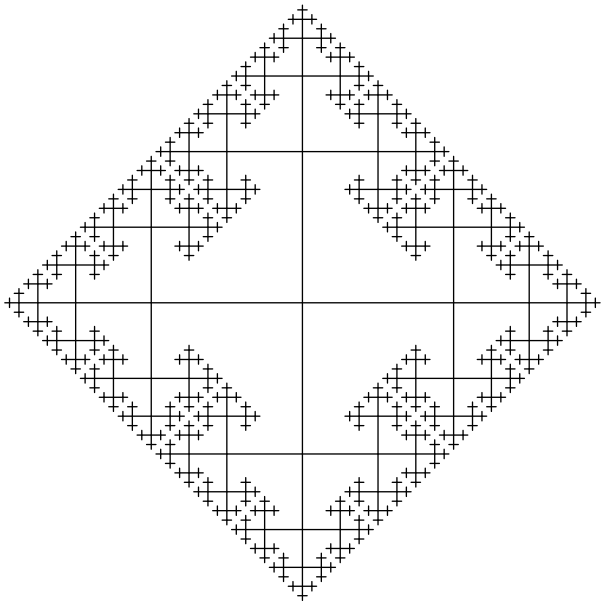
Universidad de El Salvador
2018

CURSO DE ÁLGEBRA



Alexey Beshenov
(cadadr@gmail.com)

Introducción

Álgebra.
1. Parte de las matemáticas en la cual las operaciones aritméticas son generalizadas empleando números, letras y signos.
2. Arte de restituir a su lugar los huesos dislocados.

Diccionario de la Real Academia Española

Argent, machinisme, algèbre. Les trois monstres de la civilisation actuelle. Analogie complète. L'algèbre et l'argent sont essentiellement niveleurs, la première intellectuellement, l'autre effectivement.
<...>
Il n'y a point de pensée collective. En revanche, notre science est collective comme notre technique. Spécialisation. On hérite non seulement de résultats, mais encore de méthodes qu'on ne comprend pas. Au reste les deux sont inséparables, car les résultats de l'algèbre fournissent des méthodes aux autres sciences.

Simone Weil, "La pesanteur et la grâce"

Estos son mis apuntes para las clases de álgebra que estoy dando en la Universidad de El Salvador en el año académico 2018. La selección del material es bastante modesta y típica, pero al mismo tiempo refleja mis gustos personales.

Este texto (y en particular esta breve introducción) será expandido y redactado durante el curso. Favor de enviar sus comentarios a `cadadr@gmail.com`.

Ejercicios

Todos los capítulos de estos apuntes, salvo el capítulo 0, vienen con ejercicios. La mayoría son bastante típicos y no deben ser demasiado difíciles. El lector tiene que *intentar* resolverlos todos.

Notación

Vamos a usar la notación estándar, adoptada por Bourbaki. Por ejemplo,

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

denota los números naturales, enteros, racionales, reales y complejos respectivamente. El número 0 es también natural. La unidad imaginaria se denotará por $\sqrt{-1}$.

Agradecimientos

Agradezco al Ministerio de educación de El Salvador por financiar mi estancia y personalmente al ministro Ing. Carlos Mauricio Canjura Linares; al Director de la Escuela de Matemática de la Universidad de El Salvador José Nerys Funes Torres y al director del Programa "Jovenes Talento" Prof. Ernesto Americo Hidalgo Castellanos. Dr. Riquelmi Salvador Cardona Fuentes participó en la organización de este curso y dio las primeras lecciones.

Gabriel Chicas Reyes y José Ibrahim Villanueva Gutiérrez me ayudaron con la redacción de estos apuntes e hicieron varios comentarios útiles.

Sobre todo agradezco a todos los alumnos de la universidad de El Salvador que han asistido a mis clases.

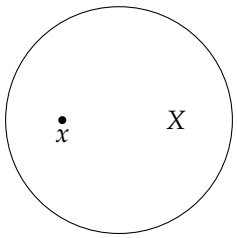
Índice general

Parte I
Introducción a estructuras algebraicas

Capítulo 0
Conjuntos

Asumo que el lector conozca algunas bases de la teoría de conjuntos elemental. En este capítulo vamos a revisar ciertas propiedades de aplicaciones entre conjuntos. Primero recordemos la notación.

- La cardinalidad de un conjunto X se denota por $|X|$. Vamos a usar esta notación para conjuntos finitos, es decir cuando $|X|$ corresponde a un número natural.
- Si un elemento x pertenece a un conjunto X, se escribe "$x \in X$" o a veces "$X \ni x$".

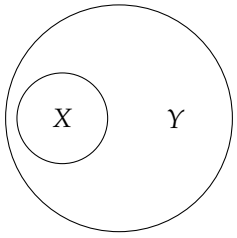


- El **conjunto vacío** se denota por $\emptyset$. Es el conjunto que no tiene ningún elemento:

$$|\emptyset| = 0.$$

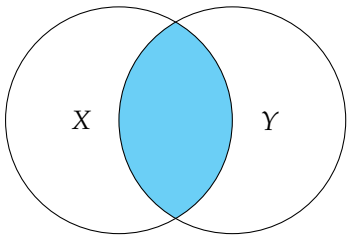
- Si un conjunto X está contenido en un conjunto Y, se escribe "$X \subseteq Y$" o "$Y \supseteq X$":

$$x \in X \Rightarrow x \in Y.$$

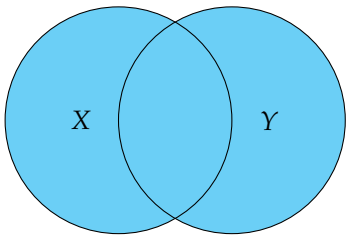


  A veces para subrayar que X está contenido en Y, pero $X \neq Y$, se escribe "$X \subsetneq Y$" o "$Y \supsetneq X$".
- La **intersección** y **unión** de dos conjuntos X y Y se denotan por "$X \cap Y$" y "$X \cup Y$" respectivamente:

$$X \cap Y := \{z \mid z \in X \text{ y } z \in Y\},$$
$$X \cup Y := \{z \mid z \in X \text{ o } z \in Y\}.$$



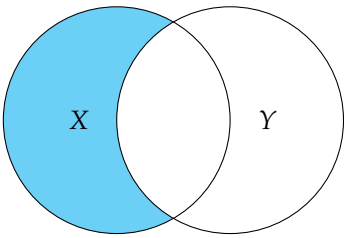
$X \cap Y$



$X \cup Y$

- La **diferencia** entre dos conjuntos X e Y se denota por "$X \setminus Y$":

$$X \setminus Y := \{x \in X \mid x \notin Y\}.$$



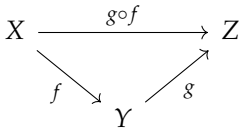
$X \setminus Y$

0.1 Aplicaciones entre conjuntos

0.1.1. Definición. Para dos aplicaciones $f\colon X \to Y$ e $g\colon Y \to Z$ la composición $g \circ f\colon X \to Y$ es la aplicación definida por

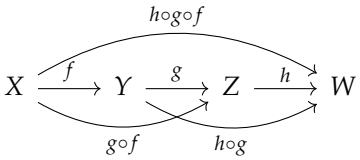
$$(g \circ f)(x) := g(f(x)).$$

Esta información puede representarse mediante un "diagrama conmutativo":



0.1.2. Observación. *La composición es* ***asociativa****: para $f\colon X \to Y$, $g\colon Y \to Z$, $h\colon Z \to W$ tenemos*

$$(h \circ g) \circ f = h \circ (g \circ f).$$



0.1.3. Corolario (Asociatividad generalizada). *Para n aplicaciones*

$$X_1 \xrightarrow{f_1} X_2 \xrightarrow{f_2} \cdots \to X_{n-1} \xrightarrow{f_{n-1}} X_n \xrightarrow{f_n} X_{n+1}$$

Toda manera de poner los paréntesis en la expresión

$$f_n \circ f_{n-1} \circ \cdots \circ f_2 \circ f_1$$

(es decir, de calcular la composición) da el mismo resultado.

0.1.4. Ejemplo. Para $n = 3$, tenemos dos posibilidades:

$$(f_3 \circ f_2) \circ f_1, \quad f_3 \circ (f_2 \circ f_1).$$

El resultado es el mismo según 0.1.2. Para $n = 4$ hay 5 posibilidades:

$$((f_4 \circ f_3) \circ f_2) \circ f_1, \quad (f_4 \circ (f_3 \circ f_2)) \circ f_1, \quad (f_4 \circ f_3) \circ (f_2 \circ f_1), \quad f_4 \circ ((f_3 \circ f_2) \circ f_1), \quad f_4 \circ (f_3 \circ (f_2 \circ f_1)).$$

En general, hay

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1}$$

posibilidades. Estos números se conocen como los **números de Catalan**[*].

n:	3	4	5	6	7	8	9	10	11	12
C_n:	2	5	14	42	132	429	1430	4862	16796	58786

▲

Demostración. Para $n = 2$ no hay que demostrar nada y el caso de $n = 3$ es el contenido de 0.1.2. Para $n > 3$, supongamos que la propiedad se cumple para toda composición de $< n$ aplicaciones. En una expresión $f_n \circ f_{n-1} \circ \cdots \circ f_2 \circ f_1$, después de poner los paréntesis de algún modo, tenemos

$$(f_n \circ \cdots \circ f_{r+1}) \circ (f_r \circ \cdots \circ f_1),$$

donde las expresiones en los paréntesis están bien definidas por la hipótesis de la inducción. Sea

$$(f_n \circ \cdots \circ f_{s+1}) \circ (f_s \circ \cdots \circ f_1)$$

otro modo de poner los paréntesis. Sin pérdida de generalidad, $r < s$. Tenemos

$$f_n \circ \cdots \circ f_{r+1} = (f_n \circ \cdots \circ f_{s+1}) \circ (f_s \circ \cdots \circ f_{r+1})$$

y

$$f_s \circ \cdots \circ f_1 = (f_s \circ \cdots \circ f_{r+1}) \circ (f_r \circ \cdots \circ f_1).$$

Ahora

$$(f_n \circ \cdots \circ f_{r+1}) \circ (f_r \circ \cdots \circ f_1) = \big((f_n \circ \cdots \circ f_{s+1}) \circ (f_s \circ \cdots \circ f_{r+1})\big) \circ (f_r \circ \cdots \circ f_1)$$

y

$$(f_n \circ \cdots \circ f_{s+1}) \circ (f_s \circ \cdots \circ f_1) = (f_n \circ \cdots \circ f_{s+1}) \circ \big((f_s \circ \cdots \circ f_{r+1}) \circ (f_r \circ \cdots \circ f_1)\big).$$

Por inducción, las últimas dos expresiones coinciden. ■

Para cualquier conjunto X, existe una aplicación distinguida $X \to X$, a saber la que aplica todo elemento en sí mismo.

0.1.5. Definición. La **aplicación identidad** $\mathrm{id}_X \colon X \to X$ se define como

$$\mathrm{id}_X(x) := x.$$

[*] Eugène Charles Catalan (1814–1894), un matemático francés-belga.

0.1.6. Observación. *Para cualesquiera aplicaciones $f\colon X \to Y$ e $g\colon Y \to X$ se cumple que*

$$f \circ \mathrm{id}_X = f, \quad \mathrm{id}_X \circ g = g. \tag{0.1}$$

Note que (0.1) define a id_X de modo único: si tenemos dos aplicaciones $i'_X, i''_X\colon X \to X$ tales que para cualesquiera $f\colon X \to Y$ e $g\colon Y \to X$ se cumple

$$f \circ i'_X = f, \quad i''_X \circ g = g,$$

en particular para $X = Y$ tenemos

$$i''_X = i''_X \circ i'_X = i'_X.$$

0.1.7. Definición. Se dice que una aplicación $f\colon X \to Y$ es **invertible** si existe otra aplicación $f^{-1}\colon Y \to X$ tal que

$$f^{-1} \circ f = \mathrm{id}_X, \quad f \circ f^{-1} = \mathrm{id}_Y. \tag{0.2}$$

La notación "f^{-1}" está justificada por el hecho de que la aplicación inversa está definida de modo único.

0.1.8. Observación. *Si $f', f''\colon Y \to X$ son dos aplicaciones que satisfacen*

$$f' \circ f = \mathrm{id}_X, \quad f \circ f' = \mathrm{id}_Y, \quad f'' \circ f = \mathrm{id}_X, \quad f \circ f'' = \mathrm{id}_Y,$$

entonces

$$f' = f''.$$

Demostración. Tenemos

$$f' = f' \circ \mathrm{id}_Y = f' \circ (f \circ f'') = (f' \circ f) \circ f'' = \mathrm{id}_X \circ f'' = f''.$$

■

0.1.9. Observación. *Si $f\colon X \to Y$ es una aplicación invertible, entonces $f^{-1}\colon Y \to X$ es también invertible: su inversa es $f\colon X \to Y$:*

$$(f^{-1})^{-1} = f.$$

0.1.10. Observación. *Si $f\colon X \to Y$ e $g\colon Y \to Z$ poseen aplicaciones inversas $f^{-1}\colon Y \to X$ y $g^{-1}\colon Z \to Y$, entonces la composición $f^{-1} \circ g^{-1}\colon Z \to X$ es inversa a $g \circ f\colon X \to Z$.*

$$X \underset{f^{-1}}{\overset{f}{\rightleftarrows}} Y \underset{g^{-1}}{\overset{g}{\rightleftarrows}} Z$$

En general, toda composición de n aplicaciones invertibles $f_n \circ \cdots \circ f_1$ es también invertible y su aplicación inversa es dada por

$$(f_n \circ \cdots \circ f_1)^{-1} = f_1^{-1} \circ \cdots \circ f_n^{-1}.$$

Demostración. Tenemos

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{id}_Y \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_Z,$$

y de la misma manera,

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_Y \circ f = f^{-1} \circ f = \mathrm{id}_X.$$

En general, $(f_n \circ \cdots \circ f_1)^{-1}$ se calcula por inducción sobre n. Acabamos de ver el caso de $n = 2$. Para el paso inductivo, escribamos

$$(f_n \circ \cdots \circ f_1)^{-1} = (f_n \circ (f_{n-1} \circ \cdots \circ f_1))^{-1} = (f_{n-1} \circ \cdots \circ f_1)^{-1} \circ f_n^{-1}.$$

■

0.2 Aplicaciones inyectivas, sobreyectivas y biyectivas

0.2.1. Definición. Una aplicación entre conjuntos $f\colon X \to Y$ es

1) **inyectiva** si f aplica diferentes elementos de X en diferentes elementos de Y; es decir, $f(x) = f(x') \Rightarrow x = x'$;

2) **sobreyectiva** si para todo $y \in Y$ existe $x \in X$ tal que $f(x) = y$;

3) **biyectiva** si es inyectiva y sobreyectiva al mismo tiempo.

0.2.2. Observación. *Sean $f\colon X \to Y$ e $g\colon Y \to Z$ dos aplicaciones. Si f y g son inyectivas (resp. sobreyectivas, biyectivas), entonces $g \circ f$ es también inyectiva (resp. sobreyectiva, biyectiva).*

Demostración. Inmediato a partir de las definiciones en 0.2.1. ■

0.2.3. Proposición. *Sea $f\colon X \to Y$ una aplicación entre conjuntos.*

1) f es inyectiva si y solamente si es cancelable por la izquierda: para todo par de aplicaciones $g, g'\colon Z \to X$ tenemos

$$f \circ g = f \circ g' \Rightarrow g = g'. \tag{0.3}$$

2) f es sobreyectiva si y solamente si es cancelable por la derecha: para todo par de aplicaciones $g, g'\colon Y \to Z$ tenemos

$$g \circ f = g' \circ f \Rightarrow g = g'. \tag{0.4}$$

3) f es biyectiva si y solamente si f es invertible.

Demostración.

1) Si f es inyectiva, entonces para todo $z \in Z$ tenemos

$$f(g(z)) = f(g'(z)) \Rightarrow g(z) = g'(z),$$

es decir, se cumple (0.3). Luego, para $x, x' \in X$ podemos considerar las aplicaciones

$$\begin{aligned} g\colon \{\bullet\} &\to X, \\ \bullet &\mapsto x, \\ g'\colon \{\bullet\} &\to X, \\ \bullet &\mapsto x'. \end{aligned}$$

La condición (0.3) quiere decir precisamente

$$f(x) = f(x') \Rightarrow x = x',$$

es decir, que f es inyectiva.

2) Si f es sobreyectiva, entonces todo $y \in Y$ es de la forma $f(x)$ para algún $x \in X$ y la identidad $g \circ f = g' \circ f$ implica que $g = g'$.
Ahora consideremos dos aplicaciones $g, g'\colon Y \to \{0,1\}$ definidas por

$$g(y) := 1 \quad \text{para todo } y \in Y$$

y

$$g'(y) := \begin{cases} 1, & \text{si } y = f(x) \text{ para algún } x \in X, \\ 0, & \text{en el caso contrario.} \end{cases}$$

Tenemos $g \circ f = g' \circ f$ y la identidad $g = g'$ quiere decir precisamente que f es sobreyectiva.

3) Supongamos que f es una biyección. Esto quiere decir que para todo $y \in Y$ existe único elemento $x \in X$ tal que $f(x) = y$. Podemos definir entonces

$$\begin{aligned} f^{-1}\colon Y &\to X, \\ y &\mapsto x \text{ tal que } f(x) = y, \end{aligned}$$

y esta aplicación satisface (0.2).
Ahora si se cumple (0.2), entonces f es cancelable por la izquierda y por la derecha: para todo $g, g'\colon Z \to X$ tenemos

$$\begin{aligned} f \circ g = f \circ g' \Rightarrow f^{-1} \circ (f \circ g) = f^{-1} \circ (f \circ g') \Rightarrow (f^{-1} \circ f) \circ g = (f^{-1} \circ f) \circ g' \\ \Rightarrow \mathrm{id}_X \circ g = \mathrm{id}_X \circ g' \Rightarrow g = g', \end{aligned}$$

y para cualesquiera $g, g'\colon Y \to Z$ tenemos

$$\begin{aligned} g \circ f = g' \circ f \Rightarrow (g \circ f) \circ f^{-1} = (g' \circ f) \circ f^{-1} \Rightarrow g \circ (f \circ f^{-1}) = g' \circ (f \circ f^{-1}) \\ \Rightarrow g \circ \mathrm{id}_Y = g' \circ \mathrm{id}_Y \Rightarrow g = g', \end{aligned}$$

y por lo tanto f es inyectiva y sobreyectiva gracias a 1) y 2).

■

0.2.4. Comentario. Usando 0.2.3, podemos dar otra demostración de 0.2.2. Sean $f\colon X \to Y$ e $g\colon Y \to Z$ dos aplicaciones.

1) Si f y g son cancelables por la izquierda, entonces la composición $f \circ g$ es también cancelable por la izquierda: para cualesquiera $h, h'\colon W \to X$ tenemos

$$(g \circ f) \circ h = (g \circ f) \circ h' \Rightarrow g \circ (f \circ h) = g \circ (f \circ h') \Rightarrow f \circ h = f \circ h' \Rightarrow h = h'.$$

$$W \underset{h'}{\overset{h}{\rightrightarrows}} X \xrightarrow{f} Y \xrightarrow{g} Z$$

2) Si f y g son cancelables por la derecha, entonces la composición $f \circ g$ es también cancelable por la derecha: para cualesquiera $h, h'\colon Z \to W$ tenemos

$$h \circ (f \circ g) = h' \circ (f \circ g) \Rightarrow (h \circ f) \circ g = (h' \circ f) \circ g \Rightarrow h \circ f = h' \circ f \Rightarrow h = h'.$$

$$X \xrightarrow{f} Y \xrightarrow{g} Z \underset{h'}{\overset{h}{\rightrightarrows}} W$$

3) Ya hemos observado en 0.1.10 que la composición de aplicaciones invertibles es también invertible.

0.2.5. Observación. *Sean $f\colon X \to Y$ e $g\colon Y \to Z$ dos aplicaciones. Consideremos su composición $g \circ f$.*

1) Si $g \circ f$ es inyectiva, entonces f es también inyectiva.

2) Si $g \circ f$ es sobreyectiva, entonces g es también sobreyectiva.

Demostración. Esto debe ser claro en términos de elementos de conjuntos, pero demostrémoslo en términos de aplicaciones cancelables. La aplicación $g \circ f$ es inyectiva precisamente si es cancelable por la izquierda: para todo h, h' tenemos

$$(g \circ f) \circ h = (g \circ f) \circ h' \Rightarrow h = h'.$$

Pero esto implica en particular que f es cancelable por la izquierda:

$$f \circ h = f \circ h' \Rightarrow g \circ f \circ h = g \circ f \circ h' \Rightarrow h = h'.$$

De la misma manera, si $g \circ f$ es sobreyectiva precisamente si es cancelable por la derecha:

$$h \circ (g \circ f) = h' \circ (g \circ f) \Rightarrow h = h'.$$

Pero en este caso g tiene que ser cancelable por la derecha:

$$h \circ g = h' \circ g \Rightarrow h \circ g \circ f = h' \circ g \circ f \Rightarrow h = h'.$$

■

0.3 Caracterización de ∅ y $\{\bullet\}$

Las siguientes propiedades son obvias, pero a la vez muy importantes.

0.3.1. Observación (Propiedad universal del conjunto vacío). *Para todo conjunto X existe una aplicación única $\emptyset \to X$.*

$$\emptyset \dashrightarrow^{\exists!} X$$

0.3.2. Observación (Propiedad universal de un conjunto de un elemento). *Si $\{\bullet\}$ es un conjunto de un elemento, entonces para cualquier conjunto X existe una aplicación única $X \to \{\bullet\}$:*

$$X \dashrightarrow^{\exists!} \{\bullet\}$$

0.4 Diagramas conmutativos

En nuestro curso vamos a usar muy a menudo diagramas conmutativos. Son dibujos con algunos objetos X, Y, Z y flechas entre ellos como $X \to Y$, tales que las composiciones de las flechas a lo largo de diferentes caminos coinciden. Por ejemplo, si tenemos

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle g} \\ Z & \xrightarrow[k]{} & W \end{array}$$

la conmutatividad quiere decir que

$$g \circ f = k \circ h.$$

Si tenemos un triángulo

$$\begin{array}{ccc} & X & \\ {\scriptstyle f}\swarrow & & \searrow{\scriptstyle g} \\ Y & \xrightarrow[h]{} & Z \end{array}$$

su conmutatividad quiere decir que

$$h \circ f = g.$$

Otro ejemplo más interesante:

$$\begin{array}{ccccc} & & Z & & \\ & {\scriptstyle f}\swarrow & \downarrow{\scriptstyle k} & \searrow{\scriptstyle g} & \\ X & \xleftarrow[j]{} & W & \xrightarrow[i]{} & Y \end{array}$$

Aquí la conmutatividad significa que

$$j \circ k = f \quad \text{y} \quad i \circ k = g.$$

0.5 Caracterización de productos y coproductos

Recordemos que para dos conjuntos X y Y su **producto cartesiano** está dado por

$$X \times Y := \{(x, y) \mid x \in X,\ y \in Y\} \tag{0.5}$$

y está dotado de dos proyecciones

$$\begin{array}{ccccc} X & \xleftarrow{p_1} & X \times Y & \xrightarrow{p_2} & Y \\ x & \longleftarrow\!\shortmid & (x, y) & \longmapsto & y \end{array}$$

A partir de ahora, en lugar de "producto cartesiano", vamos a decir simplemente "producto". Por otro lado, la **unión disjunta** de X y Y está dada por

$$X \sqcup Y := X \times \{0\} \cup Y \times \{1\} \tag{0.6}$$

y está dotada de dos inclusiones

$$\begin{array}{ccccc} X & \xrightarrow{i_1} & X \sqcup Y & \xleftarrow{i_2} & Y \\ x & \longmapsto & (x, 0) & & \\ & & (y, 1) & \longleftarrow\!\shortmid & y \end{array}$$

Notemos que, en cierto sentido, las construcciones de $X \times Y$ e $X \sqcup Y$ no son canónicas. Por ejemplo, hay varias formas de modelar los pares ordenados (x, y), o también en lugar de (0.5) podemos usar otra definición como

$$\{(y, x) \mid x \in X,\ y \in Y\}.$$

Tampoco está claro por qué (0.5) tiene que ser *el* producto. De la misma manera, en lugar de (0.6) podemos considerar, por ejemplo,

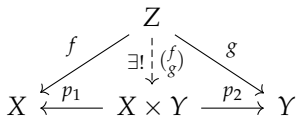
$$\{\text{☺}\} \times X \cup \{\text{☹}\} \times Y.$$

En el fondo, el aspecto más importante lo constituyen las *propiedades universales* que satisfacen $X \times Y$ e $X \sqcup Y$.

0.5.1. Observación (Propiedad universal del producto). *Sea Z un conjunto junto con dos aplicaciones $f\colon Z \to X$ y $g\colon Z \to Y$. Entonces, existe una aplicación única $\binom{f}{g}\colon Z \to X \times Y$ tal que*

$$p_1 \circ \binom{f}{g} = f, \quad p_2 \circ \binom{f}{g} = g.$$

(0.7)

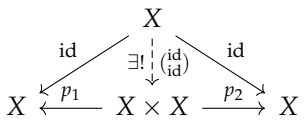


Demostración. Se ve que la única opción posible es

$$\begin{pmatrix} f \\ g \end{pmatrix} \colon Z \to X \times Y,$$
$$z \mapsto (f(z), g(z)).$$

■

0.5.2. Ejemplo. Consideremos el producto $X \times X$ y dos aplicaciones identidad $\mathrm{id}_X \colon X \to X$:



la aplicación

$$\Delta_X := \begin{pmatrix} \mathrm{id}_X \\ \mathrm{id}_X \end{pmatrix} \colon X \to X \times X$$

caracterizada por

$$p_1 \circ \Delta_X = p_2 \circ \Delta_X = \mathrm{id}_X$$

se llama la **aplicación diagonal**. En términos de los elementos del producto cartesiano $X \times X$ como lo hemos definido arriba, tenemos

$$\Delta_X \colon x \mapsto (x, x).$$

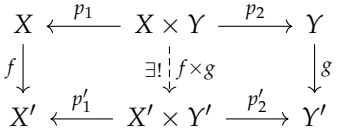
▲

0.5.3. Ejemplo. Para dos aplicaciones $f \colon X \to X'$ y $g \colon Y \to Y'$, tenemos una aplicación

$$f \times g \colon X \times Y \to X' \times Y'$$

caracterizada de modo único por

$$p_1' \circ (f \times g) = f \circ p_1, \quad p_2' \circ (f \times g) = g \circ p_2.$$



En términos de elementos,

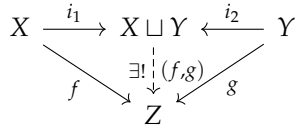
$$f \times g \colon (x, y) \mapsto (f(x), g(y)).$$

▲

0.5.4. Observación (Propiedad universal del coproducto). *Sea Z un conjunto junto con dos aplicaciones $f \colon X \to Z$ y $g \colon Y \to Z$. Entonces, existe una aplicación única $(f, g) \colon X \sqcup Y \to Z$ tal que*

$$(f, g) \circ i_1 = f, \quad (f, g) \circ i_2 = g.$$

(0.8)



Demostración. La aplicación tiene que ser dada por

$$\begin{aligned}(f,g)\colon X \sqcup Y = X \times \{0\} \cup Y \times \{1\} &\to Z,\\ (x,0) &\mapsto f(x),\\ (y,1) &\mapsto g(y).\end{aligned}$$

■

Note que el diagrama (0.8) es casi idéntico a (0.7), solo que las flechas van al revés. En este sentido, el producto y la unión disjunta de conjuntos son construcciones *duales*. Por esto a veces se dice que la unión disjunta es un **coproducto**.

0.6 Propiedades universales

Hemos dicho que 0.3.1, 0.3.2, 0.5.1 y 0.5.4 son **propiedades universales**, porque estas *definen* $\emptyset$, $\{\bullet\}$, $X \times Y$, $X \sqcup Y$ de modo único salvo biyección única. Por ejemplo, supongamos que hay un conjunto T tal que

$$\text{para todo } X \text{ existe una aplicación única } X \to T.$$

Sea T' otro conjunto que satisface la misma propiedad:

$$\text{para todo } X \text{ existe una aplicación única } X \to T'.$$

Entonces, deben existir aplicaciones *únicas*

$$T \xrightarrow{\exists! f} T' \quad \text{y} \quad T' \xrightarrow{\exists! g} T.$$

Podemos considerar sus composiciones

$$T \xrightarrow{f} T' \xrightarrow{g} T \qquad (g\circ f) \qquad\qquad T' \xrightarrow{g} T \xrightarrow{f} T' \qquad (f\circ g)$$

Pero según las propiedades que hemos supuesto, hay una sola aplicación $T \to T$, y esta debe ser la aplicación identidad id_T. De la misma manera, la única aplicación $T' \to T'$ es $\mathrm{id}_{T'}$. Entonces,

$$g \circ f = \mathrm{id}_T, \quad f \circ g = \mathrm{id}_{T'},$$

y las aplicaciones f y g nos dan una biyección entre T y T'. Por esto cuando escribimos $\{\bullet\}$, no nos interesa qué es exactamente $\bullet$; lo único que importa es que el conjunto $\{\bullet\}$ satisfaga 0.3.2, y esta propiedad define $\{\bullet\}$ salvo biyección única.

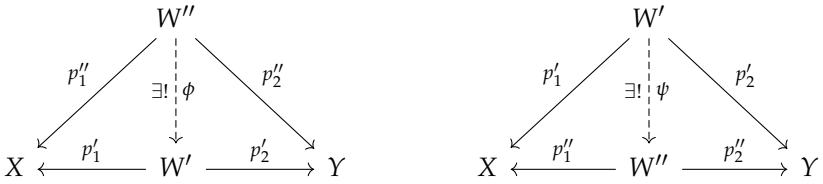
Para ver otro ejemplo más interesante de este tipo de razonamiento, consideremos el caso del producto $X \times Y$. Supongamos que hay dos conjuntos W' y W'' junto con algunas aplicaciones

$$X \xleftarrow{p_1'} W' \xrightarrow{p_2'} Y \qquad\qquad X \xleftarrow{p_1''} W'' \xrightarrow{p_2''} Y$$

y cada uno satisface la propiedad universal (0.7):

$$\begin{array}{ccccc} & & Z & & \\ & {\scriptstyle f}\swarrow & \exists!\downarrow{\scriptstyle (f\atop g)} & \searrow{\scriptstyle g} & \\ X & \xleftarrow{p_1'} & W' & \xrightarrow{p_2'} & Y \end{array} \qquad\qquad \begin{array}{ccccc} & & Z & & \\ & {\scriptstyle f}\swarrow & \exists!\downarrow{\scriptstyle (f\atop g)} & \searrow{\scriptstyle g} & \\ X & \xleftarrow{p_1''} & W'' & \xrightarrow{p_2''} & Y \end{array}$$

Aplicando estas dos propiedades se obtiene



es decir, existen aplicaciones *únicas*

$$\phi\colon W'' \to W' \quad \text{y} \quad \psi\colon W' \to W''$$

que satisfacen

$$p'_1 \circ \phi = p''_1, \quad p'_2 \circ \phi = p''_2, \quad p''_1 \circ \psi = p'_1, \quad p''_2 \circ \psi = p'_2.$$

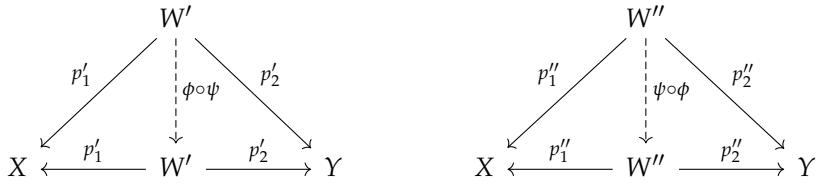
Podemos considerar sus composiciones

$$\phi \circ \psi\colon W' \to W', \quad \psi \circ \phi\colon W'' \to W''.$$

Estas satisfacen

$$\begin{aligned}
p'_1 \circ (\phi \circ \psi) &= (p'_1 \circ \phi) \circ \psi = p''_1 \circ \psi = p'_1,\\
p'_2 \circ (\phi \circ \psi) &= (p'_2 \circ \phi) \circ \psi = p''_2 \circ \psi = p'_2,\\
p''_1 \circ (\psi \circ \phi) &= (p''_1 \circ \psi) \circ \phi = p'_1 \circ \phi = p''_1,\\
p''_2 \circ (\psi \circ \phi) &= (p''_2 \circ \psi) \circ \phi = p'_2 \circ \phi = p''_2;
\end{aligned}$$

es decir, existen diagramas conmutativos



Pero las flechas verticales punteadas en los diagramas de arriba también deben ser únicas y por lo tanto coinciden con las aplicaciones identidad:

$$\phi \circ \psi = \mathrm{id}_{W'}, \quad \psi \circ \phi = \mathrm{id}_{W''}.$$

Entonces, hemos obtenido una biyección única

$$W' \cong W''.$$

Esto significa que no es importante cómo se define $X \times Y$; si hay otro conjunto W que satisface la misma propiedad universal 0.5.1, entre W y $X \times Y$ existe una biyección *canónica*.

Las consideraciones de arriba pueden parecer banales, o más bien una sobrecomplicación innecesaria de algo banal (¿quén no sabe que es el producto cartesiano de dos conjuntos?), pero estas ideas son fundamentales para las matemáticas modernas. Entre el final del siglo XIX y los inicios del siglo XX, una gran revolución sucedió cuando se descubrió que todos los objetos de interés pueden ser modelados en términos de conjuntos. A partir de los años 50 el punto de visto ha cambiado: los objetos suelen definirse en términos de propiedades universales y diagramas conmutativos.

0.7 Relaciones de equivalencia

Para terminar este capítulo, recordemos brevemente la noción de relación de equivalencia que será de mucha importancia en nuestro curso.

0.7.1. Definición. Sea X un conjunto. Una relación binaria $\sim$ sobre X es una **relación de equivalencia** si cumple los siguientes axiomas:

E1) **reflexividad**: para todo $x \in X$ se cumple $x \sim x$;

E2) **simetría**: para cualesquiera $x, y \in X$, si $x \sim y$, entonces $y \sim x$;

E3) **transitividad**: para cualesquiera $x, y, z \in X$, si $x \sim y$ e $y \sim z$, entonces $x \sim z$.

0.7.2. Ejemplo. Para algún número $n = 1, 2, 3, 4, \ldots$ consideremos la siguiente relación sobre los números enteros $\mathbb{Z}$: se dice que a y b son **congruentes módulo** n y se escribe $a \equiv b \pmod{n}$ si su diferencia es divisible por n:

$$n \mid (a - b) \iff (a - b) = n\,c \text{ para algún } c \in \mathbb{Z}.$$

Esta es una relación de equialencia. De hecho, para todo $a \in \mathbb{Z}$ tenemos $n \mid (a - a)$, ya que el cero es divisible por cualquier n (tenemos $0 = n \cdot 0$). Luego la relación es reflexiva.

Ahora si $a \equiv b \pmod{n}$, entonces $(a - b) = n\,c$ para algún c y luego $(b - a) = n\,(-c)$, así que $b \equiv a \pmod{n}$.

Por fin, si tenemos $a_1 \equiv a_2 \pmod{n}$ y $a_2 \equiv a_3 \pmod{n}$, esto significa que

$$(a_1 - a_2) = n\,c, \quad (a_2 - a_3) = n\,d,$$

y entonces

$$(a_1 - a_2) + (a_2 - a_3) = (a_1 - a_3) = n \cdot (c + d),$$

y $a_1 \equiv a_3 \pmod{n}$; la relación es transitiva. ▲

0.7.3. Definición. Sea X un conjunto dotado de una relación de equivalencia $\sim$. Para $x \in X$ su **clase de equivalencia** respecto a $\sim$ es el conjunto

$$[x] := \{y \in X \mid x \sim y\}.$$

En este caso también se dice que x **representa** la clase de equivalencia $[x]$. El conjunto de las clases de equivalencia se denota por

$$X/\!\sim := \{[x] \mid x \in X\}$$

y se dice que es el **conjunto cociente** de X bajo la relación de equivalencia $\sim$.

0.7.4. Observación. *Las clases de equivalencia son disjuntas. Específicamente, para cualesquiera $x, y \in X$ las siguientes condiciones son equivalentes:*

1) $x \sim y$,

2) $[x] = [y]$,

3) $[x] \cap [y] \neq \emptyset$.

Asimismo tenemos la descomposición

$$X = \bigcup_{[x] \in X/\!\sim} [x],$$

y diferentes conjuntos en la unión son disjuntos.

Demostración. Supongamos que $x \sim y$. Entonces para todo $z \in X$ tenemos (usando que la relación $\sim$ es simétrica y transitiva)

$$z \in [x] \iff x \sim z \Rightarrow y \sim z \iff z \in [y]$$

y de la misma manera

$$z \in [y] \iff y \sim z \Rightarrow x \sim z \iff z \in [x].$$

Esto demuestra que 1) implica 2).

