Capítulo 7
Clases laterales

En este capítulo vamos a investigar la noción del subgrupo normal, que es fundamental para la teoría. Recordemos que hemos definido el anillo $\mathbb{Z}/n\mathbb{Z}$ considerando la relación de equivalencia

$$a \equiv b \pmod{n} \iff n \mid a - b$$

sobre los números enteros. Aquí la condición $n \mid a - b$ puede ser escrita como $a - b \in n\mathbb{Z}$, donde $n\mathbb{Z}$ es el subgrupo de $\mathbb{Z}$ formado por los elementos divisibles por n. De modo similar, para cualquier grupo G y subgrupo $H \subset G$, se puede definir la "congruencia módulo H" que va a ser una relación de equivalencia. Como en el caso de $\mathbb{Z}/n\mathbb{Z}$, esto nos permite definir la operación de grupo sobre las clases de equivalencia, pero bajo una hipótesis especial sobre H.

7.1 Clases laterales

7.1.1. Notación. Para un subconjunto $S \subset G$ y un elemento fijo $g \in G$ escribimos

$$gS := \{gs \mid s \in S\},$$
$$Sg := \{sg \mid s \in S\}.$$

En particular, para dos elementos fijos $g_1, g_2 \in G$ se tiene

$$g_1 S g_2 = g_1(Sg_2) = (g_1 S)g_2 = \{g_1\, s\, g_2 \mid s \in S\}.$$

Si G es un grupo abeliano, entonces $gS = Sg$ para cualquier $g \in G$. Cuando G no es abeliano, en general $gS \neq Sg$.

7.1.2. Observación. *Sea G un grupo y H su subgrupo. Consideremos la relación*

$$g_1 \equiv g_2 \pmod{H}$$

para $g_1, g_2 \in G$ dada por una de las siguientes condiciones equivalentes:

1) $g_1^{-1} g_2 \in H$.

2) $g_2 \in g_1 H$ *(es decir, $g_2 = g_1 h$ para algún $h \in H$).*

Esta es una relación de equivalencia.

Demostración. La equivalencia de 1) y 2) está clara: la condición 1) quiere decir que $g_1^{-1}g_2 = h$ para algún $h \in H$, pero esto es equivalente a $g_2 = g_1 h$.

Ahora veamos que $g_1 \equiv g_2 \pmod{H}$ es una relación de equivalencia. Primero, es reflexiva: tenemos $g \equiv g \pmod{H}$ para todo $g \in G$, ya que $g^{-1}g = 1 \in H$. Luego, es simétrica: si $g_1 \equiv g_2 \pmod{H}$, esto quiere decir que $g_1^{-1} g_2 \in H$. Pero H es un subgrupo, y por lo tanto $(g_1^{-1} g_2)^{-1} = g_2^{-1} g_1 \in H$, así que $g_2 \equiv g_1 \pmod{H}$. Por fin, la relación es transitiva: si tenemos $g_1 \equiv g_2 \pmod{H}$ e $g_2 \equiv g_3 \pmod{H}$, esto significa que

$$g_1^{-1} g_2 \in H, \quad g_2^{-1} g_3 \in H,$$

y entonces

$$(g_1^{-1} g_2)\,(g_2^{-1} g_3) = g_1^{-1} g_3 \in H;$$

es decir, $g_1 \equiv g_3 \pmod{H}$. ■

También podríamos considerar la relación

$$g_1 \sim g_2 \iff g_2\, g_1^{-1} \in H.$$

Ya que el grupo G no es necesariamente abeliano, en general esta relación es diferente de la relación de arriba, pero es también una relación de equivalencia.

7.1.3. Observación. *Sea G un grupo y H su subgrupo. Consideremos la relación $g_1 \sim g_2$ para $g_1, g_2 \in G$ dada por una de las siguientes condiciones equivalentes:*

1) $g_2\, g_1^{-1} \in H$.

2) $g_2 \in Hg_1$ *(es decir, $g_2 = hg_1$ para algún $h \in H$).*

Esta es una relación de equivalencia.

Demostración. Similar a 7.1.2. ■

Como para toda relación de equivalencia, tenemos una descomposición de G en una unión disjunta de clases de equivalencia. Hemos visto que para la relación de 7.1.2 las clases de equivalencia son precisamente los conjuntos gH para $g \in G$, mientras que para la relación de 7.1.3 son los Hg.

7.1.4. Definición. Los subconjuntos $gH \subset G$ se llaman las **clases laterales izquierdas**[*] respecto a H. El conjunto de las clases laterales izquierdas se denota por G/H. Los subconjuntos Hg se llaman las **clases laterales derechas** respecto a H. El conjunto de las clases laterales derechas se denota por $H\backslash G$[**].

7.1.5. Observación. *Para todo $g \in G$ existen biyecciones de conjuntos*

$$gH \cong H \quad y \quad Hg \cong H.$$

En otras palabras, cada clase lateral izquierda (resp. derecha) tiene la misma cardinalidad que H.

Demostración. Por ejemplo, para las clases izquierdas, tenemos biyecciones

$$\begin{aligned} gH &\to H, \\ gh &\mapsto g^{-1} gh = h, \\ gh &\leftarrow\!\shortmid h. \end{aligned}$$

■

[*] En inglés "clase lateral" se traduce como "coset".

[**] No confundir la notación $H\backslash G$ con la diferencia de conjuntos $X \setminus Y$.

7.1.6. Observación. *La aplicación entre conjuntos*

$$\begin{aligned} i\colon G &\to G, \\ g &\mapsto g^{-1} \end{aligned}$$

induce una biyección canónica

$$\begin{aligned} G/H &\to H\backslash G, \\ gH &\mapsto Hg^{-1}. \end{aligned}$$

Demostración. La aplicación está bien definida sobre las clases de equivalencia: $g_1H = g_2H$ quiere decir que $g_2 = g_1h$ para algún $h \in H$. Luego, $g_2^{-1} = h^{-1}g_1^{-1}$, así que $Hg_2^{-1} = Hg_1^{-1}$. Entonces, la aplicación $g \mapsto g^{-1}$ envía la clase lateral izquierda gH a la clase lateral derecha Hg^{-1}.

Está claro que i es una biyección, puesto que $i \circ i = \mathrm{id}$. ■

Aunque gH y Hg tienen la misma cardinalidad, en general $gH \neq Hg$ si el grupo G no es abeliano.

7.1.7. Ejemplo. En el grupo simétrico S_n consideremos las permutaciones que dejan el número n fijo. Estas forman un subgrupo que es isomorfo a S_{n-1}:

$$H := \{\sigma \in S_n \mid \sigma(n) = n\} \cong S_{n-1}.$$

Dos permutaciones σ y τ pertenecen a la misma clase lateral *izquierda* si $\sigma^{-1}\tau \in H$; es decir, si $\sigma(n) = \tau(n)$. Entonces, tenemos n diferentes clases laterales izquierdas S_n/H

$$L_i := \{\sigma \in S_n \mid \sigma(n) = i\}, \quad 1 \leq i \leq n.$$

Por otro lado, σ y τ pertenecen a la misma clase lateral *derecha* si $\tau\sigma^{-1} \in H$; es decir, si $\sigma^{-1}(n) = \tau^{-1}(n)$. Hay n diferentes clases laterales derechas $H\backslash S_n$

$$R_i := \{\sigma \in S_n \mid \sigma(i) = n\}, \quad 1 \leq i \leq n.$$

Ahora si $L_i = R_i$ para algún i, tenemos

$$\sigma(n) = i \iff \sigma(i) = n,$$

entonces $i = n$. ▲

7.1.8. Ejemplo. Consideremos el grupo aditivo $\mathbb{C}$ e identifiquemos $\mathbb{R}$ con el subgrupo de los números complejos z tales que $\operatorname{Im} z = 0$. De la misma manera, consideremos el grupo multiplicativo $\mathbb{C}^\times$ y sus subgrupos

