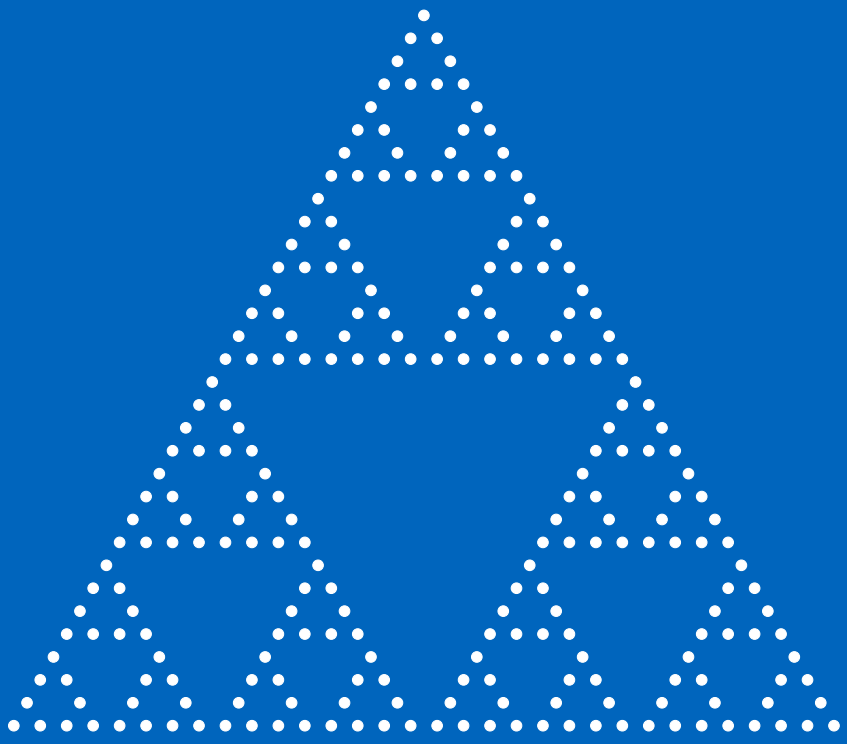
Curso de
Álgebra



Alexey Beshenov
Universidad de El Salvador
2018

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 di 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.

El nombre oficial del curso es "Álgebra moderna", pero esta es una expresión bastante anticuada: su origen es el libro de texto "Moderne Algebra" publicado en alemán en 1930–1931 por el matemático holandés B.L. van der Waerden, que a su vez se basaba en los cursos compartidos en 1924–1926 por Emil Artin y Emmy Noether, los pioneros del álgebra moderna. Aunque la influencia de van der Waerden todavía se percibe en la enseñanza de la materia, el mismo autor nombró las subsiguientes ediciones de su libro simplemente "Álgebra". Creo que en el siglo XXI no es necesario decorar la palabra "álgebra" por ningún epíteto ("abstracta", "moderna", etc.).

Considero conveniente explicar los prerrequisitos asumidos. Actualmente en San Salvador álgebra es una materia del cuarto año de licenciatura, y la preceden cursos de la teoría de números elemental y álgebra lineal. Por esto mis lecciones asumen un conocimiento de dichas materias y un cierto nivel de madurez matemática por parte del lector. Por otro lado, he tratado de enfatizar desde el principio el punto de vista categórico, usando diagramas conmutativos y propiedades universales.

Ahora voy a describir brevemente los contenidos del curso.

La parte I contiene una breve introducción a las estructuras algebraicas básicas: grupos, anillos y cuerpos. Allí se encuentran principalmente ejemplos y la teoría más sistemática se pospone para el resto del curso.

En particular, la parte II está dedicada a la teoría de grupos: se definen las nociones y construcciones fundamentales como homomorfismos, generadores de grupos, grupos cociente, abelianización, acciones sobre conjuntos y productos. En la parte III se estudian los anillos conmutativos y la parte IV está dedicada a los cuerpos.

La página oficial del curso es http://cadadr.org/san-salvador/algebra/ Allí se podrá encontrar la versión más reciente de este documento.

Favor de enviar sus comentarios a cadadr@gmail.com.

Ejercicios

Todos los capítulos de estos apuntes, salvo el capítulo 0, contienen ejercicios. La mayoría son bastante típicos y no deberían de 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 Dr. José Nerys Funes Torres y al director del Programa "Jovenes Talento" Prof. Ernesto Américo 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 leyeron una versión preliminar de estos apuntes e hicieron varios comentarios útiles. Gabriel me brindó una ayuda inestimable con la redacción de este texto.

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

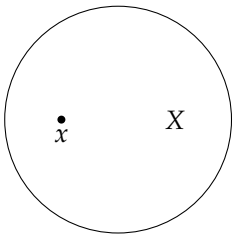
Índice general

Parte I
Primer encuentro con 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 "$X \ni x$".