Luego 2) obviamente implica 3), ya que $x \in [x]$, y por lo tanto $[x] \neq \emptyset$. Esto usa la hipótesis de que la relación $\sim$ sea reflexiva.

Por fin, 3) implica 1): si existe $z \in [x] \cap [y]$, entonces $x \sim z$ e $y \sim z$, y por la simetría y transitividad $x \sim y$. ■

0.7.5. Ejemplo. Las clases de equivalencia respecto a la relación de congruencia módulo n pueden ser representadas por diferentes restos módulo n. Vamos a usar la notación

$$[a]_n := \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}.$$

$$\begin{aligned}
[0]_n &= \{0, \pm n, \pm 2n, \pm 3n, \ldots\},\\
[1]_n &= \{1, 1 \pm n, 1 \pm 2n, 1 \pm 3n, \ldots\},\\
[2]_n &= \{2, 2 \pm n, 2 \pm 2n, 2 \pm 3n, \ldots\},\\
&\vdots\\
[n-1]_n &= \{(n-1), (n-1) \pm n, (n-1) \pm 2n, (n-1) \pm 3n, \ldots\}.
\end{aligned}$$

En este caso el conjunto $\mathbb{Z}/\sim$ se denota por

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

▲

Técnicamente hablando, $X/\sim$ es un conjunto de subconjuntos de X que son disjuntos y cubren todo X. Sin embargo, hay que pensar en $X/\sim$ como en el conjunto X donde hemos identificado los elementos equivalentes. De todos modos, lo más importante no es la construcción de $X/\sim$ sino su propiedad universal.

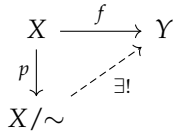
0.7.6. Observación (Propiedad universal del cociente $X/\sim$). *Para una relación de equivalencia $\sim$ sobre X, consideremos la aplicación canónica*

$$\begin{aligned}
p\colon X &\to X/\sim,\\
x &\mapsto [x].
\end{aligned}$$

Sea $f\colon X \to Y$ una aplicación tal que para cualesquiera $x, x' \in X$ se tiene

$$x \sim x' \Rightarrow f(x) = f(x').$$

Entonces, f se factoriza de modo único por p:



Demostración. La flecha punteada tiene que ser dada por $[x] \mapsto f(x)$. ■

0.7.7. Ejemplo. Consideremos la adición y multiplicación de números enteros módulo n: para dos números a y b calculemos su suma y producto habitual y luego tomemos el resto módulo n correspondiente:

$$\begin{aligned} +\colon \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}, \\ (a,b) &\mapsto [a+b]_n, \\ \cdot\colon \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}, \\ (a,b) &\mapsto [ab]_n. \end{aligned}$$

La relación de congruencia módulo n induce de modo obvio una relación de equivalencia sobre $\mathbb{Z} \times \mathbb{Z}$:

$$(a,b) \sim (a',b') \iff a \equiv a' \pmod{n}, \quad b \equiv b' \pmod{n},$$

y el cociente $(\mathbb{Z} \times \mathbb{Z})/\sim$ puede ser identificado con $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Notamos que

$$a \equiv a' \pmod{n}, \quad b \equiv b' \pmod{n} \Rightarrow a + b \equiv a' + b' \pmod{n}.$$

De hecho, si $a - a' = n\,c$ y $b - b' = n\,d$, entonces $(a+b) - (a'+b') = n\,(c+d)$. De la misma manera, tenemos

$$a \equiv a' \pmod{n}, \quad b \equiv b' \pmod{n} \Rightarrow ab \equiv a'b' \pmod{n}.$$

En efecto, si $n \mid (a - a')$ y $n \mid (b - b')$, entonces n divivde a

$$ab - a'b' = (a - a')\,b + a'\,(b - b').$$

Todo esto significa que la adición y multiplicación pueden ser definidas sobre los restos módulo n:

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{+} & \mathbb{Z}/n\mathbb{Z} \\ \downarrow & \nearrow_{\exists!} & \\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & & \end{array} \qquad \begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{\times} & \mathbb{Z}/n\mathbb{Z} \\ \downarrow & \nearrow_{\exists!} & \\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & & \end{array}$$

Las flechas punteadas están definidas por

$$\begin{aligned} [a]_n + [b]_n &= [a+b]_n, \\ [a]_n \cdot [b]_n &= [ab]_n. \end{aligned}$$

▲

Mucho más ejemplos interesantes van a surgir más adelante.

Capítulo 1
Permutaciones

Para motivar los axiomas de grupo, en este capítulo vamos a considerar solamente grupos de permutaciones, también conocidos como grupos simétricos.

1.0.1. Definición. Sea X un conjunto. Si $f\colon X \to X$ es una biyección, se dice también que f es una **permutación** de los elementos de X. El conjunto de todas las permutaciones de los elementos de X se denota por S_X.

1.0.2. Observación. *La composición de aplicaciones define una operación binaria sobre* S_X

$$\begin{aligned} S_X \times S_X &\to S_X, \\ (g, f) &\mapsto g \circ f \end{aligned}$$

que satisface las siguientes propiedades.

G1) La operación $\circ$ *es* ***asociativa****: para cualesquiera* $f, g, h \in S_X$ *tenemos*

$$(h \circ g) \circ f = h \circ (g \circ f).$$

G2) La aplicación identidad id_X *es el* ***elemento neutro*** *respecto a* $\circ$*, es decir*

$$\mathrm{id}_X \circ f = f = f \circ \mathrm{id}_X$$

para todo $f \in S_X$.

G3) Para toda permutación $f \in S_X$ *existe una permutación* ***inversa*** $f^{-1}\colon X \to X$ *que satisface*

$$f \circ f^{-1} = \mathrm{id}_X = f^{-1} \circ f.$$

Demostración. Hemos visto estos resultados en el capítulo anterior. La composición de dos permutaciones es también una permutación, y por lo tanto la operación $(g, f) \mapsto g \circ f$ está bien definida. La propiedad G1) significa nada más que la composición de aplicaciones es asociativa. Luego, la propiedad G2) es la composición con la aplicación identidad. Por fin, una aplicación $f\colon X \to X$ es biyectiva si y solamente si existe la aplicación inversa $f^{-1}\colon X \to X$, y esto nos da G3). ■

Las propiedades G1)–G3) significan que S_X es un **grupo**. Es una estructura algebraica que vamos a definir en el siguiente capítulo y estudiar durante todo el semestre.

1.0.3. Observación. *S_X satisface las siguientes propiedades:*

A1) $\mathrm{id}_X(x) = x$ *para todo* $x \in X$.

A2) $(g \circ f)(x) = g(f(x))$ *para todo* $x \in X$ *y* $f, g \in S_X$.

Demostración. A1) es nada más la definición de la aplicación identidad y A2) es la definición de la composición de aplicaciones. ■

Las propiedades A1) y A2) significan que S_X **actúa** sobre X. Las acciones de grupos sobre conjuntos serán de mucha importancia más adelante.

1.0.4. Definición. S_X junto con la operación binaria $\circ$ es el **grupo simétrico** sobre X.

Normalmente para el grupo simétrico el signo de composición $\circ$ no se escribe: "gf" significa "$g \circ f$". Lo vamos a omitir a partir he ahora. Será muy útil pensar en la composición be biyecciones como una especie de multiplicación *no conmutativa* (en general $fg \neq gf$).

1.1 El grupo simétrico S_n

Un caso particular de interés es cuando X es un conjunto finito de n elementos. Podemos suponer que $X = \{1, 2, \ldots, n\}$.

1.1.1. Notación. Para un número natural n, el grupo simétrico sobre $\{1, 2, \ldots, n\}$ se denota por

$$S_n := S_{\{1,2,\ldots,n\}}.$$

1.1.2. Ejemplo. El caso tonto es el de $n = 0$ que corresponde a... las permutaciones del conjunto vacío. Hay una aplicación única $\emptyset \to \emptyset$. Para $n = 1$ tenemos un conjunto de un elemento $\{1\}$ y una aplicación única $\mathrm{id}\colon \{1\} \to \{1\}$. El primer caso no trivial es de $n = 2$. El conjunto $\{1, 2\}$ tiene dos permutaciones: la permutación identidad

$$\mathrm{id}\colon 1 \mapsto 1,\ 2 \mapsto 2$$

y la permutación que intercambia 1 y 2:

$$\sigma\colon 1 \mapsto 2,\ 2 \mapsto 1.$$

Las composiciones de estas permutaciones son

$$\mathrm{id}\,\mathrm{id} = \mathrm{id}, \quad \sigma\,\mathrm{id} = \mathrm{id}\,\sigma = \sigma, \quad \sigma\sigma = \mathrm{id}.$$

▲

1.1.3. Notación. Una permutación $\sigma \in S_n$ puede representarse mediante una tabla donde en la primera fila están los números $i = 1, 2, \ldots, n$ y en la segunda fila están sus imágenes correspondientes $\sigma(i) \in \{1, 2, \ldots, n\}$:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Notamos que el hecho de que σ sea una biyección $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ significa precisamente que los números $\sigma(1), \sigma(2), \ldots, \sigma(n)$ no se repiten.

1.1.4. Ejemplo. Los elementos de S_2 pueden ser representados por las tablas

$$\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

El grupo simétrico S_3 consiste en 6 elementos dados por

$$\text{id} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}. \tag{1.1}$$

Notemos que en general, dos permutaciones $\sigma, \tau \in S_n$ no conmutan; es decir,

$$\sigma\tau \neq \tau\sigma.$$

En el caso de S_3 tenemos

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \cdot \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \tag{1.2}$$

mientras que

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \cdot \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}. \tag{1.3}$$

▲

1.1.5. Observación. *Tenemos*

$$|S_n| = n!$$

Demostración. La base de inducción es $|S_0| = |S_1| = 1$. Luego, supongamos que $|S_{n-1}| = (n-1)!$. Cada elemento $\sigma \in S_{n-1}$ corresponde a una lista sin repeticiones de los números entre 1 y $n-1$:

$$\sigma(1), \sigma(2), \ldots, \sigma(n-1).$$

Todos los elementos de S_n se obtienen poniendo el número n en una posición, y hay precisamente n posibilidades. Entonces,

$$|S_n| = n \cdot |S_{n-1}| = n \cdot (n-1)! = n!$$

■

1.2 Permutaciones cíclicas

1.2.1. Definición. Para $1 \leq k \leq n$ sean $i_1, i_2, i_3, \ldots, i_k$ algunos números distintos entre 1 y n. Definamos una permutación σ por

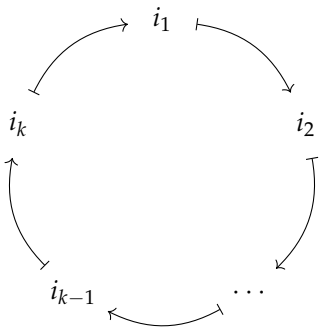
$$\begin{aligned}\sigma(i_1) &:= i_2,\\ \sigma(i_2) &:= i_3,\\ &\vdots,\\ \sigma(i_{k-1}) &:= i_k,\\ \sigma(i_k) &:= i_1\end{aligned}$$

y

$$\sigma(j) = j \quad \text{para } j \notin \{i_1, i_2, i_3, \ldots, i_k\}.$$

Entonces, se dice que σ es una **permutación cíclica de orden** k o un k**-ciclo** y se escribe

$$\sigma = (i_1\ i_2\ \cdots i_{k-1}\ i_k).$$



Note que el orden k es el mínimo número tal que

$$\underbrace{\sigma \cdots \sigma}_{k} = \mathrm{id}.$$

La permutación identidad id se considera como la permutación cíclica de orden 1, ya que esta corresponde a (i) para cualquier $i \in \{1, \ldots, n\}$.

1.2.2. Definición. Los 2-ciclos $\sigma = (i\ j)$ reciben el nombre especial de **transposiciones**.

Note que la transposición $(i\ j)$ intercambia i con j y deja otros elementos intactos.

En un ciclo, los índices en los paréntesis pueden ser *permutados cíclicamente* y el resultado no cambia:

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

Por esto normalmente se escoge la presentación $(i_1\ i_2\ \cdots i_{k-1}\ i_k)$ donde i_1 es el número mínimo (en el ejemplo de arriba es $(1\ 2\ 3)$).

1.2.3. Ejemplo. El grupo simétrico S_3 consiste en permutaciones cíclicas; sus elementos, enumerados en (1.1), también pueden ser escritos como

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

Compilemos la tabla de composición de permutaciones en S_3 en términos de ciclos. Escribamos una tabla de 6×6 indexada por los elementos de S_3 donde en la intersección de la fila σ y la columna τ está $\sigma\tau$:

$\circ$	$\cdots$	τ	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
σ	$\cdots$	$\sigma\tau$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$

Por ejemplo, las fórmulas (1.2) y (1.3) pueden ser escritas como

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

Haciendo cálculos similares, se obtiene

$\circ$	id	(1 2)	(2 3)	(1 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(2 3)	(1 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 2 3)	(1 3 2)	(2 3)	(1 3)
(2 3)	(2 3)	(1 3 2)	id	(1 2 3)	(1 3)	(1 2)
(1 3)	(1 3)	(1 2 3)	(1 3 2)	id	(1 2)	(2 3)
(1 2 3)	(1 2 3)	(1 3)	(1 2)	(2 3)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 3)	(1 2)	id	(1 2 3)

Note que los elementos no se repiten en ninguna columna o fila. No es una coincidencia: en general,

$$\sigma\tau = \sigma\tau' \Rightarrow \tau = \tau'$$

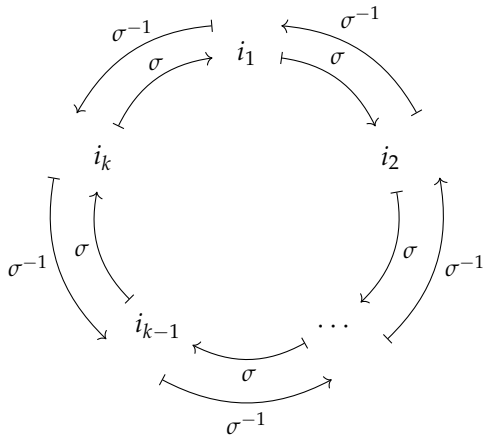
y

$$\sigma\tau = \sigma'\tau \Rightarrow \sigma = \sigma',$$

ya que toda biyección es cancelable por la izquierda y por la derecha. ▲

1.2.4. Observación. *La permutación inversa a un k-ciclo es también un k-ciclo, dado por*

$$(i_1\ i_2\ \cdots\ i_k)^{-1} = (i_k\ i_{k-1}\ \cdots\ i_1) = (i_1\ i_k\ i_{k-1}\ \cdots\ i_2).$$



1.2.5. Definición. Se dice que dos ciclos $\sigma = (i_1\ i_2\ \cdots\ i_k)$ y $\tau = (j_1\ j_2\ \cdots\ j_\ell)$ en S_n son **disjuntos** si $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_\ell\} = \emptyset$.

1.2.6. Observación. *Dos ciclos disjuntos cualesquiera conmutan entre sí:*

$$\sigma\tau = \tau\sigma.$$

Demostración. En general, si una permutación σ afecta los números $\{i_1, i_2, \ldots, i_k\}$ (es decir, $\sigma(i) = i$ para $i \notin \{i_1, i_2, \ldots, i_k\}$) y τ afecta $\{j_1, j_2, \ldots, j_\ell\}$, está claro que $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_\ell\} = \emptyset$ implica que $\sigma\tau = \tau\sigma$. ■

No todas las permutaciones son cíclicas. Por ejemplo, la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$$

es una composición de dos ciclos disjuntos:

$$\sigma = (1\ 2)\,(3\ 4) = (3\ 4)\,(1\ 2).$$

Sin embargo, tenemos el siguiente resultado.

1.2.7. Proposición. *Toda permutación $\sigma \in S_n$ puede ser escrita como una composición de ciclos disjuntos.*

Demostración. Consideremos la lista máxima

$$i_1 := 1,\ i_2 := \sigma(1),\ i_3 := \sigma(i_2),\ i_4 := \sigma(i_3),\ \ldots,\ i_k := \sigma(i_{k-1})$$

tal que $i_1, i_2, \ldots, i_k$ son números distintos; es decir, terminemos la lista cuando

$$\sigma(i_k) = i_\ell \quad \text{para algún } 1 \leq \ell \leq k.$$

Ahora si $\ell \neq 1$, tenemos

$$\sigma(i_k) = \sigma(i_{\ell-1}),$$

pero $i_k \neq i_{\ell-1}$ y esto contradice la inyectividad de σ. Entonces, $\ell = 1$, y hemos obtenido un ciclo. (Si $\sigma(1) = 1$, acabamos de encontrar un ciclo de orden 1, pero es conveniente considerarlo como un ciclo legítimo para simplificar el algoritmo.)

Luego podemos considerar el número mínimo j_1 tal que $j_1 \notin \{i_1, \ldots, i_k\}$. De la misma manera, vamos a obtener otro ciclo que empieza por j_1 y que es disjunto con el ciclo $(i_1\ i_2\ \cdots\ i_k)$.

Repitiendo este proceso, encontramos que todos los elementos pertenecen a algún ciclo, y estos ciclos son disjuntos. ■

1.2.8. Ejemplo. Consideremos la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 7 & 1 & 3 & 8 & 6 & 5 & 2 & 10 & 9 \end{pmatrix}$$

Empezando por 1, tenemos una sucesión

$$1 \mapsto 4 \mapsto 3 \mapsto 1$$

Esto nos da un ciclo $(1\ 4\ 3)$. Nos quedan los números $2, 5, 6, 7, 8, 9, 10$. Empezando por 2, se obtiene

$$2 \mapsto 7 \mapsto 5 \mapsto 8 \mapsto 2$$

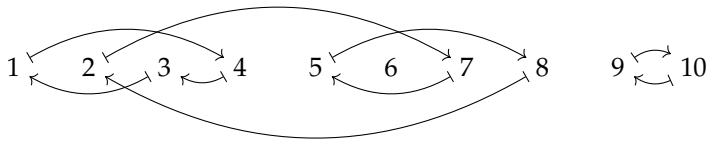
y otro ciclo es $(2\ 7\ 5\ 8)$. Luego, 6 es un punto fijo: tenemos $\sigma(6) = 6$ y un ciclo (6). Nos quedan 9 y 10:

$$9 \mapsto 10 \mapsto 9$$

lo que nos da una transposición $(9\ 10)$. Entonces, la descomposición en ciclos disjuntos es dada por

$$\sigma = (1\ 4\ 3)\,(2\ 7\ 5\ 8)\,(9\ 10)$$

(el ciclo (6) no cambia nada y se omite, como todos los ciclos de orden 1).



▲

1.2.9. Definición. Para $\sigma \in S_n$, consideremos su descomposición en ciclos disjuntos. La sucesión de órdenes de estos ciclos se llama el **tipo de ciclo** de σ.

Todos los tipos de ciclo posibles en S_n corresponden a las particiones de n en una suma de números positivos. Por ejemplo, para $n = 4$ tenemos las siguientes opciones.

$$\begin{aligned} 1+1+1+1 &\leftrightarrow (\bullet)\,(\bullet)\,(\bullet)\,(\bullet) = \mathrm{id} \\ 1+1+2 &\leftrightarrow (\bullet)\,(\bullet)\,(\bullet\ \bullet) = (\bullet\ \bullet) \\ 2+2 &\leftrightarrow (\bullet\ \bullet)\,(\bullet\ \bullet) \\ 1+3 &\leftrightarrow (\bullet)\,(\bullet\ \bullet\ \bullet) = (\bullet\ \bullet\ \bullet) \\ 4 &\leftrightarrow (\bullet\ \bullet\ \bullet\ \bullet) \end{aligned}$$

El número de particiones de n se denota por $p(n)$ y se llama la **función de particiones**. La tabla de abajo presenta algunos valores de $p(n)$. Sus propiedades se estudian extensivamente en combinatoria y teoría de números.

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$p(n)$:	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176

1.2.10. Ejemplo. Con un poco de cuidado para no olvidar ninguna permutación y no escribirla dos veces, encontramos la lista completa de las permutaciones en S_4:

$$\begin{gathered} \mathrm{id}, \\ (1\,2),\quad (1\,3),\quad (1\,4),\quad (2\,3),\quad (2\,4),\quad (3\,4), \\ (1\,2\,3),\quad (1\,2\,4),\quad (1\,3\,2),\quad (1\,3\,4),\quad (1\,4\,2),\quad (1\,4\,3),\quad (2\,3\,4),\quad (2\,4\,3), \\ (1\,2)\,(3\,4),\quad (1\,3)\,(2\,4),\quad (1\,4)\,(2\,3), \\ (1\,2\,3\,4),\quad (1\,2\,4\,3),\quad (1\,3\,2\,4),\quad (1\,3\,4\,2),\quad (1\,4\,2\,3),\quad (1\,4\,3\,2). \end{gathered}$$

Para comprobar, calculemos el número de elementos:

$$1 + 6 + 8 + 3 + 6 = 24 = 4!$$

▲

1.2.11. Proposición. *En S_n hay*

$$\frac{n!}{\prod_\ell M_\ell! \cdot \ell^{M_\ell}}$$

permutaciones con la descomposición en ciclos disjuntos de la forma

$$\sigma = \underbrace{(\bullet)\cdots(\bullet)}_{M_1 \text{ puntos fijos}}\ \underbrace{(\bullet\ \bullet)\cdots(\bullet\ \bullet)}_{M_2 \text{ transposiciones}}\ \underbrace{(\bullet\ \bullet\ \bullet)\cdots(\bullet\ \bullet\ \bullet)}_{M_3 \text{ ciclos de orden } 3}\cdots \tag{1.4}$$

(aquí $M_1 + M_2 \cdot 2 + M_3 \cdot 3 + \cdots = n$).

Demostración. Hay $n!$ posibilidades de colocar los números $\{1, \ldots, n\}$ en lugar de $\bullet$ en (1.4). En cada serie de M_ℓ ciclos de longitud ℓ, podemos escribir los ciclos en otro orden, y el resultado no cambia, así que hay que dividir $n!$ por $\prod_\ell M_\ell!$. También para cada ciclo de longitud ℓ, hay ℓ modos equivalentes de escribirlo permutando los índices cíclicamente. Por esto hay que dividir todo por $\prod_\ell \ell^{M_\ell}$. ■

1.2.12. Ejemplo. Si nos interesan los k-ciclos en S_n (donde $1 \le k \le n$), tenemos

$$M_1 = (n-k), \quad M_2 = \cdots = M_{k-1} = 0, \quad M_k = 1, \quad M_{k+1} = M_{k+2} = \cdots = 0$$

y la fórmula nos da

$$\frac{n!}{(n-k)! \cdot k}.$$

En particular, hay

$$\frac{n\,(n-1)}{2} = \binom{n}{2}$$

transposiciones. ▲

1.2.13. Ejemplo. En S_5 tenemos

- la permutación identidad id,
- $10 = \frac{5!}{3! \cdot 2}$ transposiciones $(\bullet\ \bullet)$,
- $20 = \frac{5!}{2! \cdot 3}$ ciclos $(\bullet\ \bullet\ \bullet)$,
- $30 = \frac{5!}{4}$ ciclos $(\bullet\ \bullet\ \bullet\ \bullet)$,
- $24 = \frac{5!}{5}$ ciclos $(\bullet\ \bullet\ \bullet\ \bullet\ \bullet)$,
- $15 = \frac{5!}{2! \cdot 2^2}$ permutaciones $(\bullet\ \bullet)\,(\bullet\ \bullet)$,
- $20 = \frac{5!}{2 \cdot 3}$ permutaciones $(\bullet\ \bullet)\,(\bullet\ \bullet\ \bullet)$.

▲

1.2.14. Definición. Para $\sigma, \tau \in S_n$ la permutación $\tau\sigma\tau^{-1} \in S_n$ se llama la **conjugación de σ por τ**.

1.2.15. Observación. *Para dos permutaciones $\sigma, \tau \in S_n$, si*

$$\sigma\colon i \mapsto j,$$

entonces

$$\tau\sigma\tau^{-1}\colon \tau(i) \mapsto \tau(j).$$

Demostración.

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

■

1.2.16. Corolario. *Si*

$$\sigma = (i_1\ i_2\ \cdots\ i_k)$$

es un k-ciclo, entonces para toda permutación $\tau \in S_n$, la conjugación de σ por τ es también un k-ciclo dado por

$$\tau\,(i_1\ i_2\ \cdots\ i_k)\,\tau^{-1} = (\tau(i_1)\ \tau(i_2)\ \cdots\ \tau(i_k)).$$

En general, la conjugación no cambia el tipo de ciclo de una permutación. Dos permutaciones $\sigma, \sigma' \in S_n$ son conjugadas ($\sigma' = \tau\sigma\tau^{-1}$ para alguna permutación $\tau \in S_n$) si y solamente si tienen el mismo tipo de ciclo.

Demostración. Todo esto está claro de la observación precedente: la conjugación nada más cambia la numeración de nuestros elementos $\{1, 2, \ldots, n\}$. Para una permutación

$$\sigma = (\bullet\ \bullet\ \cdots\ \bullet)\,(\bullet\ \bullet\ \cdots\ \bullet)\cdots(\bullet\ \bullet\ \cdots\ \bullet)$$

la conjugación por τ nos da

$$\tau\sigma\tau^{-1} = \tau\,(\bullet\ \bullet\ \cdots\ \bullet)\,\tau^{-1}\,\tau\,(\bullet\ \bullet\ \cdots\ \bullet)\,\tau^{-1}\cdots\tau\,(\bullet\ \bullet\ \cdots\ \bullet)\,\tau^{-1},$$

y aquí para cada k-ciclo $(\bullet\ \bullet\ \cdots\ \bullet)$ en la descomposición su conjugado $\tau\,(\bullet\ \bullet\ \cdots\ \bullet)\,\tau^{-1}$ es también un k-ciclo. Si al principio los ciclos son disjuntos, los conjugados son también disjuntos, puesto que τ es una biyección.

Ahora si σ y σ' son dos permutaciones que tienen el mismo tipo de ciclo, esto significa que son idénticas salvo renumeración de los elementos $\{1, 2, \ldots, n\}$. Esta renumeración se realiza por cierta permutación $\tau \in S_n$ y $\sigma' = \tau\sigma\tau^{-1}$. ■

1.3 Signo y el grupo alternante A_n

1.3.1. Definición. Para una permutación $\sigma \in S_n$ cuando para algunos $i < j$ se tiene $\sigma(i) > \sigma(j)$, se dice que hay una **inversión**. El número

$$\operatorname{sgn}\sigma := (-1)^{\#\text{de inversiones}}$$

se llama el **signo** de σ. Se dice que σ es **par** si $\operatorname{sgn}\sigma = +1$ e **impar** si $\operatorname{sgn}\sigma = -1$.

1.3.2. Ejemplo. Para S_3 tenemos

permutación	inversiones	signo	
$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	no hay	$+1$	(par)
$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$2>1$	-1	(impar)
$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$3>2$	-1	(impar)
$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$3>2, 3>1, 2>1$	-1	(impar)
$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$2>1, 3>1$	$+1$	(par)
$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$3>1, 3>2$	$+1$	(par)

▲

1.3.3. Digresión. El signo de permutación aparece en la famosa fórmula para el determinante de una matriz $A = (x_{ij})_{1\le i,j\le n}$:

$$\det A = \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot x_{1,\sigma(1)}\, x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}. \tag{1.5}$$

Por ejemplo, en S_2 tenemos dos permutaciones: la permutación identidad de signo $+1$ y la transposición $(1\ 2)$ de signo -1. Esto nos da

$$\det \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = x_{11}\, x_{22} - x_{12}\, x_{21}.$$

Sin embargo, la expresión (1.5) es horrible y no explica el significado geométrico del determinante, ni sirve para hacer cálculos prácticos (¡la suma es sobre $n!$ términos!).

1.3.4. Observación. *Todo k-ciclo es una composición de $k-1$ transposiciones:*

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2)\,(i_2\ i_3)\,(i_3\ i_4)\cdots(i_{k-1}\ i_k).$$

1.3.5. Corolario. *Toda permutación $\sigma \in S_n$ es una composición de transposiciones (no necesariamente disjuntas).*

Demostración. Sigue de la descomposición de permutaciones en ciclos disjuntos (1.2.7) y luego descomposición de cada ciclo en transposiciones (1.3.4). ■

El último resultado es muy natural: intuitivamente debe de ser claro que para permutar n elementos de cualquier modo, es suficiente hacer una sucesión de intercambios por pares. De hecho, se puede hacer una sucesión de intercambios de elementos adyacentes.

1.3.6. Observación. *Toda transposición $(a\ b)$ con $b-a = k$ puede ser escrita como una composición de $2k-1$ transposiciones de la forma $(i\ i+1)$.*

1.3.7. Ejemplo. Tenemos

$$(1\ 4) = (1\ 2)\,(2\ 3)\,(3\ 4)\,(2\ 3)\,(1\ 2).$$

$1 \hookleftarrow$	2	3	4
2	$1 \hookleftarrow$	3	4
2	3	$1 \hookleftarrow$	4
2	$3 \hookleftarrow$	4	1
$2 \hookleftarrow$	4	3	1
4	2	3	1

▲

Demostración de 1.3.6. La idea debe de ser clara a partir del ejemplo de arriba. Para formalizar la demostración, usamos la inducción sobre k. La base de inducción es el caso de $k = 1$ y el paso inductivo resulta de la fórmula

$$(a\ b) = (a\ a+1)\,(a+1\ b)\,(a\ a+1).$$

■

El mismo argumento formulado en otras palabras: a partir de $(b-1\ b)$ se puede hacer una sucesión de $k-1$ conjugaciones

$$\begin{aligned}(b-2\ b-1)\,(b-1\ b)\,(b-2\ b-1) &= (b-2\ b),\\ (b-3\ b-2)\,(b-2\ b)\,(b-3\ b-2) &= (b-3\ b),\\ (b-4\ b-3)\,(b-3\ b)\,(b-4\ b-3) &= (b-4\ b),\\ &\dots\end{aligned}$$

hasta que se obtenga $(a\ b)$.

1.3.8. Corolario. *Todo elemento de S_n puede ser expresado como un producto de transposiciones*

$$(1\ 2),\ (2\ 3),\ (3\ 4),\ \dots,\ (n-1\ n).$$

Demostración. Sigue de 1.3.5 y 1.3.6. ■

1.3.9. Observación. *Transposiciones cambian la paridad: si τ es una transposición y $\sigma \in S_n$ es cualquier permutación, entonces*

$$\operatorname{sgn}(\tau\sigma) = -\operatorname{sgn}\sigma.$$

Demostración. Está claro que cuando σ es de la forma $(i\ i+1)$, el signo cambia al opuesto. Luego, hemos visto en 1.3.6 que toda transposición $(a\ b)$ es una composición de $2k-1$ transposiciones de esta forma, donde $k = b-a$. El número $2k-1$ es impar. ■

Como hemos visto en el ejemplo 1.3.2, en S_3 hay 3 pares y 3 impares permutaciones. Esto no es una coincidencia.

1.3.10. Corolario. *Para $n \geq 2$ el número de permutaciones pares en S_n es igual al número de permutaciones impares.*

Demostración. Consideremos la aplicación

$$\begin{aligned}\phi\colon S_n &\to S_n,\\ \sigma &\mapsto (1\ 2)\,\sigma.\end{aligned}$$

Es una biyección (de hecho $\phi\circ\phi = \mathrm{id}$) que según 1.3.9 aplica toda permutación par a una permutación impar y viceversa. ■

1.3.11. Corolario. *La paridad de una permutación σ es precisamente la paridad de la longitud de alguna descomposición en transposiciones: si*

$$\sigma = \tau_k \cdots \tau_1,$$

para algunas transposiciones τ_i, entonces

$$\operatorname{sgn}\sigma = (-1)^k.$$

1.3.12. Corolario. *Para dos diferentes descomposiciones en transposiciones*

$$\sigma = \tau_k \cdots \tau_1 = \tau'_\ell \cdots \tau'_1$$

los números k y ℓ necesariamente tienen la misma paridad: $k \equiv \ell \pmod 2$.

1.3.13. Digresión. A veces 1.3.11 se toma por la *definición* del signo, pero luego hay que demostrar que esta fórmula tiene sentido; es decir deducir 1.3.12 sin usar el signo. He aquí una breve explicación en términos del tipo de ciclo de σ, que es evidentemente un invariante de σ, a diferencia de la longitud de una descomposición en transposiciones. Para toda transposición $\tau = (i\ j)$ hay dos posibilidades.

1) i y j pertenecen al mismo ciclo. En este caso en $\tau\sigma$ este ciclo se descompone en dos.

2) i y j pertenecen a diferentes ciclos (posiblemente de orden 1). Entonces se ve que en $\tau\sigma$ estos dos ciclos se unen en uno.

En ambos casos el número de ciclos disjuntos cambia su paridad para $\tau\sigma$. Ahora si tenemos

$$\sigma = \tau_k \cdots \tau_1 = \tau'_\ell \cdots \tau'_1,$$

entonces se ve que los números k y ℓ deben tener la misma paridad.

1.3.14. Observación. *Para dos permutaciones $\sigma, \tau \in S_n$ se tiene*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau.$$

Demostración. Está claro de la interpretación del signo en 1.3.11. ■

1.3.15. Corolario. *Tenemos*

$$\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}\sigma.$$

Demostración.

$$\operatorname{sgn}\sigma \cdot \operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma\sigma^{-1}) = \operatorname{sgn}(\mathrm{id}) = +1.$$

■

1.3.16. Definición. Al conjunto de las permutaciones pares en S_n lo llamamos **grupo alternante** y lo denotamos por A_n:

$$A_n := \{\sigma \in S_n \mid \operatorname{sgn}\sigma = +1\} \subset S_n.$$

Tenemos las siguientes propiedades:

- $\mathrm{id} \in A_n$ (puesto que $\operatorname{sgn}(\mathrm{id}) = +1$),
- si $\sigma, \tau \in A_n$, entonces $\sigma\tau \in A_n$ (véase 1.3.14),
- si $\sigma \in A_n$, entonces $\sigma^{-1} \in A_n$ (véase 1.3.15).
- conjugando las permutaciones de A_n por las permutaciones de S_n, se obtienen también permutaciones de A_n: para todo $\sigma \in A_n$ y $\tau \in S_n$ tenemos $\tau\sigma\tau^{-1} \in A_n$.

  (De hecho, $\operatorname{sgn}(\tau\sigma\tau^{-1}) = \operatorname{sgn}\tau \cdot \operatorname{sgn}\sigma \cdot \operatorname{sgn}(\tau^{-1}) = \operatorname{sgn}\sigma$.)

Además, hemos calculado en 1.3.10 que

$$|A_n| = |S_n|/2 = n!/2.$$

1.3.17. Ejemplo.

$$A_2 = \{\mathrm{id}\},$$
$$A_3 = \{\mathrm{id},\ (1\,2\,3),\ (1\,3\,2)\}.$$

En S_4 las permutaciones son de la forma

$$\mathrm{id}, \quad (\bullet\,\bullet), \quad (\bullet\,\bullet\,\bullet), \quad (\bullet\,\bullet)\,(\bullet\,\bullet), \quad (\bullet\,\bullet\,\bullet\,\bullet).$$

Luego, todas las transpocisiones son impares. Los 3-ciclos son pares, ya que son productos de dos transposiciones:

$$(i\ j\ k) = (i\ j)\,(j\ k).$$

Los 4-ciclos con impares, siendo productos de 3 transposiciones:

$$(i\ j\ k\ \ell) = (i\ j)\,(j\ k)\,(k\ \ell).$$

Entonces, los elementos de A_4 son

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

De hecho, en la lista de arriba tenemos $1 + 8 + 3 = 12 = 4!/2$ permutaciones. ▲

1.4 Ejercicios

Ejercicio 1.1. *Encuentre la descomposición en ciclos disjuntos para la permutación*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 6 & 5 & 1 & 4 & 2 & 3 & 10 & 8 & 9 \end{pmatrix} \in S_{10}$$

y su signo.

Ejercicio 1.2. *Calcule la descomposición en ciclos disjuntos del producto de ciclos*

$$(1\ 2)\,(2\ 5\ 3)\,(1\ 5\ 7\ 3\ 2\ 6\ 4)\,(4\ 7\ 6) \in S_7$$

y su signo.

Ejercicio 1.3. *Demuestre la fórmula para el signo de un k-ciclo:*

$$\operatorname{sgn}(i_1\ i_2\ \cdots\ i_k) = (-1)^{k-1}.$$

En general, si $\sigma \in S_n$ afecta m elementos (en el sentido de que $\sigma(i) \neq i$ para m números i) y tiene una descomposición en s ciclos disjuntos, entonces

$$\operatorname{sgn}\sigma = (-1)^{m-s}.$$

Por ejemplo,

$$\sigma = (1\ 2)\,(3\ 6\ 4)\,(5\ 11\ 8)$$

afecta $1, 2, 3, 4, 5, 6, 8, 11$, entonces $m = 8$, y en la expresión de arriba hay $s = 3$ ciclos disjuntos. Entonces, $\operatorname{sgn}\sigma = (-1)^{8-3} = -1$.

Ojo: según nuestra terminología, el último ejercicio nos dice que una permutación cíclica de orden par k es impar (tiene signo -1) y viceversa.

