

Leandro Vendramin

Álgebra II

– Notas –

29 de agosto de 2020

Índice general

Parte I Grupos

1. Grupos y subgrupos	3
2. Grupos cíclicos	11
3. El grupo simétrico	15
Índice alfabético	19

Parte I

Grupos

Capítulo 1

Grupos y subgrupos

Antes de dar la definición de grupo recordemos que una operación binaria en un cierto conjunto X es una función $X \times X \rightarrow X$, $(x, y) \mapsto xy$. Observemos que la notación que utilizamos para esta operación binaria genérica es la misma que usualmente se usa para la multiplicación de números, aunque nuestra operación sea algo mucho más general. Por ejemplo, $(x, y) \mapsto x - y$ es una operación binaria en \mathbb{Z} pero no lo es en \mathbb{N} .

Definición 1.1. Un **grupo** es un conjunto no vacío G junto con una operación binaria en G que satisface las siguientes propiedades:

1. Asociatividad: $x(yz) = (xy)z$ para todo $x, y, z \in G$.
2. Existencia de elemento neutro: existe un elemento $e \in G$ tal que $ex = xe = x$ para todo $x \in G$.
3. Existencia del inverso: para cada $x \in G$ existe $y \in G$ tal que $xy = yx = e$.

El axioma sobre asociatividad que aparece en nuestra definición de grupo es suficiente para demostrar que todos los productos ordenado que podamos formar con los elementos x_1, x_2, \dots, x_n son iguales. Por ejemplo

$$(x_1 x_2)((x_3 x_4)x_5) = x_1(x_2(x_3(x_4 x_5))),$$

y en virtud de esta propiedad, podemos escribir sin ambigüedad $x_1 x_2 \cdots x_5$, sin preocuparnos por poner paréntesis.

Proposición 1.2. En un grupo G , cada $x \in G$ admite un único inverso $x^{-1} \in G$.

Demostración. Si $y, z \in G$ son ambos inversos del elemento $x \in G$, entonces, gracias a los axiomas que definen un grupo, tenemos que $z = z(xy) = (zx)y = 1y = y$. \square

Ejercicio 1.3. Demuestre que el elemento neutro de un grupo es único.

El elemento neutro de un grupo G será denotado por 1_G o simplemente como 1 cuando no haya peligro de confusión. El inverso de un elemento $x \in G$ será denotado por x^{-1} .

De la definición podemos obtener fácilmente otras propiedades de los inversos de elementos de un grupo:

1. $(x^{-1})^{-1} = x$ para todo $x \in G$.
2. $(xy)^{-1} = y^{-1}x^{-1}$ para todo $x, y \in G$.

Ejercicio 1.4. Demuestre que en un grupo G la ecuación $ax = b$ tiene a $x = a^{-1}b$ como única solución. Similarmente, $x = ba^{-1}$ es la única solución de la ecuación $xa = b$.

Definición 1.5. Un grupo G se dirá **abeliano** si $xy = yx$ para todo $x, y \in G$.

A veces, cuando tratemos con grupos abelianos, utilizaremos la notación aditiva. Eso significa que la operación binaria será $(x, y) \mapsto x + y$, el neutro será denotado por 0 y el inverso de un cierto elemento x será $-x$.

Definición 1.6. El **orden** $|G|$ de un grupo G es el cardinal de G . Un grupo G se dirá finito si $|G|$ es finito e infinito en caso contrario.

Notación 1.7. Sea G un grupo y sea $g \in G$. Si $k \in \mathbb{Z} \setminus \{0\}$, escribimos

$$\begin{aligned} g^k &= g \cdots g \quad (k - \text{veces}) & \text{si } k > 0, \\ g^k &= g^{-1} \cdots g^{-1} \quad (|k| - \text{veces}) & \text{si } k < 0. \end{aligned}$$

Por convención, además, $g^0 = 1$.

Ejercicio 1.8. Si G es un grupo, entonces

1. $(g^k)^l = g^{kl}$ para todo $g \in G$ y todo $k, l \in \mathbb{Z}$.
2. Si G es abeliano, entonces $(gh)^k = g^k h^k$ para todo $g, h \in G$ y todo $k \in \mathbb{Z}$.

Ejercicio 1.9. Sean G un grupo y $g \in G$. Demuestre que las funciones $L_g: G \rightarrow G$, $x \mapsto gx$, y $R_g: G \rightarrow G$, $x \mapsto xg$, son biyectivas.

Ejemplos 1.10. Ejemplos de grupos abelianos:

1. \mathbb{Z} , \mathbb{Q} , \mathbb{R} y \mathbb{C} con la suma usual.
2. Los enteros \mathbb{Z}/n módulo n con la suma usual.
3. $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ y $\mathbb{C} \setminus \{0\}$ con la multiplicación usual.
4. El conjunto $(\mathbb{Z}/p)^\times = \mathbb{Z} \setminus \{0\}$ de enteros módulo p inversibles con la multiplicación usual, donde p es un número primo.