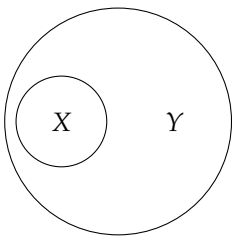


- El **conjunto vacío** se denota por $\emptyset$. Es el conjunto que no tiene ningún elemento:

$$|\emptyset| = 0.$$

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

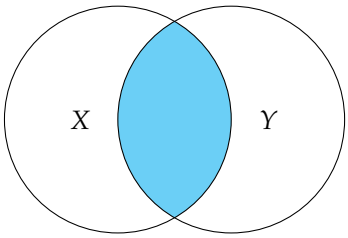
$$x \in X \Rightarrow x \in Y.$$



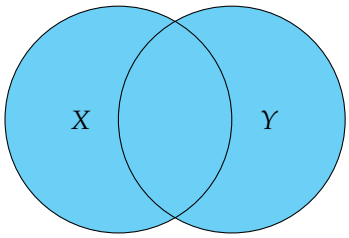
A veces para subrayar que X está contenido en Y, pero $X \neq Y$, se escribe "$X \subsetneq Y$" o "$Y \supsetneq X$".

- La **intersección** y **unión** de dos conjuntos X y Y se denotan por "$X \cap Y$" y "$X \cup Y$" respectivamente:

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



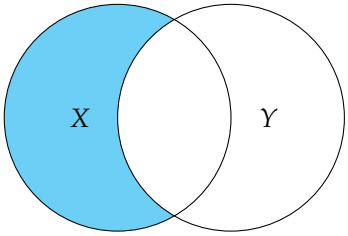
$X \cap Y$



$X \cup Y$

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

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



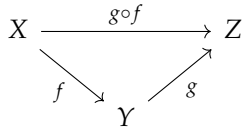
$X \setminus Y$

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

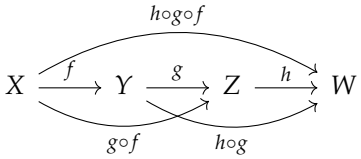
$$(g \circ f)(x) := g(f(x)).$$

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:

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

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

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

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

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

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

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

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

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

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

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,

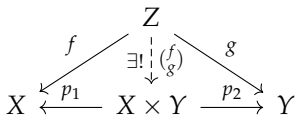
$$\{\☺\} \times X \cup \{\☹\} \times Y.$$

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)

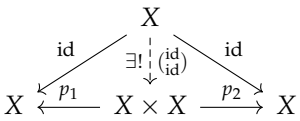


Demostración. Se ve que la única opción posible es

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

■

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



la aplicación

$$\Delta_X := \binom{\mathrm{id}_X}{\mathrm{id}_X}\colon X \to X \times X$$

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

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

$$\begin{array}{ccccc} X & \xleftarrow{p_1} & X \times Y & \xrightarrow{p_2} & Y \\ {\scriptstyle f}\downarrow & & \exists!\,\vdots\,{\scriptstyle f\times g} & & \downarrow{\scriptstyle g} \\ X' & \xleftarrow{p_1'} & X' \times Y' & \xrightarrow{p_2'} & Y' \end{array}$$

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)

$$\begin{array}{ccccc} X & \xrightarrow{i_1} & X \sqcup Y & \xleftarrow{i_2} & Y \\ & {\scriptstyle f}\searrow & \exists!\,\vdots\,{\scriptstyle (f,g)} & \swarrow{\scriptstyle g} & \\ & & Z & & \end{array}$$

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 (10.1), 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

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

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,

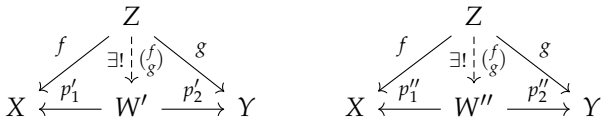
$$g \circ f = \mathrm{id}_T, \quad f \circ g = \mathrm{id}_{T'},$$

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.

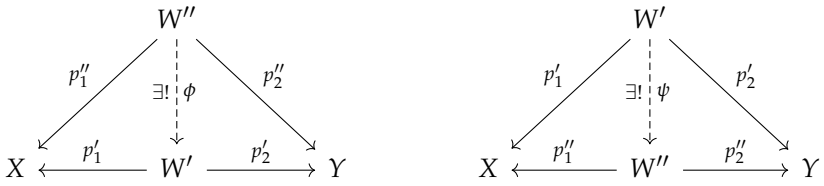
Para ver otro ejemplo más interesante de este tipo de razonamiento, consideremos el caso del producto $X \times Y$. Supongamos que hay dos conjuntos W' y W'' junto con algunas aplicaciones

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

y cada uno satisface la propiedad universal (10.1):



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

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

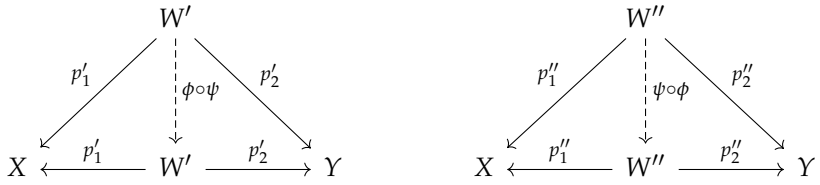
Podemos considerar sus composiciones

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

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 (¿qué 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.