Para realizar cualquier permutación, se puede fijar algún elemento y cada vez hacer intercambios solo con este.

Ejercicio 1.4. *Fijemos algún elemento de $\{1, \ldots, n\}$, por ejemplo 1. Demuestre que toda transposición $(i\ j)$ puede ser escrita como una composición de transposiciones de la forma $(1\ k)$. Deduzca que toda permutación $\sigma \in S_n$ para $n \geq 2$ es un producto de transposiciones*

$$(1\ 2),\ (1\ 3),\ \ldots,\ (1\ n).$$

De hecho, para expresar cualquier permutación, es suficiente usar una sola transposición, un n-ciclo y su inverso.

Ejercicio 1.5. *Demuestre que todo elemento de S_n puede ser expresado como un producto de*

$$(1\ 2),\ (1\ 2\ \cdots\ n),\ (1\ 2\ \cdots\ n)^{-1}.$$

Indicación: use que los elementos de S_n se expresan como productos de transposiciones de la forma $(i\ i+1)$ y la fórmula $\sigma\,(i_1\ i_2\ \cdots\ i_k)\,\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$.

En los siguientes ejercicios vamos a demostrar un resultado similar para los grupos alternantes.

Ejercicio 1.6. *Sean i, j, k, ℓ números distintos. Verifique las relaciones para la composición de transposiciones*

$$(i\ j)\,(j\ k) = (i\ j\ k),$$
$$(i\ j)\,(k\ \ell) = (i\ j\ k)\,(j\ k\ \ell).$$

Deduzca que para $n \geq 3$ todo elemento de A_n es una composición de ciclos de orden 3.

Ejercicio 1.7. *Demuestre que para $n \geq 3$ todo elemento de A_n es una composición de ciclos de la forma $(1\ i\ j)$.*
Indicación: use el ejercicio 1.6.

Ejercicio 1.8. *Demuestre que para $n \geq 3$ todo elemento de A_n es una composición de ciclos de la forma $(1\ 2\ i)$.*
Indicación: use el ejercicio 1.7.

Ejercicio 1.9. *Demuestre que para $n \geq 3$ todo elemento de A_n es una composición de ciclos de la forma $(i\ i+1\ i+2)$.*
Indicación: note que es un análogo de la descomposición de los elementos de S_n mediante las transposiciones de la forma $(i\ i+1)$. Para $i > 3$ demuestre la identidad

$$(1\ 2\ i) = (1\ 2\ i-2)\,(1\ 2\ i-1)\,(i-2\ i-1\ i)\,(1\ 2\ i-2)\,(1\ 2\ i-1)$$

Luego, proceda por inducción sobre i y use el ejercicio 1.8.

Ejercicio 1.10. *Demuestre que para $n \geq 3$ todo elemento de A_n puede ser escrito como el producto de*

- $(1\ 2\ 3)$, $(2\ 3\ \cdots\ n)$, $(2\ 3\ \cdots\ n)^{-1}$, *si n es par;*
- $(1\ 2\ 3)$, $(1\ 2\ \cdots\ n)$, $(1\ 2\ \cdots\ n)^{-1}$, *si n es impar.*

Indicación: use la fórmula $\sigma\,(i_1\ i_2\ \cdots\ i_k)\,\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$ y el ejercicio 1.9.

La moraleja de los ejercicios de arriba: aunque S_n y A_n tienen muchos elementos, estos se expresan en términos de solamente dos de ellos (y sus inversos).

Capítulo 2
Grupos

Después de estudiar el grupo simétrico S_n y el grupo alternante A_n, podemos definir qué es un grupo en general.

2.1 Definición de grupos abstractos

2.1.1. Definición. Un **grupo** es un conjunto G junto con una operación binaria

$$\begin{aligned} G \times G &\to G, \\ (g, h) &\mapsto g * h \end{aligned}$$

que satisface las siguientes propiedades.

G1) La operación $*$ es **asociativa**: para cualesquiera $g, h, k \in G$ tenemos

$$(g * h) * k = g * (h * k).$$

G2) Existe un **elemento neutro** $e \in G$ tal que

$$e * g = g = g * e$$

para todo $g \in G$.

G3) Para todo elemento $g \in G$ existe su **inverso** $g' \in G$ tal que

$$g * g' = e = g' * g.$$

2.1.2. Definición. Si G es un conjunto finito, el número $|G|$ se llama el **orden** de G.

2.1.3. Definición. Además, si la operación $*$ en G es **conmutativa**, es decir

$$g * h = h * g$$

para cualesquiera $g, h \in G$, entonces se dice que G es un grupo **abeliano**[*] o **conmutativo**.

[*] Niels Henrik Abel (1802–1829), matemático noruego, conocido por sus contribuciones en análisis (estudio de las series y de las integrales elípticas) y álgebra. Usando la teoría de grupos demostró su célebre teorema que dice que las ecuaciones polinomiales generales de grado ≥ 5 no pueden resolverse por radicales. Murió de tuberculosis a los 26 años. El lector puede buscar en internet más información sobre su trágica biografía para enterarse de cómo era la vida de los matemáticos del siglo XIX.

2.1.4. Ejemplo. Un conjunto de un elemento $\{e\}$ puede ser dotado de manera única de estructura de un grupo. Este se llama el **grupo trivial**. Es abeliano :-) Por abuso de notación este también se denota por e. ▲

2.1.5. Ejemplo. Hemos visto en el capítulo 1 que el grupo simétrico S_X y en particular S_n es un grupo. La operación es la composición de permutaciones; el elemento neutro es la permutación identidad id. El grupo $S_2 = \{\mathrm{id},\ (1\ 2)\}$ es abeliano. El grupo S_n para $n \geq 3$ no es abeliano. De hecho, este contiene, por ejemplo, las transposiciones $(1\ 2)$ y $(2\ 3)$ que no conmutan:

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

El grupo alternante $A_n \subset S_n$ es también un grupo respecto a las mismas operaciones que S_n. Notamos que

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

es abeliano. En efecto, tenemos

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

Para $n \geq 4$ el grupo A_n no es abeliano: por ejemplo, los 3-ciclos $(1\ 2\ 3)$ y $(1\ 2\ 4)$ no conmutan:

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

▲

2.2 Algunas observaciones respecto a los axiomas de grupos

2.2.1. Observación (Unicidad del elemento neutro). *En un grupo hay un elemento único $e \in G$ que satisface*

$$e * g = g = g * e$$

para todo $g \in G$.

Demostración. Sea $e' \in G$ otro elemento con la misma propiedad. Entonces,

$$e = e' * e = e'.$$

■

2.2.2. Observación (Unicidad de inversos). *Para $g \in G$ un elemento g' tal que*

$$g * g' = e = g' * g. \tag{2.1}$$

es único.

Demostración. Sea $g'' \in G$ otro elemento tal que

$$g * g'' = e = g'' * g. \tag{2.2}$$

Luego,

$$g' \overset{\text{G2)}}{=} g' * e \overset{(2.2)}{=} g' * (g * g'') \overset{\text{G1)}}{=} (g' * g) * g'' \overset{(2.1)}{=} e * g'' \overset{\text{G2)}}{=} g''.$$

■

2.2.3. Observación (Asociatividad generalizada). *Supongamos que $*$ es una operación asociativa: para cualesquiera $g, h, k \in G$ tenemos*

$$(g * h) * k = g * (h * k).$$

Entonces en una expresión

$$g_1 * g_2 * \cdots * g_n$$

todos los posibles modos de poner los paréntesis dan el mismo resultado.

Demostración. Funciona el mismo argumento que vimos en el capítulo 0 para las composiciones de aplicaciones. ■

Normalmente vamos a usar la notación **multiplicativa**: escribir "$g \cdot h$" o simplemente "gh" en vez de "$g * h$". En este caso también sería lógico denotar el elemento neutro por 1, o por 1_G para subrayar que es el elemento neutro de un grupo G. En vez de "operación $*$" vamos a decir "producto". Hay que recordar que en general este producto no es conmutativo: en general $gh \neq hg$ (cuando el grupo no es abeliano). También será útil la notación para $g \in G$ y $n \in \mathbb{Z}$

$$g^n := \begin{cases} \underbrace{g \cdots g}_{n \text{ veces}}, & \text{si } n > 0, \\ 1, & \text{si } n = 0, \\ (g^{-n})^{-1}, & \text{si } n < 0. \end{cases}$$

Note que se tiene la identidad

$$(g^m)^n = g^{mn}.$$

No olvidemos que la multiplicación no es conmutativa en general, así que, por ejemplo, $(gh)^2 = ghgh$, y en general no es lo mismo que $g^2h^2 = gghh$.

Cuando el grupo es abeliano, es común la notación **aditiva**: en vez de "$g * h$" se escribe "$g + h$". En este caso el elemento neutro se denota por 0.

Puesto que para cada $g \in G$ su inverso $g' \in G$ está definido de modo único, vamos a denotarlo por g^{-1}:

$$gg^{-1} = 1 = g^{-1}g.$$

En la notación aditiva, vamos a denotar los grupos abelianos por las letras A, B, C y sus elementos por a, b, c. En vez del elementos inversos se habla de los elementos **opuestos** que se denotan por $-a$:

$$a + (-a) = 0 = (-a) + a.$$

Se usa la notación

$$n \cdot a := \begin{cases} \underbrace{a + \cdots + a}_{n \text{ veces}}, & \text{si } n > 0, \\ 0, & \text{si } n = 0, \\ -((-n) \cdot a), & \text{si } n < 0. \end{cases} \tag{2.3}$$

Note que si A es un grupo abeliano, entonces para cualesquiera $m, n \in \mathbb{Z}$, $a, b \in A$ se tiene

$$\begin{gathered} (m + n) \cdot a = m \cdot a + n \cdot a, \\ m \cdot (a + b) = m \cdot a + m \cdot b, \\ (mn) \cdot a = m \cdot (n \cdot a), \\ 1 \cdot a = a. \end{gathered}$$

2.2.4. Observación (Cancelación). *En todo grupo se cumple la cancelación:*

$$gh' = gh'' \Rightarrow h' = h'', \quad g'h = g''h \Rightarrow g' = g''.$$

Demostración. Multiplicando la identidad $g\,h' = g\,h''$ por g^{-1} por la izquierda, se obtiene

$$g^{-1} \cdot (gh') = g^{-1} \cdot (gh'')$$

Luego,

$$h' = 1 \cdot h' = (g^{-1}g) \cdot h' = g^{-1} \cdot (g\,h') = g^{-1} \cdot (g\,h'') = (g^{-1}g) \cdot h'' = 1 \cdot h'' = h''.$$

De la misma manera, la identidad $g'h = g''h$ puede ser multiplicada por h^{-1} por la derecha. ■

2.2.5. Observación. *Para todo $g \in G$ se tiene $(g^{-1})^{-1} = g$.*

2.2.6. Observación. *Para un producto de dos elementos gh se tiene*

$$(gh)^{-1} = h^{-1}g^{-1}.$$

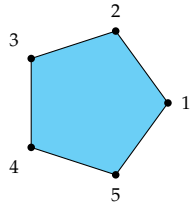
En general,

$$(g_1g_2 \cdots g_{n-1}g_n)^{-1} = g_n^{-1}g_{n-1}^{-1} \cdots g_2^{-1}g_1^{-1}.$$

Para entender la fórmula $(gh)^{-1} = h^{-1}g^{-1}$, piense en el siguiente ejemplo: primero nos ponemos los calcetines y luego los zapatos. La operación inversa es primero quitarse los zapatos y luego los calcetines.

2.3 Grupos diédricos

Para un número fijo $n = 3, 4, 5, \ldots$ consideremos un polígono regular P de n vértices centrado en el origen del plano euclidiano $\mathbb{R}^2$. Numeremos sus vértices.



Pentágono regular.

Consideremos las isometrías del plano euclidiano $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ que preservan el polígono; es decir, $f(P) = P$. Estas forman un grupo respecto a la composición. El elemento neutro es la aplicación identidad id. Este grupo se llama el **grupo de simetrías del n-ágono regular** o el **grupo diédrico**[*] D_n[**].

Recordemos que las isometrías pueden ser descompuestas en aplicaciones de tres tipos: traslación, rotación y reflexión (simetría). Podemos descartar las traslaciones, ya que solo la traslación trivial (identidad) preserva P. Para las rotaciones, está claro que solo las rotaciones por los múltiplos de $360^\circ/n$ preservan P. Por ejemplo, sea $r\colon \mathbb{R}^2 \to \mathbb{R}^2$ la rotación de $360^\circ/n$ grados en sentido antihorario. Su aplicación inversa r^{-1} es la rotación de $360^\circ/n$ grados en sentido horario, que también puede ser realizada como la rotación de $(n-1)\,360^\circ/n$ grados. Todas las rotaciones distintas son

$$r, r^2, r^3, \ldots, r^{n-1}.$$

[*]Del griego "di-", "dos" y "edra", que en este caso significa "cara". Por ejemplo, de la misma manera la palabra "dilema" significa "dos lemas [proposiciones]". El término "polígono" significa una figura que tiene varias caras. En este caso P es una figura plana y entonces se puede decir que P tiene dos caras.

[**]Ojo: en muchos textos el mismo grupo se denota por D_{2n}.

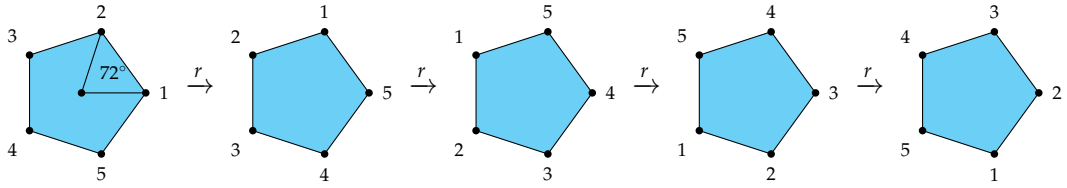
Aquí escribimos

$$r^i := \underbrace{r \circ \cdots \circ r}_{i}.$$

Por la definición, $r^0 := \mathrm{id}$ y en este caso está claro que

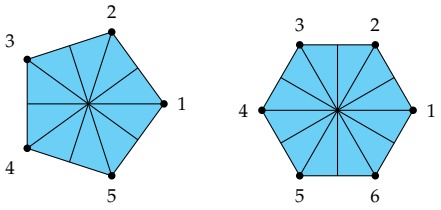
$$r^n = \mathrm{id}$$

(es la rotación de 360°).



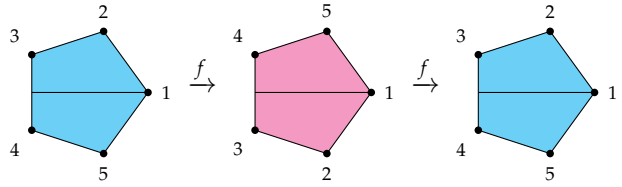
Las reflexiones que preservan P son precisamente las reflexiones respecto a los ejes de simetría de nuestro polígono regular. En total tenemos n ejes de simetría:

- si n es impar, cada uno de ellos pasa por el origen y uno de los vértices;
- si n es par, hay $n/2$ ejes de simetría que pasan por los vértices opuestos y $n/2$ que pasan por los lados opuestos.



(Más adelante veremos que de hecho, las propiedades del grupo D_n dependen la paridad de n.)

Sea f la reflexión respecto al eje que pasa por el origen y el vértice 1.



Tenemos

$$f^2 = \mathrm{id}.$$

Obviamente, f no se expresa en términos de rotaciones:

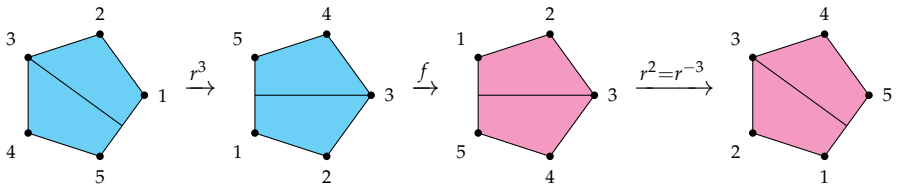
$$f \neq r^i \quad \text{para ningún } i,$$

y en general, los elementos

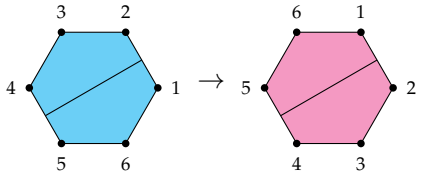
$$f, f \circ r, f \circ r^2, f \circ r^3, \ldots, f \circ r^{n-1}$$

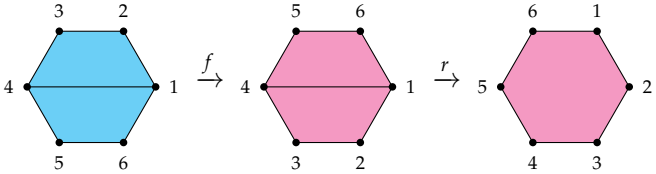
son distintos y no coinciden con los r^i.

Notemos que una reflexión respecto a otro eje puede ser realizada como una rotación seguida por f y otra rotación:



Si n es par, las reflexiones respecto a los ejes que pasan por los lados opuestos también pueden ser expresadas mediante f y r:

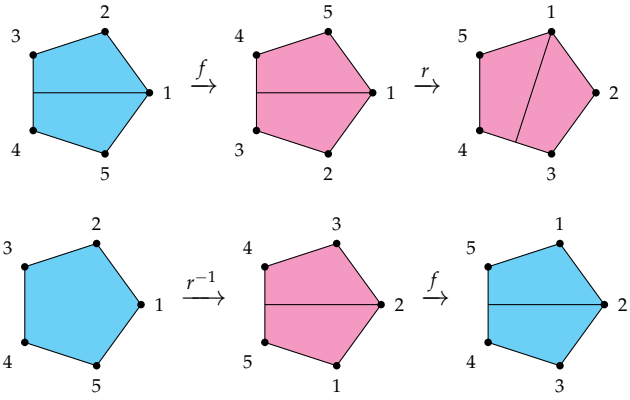




Entonces, hemos visto que todas las simetrías del n-ágono regular pueden ser expresadas como sucesiones de aplicaciones de r y f. Notamos que

$$r \circ f = f \circ r^{-1};$$

en palabras: una reflexión seguida por una rotación de $360°/n$ es lo mismo que la rotación de $360°/n$ en el sentido opuesto seguida por la reflexión respecto a la misma recta.



En particular, $r \circ f \neq f \circ r$, y el grupo D_n no es abeliano. Por inducción se sigue que

$$r^i \circ f = f \circ r^{-i} \quad \text{para todo } i.$$

Usando esto, se puede concluir que

$$D_n = \{\mathrm{id},\ r,\ r^2,\ \ldots,\ r^{n-1},\ f,\ fr,\ fr^2,\ \ldots,\ fr^{n-1}\}$$

(a partir de ahora voy a omitir el signo "$\circ$"). Los elementos enumerados son visiblemente distintos, y hemos calculado entonces que

$$|D_n| = 2n.$$

Note que la tabla de multiplicación de D_n puede ser resumida en las fórmulas

$$r^n = f^2 = \mathrm{id},\ rf = fr^{-1}.$$

Por ejemplo,

$$(fr^i) \cdot (fr^j) = f \cdot (r^i f) \cdot r^j = f \cdot (fr^{-i} \cdot r^j) = r^{j-i}.$$

2.3.1. Ejemplo. Consideremos el caso particular de D_3. Este grupo tiene 6 elementos:

$$D_3 = \{\mathrm{id},\ r,\ r^2,\ f,\ fr,\ fr^2\}$$

y la tabla de multiplicación viene dada por

$\cdot$	id	r	r^2	f	fr	fr^2
id	id	r	r^2	f	fr	fr^2
r	r	r^2	id	fr^2	f	fr
r^2	r^2	id	r	fr	fr^2	f
f	f	fr	fr^2	id	r	r^2
fr	fr	fr^2	f	r^2	id	r
fr^2	fr^2	f	fr	r	r^2	id

▲

Los grupos diédricos D_n nos van a servir como un ejemplo importante para varias definiciones y resultados.

2.4 Grupo de cuaterniones

2.4.1. Ejemplo. Consideremos el conjunto de 8 elementos

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Definamos la multiplicación de elementos de la siguiente manera. ± 1 se comporta de modo habitual: para todo $x \in Q_8$ tenemos

$$1 \cdot x = x \cdot 1, \quad (-1) \cdot x = x \cdot (-1) = -x.$$

y

$$(-1)^2 = 1.$$

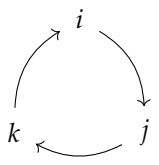
Los cuadrados de i, j, k son iguales a -1:

$$i^2 = j^2 = k^2 = -1.$$

La multiplicación de i, j, k entre ellos es dada por

$$ij = k,\ ji = -k,$$
$$jk = i,\ kj = -i,$$
$$ki = j,\ ik = -j.$$

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



El dibujo a la derecha puede ayudar a memorizar las fórmulas: los caminos nos dan $i \to j \to ij = k$, $j \to k \to jk = i$, $k \to i \to ki = j$, y cuando cambiamos el orden de múltiplos, el signo cambia.

Esto define un grupo que se llama el **grupo de cuaterniones**. El elemento neutro es 1, y el lector puede verificar existencia de elementos inversos (es fácil) y asociatividad (esto puede ser un poco tedioso). Este grupo no es abeliano.

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

▲

2.5 Subgrupos

2.5.1. Definición. Sea G un grupo. Se dice que un subconjunto $H \subseteq G$ es un **subgrupo** de G si

1) $1_G \in H$,

2) para cualesquiera $h_1, h_2 \in H$ tenemos $h_1 * h_2 \in H$,

3) para todo $h \in H$ tenemos $h^{-1} \in H$.

Las condiciones 1)–3) implican que H es también un grupo respecto a la misma operación. Ya que $h\,h^{-1} = 1$ para todo $h \in H$, la condición 1) sirve solo para decir que $H \neq \emptyset$.

2.5.2. Ejemplo. Todo grupo G tiene por lo menos dos subgrupos: el **subgrupo trivial** $\{1\}$ y el mismo G. Los subgrupos distintos de estos dos se llaman **subgrupos propios** de G. ▲

2.5.3. Ejemplo. Hemos visto que el grupo alternante A_n es un subgrupo de S_n. ▲

2.5.4. Ejemplo. Las isometrías del plano euclidiano $\mathbb{R}^2$ forman un grupo. El grupo diédrico D_n es un subgrupo finito. ▲

2.5.5. Observación. *Si $H_i \subset G$ es una familia de subgrupos de G, entonces su intersección $\bigcap_i H_i$ es también un subgrupo.*

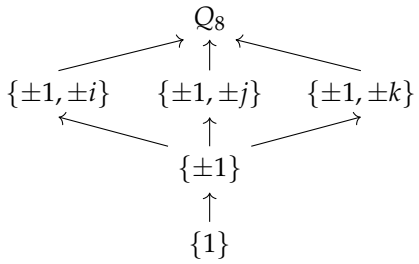
Demostración. Claro a partir de la definición de subgrupo. ■

Ahora compilemos las listas completas de subgrupos para algunos grupos de cardinalidad pequeña.

2.5.6. Ejemplo. En el grupo Q_8, aparte de los subgrupos triviales $\{1\}$ y Q_8, hay un subgrupo de orden 2, que es $\{\pm 1\}$, y tres subgrupos de orden 4:

$$\{\pm 1, \pm i\},\ \{\pm 1, \pm j\},\ \{\pm 1, \pm k\}.$$

Las inclusiones de subgrupos están dibujados en el diagrama de abajo.



▲

2.5.7. Ejemplo. Consideremos el grupo diédrico

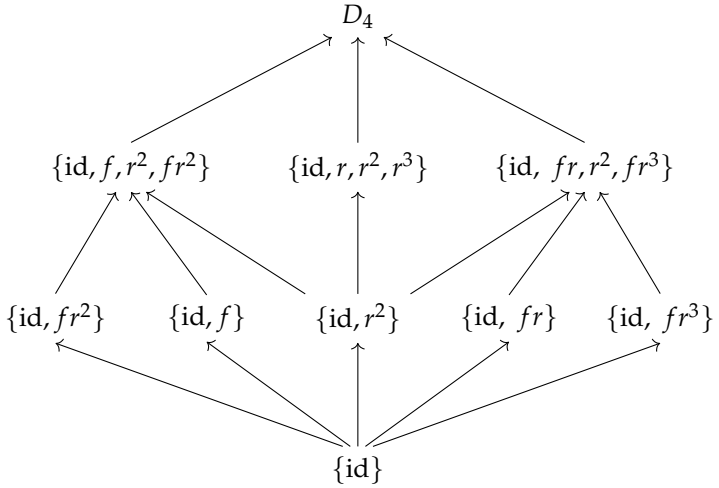
$$D_4 = \{\mathrm{id},\ r,\ r^2,\ r^3,\ f,\ fr,\ fr^2,\ fr^3\}.$$

Al igual que Q_8, este tiene 8 elementos, pero la estructura de sus subgrupos es totalmente diferente. Tenemos 5 subgrupos de orden 2:

$$\{\mathrm{id},\ r^2\},\ \{\mathrm{id},\ f\},\ \{\mathrm{id},\ fr\},\ \{\mathrm{id},\ fr^2\},\ \{\mathrm{id},\ fr^3\}.$$

y 3 subgrupos de orden 4:

$$\{\mathrm{id}, f, r^2, fr^2\},\ \{\mathrm{id}, r, r^2, r^3\},\ \{\mathrm{id},\ fr, r^2, fr^3\}.$$



▲

2.5.8. Ejemplo. Revisando los elementos del grupo alternante A_4, se puede compilar la lista de sus subgrupos.

Cada una de las tres permutaciones de la forma $(\bullet\ \bullet)\ (\bullet\ \bullet)$ corresponde a un subgrupo de orden 2:

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

Y junto con id, estas tres permutaciones forman un subgrupo de orden 4:

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

(la letra V viene del alemán "Vierergruppe", "grupo de cuatro"; el mismo grupo se conoce como el **grupo de Klein**).

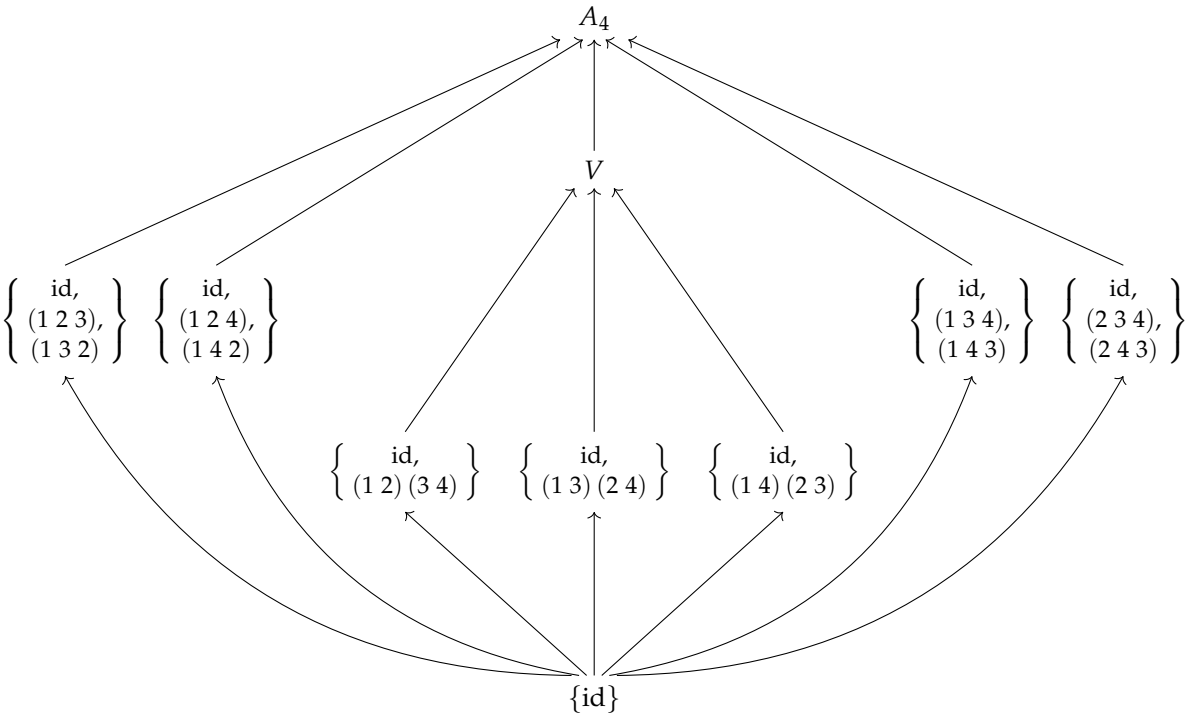
$\circ$	id	(1 2) (3 4)	(1 3) (2 4)	(1 4) (2 3)
id	id	(1 2) (3 4)	(1 3) (2 4)	(1 4) (2 3)
(1 2) (3 4)	(1 2) (3 4)	id	(1 4) (2 3)	(1 3) (2 4)
(1 3) (2 4)	(1 3) (2 4)	(1 4) (2 3)	id	(1 2) (3 4)
(1 4) (2 3)	(1 4) (2 3)	(1 3) (2 4)	(1 2) (3 4)	id

Para los 3-ciclos tenemos

$$\begin{aligned}(1\,2\,3)^2 &= (1\,3\,2), \quad (1\,3\,2)^2 = (1\,2\,3),\\ (1\,2\,4)^2 &= (1\,4\,2), \quad (1\,4\,2)^2 = (1\,2\,4),\\ (1\,3\,4)^2 &= (1\,4\,3), \quad (1\,4\,3)^2 = (1\,3\,4),\\ (2\,3\,4)^2 &= (2\,4\,3), \quad (2\,4\,3)^2 = (2\,3\,4),\end{aligned}$$

lo que nos da cuatro subgrupos de orden 3:

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



Hay una manera ingeniosa de ver que en A_4 no hay otros subgrupos, pero todavía no hemos desarrollado el lenguaje adecuado. ▲

2.5.9. Comentario. El número de subgrupos de S_n y A_n crece muy rápido con n. Hemos descrito los subgrupos de A_4, pero en A_5 ya hay 59 subgrupos. De la misma manera, en S_3 hay 6 diferentes subgrupos (haga el ejercicio 2.6 de abajo), pero en S_4 ya son 30.

n:	2	3	4	5	6	7	8	9	10
# de subgrupos de S_n:	2	6	30	156	1455	11 300	151 221	1 694 723	29 594 446
# de subgrupos de A_n:	1	2	10	59	501	3786	48 337	508 402	6 469 142

Véanse http://oeis.org/A005432 y http://oeis.org/A029725.

2.6 El centro

Un subgrupo importante es el centro.

2.6.1. Definición. Para un grupo G, se dice que g está en su **centro** si g conmuta con todos los elementos de G: tenemos $gh = hg$ para todo $h \in G$. El conjunto de los elementos del centro se denota por

$$Z(G) := \{g \in G \mid gh = hg \text{ para todo } h \in G\} = \{g \in G \mid g = hgh^{-1} \text{ para todo } h \in G\}.$$

2.6.2. Observación. *G es abeliano si y solamente si $Z(G) = G$.*

2.6.3. Observación. *$Z(G)$ es un subgrupo de G.*

Demostración. Para la identidad $1 \in G$ obviamente tenemos $1h = h1 = h$ para todo $h \in G$, entonces $1 \in Z(G)$. Luego, si $g, g' \in Z(G)$, entonces para todo $h \in G$

$$(gg')\,h = g\,(g'h) = g\,(hg') = (gh)\,g' = (hg)\,g' = h\,(gg'),$$

así que $gg' \in Z(G)$. Por fin, si $g \in Z(G)$, entonces para todo $h \in G$ tenemos

$$g^{-1}h = (h^{-1}\,g)^{-1} = (g\,h^{-1})^{-1} = hg^{-1},$$

así que $g^{-1} \in Z(G)$. ■

2.6.4. Ejemplo. Para el grupo simétrico tenemos $Z(S_n) = \{\mathrm{id}\}$ para $n \geq 3$, y en este sentido S_n está muy lejos de ser abeliano.

De hecho, sea $\sigma \in S_n$ una permutación diferente de id. Entonces existen diferentes índices $i, j \in \{1, \ldots, n\}$ tales que

$$\sigma\colon i \mapsto j.$$

Ya que $n > 2$, podemos elegir otro índice k tal que $k \neq i$ y $k \neq j$. Consideremos la transposición $\tau = (j\ k)$. Tenemos

$$\tau\sigma\tau^{-1}\colon \tau(i) = i \mapsto \tau(j) = k.$$

Entonces, $\tau\sigma\tau^{-1} \neq \sigma$ y por lo tanto $\sigma \notin Z(G)$. ▲

2.6.5. Ejemplo. Revisando la tabla de multiplicación del grupo de cuaterniones Q_8, se ve que

$$Z(Q_8) = \{\pm 1\}.$$

▲

2.6.6. Ejemplo. Calculemos el centro del grupo diédrico D_n para $n \geq 3$. Tenemos

$$D_n = \{\mathrm{id},\ r,\ r^2,\ \ldots,\ r^{n-1},\ f,\ fr,\ fr^2,\ \ldots,\ fr^{n-1}\}.$$

Ya que todos los elementos de D_n son productos de f y r, tenemos $x \in Z(D_n)$ si y solamente si

$$f\,x = x\,f, \quad r\,x = x\,r.$$

1) Para x de la forma fr^i tenemos

$$r\,x = x\,r \iff rfr^i = fr^i \cdot r \iff fr^{i-1} = fr^{i+1} \iff r^{i-1} = r^{i+1}.$$

La última condición es equivalente a $i - 1 \equiv i + 1 \pmod{n}$, lo que es imposible para $n > 2$. Podemos concluir que los elementos fr^i no están en el centro.

2) Para x de la forma r^i tenemos obviamente $r\,x = x\,r$. Luego,

$$f\,x = x\,f \iff fr^i = r^i f \iff fr^i = fr^{-i} \iff r^i = r^{-i}.$$

Esto es equivalente a $i \equiv -i \pmod{n}$; es decir, $2i \equiv 0 \pmod{n}$. Esto es posible solamente si n es par e $i = n/2$.

Resumiendo nuestros cálculos, tenemos

$$Z(D_n) = \begin{cases} \{\mathrm{id}\}, & \text{si } n \geq 3 \text{ es impar,} \\ \{\mathrm{id}, r^{n/2}\}, & \text{si } n \geq 4 \text{ es par.} \end{cases}$$

▲

2.7 Ejercicios

Ejercicio 2.1. *Calcule que* $(fr^i)^2 = \mathrm{id}$ *en* D_n *para cualquier* $i \in \mathbb{Z}$. *En general, calcule* $(fr^i)\,(fr^j)$ *para* $i, j \in \mathbb{Z}$.

Ejercicio 2.2. *Demuestre que* $\mathbb{Q} \setminus \{-1\}$ *es un grupo abeliano respecto a la operación*

$$x * y := xy + x + y.$$

Ejercicio 2.3. *Sea* X *un conjunto y* $\mathbf{2}^X$ *el conjunto de sus subconjuntos. Para* $A, B \subseteq X$, *definamos la* ***diferencia simétrica*** *por*

$$A \Delta B := (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

Demuestre que $\mathbf{2}^X$ *es un grupo abeliano respecto a* Δ.

Ejercicio 2.4. *Para dos parámetros fijos* $a, b \in \mathbb{R}$ *definamos una función*

$$\begin{aligned} \phi_{a,b} \colon \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto ax + b. \end{aligned}$$

Consideremos el conjunto

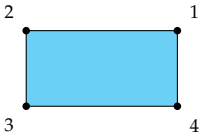
$$G := \{\phi_{a,b} \mid a \in \mathbb{R} \setminus \{0\},\ b \in \mathbb{R}\}.$$

Verifique que G es un grupo respecto a la composición habitual de aplicaciones y que no es abeliano.

Ejercicio 2.5. *Supongamos que G es un grupo donde cada elemento* $g \in G$ *satisface* $g^2 = 1$. *Demuestre que G es abeliano.*

Ejercicio 2.6. *Encuentre todos los subgrupos del grupo simétrico* S_3.