$$\mathbb{T} := \{z \in \mathbb{C}^\times \mid |z| = 1\}$$

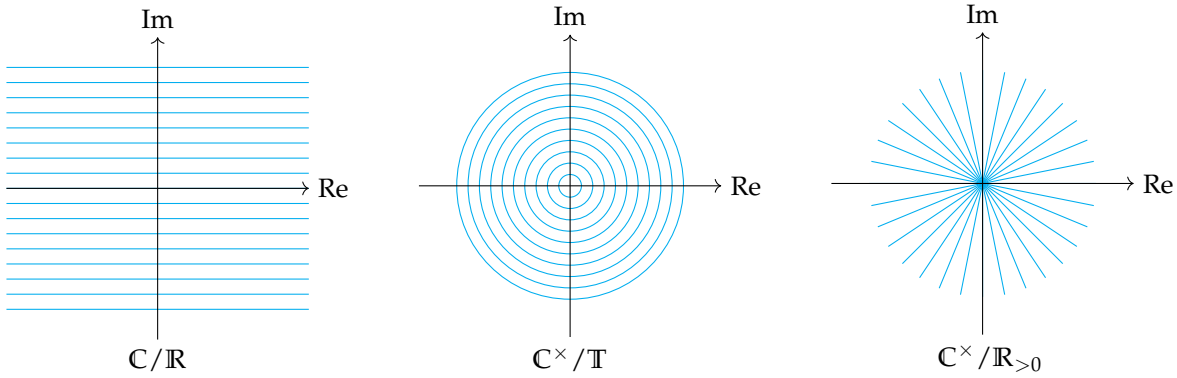
(el grupo del círculo) y

$$\mathbb{R}_{>0} = \{z \in \mathbb{C}^\times \mid \operatorname{Im} z = 0, \operatorname{Re} z > 0\}.$$

Los dibujos de abajo representan las clases laterales

$$\begin{aligned} \mathbb{C}/\mathbb{R} &= \{z + \mathbb{R} \mid z \in \mathbb{C}\}, \\ \mathbb{C}^\times/\mathbb{T} &= \{z\mathbb{T} \mid z \in \mathbb{C}^\times\}, \\ \mathbb{C}^\times/\mathbb{R}_{>0} &= \{z\mathbb{R}_{>0} \mid z \in \mathbb{C}^\times\} \end{aligned}$$

en el plano complejo.



▲

7.1.9. Ejemplo. Sea R un anillo conmutativo. Consideremos el grupo $\mathrm{GL}_n(R)$ y su subgrupo $\mathrm{SL}_n(R) := \{A \in \mathrm{GL}_n(R) \mid \det A = 1\}$. Para $A, B \in \mathrm{GL}_n(R)$ tenemos

$$A\,\mathrm{SL}_n(R) = B\,\mathrm{SL}_n(R) \iff A^{-1}B \in \mathrm{SL}_n(R) \iff \det(A^{-1}\,B) = \det(A)^{-1} \cdot \det(B) = 1 \iff \det A = \det B.$$

De la misma manera,

$$\mathrm{SL}_n(R)\,A = \mathrm{SL}_n(R)\,B \iff AB^{-1} \in \mathrm{SL}_n(R) \iff \det(A\,B^{-1}) = \det(A) \cdot \det(B)^{-1} = 1 \iff \det A = \det B.$$

Entonces, las clases laterales izquierdas y derechas coinciden:

$$A\,\mathrm{SL}_n(R) = \mathrm{SL}_n(R)\,A \quad \text{para todo } A \in \mathrm{GL}_n(R),$$

y corresponden a las matrices de determinante fijo:

$$M_a = \{A \in \mathrm{GL}_n(R) \mid \det A = a\} \quad \text{para algún } a \in R^\times.$$

▲

7.1.10. Ejemplo. Para el grupo simétrico $G = S_n$ y el grupo alternante $H = A_n$ tenemos

$$\sigma\,A_n = \tau\,A_n \iff \sigma^{-1}\,\tau \in A_n \iff \operatorname{sgn}(\sigma^{-1}\,\tau) = 1 \iff \operatorname{sgn}\sigma = \operatorname{sgn}\tau,$$

y de la misma manera,

$$A_n\,\sigma = A_n\,\tau \iff \sigma\,\tau^{-1} \in A_n \iff \operatorname{sgn}(\sigma\,\tau^{-1}) = 1 \iff \operatorname{sgn}\sigma = \operatorname{sgn}\tau.$$

Entonces, $\sigma\,A_n = A_n\,\sigma$, y hay solamente dos clases laterales: una formada por las permutaciones pares y la otra por las permutaciones impares:

$$A_n = \{\sigma \in S_n \mid \operatorname{sgn}\sigma = +1\}, \quad (1\,2)\,A_n = A_n\,(1\,2) = \{\sigma \in S_n \mid \operatorname{sgn}\sigma = -1\}.$$

▲

7.1.11. Ejemplo. El mismo razonamiento demuestra que para el grupo $\mathbb{R}^\times$ y el subgrupo $\mathbb{R}_{>0}$ hay dos clases laterales:

$$\mathbb{R}_{>0} = \{x \in \mathbb{R}^\times \mid x > 0\}, \quad -1 \cdot \mathbb{R}_{>0} = \{x \in \mathbb{R}^\times \mid x < 0\}.$$

▲

7.2 Teorema de Lagrange y sus consecuencias

7.2.1. Definición. Si la cardinalidad $|G/H| = |H\backslash G|$ es finita, este número se llama el **índice** de H en G y se denota por $|G : H|$.

7.2.2. Ejemplo. Tenemos $|S_n : A_n| = 2$ y $|\mathbb{R}^\times : \mathbb{R}_{>0}| = 2$. Note en particular que un grupo infinito puede tener subgrupos de índice finito. ▲

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

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

Demostración. G se descompone en una unión disjunta de clases de equivalencia. En total hay $|G : H|$ clases de equivalencia y cada una tiene $|H|$ elementos como vimos en 7.1.5. ■

7.2.4. Corolario. *Si G es un grupo finito y $H \subset G$ es un subgrupo, entonces $|G|$ es divisible por $|H|$.*

7.2.5. Ejemplo. En el capítulo anterior hemos visto que un grupo cíclico de orden n tiene precisamente un subgrupo de orden d para cada $d \mid n$. ▲

7.2.6. Ejemplo. Hemos visto que el grupo de cuaterniones Q_8 y el grupo diédrico D_4 tienen subgrupos de orden 1, 2, 4, 8. ▲

7.2.7. Ejemplo. El grupo alternante A_n es un subgrupo del grupo simétrico S_n. Tenemos $|A_n| = |S_n|/2$. ▲

7.2.8. Corolario. *Si G es un grupo finito, entonces el orden de todo elemento $g \in G$ divide a $|G|$.*

Demostración. El orden de g es el orden del subgrupo $\langle g \rangle$ generado por g. ■

7.2.9. Corolario. *Si $|G| = n$, entonces $g^n = 1$ para todo $g \in G$.*

Demostración. Sigue del hecho de que el orden de todo $g \in G$ divide a $|G|$. ■

7.2.10. Ejemplo. Para el anillo $\mathbb{Z}/n\mathbb{Z}$ el grupo de unidades viene dado por

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid \operatorname{mcd}(a, n) = 1\}.$$

Su cardinalidad es la función ϕ de Euler:

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n).$$

Entonces, se tiene

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad \text{si } \operatorname{mcd}(a, n) = 1.$$

Esta congruencia se conoce como el **teorema de Euler**. En particular, si $n = p$ es primo, se obtiene el pequeño teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{si } p \nmid a.$$

Ya lo demostramos usando la identidad $(x+y)^p = x^p + y^p$ en el cuerpo $\mathbb{F}_p$, y ahora obtuvimos otra prueba que usa la teoría de grupos. ▲

7.2.11. Corolario. *Todo grupo de orden primo p es cíclico.*

Demostración. Si $|G| = p$, entonces los subgrupos de G son de orden 1 o $|G|$; es decir, G no tiene subgrupos propios. Sea $g \in G$ un elemento tal que $g \neq 1$. Entonces $\langle g \rangle \neq \{1\}$, y por lo tanto $\langle g \rangle = G$. ■

Algunos ejemplos elementales

7.2.12. Ejemplo. Para el grupo alternante A_4 tenemos $|A_4| = 4!/2 = 12$, así que los subgrupos necesariamente tienen orden $1, 2, 3, 4, 6, 12$. Cada subgrupo de orden 2 es de la forma $\{\mathrm{id}, \sigma\}$ donde $\operatorname{ord}\sigma = 2$. Los elementos de orden 2 son permutaciones de la forma $(\bullet\ \bullet)\,(\bullet\ \bullet)$, productos de dos transposiciones disjuntas. Tenemos los siguientes tres subgrupos:

$$\langle (1\ 2)\,(3\ 4)\rangle, \quad \langle (1\ 3)\,(2\ 4)\rangle, \quad \langle (1\ 4)\,(2\ 3)\rangle.$$