Ejemplo 1.11. Sea $n \in \mathbb{N}$. El conjunto $\mathbb{G}_n = \{z \in \mathbb{C} : z^n = 1\}$ es un grupo abeliano con el producto usual de números complejos. También $\mathbb{G}_\infty = \cup_{n \geq 1} \mathbb{G}_n$ es un grupo abeliano.

Ejemplo 1.12. Sea $n \geq 2$. El conjunto $\mathbf{GL}_n(\mathbb{R})$ de matrices inversibles de $n \times n$ con la multiplicación usual de matrices es un grupo no abeliano.

Ejemplo 1.13. Sea X un conjunto. El conjunto \mathbb{S}_X de funciones $X \rightarrow X$ biyectivas con la composición de funciones es un grupo. Si $|X| \geq 3$, el grupo \mathbb{S}_X no es abeliano: sean tres elementos distintos $a, b, c \in X$ y sean $f: X \rightarrow X$ tal que $f(a) = b$, $f(b) = c$ y $f(c) = a$ y $g: X \rightarrow X$ tal que $g(a) = b$, $g(b) = a$ y $g(x) = x$ para todo $x \in X \setminus \{a, b\}$. Entonces $fg \neq gf$.

Si $X = \{1, 2, \dots, n\}$, \mathbb{S}_X será denotado por \mathbb{S}_n y se denominará el **grupo simétrico** de grado n . Notemos que $|\mathbb{S}_n| = n!$ y que \mathbb{S}_n es abeliano si y sólo si $n \in \{1, 2\}$. Cada elemento de \mathbb{S}_n es una función $f: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ y por lo tanto puede escribirse como nos resulte conveniente. Una notación bastante utilizada es la siguiente: escribiremos

$$\begin{pmatrix} 12345 \\ 32145 \end{pmatrix}$$

para denotar a la función $f: \{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3, 4, 5\}$ tal que $f(1) = 3$, $f(2) = 2$, $f(3) = 1$, $f(4) = 4$ y $f(5) = 5$.

Ejemplo 1.14 (el grupo de Klein). El grupo

$$K = \left\{ \text{id}, \begin{pmatrix} 1234 \\ 2143 \end{pmatrix}, \begin{pmatrix} 1234 \\ 3412 \end{pmatrix}, \begin{pmatrix} 1234 \\ 4321 \end{pmatrix} \right\}$$

es un grupo abeliano. Observar que K es subgrupo de \mathbb{S}_4 .

Ejemplo 1.15. Sabemos que el conjunto \mathbb{S}_3 de funciones $\{1, 2, 3\} \rightarrow \{1, 2, 3\}$ biyectivas es un grupo con la composición. El grupo \mathbb{S}_3 tiene orden seis y sus elementos son

$$\text{id}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix}.$$

Otra notación muy utilizada involucra la *descomposición de una permutación en ciclos disjuntos*. En este caso, los elementos de \mathbb{S}_3 serán escritos como

$$\text{id}, (12), (13), (23), (123), (132),$$

donde, por ejemplo, el símbolo (12) representa la función $\{1, 2, 3\} \rightarrow \{1, 2, 3\}$ tal que $1 \mapsto 2$, $2 \mapsto 1$ y $3 \mapsto 3$.

Más adelante veremos que la notación de una permutación como producto de ciclos disjuntos es de gran utilidad.

Ejemplo 1.16. Sea $n \in \mathbb{N}$. Las unidades de \mathbb{Z}/n forman un grupo con la multiplicación usual módulo n . La notación que utilizaremos es

$$\mathcal{U}(\mathbb{Z}/n) = \{x \in \mathbb{Z}/n : \text{mcd}(x, n) = 1\}.$$

En general, el orden de $\mathcal{U}(\mathbb{Z}/n)$ es $\varphi(n)$, donde φ denota a la función de Euler, es decir

$$\varphi(n) = |\{x \in \mathbb{Z} : 1 \leq x \leq n, \text{mcd}(x, n) = 1\}|.$$

Veamos un ejemplo concreto: $\mathcal{U}(\mathbb{Z}/8) = \{1, 3, 5, 7\}$. La tabla de multiplicación de este grupo es

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Ejemplo 1.17. Sean G y H grupos. El conjunto $G \times H$ es un grupo con la operación

$$(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2).$$

Esta estructura de grupo sobre el producto cartesiano $G \times H$ se conoce como el **producto directo** de G y H .

Si se utiliza la inducción, el ejemplo anterior puede generalizarse productos finitos de tres o más grupos.

Definición 1.18. Un subconjunto S de G es un **subgrupo** de G si se satisfacen las siguientes propiedades:

1. $1 \in S$,
2. $x \in S \implies x^{-1} \in S$, y además
3. $x, y \in S \implies xy \in S$.

Notación: S es un subgrupo de G si y sólo si $S \leq G$.

Podríamos reemplazar la primera condición de la definición de subgrupo y pedir simplemente que el conjunto sea no vacío.