Ejercicio 2.7. *Escriba la tabla de multiplicación del grupo de simetrías de un rectángulo que no es un cuadrado. (Note que este tiene menos simetrías que un cuadrado.)*



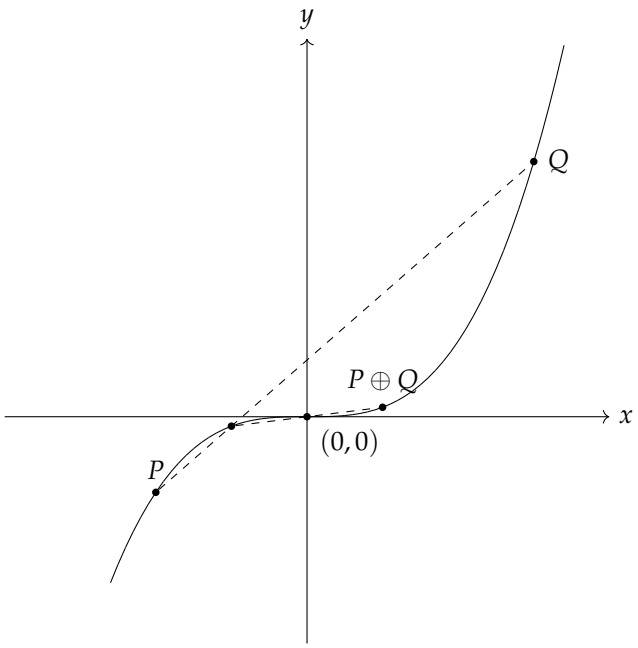
Ejercicio 2.8. *Consideremos el conjunto de puntos* (x, y) *en el plano real que satisfacen la ecuación* $y = x^3$:

$$X(\mathbb{R}) := \{(x, y) \in \mathbb{R}^2 \mid y = x^3\}.$$

Definamos la siguiente operación sobre $X(\mathbb{R})$: *para dos puntos* $P, Q \in X(\mathbb{R})$, *consideremos la recta* ℓ *que pasa por P y Q, o la tangente si* $P = Q$. *Sea R la intersección de* ℓ *con otro punto de* $X(\mathbb{R})$. *Entonces, definimos la suma de P y Q como*

$$P \oplus Q := -R;$$

es decir, el punto simétrico a R respecto al origen.



1) *Demuestre que $X(\mathbb{R})$ es un grupo abeliano respecto a $\oplus$.*

2) *Demuestre que el conjunto*

$$X(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 \mid y = x^3\}$$

(cuyos elementos se denominan "puntos racionales" de la curva X) forman un subgrupo de $X(\mathbb{R})$.

Nota: este ejercicio requiere un buen conocimiento del álgebra de nivel de Baldor.

Ejercicio 2.9. *Sea G un grupo y $H, K \subset G$ dos subgrupos. Demuestre que $H \cup K$ es un grupo si y solamente si $H \subseteq K$ o $K \subseteq H$.*

Ejercicio 2.10. *Hemos visto que el centro del grupo simétrico es trivial:*

$$Z(S_n) = \{\mathrm{id}\} \quad \textit{para } n \geq 3.$$

Demuestre que para el grupo alternante sobre 4 elementos

$$Z(A_4) = \{\mathrm{id}\}.$$

Nota: más adelante veremos en el curso que $Z(A_n) = \{\mathrm{id}\}$ para $n \geq 4$.

Capítulo 3
Anillos y cuerpos

En este curso vamos a estudiar solamente grupos, pero para ver algunos ejemplos importantes de grupos, necesitamos revisar las definiciones de diferentes estructuras algebraicas. Estas se estudian en otros cursos y bastará que el lector conozca los ejemplos principales que voy a mencionar en este capítulo.

3.1 Anillos

3.1.1. Definición. Un **anillo** R es un conjunto dotado de dos operaciones $+$ (adición) y $\cdot$ (multiplicación) que satisfacen los siguientes axiomas.

R1) R es un grupo abeliano respecto a $+$; es decir,

R1a) la adición es asociativa: para cualesquiera $x, y, z \in R$ tenemos

$$(x + y) + z = x + (y + z);$$

R1b) existe un elemento neutro $0 \in R$ (cero) tal que para todo $x \in R$ se cumple

$$0 + x = x = x + 0;$$

R1c) para todo $x \in R$ existe un elemento opuesto $-x \in R$ que satisface

$$(-x) + x = x + (-x) = 0;$$

R1d) la adición es conmutativa: para cualesquiera $x, y \in R$ se cumple

$$x + y = y + x;$$

R2) la multiplicación es distributiva respecto a la adición: para cualesquiera $x, y, z \in R$ se cumple

$$x \cdot (y + z) = xy + xz, \quad (x + y) \cdot z = xz + yz;$$

R3) la multiplicación es asociativa: para cualesquiera $x, y, z \in R$ tenemos

$$(x \cdot y) \cdot z = x \cdot (y \cdot z);$$

R4) existe un elemento neutro multiplicativo $1 \in R$ (identidad) tal que para todo $x \in R$ se cumple

$$1 \cdot x = x = x \cdot 1.$$

Además, si se cumple el axioma

R5) la multiplicación es conmutativa: para cualesquiera $x, y \in R$ se cumple

$$xy = yx.$$

se dice que R es un **anillo conmutativo**.

3.1.2. Digresión. En algunos contextos naturales también surgen anillos sin identidad (donde no se cumple el axioma R4)) y anillos no asociativos (donde nose cumple R3)), pero los vamos a ignorar en este curso.

Note que respecto a la multiplicación, no se pide existencia de elementos inversos (x^{-1} tal que $xx^{-1} = 1 = x^{-1}x$) para ningún elemento.

3.1.3. Observación. *De los axiomas de arriba siguen las propiedades habituales como*

$$\begin{gathered} 0 \cdot x = x \cdot 0 = 0, \\ x \cdot (-y) = (-x) \cdot y = -xy, \\ x\,(y - z) = xy - xz, \quad (x - y)\,z = xz - yz. \end{gathered}$$

Demostración. Ejercicio para el lector. ■

Algunas propiedades conocidas se cumplen solamente en anillos conmutativos, como, por ejemplo, el teorema del binomio

$$(x + y)^n = \sum_{0 \le k \le n} \binom{n}{k} x^{n-k}\, y^k$$

En un anillo no conmutativo tenemos

$$(x + y)^2 = x^2 + xy + yx + y^2,$$

donde xy e yx no necesariamente coinciden.

3.1.4. Ejemplo. Los números enteros $\mathbb{Z}$, racionales $\mathbb{Q}$, reales $\mathbb{R}$, complejos $\mathbb{C}$ forman anillos conmutativos respecto a la adición y multiplicación habitual. ▲

3.1.5. Ejemplo. Para $n = 1, 2, 3, \ldots$ hemos notado en el capítulo 0 que sobre el conjunto

$$\mathbb{Z}/n\mathbb{Z} := \{[a]_n \mid a \in \mathbb{Z}\} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

formado por los restos módulo n

$$[a]_n := \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$$

se puede definir la adición y multiplicación mediante las fórmulas

$$\begin{aligned} [a]_n + [b]_n &:= [a + b]_n, \\ [a]_n \cdot [b]_n &:= [ab]_n. \end{aligned}$$

Se ve que $\mathbb{Z}/n\mathbb{Z}$ es un anillo conmutativo respecto a la adición y multiplicación módulo n. De hecho, estas operaciones son visiblemente asociativas y conmutativas. Las clases de equivalencia $[0]_n$ y $[1]_n$ son el cero y la identidad respectivamente. Los elementos opuestos son dados por $-[a]_n = [-a]_n$.

He aquí la tabla de adición y multiplicación para $n = 4$ (escribo simplemente "$[a]$" en vez de "$[a]_4$"):

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[3]$	$[1]$

La notación "$\mathbb{Z}/n\mathbb{Z}$" será clara después de la definición de grupos cociente que veremos más adelante en nuestro curso. En algunos libros de texto se encuentra la notación "$\mathbb{Z}_n$", pero su uso en este contexto es un pecado mortal: si $n = p$ es primo, normalmente $\mathbb{Z}_p$ denota el *anillo de los enteros p-ádicos*. No lo vamos a ver en este curso, pero es algo muy importante en álgebra y aritmética. ▲

3.1.6. Ejemplo. El **anillo de los enteros de Gauss** es dado por

$$\mathbb{Z}[\sqrt{-1}] := \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

donde la adición y multiplicación están definidas de la manera habitual como para los números complejos. El cero es el número $0 + 0 \cdot \sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$, la identidad es $1 + 0 \cdot \sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$. Está claro que para cualesquiera $x, y \in \mathbb{Z}[\sqrt{-1}]$ tenemos $x + y \in \mathbb{Z}[\sqrt{-1}]$ y $xy \in \mathbb{Z}[\sqrt{-1}]$ y por lo tanto todos los axiomas de anillos conmutativos se verifican fácilmente, ya que estos se cumplen para los números complejos. ▲

3.1.7. Ejemplo. Otro ejemplo del mismo tipo: consideremos el número complejo

$$\zeta_3 = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}\sqrt{-1}.$$

Es una raíz cúbica de la unidad en el sentido de que $\zeta_3^3 = 1$. Se cumple la relación

$$\zeta_3^2 + \zeta_3 + 1 = 0.$$

(En general, el lector puede demostrar que para $\zeta_n := e^{2\pi i/n}$ se cumple $\sum_{0 \le k < n} \zeta_n^k = 0$.) Consideremos el conjunto

$$\mathbb{Z}[\zeta_3] := \{a + b\,\zeta_3 \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Está claro que para cualesquiera $x, y \in \mathbb{Z}[\zeta_3]$ se tiene $x + y \in \mathbb{Z}[\zeta_3]$. Para la multiplicación, si $x = a + b\,\zeta_3$ e $y = c + d\,\zeta_3$, entonces

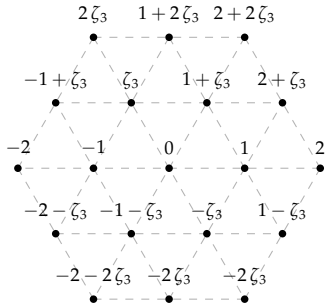
$$(a + b\,\zeta_3) \cdot (c + d\,\zeta_3) = ac + (ad + bc)\,\zeta_3 + bd\,\zeta_3^2,$$

y usando la relación $\zeta_3^2 = 1 - \zeta_3$, podemos escribir la última expresión como

$$(ac - bd) + (bc + ad - bd)\,\zeta_3.$$

Entonces, para cualesquiera $x, y \in \mathbb{Z}[\zeta_3]$ tenemos $xy \in \mathbb{Z}[\zeta_3]$. Después de esta verificación se ve fácilmente que $\mathbb{Z}[\zeta_3]$ es un anillo conmutativo, puesto que $\mathbb{C}$ lo es. Este se llama el **anillo de los enteros de Eisenstein**[*]. El dibujo de abajo representa los enteros de Eisenstein en el plano complejo.

[*] Ferdinand Gotthold Max Eisenstein (1823–1852), matemático alemán, estudiante de Dirichlet, conocido por sus contribuciones en la teoría de números. Murió a los 29 años de tuberculosis (como Abel).



▲

3.1.8. Ejemplo. Tercer y último ejemplo de este tipo: añadamos a los números enteros la raíz cuadrada de 2:

$$\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}.$$

Tenemos

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2},$$

entonces para cualesquiera $x, y \in \mathbb{Z}[\sqrt{2}]$ se tiene $xy \in \mathbb{Z}[\sqrt{2}]$. El conjunto $\mathbb{Z}[\sqrt{2}]$ es un anillo conmutativo respecto a la adición y multiplicación habitual de números reales. Podemos llamar $\mathbb{Z}[\sqrt{2}]$ el **anillo de los enteros de Pitágoras**. ▲

3.1.9. Ejemplo. En general, un **entero algebraico** es un número $\alpha \in \mathbb{C}$ que satisface alguna ecuación polinomial

$$f(\alpha) = \alpha^n + a_{n-1}\,\alpha^{n-1} + \cdots + a_1\,\alpha + a_0,$$

donde $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ y el coeficiente mayor a_n es igual a 1 (en este caso se dice que f es un polinomio **mónico**). Un resultado importante nos dice que todos los enteros algebraicos forman un anillo conmutativo, pero a priori no es claro para nada: si α es una raíz de un polinomio f como arriba y β es una raíz de otro polinomio

$$g(\beta) = \beta^m + b_{m-1}\,\beta^{m-1} + \cdots + b_1\,\beta + b_0,$$

entonces deben existir otros polinomios que tienen como sus raíces $\alpha \pm \beta$ y $\alpha\beta$, pero ¿cómo encontrarlos?

Por ejemplo, $\sqrt{2}$ es una raíz de la ecuación $x^2 - 2 = 0$ y $\sqrt{3}$ es una raíz de la ecuación $x^2 - 3 = 0$. Luego, la suma $\sqrt{2} + \sqrt{3}$ es una raíz de la ecuación

$$x^4 - 10\,x^2 + 1 = 0.$$

De hecho,

$$(\sqrt{2} + \sqrt{3})^2 = 2\sqrt{6} + 5, \quad (\sqrt{2} + \sqrt{3})^4 = 20\sqrt{6} + 49,$$

así que

$$(\sqrt{2} + \sqrt{3})^4 - 10\,(\sqrt{2} + \sqrt{3})^2 + 1 = 0.$$

El producto $\sqrt{2} \cdot \sqrt{3}$ es una raíz de

$$X^2 - 6 = 0.$$

En general, dados dos enteros algebraicos α y β, no es tan fácil encontrar los polinomios mónicos con coeficientes enteros que tienen $\alpha \pm \beta$ y $\alpha\beta$ como sus raíces. Vamos a ver más adelante que es siempre posible. ▲

3.2 Anillo de matrices $M_n(R)$

Todos los anillos de arriba son conmutativos. Mencionemos un ejemplo de anillos no conmutativos muy importante que seguramente es familiar al lector.

Sea R un anillo conmutativo. Entonces las matrices de $n \times n$ con elementos en R forman un anillo que vamos a denotar por $M_n(R)$. Recordemos que la adición de matrices se define término por término:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} := \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \cdots & a_{nn}+b_{nn} \end{pmatrix},$$

mientras que el producto

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix}$$

se define mediante la fórmula

$$c_{ij} := \sum_{1 \le k \le n} a_{ik}\, b_{kj}.$$

El cero es la matriz nula

$$0 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

y el neutro multiplicativo es la matriz identidad

$$I = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

En un primer curso de álgebra lineal normalmente se considera $R = \mathbb{R}$ o $\mathbb{C}$ y se verifican los axiomas de anillos para este caso, pero el anillo específico R es irrelevante para llevar a cabo la construcción general.

El anillo $M_n(R)$ no es conmutativo para $n \ge 2$: por ejemplo, para $n = 2$ tenemos

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \tag{3.1}$$

y luego

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

se cumple si y solamente si $1 = 0$. El lector puede verificar que esto es posible si y solamente si $R = \{0\}$ es un anillo que consiste en un elemento. Este se conoce como el **anillo nulo**.

En general, las únicas matrices que conmutan con todas las matrices son las **matrices escalares** que tienen forma

$$\begin{pmatrix} a & 0 & \cdots & 0 & 0 \\ 0 & a & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a & 0 \\ 0 & 0 & \cdots & 0 & a \end{pmatrix}$$

para algún $a \in R$. Lo vamos a ver en los ejercicios, pero el lector puede tratar de probarlo para las matrices de 2×2. Por ejemplo, se puede considerar una matriz $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ y ver qué significan las identidades $AB = BA$ para

$$B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

3.3 Cuerpos

3.3.1. Definición. Un **cuerpo** k es un anillo conmutativo donde $1 \neq 0$ (es decir, $k \neq \{0\}$) y todo elemento no nulo es invertible. Es decir, para todo $x \neq 0$ existe x^{-1} tal que

$$xx^{-1} = x^{-1}x = 1.$$

3.3.2. Ejemplo. Los anillos conmutativos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son cuerpos. ▲

3.3.3. Definición. Cuando en un anillo se tiene $xy = 0$ para algunos elementos no nulos x e y, se dice que estos son **divisores de cero**. Si un anillo R no tiene divisores de cero, se dice que R es un **dominio de integridad**.

En otras palabras, R es un dominio de integridad si para cualesquiera $x, y \in R$ se cumple

$$\text{si } xy = 0 \text{ entonces } x = 0 \text{ o } y = 0. \tag{3.2}$$

La existencia de elementos inversos en un cuerpo garantiza que es un dominio de integridad.

3.3.4. Observación. *Todo cuerpo es un dominio de integridad.*

Demostración. En un cuerpo, si $x \neq 0$, entonces existe su inverso x^{-1} y multiplicando la identidad $xy = 0$ por x^{-1}, se obtiene

$$x^{-1}(xy) = (x^{-1}x)\, y = 1 \cdot y = y = 0.$$

De la misma manera, $y \neq 0$ implica que $x = 0$. ■

3.3.5. Ejemplo. El anillo conmutativo $\mathbb{Z}/n\mathbb{Z}$ no es un cuerpo en general. Por ejemplo, en $\mathbb{Z}/4\mathbb{Z}$ tenemos divisores de cero

$$[2]_4 \cdot [2]_4 := [2 \cdot 2]_4 = [0]_4,$$

lo que contradice (3.2). El problema es que el elemento $[2]_2$ no es invertible. ▲

3.3.6. Observación. *El anillo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo n es un cuerpo si y solamente si $n = p$ es primo.*

Demostración. Si n no es primo, es decir, $n = ab$ para algunos $a, b < n$, entonces

$$[a]_n \cdot [b]_n = [0]_n,$$

y por lo tanto $\mathbb{Z}/n\mathbb{Z}$ no es un cuerpo. En general, para un entero a existe b tal que

$$ab \equiv 1 \pmod{n}$$

(inverso módulo n) si y solamente si a es coprimo con n; es decir, $\mathrm{mcd}(a, n) = 1$. De hecho, si $\mathrm{mcd}(a, n) = 1$, entonces tenemos la identidad de Bézout[*]

$$ab + nc = 1 \quad \text{para algunos } b, c \in \mathbb{Z}.$$

Reduciendo esta identidad módulo n, se obtiene $ab \equiv 1 \pmod{n}$. En la otra dirección, supongamos que $ab \equiv 1 \pmod{n}$ para algún b. Entonces, tenemos

$$ab + nc = 1$$

para algún $c \in \mathbb{Z}$. Pero $\mathrm{mcd}(a, n)$ es el mínimo número positivo de la forma $ax + ny$ para $x, y \in \mathbb{Z}$.

En particular, si p es primo, para todo $a \not\equiv 0 \pmod{p}$ existe b tal que $ab \equiv 1 \pmod{p}$. ■

3.3.7. Digresión. De hecho, existe un cuerpo de 4 elementos, mas es diferente de $\mathbb{Z}/4\mathbb{Z}$. He aquí su tabla de adición y multiplicación:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

En general, todo cuerpo finito necesariamente tiene orden $q = p^k$ donde $p = 2, 3, 5, 7, 11, \ldots$ es primo y $k = 1, 2, 3, 4, \ldots$ Estos cuerpos se denotan por $\mathbb{F}_{p^k}$. Cuando $k = 1$, es la misma cosa que $\mathbb{Z}/p\mathbb{Z}$, pero para $k > 1$, como hemos notado, $\mathbb{Z}/p^k\mathbb{Z}$ no es un cuerpo, así que $\mathbb{F}_{p^k}$ tiene construcción diferente. Vamos a estudiarlo en la continuación de este curso.

He aquí una aplicación interesante de los cuerpos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

3.3.8. Observación. *Si p es primo, entonces en el cuerpo $\mathbb{F}_p$ tenemos*

$$(x + y)^p = x^p + y^p$$

para cualesquiera $x, y \in \mathbb{F}_p$

Demostración. El teorema del binomio nos da

$$(x + y)^p = x^p + \binom{p}{1} x^{p-1}y + \binom{p}{2} x^{p-2}y^2 + \cdots + \binom{p}{p-1} xy^{p-1} + y^p.$$

Pero $p \mid \binom{p}{i}$ para $i = 1, \ldots, p-1$ (¡ejercicio!), así que todos los términos de la suma son congruentes a cero módulo p (es decir, son nulos en $\mathbb{F}_p$), excepto x^p e y^p. ■

La aplicación $x \mapsto x^p$ sobre $\mathbb{F}_p$ se conoce como la **aplicación de Frobenius**.

[*] El lector que no se acuerda del mcd y sus propiedades debería consultar el apéndice A.

3.3.9. Corolario (Pequeño teorema de Fermat). *Sea p un número entero. Si a es un número entero tal que $p \nmid a$, entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demostración. Notemos que en $\mathbb{F}_p$ se cumple

$$x^p = x. \tag{3.3}$$

De hecho, si $x = [0]$ o $x = [1]$, es obvio. Luego, por inducción, si esto se cumple para $x = [a]$, entonces

$$([a+1])^p = ([a] + [1])^p = [a]^p + [1]^p = [a] + [1] = [a+1].$$

Ahora si a es un entero tal que $p \nmid a$, entonces $x = [a]$ es un elemento no nulo en $\mathbb{F}_p$, y por lo tanto es invertible. La identidad (3.3) implica

$$a^{p-1} = a^{-1}a^p = a^{-1}a = 1.$$

Es decir,

$$[a^{p-1}] = [a]^{p-1} = [1] \iff a^{p-1} \equiv 1 \pmod{p}.$$

■

3.4 Anillo de polinomios $R[X]$

3.4.1. Definición. Sea R un anillo conmutativo. Un **polinomio** con coeficientes en R en una variable X es una *suma formal*

$$f = \sum_{i \geq 0} a_i X^i,$$

donde $a_i \in R$, y casi todos los a_i son nulos, excepto un número finito de ellos. Esto quiere decir que la suma formal de arriba es finita: $f = \sum_{0 \leq i \leq n} a_i X^i$ para algún n.

Las sumas de polinomios están definidas por

$$\sum_{i \geq 0} a_i X^i + \sum_{i \geq 0} b_i X^i := \sum_{i \geq 0} (a_i + b_i) X^i \tag{3.4}$$

y los productos por

$$\left(\sum_{i \geq 0} a_i X^i \right) \cdot \left(\sum_{i \geq 0} b_i X^i \right) := \sum_{k \geq 0} \left(\sum_{i+j=k} a_i b_j \right) X^k. \tag{3.5}$$

El cero es el polinomio $0 = \sum_{0 \leq i \leq n} a_i X^i$ donde todos los coeficientes a_i son nulos y la identidad es el polinomio $1 = \sum_{0 \leq i \leq n} a_i X^i$ donde $a_0 = 1$ y el resto de los coeficientes son nulos. Ya que R es un anillo conmutativo, de la definición de producto está claro que $f \cdot g = g \cdot f$, y también se puede ver que el producto es asociativo: $f \cdot (g \cdot h) = (f \cdot g) \cdot h$. Todos los polinomios forman un anillo conmutativo que se denota por $R[X]$.

3.4.2. Definición. Para un polinomio $f = \sum_{i\geq 0} a_i\, X^i \in R[X]$ su **grado** es dado por

$$\deg f := \max\{i \mid a_i \neq 0\}.$$

Para el polinomio nulo, se define

$$\deg 0 := -\infty.$$

Si $f = 0$ o $\deg f = 0$, se dice que f es un polinomio **constante**.

3.4.3. Proposición. *Para cualesquera $f, g \in R[X]$ se tiene*

$$\deg(fg) \leq \deg f + \deg g.$$

Además, si R es un dominio de integridad, entonces

$$\deg(fg) = \deg f + \deg g.$$

Demostración. Para $f = 0$ o $g = 0$ la identidad $\deg(fg) = \deg f + \deg g$ se cumple gracias a nuestra definición del grado del polinomio nulo. Supongamos entonces que f y g no son nulos y que $\deg f = m$, $\deg g = n$,

$$f = \sum_{0\leq i\leq m} a_i\, X^i, \quad g = \sum_{0\leq i\leq n} b_i\, X^i.$$

El coeficiente de X^k en el producto fg es $c_k = \sum_{i+j=k} a_i\, b_j$. Ya que $a_i = 0$ para $i > m$ y $b_j = 0$ para $j > n$, está claro que $c_k = 0$ para $k > n + m$, así que por lo menos se cumple $\deg(fg) \leq \deg f + \deg g$. Para $k = m + n$ tenemos

$$c_{m+n} = a_0\, b_{m+n} + a_1\, b_{m+n-1} + \cdots + a_m\, b_n + \cdots + a_{m+n-1}\, b_1 + a_{m+n}\, b_0 = a_m\, b_n$$

(casi todos los términos en la suma son nulos por la misma razón). Si R es un dominio de integridad, entonces $a_m \neq 0$ y $b_n \neq 0$ implica que $c_{m+n} = a_m\, b_n \neq 0$. Esto demuestra que $\deg(fg) = \deg f + \deg g$. ■

3.4.4. Corolario. *El anillo $R[X]$ es un dominio de integridad si y solamente si R lo es.*

Demostración. Si R es un dominio de integridad, entonces para el producto de dos polinomios tenemos

$$\deg(fg) = \deg f + \deg g.$$

En particular, si $\deg f > -\infty$ y $\deg g > -\infty$, tenemos $\deg(fg) > -\infty$. En otras palabras, $f \neq 0$ y $g \neq 0$ implica $fg \neq 0$.

Viceversa, si $R[X]$ es un dominio de integridad, el anillo R corresponde a los polinomios de grado 0 y por lo tanto es también un dominio de integridad. ■

3.4.5. Comentario. Por nuestra definición, un polinomio es una suma formal $\sum_{i\geq 0} a_i\, X^i$ donde casi todos los coeficientes son nulos. Si permitimos existencia de un número infinito de coeficientes no nulos, estas sumas formales forman un anillo conmutativo respecto a la suma y producto dados por las mismas fórmulas (3.4) y (3.5). Este anillo se llama el **anillo de series formales en** X y se denota por $R[\![X]\!]$. Si R es un dominio de integridad, entonces $R[\![X]\!]$ es también un dominio de integridad. Sin embargo, esto se demuestra de otra manera: la noción de grado no tiene sentido si en $\sum_{i\geq 0} a_i\, X^i$ puede haber coeficientes no nulos de grado arbitrariamente grande. Para los detalles, haga los ejercicios al final de este capítulo.

3.4.6. Definición. Para un polinomio $f = \sum_{0\leq i\leq n} a_i\, X^i \in R[X]$ y un elemento $c \in R$ la **evaluación de f en** c es el elemento

$$f(c) := \sum_{0\leq i\leq n} a_i\, c^i \in R.$$

Si $f(c) = 0$, se dice que c es un **cero** de f.

3.4.7. Proposición. *Sea $f \in R[X]$ un polinomio no nulo con coeficientes en un dominio de integridad R. Entonces f tiene $\leq \deg f$ raíces distintas en R.*

3.4.8. Ejemplo. El polinomio cuadrático $f = X^2 + 1 \in \mathbb{C}[X]$ tiene dos raíces complejas $\pm\sqrt{-1} \in \mathbb{C}$. Si lo consideramos como un polinomio en $\mathbb{R}[X]$, entonces este no tiene raíces.

El polinomio $f = X^2 + 1 \in \mathbb{F}_3[X]$ no tiene raíces en $\mathbb{F}_3$: tenemos

$$f([0]) = [1], \quad f([1]) = [2], \quad f([2]) = [2]^2 + [1] = [2].$$

El polinomio $f = 2\,X^4 - 3\,X^3 + 3\,X^2 - 3\,X + 1 \in \mathbb{Z}[X]$ puede ser escrito como

$$f = 2\,(X-1)\,(X-\sqrt{-1})\,(X+\sqrt{-1})\,(X-1/2).$$

Su única raíz en $\mathbb{Z}$ es 1.

El polinomio $f = 2\,X^2 + 2\,X \in \mathbb{Z}/4\mathbb{Z}$ es cuadrático, pero todo elemento de $\mathbb{Z}/4\mathbb{Z}$ es su raíz:

$$f([0]) = f([1]) = f([2]) = f([3]) = [0].$$

Esto no contradice el enunciado de arriba, ya que $\mathbb{Z}/4\mathbb{Z}$ no es un dominio de integridad. ▲

Para demostrar 3.4.7, necesitamos el siguiente resultado auxiliar.

3.4.9. Lema. *Sea $f \in R[X]$ un polinomio con coeficientes en un anillo conmutativo R. Entonces $f(c) = 0$ para algún $c \in R$ si y solamente si*

$$f = (X - c) \cdot g$$

para algún polinomio $g \in R[X]$.

Demostración (división sintética). En una dirección es obvio: si podemos escribir

$$f = (X - c) \cdot g,$$

entonces la evaluación en c nos da

$$f(c) = (c - c) \cdot g(c) = 0.$$

En la otra dirección, supongamos que $\deg f = n$ y escribamos

$$f = \sum_{0 \leq i \leq n} a_i\, X^i.$$

Es posible encontrar g de la forma deseada de grado $n - 1$. Escribamos

$$g = \sum_{0 \leq i \leq n-1} b_i\, X^i,$$

donde b_i son ciertos coeficientes que necesitamos encontrar. Analicemos la identidad

$$f = (X - c) \cdot g + b_{-1},$$

donde $b_{-1} \in R$ es alguna constante. Tenemos

$$\sum_{0 \leq i \leq n} a_i\, X^i = (X - c) \sum_{0 \leq i \leq n-1} b_i\, X^i + b_{-1}.$$

Desarrollando la parte derecha, se obtiene

$$\sum_{0\le i\le n} a_i\, X^i = \sum_{1\le i\le n} b_{i-1}\, X^i - \sum_{0\le i\le n-1} c\, b_i\, X^i + b_{-1} = \sum_{0\le i\le n-1} (b_{i-1} - c\, b_i)\, X^i + b_{n-1}\, X^n.$$

Esto corresponde al siguiente sistema de ecuaciones sobre los b_i:

$$\begin{aligned} a_n &= b_{n-1},\\ a_{n-1} &= b_{n-2} - cb_{n-1},\\ a_{n-2} &= b_{n-3} - cb_{n-2},\\ &\cdots\\ a_1 &= b_0 - cb_1,\\ a_0 &= b_{-1} - c\, b_0 \end{aligned}$$

y nos lleva a las recurrencias

$$\begin{aligned} b_{n-1} &= a_n,\\ b_{n-2} &= a_{n-1} + cb_{n-1},\\ b_{n-3} &= a_{n-2} + cb_{n-2},\\ &\cdots\\ b_i &= a_{i+1} + cb_{i+1},\\ &\cdots\\ b_0 &= a_1 + cb_1,\\ b_{-1} &= a_0 + cb_0 \end{aligned}$$

que definen el polinomio g y la constante b_{-1}. Evaluando en $X = c$ ambas partes de la identidad

$$f = (X - c)\cdot g + b_{-1},$$

se obtiene

$$b_{-1} = f(c) = 0.$$

■

3.4.10. Comentario. Las recurrencias de la demostración precedente nos dan un modo eficaz de calcular el valor $f(c)$ para un polinomio $f = \sum_{0\le i\le n} a_i\, X^n$: si

$$b_{n-1} = a_n \quad \text{y} \quad b_i = a_{i+1} + cb_{i+1} \text{ para } -1 \le i \le n-1,$$

entonces

$$f(c) = b_{-1}.$$

Esto se conoce como el **algoritmo de Horner**[*]. Note que usando las recurrencias de arriba, $f(c)$ puede ser calculado usando solamente n sumas y n multiplicaciones, lo que es mucho más eficaz que calcular directamente

$$a_0 + a_1\, c + a_2\, c^2 + \cdots + a_n\, c^n.$$

Ahora estamos listos para probar 3.4.7.

[*] William George Horner (1786–1837), matemático inglés.

Demostración de 3.4.7. Inducción sobre $n = \deg f$. Si $n = 0$, entonces f, siendo un polinomio constante no nulo, no tiene raíces. Para el paso inductivo, notamos que si $c \in R$ es una raíz de f, entonces

$$f = (X - c)\, g$$

para algún polinomio $g \in R[X]$. Luego,

$$\deg f = \deg(X - c) \cdot \deg g$$

(aquí se usa la hipótesis que R es un dominio de integridad), así que $\deg g = n - 1$ y por la hipótesis de inducción sabemos que g tiene $\leq n - 1$ raíces. Toda raíz de g es una raíz de f, y si $c' \neq c$ es una raíz de f, entonces la identidad en R

$$0 = f(c') = (c - c') \cdot g(c')$$

implica que $g(c') = 0$ y c' es una raíz de g (de nuevo, se usa la hipótesis que R es un dominio de integridad). Podemos concluir que f tiene $\leq n$ diferentes raíces. ■

3.4.11. Comentario. A veces hay cierta confusión entre los polinomios y funciones polinomiales. Para cualquier polinomio $f \in R[X]$ la evaluación define una función

$$\begin{aligned} R &\to R, \\ c &\mapsto f(c). \end{aligned}$$

Sin embargo, no siempre existe una correspondencia biyectiva entre las aplicaciones que surgen de esta manera y los elementos de $R[X]$. Por ejemplo, para $R = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ hay solamente p^p diferentes aplicaciones $\mathbb{F}_p \to \mathbb{F}_p$, mientras que el anillo $\mathbb{F}_p[X]$ es infinito: sus elementos son las expresiones formales $\sum_{0 \leq i \leq n} a_i\, X^i$ con $a_i \in \mathbb{F}_p$.

Para dar un ejemplo específico: el polinomio $X^p - X \in \mathbb{F}_p[X]$ evaluado en cualquier elemento de $\mathbb{F}_p$ nos da 0, gracias al pequeño teorema de Fermat que acabamos de revisar arriba, mientras que $X^p - X$ no es nulo como un elemento de $\mathbb{F}_p[X]$ (es decir, como una *expresión formal*).

3.5 ¿Para qué sirven los anillos?

Hay mucho más ejemplos importantes de anillos conmutativos y cuerpos, pero no es el tema principal de nuestro curso, así que por el momento es todo. Los anillos conmutativos tienen mucha importancia en las matemáticas modernas. En muchas situaciones hay una correspondencia

Objetos geométricos ("espacios") $\longleftrightarrow$ Objetos algebraicos hechos de anillos conmutativos.

A veces para solucionar problemas geométricos, se puede pasar a los objetos algebraicos correspondientes. Por otro lado, hay muchos objetos algebraicos que surgen naturalmente en la teoría de números; un ejemplo básico son los anillos como $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{2}]$ que hemos visto arriba. A tales objetos se puede asociar ciertos "espacios" y aplicar la intuición geométrica para resolver problemas aritméticos. Es uno de los temas principales de las matemáticas a partir de los años 50-60 del siglo pasado. Preguntar a un matemático moderno si él prefiere trabajar con objetos algebraicos o usar la intuición geométrica es como preguntarse si uno prefiere quedarse ciego o sordo.

Los cuerpos son un caso muy especial de anillos, y de hecho, bajo la correspondencia geométrica-algebraica que mencioné, a un cuerpo corresponde un espacio que consiste solo de un punto. Los anillos $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{2}]$ son también bastante sencillos: si los cuerpos tienen dimensión 0, estos tienen dimensión 1.

Hay anillos de dimensiones superiores, por ejemplo si consideramos el anillo de polinomios $R[X]$, la dimensión sube por 1:

$$\dim R[X] = \dim R + 1.$$

En particular, la dimensión de $k[X]$ para un cuerpo k es igual a 1. También hay anillos de dimensión infinita, pero no los vamos a encontrar en este curso.

3.6 Espacios vectoriales

Para terminar, recordemos la definición de espacios vectoriales que el lector probablemente conoce de cursos de álgebra lineal.

3.6.1. Definición. Sea k un cuerpo. Un **espacio vectorial** es un conjunto V dotado de dos operaciones

$$\begin{aligned} +\colon V \times V &\to V, \\ (u, v) &\mapsto u + v; \\ \cdot\colon k \times V &\to V, \\ (a, u) &\mapsto a \cdot u. \end{aligned}$$

Los elementos de V se llaman **vectores** mientras que los elementos de k se llaman **escalares**. La operación $+$ se llama la **adición** de vectores y la operación $\cdot$ se llama la **acción** de los escalares sobre los vectores. Se pide que se cumplan los siguientes axiomas.

V1) V es un grupo abeliano respecto a la operación $+$; es decir, la adición es asociativa:

$$(u + v) + w = u + (v + w) \quad \text{para cualesquiera } u, v, w \in V,$$

existe el elemento neutro (**vector nulo**) $0 \in V$ tal que

$$0 + u = u + 0 = u \quad \text{para todo } u \in V,$$

para todo vector $u \in V$ existe el **vector opuesto** $-u$ tal que

$$u + (-u) = (-u) + u = 0 \quad \text{para todo } u \in V,$$

y la adición es conmutativa:

$$u + v = v + u \quad \text{para cualesquiera } u, v \in V.$$

V2) La multiplicación por escalares es bilineal: se cumple

$$(a + b) \cdot u = a \cdot u + b \cdot u \quad \text{para cualesquiera } a, b \in k,\ u \in V$$

y

$$a \cdot (u + v) = a \cdot u + a \cdot v \quad \text{para todo } a \in k,\ u, v \in V.$$

V3) La multiplicación por escalares es compatible con la multiplicación en k:

$$(ab) \cdot u = a \cdot (b \cdot u) \quad \text{para cualesquiera } a, b \in k,\ u \in V.$$

V4) La multiplicación por la identidad de k es la indentidad:

$$1 \cdot u = u \quad \text{para todo } u \in V.$$

Muchas propiedades habituales siguen de V1)–V4):

1) $a \cdot 0 = 0$ para todo $a \in k$,

2) $0 \cdot u = 0$ para todo $u \in V$,

3) $(-1) \cdot u = -u$ para todo $u \in V$,

4) $a \cdot (-u) = -(a \cdot u)$ para todo $a \in k$, $u \in V$,

5) $a \cdot (u - v) = a \cdot u - a \cdot v$ para todo $a \in k$, $u, v \in V$,

6) $(a - b) \cdot u = a \cdot u - b \cdot u$ para cualesquiera $a, b \in k$, $u \in V$.