Cada subgrupo de orden 3 es cíclico, generado por un elemento de orden 3, en este caso un 3-ciclo. Tenemos los siguientes cuatro subgrupos:

$$\langle (1\ 2\ 3)\rangle = \langle (1\ 3\ 2)\rangle, \quad \langle (1\ 2\ 4)\rangle = \langle (1\ 4\ 2)\rangle, \quad \langle (1\ 3\ 4)\rangle = \langle (1\ 4\ 3)\rangle, \quad \langle (2\ 3\ 4)\rangle = \langle (2\ 4\ 3)\rangle.$$

Ahora si G es un subgrupo de orden 4, sus elementos necesariamente tienen orden 2 o 4. En A_4 no hay elementos de orden 4, y la única opción que nos queda es de considerar todos los tres elementos de orden 2 junto con la permutación identidad:

$$V = \{\mathrm{id}, (1\ 2)\,(3\ 4), (1\ 3)\,(2\ 4), (1\ 4)\,(2\ 3)\}.$$

Se ve que esto es un subgrupo.

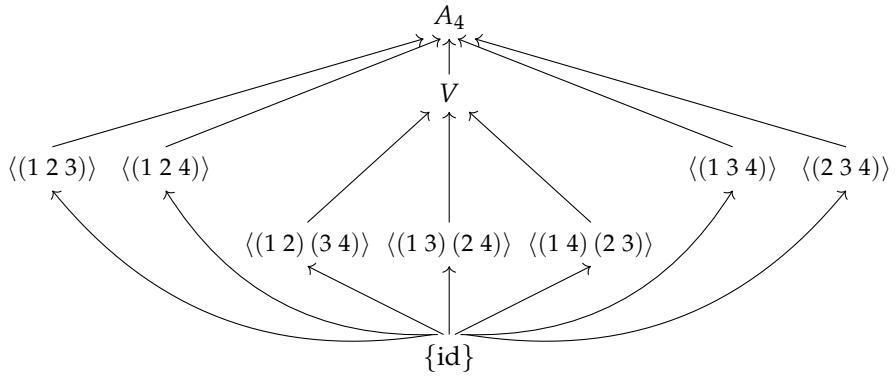
Si G es un subgrupo de orden 6, sus elementos necesariamente tienen orden 2 o 3; es decir, son 3-ciclos o permutaciones de la forma $(\bullet\ \bullet)\,(\bullet\ \bullet)$. Junto con cada 3-ciclo G debe contener su inverso. Las posibles opciones son

$$\{\mathrm{id}, (a\ b\ c), (a\ c\ b), (1\ 2)\,(3\ 4), (1\ 3)\,(2\ 4), (1\ 4)\,(2\ 3)\}$$

y

$$\{\mathrm{id}, (a\ b\ c), (a\ c\ b), (i\ j\ k), (i\ k\ j), (p\ q)\,(r\ s)\}.$$

Podemos descartar el primer caso: conjugando $(a\ b\ c)$ por una de las permutaciones $(\bullet\ \bullet)\,(\bullet\ \bullet)$ se obtiene otro 3-ciclo $(a'\ b'\ c') \neq (a\ b\ c), (a\ c\ b)$. De la misma manera, en el segundo caso, conjugando $(p\ q)\,(r\ s)$ por un 3-ciclo se obtiene $(p'\ q')\,(r'\ s') \neq (p\ q)\,(r\ s)$. Podemos concluir que en A_4 no hay subgrupos de orden 6.



▲

7.2.13. Comentario. El último ejemplo demuestra que si $d \mid |G|$, entonces G no necesariamente tiene subgrupos de orden d.

7.2.14. Ejemplo. Sea

$$G = \{1, a, b, c\}.$$

un grupo de orden 4. Sus elementos no triviales necesariamente tienen orden 2 o 4. Si en G hay un elemento de orden 4, entonces G es cíclico, isomorfo a $\mathbb{Z}/4\mathbb{Z}$. En el caso contrario, todos los elementos no triviales son de orden 2 y la tabla de multiplicación viene dada por

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1		
b	b		1	
c	c			1

Ya que los elementos en las filas y columnas no se pueden repetir, tenemos una especie de sudoku y la única opción de completar la tabla es la siguiente:

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Este grupo es isomorfo al grupo $V \subset A_4$. Acabamos de demostrar que $\mathbb{Z}/4\mathbb{Z}$ y V son los únicos grupos de orden 4 salvo isomorfismo. ▲

7.2.15. Ejemplo. Sea G un grupo de orden 6. Sus elementos no triviales necesariamente tienen orden 2, 3, o 6. Si hay un elemento de orden 6, entonces G es isomorfo a $\mathbb{Z}/6\mathbb{Z}$.

1. Primero, recordemos el siguiente resultado general: todo grupo de orden par tiene por lo menos un elemento de orden 2[*]. En nuestro caso, ya que $|G| = 6$ es par, sabemos que G tiene un elemento de orden 2. Sea a este elemento.

2. Se puede ver que G también contiene un elemento de orden 3. En el caso contrario, si todos los elementos no triviales son de orden 2, para dos elementos a, b su producto ab es otro elemento de orden 2 (en efecto, un grupo donde $g^2 = 1$ para todo g es necesariamente abeliano y luego $(ab)^2 = a^2 b^2 = 1$). Esto significa que

$$\langle a, b\rangle = \{1, a, b, ab\}$$

es un subgrupo de orden 4, pero esto contradice el teorema de Lagrange.

Podemos concluir que hay algún elemento b de orden 3.

[*]En efecto, $g^2 = 1$ si y solamente si $g = g^{-1}$. Luego, si todos los elementos no triviales tienen orden > 2, podemos escribir

(*) $$G = \{1\} \sqcup \{g_1, g_1^{-1}\} \sqcup \{g_2, g_2^{-1}\} \sqcup \cdots$$

donde $g_i \neq g_i^{-1}$, dado que $\operatorname{ord} g_i > 2$. Es nada más la partición de G respecto a la relación de equivalencia

$$g \sim g' \iff g' = g^{-1}.$$

Luego, (*) implica que el orden del grupo es impar.

3. Tenemos la siguiente tabla de multiplicación:

$\cdot$	1	a	b	b^2	ab	ab^2
1	1	a	b	b^2	ab	ab^2
a	a	1	ab	ab^2	b	b^2
b	b		b^2	1		
b^2	b^2		1	b		
ab	ab		ab^2	a		
ab^2	ab^2		a	ab		

Fijémonos ahora en la tercera fila. Para el producto $b \cdot a$ hay dos opciones diferentes: $ba = ab$ o $ba = ab^2$.

I. Si $ba = ab$, entonces el grupo es abeliano y es cíclico, generado por ab: tenemos

$$(ab)^2 = b^2, \quad (ab)^3 = a, \quad (ab)^4 = b, \quad (ab)^5 = ab^2.$$

II. Si $ba = ab^2$, entonces el resto de la tabla se completa automáticamente.

$$b \cdot ab = a, \quad b \cdot ab^2 = ab,$$
$$b^2 \cdot a = b \cdot ab^2 = ab^2 \cdot b^4 = ab, \quad b^2 \cdot ab = ab^2, \quad b^2 \cdot ab^2 = a,$$
$$ab \cdot a = a \cdot ab^2 = b^2, \quad ab \cdot ab = a \cdot ab^2 \cdot b = 1, \quad \text{etc.}$$

$\cdot$	1	a	b	b^2	ab	ab^2
1	1	a	b	b^2	ab	ab^2
a	a	1	ab	ab^2	b	b^2
b	b	ab^2	b^2	1	a	ab
b^2	b^2	ab	1	b	ab^2	a
ab	ab	b^2	ab^2	a	1	b
ab^2	ab^2	b	a	ab	b^2	1

Podemos concluir que salvo isomorfismo, hay dos grupos de orden 6: uno abeliano que es $\mathbb{Z}/6\mathbb{Z}$ y el otro es no abeliano S_3.