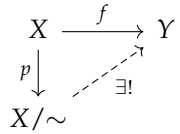
0.7.6. Observación (Propiedad universal del cociente $X/\sim$). *Para una relación de equivalencia $\sim$ sobre X, consideremos la aplicación canónica*

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

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

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

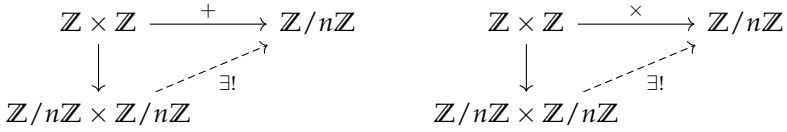
De hecho, si $a - a' = n\,c$ y $b - b' = n\,d$, entonces $(a + b) - (a' + b') = n\,(c + d)$. De la misma manera, tenemos

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

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:



Las flechas punteadas están definidas por

$$[a]_n + [b]_n = [a + b]_n,$$
$$[a]_n \cdot [b]_n = [ab]_n.$$

▲

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

(1.1)
$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

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

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

mientras que

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

▲

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

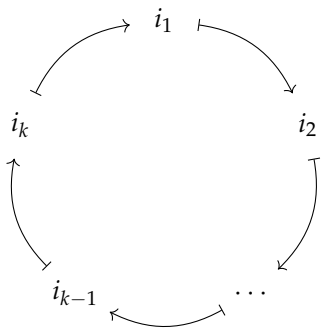
$$\begin{aligned} \sigma(i_1) &:= i_2, \\ \sigma(i_2) &:= i_3, \\ &\vdots, \\ \sigma(i_{k-1}) &:= i_k, \\ \sigma(i_k) &:= i_1 \end{aligned}$$

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,

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

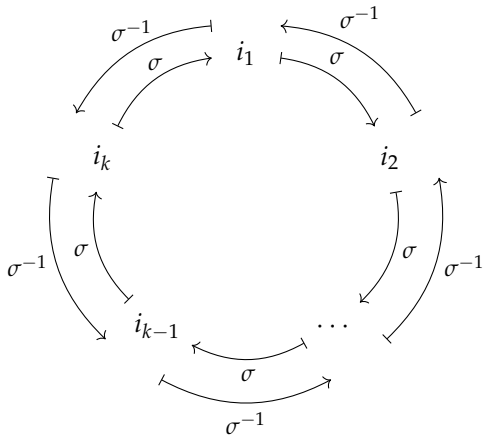
y

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

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

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

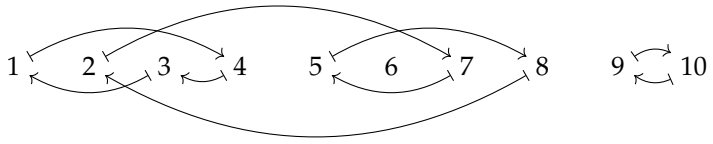
y otro ciclo es $(2\ 7\ 5\ 8)$. Luego, 6 es un punto fijo: tenemos $\sigma(6) = 6$ y un ciclo (6). Nos quedan 9 y 10:

$$9 \mapsto 10 \mapsto 9$$

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
$p(n)$:	1	2	3	5	7	11	15	22	30	42
n:	11	12	13	14	15	16	17	18	19	20
$p(n)$:	56	77	101	135	176	231	297	385	490	627

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 $1 \leq k \leq n$), 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

> Cuando alguno me muestra un signo, si ignoro lo que significa no me puede enseñar nada; pero si lo sé, ¿qué es lo que aprendo por el signo?
>
> San Agustín, "El Maestro", Capítulo X

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

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

$1 \leftrightarrow$	2	3	4
2	$1 \leftrightarrow$	3	4
2	3	$1 \leftrightarrow$	4
2	$3 \leftrightarrow$	4	1
$2 \leftrightarrow$	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**.

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 (*trivialmente*). 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,

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

■

[*] 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.

2.2.2. 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*

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

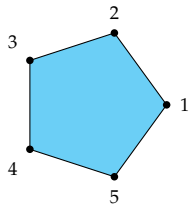
En general,

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

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

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

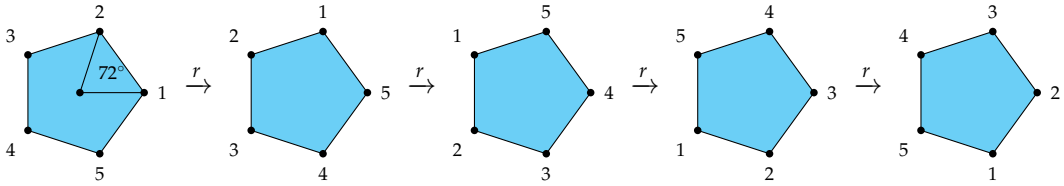
Aquí escribimos

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

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

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

(es la rotación de 360°).

