Leandro Vendramin

Álgebra II

– Notas –

1 de septiembre de 2020

Índice general

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 $X \times X \to X$, $(x,y) \mapsto xy$. 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 ordenados que podamos formar con los elementos $x_1, x_2, \ldots, x_n$ son iguales. Por ejemplo

$$(x_1x_2)((x_3x_4)x_5) = x_1(x_2(x_3(x_4x_5))),$$

y en virtud de esta propiedad, podemos escribir sin ambigüedad $x_1x_2\cdots x_5$, sin preocuparnos por poner paréntesis. Esta observación suele demostrarse por inducción, así se hace por ejemplo en el libro de Lang. Daremos una demostración mucho más sencilla en el capítulo 5, como aplicación del teorema de Cayley.

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 $z = z(xy) = (zx)y = 1y = y$. □

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 $L_g \colon G \to G$, $x \mapsto gx$, y $R_g \colon G \to G$, $x \mapsto xg$, 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 $(\mathbb{Z}/p)^\times = \mathbb{Z}/p \setminus \{0\}$ 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 $G_n = \{z \in \mathbb{C} : z^n = 1\}$ es un grupo abeliano con el producto usual de números complejos. También $\cup_{n \geq 1} G_n$ 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 $X \to X$ 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 $f\colon X \to X$ biyectiva tal que $f(a) = b$, $f(b) = c$ y $f(c) = a$ y $g\colon X \to X$ biyectiva 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 $X = \{1, 2, \ldots, n\}$, $\mathbb{S}_X$ 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 $f\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ 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 $f\colon \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ 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

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

es un grupo abeliano. Observar que K está contenido en $\mathbb{S}_4$.

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

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

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

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

donde, por ejemplo, el símbolo (12) representa la función $\{1, 2, 3\} \to \{1, 2, 3\}$ 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

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

En general, el orden de $\mathscr{U}(\mathbb{Z}/n)$ 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: $\mathscr{U}(\mathbb{Z}/8) = \{1,3,5,7\}$. 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. Si G es un grupo, entonces $\{1\}$ y G son subgrupos de G.

Ejemplo 1.20. $2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

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

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

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

Entonces

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

Ejercicio 1.23. 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 1.24. 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 1.25. Demuestre que $Z(\mathbb{S}_3) = \{\mathrm{id}\}$ y calcule $C_{\mathbb{S}_3}((12))$.

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

Ejercicio 1.26. 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 $xy^{-1} \in G$.

Ejemplo 1.27. $\mathbf{SL}_n(\mathbb{R}) = \{a \in \mathbf{GL}_n(\mathbb{R}) : \det(a) = 1\} \leq \mathbf{GL}_n(\mathbb{R})$. 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 1.28. 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 $m \in \mathbb{N}_0$.*

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 $x = my \in m\mathbb{Z}$. □

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 $d = \mathrm{mcd}(a, b)$.

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

1. d divide 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. Exiten $r,s \in \mathbb{Z}$ 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 el **conjugado** gSg^{-1} de S por g 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

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

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

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

Ejercicio 1.38. Demuestre que

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

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

Ejemplo 1.39. El conjunto

$$D_4 = \{\text{id}, (1234), (1432), (13)(24), (14)(23), (12)(34), (24), (13)\}$$

es un subgrupo no abeliano de $\mathbb{S}_4$.

Ejemplo 1.40. 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 $\mathbf{GL}(2,\mathbb{R})$ 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 1.41. 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 1.42. $[\mathbb{Z},\mathbb{Z}] = \{0\}$ pues $\mathbb{Z}$ es un grupo abeliano. Obviamente, en este ejemplo utilizamos la notación aditiva.

Ejercicio 1.43. Demuestre que $[\mathbb{S}_3,\mathbb{S}_3] = \{\mathrm{id}, (123), (132)\}$.

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.

Ejemplo 1.44. Sea G el subgrupo de $\mathbb{S}_{16}$ generado por las permutaciones

$$\begin{aligned}
a &= (13)(24), & b &= (57)(68),\\
c &= (9\,11)(10\,12), & d &= (13\,15)(14\,16),\\
e &= (13)(57)(9\,11), & f &= (12)(34)(13\,15),\\
g &= (56)(78)(13\,14)(15\,16), & h &= (9\,10)(11\,12).
\end{aligned}$$

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 1.45. El grupo

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

tiene orden 96 y su subgrupo de conmutadores de G 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. Observemos que $HK \leq G$ si y sólo si $\langle H \cup K \rangle = HK$.