·	1	(1 2)	(1 2 3)	(1 3 2)	(2 3)	(1 3)
id	id	(1 2)	(1 2 3)	(1 3 2)	(2 3)	(1 3)
(1 2)	(1 2)	id	(2 3)	(1 3)	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3)	(1 3 2)	id	(1 2)	(2 3)
(1 3 2)	(1 3 2)	(2 3)	id	(1 2 3)	(1 3)	(1 2)
(2 3)	(2 3)	(1 3 2)	(1 3)	(1 2)	id	(1 2 3)
(1 3)	(1 3)	(1 2 3)	(1 2)	(2 3)	(1 3 2)	id

▲

El último ejemplo es divertido, pero usando solamente las ideas elementales no se puede decir mucho sobre los grupos finitos de orden mayor. Sin embargo, como vimos, el teorema de Lagrange ya impone muchas restricciones sobre la estructura de grupos finitos.

Una aplicación seria

Terminemos esta sección por el siguiente resultado importante.

7.2.16. Proposición. *Sea k un cuerpo. Entonces, todo subgrupo finito de su grupo de unidades $k^\times$ es cíclico.*

Para demostrarlo, necesitamos el siguiente resultado auxiliar.

7.2.17. Lema. *Sea G un grupo de orden finito n. Supongamos que para todo $d \mid n$ se cumple*

$$\#\{x \in G \mid x^d = 1\} \leq d. \tag{7.1}$$

Entonces G es cíclico.

Demostración. Si G tiene un elemento g de orden d, entonces este genera el subgrupo $\langle g \rangle$ que es cíclico de orden d. Todo elemento $h \in G$ tal que $h^d = 1$ pertenece a este subgrupo gracias a la hipótesis (7.1), y si h tiene orden d, entonces es otro generador de $\langle g \rangle$. En total este subgrupo tiene $\phi(d)$ generadores. Entonces, el número de elementos de orden d es igual a 0 o $\phi(d)$. De hecho, el primer caso no es posible: la fórmula

$$\sum_{d|n} \phi(d) = n$$

demuestra que si para algún $d \mid n$ el grupo G no tiene elementos de orden d, entonces $|G| < n$. En particular, G debe tener un elemento de orden n y por lo tanto es cíclico. ■

Demostración de 7.2.16 [Ser1973]. Para un cuerpo, la ecuación polinomial $x^d - 1 = 0$ tiene como máximo d soluciones. Entonces, se cumple la hipótesis (7.1) y podemos aplicar 7.2.17. ■

7.2.18. Ejemplo. Para $k = \mathbb{R}$ los únicos elementos de orden finito en $\mathbb{R}^\times$ son ± 1. ▲

7.2.19. Ejemplo. Para $k = \mathbb{C}$ los elementos de orden finito en $\mathbb{C}^\times$ forman el subgrupo de las raíces de la unidad $\mu_\infty(\mathbb{C})$. El resultado de 7.2.16 nos dice que todos los subgrupos finitos de $\mathbb{C}^\times$ son cíclicos. ▲

7.2.20. Ejemplo. Si $k = \mathbb{F}_q$ es un cuerpo finito (donde $q = p^k$ para algún primo p), 7.2.16 implica que el grupo $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ es cíclico de orden $q-1$. Note que la demostración de 7.2.16 no es constructiva: un conteo implica que $\mathbb{F}_{p^k}^\times$ posee un generador, pero no dice cuál elemento particular[*] es. En este sentido, aunque se puede escribir

$$\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z},$$

el grupo aditivo $\mathbb{Z}/(q-1)\mathbb{Z}$ tiene un generador distinguido $[1]$, mientras que para $\mathbb{F}_q^\times$ no está claro cuál generador hay que escoger (hay $\phi(q-1)$ posibilidades). El isomorfismo de arriba depende de esta elección.

Para dar un ejemplo particular, el grupo $\mathbb{F}_4^\times$ es cíclico de orden 3 y puede ser escrito como

$$\mathbb{F}_4^\times = \{1, a, a^2\}$$

donde a es un generador (tenemos $\phi(4-1) = 2$ opciones para escogerlo: a^2 sería el otro generador). Luego la tabla de adición en $\mathbb{F}_4$ viene dada por

$+$	0	1	a	a^2
0	0	1	a	a^2
1	1	0	a^2	a
a	a	a^2	0	1
a^2	a^2	a	1	0

Note que este grupo es isomorfo al grupo V.

Para el cuerpo $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, el grupo

$$\mathbb{F}_5^\times = \{[1], [2], [3], [4]\}$$

es cíclico. Sus generadores son $[2]$ y $[3]$: tenemos

$$2^2 \equiv 4 \pmod 5, \quad 2^3 \equiv 3 \pmod 5, \quad 2^4 \equiv 1 \pmod 5$$

y

$$3^2 \equiv 4 \pmod 5, \quad 3^3 \equiv 2 \pmod 5, \quad 3^4 \equiv 1 \pmod 5.$$

▲

Usando la estructura cíclica de $\mathbb{F}_p^\times$, podemos demostrar algunos resultados clásicos sobre los cuadrados módulo p. Recordemos que cuando para $x \in \mathbb{F}_p$ se tiene $x = y^2$ para algún $y \in \mathbb{F}_p$, se dice que x es un **residuo cuadrático módulo** p.

7.2.21. Proposición. *El producto de dos no-cuadrados es un cuadrado.*

Para $p > 2$ hay precisamente $(p+1)/2$ residuos cuadráticos módulo p.

Demostración. Primero, $0 \in \mathbb{F}_p$ es un residuo cuadrático. Para contar los residuos no nulos, notamos que

$$\mathbb{F}_p^\times = \{1, x, x^2, \ldots, x^{p-2}\}$$

para algún generador $x \in \mathbb{F}_p^\times$. Luego x^k es un cuadrado si y solamente si k es par. Esto demuestra que el producto de dos no-cuadrados es un cuadrado. Luego, entre los números $k = 0, 1, 2, \ldots, p-2$ precisamente $(p-1)/2$ son pares. ■

7.2.22. Proposición. -1 *es un residuo cuadrático módulo p si y solamente si $p \not\equiv 3 \pmod 4$.*

[*] Recuerdo al lector que no hemos construido los cuerpos $\mathbb{F}_{p^k}$ para $k > 1$; solo mencioné que estos existen.

Demostración. Necesitamos ver que en el cuerpo finito $\mathbb{F}_p$ se cumple $-1 = x^2$ para algún $x \in \mathbb{F}_p$ si y solamente si $p \not\equiv 3 \pmod 4$.

Si $p = 2$, entonces $-1 = 1 = 1^2$. Podemos suponer que $p > 2$.

Para $p > 2$ la identidad $-1 = x^2$ en $\mathbb{F}_p$ implica que x es una raíz cuarta primitiva de la unidad:

$$x \neq 1, \quad x^2 = -1 \neq 1, \quad x^3 = -x \neq 1, \quad x^4 = 1.$$

Viceversa, supongamos que existe $x \in \mathbb{F}_p$ tal que

$$x \neq 1, \quad x^2 \neq 1, \quad x^3 \neq 1, \quad x^4 = 1.$$

En particular, $x^2 \neq 1$ implica que también $x \neq -1$. Luego, de la ecuación

$$0 = x^4 - 1 = (x-1)(x+1)(x^2+1),$$

podemos deducir que $x^2 = -1$.

Esto demuestra que -1 es un residuo cuadrático en $\mathbb{F}_p$ si y solamente si $\mathbb{F}_p$ contiene una raíz cuarta primitiva de la unidad. Esto se reduce a la existencia de un elemento de orden 4 en el grupo $\mathbb{F}_p^\times$. El último es cíclico de orden $p-1$ y por lo tanto contiene un elemento de orden 4 si y solamente si

$$4 \mid (p-1) \iff p - 1 = 4k \text{ para algún } k \iff p \equiv 1 \pmod 4.$$

■

7.3 Subgrupos normales

Si G no es abeliano y $H \subset G$ es un subgrupo, en general tenemos $gH \neq Hg$. Cuando esto se cumple, se dice que H es un subgrupo normal. Esto también puede ser formulado en términos de **conjugación**. Cuando para dos elementos h y h' se cumple $h' = g\,h\,g^{-1}$ para algún $g \in G$, se dice que h y h' son **conjugados**, o que h' es el resultado de la **conjugación de** h **por** g.