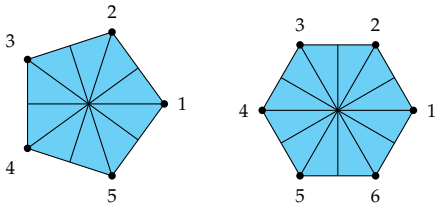


[*]Del griego "di-", "dos" y "edra", que en este caso significa "cara". Por ejemplo, de la misma manera la palabra "dilema" significa "dos lemas [proposiciones]". El término "poliedro" significa una figura que tiene varias caras. En este caso P es una figura plana y entonces se puede decir que P tiene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

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

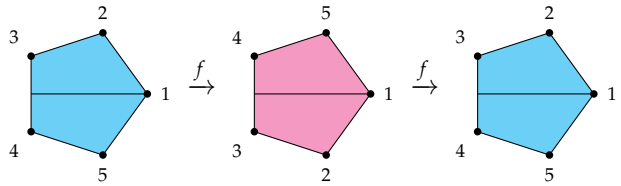
Las reflexiones que preservan P son precisamente las reflexiones respecto a los ejes de simetría de nuestro polígono regular. En total tenemos n ejes de simetría:

- 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:

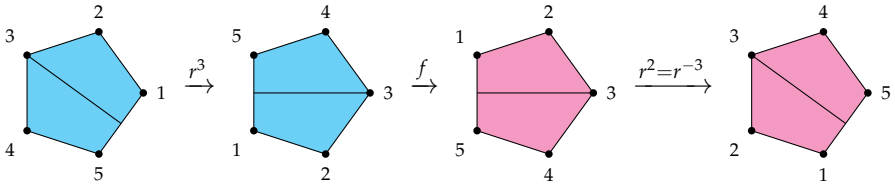
$$f \neq r^i \quad \text{para ningún } i,$$

y en general, los elementos

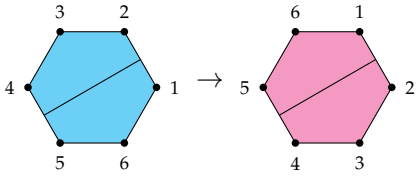
$$f, f \circ r, f \circ r^2, f \circ r^3, \ldots, f \circ r^{n-1}$$

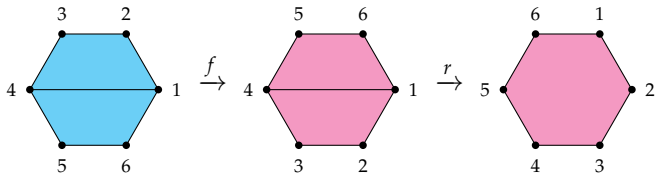
son distintos y no coinciden con los r^i.

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:

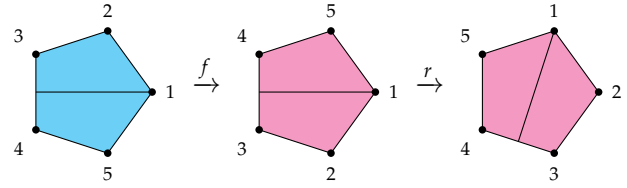


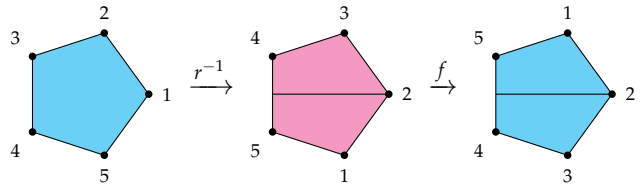


Entonces, hemos visto que todas las simetrías del n-ágono regular pueden ser expresadas como sucesiones de aplicaciones de r y f. Notamos que

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

en palabras: una reflexión seguida por una rotación de $360^\circ/n$ es lo mismo que la rotación de $360^\circ/n$ 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

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

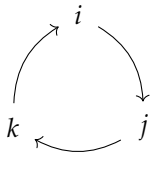
Los cuadrados de i, j, k son iguales a -1:

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

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.*

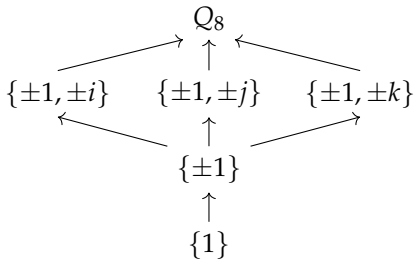
Demostración. Claro a partir de la definición de subgrupo. ■