Ejemplo 1.19 (subgrupos triviales). Si G es un grupo, entonces $\{1\}$ y G son subgrupos de G .

Ejemplo 1.20. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Ejemplo 1.21. $S^1 = \{z \in \mathbb{C} : |z| = 1\} \leq \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

Ejemplo 1.22. Para cada $n \in \mathbb{N}$, se define el grupo de raíces n -ésimas de la unidad como $U_n = \{z \in \mathbb{C} : z^n = 1\}$, es decir

$$U_n = \{1, \exp(2\pi i/n), \exp(4\pi i/n), \dots, \exp(2(n-1)\pi i/n)\}.$$

Entonces

$$U_n \leq \bigcup_{n \in \mathbb{N}} U_n \leq S^1 \leq \mathbb{C}^\times.$$

Ejemplo 1.23. $\mathbf{SL}_n(\mathbb{R}) = \{a \in \mathbf{GL}_n(\mathbb{R}) : \det(a) = 1\} \leq \mathbf{GL}_n(\mathbb{R})$. En efecto, la matriz identidad pertenece a $\mathbf{SL}_2(\mathbb{R})$ y luego $\mathbf{SL}_2(\mathbb{R})$ es no vacío. Además si $a, b \in \mathbf{SL}_n(\mathbb{R})$, entonces $ab^{-1} \in \mathbf{SL}_2(\mathbb{R})$ pues $\det(ab^{-1}) = \det(a)\det(b)^{-1} = 1$.

Ejercicio 1.24. Si G un grupo, el **centro**

$$Z(G) = \{g \in G : gh = hg \text{ para todo } h \in G\}$$

de G es un subgrupo de G .

Ejercicio 1.25. Si G es un grupo y $g \in G$, entonces el **centralizador**

$$C_G(g) = \{h \in G : gh = hg\}$$

de g en G es un subgrupo de G .

Ejercicio 1.26. Demuestre que $Z(\mathbb{S}_3) = \{\text{id}\}$ y calcule $C_{\mathbb{S}_3}((12))$.

Una forma fácil de chequear que un cierto subconjunto es un subgrupo es la siguiente:

Ejercicio 1.27. Sea G un grupo y sea S un subconjunto de G . Demuestre que S es un subgrupo de G si y sólo si S es no vacío y para todo $x, y \in G$ vale que $xy^{-1} \in G$.

Ejercicio 1.28. La intersección de subgrupos es también un subgrupo.

La unión de subgrupos no es, en general, un subgrupo. Para convencerse, basta por ejemplo ver qué pasa en el subgrupo de Klein.

Teorema 1.29. Si S es un subgrupo de \mathbb{Z} , entonces $S = m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$ para algún $m \in \mathbb{N}$.

Demostración. Si $S = \{0\}$, no hay nada para demostrar pues podemos tomar $m = 0$. Supongamos entonces que $S \neq \{0\}$ y sea $m = \min\{s \in S : s > 0\}$. Si $x \in S$, entonces $x = my + r$ para $y, r \in \mathbb{Z}$ con r tal que $0 \leq r < m$. Supongamos que $r \neq 0$. Como $x, m \in S$, entonces $r \in S$, una contradicción a la minimalidad de S . Luego $r = 0$ y entonces $x = my \in m\mathbb{Z}$. \square

Como la intersección de subgrupos es un subgrupo, el resultado anterior tiene además aplicaciones interesantes:

Ejemplo 1.30. Si $a, b \in \mathbb{Z}$ son tales que $ab \neq 0$, entonces

$$S = a\mathbb{Z} + b\mathbb{Z} = \{m \in \mathbb{Z} : m = ar + bs \text{ para } r, s \in \mathbb{Z}\}$$

es un subgrupo de \mathbb{Z} (ejercicio). El teorema anterior nos permite escribir a S como $S = d\mathbb{Z}$ para algún entero positivo d . Este entero d es el **máximo común divisor** de a y b , es decir $d = \text{mcd}(a, b)$.

Ejercicio 1.31. Sean $a, b \in \mathbb{Z}$ tales que $ab \neq 0$ y sea $d = \text{mcd}(a, b)$. Valen entonces las siguientes afirmaciones:

1. d simultáneamente a los enteros a y b .
2. Si $e \in \mathbb{Z}$ divide a los enteros a y b , entonces e también divide a d .

3. Existen $r, s \in \mathbb{Z}$ tales que $d = ar + bs$.

Observemos que dos enteros a y b serán **coprimos** si y sólo si $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

Ejemplo 1.32. Si S y T son subgrupos de \mathbb{Z} , entonces $S \cap T$ es también un subgrupo de \mathbb{Z} . Sabemos que $S = a\mathbb{Z}$ para algún $a \in \mathbb{N}$ y $T = b\mathbb{Z}$ para algún $b \in \mathbb{N}$. Además $S \cap T = m\mathbb{Z}$ para algún $m \in \mathbb{N}$ porque $S \cap T$ es también un subgrupo de \mathbb{Z} . Ese entero positivo m es el **mínimo común múltiplo** de a y b , es decir $m = \text{mcm}(a, b)$.