7.3.1. Definición (Galois, 1832). Sea G un grupo y $H \subset G$ un subgrupo. Se dice que H es **normal** si se cumple una de las propiedades equivalentes:

1) toda clase lateral izquierda coincide con la clase lateral derecha correspondiente:
$$gH = Hg \quad \text{para todo } g \in G;$$

2) la conjugación de H por los elementos de G coincide con H:
$$gHg^{-1} := \{ghg^{-1} \mid h \in H\} = H \quad \text{para todo } g \in G;$$

3) una variación de 2):
$$ghg^{-1} \in H \quad \text{para todo } g \in G \text{ y } h \in H.$$

La equivalencia de 1) y 2) está clara. La condición 3) significa que $gHg^{-1} \subseteq H$ para todo $g \in G$ y por lo tanto 2) implica 3). Por fin, si se cumple 3), entonces para cualesquiera g y h tenemos $g^{-1}hg \in H$, y luego $g\,(g^{-1}hg)\,g^{-1} = h$, lo que implica $H \subseteq gHg^{-1}$. Entonces, 3) implica 2).

Cuidado: si tenemos una cadena de subgrupos

$$K \subset H \subset G$$

y K es normal en H, esto no quiere decir que K es normal en G.

7.3.2. Ejemplo. Si G es un grupo abeliano, todo subgrupo es normal. ▲

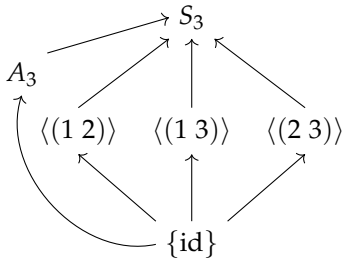
7.3.3. Ejemplo. Los subgrupos $\{1\}$ y G son normales. ▲

7.3.4. Ejemplo. En el grupo simétrico S_3 hay 3 subgrupos de orden 2 que corresponden a las transposiciones:

$$\langle(1\ 2)\rangle,\ \langle(1\ 3)\rangle,\ \langle(2\ 3)\rangle.$$

Luego, tenemos el grupo alternante, que es el único subgrupo de orden 3:

$$A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}.$$



El subgrupo A_3 es normal, ya que para todo $\tau \in S_3$, si σ es un 3-ciclo, entonces $\tau\sigma\tau^{-1}$ es también un 3-ciclo. Las relaciones

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

demuestran que los subgrupos de orden 2 no son normales. ▲

7.3.5. Ejemplo. De nuestra descripción de los subgrupos del grupo alternante A_4 en 7.2.12 se ve que el único subgrupo normal propio no trivial es

$$V = \{\mathrm{id}, (1\ 2)\,(3\ 4), (1\ 3)\,(2\ 4), (1\ 4)\,(2\ 3)\}.$$

En efecto, los subgrupos $\langle(a\ b)\,(c\ d)\rangle$ no pueden ser normales: conjugando $(a\ b)\,(c\ d)$ por un 3-ciclo se obtiene $(a'\ b')\,(c'\ d') \neq (a\ b)\,(c\ d)$. Por la misma razón, los subgrupos $\langle(a\ b\ c)\rangle$ tampoco son normales. Nos queda V, y sus elementos no triviales son precisamente todos los elementos de tipo de ciclo $(\bullet\ \bullet)\,(\bullet\ \bullet)$. Conjugando tales elementos, siempre se obtienen permutaciones del mismo tipo de ciclo. ▲

7.3.6. Ejemplo. El subgrupo de S_n

$$H := \{\sigma \in S_n \mid \sigma(n) = n\} \cong S_{n-1}$$

considerado en 7.1.7 no es normal para $n \geq 3$, puesto que $\sigma H = H\sigma$ solo para $\sigma = \mathrm{id}$. ▲

7.3.7. Observación. *Para todo grupo G su centro $Z(G)$ es un subgrupo normal.*

Demostración. Tenemos

$$Z(G) := \{x \in G \mid xg = gx \text{ para todo } g \in G\} = \{x \in G \mid x = gxg^{-1} \text{ para todo } g \in G\},$$

y en particular, para todo $g \in G$ tenemos

$$gZ(G)g^{-1} = Z(G).$$

■

7.3.8. Observación. *Para todo homomorfismo $f\colon G \to H$ el núcleo* $\ker f$ *es un subgrupo normal de G.*

Demostración. Para todo $g \in G$ y $k \in \ker f$ tenemos

$$f(g\,k\,g^{-1}) = f(g)\cdot f(k)\cdot f(g)^{-1} = f(g)\cdot f(g)^{-1} = 1,$$

así que $g\cdot(\ker f)\cdot g^{-1} \subseteq \ker f$. ■

7.3.9. Ejemplo. A_n es un subgrupo normal de S_n, siendo el núcleo del homomorfismo $\operatorname{sgn}\colon S_n \to \{\pm 1\}$. ▲

7.3.10. Ejemplo. $\mathrm{SL}_n(R)$ es un subgrupo normal de $\mathrm{GL}_n(R)$, siendo el núcleo de $\det\colon \mathrm{GL}_n(R) \to R^\times$. ▲

7.3.11. Ejemplo. El signo de un número real es un homomorfismo $\operatorname{sgn}\colon \mathbb{R}^\times \to \{\pm 1\}$. Consideremos el homomorfismo

$$\mathrm{GL}_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^\times \xrightarrow{\operatorname{sgn}} \{\pm 1\}.$$

Su núcleo es el subgrupo normal

$$\mathrm{GL}_n(\mathbb{R})^+ := \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A > 0\}.$$

▲

A diferencia del núcleo $\ker f \subset G$, la imagen $\operatorname{im} f \subset H$ de un homomorfismo $f\colon G \to H$ en general no es un subgrupo normal. De hecho, si $K \subset H$ no es un subgrupo normal, entonces la inclusión $i\colon K \rightarrowtail H$ tiene K como su imagen. En los grupos abelianos, todos subgrupos son normales, así que si $f\colon A \to B$ es un homomorfismo de grupos abelianos, entonces $\operatorname{im} f \subset B$ es un subgrupo normal. Es una diferencia fundamental entre los grupos abelianos y no abelianos.

7.4 Grupos cociente

El siguiente resultado explica el significado de la noción de subgrupo normal. La normalidad de $H \subset G$ significa precisamente que la multiplicación en G es compatible con la relación de equivalencia módulo H.

7.4.1. Proposición. *Sea $H \subset G$ un subgrupo. Para cualesquiera $g_1, g_1', g_2, g_2' \in G$ se tiene*

$$g_1 \equiv g_1' \pmod{H},\quad g_2 \equiv g_2' \pmod{H} \implies g_1 g_2 \equiv g_1' g_2' \pmod{H} \tag{7.2}$$

si y solamente si H es normal.

Demostración. Recordemos que por la definición de la relación de equivalencia módulo H, la condición (7.2) nos dice que para cualesquiera $g_1, g_1', g_2, g_2' \in G$

$$g_1' \in g_1 H,\quad g_2' \in g_2 H \implies g_1 g_2 \equiv g_1' g_2' \pmod{H}.$$

Es decir, para cualesquiera $g_1, g_2 \in G$, $h_1, h_2 \in H$

$$g_1 g_2 \equiv (g_1 h_1)(g_2 h_2) \pmod{H},$$

los que es equivalente a

$$(g_1 g_2)^{-1}(g_1 h_1)(g_2 h_2) \in H$$

Luego,

$$(g_1 g_2)^{-1}(g_1 h_1)(g_2 h_2) = g_2^{-1} h_1 g_2 h_2,$$

entonces la condición es

$$g_2^{-1} h_1 g_2 \in H.$$

Esto es equivalente a la normalidad de H. ■

7.4.2. Definición. Si $H \subset G$ es un subgrupo normal, entonces el **grupo cociente** correspondiente es el conjunto de las clases laterales G/H junto con la operación

$$g_1H \cdot g_2H = (g_1g_2)H.$$

En otras palabras, el producto de las clases de equivalencia de g_1 y g_2 módulo H es la clase de equivalencia de g_1g_2.

Como acabamos de ver, la fórmula de arriba tiene sentido: si H es normal, entonces la clase lateral $(g_1g_2)H$ no depende de g_1 y g_2, sino de las clases laterales g_1H y g_2H. Esta operación es asociativa, puesto que la operación en G lo es; la identidad en G/H es la clase lateral $1H = H$; los inversos vienen dados por $(gH)^{-1} = g^{-1}H$.