3.6.2. Ejemplo. Si k es un cuerpo y $n = 0, 1, 2, 3, \ldots$ es un número natural fijo, entonces el conjunto

$$k^n := \underbrace{k \times \cdots \times k}_{n} = \{(a_1, \ldots, a_n) \mid a_i \in k\}$$

respecto a las operaciones

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

y

$$a \cdot (a_1, \ldots, a_n) := (aa_1, \ldots, aa_n)$$

forma un espacio vectorial. El vector nulo es dado por $0 = (0, \ldots, 0)$ y los vectores opuestos son $-(a_1, \ldots, a_n) = (-a_1, \ldots, -a_n)$.

Para $n = 0$ tenemos $k^0 := \{0\}$ que se llama el **espacio vectorial nulo**. ▲

El lector debe conocer bien los espacios como $\mathbb{R}^n$ y $\mathbb{C}^n$. En geometría y análisis a veces se usan estructuras extra sobre estos espacios como una métrica, la topología asociada, productos interiores, etc. Todo esto no hace parte de la definición abstracta de espacios vectoriales. Sin embargo, muchos resultados básicos que se estudian en un curso introductivo de álgebra lineal siguen de los axiomas V1)–V4).

3.6.3. Definición. Una **base** de un espacio vectorial V es una familia de vectores $(u_i)_{i \in I}$ tal que todo vector $u \in V$ puede ser escrito como una combinación lineal de los u_i:

$$u = \sum_{i \in I} a_i \cdot u_i,$$

donde $a_i = 0$ para todo i, excepto un número finito. Además, se pide que los u_i sean linealmente independientes; es decir,

$$\text{si } \sum_{i \in I} a_i \cdot u_i = 0, \text{ entonces } a_i = 0 \text{ para todo } i \in I.$$

3.6.4. Ejemplo. El espacio k^n viene con una base canónica dada por

$$e_1 := (1, 0, 0, \ldots, 0), \quad e_2 := (0, 1, 0, \ldots, 0), \quad \ldots, \quad e_n = (0, 0, 0, \ldots, 1).$$

▲

Recordemos que todo espacio vectorial V posee una base y todas las bases tienen la misma cardinalidad que es la **dimensión** de V. La existencia de base en cualquier espacio vectorial se demuestra mediante el lema de Zorn.

3.6.5. Ejemplo. $\mathbb{R}$ es un espacio vectorial sobre $\mathbb{Q}$ y por lo tanto posee una base sobre $\mathbb{Q}$. Es decir, existe una familia de números reales linealmente independientes sobre $\mathbb{Q}$ tal que todo número $x \in \mathbb{R}$ es una combinación lineal de ellos. Esta base se conoce como la **base de Hamel**. Es infinita y no es explícita; su existencia puede ser justificada por el lema de Zorn. ▲

3.7 Ejercicios

Ejercicio 3.1. *Sea p un número primo. Demuestre que los coeficientes binomiales $\binom{p}{i}$ son divisibles por p para $i = 1, \ldots, p-1$.*

Ejercicio 3.2. *Para $n = 2, 3, 4, 5, \ldots$ consideremos la raíz de la unidad $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$.*

1) *Demuestre la identidad $1 + \zeta_n + \zeta_n^2 + \cdots + \zeta_n^{n-1} = 0$.*

2) *Consideremos el conjunto*

$$\mathbb{Z}[\zeta_n] := \{a_0 + a_1\,\zeta_n + a_2\,\zeta_n^2 + \cdots + a_{n-1}\,\zeta_n^{n-1} \mid a_i \in \mathbb{Z}\}.$$

Demuestre que es un anillo conmutativo respecto a la suma y adición habitual de los números complejos.

Ejercicio 3.3. *Deduzca de los axiomas de anillos las siguientes propiedades:*

$$0 \cdot x = x \cdot 0 = 0, \quad x \cdot (-y) = (-x) \cdot y = -xy, \quad x\,(y - z) = xy - xz, \quad (x - y)\,z = xz - yz$$

para cualesquiera $x, y, z \in R$.

Ejercicio 3.4. *En un anillo R puede ser que $0 = 1$. Pero en este caso R tiene solo un elemento.*

1) *Demuestre que un conjunto $R = \{0\}$ que consiste en un elemento puede ser dotado de modo único de una estructura de un anillo conmutativo. Este anillo se llama el **anillo nulo**.*

2) *Demuestre que si en un anillo R se cumple $1 = 0$, entonces $R = \{0\}$.*

Ejercicio 3.5. *Para un número fijo $n = 1, 2, 3, \ldots$ consideremos el conjunto de fracciones con n en el denominador:*

$$\mathbb{Z}[1/n] := \left\{ \frac{m}{n^k} \;\middle|\; m \in \mathbb{Z},\ k = 0, 1, 2, 3, \ldots \right\} \subset \mathbb{Q}.$$

De modo similar, para un número primo fijo $p = 2, 3, 5, 7, 11, \ldots$ consideremos las fracciones con denominador no divisible por p:

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0,\ p \nmid b \right\} \subset \mathbb{Q}.$$

Verifique que $\mathbb{Z}[1/n]$ y $\mathbb{Z}_{(p)}$ son anillos conmutativos respecto a la suma y producto habituales.

Ejercicio 3.6. *Sea R un anillo conmutativo. Una **serie formal de potencias** con coeficientes en R en una variable X es una suma formal*

$$f = \sum_{i \geq 0} a_i\, X^i,$$

donde $a_i \in R$. A diferencia de polinomios, se puede tener un número infinito de coeficientes no nulos. Las sumas y productos de series formales están definidos por

$$\sum_{i \geq 0} a_i\, X^i + \sum_{i \geq 0} b_i\, X^i := \sum_{i \geq 0} (a_i + b_i)\, X^i, \quad \left(\sum_{i \geq 0} a_i\, X^i \right) \cdot \left(\sum_{i \geq 0} b_i\, X^i \right) := \sum_{k \geq 0} \left(\sum_{i+j=k} a_i b_j \right) X^k.$$

1) *Note que las series formales forman un anillo conmutativo. Este se denota por $R[\![X]\!]$.*

2) *Verifique la identidad*

$$(1 + X) \cdot (1 - X + X^2 - X^3 + X^4 - X^5 + \cdots) = 1$$

en $R[\![X]\!]$ (es decir, los coeficientes de la serie formal al lado derecho son $a_0 = 1$ y $a_i = 0$ para $i > 0$).

3) *Para $R = \mathbb{Q}$ verifique la identidad $\left(\sum_{i\geq 0} \frac{X^i}{i!}\right)^n = \sum_{i\geq 0} \frac{n^i}{i!} X^i$ en el anillo de series formales $\mathbb{Q}[\![X]\!]$.*

Ejercicio 3.7. *Para una serie de potencias $f \in R[\![X]\!]$ sea $v(f)$ el mínimo índice tal que el coeficiente correspondiente no es nulo:*

$$v(f) := \text{mín}\{i \mid a_i \neq 0\};$$

y si $f = 0$, pongamos $v(0) := +\infty$.

1) *Demuestre que para cualesquiera $f, g \in R[\![X]\!]$ se cumple la desigualdad*

$$v(fg) \geq v(f) + v(g)$$

y la igualdad $v(fg) = v(f) + v(g)$ si R es un dominio de integridad.

2) *Demuestre que $R[\![X]\!]$ es un dominio de integridad si y solamente si R lo es.*

Ejercicio 3.8. *Sea R un anillo conmutativo. En el anillo de matrices $M_n(R)$ denotemos por e_{ij} para $1 \leq i, j \leq n$ la matriz cuyos coeficientes son nulos, salvo el coeficiente (i, j) que es igual a 1. Sea $A \in M_n(R)$ una matriz arbitraria de $n \times n$ con coeficientes en R.*

1) *Demuestre que en el producto de matrices $e_{ij}\, A$ la fila i es igual a la fila j de A y el resto de los coeficientes son nulos.*

2) *Demuestre que en el producto de matrices $A\, e_{ij}$ la columna j es igual a la columna i de A y el resto de los coeficientes son nulos.*

3) *Demuestre que*

$$e_{ij}\, A = A\, e_{ij}$$

*para todo $1 \leq i, j \leq n$, $i \neq j$ si y solamente si A es una **matriz escalar**:*

$$A = aI = \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}$$

para algún $a \in R$.

4) *Concluya que las únicas matrices en $M_n(R)$ que conmutan con todas las matrices son las matrices escalares.*

Capítulo 4
Grupos de unidades

Después del capítulo precedente, podemos dar algunos ejemplos de grupos que no hemos visto antes. Los siguientes ejemplos son banales en el sentido de que ciertas estructuras algebraicas ya tienen axiomas de grupos como una parte de su definición.

4.0.1. Ejemplo. Todo anillo (y en particular todo cuerpo) es un grupo abeliano respecto a la adición. Por ejemplo, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son grupos abelianos respecto a la adición habitual de números. ▲

4.0.2. Ejemplo. Los restos módulo n forman un anillo y en particular un grupo abeliano respecto a la adición. ▲

4.0.3. Ejemplo. Tenemos una cadena de subgrupos aditivos

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

▲

4.0.4. Ejemplo. Los números enteros divisibles por n forman un subgrupo de $\mathbb{Z}$:

$$n\mathbb{Z} := \{n\,x \mid x \in \mathbb{Z}\}.$$

▲

4.0.5. Ejemplo. Todo espacio vectorial es un grupo abeliano respecto a la adición de vectores. Por ejemplo, para todo cuerpo k, el espacio vectorial k^n es un grupo abeliano. ▲

4.1 El grupo de unidades de un anillo

En general, salvo 1 (identidad) en un anillo R no hay elementos inversos respecto a la multiplicación. Los elementos que tienen inversos forman un grupo.

4.1.1. Definición. Si para $u \in R$ existe u^{-1} tal que

$$u\,u^{-1} = u^{-1}\,u = 1, \tag{4.1}$$

se dice que u es una **unidad**[*] o un **elemento invertible**.

[*]No confundir con *la identidad* $1 \in R$, que es nada más un ejemplo muy particular de unidades.

Como siempre, el elemento u^{-1} está definido de modo único por (4.1); esto se demuestra de la misma manera que la unicidad de los elementos inversos en un grupo.

4.1.2. Comentario. Supongamos que para $u \in R$ existen dos elementos $a, b \in R$ tales que $au = 1$ y $ub = 1$. En este caso necesariamente $a = b$:

$$a = a \cdot 1 = a\,(ub) = (au)\,b = 1 \cdot b = b.$$

Las unidades forman un grupo respecto a la multiplicación que se denota por $R^\times$. De hecho, $1 \in R^\times$ es el elemento neutro y si $u, v \in R^\times$, entonces $uv \in R^\times$:

$$(uv) \cdot (v^{-1}\,u^{-1}) = (v^{-1}\,u^{-1}) \cdot (uv) = 1.$$

4.1.3. Ejemplo. En un cuerpo todo elemento no nulo $x \in k$ tiene su inverso x^{-1}, así que el grupo de unidades viene dado por

$$k^\times = k \setminus \{0\}.$$

Es abeliano (por nuestra definición, la multiplicación en cuerpo es conmutativa). ▲

4.1.4. Ejemplo. Para $\mathbb{Z}$ obviamente tenemos

$$\mathbb{Z}^\times = \{\pm 1\}.$$

▲

4.1.5. Ejemplo. Tenemos una cadena de subgrupos multiplicativos

$$\{\pm 1\} \subset \mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times.$$

▲

4.1.6. Ejemplo. El grupo $\mathbb{Q}^\times$ tiene como su subgrupo el conjunto $\mathbb{Q}_{>0}$ formado por los números racionales positivos. De la misma manera, los números reales positivos $\mathbb{R}_{>0}$ forman un subgrupo de $\mathbb{R}^\times$. ▲

4.2 El círculo y las raíces de la unidad

El grupo $\mathbb{C}^\times$ contiene varios subgrupos interesantes.

4.2.1. Ejemplo. Recordemos que para un número complejo $z = x + y\sqrt{-1} \in \mathbb{C}$ su **valor absoluto** es dado por

$$|z| := \sqrt{z\overline{z}} = \sqrt{(x + y\sqrt{-1}) \cdot (x - y\sqrt{-1})} = \sqrt{x^2 + y^2}.$$

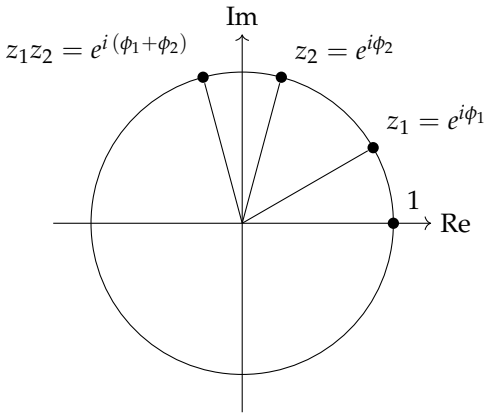
Notamos que para cualesquiera $z_1, z_2 \in \mathbb{C}$ se cumple

$$|z_1 z_2| = |z_1| \cdot |z_2|.$$

Se ve que el conjunto de los números complejos de valor absoluto 1

$$\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\} = \{e^{i\phi} \mid 0 \leq \phi < 2\pi\}$$

es un subgrupo de $\mathbb{C}^\times$ respecto a la multiplicación. Este grupo se llama el **grupo del círculo**, ya que sus elementos son los puntos del círculo unitario en el plano complejo.



▲

4.2.2. Ejemplo. Para un número $n = 1, 2, 3, 4, \ldots$, una **raíz n-ésima de la unidad** es un número complejo z tal que

$$z^n = 1.$$

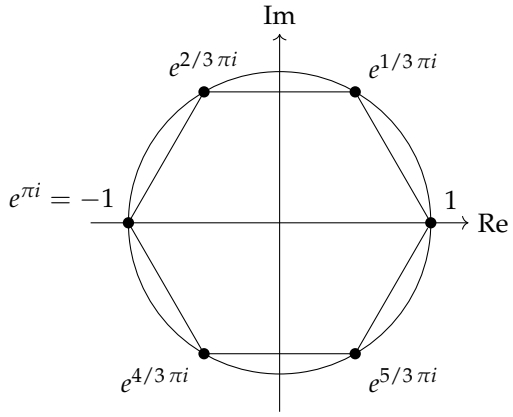
Como sabemos, esta ecuación tiene precisamente n soluciones diferentes

$$e^{2\pi i k/n}, \quad k = 0, 1, \ldots, n-1.$$

Estas forman un grupo abeliano respecto a la multiplicación compleja. Este grupo se denota por $\mu_n(\mathbb{C})$ y se llama el **grupo de las raíces n-ésimas de la unidad**:

$$\mu_n(\mathbb{C}) := \{z \in \mathbb{C} \mid z^n = 1\}.$$

Como el ejemplo más sencillo tenemos $\mu_2(\mathbb{C}) = \{\pm 1\}$. El dibujo de abajo representa el grupo $\mu_6(\mathbb{C})$ en el plano complejo.



Si $m \mid n$, entonces $z^m = 1$ implica $z^n = 1$ y se ve que $\mu_m(\mathbb{C})$ es un subgrupo de $\mu_n(\mathbb{C})$. Por ejemplo, en el dibujo de arriba se ve que $\mu_2(\mathbb{C}) \subset \mu_6(\mathbb{C})$ y $\mu_3(\mathbb{C}) \subset \mu_6(\mathbb{C})$. Todas las raíces de la unidad forman un grupo

$$\mu_\infty(\mathbb{C}) = \{z \in \mathbb{C}^\times \mid z^n = 1 \text{ para algún } n = 1, 2, 3, \ldots\} = \bigcup_{n \geq 1} \mu_n(\mathbb{C}).$$

Tenemos una cadena de subgrupos

$$\mu_m(\mathbb{C}) \overset{\text{si } m|n}{\subset} \mu_n(\mathbb{C}) \subset \mu_\infty(\mathbb{C}) \subset \mathbb{T} \subset \mathbb{C}^\times.$$

▲

4.3 Los restos módulo n invertibles

4.3.1. Ejemplo. Un número $a \in \mathbb{Z}$ es invertible módulo $n = 1, 2, 3, \ldots$ si y solamente si $\mathrm{mcd}(a, n) = 1$:

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

Por ejemplo,

$$\begin{aligned}
(\mathbb{Z}/2\mathbb{Z})^\times &= \{[1]_1\},\\
(\mathbb{Z}/3\mathbb{Z})^\times &= \{[1]_3, [2]_3\},\\
(\mathbb{Z}/4\mathbb{Z})^\times &= \{[1]_4, [3]_4\},\\
(\mathbb{Z}/5\mathbb{Z})^\times &= \{[1]_5, [2]_5, [3]_5, [4]_5\},\\
(\mathbb{Z}/6\mathbb{Z})^\times &= \{[1]_6, [5]_6\},\\
(\mathbb{Z}/7\mathbb{Z})^\times &= \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\},\\
(\mathbb{Z}/8\mathbb{Z})^\times &= \{[1]_8, [3]_8, [5]_8, [7]_8\},\\
(\mathbb{Z}/9\mathbb{Z})^\times &= \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\},\\
(\mathbb{Z}/10\mathbb{Z})^\times &= \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\},\\
&\ldots
\end{aligned}$$

La función

$$\phi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times| = \text{número de enteros entre 0 y } n-1 \text{ coprimos con } n$$

se llama la **función ϕ de Euler**. He aquí algunos de sus valores[*]:

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\phi(n)$:	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

ϕ cumple las siguientes propiedades.

1) si $p = 2, 3, 5, 7, 11, \ldots$ es primo y $k = 1, 2, 3, 4, \ldots$, tenemos

$$\phi(p^k) = p^k \left(1 - \frac{1}{p}\right).$$

2) si m y n son coprimos, entonces

$$\phi(mn) = \phi(m) \cdot \phi(n)$$

(se dice que ϕ es una **función multiplicativa**).

Para demostrar 1), consideramos los números

$$a = 0, 1, 2, \ldots, p^k - 2, p^k - 1.$$

En esta lista hay p^k elementos. Luego, $\mathrm{mcd}(a, p^k) = 1$ si y solamente si $p \nmid a$. Los números en la esta tales que $p \mid a$ son los múltiplos de p: $0, p, 2p, 3p, \ldots$—cada p-ésimo número, en total p^k/p de ellos. Entonces,

$$\phi(p^k) = p^k - p^k/p = p^k \left(1 - \frac{1}{p}\right).$$

[*]Tenemos $\phi(1) = 1$. De hecho, $\mathbb{Z}/1\mathbb{Z}$ es el anillo nulo, y su único elemento es invertible.

En particular, para $k = 1$ tenemos $\phi(p) = p - 1$. Es otro modo de decir que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo (tiene todos sus elementos invertibles, salvo el cero).

En general, las mismas consideraciones pueden ser aplicadas a un número arbitario $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$. De los números

$$0, 1, 2, \ldots, n-1$$

para cada p_i se puede quitar los n/p_i múltiplos de p_i. Pero algunos de estos múltiplos son divisibles al mismo tiempo por p_i y p_j para $i \neq j$, o por tres diferentes primos, etc. El conteo requiere una especie del principio de inclusión-exclusión y nos lleva a la fórmula

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\ell}\right). \tag{4.2}$$

De esta expresión está clara la propiedad 2). Sin embargo, sería más convincente primero demostrar 2) de otra manera y luego deducir (4.2). Es lo que vamos a hacer más adelante. ▲

4.4 Unidades en anillos aritméticos

4.4.1. Ejemplo. Para los enteros de Gauss el grupo de unidades es de orden 4:

$$\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm\sqrt{-1}\}.$$

Para verlo, definamos la aplicación

$$\begin{aligned} N\colon \mathbb{Z}[\sqrt{-1}] &\to \mathbb{Z}, \\ a + b\sqrt{-1} &\mapsto (a + b\sqrt{-1})\,(a - b\sqrt{-1}) = a^2 + b^2, \end{aligned}$$

llamada la **norma**. Note que $N(x) \geq 0$ para todo $x \in \mathbb{Z}[\sqrt{-1}]$. La norma es multiplicativa:

$$N(xy) = N(x)\,N(y).$$

Esto implica que para todo $u \in \mathbb{Z}[\sqrt{-1}]^\times$ se tiene

$$N(u)\,N(u^{-1}) = N(u\,u^{-1}) = N(1) = 1,$$

y por lo tanto $N(u) = 1$. Viceversa, para $a + b\sqrt{-1}$ podemos calcular su inverso en el cuerpo de números complejos:

$$(a + b\sqrt{-1})^{-1} = \frac{a - b\sqrt{-1}}{(a + b\sqrt{-1})\,(a - b\sqrt{-1})} = \frac{a - b\sqrt{-1}}{a^2 + b^2}.$$

Si $N(a + b\sqrt{-1}) = a^2 + b^2 = 1$, entonces $(a + b\sqrt{-1})^{-1} \in \mathbb{Z}[\sqrt{-1}]$. Esto demuestra que

$$a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]^\times \quad \text{si y solamente si} \quad N(a + b\sqrt{-1}) = a^2 + b^2 = 1.$$

La ecuación $a^2 + b^2 = 1$ tiene 4 soluciones enteras $(\pm 1, 0), (0, \pm 1)$ que corresponden a $\pm 1, \pm\sqrt{-1}$. Estos elementos son invertibles.

$\cdot$	$+1$	-1	$+\sqrt{-1}$	$-\sqrt{-1}$
$+1$	$+1$	-1	$+\sqrt{-1}$	$-\sqrt{-1}$
-1	-1	$+1$	$-\sqrt{-1}$	$+\sqrt{-1}$
$+\sqrt{-1}$	$+\sqrt{-1}$	$-\sqrt{-1}$	-1	$+1$
$-\sqrt{-1}$	$-\sqrt{-1}$	$+\sqrt{-1}$	$+1$	-1

El mismo argumento demuestra que para un entero $n = 2, 3, 4, \ldots$ y el anillo conmutativo

$$\mathbb{Z}[\sqrt{-n}] = \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}$$

se tiene $\mathbb{Z}[\sqrt{-n}]^\times = \{\pm 1\}$ para todo $n \geq 2$ —para verlo, considere la norma

$$N(a + b\sqrt{-n}) := (a + b\sqrt{-n})\,(a - b\sqrt{-n}) = a^2 + nb^2.$$

▲

4.4.2. Ejemplo. Para el anillo $\mathbb{Z}[\sqrt{2}]$ podemos considerar la norma

$$\begin{aligned} N\colon \mathbb{Z}[\sqrt{2}] &\to \mathbb{Z}, \\ a + b\sqrt{2} &\mapsto (a + b\sqrt{2})\,(a - b\sqrt{2}) = a^2 - 2b^2. \end{aligned}$$

Esta aplicación es también multiplicativa y por lo tanto $N(u) = \pm 1$ para todo $u \in R^\times$. Luego, tenemos

$$(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})\,(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2},$$

así que

$$a + b\sqrt{2} \quad \text{si y solamente si} \quad N(a + b\sqrt{2}) = a^2 - 2b^2 = 1.$$

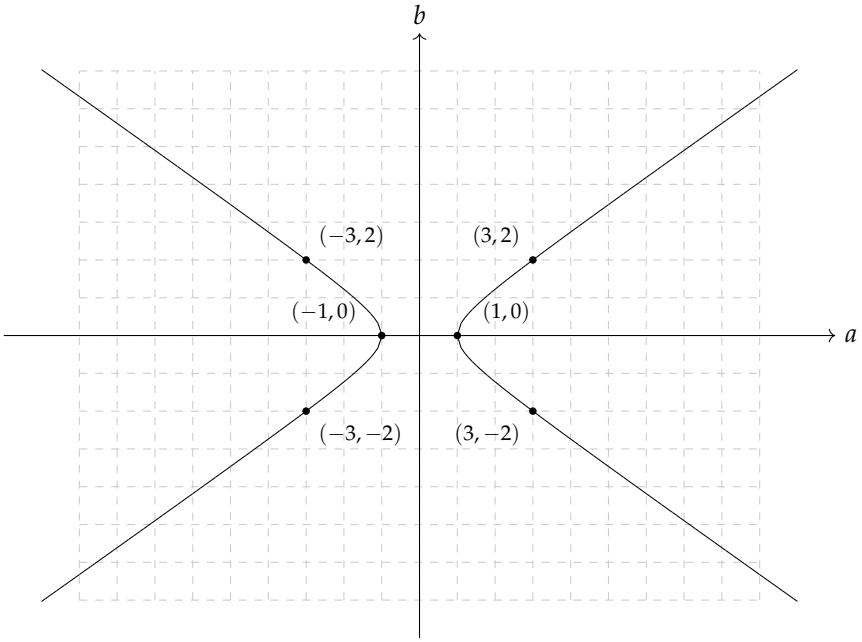
Entonces, para calcular el grupo $\mathbb{Z}[\sqrt{2}]$, hay que encontrar las soluciones enteras de la ecuación

$$a^2 - 2b^2 = \pm 1.$$

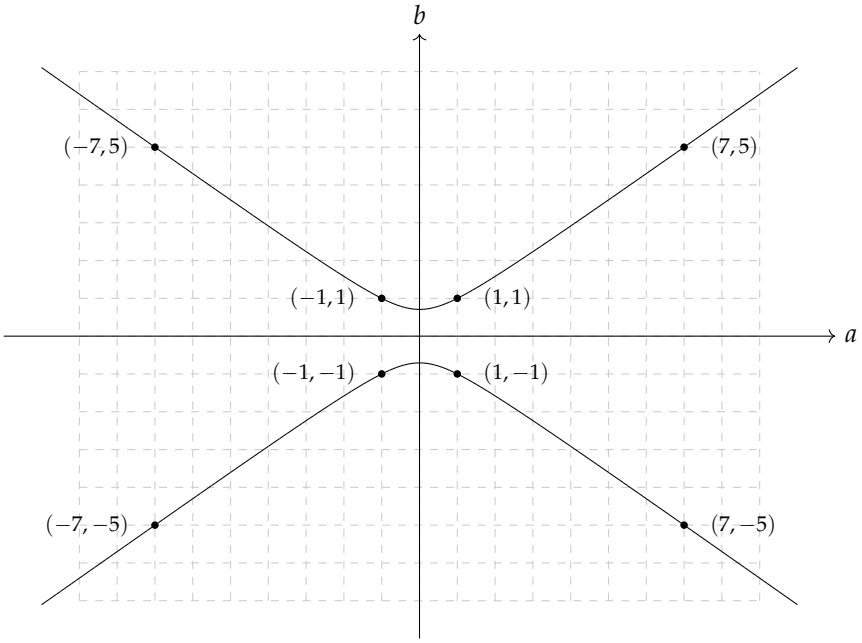
Esta se conoce como la **ecuación de Pell**[*]. No vamos a entrar en los detalles, pero hay un número infinito de soluciones $(a, b) \in \mathbb{Z}^2$. Por ejemplo,

$$(a, b) = (\pm 1, 0),\ (\pm 1, \pm 1),\ (\pm 3, \pm 2),\ (\pm 7, \pm 5),\ \ldots \tag{4.3}$$

[*] John Pell (1611–1685), matemático inglés. No hay documentos que demuestren que Pell trabajó en algún momento de su vida en la "ecuación de Pell"; la atribución del nombre se debe a Euler. Así que como matemático, Pell es conocido por una ecuación que nunca estudió.



$a^2 - 2b^2 = 1$



$a^2 - 2b^2 = -1$

Las soluciones (4.3) corresponden a las unidades

$$\begin{gathered}\pm 1 = \pm(1-\sqrt{2})^0,\\ \pm(1+\sqrt{2}),\ \pm(1-\sqrt{2}) = \mp(1+\sqrt{2})^{-1},\\ \pm(3+2\sqrt{2}) = \pm(1+\sqrt{2})^2,\ \pm(3-2\sqrt{2}) = \pm(1+\sqrt{2})^{-2},\\ \pm(7+5\sqrt{2}) = \pm(1+\sqrt{2})^3,\ \pm(7-5\sqrt{2}) = \mp(1+\sqrt{2})^{-3},\\ \dots\end{gathered}$$

Note que todas las soluciones de arriba son de la forma $\pm(1+\sqrt{2})^n$ para algún $n \in \mathbb{Z}$. Evidentemente, son unidades y estas forman un subgrupo de $\mathbb{Z}[\sqrt{2}]^\times$. De hecho, no hay otras unidades:

$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}.$$

Vamos a omitir la demostración ya que esta requiere un análisis más atento de la ecuación de Pell. ▲

La diferencia entre $\mathbb{Z}[\sqrt{-1}]^\times$ por un lado y $\mathbb{Z}[\sqrt{2}]$ por el otro lado es que en el primer anillo el elemento que hemos añadido a $\mathbb{Z}$ es complejo (es decir, $\operatorname{Im}\sqrt{-1} \neq 0$), mientras que $\sqrt{2}$ es real. Esto se estudia en la teoría de números algebraica. Para otro ejemplo similar, véase el ejercicio 4.1.

4.5 Polinomios invertibles

En el capítulo anterior hemos introducido el anillo de polinomios $R[X]$, y sería interesante calcular su grupo de unidades.

4.5.1. Observación. *Si un polinomio $f = \sum_{i\geq 0} a_i X^i \in R[X]$ es invertible, entonces su coeficiente constante es invertible en R; es decir, $a_0 \in R^\times$.*

Demostración. Si existe otro polinomio $g = \sum_{i\geq 0} b_i X^i \in R[X]$ tal que $fg = 1$, esto significa que los coeficientes del producto de f y g están dados por

$$c_k := \sum_{i+j=k} a_i b_j = \begin{cases} 1, & \text{si } k = 0,\\ 0, & \text{si } k > 0.\end{cases}.$$

En particular, $a_0\, b_0 = 1$, lo que significa que $b_0 = a_0^{-1}$. ■

Entonces, la condición $a_0 \in R^\times$ es necesaria para que $f = \sum_{i\geq 0} a_i X^i \in R[X]$ sea invertible, pero no es suficiente. Para simplificar la vida, supongamos que R es un dominio de integridad: $ab = 0$ implica $a = 0$ o $b = 0$. En este caso nos puede servir la noción del grado de un polinomio.

4.5.2. Proposición. *Si R es un dominio de integridad, entonces un polinomio $f = \sum_{i\geq 0} a_i X^i \in R[X]$ es invertible en $R[X]$ si y solamente si $a_0 \in R^\times$ y $a_i = 0$ para $i > 0$. En otras palabras, se tiene una identificación*

$$R[X]^\times = R^\times.$$

Demostración. Apenas hemos visto que la condición $a_0 \in R^\times$ es necesaria. Ahora si f es invertible, tenemos $fg = 1$ para algún polinomio g y luego la identidad

$$0 = \deg(fg) = \deg f + \deg g$$

implica que $\deg f = \deg g = 0$. ■

4.5.3. Comentario. Si en R hay divisores de cero, por ejemplo si $R = \mathbb{Z}/4\mathbb{Z}$, entonces tenemos solamente la desigualdad $\deg(fg) \leq \deg f + \deg g$ en lugar de $\deg(fg) = \deg f + \deg g$ y nuestro argumento no funcióna. En este caso existen polinomios invertibles de grados superiores. Por ejemplo, en el anillo $\mathbb{Z}/4\mathbb{Z}[X]$ se cumple

$$(2X+1)\cdot(2X+1) = 4X^2 + 4X + 1 \equiv 1 \pmod 4.$$

4.6 El grupo lineal general

En los cursos básicos de álgebra lineal mucho tiempo se dedica a multiplicación e inversión de matrices. De hecho, detrás de todo esto hay un grupo.

4.6.1. Definición. Sea V un espacio vectorial sobre un cuerpo. Consideremos todas las aplicaciones lineales *invertibles* $f\colon V \to V$ (isomorfismos entre V y sí mismo); es decir, las que poseen un aplicación lineal inversa $f^{-1}\colon V \to V$ tal que

$$f \circ f^{-1} = \mathrm{id}_V = f^{-1} \circ f.$$

Estas forman un grupo respecto a la composición habitual de aplicaciones. El elemento neutro es la aplicación identidad y los elementos inversos son las aplicaciones inversas. Este grupo se denota por $\mathrm{GL}(V)$ y se llama el **grupo lineal general** de V.

Note que este es un análogo lineal del grupo simétrico S_X. De hecho, $\mathrm{GL}(V)$ es un subconjunto de S_V, pero no tiene sentido considerar todas las biyecciones de conjuntos $V \to V$—son muchas—y por esto restringimos nuestra atención a las biyecciones lineales; es decir, las biyecciones que preservan la estructura algebraica de V.

En general, todas las aplicaciones lineales $f\colon V \to V$ forman un anillo $\mathrm{End}(V)$ que se llama el **anillo de endomorfismos** de V. La adición en este anillo viene dada por

$$(f+g)(v) := f(v) + g(v)$$

y la multiplicación de f por g es la composición $f \circ g$. Este anillo no es conmutativo si $\dim V > 1$. El grupo lineal general es el grupo de unidades correspondiente:

$$\mathrm{GL}(V) = \mathrm{End}(V)^\times.$$

El procedimiento habitual para hacer cálculos con aplicaciones lineales es fijar una base y usar matrices. En el capitulo anterior hemos encontrado el anillo de matrices $M_n(R)$. Es un anillo no conmutativo, pero también tiene sentido considerar su grupo de unidades.

4.6.2. Observación. *Los elementos invertibles en el anillo de matrices $M_n(R)$ son precisamente las matrices con determinante invertible en R:*

$$M_n(R)^\times = \{A \in M_n(R) \mid \det A \in R^\times\}.$$

Demostración. El determinante satisface

$$\det(AB) = \det(A)\cdot\det(B)$$

para cualesquiera $A, B \in M_n(R)$. Luego, si para $A \in M_n(R)$ existe su matriz inversa $A^{-1} \in M_n(R)$, entonces

$$1 = \det(I) = \det(A\,A^{-1}) = \det(A)\cdot\det(A^{-1}) = \det(A^{-1})\cdot\det(A),$$

lo que demuestra que para toda matriz invertible en $M_n(R)$ se tiene necesariamente $\det(A) \in R^\times$. En la otra dirección, si $\det(A) \in R^\times$, podemos usar la fórmula (también conocida como la "regla de Cramer")

$$A^{-1} = \det(A)^{-1} \operatorname{adj}(A),$$

donde $\operatorname{adj}(A)$ es la **matriz adjunta**. ■

4.6.3. Definición. El grupo

$$\mathrm{GL}_n(R) := M_n(R)^\times = \{A \in M_n(R) \mid \det A \in R^\times\}$$

se llama el **grupo lineal general** sobre R.

4.6.4. Ejemplo. Si $R = k$ es un cuerpo, entonces

$$\mathrm{GL}_n(k) = \{A \in M_n(k) \mid \det A \neq 0\}.$$

▲

4.6.5. Ejemplo. Para las matrices con elementos enteros, tenemos

$$\mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}.$$

▲

4.6.6. Ejemplo. Para $n = 1$ tenemos

$$\mathrm{GL}_1(R) = R^\times.$$

Para $n \geq 2$ y $R \neq 0$ el grupo $\mathrm{GL}_n(R)$ no es abeliano (en los ejercicios de abajo vamos a calcular su centro). ▲

4.6.7. Ejemplo. Las matrices de $n \times n$ con determinante 1 forman un grupo

$$\mathrm{SL}_n(R) := \{A \in \mathrm{GL}_n(R) \mid \det A = 1\}.$$

Es un subgrupo de $\mathrm{GL}_n(R)$ conocido como el **grupo lineal especial**. En particular, el grupo

$$\mathrm{SL}_2(\mathbb{Z}) := \{A \in M_2(\mathbb{Z}) \mid \det A = 1\}$$

tiene mucha importancia en aritmética; es conocido como el **grupo modular** y vamos a verlo más adelante. ▲

4.6.8. Ejemplo. Hemos visto que para todo primo p los restos módulo p forman un cuerpo $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Entonces, el anillo de matrices $M_n(\mathbb{F}_p)$ es finito, de orden p^{n^2}, y en particular los grupos $\mathrm{GL}_n(\mathbb{F}_p)$ y $\mathrm{SL}_n(\mathbb{F}_p)$ son también finitos. ¿Cuál es su orden?

El grupo $\mathrm{GL}_n(\mathbb{F}_p)$ consiste de matrices invertibles de $n \times n$. Para contarlas, podemos escribirlas fila por fila (o columna por columna), recordando que entre estas no podemos tener dependencias lineales. En la primera fila podemos escribir cualquier vector $(x_{11}, x_{12}, \ldots, x_{1n})$, salvo el vector nulo $(0, 0, \ldots, 0)$. Tenemos $|\mathbb{F}_p|^n = p^n - 1$ posibilidades. Luego, en la segunda fila podemos poner cualquier vector $(x_{21}, x_{22}, \ldots, x_{2n})$, salvo los $p = |\mathbb{F}_p|$ vectores linealmente dependientes con $(x_{11}, x_{12}, \ldots, x_{1n})$. Continuando de este modo notamos que para la i-ésima fila hay $p^n - p^i$ posibilidades. Entonces, el número de matrices invertibles de $n \times n$ con elementos en un cuerpo finito $\mathbb{F}_p$ es[*]

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1) \cdot (p^n - p) \cdots (p^n - p^{n-1}).$$

[*]En general existen cuerpos finitos $\mathbb{F}_q$ de orden $q = p^k$ donde p es primo. Para $k = 1$ tenemos $\mathbb{F}_q = \mathbb{Z}/p\mathbb{Z}$ y para $k > 1$ omití la construcción por falta de tiempo. Para $\mathbb{F}_q$ la fórmula y su prueba sería idéntica, solo hay que reemplazar "p" por "q".