Ejercicio 1.33. Sean $a, b \in \mathbb{Z} \setminus \{0\}$ y sea $m = \text{mcm}(a, b)$. Valen entonces las siguientes propiedades:

1. m es simultáneamente divisible por a y b .
2. Si n es simultáneamente divisible por a y b , entonces n es divisible por m .

Ejercicio 1.34. Sean $a, b \in \mathbb{N}$, $d = \text{mcd}(a, b)$ y $m = \text{mcm}(a, b)$. Entonces $ab = dm$.

Ejercicio 1.35. Sea S un subgrupo de G y sea $g \in G$. Demuestre que gSg^{-1} es también un subgrupo de G . Notación: ${}^gS = gSg^{-1}$.

Definición 1.36. Sean G un grupo y X un subconjunto de G . El **subgrupo generado** por X se define como la intersección de todos los subgrupos de G que contienen a X , es decir

$$\langle X \rangle = \bigcap \{S : S \leq G, X \leq S\}.$$

Cuando el conjunto de generadores sea finito, se utilizará la siguiente notación. Si $X = \{g_1, \dots, g_k\}$, entonces $\langle X \rangle = \langle \{g_1, \dots, g_k\} \rangle = \langle g_1, \dots, g_k \rangle$.

Ejercicio 1.37. Demuestre que $\langle X \rangle$ será el menor subgrupo de G que contiene a X , es decir que si S es un subgrupo de G tal que $X \subseteq S$, entonces $\langle X \rangle \subseteq S$.

Ejercicio 1.38. Demuestre que

$$\langle X \rangle = \{x_1^{n_1} \cdots x_k^{n_k} : k \in \mathbb{N}, x_1, \dots, x_k \in X, 0 \leq n_1, \dots, n_k \leq 1\}.$$

Un ejemplo importante de un grupo generado por dos elementos es el grupo diedral.

Ejemplo 1.39. Para $n \geq 2$ y $\theta = 2\pi/n$ sean

$$r = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Se define entonces al **grupo diedral** \mathbb{D}_n como el subgrupo de $\text{GL}(2, \mathbb{R})$ generado por r y s , es decir $\mathbb{D}_n = \langle r, s \rangle$. Observar que

$$s^2 = r^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad srs = r^{-1}.$$

Además $|\mathbb{D}_n| = 2n$.

Es conveniente mencionar que la notación que suele usarse para el grupo diedral no es estándar. Para nosotros \mathbb{D}_n será el grupo diedral de orden $2n$.

Definición 1.40. El **conmutador** $[G, G]$ de G es el subgrupo generado por los conmutadores, es decir

$$[G, G] = \langle [x, y] \mid x, y \in G \rangle,$$

donde $[x, y] = xyx^{-1}y^{-1}$ es el conmutador de x e y .

El conmutador de un grupo G a veces se conoce como el **subgrupo derivado** de G . Más adelante se justificará esta terminología.

Ejemplo 1.41. $[\mathbb{Z}, \mathbb{Z}] = \{0\}$ pues \mathbb{Z} es un grupo abeliano. Obviamente, en este ejemplo utilizamos la notación aditiva.

Ejercicio 1.42. Demuestre que $[\mathbb{S}_3, \mathbb{S}_3] = \{\text{id}, (123), (132)\}$.

Es natural preguntarse por qué el conmutador se define como el subgrupo generado por los conmutadores y no directamente como el subconjunto formado por los conmutadores. En realidad, esto se hace porque no es cierto que el subconjunto formado por los conmutadores sea un subgrupo, aunque no es muy fácil conseguir ejemplos. Con ayuda de algún software de matemática que permita trabajar con grupos, se pueden verificar los ejemplos que mencionamos a continuación. El libro de Carmichael muestra el siguiente ejemplo.

Ejemplo 1.43. Sea G el subgrupo de \mathbb{S}_{16} generado por las permutaciones

$$\begin{aligned} a &= (13)(24), & b &= (57)(6, 8), \\ c &= (911)(10, 12), & d &= (13, 15)(14, 16), \\ e &= (13)(5, 7)(9, 11), & f &= (12)(3, 4)(13, 15), \\ g &= (56)(7, 8)(13, 14)(15, 16), & h &= (9\ 10)(11\ 12). \end{aligned}$$

Puede demostrarse que $[G, G]$ tiene orden 16 y que el conjunto de conmutadores tiene tamaño 15.

Mencionamos otro ejemplo, encontrado por Guralnick antes de que el uso de computadoras en teoría de grupos fuera masivo.

Ejemplo 1.44. El grupo

$$G = \langle (135)(246)(7\ 11\ 9)(8\ 12\ 10), (394\ 10)(58)(67)(11\ 12) \rangle.$$

tiene orden 96 tal que el subgrupo de conmutadores no es igual al conjunto de conmutadores. Puede demostrarse además que es el menor grupo finito con esta propiedad.