7.4.3. Comentario. El lector debe de conocer esta definición del curso de álgebra lineal. Si U es un espacio vectorial y $V \subset U$ es un subespacio, entonces sobre el espacio cociente

$$U/V = \{u + V \mid u \in U\}$$

la adición se define por

$$(u_1 + V) + (u_2 + V) := (u_1 + u_2) + V.$$

De la misma manera, para un grupo abeliano A y su subgrupo $B \subset A$ se define el grupo cociente A/B. Para los grupos no abelianos, todo se complica: como acabamos de ver, para que la multiplicación sobre G/H tenga sentido, necesitamos que H sea normal en G.

La fórmula $|G/H| = |G|/|H|$ para grupos finitos (el teorema de Lagrange) es un análogo de la fórmula $\dim_k U/V = \dim_k U - \dim_k V$ en álgebra lineal para espacios vectoriales de dimensión finita.

7.4.4. Ejemplo. Todos los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$. Son automáticamente normales, ya que nuestro grupo es abeliano. La relación $a \equiv b \pmod{n\mathbb{Z}}$ significa que $a \equiv b \pmod{n}$. El grupo cociente $\mathbb{Z}/n\mathbb{Z}$ no es otra cosa que el grupo de los restos módulo n que hemos denotado por $\mathbb{Z}/n\mathbb{Z}$ desde el principio. ▲

7.4.5. Ejemplo. El grupo alternante A_n es un subgrupo normal del grupo simétrico S_n. Para el grupo cociente S_n/A_n tenemos

$$|S_n/A_n| = |S_n|/|A_n| = \frac{n!}{n!/2} = 2,$$

entonces $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$. De hecho, es más lógico escribir "$\{\pm 1\}$", ya que todo esto viene del signo de permutaciones. ▲

7.4.6. Ejemplo. En el grupo alternante A_4 el único subgrupo normal propio es V. Tenemos

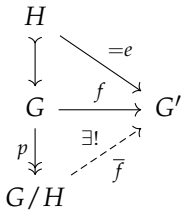
$$|A_4/V| = |A_4|/|V| = \frac{4!/2}{4} = 3,$$

así que $A_4/V \cong \mathbb{Z}/3\mathbb{Z}$. ▲

7.4.7. Proposición (Propiedad universal del cociente). *Sea $H \subseteq G$ un subgrupo normal. Sea*

$$p\colon G \twoheadrightarrow G/H,$$
$$g \mapsto gH$$

el epimorfismo sobre el grupo cociente. Si $f\colon G \to G'$ es un homomorfismo de grupos tal que $H \subseteq \ker f$, entonces f se factoriza de modo único por G/H: existe un homomorfismo único $\overline{f}\colon G/H \to G'$ tal que $f = \overline{f} \circ p$.



Demostración. La flecha punteada $\overline{f}$ es necesariamente

$$gH \mapsto f(g).$$

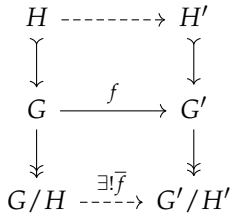
Es una aplicación bien definida: si $gH = g'H$ para algunos $g, g' \in G$, entonces $g^{-1}g' \in H$, luego $g^{-1}g' \in \ker f$ y

$$f(g^{-1}g') = 1 \iff f(g) = f(g').$$

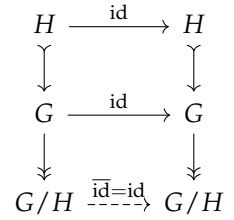
La aplicación $\overline{f}$ es un homomorfismo de grupos, puesto que f lo es. ■

7.4.8. Corolario (Funtorialidad del cociente).

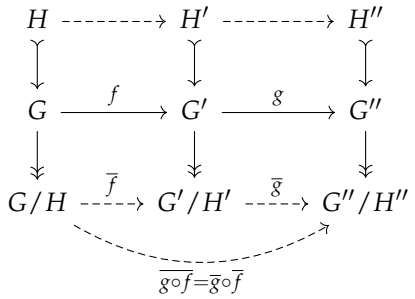
1) *Sea $f\colon G \to G'$ un homomorfismo de grupos. Sean $H \subseteq G$ y $H' \subseteq G'$ subgrupos normales. Supongamos que $f(H) \subseteq H'$. Entonces f induce un homomorfismo canónico $\widetilde{f}\colon G/H \to G'/H'$ que conmuta con las proyecciones canónicas:*



2) *La aplicación identidad* $\mathrm{id}\colon G \to G$ *induce la aplicación identidad* $\mathrm{id}\colon G/H \to G/H$*:*



3) *Sean $f\colon G \to G'$ y $g\colon G' \to G''$ dos homomorfismos y sean $H \subseteq G$, $H' \subseteq G'$, $H'' \subseteq G''$ subgrupos normales tales que $f(H) \subseteq H'$ y $g(H') \subseteq H''$. Luego, $\overline{g \circ f} = \overline{g} \circ \overline{f}$:*



Demostración. En 1) la flecha $\overline{f}$ existe y es única gracias a la propiedad universal de G/H aplicada a la composición $G \xrightarrow{f} G' \twoheadrightarrow G'/H'$. Los resultados de 2) y 3) siguen de la unicidad del homomorfismo inducido sobre los grupos cociente. ■

7.5 Grupos simples

Los grupos simples tienen importancia inestimable en la teoría de grupos, pero por falta de tiempo, voy a mencionar solamente algunos ejemplos de ellos.

7.5.1. Definición. Se dice que un grupo G es **simple** si los únicos subgrupos normales de G son $\{1\}$ y el mismo G.

7.5.2. Ejemplo. Un grupo abeliano es simple si y solamente si es isomorfo al grupo cíclico $\mathbb{Z}/p\mathbb{Z}$ de orden primo p. ▲

7.5.3. Ejemplo. Los grupos $\mathrm{SL}_n(k)$ no son simples, puesto que estos tienen centro que consiste en las matrices escalares

$$\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}, \quad a^n = 1.$$

Se puede pasar al grupo cociente

$$\mathrm{PSL}_n(k) := \mathrm{SL}_n(k)/Z(\mathrm{SL}_n(k))$$

llamado el **grupo especial lineal proyectivo**. Resulta que el grupo $\mathrm{PSL}_n(k)$ es simple con dos excepciones:

1) $n = 2$ y $k = \mathbb{F}_2$, donde

$$\mathrm{PSL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$$

y S_3 tiene un subgrupo normal A_3,

2) $n = 2$ y $k = \mathbb{F}_3$, donde

$$\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4 \tag{7.3}$$

y A_4 tiene un subgrupo normal V.

Para las demostraciones, refiero a [Lan2002, §§XIII.8–9]. ▲

Simplicidad de A_n

Junto con (7.3), se tiene otro "isomorfismo excepcional"

$$\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5,$$

y este grupo es simple. Esto también se puede ver directamente para A_5, pero por el momento voy a omitir la prueba, que no me parece muy instructiva.

7.5.4. Lema. *Para $n \geq 5$ todos los 3-ciclos son conjugados en A_n. A saber, si $(a\ b\ c)$ y $(a'\ b'\ c')$ son dos 3-ciclos en A_n, entonces existe $\sigma \in A_n$ tal que*

$$(a'\ b'\ c') = \sigma\,(a\ b\ c)\,\sigma^{-1}.$$

Demostración. A priori sabemos que $(a\ b\ c)$ y $(a'\ b'\ c')$ son conjugados en S_n: existe $\sigma \in S_n$ tal que

$$(a'\ b'\ c') = \sigma\,(a\ b\ c)\,\sigma^{-1}.$$

Ahora si $\operatorname{sgn}\sigma = +1$, entonces $\sigma \in A_n$ y no hay nada que probar. Si $\operatorname{sgn}\sigma = -1$, entonces gracias a nuestra hipótesis que $n \geq 5$, existen índices $1 \leq i < j \leq n$ tales que $i, j \notin \{a, b, c\}$. Tenemos $\sigma\,(i\ j) \in A_n$, y luego

$$(\sigma\,(i\ j))\,(a\ b\ c)\,(\sigma\,(i\ j))^{-1} = \sigma\,(i\ j)\,(a\ b\ c)\,(i\ j)\,\sigma^{-1} = \sigma\,(i\ j)\,(i\ j)\,(a\ b\ c)\,\sigma^{-1} = \sigma\,(a\ b\ c)\,\sigma^{-1} = (a'\ b'\ c'),$$

usando que $(a\ b\ c)$ e $(i\ j)$ conmutan, siendo ciclos disjuntos. ■

7.5.5. Comentario. En general, dos permutaciones con el mismo tipo de ciclo no son necesariamente conjugadas en A_n. Por ejemplo, los 5-ciclos $(1\ 2\ 3\ 4\ 5)$ y $(1\ 2\ 3\ 5\ 4)$ no son conjugados en A_5.

