Theory*, Cambridge U. P. (2004)