Para el grupo $\mathrm{SL}_n(\mathbb{F}_p)$ es suficiente notar que si hay una matriz $A \in \mathrm{SL}_n(\mathbb{F}_p)$, es decir, $\det A = 1$, entonces multiplicando A por un escalar $a \in \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$, se obtiene una matriz $A' := a\,A$ con $\det A' = a$. Además, todas las matrices con determinante a se producen de este modo. Esto demuestra que

$$|\,\mathrm{GL}_n(\mathbb{F}_p)| = |\mathbb{F}_p^\times| \cdot |\,\mathrm{SL}_n(\mathbb{F}_p)|;$$

es decir,

$$|\,\mathrm{SL}_n(\mathbb{F}_p)| = \frac{1}{p-1} \cdot |\,\mathrm{GL}_n(\mathbb{F}_p)|.$$

Notamos que para $p = 2$ se tiene

$$\mathrm{GL}_n(\mathbb{F}_2) = \mathrm{SL}_n(\mathbb{F}_2)$$

(de hecho, en $\mathbb{F}_2$ el único elemento no nulo es 1).

Por ejemplo, el grupo $\mathrm{GL}_2(\mathbb{F}_2)$ tiene 6 elementos:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ A := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ B := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ C := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ D := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},\ E := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

He aquí su tabla de multiplicación[*].

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	I	D	E	B	C
B	B	E	I	D	C	A
C	C	D	E	I	A	B
D	D	C	A	B	E	I
E	E	B	C	A	I	D

El siguiente caso no trivial sería de $\mathrm{GL}_2(\mathbb{F}_3)$, y este grupo ya tiene $(3^2-1)\cdot(3^2-3) = 48$ elementos y no es muy instructivo enumerarlos todos...

Sería interesante comparar la tabla de multiplicación de arriba con la tabla de multiplicación en el grupo simétrico S_3.

[*]La compilé con ayuda de computadora para no equivocarme. Favor de no hacer estos cálculos otra vez; verifique alguna fila para ver cómo se multiplican las matrices sobre $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Por ejemplo,

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad (\text{mód } 2).$$

$\circ$	id	(1 2)	(2 3)	(1 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(2 3)	(1 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 2 3)	(1 3 2)	(2 3)	(1 3)
(2 3)	(2 3)	(1 3 2)	id	(1 2 3)	(1 3)	(1 2)
(1 3)	(1 3)	(1 2 3)	(1 3 2)	id	(1 2)	(2 3)
(1 2 3)	(1 2 3)	(1 3)	(1 2)	(2 3)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 3)	(1 2)	id	(1 2 3)

▲

4.7 Ejercicios

Ejercicio 4.1. *Para el anillo de los enteros de Eisenstein $\mathbb{Z}[\zeta_3]$, calcule el grupo de unidades $\mathbb{Z}[\zeta_3]^\times$ y escriba la tabla de multiplicación correspondiente.*
Indicación: considere la norma

$$N(a+b\,\zeta_3) := (a+b\,\zeta_3)\,\overline{(a+b\,\zeta_3)} = a^2 - ab + b^2.$$

Ejercicio 4.2. *Sea R un anillo conmutativo. Se dice que un elemento $u \in R$ es una **unidad** si existe un elemento $u^{-1} \in R$ tal que $uu^{-1} = u^{-1}u = 1$. Se dice que $x \in R$ es un **nilpotente** si existe un número $n = 1, 2, 3, \ldots$ tal que $x^n = 0$.*

Encuentre las unidades y nilpotentes en los anillos $\mathbb{Z}/4\mathbb{Z}$ y $\mathbb{Z}/9\mathbb{Z}$.

Ejercicio 4.3. *Continuemos con las nociones introducidas en el ejercicio precedente. Sea R un anillo conmutativo.*

1) *Demuestre que si $x \in R$ es un nilpotente y $a \in R$ es cualquier elemento del anillo, entonces ax es un nilpotente.*
2) *Demuestre que si $x, y \in R$ son nilpotentes, entonces $x + y$ es también un nilpotente.*
3) *Demuestre que si $x \in R$ es un nilpotente, entonces $1 + x$ es una unidad.*
   Indicación: recuerde la identidad
   $$(1+X)\cdot(1 - X + X^2 - X^3 + X^4 - X^5 + \cdots) = 1$$
   en $R[\![X]\!]$.
4) *Demuestre que si $u \in R$ es una unidad y $x \in R$ es un nilpotente, entonces $u + x$ es una unidad.*

Ejercicio 4.4. *Calcule la matriz inversa para las siguientes matrices:*

$$\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix} \in M_3(\mathbb{F}_3), \quad \begin{pmatrix} 1 & X & 0 \\ 0 & 1 & X \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Z}[X]).$$

Ejercicio 4.5. *Consideremos las matrices de $n \times n$ que tienen 1 en las entradas diagonales, ceros debajo de la diagonal y números arbitrarios arriba de la diagonal.*

$$\{(x_{ij}) \mid x_{ii} = 1 \text{ para todo } i,\ x_{ij} = 0 \text{ para } i > j\}.$$

Por ejemplo, para $n = 3$ son de la forma

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

Demuestre que estas matrices forman un subgrupo de $\mathrm{GL}_n(R)$.

Ejercicio 4.6. *Consideremos el conjunto de matrices*

$$O_n(k) = \{A \in \mathrm{GL}_n(k) \mid A^t\,A = A\,A^t = I\},$$

donde A^t denota la matriz transpuesta.

1) *Demuestre que $O_n(k)$ es un subgrupo de $\mathrm{GL}_n(k)$. Este se llama el **grupo ortogonal** sobre k.*
2) *Para $n = 2$ y $k = \mathbb{R}$ demuestre que los elementos de $O_2(\mathbb{R})$ son de la forma*
   $$\begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix} \quad o \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix}.$$
3) *Demuestre que el grupo diédrico D_n es un subgrupo de $O_2(\mathbb{R})$. Escriba las matrices[*] que corresponden a los*

[*] En este ejercicio hay que identificar las aplicaciones lineales $\mathbb{R}^2 \to \mathbb{R}^2$ con matrices de 2×2.

elementos r y f.

Ejercicio 4.7. *Demuestre que el grupo $\mathrm{SL}_2(\mathbb{Z})$ es infinito.*

Ejercicio 4.8. *Demuestre que las únicas matrices invertibles que conmutan con todas las matrices son las* ***matrices escalares***

$$aI = \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} \quad \text{para } a \in R^\times.$$

Es decir,

$$Z(\mathrm{GL}_n(R)) = \{aI \mid a \in R^\times\}.$$

1) *Fijemos algunos índices $1 \leq i, j \leq n$, $i \neq j$. Denotemos por e_{ij} la matriz de $n \times n$ cuyos coeficientes son nulos, excepto el coeficiente (i, j) que es igual a 1. Consideremos las matrices $I + e_{ij}$. Estas tienen ceros en todas las entradas, excepto 1 en la posición (i, j) y en la diagonal. Demuestre que*

$$\det(I + e_{ij}) = 1$$

En particular, $I + e_{ij} \in \mathrm{GL}_n(R)$.

2) *Supongamos que $A \in Z(\mathrm{GL}_n(R))$. En particular, debe cumplirse*

$$(I + e_{ij})\, A = A\, (I + e_{ij}),$$

que es equivalente a la identidad

$$e_{ij}\, A = A\, e_{ij}$$

en el anillo de matrices $M_n(R)$. Recuerde la tarea anterior donde hemos visto que esto implica que A es una matriz escalar.

3) *Note que el centro de $Z(\mathrm{SL}_n(R))$ también consiste en las matrices escalares (de determinante 1).*

Ejercicio 4.9. *Demuestre que una serie formal de potencias $f = \sum_{i \geq 0} a_i\, X^i \in R[\![X]\!]$ es invertible (pertenece a $R[\![X]\!]^\times$) si y solamente si su coeficiente constante es invertible ($a_0 \in R^\times$).*

Ejercicio 4.10. *Calcule las series $(1 - X)^{-1}$, $(1 - X^2)^{-1}$, $(1 - (X + X^2))^{-1}$ en el anillo $\mathbb{Z}[\![X]\!]$.*

Parte II
Teoría de grupos

Capítulo 5
Homomorfismos

> Les mathématiciens n'étudient pas des objets, mais des relations entre les objets
>
> Poincaré

Hemos visto algunas nociones básicas de grupos y varios ejemplos. Para comparar grupos, estudiar construcciones sobre ellos e investigar sus propiedades más sutiles, hay que saber cómo estos se relacionan. Aquí el concepto clave es el de homomorfismo, una aplicación entre grupos que preserva su estructura (la operación del grupo).

5.0.1. Definición. Un **homomorfismo** de grupos G y H es una aplicación $f\colon G \to H$ tal que para cualesquiera $g_1, g_2 \in G$ se cumple:

$$f(g_1 g_2) = f(g_1)\, f(g_2).$$

5.1 Ejemplos de homomorfismos

5.1.1. Ejemplo. Para todo grupo G la aplicación identidad $\mathrm{id}\colon G \to G$ es un homomorfismo. ▲

5.1.2. Ejemplo. Para ver más homomorfismos familiares, podemos revisar algunas propiedades del análisis real y complejo conocidas a todo el mundo.

1) El signo de un número racional (resp. real) no nulo es un homomorfismo

$$\mathbb{Q}^\times \to \{\pm 1\} \text{ (resp. } \mathbb{R}^\times \to \{\pm 1\}), \quad x \mapsto \operatorname{sgn} x := \begin{cases} +1, & \text{si } x > 0, \\ -1, & \text{si } x < 0, \end{cases}$$

   donde $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ (resp. $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$) es el grupo de los números racionales (resp. reales) no nulos.

2) El valor absoluto de un número racional (resp. real, complejo) no nulo es un homomorfismo

$$\mathbb{Q}^\times \to \mathbb{Q}_{>0}, \text{ (resp. } \mathbb{R}^\times \to \mathbb{R}_{>0}, \mathbb{C}^\times \to \mathbb{R}_{>0}), \quad x \mapsto |x|.$$

   De hecho, para cualesquiera x e y se tiene

$$|xy| = |x| \cdot |y|.$$

3) Consideremos el grupo de los números reales respecto a la adición $\mathbb{R}$ y el grupo de los números reales positivos respecto a la multiplicación $\mathbb{R}_{>0}$. La función exponencial es un homomorfismo

$$\exp\colon \mathbb{R} \to \mathbb{R}_{>0}, \quad x \mapsto e^x.$$

De hecho, para cualesquiera $x, y \in \mathbb{R}$ tenemos

$$e^{x+y} = e^x\, e^y.$$

En general, para $a > 0$, la aplicación

$$\mathbb{R} \to \mathbb{R}^\times, \quad x \mapsto a^x$$

es un homomorfismo: se cumple

$$a^{x+y} = a^x\, a^y.$$

4) Para los números complejos la exponencial es un homomorfismo

$$\exp\colon \mathbb{C} \to \mathbb{C}^\times, \quad z \mapsto e^z.$$

Para cualesquiera $z, w \in \mathbb{C}$ tenemos

$$e^{z+w} = e^z\, e^w.$$

5) El logaritmo natural es un homomorfismo

$$\log\colon \mathbb{R}_{>0} \to \mathbb{R}, \quad x \mapsto \log x;$$

para cualesquiera $x, y > 0$ se cumple

$$\log(xy) = \log(x) + \log(y).$$

En general, para $a > 0$, $a \neq 1$ el logaritmo de base a

$$\log_a\colon \mathbb{R}_{>0} \to \mathbb{R}, \quad x \mapsto \log_a x$$

es un homomorfismo: para cualesquiera $x, y > 0$ se tiene

$$\log_a(xy) = \log_a(x) + \log_a(y).$$

6) La raíz n-ésima es un homomorfismo

$$\mathbb{R}_{>0} \to \mathbb{R}_{>0}, \quad x \mapsto \sqrt[n]{x}.$$

De hecho, tenemos

$$\sqrt[n]{xy} = \sqrt[n]{x} \cdot \sqrt[n]{y}.$$

En general, para cualquier número real positivo $\alpha > 0$ la aplicación

$$\mathbb{R}_{>0} \to \mathbb{R}_{>0}, \quad x \mapsto x^\alpha$$

es un homomorfismo: se tiene

$$(xy)^\alpha = x^\alpha\, y^\alpha.$$

7) La conjugación compleja $z \mapsto \overline{z}$ es un homomorfismo aditivo y multiplicativo a la vez:

$$\mathbb{C} \to \mathbb{C} \quad \text{y} \quad \mathbb{C}^\times \to \mathbb{C}^\times.$$

Para cualesquiera z, w se cumple

$$\overline{z+w} = \overline{z} + \overline{w}, \quad \overline{zw} = \overline{z}\,\overline{w}.$$

▲

5.1.3. Ejemplo. En el primer capítulo hemos estudiado el signo de permutación

$$\operatorname{sgn}\colon S_n \to \{\pm 1\}$$

que es un homomorfismo entre el grupo simétrico y el grupo multiplicativo $\{\pm 1\}$. De hecho, hemos visto que para cualesquiera $\sigma, \tau \in S_n$ se cumple

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau.$$

▲

5.1.4. Ejemplo. El determinante de matrices invertibles de $n \times n$ es un homomorfismo de grupos

$$\det\colon \mathrm{GL}_n(R) \to R^\times.$$

▲

5.1.5. Ejemplo. La reducción módulo n es un homomorfismo de grupos aditivos

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}, \\ a &\mapsto [a]_n. \end{aligned}$$

En efecto, $[a+b]_n = [a]_n + [b]_n$ por la misma definición de la adición de los restos módulo n (recordemos que uno tiene que verificar por separado que esta adición no depende de los representantes particulares de las clases de equivalencia).

Si $n \mid m$, entonces tenemos un homomorfismo de grupos aditivos

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}, \\ [a]_m &\mapsto [a]_n. \end{aligned}$$

De hecho, primero notamos que esta aplicación está bien definida: si $a \equiv a' \pmod{m}$, esto quiere decir que $m \mid (a - a')$, pero luego $n \mid (a - a')$, así que $a \equiv a' \pmod{n}$. Es un homomorfismo por la definición de la adición módulo m y n:

$$[a]_m + [b]_m = [a+b]_m = [a+b]_n = [a]_n + [b]_n.$$

De la misma manera, se ve que hay un homomorfismo de grupos multiplicativos

$$\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^\times &\to (\mathbb{Z}/n\mathbb{Z})^\times, \\ [a]_m &\mapsto [a]_n. \end{aligned}$$

▲

5.1.6. Ejemplo. Para un número entero no nulo $n \in \mathbb{Z} \setminus \{0\}$ su **valuación p-ádica** es el máximo número natural k tal que p^k divide a n:

$$v_p(n) := \max\{k \mid p^k \mid n\}.$$

(Para $n = 0$ normalmente se define $v_p(0) := +\infty$, pero no vamos a usar esta convención.)

Ahora para dos números no nulos $m, n \in \mathbb{Z}$ se puede escribir

$$m = p^{v_p(m)}\, m', \quad n = p^{v_p(n)}\, n',$$

donde $p \nmid m'$ y $p \nmid n'$, y luego,

$$mn = p^{v_p(m)+v_p(n)}\, m'n',$$

donde $p \nmid (m'n')$, así que

$$v_p(mn) = v_p(m) + v_p(n).$$

Ahora todo número racional no nulo puede ser representado por una fracción m/n, donde $m, n \neq 0$ son algunos números enteros. Podemos definir

$$v_p\left(\frac{m}{n}\right) := v_p(m) - v_p(n).$$

Esta definición depende del número racional y no de su representación como fracción. De hecho, tenemos

$$\frac{m}{n} = \frac{m'}{n'} \iff mn' = m'n.$$

Ahora

$$v_p(m) + v_p(n') = v_p(mn') = v_p(m'n) = v_p(m') + v_p(n),$$

así que

$$v_p\left(\frac{m}{n}\right) := v_p(m) - v_p(n) = v_p(m') - v_p(n') =: v_p\left(\frac{m'}{n'}\right).$$

Esto significa que la función

$$\begin{aligned} v_p \colon \mathbb{Q}^\times &\to \mathbb{Z}, \\ \frac{m}{n} &\mapsto v_p\left(\frac{m}{n}\right) := v_p(m) - v_p(n) \end{aligned}$$

está bien definida. Es un homomorfismo entre el grupo multiplicativo $\mathbb{Q}^\times$ y el grupo aditivo $\mathbb{Z}$: para cualesquiera $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in \mathbb{Q}^\times$ tenemos

$$\begin{aligned} v_p\left(\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}\right) = v_p\left(\frac{m_1 m_2}{n_1 n_2}\right) = v_p(m_1 m_2) - v_p(n_1 n_2) &= v_p(m_1) - v_p(n_1) + v_p(m_2) - v_p(n_2) \\ &= v_p\left(\frac{m_1}{n_1}\right) + v_p\left(\frac{m_2}{n_2}\right). \end{aligned}$$

Si en lugar de $\mathbb{Z}$ queremos trabajar con un grupo multiplicativo, podemos definir el **valor absoluto p-ádico** de $x \in \mathbb{Q}^\times$ como sigue:

$$|x|_p := p^{-v_p(x)}.$$

Entonces, para cualesquiera $x, y \in \mathbb{Q}^\times$ se cumple

$$|x\,y|_p = p^{-v_p(xy)} = p^{-v_p(x)} \cdot p^{-v_p(y)} = |x|_p \cdot |y|_p.$$

De esta manera se obtiene un homomorfismo de grupos multiplicativos

$$\begin{aligned} |\cdot|_p \colon \mathbb{Q}^\times &\to \mathbb{R}_{>0}, \\ x &\mapsto |x|_p. \end{aligned}$$

(Para $x = 0$ se define $|0|_p := 0$, lo que concuerda con la definición $v_p(0) := \infty$.) ▲

5.1.7. Ejemplo. He aquí otro ejemplo curioso de la teoría de números. Para un número primo p, decimos que un entero $a \in \mathbb{Z}$ es un **cuadrado módulo** p si

$$a \equiv b^2 \pmod{p}$$

para algún $b \in \mathbb{Z}$. Podemos definir el **símbolo de Legendre** mediante

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{si } p \nmid a \text{ y } a \text{ es un cuadrado módulo } p, \\ -1, & \text{si } p \nmid a \text{ y } a \text{ no es un cuadrado módulo } p, \\ 0, & \text{si } p \mid a. \end{cases}$$

Obviamente, si $a \equiv a' \pmod{p}$, entonces

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right),$$

así que el símbolo de Legedre está definido sobre los restos módulo p. Luego, para cualesquiera $a, b \in \mathbb{Z}$ se tiene

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(está claro que el producto de dos cuadrados es un cuadrados; un poco menos claro que el producto de dos no-cuadrados es un cuadrado, pero lo veremos más adelante). Esto quiere decir que el símbolo de Legendre es un homomorfismo de grupos multiplicativos

$$\begin{aligned} \left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times &\to \{\pm 1\}, \\ [a]_p &\mapsto \left(\frac{a}{p}\right). \end{aligned}$$

▲

Las siguientes aplicaciones son homomorfismos por la definición de las estructuras algebraicas correspondientes.

5.1.8. Ejemplo.

1) Si R es un anillo (no necesariamente conmutativo) y $c \in R$ su elemento fijo, entonces la multiplicación por c por la izquierda es un homomorfismo de grupos aditivos

$$R \to R, \quad x \mapsto cx.$$

En efecto, la multiplicación es distributiva por la definición de anillos: para cualesquiera $x, y \in R$ debe cumplirse

$$c\,(x + y) = cx + cy.$$

De la misma manera, la multiplicación por la derecha es un homomorfismo

$$R \to R, \quad x \mapsto xc.$$

2) Si V es un espacio vectorial sobre un cuerpo k y $\lambda \in k$ es un escalar fijo, entonces la multiplicación por λ es un homomorfismo de grupos aditivos

$$V \to V, \quad v \mapsto \lambda \cdot v.$$

En efecto, según los axiomas de espacios vectoriales, se tiene

$$\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v.$$

3) Recordemos que para un anillo conmutativo R y un polinomio

$$f = \sum_{0 \leq i \leq n} a_i \, X^i \in R[X],$$

su valor en $c \in R$ viene dado por

$$f(c) = \sum_{0 \leq i \leq n} a_i \, c^i \in R.$$

Esto nos da un **homomorfismo de evaluación**

$$ev_c \colon R[X] \to R, \quad f \mapsto f(c).$$

▲

5.1.9. Digresión. En los ejercicios hemos mencionado el anillo de series de potencias $R[\![X]\!]$. En general, ya que una suma $f = \sum_{i \geq 0} a_i \, X^i \in R[\![X]\!]$ puede tener un número infinito de coeficientes no nulos, no tiene sentido evaluar f en un elemento $c \in R$. Lo que siempre podemos hacer es "evaluar f en 0":

$$\begin{gathered} R[\![X]\!] \to R, \\ f = \sum_{i \geq 0} a_i \, X^i \mapsto f(0) = a_0. \end{gathered}$$

En general, evaluación de una serie $f \in R[\![X]\!]$ en un elemento arbitrario $c \in R$ requiere de una noción de convergencia.

5.1.10. Ejemplo. Si A es un grupo abeliano, entonces para $n \in \mathbb{Z}$ y para cualesquiera $a, b \in A$ tenemos

$$n \cdot (a + b) := \underbrace{(a + b) + \cdots + (a + b)}_{n} = \underbrace{a + \cdots + a}_{n} + \underbrace{b + \cdots + b}_{n} = n \cdot a + n \cdot b,$$

así que la multiplicación por n es un homomorfismo que se denota por

$$A \xrightarrow{\times n} A$$

Cuando el grupo es abeliano, pero se usa la notación multiplicativa, se trata de las potencias n-ésimas $a \mapsto a^n$:

$$(ab)^n := \underbrace{ab \cdots ab}_{n} = \underbrace{a \cdots a}_{n} \cdot \underbrace{b \cdots b}_{n} =: a^n b^n.$$

Note que en un grupo no abeliano, en general $(gh)^n \neq g^n \, h^n$. Por ejemplo, se puede ver que G es abeliano si y solamente si $(gh)^2 = g^2 \, h^2$ para cualesquiera $g, h \in G$. ▲

5.1.11. Ejemplo. En particular, si R es un anillo conmutativo y $n \in \mathbb{Z}$, entonces la n-ésima potencia es un homomorfismo de grupos multiplicativos

$$R^\times \to R^\times, \quad x \mapsto x^n.$$

Para el grupo aditivo subyacente, tenemos

$$(x+y)^n = \sum_{0 \le i \le n} \binom{n}{i} x^i\, y^{n-i},$$

y esta expresión normalmente no es igual a $x^n + y^n$. Sin embargo, si en R se cumple $p \cdot x$ para cualesquiera $x \in R$, por ejemplo para $R = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, entonces

$$(x+y)^p = x^p + y^p.$$

Por ejemplo,

$$\mathbb{F}_p \to \mathbb{F}_p, \quad x \mapsto x^n$$

es un homomorfismo de grupos aditivos. ▲

5.2 Propiedades básicas de homomorfismos

5.2.1. Observación. *La composición de dos homomorfismos $f_1 \colon G \to G'$ y $f_2 \colon G' \to G''$ es un homomorfismo $f_2 \circ f_1 \colon G \to G''$.*

Demostración. Para cualesquiera $g_1, g_2 \in G$ tenemos

$$(f_2 \circ f_1)(g_1 g_2) = f_2(f_1(g_1 g_2)) = f_2(f_1(g_1)\, f_1(g_2)) = f_2(f_1(g_1)) \cdot f_2(f_1(g_2)) = (f_2 \circ f_1)(g_1) \cdot (f_2 \circ f_1)(g_2).$$

■

5.2.2. Observación (Homomorfismos preservan el elemento neutro). *Si $f \colon G \to H$ es un homomorfismo, entonces*

$$f(1_G) = 1_H$$

Demostración. Tenemos

$$f(1_G) = f(1_G \cdot 1_G) = f(1_G) \cdot f(1_G),$$

y por lo tanto $f(1_G)$ es el elemento neutro. ■

5.2.3. Observación (Homomorfismos preservan los elementos inversos). *Si $f \colon G \to H$ es un homomorfismo, entonces para todo $g \in G$*

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

Demostración.

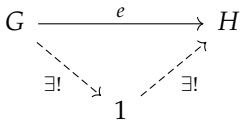
$$f(g^{-1}) \cdot f(g) = f(g^{-1} g) = f(1) = 1.$$

■

5.2.4. Observación. *Sea 1 el grupo trivial. Para todo grupo G existe un homomorfismo único $1 \to G$ y un homomorfismo único $G \to 1$.*

Note que la situación con conjuntos es diferente: allí para todo X existe una aplicación única $\varnothing \to X$ y una aplicación única $X \to \{\bullet\}$. Los conjuntos $\varnothing$ y $\{\bullet\}$ son diferentes (entre ellos no hay biyección). En el caso de grupos, el mismo grupo trivial 1 satisface ambas propiedades $1 \xrightarrow{\exists!} G$ y $G \xrightarrow{\exists!} 1$.

5.2.5. Corolario. *Para dos grupos G y H existe un homomorfismo único $e\colon G \to H$ que se factoriza por el grupo trivial:*



*Este se llama el **homomorfismo trivial** y está definido por*

$$e(g) = 1_H \quad \textit{para todo } g \in G.$$

5.2.6. Ejemplo. Para el signo de permutaciones tenemos

$$\operatorname{sgn}(\mathrm{id}) = +1$$

y

$$\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)^{-1} = \operatorname{sgn}(\sigma).$$

▲

5.2.7. Observación (Homomorfismos preservan potencias). *Para todo $n \in \mathbb{Z}$ tenemos*

$$f(g^n) = f(g)^n.$$

Demostración. Inducción sobre n. La base es el caso de $n = 0$ que corresponde a 5.2.2. Si $n < 0$, aplicamos 5.2.3. ■

5.2.8. Corolario. *Si $g^n = 1$, entonces $f(g)^n = 1$.*

5.3 Mono, epi, iso

5.3.1. Definición (clásica). Sea $f\colon G \to H$ un homomorfismo de grupos.

1) Si f es una aplicación inyectiva, se dice que f es un **monomorfismo** y se escribe $f\colon G \rightarrowtail H$.
2) Si f es una aplicación sobreyectiva, se dice que f es un **epimorfismo** y se escribe $f\colon G \twoheadrightarrow H$.
3) Si f es una aplicación biyectiva, se dice que f es un **isomorfismo** y se escribe $f\colon G \xrightarrow{\cong} H$.

   Cuando entre G y H existe un isomorfismo $G \xrightarrow{\cong} H$, se dice que G y H son grupos **isomorfos** y se escribe $G \cong H$.

En lugar de los sustantivos *monomorfismo*, *epimorfismo*, *isomorfismo* a veces se usan los adjetivos *mono*, *epi*, *iso*, por ejemplo "f es mono".

5.3.2. Ejemplo. Si $G \subset H$ es un subgrupo, la inclusión $G \hookrightarrow H$ es un monomorfismo de grupos. ▲

5.3.3. Ejemplo. Los homomorfismos

$$\det\colon \mathrm{GL}_n(R) \to R^\times$$

y

$$\operatorname{sgn}\colon S_n \to \{\pm 1\}$$

son epi. ▲

5.3.4. Ejemplo. La exponencial compleja

$$\exp\colon \mathbb{C} \to \mathbb{C}^\times, \quad z \mapsto e^z$$

es epi, pero no es mono: para cualesquiera $z \in \mathbb{C}$, $k \in \mathbb{Z}$ tenemos $e^z = e^{z+2\pi ik}$. ▲

5.3.5. Ejemplo. Se ve que la aplicación $f\colon x \mapsto x^p$ es un isomorfismo de grupos aditivos $\mathbb{F}_p \to \mathbb{F}_p$ y grupos multiplicativos $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$. De hecho,

$$f(x) = f(y) \iff x^p = y^p \iff (x-y)^p = x - y = 0,$$

donde la igualdad $(x-y)^p = x - y$ es el pequeño teorema de Fermat. ▲

5.3.6. Ejemplo. Un grupo puede ser isomorfo a un subgrupo propio. Obviamente, es imposible para grupos finitos, pero para grupos infinitos, por ejemplo, tenemos un isomorfismo

$$\begin{aligned} \mathbb{Z} &\to 2\mathbb{Z} := \{2n \mid n \in \mathbb{Z}\}, \\ n &\mapsto 2n. \end{aligned}$$

▲

5.3.7. Ejemplo. Sean X e Y dos conjuntos tales que existe una biyección $f\colon X \to Y$. Una elección de f induce un isomorfismo entre los grupos simétricos

$$\begin{aligned} S_X &\to S_Y, \\ (X \xrightarrow{\sigma} X) &\mapsto (Y \xrightarrow{f^{-1}} X \xrightarrow{\sigma} X \xrightarrow{f} Y). \end{aligned}$$

De hecho, es un homomorfismo de grupos:

$$f \circ (\sigma \circ \tau) \circ f^{-1} = (f \circ \sigma \circ f^{-1}) \circ (f \circ \tau \circ f^{-1}).$$

Es inyectivo, ya que f y f^{-1} son cancelables, siendo biyecciones:

$$f \circ \sigma \circ f^{-1} = f \circ \tau \circ f^{-1} \Rightarrow \sigma = \tau.$$

Es sobreyectivo: para toda biyección $\phi\colon Y \to Y$, consideremos la biyección $\sigma\colon X \to X$ dada por

$$X \xrightarrow{f} Y \xrightarrow{\phi} Y \xrightarrow{f^{-1}} X$$

Entonces

$$f \circ \sigma \circ f^{-1} = f \circ (f^{-1} \circ \phi \circ f) \circ f^{-1} = \phi.$$

En particular, el grupo de permutaciones de los elementos de un conjunto finito X es isomorfo a S_n donde $n = |X|$. ▲

5.3.8. Ejemplo. Dado un cuerpo k consideremos el espacio vectorial k^n junto con su base estándar

$$e_1 = (1,0,0,\ldots,0),\ e_2 = (0,1,0,\ldots,0),\ \ldots,\ e_n = (0,0,0,\ldots,1).$$

En los cursos de álgebra lineal se estudia que las aplicaciones lineales $k^n \to k^n$ pueden ser representadas por las matrices de $n \times n$, de tal modo que la composición de aplicaciones lineales corresponde a la

multiplicación de matrices. Aplicaciones lineales invertibles corresponden a matrices invertibles. Esto nos da un isomorfismo de grupos

$$\mathrm{GL}(k^n) \cong \mathrm{GL}_n(k).$$

Cuidado: en general, si V es cualquier espacio vectorial sobre k de dimensión n, una *elección de base* nos da un isomorfismo de espacios vectoriales $f\colon V \xrightarrow{\cong} k^n$, y por lo tanto un isomorfismo de grupos

$$\begin{aligned}\mathrm{GL}(V) &\xrightarrow{\cong} \mathrm{GL}(k^n),\\ (\phi\colon V \to V) &\mapsto (f \circ \phi \circ f^{-1}\colon k^n \to k^n),\end{aligned}$$

pero este no es canónico ya que depende de la base escogida. ▲

5.3.9. Observación. *$f\colon G \to H$ es iso si y solamente si es invertible: existe otro homomorfismo de grupos $f^{-1}\colon H \to G$ tal que*

$$f^{-1} \circ f = \mathrm{id}_G, \quad f \circ f^{-1} = \mathrm{id}_H.$$

Demostración. Para $h_1, h_2 \in H$ tenemos

$$f^{-1}(h_1h_2) = f^{-1}\Big(f(f^{-1}(h_1)) \cdot f(f^{-1}(h_2))\Big) = f^{-1}\Big(f\big(f^{-1}(h_1) \cdot f^{-1}(h_2)\big)\Big) = f^{-1}(h_1) \cdot f^{-1}(h_2),$$

donde la primera igualdad viene de $f \circ f^{-1} = \mathrm{id}_H$, la segunda igualdad se cumple porque f es un homomorfismo, y la tercera igualdad viene de $f^{-1} \circ f = \mathrm{id}_G$. ■

5.3.10. Ejemplo. La exponencial real

$$\exp\colon \mathbb{R} \to \mathbb{R}_{>0}, \quad x \mapsto \exp(x)$$

es un isomorfismo de grupos que posee una aplicación inversa, a saber el logaritmo:

$$\log\colon \mathbb{R}_{>0} \to \mathbb{R}_{>0}, \quad x \mapsto \log(x).$$

Como hemos visto, la aplicación inversa es automáticamente un homomorfismo:

$$\log(xy) = \log(x) + \log(y).$$

▲

5.3.11. Corolario. *La isomorfía de grupos es una relación de equivalencia en el sentido de que para cualesquiera G, H, K tenemos*

$$G \cong G, \quad G \cong H \Rightarrow H \cong G, \quad G \cong H, H \cong K \Rightarrow G \cong K.$$

5.3.12. Ejemplo. Salvo isomorfismo, los primeros grupos finitos son

1) el grupo trivial 1;
2) el grupo $\mathbb{Z}/2\mathbb{Z}$;
3) el grupo $\mathbb{Z}/3\mathbb{Z}$;
4) el grupo $\mathbb{Z}/4\mathbb{Z}$ y el grupo de cuatro $V = \{\mathrm{id}, (1\,2)\,(3\,4), (1\,3)\,(2\,4), (1\,4)\,(2\,3)\} \subset A_4$;
5) el grupo $\mathbb{Z}/5\mathbb{Z}$;
6) el grupo simétrico S_3, que es isomorfo al grupo diédrico D_3;

7) el grupo $\mathbb{Z}/7\mathbb{Z}$;

8) hay tres grupos abelianos de orden 8: uno de ellos es $\mathbb{Z}/8\mathbb{Z}$ y otros dos que vamos a construir más adelante; además, hay dos grupos no abelianos que ya conocemos: el grupo diédrico D_4 y el grupo de cuaterniones Q_8.

Más adelante veremos que para todo primo p hay un grupo único de orden p salvo isomorfismo y es el grupo $\mathbb{Z}/p\mathbb{Z}$. También vamos a describir todos los grupos *abelianos* finitos salvo isomorfismo. Es muy difícil clasificar los grupos *no abelianos* finitos y no vamos a tocar el tema. ▲

Cuando dos grupos son isomorfos, estos pueden ser identificados, salvo alguna permutación de elementos que respecta la operación del grupo. En particular, dos grupos isomorfos tienen las mismas propiedades.

5.3.13. Observación. *Si $G \cong H$, entonces G es abeliano si y solamente si H es abeliano.*

5.3.14. Ejemplo. Ya que todo isomorfismo $G \xrightarrow{\cong} H$ es una biyección de conjuntos, si G y H tienen diferente cardinalidad, estos no pueden ser isomorfos. Los grupos $\mathbb{Z}/6\mathbb{Z}$ y S_3 tienen la misma cardinalidad $6 = 3!$. Sin embargo, $\mathbb{Z}/6\mathbb{Z}$ es un grupo abeliano, mientras que S_3 no lo es, y por lo tanto no son isomorfos. ▲

5.3.15. Definición. Fijemos un grupo G. Un isomorfismo entre G y sí mismo se llama un **automorfismo**.

5.3.16. Observación. *Los automorfismos de G forman un grupo respecto a la composición. Este se denota por* $\mathrm{Aut}(G)$.

Demostración. Siempre existe el automorfismo identidad $\mathrm{id}\colon G \to G$ y es el elemento neutro de $\mathrm{Aut}(G)$. Si $f_1\colon G \to G$ y $f_2\colon G \to G$ son dos automorfismos, entonces su composición $f_2 \circ f_1\colon G \to G$ es también un automorfismo. Todo automorfismo $f\colon G \to G$ posee una aplicación inversa $f^{-1}\colon G \to G$, y como hemos visto arriba, es automáticamente un automorfismo. ■

5.3.17. Ejemplo. El grupo $\mathbb{Z}/3\mathbb{Z}$ respecto a la adición tiene dos automorfismos: id y un automorfismo no trivial

$$f\colon [0] \mapsto [0], \quad [1] \mapsto [2], \quad [2] \mapsto [1].$$

Tenemos $f \circ f = \mathrm{id}$ y luego $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. ▲

5.4 Imágenes

5.4.1. Definición. Sea $f\colon G \to H$ un homomorfismo de grupos. El conjunto

$$\mathrm{im}\, f := \{f(g) \mid g \in G\}$$

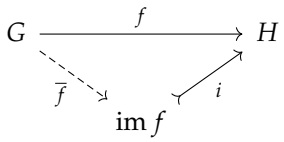
se llama la **imagen** de f.