Proposición 1.46. *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 $g = k^{-1}h^{-1} \in KH$. □

El siguiente resultado será de mucha utilidad más adelante:

Teorema 1.47. *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

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

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

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

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. $G_n = \langle \exp(2i\pi/n) \rangle$.

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

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. $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$ *y los* $1, g, \ldots, g^{n-1}$ *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 $1, g, g^2, \ldots, g^{k-1}$ son elementos distintos, y sea $j \in \{0, \ldots, k-1\}$ 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 $\langle g \rangle = \{1, g, g^2, \ldots, g^{k-1}\}$. 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 $\{1, g, \ldots, g^{n-1}\} \subseteq \langle g \rangle$. 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 $1, g, \ldots, g^{n-1}$ 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. □

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. □

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 un grupo abeliano. Demuestre que $T(G) = \{g \in G : |g| < \infty\}$ es un subgrupo de G. Calcule $T(\mathbb{C}^\times)$.

Ejercicio 2.11. 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.

xca:orden2 **Ejercicio 2.12.** Demuestre que todo grupo de orden par contiene un elemento de orden dos.

Mostremos ahora algunos órdenes de elementos concretos:

Ejemplo 2.13. En $\mathbb{S}_3$ tenemos los siguiente:

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

Ejemplo 2.14. En $\mathbb{Z}$ todo elemento no nulo tiene orden infinito.

Ejemplo 2.15. 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 2.16. Calcule los órdenes de los elementos de $\mathbb{Z}/6$.

Ejemplo 2.17. La matriz $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$ tiene orden infinito.

Ejercicio 2.18. Calcule el orden de la matrix $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$.

Ejercicio 2.19. Demuestre que en $\mathbb{D}_n$ se tiene $|r^j s| = 2$ y $|r^j| = n/\operatorname{mcd}(n, j)$. 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 $a_1, \ldots, a_r \in \{1, \ldots, n\}$ tales que $\sigma(j) = j$ para todo $j \notin \{a_1, \ldots, a_r\}$ 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 $j \in \{1, \ldots, n\}$ 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, $\sigma^k(i) = (\alpha\beta)^k(i) = \alpha^k(\beta^k(i)) = \alpha^k(i)$. □

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 $\{1,\ldots,n\}$ 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 $i_1 \in \{1,\ldots,n\}$ 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 $j \in \{2,\ldots,n\}$, 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 $\sigma_2, \ldots, \sigma_s$ son ciclos disjuntos. Esto implica que $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$, tal como queríamos.

Demostremos ahora la unicidad. Supongamos que $\sigma = \sigma_1 \cdots \sigma_s = \tau_1 \cdots \tau_t$, con $s > 0$. Sea $i_1 \in \{1,\ldots,n\}$ 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 $j \in \{1,\ldots,t\}$ tal que $\tau_j(i_1) \neq i_1$. Como los t_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. □

Corolario 3.7.

1. $\mathbb{S}_n = \langle (ij) : i < j \rangle$.
2. $\mathbb{S}_n = \langle (12), (13), \ldots, (1n) \rangle$.
3. $\mathbb{S}_n = \langle (12), (23), \ldots, (n-1\,n) \rangle$.
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 $\sigma = \mathrm{id} \in \mathbb{S}_3$ 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

$$E_{i,j}E_{k,l} = \begin{cases} E_{i,l} & \text{si } j = k, \\ 0 & \text{si } j \neq k. \end{cases} \tag{3.1}$$ 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 $\mathrm{signo}(\sigma) = \det P_\sigma$. Una permutación σ se dirá **par** si $\mathrm{signo}(\sigma) = 1$ e **impar** si $\mathrm{signo}(\sigma) = -1$.

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 traposiciones $\sigma = \sigma_1 \cdots \sigma_s$, 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

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

Ejemplo 3.12. Vamos a demostrar que si $n \geq 3$ entonces $Z(\mathbb{S}_n) = \{\text{id}\}$. Supongamos que $Z(\mathbb{S}_n) \neq \{\text{id}\}$ y sea $\sigma \in Z(\mathbb{S}_n)$ tal que $\sigma(i) = j$ para $i \neq j$. Como $n \geq 3$, existe $k \in \{1, \ldots, n\} \setminus \{i, j\}$ y entonces $\tau = (jk) \in \mathbb{S}_n$. Como σ es central,

$$j = \sigma(i) = \tau\sigma\tau^{-1}(i) = \tau(\sigma(i)) = \tau(j) = k,$$

una contradicción.