7.5.6. Corolario. *Sea $H \subseteq A_n$ un subgrupo normal tal que H contiene un 3-ciclo. Entonces, $H = A_n$.*

Demostración. Si H es normal, junto con todo elemento $\sigma \in H$, este debe contener todos sus conjugados $\tau\,\sigma\,\tau^{-1}$ para $\tau \in A_n$. Entonces, la hipótesis implica que H contiene todos los 3-ciclos. Estos generan A_n. ■

7.5.7. Teorema. *El grupo alternante A_n es simple para $n \geq 5$.*

Demostración ([Per1996]). Ya aceptamos este resultado para $n = 5$. Sea $n \geq 6$ y sea H un subgrupo normal en A_n tal que $H \neq \{\mathrm{id}\}$. Vamos a ver que usando cierto truco, la simplicidad de A_n sigue de la simplicidad de A_5.

Sea $\sigma \in H$ una permutación no trivial. Esto significa que $b = \sigma(a) \neq a$ para algunos $a, b \in \{1, \ldots, n\}$. Escojamos un elemento $c \in \{1, \ldots, n\}$ tal que $c \neq a, b, \sigma(b)$. Consideremos la permutación

$$\tau = (a\ c\ b)\,\sigma\,(a\ c\ b)^{-1}\,\sigma^{-1} = (a\ c\ b)\,\sigma\,(a\ b\ c)\,\sigma^{-1}.$$

Por nuestra hipótesis que H es un subgrupo normal, se tiene $(a\ c\ b)\,\sigma\,(a\ c\ b)^{-1} \in H$, y por lo tanto $\tau \in H$. Ahora notamos que para

$$i \notin \{a, b, c, \sigma(b), \sigma(c)\}$$

se cumple $\sigma^{-1}(i) \notin \{a, b, c\}$ y luego $\tau(i) = i$. Esto significa que τ pertenece al subgrupo

$$H_0 := \{\sigma \in A_n \mid \sigma(i) = i \text{ para } i \notin \{a, b, c, \sigma(b), \sigma(c)\}\}.$$

Ya que $\tau(b) = (a\ c\ b)\,\sigma(b) \neq b$, la permutación τ no es trivial.

Ya que H es normal en A_n, entonces $H \cap H_0$ es un subgrupo normal no trivial en H_0. Pero $H_0 \cong A_5$, y este grupo es simple, así que se puede concluir que $H \cap H_0 = H_0$. En particular, $(a\ b\ c) \in H$, pero esto implica que $H = A_n$. ■

7.5.8. Corolario. $Z(A_n) = \{\mathrm{id}\}$ *para* $n \geq 4$.

Demostración. Para $n = 4$ esto se puede verificar directamente. Para $n \geq 5$, es suficiente notar que $Z(A_n)$ es un subgrupo normal y $Z(A_n) \neq A_n$, ya que A_n no es conmutativo. Luego, $Z(A_n)$ es trivial. ■

7.5.9. Corolario. *Para* $n \geq 5$ *los únicos subgrupos normales de* S_n *son* $\{\mathrm{id}\}$, A_n *y* S_n.

Demostración. Sea $H \subseteq S_n$ un subgrupo normal. El grupo $H \cap A_n$ es un subgrupo normal de A_n y por lo tanto es igual a A_n o $\{\mathrm{id}\}$.

Si $H \cap A_n = A_n$, entonces $H = A_n$, o H contiene una permutación impar junto con todos los elementos de A_n y luego $H = S_n$.

Si $H \cap A_n = \{\mathrm{id}\}$, entonces H no contiene permutaciones pares no triviales. Pero si σ y τ son dos permutaciones impares, entonces $\sigma\tau$ es par, así que la única posibilidad es $H = \{\mathrm{id}, \sigma\}$ para una permutación impar. Pero este subgrupo está muy lejos de ser normal: conjugando σ por los elementos de S_n, se puede obtener cualquier permutación del mismo tipo de ciclo y así salir de H. ■

7.5.10. Comentario. Para $n = 4$ el subgrupo

$$V = \{\mathrm{id}, (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\}$$

es normal en S_4, dado que sus elementos no triviales son todas las permutaciones del tipo de ciclo $(\bullet\ \bullet)\ (\bullet\ \bullet)$.

7.6 Primer teorema de isomorfía

El lector debe de conocer el siguiente resultado de álgebra lineal: si $f\colon U \to V$ es una aplicación lineal, entonces $U/\ker f \cong \operatorname{im} f$. El mismo resultado se cumple para grupos cociente.

7.6.1. Proposición (Primer teorema de isomorfía). *Sea* $f\colon G \to H$ *un homomorfismo de grupos. Entonces, existe un isomorfismo canónico*

$$\overline{f}\colon G/\ker f \xrightarrow{\cong} \operatorname{im} f$$

que hace parte del diagrama conmutativo

(7.4)
$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ \downarrow & & \uparrow \\ G/\ker f & \xrightarrow[\cong]{\exists!\,\overline{f}} & \operatorname{im} f \end{array}$$

Descifremos el diagrama conmutativo: la flecha $G \twoheadrightarrow G/\ker f$ es la proyección canónica $g \mapsto g \cdot \ker f$, y la flecha $\operatorname{im} f \rightarrowtail H$ es la inclusión de subgrupo, así que el isomorfismo $\overline{f}$ necesariamente viene dado por

$$\overline{f}\colon g \cdot \ker f \mapsto f(g).$$

Demostración. La flecha $\overline{f}$ es dada por la propiedad universal de $G/\ker f$:

$$\begin{array}{ccccc} \ker f & & & & \\ \downarrow & \searrow^{=e} & & & \\ G & \xrightarrow{\quad f \quad} & \operatorname{im} f & & \\ \downarrow & \nearrow_{\exists!\,\overline{f}} & & & \\ G/\ker f & & & & \end{array}$$

Luego, el homomorfismo $\overline{f}$ es evidentemente sobreyectivo. Para ver que es inyectivo, recordamos que

$$f(g_1) = f(g_2) \iff g_1^{-1}g_2 \in \ker f \iff g_1 \cdot \ker f = g_2 \cdot \ker f.$$

■

El diagrama (7.4) demuestra que todo homomorfismo de grupos puede ser escrito como una composición de un epimorfismo y un monomorfismo. Esto se conoce como la **factorización epi-mono** de f.

También hay segundo y tercer teorema de isomorfía, pero los vamos a ver en los ejercicios.

7.6.2. Corolario. *Si G es un grupo finito, entonces para todo homomorfismo $f\colon G \to H$ tenemos*

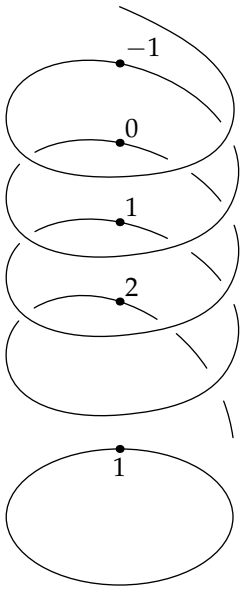
$$|G| = |\operatorname{im} f| \cdot |\ker f|.$$

El último resultado es un análogo de la fórmula $\dim_k U = \dim_k \operatorname{im} f + \dim_k \ker f$ que tenemos para una aplicación lineal $f\colon U \to V$, donde U es un espacio de dimensión finita.