Si X e Y son subconjuntos de un grupo G , definimos

$$XY = \{xy : x \in X, y \in Y\}.$$

Observemos que

$$H \cup K \subseteq HK \subseteq \langle H \cup K \rangle.$$

Nos interesa saber cuándo XY es un subgrupo de G .

Proposición 1.45. *Sean H y K subgrupos de un grupo G . Entonces HK es un subgrupo de G si y sólo si $HK = KH$.*

Demostración. Supongamos que $HK = KH$. Como $1 \in H \cap K$, el conjunto HK es no vacío. Si $h \in H$ y $k \in K$, entonces $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Además $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$ y luego HK es cerrado para la multiplicación.

Supongamos ahora que HK es un subgrupo de G . Como $H \subseteq HK$, $K \subseteq HK$ y además HK es cerrado para la multiplicación, $KH \subseteq (HK)(HK) \subseteq HK$. Recíprocamente, sea $g \in HK$. Como $g^{-1} \in HK$, existen $h \in H$ y $k \in K$ tales que $g^{-1} = hk$. Luego $HK \subseteq KH$ pues $g = k^{-1}h^{-1} \in KH$. \square

El siguiente resultado será de mucha utilidad más adelante:

Teorema 1.46. *Sean H y K subgrupos finitos de un grupo G . Entonces*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Demostración. Sea $Q = H \cap K$ y sea

$$\theta: H \times K \rightarrow HK, \quad \theta(h, k) = hk,$$

La función θ es claramente sobreyectiva.

Vamos a demostrar que si $x \in HK$, entonces $|\theta^{-1}(x)| = |H \cap K|$. Si $x \in HK$, entonces $x = hk$ para algún $h \in H$ y $k \in K$. Alcanza con ver que

$$\theta^{-1}(x) = \{(h\gamma, \gamma^{-1}k) : \gamma \in H \cap K\}.$$

Veamos que la inclusión no trivial. Si $(h_1, k_1) \in \theta^{-1}(x)$, entonces

$$\theta(h_1, k_1) = h_1k_1 = x = hk.$$

En consecuencia, $\gamma = h^{-1}h_1 = kk_1^{-1} \in H \cap K$. Luego $(h_1, k_1) = (h\gamma, \gamma^{-1}k)$ para algún $\gamma \in H \cap K$. Como la otra inclusión es trivial, el teorema queda demostrado al observar que

$$|HK| = \frac{|H \times K|}{|H \cap K|} = \frac{|H||K|}{|H \cap K|}. \quad \square$$

Capítulo 2

Grupos cíclicos

Definición 2.1. Un grupo G se dice **cíclico** si $G = \langle g \rangle$ para algún $g \in G$.

Un grupo cíclico G generado por el elemento g estará compuesto entonces por las potencias de g , es decir $G = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$. Todo grupo cíclico es entonces en particular un grupo abeliano.

Ejemplos 2.2.

1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
2. $\mathbb{Z}/n = \langle 1 \rangle$.
3. $U_n = \langle \exp(2i\pi/n) \rangle$.

Ejemplo 2.3. $\mathcal{U}(\mathbb{Z}/8) \neq \langle 3 \rangle$. De hecho, $\langle 3 \rangle = \{1, 3\} \subsetneq \{1, 3, 5, 7\} = \mathcal{U}(\mathbb{Z}/8)$.

Antes de resolver el siguiente ejercicio, es conveniente recordar cómo son los subgrupos de \mathbb{Z} .

Ejercicio 2.4. Todo subgrupo de un grupo cíclico es también un grupo cíclico.

Definición 2.5. Sean G un grupo y $g \in G$. El **orden** de g se define como el orden del subgrupo generado por g . Notación: $|g| = |\langle g \rangle|$.

Proposición 2.6. Sean G un grupo, $g \in G$ y $n \in \mathbb{N}$. Las siguientes afirmaciones son equivalentes:

1. $|g| = n$.
2. $n = \min\{k \in \mathbb{N} : g^k = 1\}$.
3. Para todo $k \in \mathbb{Z}$, $g^k = 1 \iff n \mid k$.
4. $\langle g \rangle = \{1, g, \dots, g^{n-1}\}$ y los $1, g, \dots, g^{n-1}$ son todos distintos.

Demostración. Veamos que (1) \implies (2). Si $g = 1$ entonces $m = 1$. Supongamos entonces que $g \neq 1$. Tomemos el mínimo $k > 1$ tal que $1, g, g^2, \dots, g^{k-1}$ son elementos distintos, y sea $j \in \{0, \dots, k-1\}$ tal que $g^k = g^j$. Afirmamos que $g^k = 1$. Si $g^k = g^j$ para algún $j \geq 1$, entonces $g^{k-j} = 1$ con $k-j \leq k-1 < k$, una contradicción. Afirmamos ahora que $\langle g \rangle = \{1, g, g^2, \dots, g^{k-1}\}$. La inclusión \supseteq trivial.