El **grupo alternado**

$$\mathbb{A}_n = \{\sigma \in \mathbb{S}_n : \text{signo}(\sigma) = 1\}$$

es el subgrupo de $\mathbb{S}_n$ formado por las permutaciones de signo positivo. Se demuestra que $|\mathbb{A}_n| = n!/2$.

Ejemplo 3.13. Es fácil verificar que $\mathbb{A}_3 = \{\text{id}, (123), (132)\}$ y que

$$\mathbb{A}_4 = \{\text{id}, (234), (243), (12)(34), (123), (124), \\ (132), (134), (13)(24), (142), (143), (14)(23)\}.$$

pro:A_n3ciclos **Proposición 3.14.** $\mathbb{A}_n = \langle\{\textit{3-ciclos}\}\rangle$.

Demostración. Todo 3-ciclo es una permutación par pues $(ijk) = (ik)(ij)$. Demostremos entonces la otra inclusión. Sea $\sigma \in \mathbb{A}_n$. Escribimos $\sigma = \sigma_1 \cdots \sigma_s$ para algún entero s par y $\sigma_1, \ldots, \sigma_s$ trasposiciones. Para completar la demostración de la proposición basta utilizar las fórmulas

$$(kl)(ij) = (kl)(ki)(ki)(ij) = (kil)(ijk), \quad (ijk) = (ik)(ij). \qquad \square$$

Veamos algunas aplicaciones sencillas:

Ejemplo 3.15. Veamos que si $n \geq 5$ entonces $[\mathbb{A}_n, \mathbb{A}_n] = \mathbb{A}_n$. Vamos a demostrar la inclusión no trivial y para eso basta con observar que $\mathbb{A}_n$ está generado por 3-ciclos y que, como $n \geq 5$, cada 3-ciclo puede escribirse como producto de conmutadores. En efecto,

$$(abc) = [(acd),(ade)][(ade),(abd)],$$

donde $\#\{a,b,c,d,e\} = 5$.

Ejemplo 3.16. Si $n \geq 3$ entonces $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$. Primero veamos que $[\mathbb{S}_n, \mathbb{S}_n] \subseteq \mathbb{A}_n$. Si $\sigma \in [\mathbb{S}_n, \mathbb{S}_n]$, digamos $\sigma = [\sigma_1, \tau_1][\sigma_2, \tau_2] \cdots [\sigma_k, \tau_k]$, entonces

$$\text{signo}(\sigma) = \text{signo}([\sigma_1, \tau_1]) \cdots \text{signo}([\sigma_k, \tau_k]) = 1.$$

Recíprocamente, si $\sigma \in \mathbb{A}_n$, la proposición anterior nos dice que podemos escribir a σ como producto de 3-ciclos. De aquí el resultado se obtiene inmediatamente pues cada 3-ciclo es un conmutador, tal como vemos en la siguiente fórmula

$$(abc) = (ab)(ac)(ab)(ac) = [(ab),(ac)] \in [\mathbb{S}_n, \mathbb{S}_n].$$

Capítulo 4
El teorema de Lagrange

Sean G un grupo y H un subgrupo de G. Diremos que dos elementos $x, y \in G$ son equivalentes a izquierda módulo H si $x^{-1}y \in H$. Usaremos la siguiente notación:

$$x \equiv y \text{ mód } H \iff x^{-1}y \in H.$$

Ejercicio 4.1. Demuestre que hemos definido una relación de equivalencia. Esto significa que se tienen las siguientes propiedades:

1. $x \equiv x$ mód H para todo x.
2. Si $x \equiv y$ mód H, entonces $y \equiv x$ mód H.
3. Si $x \equiv y$ mód H y además $y \equiv z$ mód H, entonces $x \equiv z$ mód H.

Las clases de equivalencia de esta relación módulo H son los conjuntos de la forma $xH = \{xh : h \in H\}$ pues la clase de un cierto elemento $x \in G$ es el conjunto

$$\{y \in G : x \equiv y \text{ mód } H\} = \{y \in G : x^{-1}y \in H\} = \{y \in G : y \in xH\} = xH.$$

El conjunto xH se llama **coclase a izquierda** de H en G.

Podríamos haber definido coclases a derecha mediante la relación $x \equiv y$ mód H si y sólo si $xy^{-1} \in H$. En este caso, las clases de equivalencia serían los conjuntos Hx con $x \in X$. Hx se llama **coclase a derecha** de H en G.