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

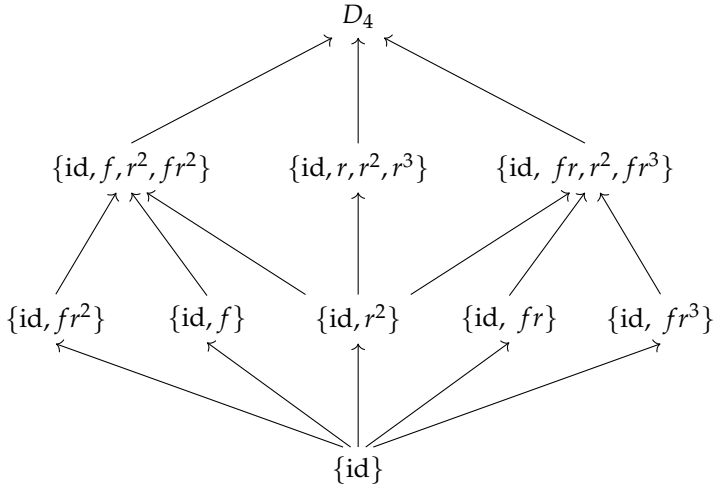
$$D_4 = \{\mathrm{id},\ r,\ r^2,\ r^3,\ f,\ fr,\ fr^2,\ fr^3\}.$$

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**).

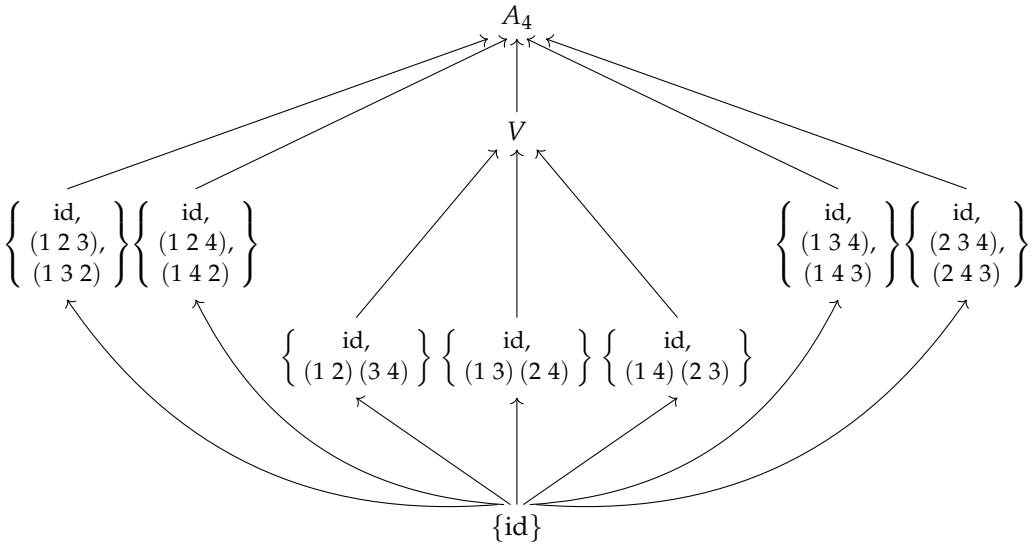
$\circ$	id	$(1\ 2)\ (3\ 4)$	$(1\ 3)\ (2\ 4)$	$(1\ 4)\ (2\ 3)$
id	id	$(1\ 2)\ (3\ 4)$	$(1\ 3)\ (2\ 4)$	$(1\ 4)\ (2\ 3)$
$(1\ 2)\ (3\ 4)$	$(1\ 2)\ (3\ 4)$	id	$(1\ 4)\ (2\ 3)$	$(1\ 3)\ (2\ 4)$
$(1\ 3)\ (2\ 4)$	$(1\ 3)\ (2\ 4)$	$(1\ 4)\ (2\ 3)$	id	$(1\ 2)\ (3\ 4)$
$(1\ 4)\ (2\ 3)$	$(1\ 4)\ (2\ 3)$	$(1\ 3)\ (2\ 4)$	$(1\ 2)\ (3\ 4)$	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
subgrupos de S_n:	2	6	30	156	1455	11 300	151 221	1 694 723	29 594 446
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

$$\mathrm{Aff}_1(\mathbb{R}) := \{\phi_{a,b} \mid a \in \mathbb{R} \setminus \{0\},\ b \in \mathbb{R}\}.$$

Verifique que $\mathrm{Aff}_1(\mathbb{R})$ *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.)*