Para probar la otra inclusión, sea $g^l \in \langle g \rangle$. Escribimos $l = kq + r$ con $0 \leq r < k$, y entonces $g^l = g^{kq+r} = g^r$.

Ahora demostremos que (2) \implies (3). Supongamos que $g^k = 1$. Si escribimos $k = nt + r$ con $0 \leq r < n$, entonces $g^k = g^{nt+r} = g^r$. La minimalidad de n implica entonces que $r = 0$ y luego n divide a k . Recíprocamente, si $k = nt$ para algún $t \in \mathbb{Z}$, entonces $g^k = (g^n)^t = 1$.

Demostremos que (3) \implies (4). Es trivial que $\{1, g, \dots, g^{n-1}\} \subseteq \langle g \rangle$. Para demostrar la otra inclusión, escribimos $k = nt + r$ con $0 \leq r \leq n - 1$. Entonces

$$g^k = g^{nt+r} = (g^n)^t g^r = g^r$$

pues por hipótesis $g^n = 1$. Para ver que los $1, g, \dots, g^{n-1}$ son todos distintos, basta observar que si $g^k = g^l$ con $0 \leq k < l \leq n - 1$, entonces, como $g^{l-k} = 1$ y además $0 < l - k \leq n - 1$, se concluye que $k = l$, una contradicción.

La implicación (4) \implies (1) es trivial. \square

Veamos una aplicación de la proposición anterior:

Corolario 2.7. Si G es un grupo y $g \in G$ tiene orden n , entonces

$$|g^m| = \frac{n}{\text{mcd}(n, m)}.$$

Demostración. Sea k tal que $(g^m)^k = 1 = g^{mk}$. Esto es equivalente a decir que n divide a km , pues g tiene orden n . A su vez esto es equivalente a pedir que n/d divida a mk/d , donde $d = \text{mcd}(n, m)$. En consecuencia, como los enteros n/d y m/d son coprimos, $(g^m)^k = 1$ es equivalente a pedir que n/d divida a k , que implica que g^m tiene orden n/d . \square

Ejercicio 2.8. Sea G un grupo y sea $g \in G$. Demuestre que las siguientes afirmaciones son equivalentes:

1. g tiene orden infinito.
2. El conjunto $\{k \in \mathbb{N} : g^k = 1\}$ es vacío.
3. Si $g^k = 1$, entonces $k = 0$.
4. Si $k \neq l$, entonces $g^k \neq g^l$.

Ejercicio 2.9. Sea G un grupo y sea $g \in G \setminus \{1\}$. Demuestre las siguientes afirmaciones:

1. $|g| = 2$ si y sólo si $g = g^{-1}$.
2. $|g| = |g^{-1}|$.
3. Si $|g| = nm$ y $\text{mcd}(n, m) = 1$, entonces $|g^m| = n$.

Ejercicio 2.10. Sea $G = \langle g \rangle$ un grupo cíclico.

1. Si G es infinito, los únicos generadores de G son g y g^{-1} .
2. Si G es finito de orden n , $G = \langle g^k \rangle$ si y sólo si k es coprimo con n .

El siguiente ejercicio es un caso particular del teorema de Cauchy, que veremos más adelante.

Ejercicio 2.11. Demuestre que todo grupo de orden par contiene un elemento de orden dos.

Mostremos ahora algunos órdenes de elementos concretos:

Ejemplo 2.12. En \mathbb{S}_3 tenemos los siguiente:

$$|\text{id}| = 1, \quad |(12)| = |(13)| = |(23)| = 2, \quad |(123)| = |(132)| = 3.$$

Ejemplo 2.13. En \mathbb{Z} todo elemento no nulo tiene orden infinito.

Ejemplo 2.14. En $\mathbb{Z} \times \mathbb{Z}/6$ hay elementos de orden finito y elementos de orden infinito. Por ejemplo, $(1, 0)$ tiene orden infinito y $(0, 1)$ tiene orden seis.

Ejercicio 2.15. Calcule los órdenes de los elementos de $\mathbb{Z}/6$.

Ejemplo 2.16. La matriz $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$ tiene orden infinito.

Ejercicio 2.17. Calcule el orden de la matrix $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$.

Ejercicio 2.18. Demuestre que en \mathbb{D}_n se tiene $|r^j s| = 2$ y $|r^j| = n/\text{mcd}(n, j)$. Demuestre además que \mathbb{D}_n tiene orden $2n$.

Capítulo 3

El grupo simétrico

Sea $\sigma \in \mathbb{S}_n$. Diremos que σ es un r -ciclo si existen $a_1, \dots, a_r \in \{1, \dots, n\}$ tales que $\sigma(j) = j$ para todo $j \notin \{a_1, \dots, a_r\}$ y

$$\sigma(a_i) = \begin{cases} a_{i+1} & \text{si } i < r, \\ a_1 & \text{si } i = r. \end{cases}$$

Ejemplos 3.1. Por ejemplo, (12), (13) y (23) son 2-ciclos de \mathbb{S}_3 . Los 2-ciclos se denominan **trasposiciones**. Las permutaciones (123) y (132) son 3-ciclos de \mathbb{S}_3 .