Proposición 4.2. *Si H es un subgrupo de G, entonces $|Hx| = |H| = |xH|$ para todo $x \in G$.*

Demostración. Sea $x \in G$. La función $H \to Hx$, $h \mapsto hx$, es una biyección con inversa $hx \mapsto h$. Análogamente se demuestra que la función $H \to xH$, $h \mapsto xh$, es una biyección. □

La función

$$\{\text{coclases a derecha de } H \text{ en } G\} \to \{\text{coclases a izquierda de } H \text{ en } G\}$$

dada por $Hx \mapsto x^{-1}H$ es una biyección pues

$$Hx = Hy \iff xy^{-1} \in H \iff (x^{-1})^{-1}y^{-1} \in H \iff x^{-1}H = y^{-1}H.$$

En particular, la cantidad de coclases a derecha de H en G coincide con la cantidad de coclases a izquierda de H en G.

Ejemplo 4.3. Si $G = \mathbb{Z}$ y $S = n\mathbb{Z}$, entonces

$$a + S = \{a + nq : q \in \mathbb{Z}\} = \{k \in \mathbb{Z} : k \equiv a \text{ mód } n\}.$$

Ejemplo 4.4. Los subgrupos de $\mathbb{S}_3$ son $\{id\}$, $\mathbb{S}_3$, los subgrupos $\langle(12)\rangle$, $\langle(13)\rangle$ y $\langle(23)\rangle$ de orden dos y el subgrupo $\langle(123)\rangle = \{\mathrm{id}, (123), (132)\}$ de orden tres. Si $H = \langle(12)\rangle = \{id, (12)\}$, entonces

$$\begin{aligned} H &= (12)H = \{id, (12)\}, \\ (123)H &= (13)H = \{(13), (123)\}, \\ (132)H &= (23)H = \{(23), (132)\}. \end{aligned}$$

Ejemplo 4.5. Sea $G = \mathbb{R}^2$ con la suma usual y sea $v \in \mathbb{R}^2$. La recta $L = \{\lambda v : \lambda \in \mathbb{R}\}$ es un subgrupo de G y para cada $p \in R^2$, la coclase $p + L$ es la recta paralela a L que pasa por el punto p.

Definición 4.6. Si H es un subgrupo de G, se define el **índice** de H en G como la cantidad $(G : H)$ de coclases a izquierda (o a derecha) de H en G.

Tener una relación de equivalencia módulo H nos permite escribir a G como unión disjunta de coclases a izquierda (o a derecha) de H en G. Además dos coclases cualesquiera son iguales o disjuntas.

Teorema 4.7 (Lagrange). *Si G es un grupo finito y H es un subgrupo de G, entonces $|G| = |H|(G : H)$. En particular, $|H|$ divide a $|G|$.*

Demostración. Tenemos una relación de equivalencia módulo H que nos permite descomponer en G en clases de equivalencia, digamos

$$G = \bigcup_{i=1}^{n} x_i H \quad \text{(unión disjunta)}$$

para ciertos $x_1, \ldots, x_n \in G$, donde $n = (G : H)$. Como cada una de esas clases tiene exáctamente $|H|$ elementos,

$$|G| = \sum_{i=1}^{n} |x_i H| = \sum_{i=1}^{n} |H| = |H|(G : H). \qquad \square$$

Veamos algunos corolarios.

Corolario 4.8. *Si G es un grupo finito y $g \in G$, entonces $g^{|G|} = 1$.*

Demostración. Por definición $|g| = |\langle g \rangle|$. El teorema de Lagrange aplicado al subgrupo $H = \langle g \rangle$ nos dice que

$$g^{|G|} = g^{|H|(G:H)} = (g^{|H|})^{(G:H)} = 1. \qquad \square$$

Corolario 4.9. *Si G es un grupo de orden primo, entonces G es cíclico.*

Demostración. Sea $g \in G \setminus \{1\}$ y sea $H = \langle g \rangle$. Por el teorema de Lagrange, $|H|$ divide a $|G|$ y luego $|H| = |G|$ pues $|G|$ es un número primo. En consecuencia, $G = H = \langle g \rangle$. $\square$

Corolario 4.10. *Si G es un grupo y $g,h \in G$ son elementos de órdenes finitos y coprimos, entonces $|gh| = |g||h|$.*