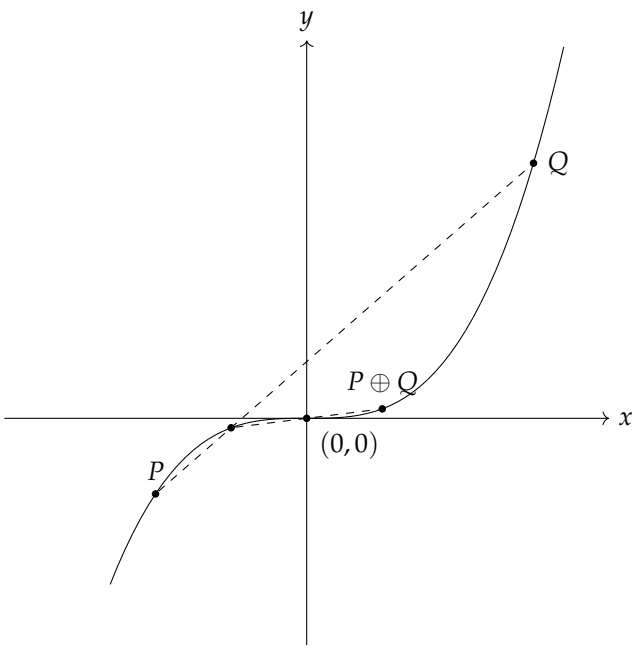
Ejercicio 2.8. *Consideremos el conjunto de puntos* (x, y) *en el plano real que satisfacen la ecuación* $y = x^3$:

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

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 (primer encuentro)

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

$$[a]_n + [b]_n := [a+b]_n,$$
$$[a]_n \cdot [b]_n := [ab]_n.$$

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 y la identidad son los números $0 + 0 \cdot \sqrt{-1}$ y $1 + 0 \cdot \sqrt{-1}$ respectivamente. 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

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

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 $\zeta_n := e^{2\pi\sqrt{-1}/n}$ se cumple $\sum_{0\le k<n} \zeta_n^k = 0$.) Consideremos el conjunto

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

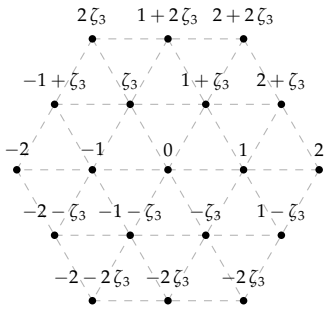
Está claro que para cualesquiera $x, y \in \mathbb{Z}[\zeta_3]$ se tiene $x + y \in \mathbb{Z}[\zeta_3]$. Para la multiplicación, si $x = a + b\,\zeta_3$ e $y = c + d\,\zeta_3$, entonces

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

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.



▲

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

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

[*] 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).

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

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

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 $n \geq 2$: 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 es nulo y 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, $\operatorname{mcd}(a, n) = 1$. De hecho, si $\operatorname{mcd}(a, n) = 1$, entonces tenemos la identidad de Bézout*

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

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

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 (Euler). *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**. En efecto, es la aplicación identidad: tenemos $x^p = x$ para todo $x = \mathbb{F}_p$.

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

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

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

3.4.7. Proposición (Lagrange, 1768). *Sea $f \in R[X]$ un polinomio no nulo con coeficientes en un dominio de integridad R. Entonces f tiene $\le \deg f$ 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

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

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

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

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

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

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:

$$\begin{aligned} a_n &= b_{n-1}, \\ a_{n-1} &= b_{n-2} - c b_{n-1}, \\ a_{n-2} &= b_{n-3} - c b_{n-2}, \\ &\cdots \\ a_1 &= b_0 - c b_1, \\ a_0 &= b_{-1} - c \, b_0 \end{aligned}$$

y nos lleva a las recurrencias

$$\begin{aligned} b_{n-1} &= a_n, \\ b_{n-2} &= a_{n-1} + c b_{n-1}, \\ b_{n-3} &= a_{n-2} + c b_{n-2}, \\ &\cdots \\ b_i &= a_{i+1} + c b_{i+1}, \\ &\cdots \\ b_0 &= a_1 + c b_1, \\ b_{-1} &= a_0 + c b_0 \end{aligned}$$

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

$$b_{n-1} = a_n \quad \text{y} \quad b_i = a_{i+1} + c b_{i+1} \text{ para } -1 \le i \le n-1,$$

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.

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*).

[*] William George Horner (1786–1837), matemático inglés.

3.5 ¿Para qué sirven los anillos?

Hay mucho más ejemplos importantes de anillos conmutativos y cuerpos, pero no es el tema principal de esta parte del 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 (véase el apéndice B).

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**.

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

$$|z| := \sqrt{z\,\overline{z}} = \sqrt{(x + y\sqrt{-1}) \cdot (x - y\sqrt{-1})} = \sqrt{x^2 + y^2}.$$

[*]No confundir con *la identidad* $1 \in R$, que es nada más un ejemplo muy particular de unidades.