5.4.2. Observación. *Para todo homomorfismo $f\colon G \to H$ la imagen* $\mathrm{im}\, f$ *es un subgrupo de H.*

Demostración. Como hemos notado en 5.2.2, tenemos $1_H \in \mathrm{im}\, f$. Luego, si $f(g_1), f(g_2) \in \mathrm{im}\, f$, entonces $f(g_1)\, f(g_2) = f(g_1 g_2) \in \mathrm{im}\, f$. En fin, gracias a 5.2.3, si $f(g) \in \mathrm{im}\, f$, entonces $f(g)^{-1} = f(g^{-1}) \in \mathrm{im}\, f$. ■

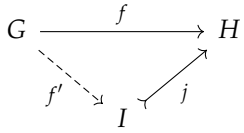
5.4.3. Proposición (Propiedad universal de la imagen). *Sea $f\colon G \to H$ un homomorfismo de grupos.*

1) Existe una factorización de f por el monomorfismo canónico $i\colon \operatorname{im} f \rightarrowtail H$ (inclusión de subgrupo):



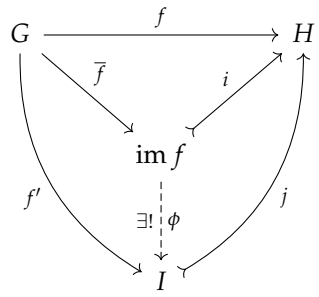
$$f = i \circ \overline{f}.$$

2) Supongamos que hay otro grupo I junto con un monomorfismo $j\colon I \rightarrowtail H$ y una factorización de f por I:



$$f = j \circ f'.$$

Luego existe un único homomorfismo $\phi\colon \operatorname{im} f \to I$ que hace conmutar el siguiente diagrama:



$$\phi \circ \overline{f} = f', \quad j \circ \phi = i.$$

(ϕ es mono, puesto que $i = j \circ \phi$ lo es).

Demostración. La parte 1) está clara de la definición de la imagen: ya que f toma sus valores en $\operatorname{im} f \subset H$, en realidad f puede ser vista como una aplicación $\overline{f}\colon G \to \operatorname{im} f$. Es un homomorfismo, puesto que f es un homomorfismo. Su composición con la inclusión del subgrupo $i\colon \operatorname{im} f \rightarrowtail H$ coincide con f.

En 2), la única opción para ϕ para que se cumpla $\phi \circ \overline{f} = f'$ es definir

$$\begin{aligned} \phi\colon & \operatorname{im} f \to I, \\ & f(g) \mapsto f'(g). \end{aligned}$$

Esta aplicación está bien definida: si tenemos $f(g_1) = f(g_2)$, entonces

$$j(f'(g_1)) = f(g_1) = f(g_2) = j(f'(g_2)) \Rightarrow f'(g_1) = f'(g_2).$$

También se cumple $i = j \circ \phi$. En efecto, para $h = f(g) \in \operatorname{im} f$ tenemos

$$j(\phi(h)) = j(f'(g)) = f(g).$$

■

5.4.4. Observación. *Todo monomorfismo $f\colon G \rightarrowtail H$ corresponde a un isomorfismo*

$$G \xrightarrow{\cong} \operatorname{im} f \subset H.$$

5.4.5. Ejemplo. Toda permutación $\sigma \in S_n$ puede ser extendida a una permutación de $\{1, \ldots, n, n+1\}$ poniendo

$$\sigma(n+1) := n+1.$$

Esto define un monomorfismo

$$S_n \rightarrowtail S_{n+1}.$$

De este modo S_n se identifica con un subgrupo de S_{n+1}. En este sentido, tenemos una cadena de subgrupos

$$S_1 \subset S_2 \subset S_3 \subset S_4 \subset S_5 \subset \cdots$$

y podemos considerar su unión

$$S_\infty := \bigcup_{n \geq 1} S_n.$$

Este grupo permuta los elementos de $\{1, 2, 3, \ldots\}$, pero para cada $\sigma \in S_\infty$ tenemos $\sigma(i) = i$ para todo i, excepto un número finito. ▲

Es algo parecido al grupo $\mu_\infty(\mathbb{C}) := \bigcup_{n \geq 1} \mu_n(\mathbb{C})$.

5.4.6. Ejemplo. A una matriz invertible $A \in \mathrm{GL}_n(R)$ podemos asociar una matriz invertible $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_{n+1}(R)$ poniendo 1 en la entrada $(n+1, n+1)$. En este sentido se obtiene una cadena de subgrupos

$$\mathrm{GL}_1(R) \subset \mathrm{GL}_2(R) \subset \mathrm{GL}_3(R) \subset \mathrm{GL}_4(R) \subset \cdots$$

Luego, se obtiene un grupo

$$\mathrm{GL}_\infty(R) := \bigcup_{n \geq 1} \mathrm{GL}_n(R).$$

Este consiste en matrices infinitas, pero cada una de ellas afecta solamente la parte finita de $R \times R \times R \times \cdots$ y deja el resto intacto. ▲

5.5 Núcleos

5.5.1. Definición. Sea $f\colon G \to H$ un homomorfismo de grupos. El conjunto

$$\ker f := \{g \in G \mid f(g) = 1_H\}$$

se llama el **núcleo** de f.

A priori f es un subconjunto de G, pero en realidad, es su subgrupo.

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

Demostración. Primero, $f(1_G) = 1_H$ (véase 5.2.2), entonces $1_G \in \ker f$. Luego, $f(g_1 g_2) = f(g_1)\, f(g_2)$, así que

$$g_1, g_2 \in \ker f \Rightarrow g_1 g_2 \in \ker f.$$

Por último, para todo $x \in \ker f$ tenemos

$$f(g^{-1}) = f(g)^{-1} = (1_H)^{-1} = 1_H,$$

así que también $g^{-1} \in \ker f$. ■

5.5.3. Ejemplo. Por la definición, el grupo alternante es el núcleo del homomorfismo de signo:

$$A_n := \ker(S_n \xrightarrow{\text{sgn}} \{\pm 1\}).$$

▲

5.5.4. Ejemplo. Tenemos

$$\ker(\mathbb{R}^\times \xrightarrow{\text{sgn}} \{\pm 1\}) = \mathbb{R}_{>0}.$$

▲

5.5.5. Ejemplo. Por definición, el grupo $\mathrm{SL}_n(R)$ es el núcleo del homomorfismo del determinante sobre $\mathrm{GL}_n(R)$:

$$\mathrm{SL}_n(R) := \ker(\mathrm{GL}_n(R) \xrightarrow{\det} R^\times).$$

▲

5.5.6. Ejemplo. Por definición, el grupo de las n-ésimas raíces de la unidad $\mu_n(\mathbb{C})$ es el núcleo del homomorfismo $z \mapsto z^n$ sobre $\mathbb{C}^\times$:

$$\mu_n(\mathbb{C}) := \ker(\mathbb{C}^\times \xrightarrow{(-)^n} \mathbb{C}^\times).$$

▲

5.5.7. Observación. *Un homomorfismo $f\colon G \to H$ es mono si y solamente si* $\ker f = \{1_G\}$.

Demostración. Tenemos que ver que f es una aplicación inyectiva. Primero notamos que si $\ker f$ contiene otro elemento $g \neq 1_G$, entonces

$$f(g) = f(1_G) = 1_H,$$

así que f no es inyectiva. Entonces, la condición $\ker f = \{1_G\}$ es necesaria. Para ver que es también suficiente, notamos que si $f(g_1) = f(g_2)$ para $g_1, g_2 \in G$, entonces

$$f(g_1 g_2^{-1}) = f(g_1) f(g_2^{-1}) = f(g_1) f(g_2)^{-1} = 1_H,$$

así que $g_1 = g_2$. ■

5.5.8. Ejemplo. Para la exponente compleja

$$\exp\colon \mathbb{C} \to \mathbb{C}^\times, \quad z \mapsto e^z$$

se tiene

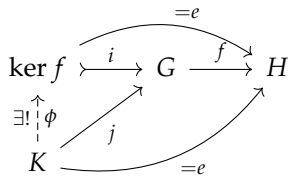
$$\ker(\exp\colon \mathbb{C} \to \mathbb{C}^\times) = 2\pi i\,\mathbb{Z} = \{2\pi i n \mid n \in \mathbb{Z}\} \subset \mathbb{C}.$$

Por esto en el caso complejo, el logaritmo es más sutil: la exponencial toma el mismo valor en $z + 2\pi i n$ para todo $n \in \mathbb{Z}$, lo que impide definir una función inversa $\log\colon \mathbb{C}^\times \to \mathbb{C}$. ▲

5.5.9. Proposición (Propiedad universal del núcleo). *Para un homomorfismo de grupos $f\colon G \to H$, sea* $\ker f$ *su núcleo y sea $i\colon \ker f \rightarrowtail G$ la inclusión.*

1) *La composición* $\ker f \xrightarrow{i} G \xrightarrow{f} H$ *es el homomorfismo trivial.*

2) *Si $j\colon K \to G$ es otro morfismo tal que la composición $K \xrightarrow{j} G \xrightarrow{f} H$ es trivial, entonces existe un único homomorfismo de grupos $\phi\colon K \to \ker f$ tal que $i \circ \phi = j$.*



Demostración. La parte 1) es evidente de la definición de $\ker f$. En la parte 2), tenemos $f(j(x)) = 1$ para todo $x \in K$. Entonces, $\operatorname{im} j \subseteq \ker f$, y esto nos da la factorización única de $j\colon K \to G$ por $\ker f$. ■

5.5.10. Observación. *Si tenemos un diagrama conmutativo de homomorfismos de grupos*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ G' & \xrightarrow[f']{} & H' \end{array}$$

entonces existe una único homomorfismo $\ker f \to \ker f'$ *que hace conmutar el diagrama*

$$\begin{array}{ccccc} \ker f & \rightarrowtail & G & \xrightarrow{f} & H \\ \downarrow{\scriptstyle\exists!} & & {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ \ker f' & \rightarrowtail & G' & \xrightarrow[f']{} & H' \end{array}$$

Demostración. La flecha punteada existe y es única gracias a la propiedad universal de $\ker f'$, pero es nada más la restricción de ϕ a $\ker f$. Tenemos que comprobar que su imagen pertenece a $\ker f'$. Si $g \in \ker f$, entonces $f(g) = 1$, y por lo tanto $f'(\phi(g)) = \psi(f(g)) = 1$ y $\phi(g) \in \ker f'$, y la aplicación $g \mapsto \phi(g)$ se restringe correctamente a $\ker f \to \ker f'$. ■

5.6 Caracterización de mono, epi, iso

5.6.1. Proposición. *Un homomorfismo de grupos* $f\colon G \to H$ *es inyectivo si y solamente si es cancelable por la izquierda: para todo par de homomorfismos de grupos*

$$g, g'\colon G' \to G$$

tenemos

$$f \circ g = f \circ g' \Rightarrow g = g'.$$

Demostración. Si $f\colon G \to H$ es una aplicación inyectiva, entonces es cancelable por la izquierda para todas *aplicaciones entre conjuntos* g, g' (no necesariamente homomorfismos de grupos) como hemos notado en el capítulo 0.

La otra dirección es un poco más sútil: necesitamos ver que si un homomorfismo f es cancelable por la izquierda para homomorfismos de grupos g, g', entonces es inyectivo. Consideramos la inclusión canónica $i\colon \ker f \to G$ y el homomorfismo trivial $e\colon \ker f \to G$. Entonces,

$$f \circ i = f \circ e$$

—ambas composiciones nos dan un homomorfismo trivial $\ker f \to H$. Si f es cancelable por la izquierda, esto implica $i = e$; es decir, que $\ker f = \{1_G\}$ y por lo tanto f es inyectivo gracias a 5.5.7. ■

Entonces, para homomorfismos de grupos $f\colon G \to H$ tenemos las equivalencias

$$\begin{aligned} f \text{ es un homomorfismo inyectivo} &\iff f \text{ es cancelable por la izquierda} \\ &\quad (f \circ g = f \circ g' \Rightarrow g = g' \text{ para homomorfismos } g, g'), \\ f \text{ es un homomorfismo biyectivo} &\iff f \text{ es invertible (existe homomorfismo } f^{-1}). \end{aligned}$$

El lector puede adivinar que también existe otra equivalencia

$$\begin{aligned} f \text{ es un homomorfismo sobreyectivo} &\iff f \text{ es cancelable por la derecha} \\ &\quad (g \circ f = g' \circ f \Rightarrow g = g' \text{ para homomorfismos } g, g'). \end{aligned}$$

Aquí la implicación "$\Rightarrow$" es fácil (véase el capítulo 0), pero la otra implicación "$\Leftarrow$" es más difícil y no la vamos a probar.

5.7 Ejercicios

Ejercicio 5.1. *Sea R un anillo conmutativo. Para una matriz invertible $A \in \mathrm{GL}_n(R)$ definamos su matriz **transpuesta inversa** por $A^{-t} := (A^{-1})^t = (A^t)^{-1}$. Demuestre que la aplicación $A \mapsto A^{-t}$ es un automorfismo $\mathrm{GL}_n(R) \to \mathrm{GL}_n(R)$.*

Ejercicio 5.2. *Sea G cualquier grupo, $\mathbb{Z}$ el grupo aditivo de los números enteros y $\mathbb{Q}$ el grupo aditivo de los números racionales.*

1) *Demuestre que todo homomorfismo $f\colon \mathbb{Z} \to G$ está definido de modo único por el valor de $f(1) \in G$. Esto nos da una biyección natural*

$$\mathrm{Hom}(\mathbb{Z}, G) \xrightarrow{\cong} G, \quad f \mapsto f(1),$$

donde $\mathrm{Hom}(\mathbb{Z}, G)$ es el conjunto de homomorfismos $\mathbb{Z} \to G$.

2) *Demuestre que todo homomorfismo $f\colon \mathbb{Q} \to \mathbb{Q}$ del grupo aditivo de los números racionales está definido de modo único por el valor $f(1) \in \mathbb{Q}$. Esto nos da una biyección natural*

$$\mathrm{Hom}(\mathbb{Q}, \mathbb{Q}) \xrightarrow{\cong} \mathbb{Q}, \quad f \mapsto f(1),$$

donde $\mathrm{Hom}(\mathbb{Q}, \mathbb{Q})$ es el conjunto de homomorfismos $\mathbb{Q} \to \mathbb{Q}$.

Ejercicio 5.3.

1) *Encuentre los grupos $\ker f$ e $\mathrm{im}\, f$ para el homomorfismo*

$$\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}, \quad x \mapsto nx$$

donde $n = 2, 3, 4, 5$.

2) *Calcule los grupos $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ y $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$.*

Ejercicio 5.4. *Consideremos el conjunto de matrices*

$$G := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \mid x, y \in \mathbb{R},\ x^2 + y^2 > 0 \right\}.$$

Demuestre que es un subgrupo de $\mathrm{GL}_2(\mathbb{R})$ que es isomorfo a $\mathbb{C}^\times$.

Ejercicio 5.5. *Encuentre isomorfismos de grupos $D_3 \cong S_3 \cong \mathrm{GL}_2(\mathbb{F}_2)$. ¿Puede haber isomorfismos $D_n \cong S_n$ para $n \neq 3$? ¿$S_n \cong \mathrm{GL}_m(\mathbb{F}_p)$?*

Ejercicio 5.6. *Demuestre que los grupos $\mathbb{R}^\times$ y $\mathbb{C}^\times$ no son isomorfos.*

Ejercicio 5.7. *Asociemos a cada elemento del grupo de cuaterniones Q_8 una matriz compleja de la siguiente manera:*

$$\pm 1 \mapsto \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \quad \pm i \mapsto \begin{pmatrix} \pm\sqrt{-1} & 0 \\ 0 & \mp\sqrt{-1} \end{pmatrix}, \quad \pm j \mapsto \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}, \quad \pm k \mapsto \begin{pmatrix} 0 & \pm\sqrt{-1} \\ \pm\sqrt{-1} & 0 \end{pmatrix}.$$

Demuestre que esta correspondencia es un monomorfismo $Q_8 \rightarrowtail \mathrm{SL}_2(\mathbb{C}) \subset \mathrm{GL}_2(\mathbb{C})$.

Ejercicio 5.8. *Consideremos las* ***matrices triangulares superiores invertibles*** *(es decir, las matrices invertibles que tienen ceros debajo de la diagonal) y las matrices diagonales invertibles. Note que en ambos casos se tiene un subgrupo de* $\mathrm{GL}_n(R)$*. Demuestre que la aplicación*

$$\begin{pmatrix} * & * & * & \cdots & * & * \\ 0 & * & * & \cdots & * & * \\ 0 & 0 & * & \cdots & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & * & * \\ 0 & 0 & 0 & \cdots & 0 & * \end{pmatrix} \mapsto \begin{pmatrix} * & 0 & 0 & \cdots & 0 & 0 \\ 0 & * & 0 & \cdots & 0 & 0 \\ 0 & 0 & * & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & * & 0 \\ 0 & 0 & 0 & \cdots & 0 & * \end{pmatrix}$$

que deja las entradas diagonales intactas y aplica el resto de las entradas a 0 *es un homomorfismo de grupos.*

Ejercicio 5.9. *La función exponencial puede ser definida para cualquier matriz* $A \in M_n(\mathbb{R})$ *mediante la serie habitual* $e^A := \sum_{n\geq 0} \frac{1}{n!} A^n$*, donde* $A^n := \underbrace{A \cdots A}_{n}$ *son productos de matrices iterados. Esta serie siempre converge a alguna matriz invertible. Demuestre que para* $n > 1$ *la exponencial no es un homomorfismo* $M_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$*; es decir, en general* $e^{A+B} \neq e^A \cdot e^B$*.*

Indicación: considere $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *y* $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$*.*

Ejercicio 5.10. *En los ejercicios para el capítulo anterior hemos mencionado el grupo de matrices ortogonales*

$$O_n(k) = \{A \in \mathrm{GL}_n(k) \mid A^t A = A A^t = I\}.$$

1) *Demuestre que el determinante de una matriz ortogonal es igual a* ± 1*.*
   Indicación: el determinante es un homomorfismo y $\det A^t = \det A$*.*

2) *Demuestre que las matrices ortogonales de determinante* $+1$ *forman un subgrupo*

$$SO_n(k) := \{A \in \mathrm{GL}_n(k) \mid A^t A = A A^t = I,\ \det A = +1\} \subset O_n(k).$$

   Este se llama el ***grupo ortogonal especial****.*

3) *Demuestre que el grupo* $\mathrm{SO}_2(\mathbb{R})$ *es isomorfo al grupo del círculo* $\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\}$*.*

Capítulo 6
Generadores

En este capítulo veremos más ejemplos concretos de grupos y subgrupos. Un caso muy importante es el subgrupo generado por una colección de elementos. Cuando un grupo puede ser generado por un solo elemento, se dice que es cíclico. Ya conocimos a los grupos cíclicos (son precisamente los grupos aditivos $\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$), pero ahora vamos a investigar sus propiedades de manera más sistemática.

6.1 Subgrupos generados

6.1.1. Observación. *Sea G un grupo y $X \subset G$ algún subconjunto. Entonces existe un subgrupo mínimo de G que contiene a X. Este se denota por $\langle X \rangle$ y consiste precisamente en todos los productos finitos de la forma*

$$g_1^{\epsilon_1} \cdots g_k^{\epsilon_k}, \quad k \geq 0,$$

donde $g_i \in X$ y $\epsilon_i = \pm 1$. Para $k = 0$ el producto vacío se considera como la identidad $1 \in G$.

Demostración. Evidentemente, tenemos

$$\langle X \rangle = \bigcap_{\substack{H \subseteq G \text{ subgrupo} \\ X \subseteq H}} H.$$

Este es un subgrupo, siendo una intersección de subgrupos. Luego, junto con todos los elementos de X, este debe contener todos sus inversos y sus productos, de donde el conjunto de productos finitos $g_1^{\epsilon_1} \cdots g_k^{\epsilon_k}$ está contenido en $\langle X \rangle$. Pero este conjunto es un subgrupo, y por lo tanto coincide con $\langle X \rangle$. ■

6.1.2. Comentario. Escribamos el resultado de arriba para los grupos abelianos usando la notación aditiva. Si A es un grupo aditivo y $X \subset A$ es su subconjunto, entonces tenemos

$$\langle X \rangle = \{ \sum_{a \in X} n_a \, a \mid n_a \in \mathbb{Z},\ a \in X,\ n_a \neq 0 \text{ solo para un número finito de } a \}$$

(en otras palabras, tenemos combinaciones $\mathbb{Z}$-lineales *finitas* de los elementos de X.)

6.1.3. Definición. Se dice que $\langle X \rangle$ es el subgrupo de G **generado** por X. Si $\langle X \rangle = G$, se dice que los elementos de X son **generadores** de G.

Por supuesto, $X = G$ es un conjunto de generadores para cualquier grupo G. Pero en realidad, muchos grupos pueden ser generados por pocos elementos, muchos grupos infinitos se generan por un número finito de elementos, etc.

6.1.4. Definición. Si G posee un conjunto finito de generadores, se dice que G es **finitamente generado**.

6.1.5. Ejemplo. Hemos visto que el grupo diédrico D_n es generado por dos elementos r (rotación) y f (reflexión):

$$D_n = \langle r, f \rangle.$$

▲

6.1.6. Ejemplo. En el capítulo sobre los grupos simétricos y alternantes hemos visto que los siguientes son conjuntos de generadores para S_n:

- todas las transposiciones $(i\ j)$ para $1 \leq i < j \leq n$,
- las transposiciones $(1\ 2)$, $(2\ 3)$, $(3\ 4)$, …, $(n-1\ n)$,
- las transposiciones $(1\ 2)$, $(1\ 3)$, …, $(1\ n)$,
- una transposición $(1\ 2)$ y un n-ciclo $(1\ 2\ \cdots\ n)$.

De modo similar, para el grupo alternante A_n con $n \geq 3$, tenemos los siguientes conjuntos de generadores:

- todos los 3-ciclos $(i\ j\ k)$,
- los 3-ciclos de la forma $(1\ 2\ i)$,
- los 3-ciclos de la forma $(i\ i+1\ i+2)$,
- el 3-ciclo $(1\ 2\ 3)$ y el ciclo

$$\begin{cases} (2\ 3\ \cdots\ n), & \text{si } n \text{ es par,} \\ (1\ 2\ 3\ \cdots\ n), & \text{si } n \text{ es impar.} \end{cases}$$

▲

6.1.7. Ejemplo. El grupo

$$\mathrm{SL}_2(\mathbb{Z}) := \{A \in M_2(\mathbb{Z}) \mid \det A = 1\}$$

puede ser generado por dos matrices:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Calculamos que

$$S^2 = -I, \quad T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \text{para todo } n \in \mathbb{Z}.$$

Si tenemos una matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ con $c = 0$, entonces $ad = 1$ y luego $A = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix}$. Pero

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = T^b, \quad \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} = S^2\, T^{-b}.$$

Ahora vamos a ver que toda matriz en $\mathrm{SL}_2(\mathbb{Z})$ puede ser "reducida" a una matriz con $c = 0$ mediante multiplicaciones por S y T. Calculamos el efecto de la multiplicación por S y T^n para $n \in \mathbb{Z}$:

$$S \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix},$$
$$T^n \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}.$$

Si en una matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tenemos $c \neq 0$ y $|a| < |c|$, podemos pasar a $S \cdot A$ donde $|a| \geq |c|$. Entonces, se puede asumir que $|a| \geq |c|$. La división con resto nos da

$$a = cq + r, \quad \text{para } 0 \leq r < |c|.$$

Luego,

$$T^{-q}A = \begin{pmatrix} a-qc & b-qd \\ c & d \end{pmatrix} = \begin{pmatrix} r & b-qd \\ c & d \end{pmatrix}.$$

Multipliquemos esta matriz por S:

$$ST^{-q}A = S \cdot \begin{pmatrix} r & b-qd \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ r & b-qd \end{pmatrix}.$$

Hemos obtenido una matriz donde el valor absoluto del primer elemento en la segunda fila se volvió estrictamente más pequeño. Podemos continuar de esta manera hasta que este se vuelva nulo. Esto quiere decir que para alguna matriz $B \in \langle S, T \rangle$, la matriz BA es de la forma $\begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix} \in \langle S, T \rangle$. Podemos concluir que $A \in \langle S, T \rangle$.

Lo que acabamos de describir es un *algoritmo* que a partir de toda matriz en $\mathrm{SL}_2(\mathbb{Z})$ produce su expresión en términos se S y T. ▲

6.1.8. Ejemplo. Los números racionales $\mathbb{Q}$ respecto a la adición forman un grupo que no es finitamente generado. De hecho, sea $X \subset \mathbb{Q}$ un subconjunto finito:

$$X = \left\{ \frac{a_1}{b_1}, \ldots, \frac{a_k}{b_k} \right\}.$$

Entonces,

$$\langle X \rangle = \left\{ n_1 \frac{a_1}{b_1} + \cdots + n_k \frac{a_k}{b_k} \;\middle|\; n_1, \ldots, n_k \in \mathbb{Z} \right\}.$$

Sin embargo,

$$n_1 \frac{a_1}{b_1} + \cdots + n_k \frac{a_k}{b_k} = \frac{\text{algún entero}}{b_1 \cdots b_k}.$$

En particular, si p es algún primo que no divide a ningún denominador $b_1, \ldots, b_k$, entonces $\frac{1}{p} \notin \langle X \rangle$. ▲

6.2 Orden de un elemento

Un caso muy particular de subgrupos generados $\langle X \rangle \subseteq G$ es cuando el conjunto X tiene solo un elemento g. En este caso el subgrupo generado por g es

$$\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}.$$

Hay dos posibilidades diferentes.

1) Si todas las potencias g^n son diferentes, entonces $\langle g \rangle$ es un subgrupo infinito.

2) Si tenemos $g^k = g^\ell$ para algunos $k \neq \ell$, entonces sin pérdida de generalidad $k > \ell$, luego $g^{k-\ell} = 1$ y se ve que la sucesión $(g^n)_{n\in\mathbb{Z}}$ es periódica y el subgrupo $\langle g \rangle$ es finito.

6.2.1. Definición. Para un elemento $g \in G$, el mínimo número $n = 1, 2, 3, \ldots$ tal que $g^n = 1$ se llama el **orden** de g y se denota por $\operatorname{ord} g$. Si $g^n \neq 1$ para ningún n, se dice que g tiene orden infinito.

(Como siempre, vamos a usar la notación multiplicativa para la teoría general, pero no olvidemos que para un grupo abeliano con notación aditiva, en lugar de "$g^n = 1$" se escribe "$n \cdot a = 0$".)

6.2.2. Observación. *Si G es un grupo finito, entonces todos sus elementos tienen orden finito.*

Demostración. Si g tuviera orden infinito, entre los elementos g^n para $n \in \mathbb{Z}$ no habría repeticiones. Esto no es posible si G es finito. ■

6.2.3. Ejemplo. La identidad $1 \in G$ es el único elemento de orden 1. ▲

6.2.4. Ejemplo. Un elemento g tiene orden 2 si y solamente si $g \neq 1$ y $g^{-1} = g$. ▲

6.2.5. Ejemplo. En el grupo diédrico la reflexión f tiene orden 2, ya que $f^2 = \mathrm{id}$ y la rotación r tiene orden n. ▲

6.2.6. Ejemplo. La matriz $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ tiene orden 4 en $\mathrm{SL}_2(\mathbb{Z})$. De hecho,

$$S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I,\ S^3 = -S,\ S^4 = (S^2)^2 = I.$$

La matriz $R = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ tene orden 3:

$$R^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},\ R^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Sin embargo, el producto

$$SR = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} =: T$$

tiene orden infinito: para todo $n \in \mathbb{Z}$ tenemos

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Recordamos que hemos visto en 6.1.7 que las matrices S y T generan el grupo $\mathrm{SL}_2(\mathbb{Z})$. Ya que $T = SR$, se sigue que S y R generan $\mathrm{SL}_2(\mathbb{Z})$. ▲

Este ejemplo demuestra que en general, en un grupo no abeliano, no hay ninguna relación entre $\operatorname{ord} g$, $\operatorname{ord} h$ y $\operatorname{ord}(gh)$: puede ser que $\operatorname{ord} g < \infty$, $\operatorname{ord} h < \infty$, pero $\operatorname{ord} gh = \infty$. Esto sucede solamente para grupos no abelianos. El caso de grupos abelianos es más sencillo y más adelante vamos a describir la estructura de grupos abelianos finitamente generados.

Examinemos algunas propiedades básicas de órdenes.

6.2.7. Observación. *Si g es un elemento de orden finito, entonces para todo número entero m tenemos*

$$g^m = 1 \quad \textit{si y solamente si} \quad \operatorname{ord} g \mid m.$$

(En la notación aditiva: $m \cdot a = 0$ si y solamente si $\operatorname{ord} a \mid m$.)

Demostración. Sea $n = \operatorname{ord} g$. Podemos dividir con resto m por n:

$$m = qn + r, \quad \text{para algún } 0 \leq r < n.$$

Luego,

$$g^m = g^{qn+r} = (g^n)^q \cdot q^r = g^r = 1,$$

pero puesto que $r < n$ y n es el mínimo número positivo tal que $g^n = 1$, se sigue que $r = 0$. ■

6.2.8. Ejemplo. El orden de un k-ciclo $(i_1\ i_2\ \cdots\ i_k)$ en el grupo simétrico S_n es igual a k. En general, para toda permutación $\sigma \in S_n$ podemos considerar su descomposición en ciclos disjuntos

$$\sigma = \tau_1 \cdots \tau_s.$$

Luego, los τ_i conmutan entre sí, así que

$$\sigma^k = \tau_1^k \cdots \tau_s^k.$$

Los τ_i^k son también disjuntos para cualquier k, así que $\sigma^k = \mathrm{id}$ si y solamente si $\tau_i^k = \mathrm{id}$ para todo i. Entonces,

$$\operatorname{ord}(\sigma) = \min\{k \mid \tau_1^k = \mathrm{id},\ \ldots,\ \tau_s^k = \mathrm{id}\} = \min\{k \mid \operatorname{ord}\tau_1 \mid k,\ \ldots,\ \operatorname{ord}\tau_s \mid k\} = \operatorname{mcm}(\tau_1, \ldots, \tau_s).$$

Por ejemplo, para la permutación $\sigma = (1\ 2)\,(3\ 4)\,(5\ 6\ 7)$ tenemos

$$\sigma^2 = (5\ 7\ 6),\ \sigma^3 = (1\ 2)\,(3\ 4),\ \sigma^4 = (5\ 6\ 7),\ \sigma^5 = (1\ 2)\,(3\ 4)\,(5\ 7\ 6),\ \sigma^6 = \mathrm{id}.$$

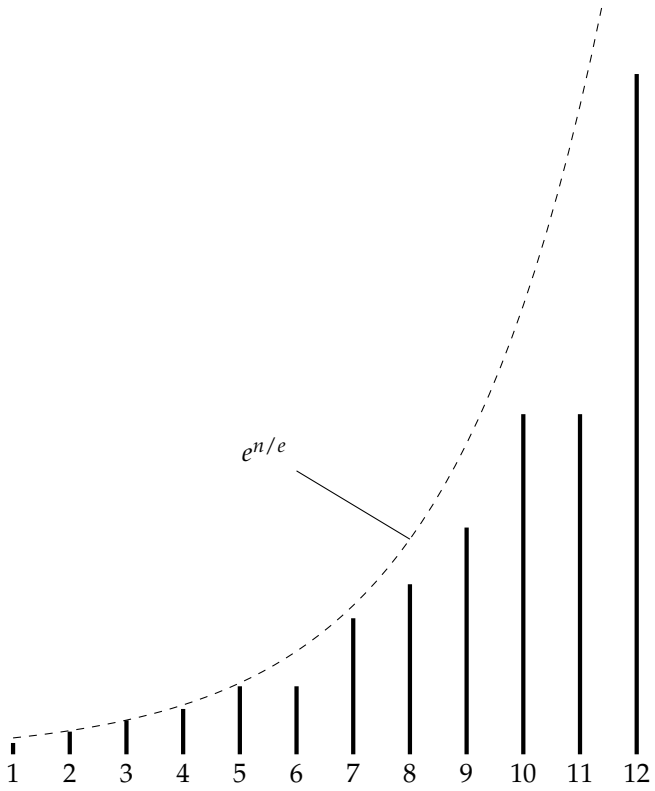
El número

$$g(n) := \max\{\operatorname{ord}\sigma \mid \sigma \in S_n\} = \max\{\operatorname{mcm}(n_1, \ldots, n_s) \mid n_1 + \cdots + n_s = n\}$$

se llama la **función de Landau**. He aquí algunos de sus valores (véase http://oeis.org/A000793):

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$g(n)$:	1	2	3	4	6	6	12	15	20	30	30	60	60	84	105

Hay varias expresiones asintóticas y desigualdades, por ejemplo $g(n) \leq e^{n/e}$.



▲

6.2.9. Corolario. *Si* $\operatorname{ord} g = n$*, entonces*

$$g^k = g^\ell \iff k \equiv \ell \pmod{n}.$$

Demostración. La igualdad $g^k = g^\ell$ es equivalente a $g^{k-\ell} = 1$ y luego a $n \mid (k - \ell)$ gracias a la observación 6.2.7; es decir, $k \equiv \ell \pmod{n}$. ■

6.2.10. Corolario. *Si* $\operatorname{ord} g = n$*, entonces el subgrupo* $\langle g \rangle$ *tiene n elementos.*

Demostración. Tenemos

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{1, g, g^2, \ldots, g^{n-1}\},$$

ya que $0, 1, 2, \ldots, n-1$ representan todos los restos módulo n. ■

6.2.11. Observación. *Si g es un elemento de orden finito, entonces*

$$\operatorname{ord} g^k = \frac{\operatorname{ord} g}{\operatorname{mcd}(\operatorname{ord} g, k)}.$$

Demostración. Sea $n = \operatorname{ord} g$. Si $\operatorname{mcd}(k, n) = d$, entonces podemos escribir

$$n = n'd, \quad k = k'd, \quad \text{donde } \operatorname{mcd}(n', k') = 1.$$

Luego,

$$n \mid km \iff n'd \mid k'dm \iff n' \mid k'm \iff n' \mid m,$$

y tenemos

$$\operatorname{ord} g^k = \min\{m \mid (g^k)^m = 1\} = \min\{m \mid n \mid km\} = \min\{m \mid n' \mid m\} = n' = n/d.$$

■

6.3 Grupos cíclicos

6.3.1. Definición. Se dice que un grupo G es **cíclico** si existe un elemento $g \in G$ que genera todo G; es decir $G = \langle g \rangle$.

En la situación de arriba, si g tiene orden finito, entonces, como hemos notado en 6.2.10, tenemos $|\langle g \rangle| = \operatorname{ord} g$. Esto significa que un grupo finito es cíclico si y solamente si este posee un elemento de orden $n = |G|$. En este caso los elementos de G son

$$\{1, g, g^2, \ldots, g^{n-1}\}.$$

6.3.2. Observación. *Sea $G = \langle g \rangle$ un grupo cíclico finito de orden n. Entonces, otro elemento $g^k \in G$ es un generador de G si y solamente si* $\operatorname{mcd}(k, n) = 1$.

Demostración. g^k es un generador si y solamente si $\operatorname{ord} g^k = n$. Para el orden de g^k tenemos la fórmula

$$\operatorname{ord} g^k = \frac{n}{\operatorname{mcd}(k, n)}$$

(véase 6.2.11). ■

6.3.3. Ejemplo. El grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ es generado por $[1]_n$.

$$\begin{aligned}
[0]_n &= 0 \cdot [1]_n, \\
[1]_n &= [1]_n, \\
[2]_n &= 2 \cdot [1]_n := [1]_n + [1]_n, \\
[3]_n &= 3 \cdot [1]_n := [1]_n + [1]_n + [1]_n, \\
&\vdots
\end{aligned}$$

En general, $[k]_n$ es un generador de $\mathbb{Z}/n\mathbb{Z}$ si y solamente si $\operatorname{mcd}(k, n) = 1$. El número de generadores de $\mathbb{Z}/n\mathbb{Z}$ coincide con el valor de la función de Euler $\phi(n)$. ▲

6.3.4. Ejemplo. El grupo aditivo $\mathbb{Z}$ es cíclico, generado por 1, ya que todo número entero puede ser escrito como $\pm(1 + \cdots + 1)$. Otro generador de $\mathbb{Z}$ es -1.

En general, si $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ es un grupo cíclico infinito, se ve que los únicos generadores son g y g^{-1}. ▲

Los ejemplos de arriba son de hecho todos los grupos cíclicos posibles, salvo isomorfismo.

6.3.5. Proposición. *Todo grupo cíclico finito de orden n es isomorfo a $\mathbb{Z}/n\mathbb{Z}$.*
Todo grupo cíclico infinito es isomorfo a $\mathbb{Z}$.