Demostración. Sean $n = |g|$, $m = |h|$ y $l = |gh|$. Como G es abeliano,

$$(gh)^{nm} = (g^n)^m (h^m)^n = 1$$

y luego l divide a nm. Por otro lado, como $(gh)^l = 1$, $g^l = h^{-l} \in \langle g \rangle \cap \langle h \rangle = \{1\}$ (pues como $|\langle g \rangle| = n$ y $|\langle h \rangle| = m$ son coprimos, entonces nm divide a l gracias al teorema de Lagrange). $\square$

Ejemplo 4.11. Gracias al teorema de Lagrange podemos demostrar fácilmente que $(n+m)!$ divide a $n!m!$, basta con observar que $\mathbb{S}_n \times \mathbb{S}_n \leq \mathbb{S}_{n+m}$.

El pequeño teorema de Fermat es un caso particular del teorema de Lagrange.

Ejercicio 4.12 (pequeño teorema de Fermat). Sea p un número primo. Demuestre que $a^{p-1} \equiv 1 \mod p$ para todo $a \in \{1, 2, \ldots, p-1\}$.

El siguiente corolario utiliza la función φ de Euler. Recordemos que $\varphi(n)$ es la cantidad de enteros positivos coprimos con n. El grupo de unidades de $\mathbb{Z}/n$ tiene $\varphi(n)$ elementos (pues $x \in \mathbb{Z}/p$ es inversible si y sólo si x es coprimo con n).

Ejercicio 4.13 (teorema de Euler). Sean a y n enteros coprimos. Demuestre que $a^{\phi(n)} \equiv 1 \mod n$.

No vale la recíproca del teorema de Lagrange.

Ejemplo 4.14. Consideremos el grupo alternado

$$\begin{aligned}\mathbb{A}_4 = \{&\mathrm{id}, (234), (243), (12)(34), (123), (124),\\ &(132), (134), (13)(24), (142), (143), (14)(23)\} \leq \mathbb{S}_4.\end{aligned}$$

Es fácil verificar que $|\mathbb{A}_4| = 12$. Vamos a demostrar que $\mathbb{A}_4$ no tiene subgrupos de orden seis. En efecto, si $H \leq \mathbb{A}_4$ es tal que $|H| = 6$, entonces, como $(\mathbb{A}_4 : H) = 6$, para todo $x \notin H$ podríamos descomponer a $\mathbb{A}_4$ como $\mathbb{A}_4 = H \cup xH$ (unión disjunta).

Afirmamos que para todo $g \in \mathbb{A}_4$ vale que $g^2 \in H$ (pues si $g \notin H$, entonces, como $g^2 \in \mathbb{A}_4 = H \cup gH$, se concluye que $g^2 \in H$). En particular, todos los elementos de orden tres de $\mathbb{A}_4$ están en el subgrupo H, una contradicción pues hay ocho elementos de orden tres.

Ejercicio 4.15. Demuestre que

$$\mathbf{SL}_2(3) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1, a, b, c, d \in \mathbb{Z}/3 \right\}$$

es un grupo de orden 24 que no posee subgrupos de orden 12.

Capítulo 5
Cocientes

cocientes

Si G es un grupo y N es un subgrupo de G, nos interesa saber cuándo la operación $(xN, yN) \mapsto xyN$ está bien definida. Para eso, se necesita que si $xN = x_1N$ y además $yN = y_1N$, entonces $xyN = x_1y_1N$. Veamos cómo puede interpretarse esa condición. Si $x^{-1}x_1 \in N$ y $y^{-1}y_1 \in N$, entonces $x_1 = xn$ y además $y_1 = ym$ para ciertos $m, n \in N$. Entonces

$$(xy)^{-1}(x_1y_1) = y^{-1}x^{-1}x_1y_1 = y^{-1}nym \in N$$

si y sólo si $y^{-1}ny \in N$.

Definición 5.1. Sea G un grupo. Un subgrupo N de G se dice **normal** si $gNg^{-1} \subseteq N$ para todo $g \in G$. Notación: si N es normal en G, entonces $N \trianglelefteq G$.