Dos permutaciones $\sigma, \tau \in \mathbb{S}_n$ se dicen **disjuntas** si para todo $j \in \{1, \dots, n\}$ se tiene que $\sigma(j) = j$ o bien $\tau(j) = j$.

Ejemplos 3.2. Las permutaciones (134) y (25) son disjuntas. En cambio, las permutaciones (134) y (24) no lo son.

Si $\sigma \in \mathbb{S}_n$ y j es tal que $\sigma(j) = j$, entonces j es un punto fijo de σ . En cambio, los j tales que $\sigma(j) \neq j$ son los puntos movidos por σ .

Observación 3.3. Las permutaciones disjuntas conmutan.

Observación 3.4. Cada permutación puede escribirse como producto de trasposiciones. Para demostrar esta afirmación procederemos de la siguiente forma. Supongamos que las personas invitadas a un concierto se sientan en la primera fila, pero sin respetar el orden que figura en la lista de invitados. ¿Qué podemos hacer para ordenar a esas personas? Primero identificamos a la persona que debería sentarse en el primer lugar y le pedimos que intercambie asientos con la persona sentada en esa primera butaca. Luego identificamos a la persona que debería sentarse en el segundo lugar y le pedimos que intercambie asientos con la persona que ocupe la segunda butaca. Hacemos lo mismo con el tercer lugar, con el cuarto... y una vez terminado el proceso, gracias a haber utilizado finitas trasposiciones, habremos conseguido acomodar correctamente a cada una de las personas invitadas al concierto.

A continuación demostraremos que toda permutación puede escribirse como producto de ciclos disjuntos, algo que usamos en el primer capítulo en el caso particular del grupo \mathbb{S}_3 . Necesitamos el siguiente lema:

Lema 3.5. *Sea $\sigma = \alpha\beta \in \mathbb{S}_n$ con α y β permutaciones disjuntas. Si $\alpha(i) \neq i$, entonces $\sigma^k(i) = \alpha^k(i)$ para todo $k \geq 0$.*

Demostración. Sin perder generalidad podemos suponer que $k > 0$. En ese caso, $\sigma^k(i) = (\alpha\beta)^k(i) = \alpha^k(\beta^k(i)) = \alpha^k(i)$. \square

Ahora sí estamos en condiciones de demostrar el teorema:

Teorema 3.6. *Toda $\sigma \in \mathbb{S}_n \setminus \{id\}$ puede escribirse como producto de ciclos disjuntos de longitud ≥ 2 . Además esta descomposición es única salvo el orden de los factores involucrados.*

Demostración. Procederemos por inducción en el número k de elementos del conjunto $\{1, \dots, n\}$ movidos por σ . Si $k = 2$ el resultado es trivial. Supongamos entonces que el resultado es cierto para todas las permutaciones que mueven $< k$ puntos. Sea $i_1 \in \{1, \dots, n\}$ tal que $\sigma(i_1) \neq i_1$. Sea entonces $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$... Sabemos que existe $r \in \mathbb{N}$ tal que $\sigma(i_r) = i_1$ (pues, de lo contrario, si $\sigma(i_r) = i_j$ para algún $j \in \{2, \dots, n\}$, entonces $\sigma(i_{j-1}) = i_j = \sigma(i_r)$, una contradicción a la biyectividad de σ). Sea $\sigma_1 = (i_1 \cdots i_r)$. La hipótesis inductiva nos dice que, como $\sigma_1^{-1}\sigma$ mueve $< k$ puntos, podemos escribir $\sigma_1^{-1}\sigma = \sigma_2 \cdots \sigma_s$, donde $\sigma_2, \dots, \sigma_s$ son ciclos disjuntos. Esto implica que $\sigma = \sigma_1\sigma_2 \cdots \sigma_s$, tal como queríamos.

Demostremos ahora la unicidad. Supongamos que $\sigma = \sigma_1 \cdots \sigma_s = \tau_1 \cdots \tau_t$, con $s > 0$. Sea $i_1 \in \{1, \dots, n\}$ tal que $\sigma(i_1) \neq i_1$. El lema implica que $\sigma^k(i_1) = \sigma_1^k(i_1)$ para todo $k \geq 0$. Existe entonces $j \in \{1, \dots, t\}$ tal que $\tau_j(i_1) \neq i_1$. Como los τ_k conmutan, sin perder generalidad podemos suponer que $j = 1$. Luego $\sigma^k(i_1) = \tau_1^k(i_1)$ para todo $k \geq 0$. Esto implica que $\sigma_1 = \tau_1$ y entonces $\sigma_2 \cdots \sigma_s = \tau_2 \cdots \tau_t$. Al repetir el argumento, vemos que $s = t$ y luego $\sigma_j = \tau_j$ para todo j . \square

Corolario 3.7.