Demostración. Si G es un grupo cíclico finito de orden n, entonces

$$G = \langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}.$$

para algún $g \in G$. Definamos la aplicación

$$\begin{aligned}
f \colon G &\to \mathbb{Z}/n\mathbb{Z}, \\
g^k &\mapsto [k]_n.
\end{aligned}$$

Esta aplicación está bien definida: $g^k = g^\ell$ si y solamente si $k \equiv \ell \pmod{n}$ (véase 6.2.9). Note que esto también demuestra que f es una biyección. Es un homomorfismo, ya que

$$f(g^k \cdot g^\ell) = f(g^{k+\ell}) = [k+\ell]_n = [k]_n + [\ell]_n = f(g^k) + f(g^\ell).$$

Ahora si

$$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

es un grupo cíclico infinito, entonces la aplicación

$$\begin{aligned} G &\to \mathbb{Z}, \\ g^n &\mapsto n \end{aligned}$$

es visiblemente un isomorfismo. ■

6.3.6. Ejemplo. El grupo de las raíces n-ésimas de la unidad $\mu_n(\mathbb{C})$ es cíclico, generado por $\zeta_n := e^{2\pi i/n}$:

$$\mu_n(\mathbb{C}) = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}.$$

Tenemos un isomorfismo

$$\begin{aligned} \mu_n(\mathbb{C}) &\to \mathbb{Z}/n\mathbb{Z}, \\ \zeta_n^k &\mapsto [k]_n. \end{aligned}$$

En general, ζ_n^k es un generador si y solamente si $\mathrm{mcd}(k, n) = 1$. Los generadores de $\mu_n(\mathbb{C})$ se llaman las raíces n-ésimas **primitivas** de la unidad. ▲

Note que el isomorfismo construido en 6.3.5 no es canónico: para construirlo, hemos *escogido* un generador $g \in G$. Diferentes generadores nos dan diferentes isomorfismos. Los grupos específicos $\mathbb{Z}/n\mathbb{Z}$, $\mu_n(\mathbb{C})$, $\mathbb{Z}$ vienen con un generador canónico: $[1]_n$, $\zeta_n := e^{2\pi i/n}$, $+1$ respectivamente.

6.3.7. Ejemplo. El grupo alternante

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

es cíclico, generado por $(1\ 2\ 3)$ o por $(1\ 3\ 2)$. Es isomorfo a $\mathbb{Z}/3\mathbb{Z}$. ▲

6.3.8. Proposición. *Sea G un grupo cíclico. Si $H \subset G$ es un subgrupo, entonces H es también cíclico.*

Demostración. Sea g un generador de G:

$$G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

Sin pérdida de generalidad $H \neq \{\mathrm{id}\}$ (en el caso contrario, la proposición es obvia). Entonces existe un número mínimo positivo $k_0 = 1, 2, 3, \ldots$ tal que $g^{k_0} \in H$ (siendo un subgrupo, H contiene g^{-k} junto con g^k, así que este g^{k_0} siempre existe). Vamos a ver que g^{k_0} es un generador de H; es decir, $H = \langle g^{k_0} \rangle$. De hecho, para todo $g^k \in H$ podemos dividir con resto k por k_0:

$$k = qk_0 + r, \quad 0 \leq r < k_0.$$

Ahora, ya que H es un subgrupo, tenemos $g^{-k_0} = (g^{k_0})^{-1} \in H$ y $g^{-qk_0} = (g^{-k_0})^q \in H$, y luego

$$g^{-qk_0} \cdot g^k = g^{-qk_0} \cdot g^{qk_0+r} = g^r \in H,$$

pero nuestra elección de k_0 implica que $r = 0$. Entonces, $k = qk_0$ y $g^k = (g^{k_0})^q$. ■

6.3.9. Ejemplo. Todos los subgrupos de $\mathbb{Z}$ son de la forma

$$n\mathbb{Z} := \{0, \pm n, \pm 2n, \pm 3n, \dots\}.$$

Son cíclicos, generados por n. ▲

6.3.10. Proposición. *Sea G es un grupo cíclico finito de orden n. Para todo subgrupo $H \subset G$ se tiene $|H| \mid n$. Además, para todo $d \mid n$ el grupo G contiene precisamente un subgrupo de orden d.*

Demostración. Todo subgrupo $H \subset G$ es necesariamente cíclico según 6.3.8, generado por g^k para algún k. Luego,

$$|H| = |\langle g^k \rangle| = \operatorname{ord} g^k = n/d, \quad \text{donde } d = \operatorname{mcd}(k, n).$$

De hecho, se tiene $\langle g^k \rangle = \langle g^d \rangle$. En efecto, $d \mid k$ implica que $\langle g^k \rangle \subseteq \langle g^d \rangle$. Por otro lado,

$$|\langle g^d \rangle| = \operatorname{ord} g^d = \frac{n}{\operatorname{mcd}(d, n)} = n/d,$$

ya que $d \mid n$. Esto significa que $\langle g^k \rangle = \langle g^d \rangle$. Entonces,

$$H = \langle g^d \rangle.$$

Viceversa, a partir de cualquier $d \mid n$ podemos considerar el subgrupo $\langle g^d \rangle$. Su orden es n/d. Para diferentes $d, d' \mid n$ los subgrupos $\langle g^d \rangle$ y $\langle g^{d'} \rangle$ son diferentes, siendo grupos de diferente orden. ■

6.3.11. Ejemplo. En el grupo de las n-ésimas raíces de la unidad $\mu_n(\mathbb{C})$ para todo $m \mid n$ tenemos el subgrupo $\mu_m(\mathbb{C}) \subset \mu_n(\mathbb{C})$, y todos los subgrupos surgen de este modo. ▲

6.3.12. Corolario. *Para la función ϕ de Euler se cumple la identidad*

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

donde la suma es sobre todos los divisores de n.

Demostración. Todo elemento $x \in \mathbb{Z}/n\mathbb{Z}$ tiene orden $d = |\langle x \rangle|$ donde $d \mid n$ y en total hay $\phi(d)$ diferentes elementos de orden d que corresponden a diferentes generadores del único subgrupo de orden d. Entonces, la suma $\sum_{d \mid n} \phi(d)$ nada más cuenta todos los n elementos de $\mathbb{Z}/n\mathbb{Z}$. ■

6.3.13. Ejemplo. $\phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6$. ▲

Los grupos cíclicos son los grupos más simples que se pueden imaginar (¡salvo los grupos triviales!). Sin embargo, son de mucha importancia en aritmética.

6.4 Ejercicios

Ejercicio 6.1. *Sea G un grupo. Supongamos que para dos elementos $g, h \in G$ se cumple $h = k\,g\,k^{-1}$ para algún $k \in G$ (en este caso se dice que g y h son **conjugados**). Demuestre que el orden de g es finito si y solamente si el orden de h es finito, y en este caso* $\operatorname{ord} g = \operatorname{ord} h$.

Ejercicio 6.2. *Describa todos los tipos de ciclo posibles en el grupo simétrico S_5 y encuentre los ordenes correspondientes.*

Ejercicio 6.3. *Exprese la matriz $\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$ como un producto de matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.*

Ejercicio 6.4. *Demuestre que el conjunto*

$$X = \{1/p^k \mid p \text{ primo}, k = 0, 1, 2, 3, \dots\}$$

genera el grupo aditivo $\mathbb{Q}$.

Ejercicio 6.5. *Encuentre los elementos de orden finito en el grupo de isometrías del plano euclidiano $\mathbb{R}^2 \to \mathbb{R}^2$.*

Ejercicio 6.6. *Supongamos que G es un grupo finito de orden par. Demuestre que G tiene un elemento de orden 2.*

Ejercicio 6.7. *Supongamos que G es un grupo no trivial que no tiene subgrupos propios. Demuestre que G es un grupo cíclico finito de orden p, donde p es un número primo.*

El ejemplo de $R = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ y $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ en $\mathrm{SL}_2(\mathbb{Z})$ demuestra que para dos elementos de orden finito, su producto puede tener orden infinito y además que un número finito de elementos de orden finito pueden generar un grupo infinito. Esto sucede gracias a la nonconmutatividad. La situación en grupos abelianos es más sencilla.

Ejercicio 6.8. *Sea A un grupo abeliano (escrito en la notación aditiva).*

1) *Sea $m = 1, 2, 3, \dots$ un número fijo. Demuestre que los elementos $a \in A$ tales que $m \cdot a = 0$ forman un subgrupo de A. Este se denota por $A[m]$ y se llama el **subgrupo de m-torsión** en A.*

2) *Demuestre que todos los elementos de orden finito en A forman un subgrupo. Este se llama el **subgrupo de torsión** y se denota por A_{tors}:*

$$A_{tors} = \bigcup_{m \geq 1} A[m].$$

3) *Encuentre los grupos $A[m]$ y A_{tors} para $A = \mathbb{R}, \mathbb{C}, \mathbb{R}^\times, \mathbb{C}^\times$.*

Ejercicio 6.9. *Sea A un grupo abeliano.*

1) *Demuestre que para todo homomorfismo $f\colon \mathbb{Z}/m\mathbb{Z} \to A$ se tiene necesariamente $f([1]_m) \in A[m]$.*

2) *Demuestre que*

$$\operatorname{Hom}(\mathbb{Z}/m\mathbb{Z}, A) \to A[m], \quad f \mapsto f([1]_m)$$

es una biyección.

3) *Describa todos los homomorfismos de grupos abelianos*

$$\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}, \quad \mathbb{Z}/m\mathbb{Z} \to \mathbb{Q}, \quad \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

para diferentes $m, n = 2, 3, 4, 5, \dots$

Ejercicio 6.10. *Demuestre que* $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

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

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

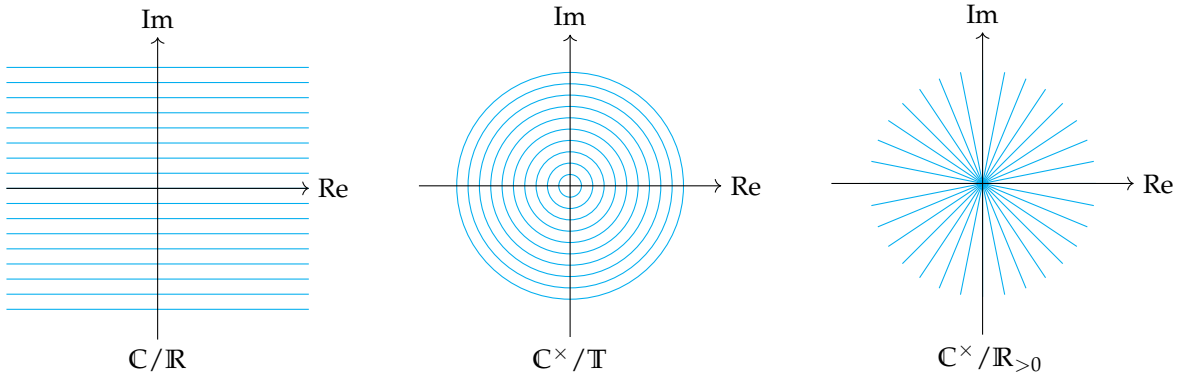
(el grupo del círculo) y

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

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.

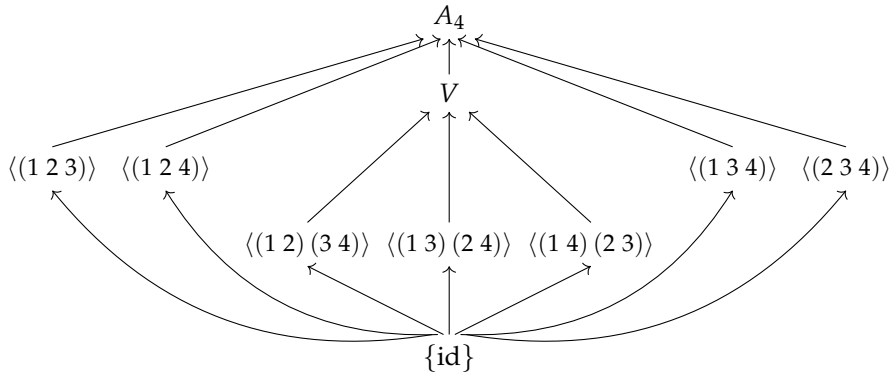
Si G es un subgrupo de orden 6, sus elementos necesariamente tienen orden 2 o 3; es decir, son 3-ciclos o permutaciones de la forma $(\bullet\ \bullet)\,(\bullet\ \bullet)$. Junto con cada 3-ciclo G debe contener su inverso. Las posibles opciones son

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

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. ▲

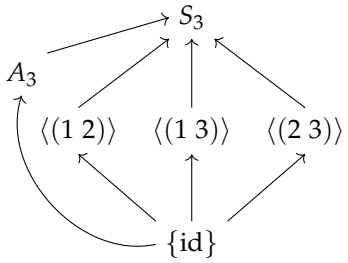
7.3.3. Ejemplo. Los subgrupos $\{1\}$ y G son normales. ▲

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

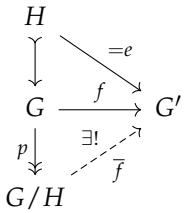
$$|A_4/V| = |A_4|/|V| = \frac{4!/2}{4} = 3,$$

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

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

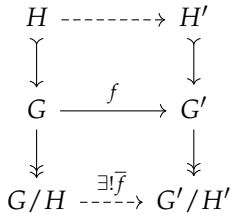
Es una aplicación bien definida: si $gH = g'H$ para algunos $g, g' \in G$, entonces $g^{-1}g' \in H$, luego $g^{-1}g' \in \ker f$ y

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

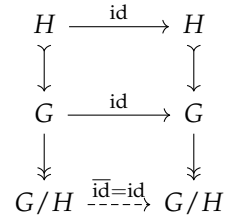
La aplicación $\overline{f}$ es un homomorfismo de grupos, puesto que f lo es. ■

7.4.8. Corolario (Funtorialidad del cociente).

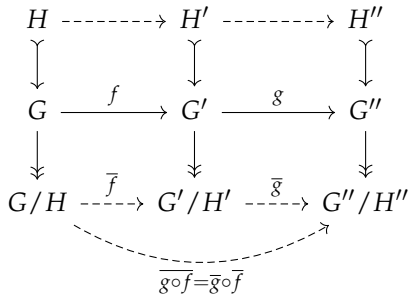
1) *Sea $f\colon G \to G'$ un homomorfismo de grupos. Sean $H \subseteq G$ y $H' \subseteq G'$ subgrupos normales. Supongamos que $f(H) \subseteq H'$. Entonces f induce un homomorfismo canónico $\widetilde{f}\colon G/H \to G'/H'$ que conmuta con las proyecciones canónicas:*



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*

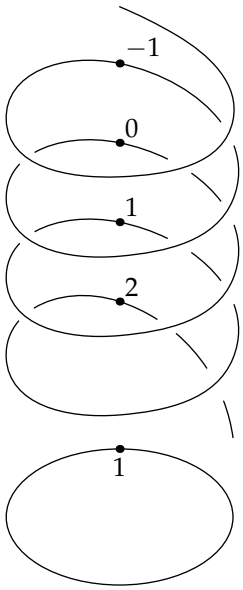
$$|G| = |\operatorname{im} f| \cdot |\ker f|.$$

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* $\mathbb{Q}/\mathbb{Z} \to \mathbb{Z}$.

Apéndice A
Divisibilidad en $\mathbb{Z}$

Todo número compuesto es medido por algún número primo.
Todo número o bien es número primo o es medido por algún número primo.

Euclides, "Elementos", Libro VII

Cualquier número compuesto puede resolverse en factores primos de una manera única.

Gauss, "Disquisitiones Arithmeticae", §16

Este apéndice contiene un breve resumen de la teoría de números elemental que necesitamos en el curso, específicamente los resultados básicos relacionados con la divisibilidad de números enteros. Algunos otros temas, como la aritmética módulo n, hacen parte del texto principal. El lector interesado puede consultar, por ejemplo, el libro de texto [IR1990].

A.0 Subgrupos de $\mathbb{Z}$

Ya que nuestro curso está dedicado a la teoría de grupos, algunas demostraciones de abajo usan la noción de grupo abeliano. Solamente para facilitar la lectura y no dejar la impresión de que en nuestra exposición hay argumentos circulares, revisemos toda la teoría de grupos necesaria.

Recordemos que un **subgrupo** $A \subset \mathbb{Z}$ es un subconjunto de números enteros que satisface las siguientes condiciones:

1) $0 \in A$,

2) para cualesquiera $a, b \in A$ tenemos $a + b \in A$,

3) para cualquier $a \in A$ tenemos $-a \in A$.

A.0.1. Observación. *Si A y B son dos subgrupos de $\mathbb{Z}$, entonces su intersección $A \cap B$ es también un subgrupo.*

Para $a_1, \ldots, a_n \in \mathbb{Z}$ el **subgrupo generado** por $a_1, \ldots, a_n$ es el subconjunto $\langle a_1, \ldots, a_n \rangle \subseteq \mathbb{Z}$ que satisface una de las siguientes condiciones equivalentes.

1) $\langle a_1, \ldots, a_n \rangle$ es el mínimo subgrupo de $\mathbb{Z}$ que contiene todos los números $a_1, \ldots, a_n$,

2) $\langle a_1, \ldots, a_n \rangle$ es el conjunto de las combinaciones $\mathbb{Z}$-lineales de $a_1, \ldots, a_n$:

$$\langle a_1, \ldots, a_n \rangle = \Big\{ \sum_i n_i a_i \;\Big|\; n_i \in \mathbb{Z} \Big\}.$$

Nos van a interesar dos casos particulares: los subgrupos generados por un número $d \in \mathbb{Z}$:

$$\langle d \rangle = \{ md \mid m \in \mathbb{Z} \}$$

y subgrupos generados por dos números:

$$\langle a, b \rangle = \{ ma + nb \mid m, n \in \mathbb{Z} \}.$$

A.1 División con resto

A.1.1. Teorema (Euclides). *Sean $a, b \in \mathbb{Z}$ dos números enteros, con $b \neq 0$. Entonces, existen $q, r \in \mathbb{Z}$ tales que*

$$a = qb + r, \quad 0 \leq r < |b|.$$

Demostración. Para el conjunto

$$\{ a - xb \mid x \in \mathbb{Z} \}$$

sea

$$r = a - qb$$

su mínimo elemento tal que $r \geq 0$ (este existe, puesto que $b \neq 0$). Supongamos que $r \geq |b|$. Si $b > 0$, tenemos

$$0 \leq r - b = a - qb - b = a - (q+1)\, b < r.$$

De la misma manera, si $b < 0$, entonces

$$0 \leq r + b = a - qb + b = a - (q-1)\, b < r.$$

En ambos casos se produce un elemento $a - (q \pm 1)\, b$, lo que contradice nuestra elección de r. Podemos concluir que $r < |b|$. ■

El resultado que acabamos de describir se llama la **división con resto** de a por b. He aquí una de sus consecuencias importantes.

A.1.2. Proposición. *Todo subgrupo de $\mathbb{Z}$ es de la forma $\langle d \rangle$ para algún $d \in \mathbb{Z}$. En particular, para cualesquiera $a, b \in \mathbb{Z}$ se tiene*

1) $\langle a, b \rangle = \langle d \rangle$ para algún $d \in \mathbb{Z}$,

2) $\langle a \rangle \cap \langle b \rangle = \langle d \rangle$ para algún $d \in \mathbb{Z}$.

Demostración. Sea $A \subseteq \mathbb{Z}$ un subgrupo. Si $A = 0$, entonces $A = \langle 0 \rangle$ y enunciado es trivial. Luego, si $A \neq 0$, entonces A contiene números no nulos. Para cada $x \in A$ también $-x \in A$, así que A contiene números positivos. Sea entonces

$$d := \min\{ x \in A \mid x > 0 \}.$$

Está claro que $\langle d \rangle \subseteq A$. Para ver la otra inclusión, consideremos un elemento arbitrario $c \in A$. La división con resto por d nos da

$$c = qd + r, \quad 0 \leq r < d.$$

Luego, puesto que $c, d \in A$, tenemos también $r = c - qd \in A$. Por nuestra elección de d, podemos descartar el caso $0 < r < d$. Entonces, $r = 0$ y $c = qd \in \langle d \rangle$. ■

A.2 Divisibilidad y los números primos

A.2.1. Definición. Para dos números enteros $d, n \in \mathbb{Z}$ se dice que d **divide a** n y se escribe "$d \mid n$" si $n = mx$ para algún $m \in \mathbb{Z}$. En este caso también se dice que d es un **divisor** de n o que n es **divisible por** d. Cuando d no divide a n, se escribe "$d \nmid n$".

Notamos que en términos de subgrupos de $\mathbb{Z}$,

$$d \mid n \iff \langle n \rangle \subseteq \langle d \rangle.$$

El lector puede comprobar las siguientes propiedades de la relación de divisibilidad.

0) $a \mid 0$ para todo[*] $a \in \mathbb{Z}$. Esto caracteriza a 0 de modo único. Tenemos $0 \mid a$ solamente para $a = 0$.

1) $a \mid a$ y $\pm 1 \mid a$ para todo $a \in \mathbb{Z}$.

2) Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$.

3) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

4) Si $a \mid b$, entonces $a \mid bc$ para cualquier $c \in \mathbb{Z}$.

5) Si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$.

A.2.2. Definición. Se dice que un número entero positivo $p > 0$ es **primo** si $p \neq 1$ y los únicos divisores de p son ± 1 y $\pm p$.

En otras palabras, p es primo si y solamente si para $m, n > 0$, si tenemos $p = mn$, entonces o bien $m = p$, $n = 1$ o bien $m = 1$, $n = p$. Los primeros números primos son

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, ...

Por ejemplo, $57 = 3 \cdot 19$ no es primo.

A.2.3. Proposición. *Todo entero no nulo puede ser expresado como*

$$n = \pm p_1^{k_1} \, p_2^{k_2} \cdots p_\ell^{k_\ell}$$

donde p_i son primos diferentes.

Demostración. Sin pérdida de generalidad, podemos considerar el caso de $n > 0$. Sería suficiente ver que n es un producto de primos y juntando múltiplos iguales, se obtiene la expresión de arriba.

Para $n = 1$ tenemos $n = p^0$ para cualquier primo p. Luego, se puede proceder por inducción. Supongamos que el resultado se cumple para todos los números positivos $< n$. Si n es primo, no hay que demostrar nada. Si n no es primo, entonces $n = ab$ donde $a < n$ y $b < n$. Por la hipótesis de inducción, a y b son productos de números primos, y por lo tanto n lo es. ■

En este caso la palabra "primo" es un sinónimo de "primero" y refiere precisamente al hecho de que todo número entero sea un producto de primos. No se trata de ninguna relación de parentesco entre los números.

A.2.4. Teorema (Euclides). *Hay un número infinito de primos.*

[*] Algunas fuentes insisten que $0 \nmid 0$, pero la relación $0 \mid 0$ no tiene nada de malo. De hecho $0 \in \langle d \rangle$ para cualquier $d \in \mathbb{Z}$, en particular para $d = 0$.

Demostración. Consideremos los primeros n números primos

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ \ldots,\ p_n.$$

Luego, el número

$$N := p_1 p_2 \cdots p_n + 1$$

no es divisible por ningún primo entre $p_1, \ldots, p_n$. Sin embargo, N tiene que ser un producto de primos, así que es necesariamente divisible por algún primo p tal que $p_n < p \leq N$. ■

A.3 El máximo común divisor

A.3.1. Definición. Para dos números enteros $a, b \in \mathbb{Z}$ su **máximo común divisor** (**mcd**) es un número $d := \text{mcd}(a, b)$ caracterizado por las siguientes propiedades:

1) $d \mid a$ y $d \mid b$,

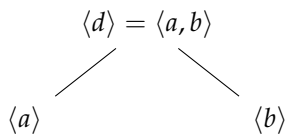
2) si d' es otro número tal que $d' \mid a$ y $d' \mid b$, entonces $d' \mid d$.

Las condiciones de arriba pueden ser escritas como

1) $\langle a \rangle \subseteq \langle d \rangle$ y $\langle b \rangle \subseteq \langle d \rangle$,

2) si $\langle a \rangle \subseteq \langle d' \rangle$ y $\langle b \rangle \subseteq \langle d' \rangle$, entonces $\langle d \rangle \subseteq \langle d' \rangle$.

El subgrupo mínimo de $\mathbb{Z}$ que contiene a $\langle a \rangle$ y $\langle b \rangle$ es $\langle a, b \rangle$. Gracias a A.1.2, sabemos que $\langle a, b \rangle = \langle d \rangle$ para algún $d \in \mathbb{Z}$.



Esto nos lleva al siguiente resultado.

A.3.2. Proposición. *El mcd siempre existe: tenemos*

$$\langle a, b \rangle = \langle d \rangle \quad \textit{donde } d = \text{mcd}(a, b).$$

En particular, se cumple

$$ax + by = \text{mcd}(a, b) \quad \textit{para algunos } x, y \in \mathbb{Z}$$

y $\text{mcd}(a, b)$ *es el mínimo número posible que puede ser representado como una combinación* $\mathbb{Z}$*-lineal de* a *y* b*.*

La última expresión se conoce como la **identidad de Bézout**. Aquí los coeficientes x e y no son únicos. Por ejemplo,

$$2 \cdot (-1) + 3 \cdot 1 = 2 \cdot (-4) + 3 \cdot 3 = 2 \cdot 2 + 3 \cdot (-1) = \cdots = 1.$$

He aquí algunas observaciones respecto a $\text{mcd}(a, b)$.

1) La definición de $d := \text{mcd}(a, b)$ caracteriza a d *salvo signo*. De hecho, si d y d' satisfacen las condiciones de $\text{mcd}(a, b)$, entonces $d \mid d'$ y $d' \mid d$ (o la condición equivalente $\langle d \rangle = \langle d' \rangle$) implica que $d' = \pm d$. Normalmente se escoge $d > 0$, pero estrictamente hablando, todas las identidades con $\text{mcd}(a, b)$ pueden ser interpretadas salvo signo.

2) La definición de $\text{mcd}(a,b)$ es visiblemente simétrica en a y b, así que

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

3) Para todo $a \in \mathbb{Z}$ se tiene

$$\text{mcd}(a,0) = a.$$

En particular*,

$$\text{mcd}(0,0) = 0.$$

Esto nada más significa que cualquier número divide a 0, o de manera equivalente, que $\langle 0\rangle \subseteq \langle a\rangle$ para todo $a \in \mathbb{Z}$, y también para $a = 0$.

A.3.3. Definición. Si $\text{mcd}(a,b) = 1$, se dice que a y b son **coprimos**.

Si a y b son coprimos, entonces $\langle a,b\rangle = \langle 1\rangle = \mathbb{Z}$, y en particular tenemos

$$ax + by = 1 \quad \text{para algunos } x, y \in \mathbb{Z}.$$

A.3.4. Observación. *Si $a \mid bc$ donde a y b son coprimos, entonces $a \mid c$.*

Demostración. Tenemos

$$ax + by = 1$$

para algunos $x, y \in \mathbb{Z}$. Luego,

$$axc + byc = c,$$

y la expresión a la izquierda es divisible por a. ■

A.3.5. Corolario. *Si p es primo y $p \mid bc$, entonces $p \mid b$ o $p \mid c$.*

Muy a menudo se usa el contrapuesto: si $p \nmid b$ y $p \nmid c$, entonces $p \nmid bc$.

Demostración. Ya que los únicos divisores de p son ± 1 y $\pm p$, tenemos dos casos posibles. En el primer caso, $\text{mcd}(p,b) = 1$ y luego $p \mid c$ por el resultado precedente. En el segundo caso, $\text{mcd}(p,b) = p$, lo que significa que $p \mid b$. ■

A.4 El mínimo común múltiplo

A.4.1. Definición. Para dos números enteros $a, b \in \mathbb{Z}$ su **mínimo común múltiplo (mcm)** es un número $m := \text{mcm}(a,b)$ caracterizado por las siguientes propiedades:

1) $a \mid m$ y $b \mid m$,

2) si m' es otro número tal que $a \mid m'$ y $b \mid m'$, entonces $m \mid m'$.

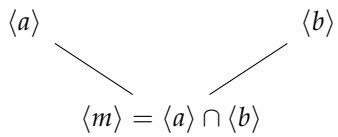
Las condiciones de arriba pueden ser escritas como

1) $\langle m\rangle \subseteq \langle a\rangle$ y $\langle m\rangle \subseteq \langle b\rangle$,

2) si m' es otro número tal que $\langle m'\rangle \subseteq \langle a\rangle$ y $\langle m'\rangle \subseteq \langle b\rangle$, entonces $\langle m'\rangle \subseteq \langle m\rangle$.

*Algunas fuentes insisten que $\text{mcd}(0,0)$ no está definido, pero como vemos, es lógico poner $\text{mcd}(0,0) = 0$.

El subgrupo máximo de $\mathbb{Z}$ que contiene a $\langle a\rangle$ y $\langle b\rangle$ es su intersección $\langle a\rangle \cap \langle b\rangle$. Gracias a A.1.2 sabemos que es también de la forma $\langle m\rangle$ para algún $m \in \mathbb{Z}$.



A.4.2. Proposición. *El mcm siempre existe: tenemos*

$$\langle a\rangle \cap \langle b\rangle = \langle m\rangle \quad \textit{donde } m = \operatorname{mcm}(a,b).$$

Tenemos las siguientes propiedades.

1) La definición caracteriza a $\operatorname{mcm}(a,b)$ de modo único salvo signo.

2) Para cualesquiera $a, b \in \mathbb{Z}$ se tiene

$$\operatorname{mcm}(a,b) = \operatorname{mcm}(b,a).$$

3) Para todo a se cumple

$$\operatorname{mcm}(a,0) = a.$$

En particular,

$$\operatorname{mcm}(0,0) = 0.$$

(De hecho, $0 \mid m$ implica que $m = 0$.)

A.4.3. Proposición. *Para cualesquiera $a, b \in \mathbb{Z}$ tenemos*

$$\operatorname{mcm}(a,b) \cdot \operatorname{mcd}(a,b) = ab.$$

En particular,

$$\operatorname{mcm}(a,b) = ab \textit{ si y solamente si } a \textit{ y } b \textit{ son coprimos.}$$

Demostración. El caso de $a = b = 0$ es trivial y podemos descartarlo. Sea $d := \operatorname{mcd}(a,b)$ y $m := ab/d$. Vamos a ver que $m = \operatorname{mcm}(a,b)$.

Primero, puesto que $d \mid a$ y $d \mid b$, podemos escribir

$$a = da', \quad b = db'.$$

Luego,

$$m = da'b' = ab' = ba',$$

así que $a \mid m$ y $b \mid m$.

Ahora notemos que

$$d = \operatorname{mcd}(a,b) = \operatorname{mcd}(da', db') = d \cdot \operatorname{mcd}(a', b'),$$

así que

$$\operatorname{mcd}(a', b') = 1$$

y los números a' y b' son coprimos.

Sea m' otro número tal que $a \mid m'$ y $b \mid m'$. Queremos ver que $m \mid m'$. Escribamos

$$m' = ax = by.$$

Luego,

$$m'b' = ab'x = mx, \quad m'a' = ba'y = my,$$

lo que nos da $m \mid m'b'$ y $m \mid m'a'$ y por lo tanto

$$m \mid \operatorname{mcd}(m'b', m'a') = m' \cdot \operatorname{mcd}(a', b') = m'.$$

■

Note que la última proposición nos dice básicamente que la existencia de $\operatorname{mcd}(a, b)$ es equivalente a la existencia de $\operatorname{mcm}(a, b)$.

También se pueden definir mcd y mcm de n números. El lector puede generalizar de manera evidente las definiciones A.3.1 y A.4.1 y ver que estas generalizaciones son equivalentes a

1) $\langle a_1, \ldots, a_n \rangle = \langle d \rangle$ para $d = \operatorname{mcd}(a_1, \ldots, a_n)$,

2) $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle = \langle m \rangle$ para $m = \operatorname{mcm}(a_1, \ldots, a_n)$.

Por ejemplo, tenemos la siguiente generalización de la identidad de Bézout: existen $x_1, \ldots, x_n \in \mathbb{Z}$ tales que

$$x_1 a_1 + \cdots + x_n a_n = \operatorname{mcd}(a_1, \ldots, a_n).$$

Además, se puede ver que las operaciones $\operatorname{mcd}(-,-)$ y $\operatorname{mcm}(-,-)$ son asociativas y por lo tanto la definición generalizada se reduce al caso binario:

1) $\operatorname{mcd}(\operatorname{mcd}(a, b), c) = \operatorname{mcd}(a, \operatorname{mcd}(b, c)) = \operatorname{mcd}(a, b, c)$,

2) $\operatorname{mcm}(\operatorname{mcm}(a, b), c) = \operatorname{mcm}(a, \operatorname{mcm}(b, c)) = \operatorname{mcm}(a, b, c)$.

A.5 El teorema fundamental de la aritmética

A.5.1. Definición. Sea p un número primo fijo. Para un número entero no nulo n su **valuación p-ádica** es el número natural máximo k tal que p^k divide a n:

$$v_p(n) := \operatorname{máx}\{k \mid p^k \mid n\}.$$

(Para $n = 0$ normalmente se pone $v_p(0) := +\infty$, pero no vamos a necesitar esta convención.)

Notamos que $v_p(n) = 0$ si y solamente si $p \nmid n$. La valuación p-ádica se caracteriza por

$$n = p^{v_p(n)}\, n',$$

donde $p \nmid n'$ (véase A.3.5).

A.5.2. Lema. *Para cualesquiera $m, n \in \mathbb{Z}$ se cumple*

$$v_p(mn) = v_p(m) + v_p(n).$$

Demostración. Tenemos

$$m = p^{v_p(m)}\, m', \quad n = p^{v_p(n)}\, n',$$

donde $p \nmid m'$ y $p \nmid n'$. Luego,

$$mn = p^{v_p(m)+v_p(n)}\, m'n',$$

donde $p \nmid (m'n')$, así que $v_p(mn) = v_p(m) + v_p(n)$. ■

A.5.3. Teorema. *Todo número entero entero no nulo puede ser representado de modo único como*

$$n = \pm p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$$

donde p_i son algunos primos diferentes. A saber, tenemos $k_i = v_{p_i}(n)$.

(La unicidad se entiende salvo permutaciones de los factores $p_i^{k_i}$.)

Demostración. Ya hemos notado en A.2.3 que todo entero no nulo es un producto de primos; la parte interesante es la unicidad. Dada una expresión

$$n = \pm p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell},$$

para todo primo p podemos calcular la valuación p-ádica correspondiente:

$$v_p(n) = v_p(p_1^{k_1}) + v_p(p_2^{k_2}) + \cdots + v_p(p_\ell^{k_\ell}).$$

Aquí

$$v_p(p_i^{k_i}) = \begin{cases} k_i, & p = p_i, \\ 0, & p \neq p_i. \end{cases}$$

Entonces, $k_i = v_{p_i}(n)$. ■

Entonces, podemos escribir

$$n = \pm \prod_{p \text{ primo}} p^{v_p(n)},$$

donde el producto es sobre todos los números primos, pero $v_p(n) \neq 0$ solamente para un número finito de p.

El último resultado se conoce como el **teorema fundamental de la aritmética**. Su primera demostración completa fue publicada por Gauss en el tratado "Disquisitiones Arithmeticae".

Notamos que

$$\operatorname{mcd}(m,n) = \prod_{p \text{ primo}} p^{\min\{v_p(m), v_p(n)\}}$$

y

$$\operatorname{mcm}(m,n) = \prod_{p \text{ primo}} p^{\max\{v_p(m), v_p(n)\}}.$$

Estas fórmulas no ayudan mucho para grandes valores de m y n. En práctica se usa el **algoritmo de Euclides** basado en la división con resto repetida (es algo parecido a nuestra demostración de A.1.2).

A.6 Generalizaciones

Las definiciones A.3.1 y A.4.1 de mcd y mcm tienen sentido en cualquier dominio de integridad R. En este caso $\operatorname{mcm}(a,b)$ y $\operatorname{mcd}(a,b)$ están definidos salvo un múltiplo $u \in R^\times$. Para $R = \mathbb{Z}$ tenemos $\mathbb{Z}^\times = \{\pm 1\}$. Sin embargo, la existencia de $\operatorname{mcm}(a,b)$ y $\operatorname{mcd}(a,b)$ no está garantizada en general.

Un dominio de integridad donde se puede definir un análogo de la división con resto se llama un **dominio euclidiano**; en este caso mcd y mcm siempre existen gracias a los mismos argumentos que vimos arriba (solo hay que reemplazar los subgrupos $A \subseteq \mathbb{Z}$ por **ideales** $I \subseteq R$). Un ejemplo típico de dominios euclidianos, excepto $\mathbb{Z}$, es el anillo de polinomios $k[X]$ sobre un cuerpo k: para $f, g \in k[X]$, $g \neq 0$ existen $q, r \in k[X]$ tales que $f = qg + r$ donde $-\infty \leq \deg r < \deg g$.

Un dominio de integridad donde se cumple la factorización única (un análogo del teorema fundamental de la aritmética) se llama un **dominio factorización única**. Un típico ejemplo es el anillo de polinomios $k[X_1, \ldots, X_n]$ en n variables sobre un cuerpo k. Todos los dominios euclidianos son dominios de factorización única.

Todo esto se estudiará en la continuación de nuestro curso.

Bibliografía

[IR1990] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716
https://doi.org/10.1007/978-1-4757-2103-4

[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*, 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