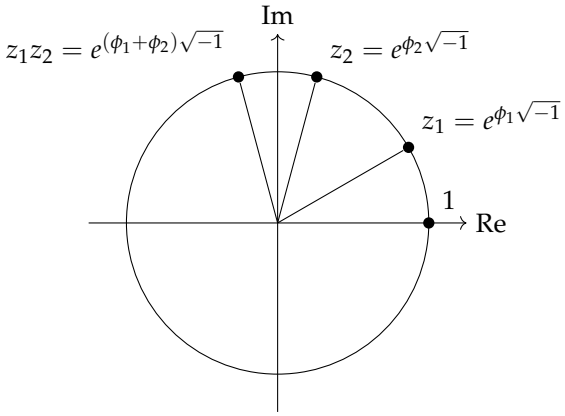
Notamos que para cualesquiera $z_1, z_2 \in \mathbb{C}$ se cumple

$$|z_1 z_2| = |z_1| \cdot |z_2|.$$

Se ve que el conjunto de los números complejos de valor absoluto 1

$$\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\} = \{e^{\phi\sqrt{-1}} \mid 0 \leq \phi < 2\pi\}$$

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

$$z^n = 1.$$

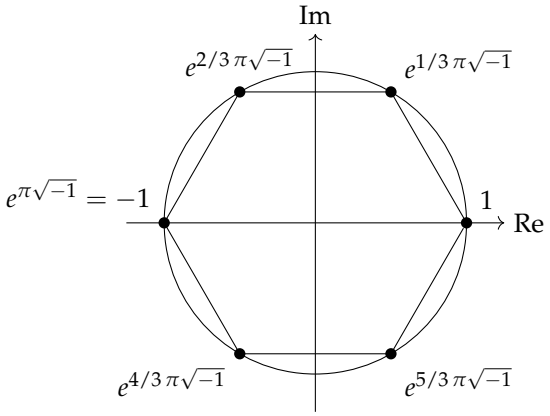
Como sabemos, esta ecuación tiene precisamente n soluciones diferentes

$$e^{2\pi k\sqrt{-1}/n}, \quad k = 0, 1, \ldots, n-1.$$

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

$$\mu_m(\mathbb{C}) \overset{\text{si } m|n}{\subset} \mu_n(\mathbb{C}) \subset \mu_\infty(\mathbb{C}) \subset \mathbb{S}^1 \subset \mathbb{C}^\times.$$

▲

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 $\operatorname{mcd}(a, n) = 1$:

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

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
$\phi(n)$:	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8
n:	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\phi(n)$:	8	16	6	18	8	12	10	22	8	20	12	18	12	28	8

La función ϕ de Euler 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,

$$\phi(p^k) = p^k - p^k/p = p^k \left(1 - \frac{1}{p}\right).$$

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. ▲

[*]Tenemos $\phi(1) = 1$. De hecho, $\mathbb{Z}/1\mathbb{Z}$ es el anillo nulo, y su único elemento es invertible.

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

$$a + b\sqrt{2} \quad \text{si y solamente si} \quad N(a + b\sqrt{2}) = a^2 - 2b^2 = 1.$$

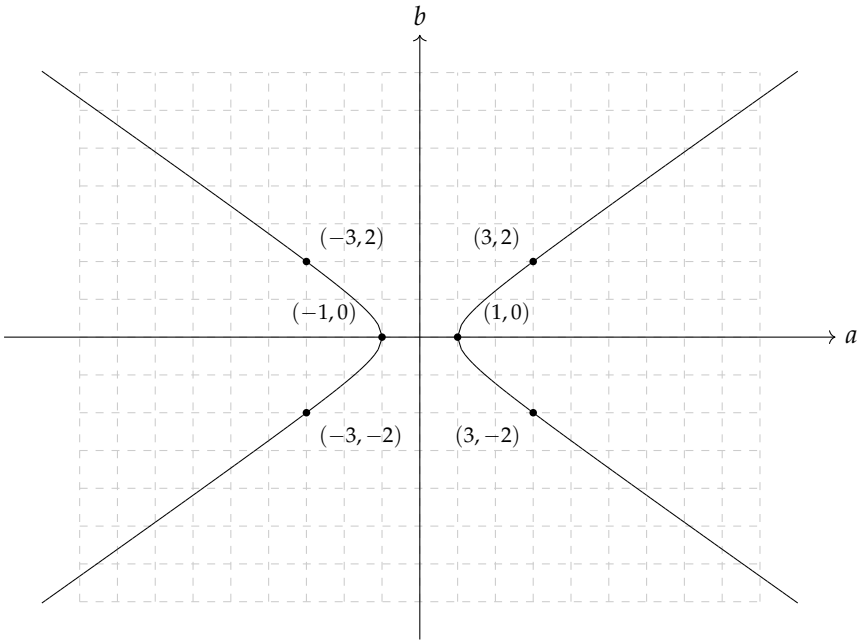
Entonces, para calcular el grupo $\mathbb{Z}[\sqrt{2}]$, hay que encontrar las soluciones enteras de la ecuación