1. $\mathbb{S}_n = \langle (ij) : i < j \rangle$.
2. $\mathbb{S}_n = \langle (12), (13), \dots, (1n) \rangle$.
3. $\mathbb{S}_n = \langle (12), (23), \dots, (n-1n) \rangle$.
4. $\mathbb{S}_n = \langle (12), (12 \cdots n) \rangle$.

Demostración. Ya demostramos que toda permutación puede escribirse como producto de trasposiciones. Otra demostración puede obtenerse al usar el teorema anterior ya que

$$(a_1 \cdots a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2).$$

Para demostrar la segunda afirmación hay que usar la primera afirmación y las fórmulas

$$(1i)(1j)(1i) = (ij)$$

válidas siempre que $i \neq j$.

Para la tercera afirmación escribimos a σ como producto de trasposiciones y luego observamos que

$$(13) = (12)(23)(12), \quad (1k+1) = (kk+1)(1k)(kk+1)$$

para todo $k \geq 3$.

Por último, la cuarta afirmación se obtiene al utilizar la tercera propiedad junto con la fórmula

$$(12 \cdots n)^{k-1} (12) (12 \cdots n)^{1-k} = (kk+1),$$

válida para todo $k \geq 1$. □

Cada permutación tiene asociada una matriz de permutación. Por ejemplo, para $\sigma = \text{id} \in \mathbb{S}_3$ se tiene a P_σ como la matriz identidad de 3×3 . Para la permutación $\sigma = (123)$ se tiene $P_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. En general, si $\sigma \in \mathbb{S}_n$, entonces

$$P_\sigma = \sum_{i=1}^n E_{\sigma(i),i},$$

donde $E_{i,j}$ es la matriz con un uno en la posición (i,j) e igual a cero en todas las otras entradas. Recordemos que valen las siguientes fórmulas

$$E_{i,j}E_{k,l} = \begin{cases} E_{i,l} & \text{si } j = k, \\ 0 & \text{si } j \neq k. \end{cases} \quad (3.1) \quad \boxed{\text{eq:E}}$$

Es claro que toda matriz de permutación tendrá un único uno en cada fila y cada columna y que el resto de las entradas serán todas iguales a cero. Luego el determinante de una matriz de permutación será ± 1 .

Proposición 3.8. Si $\sigma, \tau \in \mathbb{S}_n$, entonces $P_{\sigma\tau} = P_\sigma P_\tau$.

Demostración. Es un cálculo directa que utiliza la fórmula (3.1). Tenemos

$$\begin{aligned} P_\sigma P_\tau &= \left(\sum_{i=1}^n E_{\sigma(i),i} \right) \left(\sum_{j=1}^n E_{\tau(j),j} \right) \\ &= \sum_{i=1}^n \sum_{j=1}^n E_{\sigma(i),i} E_{\tau(j),j} = \sum_{j=1}^n E_{\sigma(\tau(j)),j} = P_{\sigma\tau}, \end{aligned}$$

ya que la suma doble será nula a menos que $i = \tau(j)$. □

Definición 3.9. El **signo** de una permutación $\sigma \in \mathbb{S}_n$ se define como el determinante de la matriz P_σ , es decir $\text{signo}(\sigma) = \det P_\sigma$. Una permutación σ se dirá **par** si $\text{signo}(\sigma) = 1$ e **impar** si $\text{signo}(\sigma) = -1$.

Ejemplos 3.10. La identidad es una permutación par y todo 3-ciclo es también una permutación par. Cualquier trasposición es una permutación impar.

Toda permutación puede escribirse como producto de trasposiciones, aunque no de forma única. Sin embargo, puede demostrarse el siguiente resultado. Si σ se escribe como producto de trasposiciones $\sigma = \sigma_1 \cdots \sigma_s$, entonces

$$\text{signo}(\sigma) = (-1)^s.$$

En particular, σ es una permutación par si y sólo si s es par.

Proposición 3.11. Si $\sigma, \tau \in \mathbb{S}_n$, entonces $\text{signo}(\sigma\tau) = (\text{signo } \sigma)(\text{signo } \tau)$.

Demostración. Es fácil pues

$$\text{signo}(\sigma\tau) = \det(P_\sigma P_\tau) = (\det P_\sigma)(\det P_\tau) = \text{signo}(\sigma) \text{signo}(\tau). \quad \square$$

Índice alfabético

Centralizador
de un elemento, 7

Centro
de un grupo, 7

Grupo, 3
abeliano, 4
cíclico, 11
de Klein, 5
diedral, 8
finito, 4
infinito, 4
orden de un, 4
simétrico, 5

Orden

de un elemento de un grupo, 11

Permutación
impar, 17
par, 17

Producto
directo de grupos, 6

Signo
de una permutación, 17

Subgrupo
conjugado, 8
conmutador, 9
derivado, 9
generado por un conjunto, 8