7.6.3. Ejemplo. Compilemos una tabla con ejemplos familiares de homomorfismos.

	epimorfismo	núcleo	conclusión
1)	$\mathbb{R}^\times \xrightarrow{x\mapsto\lvert x\rvert} \mathbb{R}_{>0}$	$\{\pm 1\}$	$\mathbb{R}^\times/\{\pm 1\} \cong \mathbb{R}_{>0}$
2)	$\mathbb{C}^\times \xrightarrow{z\mapsto z^n} \mathbb{C}^\times$	$\mu_n(\mathbb{C})$	$\mathbb{C}^\times/\mu_n(\mathbb{C}) \cong \mathbb{C}^\times$
3)	$\mathbb{R} \xrightarrow{x\mapsto e^{2\pi i x}} \mathbb{T}$	$\mathbb{Z}$	$\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$
4)	$\mathrm{GL}_n(R) \xrightarrow{\det} R^\times$	$\mathrm{SL}_n(R)$	$\mathrm{GL}_n(R)/\mathrm{SL}_n(R) \cong R^\times$
5)	$S_n \xrightarrow{\mathrm{sgn}} \{\pm 1\}$	A_n	$S_n/A_n \cong \{\pm 1\}$
6)	$\mathrm{GL}_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^\times \xrightarrow{\mathrm{sgn}} \{\pm 1\}$	$\mathrm{GL}_n(\mathbb{R})^+$	$\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{R})^+ \cong \{\pm 1\}$
7)	$\mathbb{C}^\times \xrightarrow{z\mapsto\lvert z\rvert} \mathbb{R}_{>0}$	$\mathbb{T}$	$\mathbb{C}^\times/\mathbb{T} \cong \mathbb{R}_{>0}$
8)	$\mathbb{C}^\times \xrightarrow{z\mapsto z/\lvert z\rvert} \mathbb{T}$	$\mathbb{R}_{>0}$	$\mathbb{C}^\times/\mathbb{R}_{>0} \cong \mathbb{T}$

El ejemplo bastante curioso es 2): el cociente de $\mathbb{C}^\times$ por un subgrupo propio $\mu_n(\mathbb{C})$ es isomorfo al mismo grupo $\mathbb{C}^\times$. En 3) la aplicación $x \mapsto e^{2\pi i x}$ puede ser visualizada como una hélice que se proyecta al círculo:



Los isomorfismos en 7) y 8) vienen de la representación canónica de un número complejo $z = r\,e^{i\phi}$ donde $r \in \mathbb{R}_{>0}$ y $0 \leq \phi < 2\pi$. ▲

7.6.4. Ejemplo. Consideremos la aplicación

$$\begin{aligned} \mathbb{Q} &\to \mathbb{C}^\times, \\ m/n &\mapsto e^{2\pi i \cdot m/n}. \end{aligned}$$

Es un homomorfismo de grupos. Su imagen coincide con el subgrupo $\mu_\infty(\mathbb{C})$ formado por todas las raíces de la unidad. El núcleo de este homomorfismo es $\mathbb{Z}$. Entonces, tenemos

$$\mathbb{Q}/\mathbb{Z} \cong \mu_\infty(\mathbb{C});$$

el grupo multiplicativo de las raíces de la unidad corresponde nada más al grupo aditivo de los "números racionales módulo $\mathbb{Z}$". Los elementos de $\mathbb{Q}/\mathbb{Z}$ pueden ser representados por las fracciones de la forma a/b donde $a < b$. Por ejemplo,

$$[1/2] + [3/4] = [5/4] = [1/4]$$

y

$$-[3/4] = [1/4].$$

En particular, bajo el isomorfismo de arriba, el grupo $\mu_n(\mathbb{C})$ de las raíces n-ésimas de la unidad corresponde al grupo cíclico

$$\left\langle \frac{1}{n} \right\rangle = \left\{ 0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n} \right\} \subset \mathbb{Q}/\mathbb{Z}.$$

▲

7.7 Ejercicios

Ejercicio 7.1. *Demuestre que si $H \subset G$ es un subgrupo de índice $|G : H| = 2$, entonces H es normal.*

Ejercicio 7.2. *Demuestre que todo cociente de un grupo cíclico es cíclico.*

Ejercicio 7.3 (Segundo teorema de isomorfía). *Sea G un grupo, sea $H \subset G$ un subgrupo y $K \subset G$ un subgrupo normal.*

1) *Demuestre que $HK := \{hk \mid h \in H,\ k \in K\}$ es un subgrupo de G.*

2) *Demuestre que K es un subgrupo normal de HK.*

3) *Demuestre que la aplicación*
$$H \to HK/K, \quad h \mapsto hK$$
es un homomorfismo sobreyectivo de grupos y su núcleo es $H \cap K$.

4) *Deduzca que $H/(H \cap K) \cong HK/K$.*

Ejercicio 7.4. *Para un cuerpo k sea $G = \mathrm{GL}_2(k)$, $H = \mathrm{SL}_2(k)$, $K = k^\times \cdot I \subset \mathrm{GL}_2(k)$. Deduzca que*
$$\mathrm{SL}_2(k)/\{\pm I\} \cong \mathrm{GL}_2(k)/k^\times.$$

Ejercicio 7.5 (Tercer teorema de isomorfía). *Sea G un grupo. Sea K un subgrupo normal de G y sea N un subgrupo de K tal que N es normal en G.*

1) *Demuestre que la aplicación*
$$G/N \to G/K, \quad gN \mapsto gK$$
está bien definida y es un homomorfismo sobreyectivo y su núcleo es $K/N \subset G/N$.

2) *Deduzca que $(G/N)/(K/N) \cong G/K$.*

Ejercicio 7.6. *Sean m y n dos enteros positivos tales que $n \mid m$, así que $m\mathbb{Z} \subset n\mathbb{Z}$. Demuestre que*
$$(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}.$$

Se dice que un grupo abeliano A un elemento $x \in A$ es **divisible** si para todo $a \in A$ y todo entero positivo $n = 1, 2, 3, \ldots$ existe $b \in A$ (no necesariamente único) tal que $nb = a$. Si todos los elementos de A son divisibles, se dice que A es un **grupo divisible**.

Ejercicio 7.7.

1) *Demuestre que los grupos aditivos $\mathbb{Q}$ y $\mathbb{R}$ son divisibles.*

2) *Demuestre que un grupo abeliano finito no nulo nunca es divisible.*

Ejercicio 7.8. *Sea p un número primo. El **p-grupo de Prüfer** es el grupo de las raíces de la unidad de orden p^n para $n \in \mathbb{N}$:*
$$\mu_{p^\infty}(\mathbb{C}) := \bigcup_{n \geq 0} \mu_{p^n}(\mathbb{C}) = \{z \in \mathbb{C}^\times \mid z^{p^n} = 1 \text{ para algún } n = 0, 1, 2, \ldots\}$$

1) *Demuestre que $\mu_{p^\infty}(\mathbb{C})$ es divisible.*

2) *Demuestre que existe un isomorfismo* $\mu_{p^\infty}(\mathbb{C}) \cong \mathbb{Z}[1/p]/\mathbb{Z}$ *donde*

$$\mathbb{Z}[1/p] := \{a/p^n \mid a \in \mathbb{Z},\ n = 0, 1, 2, \ldots\}.$$

Ejercicio 7.9.

1) *Demuestre que todos los elementos divisibles forman un subgrupo*

$$A_{div} := \{a \in A \mid a \text{ es divisible } \}.$$

Este se llama el ***subgrupo máximo divisible*** *de* A.

2) *Sea* $f\colon A \to B$ *un homomorfismo de grupos. Demuestre que si* $a \in A$ *es divisible, entonces* $f(a) \in B$ *es también divisible. En particular,* f *se restringe a un homomorfismo* $A_{div} \to B_{div}$.

$$\begin{array}{ccc} A_{div} & \dashrightarrow & B_{div} \\ \downarrow & & \downarrow \\ A & \xrightarrow{f} & B \end{array}$$

3) *Demuestre que todo grupo cociente de un grupo divisible es también divisible. En particular,* $\mathbb{Q}/\mathbb{Z}$ *y* $\mathbb{R}/\mathbb{Z}$ *son divisibles.*

Ejercicio 7.10. *Demuestre que no hay homomorfismos no triviales* $\mathbb{Q} \to \mathbb{Z}$ *y* $\mathbb{Q}/\mathbb{Z} \to \mathbb{Z}$.

Bibliografía

[Lan2002] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556
http://dx.doi.org/10.1007/978-1-4613-0041-0

[Per1996] Daniel Perrin, *Cours d'algèbre*, third ed., CAPES / AGREG Mathématiques, Ellipses, 1996.

[Ser1973] Jean-Pierre Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7. MR0344216