Proposición 5.2. *Sea N un subgrupo de G. Las siguientes afirmaciones son equivalentes:*

1. *$gNg^{-1} \subseteq N$ para todo $g \in G$.*
2. *$gNg^{-1} = N$ para todo $g \in G$.*
3. *$gN = Ng$ para todo $g \in G$.*

Demostración. Demostremos que $(1) \implies (3)$, que es la única implicación no trivial. Si $n \in N$ y $g \in G$, entonces $n = g(g^{-1}ng)g^{-1} \in gNg^{-1}$. □

Proposición 5.3. *Sea N un subgrupo de G. Las siguientes propiedades son equivalentes:*

1. *N es normal en G.*
2. *$(gN)(hN) = (gh)N$ para todo $g, h \in G$.*

Demostración. Vamos a demostrar que $(1) \implies (2)$. Sea $g \in G$. Como $gNg^{-1} = N$, entonces $(gN)(hN) = g(Nh)N = g(hN)N = (gh)N$. Veamos ahora que $(2) \implies (1)$. Si $g \in G$, entonces $gNg^{-1} \subseteq (gN)(g^{-1}N) = (gg^{-1})N = N$. □

Ejemplos 5.4. Si G es un grupo, entonces $\{1\}$ y G son subgrupos normales de G.

Ejemplo 5.5. Si G es un grupo, $Z(G)$ es un subgrupo normal de G. Más aún, si $N \leq Z(G)$, entonces $N \trianglelefteq G$.

Ejemplo 5.6. Si G es un grupo, entonces $[G,G]$ es un subgrupo normal de G pues

$$g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

para todo $g,x,y \in G$.

Ejemplo 5.7. Si N es un subgrupo de G tal que $(G:N) = 2$, entonces N es normal en G. Queremos demostrar que $gN = Ng$ para todo $g \in G$. Sea $g \in G$. Si $g \in N$, entonces $gN = Ng$. Si $g \notin N$, entonces $gN \neq N$. Como $(G:N) = 2$, podemos escribir a G como $G = N \cup gN$ (unión disjunta). En consecuencia, $gN = G \setminus N$. Similarmente se demuestra que $Ng = G \setminus N$ y luego $gN = Ng$.

Ejemplo 5.8. El ejemplo anterior nos permite demostrar que $\langle (123) \rangle \trianglelefteq \mathbb{S}_3$. Por otro lado, $\langle (12) \rangle$ no es normal en $\mathbb{S}_3$ pues por ejemplo $(13)(12)(13) = (23) \notin \langle (12) \rangle$.

Ejemplo 5.9. $\mathbf{SL}_n(\mathbb{R})$ es normal en $\mathbf{GL}_n(\mathbb{R})$ pues si $g \in \mathbf{GL}_n(\mathbb{R})$ y $x \in \mathbf{SL}_n(\mathbb{R})$, entonces $\det(gxg^{-1}) = (\det g)(\det x)(\det g)^{-1} = 1$.

Ejemplo 5.10. El grupo de Klein $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ es normal en $\mathbb{S}_4$.

Ejercicio 5.11. Sea $G = \mathbb{Z}/p \times (\mathbb{Z}/p)^\times$ el grupo dado por la operación

$$(x,y)(u,v) = (x + yu, yv).$$

Demuestre que $\{(x,1) : x \in \mathbb{Z}/p\}$ es normal en G y que $\{(0,y) : y \in (\mathbb{Z}/p)^\times\}$ no es normal en G.

El siguiente ejercicio es útil:

Ejercicio 5.12. Si S es un subgrupo de G, se define el **normalizador** de S en G al subgrupo

$$N_G(S) = \{g \in G : gSg^{-1} = S\}.$$

Demuestre que valen las siguientes afirmaciones:

1. $S \trianglelefteq N_G(S)$.
2. Si $S \leq T \leq G$ y $S \trianglelefteq G$, entonces $T \leq N_G(S)$.
3. Si $T \leq N_G(S)$, entonces TS es un grupo y además $S \leq TS$.

Veamos algunos ejemplos de subgrupos normales un poco más difíciles. Primero calcularemos los subgrupos normales de $\mathbb{A}_4$.

Ejemplo 5.13. Vamos a demostrar que $\{\mathrm{id}\}$, $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ y $\mathbb{A}_4$ son los únicos subgrupos normales de $\mathbb{A}_4$.

Como $\mathbb{A}_4 = \{3\text{-ciclos}\} \cup K$, K es el único subgrupo de $\mathbb{A}_4$ con cuatro elementos, y esto implica que K es normal en $\mathbb{A}_4$ (pues cada conjugado gKg^{-1} también será un

subgrupo de $\mathbb{A}_4$ de cuatro elementos). Sea $N \neq \{\mathrm{id}\}$ un subgrupo normal de $\mathbb{A}_4$. Si N contiene un 3-ciclo, digamos $(abc) \in N$. entonces

$$(acd) = (bcd)(abc)(bcd)^{-1} \in N$$

y luego $N = \mathbb{A}_4$ (pues todos los 3-ciclos están en N). Supongamos entonces que N no contiene 3-ciclos. Entonces algún elemento no trivial de K pertenece a N, digamos $(ab)(cd) \in N$. En consecuencia,

$$(ac)(bd) = (bcd)(ab)(cd)(bcd)^{-1} \in N, \quad (ad)(bc) = (ab)(cd)(ac)(bd) \in N$$

y luego $N = K$.

Vamos a calcular ahora los subgrupos normales de $\mathbb{S}_4$.

Ejemplo 5.14. Vamos a demostrar que $\{\mathrm{id}\}$, K, $\mathbb{A}_4$ y $\mathbb{S}_4$ son los únicos subgrupos normales de $\mathbb{S}_4$.

Sea N un subgrupo normal de $\mathbb{S}_4$. Si $N \subseteq \mathbb{A}_4$, entonces N es normal en $\mathbb{A}_4$ y luego, por lo visto en el ejemplo anterior, $N = \{\mathrm{id}\}$, $N = K$ o bien $N = \mathbb{A}_4$. Supongamos entonces que $N \not\subseteq \mathbb{A}_4$, es decir N contiene una permutación impar. Si $\sigma \in \mathbb{S}_4$ es una permutación impar, entonces σ es una trasposición o σ es un 4-ciclo.

Si N contiene una trasposición, entonces todas las trasposiciones también pertenecen a N pues

$$\tau(ij)\tau^{-1} = (\tau(i)\,\tau(j))$$

para todo $\tau \in \mathbb{S}_4$. En este caso, $N = \mathbb{S}_4$ pues $\mathbb{S}_4$ está generado por trasposiciones.

Si N contiene un 4-ciclo, todos los 4-ciclos también están en N pues

$$\tau(ijkl)\tau^{-1} = (\tau(i)\,\tau(j)\,\tau(k)\,\tau(l))$$

para todo $\tau \in \mathbb{S}_4$ y además $K \subseteq N$ pues

$$(ac)(bd) = (abcd)^2.$$

Esto nos dice que $|N| \geq 10$. Como además $K \subseteq N$, se tiene que $|N \cap \mathbb{A}_4| \geq 5$. Por otro lado, $N \cap \mathbb{A}_4$ es un subgrupo normal de $\mathbb{A}_4$. Por lo visto en el ejemplo anterior, $N \cap \mathbb{A}_4 = \mathbb{A}_4 \subseteq N$. En conclusión, $N = \mathbb{S}_4$.

Proposición 5.15. *Sean H y K subgrupos de G. Si H es normal en G, entonces HK es un subgrupo de G.*

Demostración. Nos alcanza con demostrar que $HK = KH$. Veamos primero que $HK \subseteq KH$. Si $x = hk \in HK$, entonces $x = k(k^{-1}hk) \in KH$ pues $k^{-1}hk \in H$. Para demostrar la otra inclusión, sea $y = kh \in KH$. Entonces $y = (khk^{-1})k \in HK$ pues $khk^{-1} \in H$. □

Ejercicio 5.16. Demuestre que si H y K son subgrupos normales de G, entonces HK es también normal en G.

Teorema 5.17. *Si N es un subgrupo normal de G, entonces G/N es un grupo con la operación $(xN)(yN) = (xy)N$.*

Demostración. Sabemos que la normalidad de N en G garantiza la buena definición de la operación. Calculos rutinarios, que dejamos como ejercicio, demuestran que esta operación transforma al conjunto G/N en un grupo. □

Veamos cómo son los posibles cocientes de $\mathbb{S}_4$.

Ejemplo 5.18. Sabemos que $\{\mathrm{id}\}$, K, $\mathbb{A}_4$ y $\mathbb{S}_4$ son los únicos subgrupos normales de $\mathbb{S}_4$. Trivialmente obtenemos que

$$\mathbb{S}_4/\{\mathrm{id}\} \simeq \mathbb{S}_4, \quad \mathbb{S}_4/\mathbb{A}_4 \simeq \mathbb{Z}/2, \quad \mathbb{S}_4/\mathbb{S}_4 \simeq \{\mathrm{id}\}.$$

Veamos qué podemos decir del cociente $Q = \mathbb{S}_4/K$. Sabemos que Q tiene orden seis y que Q es no abeliano pues

$$(12)K(13)K = (12)(13)K = (132)K \neq (123)K = (13)(12)K = (13)K(12)K.$$

Vimos que existe un único grupo no abeliano de orden seis. Luego $Q \simeq \mathbb{S}_3$.

Para terminar el capítulo mencionamos dos ejercicios de mucha utilidad.

Ejercicio 5.19. Si H es un subgrupo normal de G, entonces G/H es abeliano si y sólo si $[G,G] \subseteq H$.

Veamos una pequeña aplicación:

Ejemplo 5.20. $[\mathbb{A}_4, \mathbb{A}_4] = K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Sabemos que K es normal en $\mathbb{A}_4$. Como $\mathbb{A}_4/K \simeq \mathbb{Z}/3$ es abeliano, el ejercicio anterior nos dice que $[\mathbb{A}_4, \mathbb{A}_4] \subseteq K$. Por otro lado, como

$$(ab)(cd) = [(abc), (cda)],$$

se concluye que $K \subseteq [\mathbb{A}_4, \mathbb{A}_4]$.

Ejercicio 5.21. Si $G/Z(G)$ es cíclico, entonces G es abeliano.

Teorema 5.22. *Sea p un número primo y sea H un subgrupo de G. Si $(G:H) = p$, las siguientes afirmaciones son equivalentes:*

1. *H es normal en G.*
2. *Si $g \in G \setminus H$, entonces $g^p \in H$.*
3. *Si $g \in G \setminus H$, entonces $g^n \in H$ para algún $n \in \mathbb{N}$ sin divisores primos $< p$.*
4. *Si $g \in G \setminus H$, entonces $g^k \notin H$ para todo $k \in \{2, \ldots, p-1\}$.*

Demostración. La implicación $(1) \implies (2)$ es consecuencia inmediata del teorema de Lagrange, pues $|G/H| = p$.

La implicación $(2) \implies (3)$ es trivial pues p es un número primo.

Demostremos que (3) $\implies$ (4). Si $g^k \in H$ para algún $k \in \{2,\dots,p-1\}$, como $\mathrm{mcd}(k,n) = 1$, existen $r,s \in \mathbb{Z}$ tales que $rk+sn = 1$. Luego

$$g = g^1 = g^{rk+sn} = (g^k)^r (g^n)^s \in H,$$

una contradicción.

Para finalizar demostremos que (4) $\implies$ (1). Sea $x \in G \setminus H$ y sea $h \in H$. Queremos demostrar que entonces $xhx^{-1} \in H$. Si $y = xhx^{-1} \notin H$, entonces $y^k \notin H$ para todo $k \in \{2,\dots,p-1\}$. Esto implica que las coclases

$$H, yH, y^2H, \dots, y^{p-1}H$$

son todas distintas (pues si $y^iH = y^jH$ para i,j tales que $i < j$, entonces $y^{j-i} \in H$ con $j-i \leq p-2$). Como $y = xhx^{-1}$, entonces

$$(yx)H = (xh)H = xH = y^iH$$

para algún $i \in \{0,1,\dots,p-1\}$. Si $i = 0$, entonces $yx = xh \in H$ y luego $x \in H$, una contradicción. Luego $(yx)H = y^iH$ para algún $i \in \{1,\dots,p-1\}$ y entonces

$$y^iH = xH = y^{i-1}H$$

para algún $i \in \{0,\dots,p-2\}$, una contradicción. □

Veamos algunas consecuencias. La primera se hará en el caso en que el grupo sea finito.

cor:p_menor **Corolario 5.23.** *Sea p el menor número primo que divide al orden de un grupo finito G y sea H es un subgrupo de G índice p. Entonces H es normal en G.*

Demostración. Si $g \in G \setminus H$, entonces $g^n = 1 \in H$, donde $n = |G|$. Como p es primo, n no tiene divisores primos $< p$. El teorema anterior impica entonces que H es normal en G. □

En el teorema no pedimos que G sea un grupo finito. Podemos entonces obtener el siguiente resultado.

Corolario 5.24. *Sea p un número primo y sea G un grupo tal que todo elemento tiene orden una potencia de p. Si H es un subgrupo de G de índice p, entonces H es normal en G.*

Demostración. Sea $g \in G \setminus H$ y sea $n = |g|$. Como todo elemento de G tiene orden una potencia de p, n es en particular una potencia de p y, en consecuencia, n no posee divisores primos $< p$. Como además $g^n = 1 \in H$, el teorema anterior implica que H es normal en G. en particular $g^n \in H$. □

Índice alfabético