$$a^2 - 2b^2 = \pm 1.$$

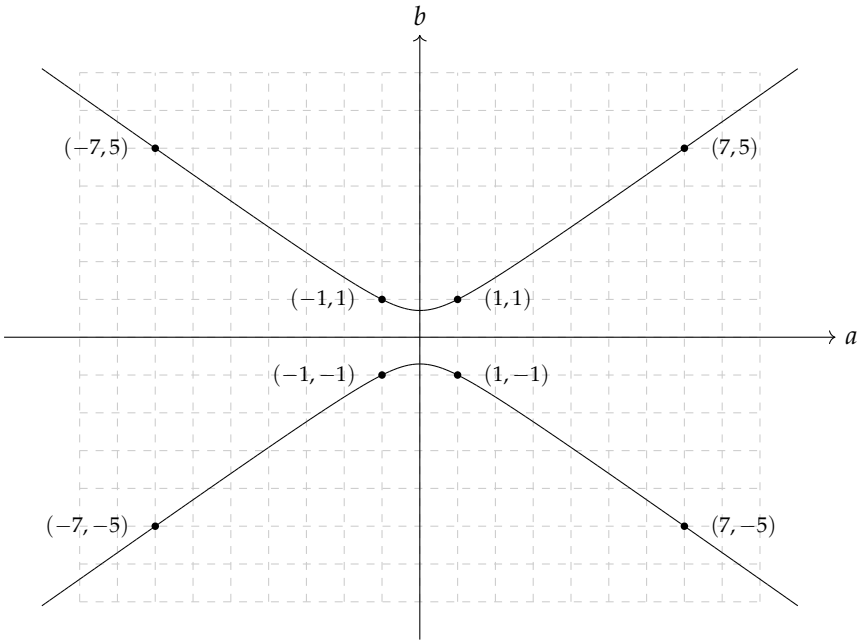
Esta se conoce como la **ecuación de Pell**[*]. No vamos a entrar en los detalles, pero hay un número infinito de soluciones $(a, b) \in \mathbb{Z}^2$. Por ejemplo,

$$(a, b) = (\pm 1, 0),\ (\pm 1, \pm 1),\ (\pm 3, \pm 2),\ (\pm 7, \pm 5),\ \ldots \tag{4.3}$$

[*] 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:

$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$$

—véase [AW2004, §11.1] para una prueba. ▲

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")

$$A^{-1} = \det(A)^{-1}\ \mathrm{adj}(A),$$

donde $\mathrm{adj}(A)$ 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[*]

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1) \cdot (p^n - p) \cdots (p^n - p^{n-1}).$$

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[**].

[*] 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".

[**] 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,

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \pmod 2.$$

$\cdot$	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.

$\circ$	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 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 $\mathbb{Z}[\![X]\!]$.*

[*] En este ejercicio hay que identificar las aplicaciones lineales $\mathbb{R}^2 \to \mathbb{R}^2$ con matrices de 2×2.

Parte II
Teoría de grupos

Capítulo 5
Homomorfismos de grupos

> 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

$$\begin{aligned} v_p\left(\frac{m_1}{n_1}\cdot\frac{m_2}{n_2}\right) = v_p\left(\frac{m_1m_2}{n_1n_2}\right) &= v_p(m_1m_2) - v_p(n_1n_2) \\ &= v_p(m_1) - v_p(n_1) + v_p(m_2) - v_p(n_2) = v_p\left(\frac{m_1}{n_1}\right) + v_p\left(\frac{m_2}{n_2}\right). \end{aligned}$$

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 **resíduo cuadrático módulo** p si

$$a \equiv b^2 \pmod{p}$$

para algún $b \in \mathbb{Z}$. Podemos definir el **símbolo de Legendre** mediante

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{si } p \nmid a \text{ y } a \text{ es un resíduo cuadrático módulo } p, \\ -1, & \text{si } p \nmid a \text{ y } a \text{ no es un resíduo cuadrático módulo } p, \\ 0, & \text{si } p \mid a. \end{cases}$$

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 resíduos cuadráticos es un resíduo cuadrático; un poco menos claro que el producto de dos no-resíduos cuadráticos es un resíduo cuadrático, pero lo

veremos más adelante). Esto quiere decir que el símbolo de Legendre es un homomorfismo de grupos multiplicativos

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\},$$
$$[a]_p \mapsto \left(\frac{a}{p}\right).$$

▲

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

$$f = \sum_{0 \le i \le n} a_i\, X^i \in R[X],$$

su valor en $c \in R$ viene dado por

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

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":

$$R[\![X]\!] \to R,$$
$$f = \sum_{i\geq 0} a_i X^i \mapsto f(0) = a_0.$$

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

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

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

$$\begin{aligned}(f_2 \circ f_1)(g_1g_2) = f_2(f_1(g_1g_2)) = f_2(f_1(g_1)\,f_1(g_2)) = f_2(f_1(g_1)) \cdot f_2(f_1(g_2)) \\ = (f_2 \circ f_1)(g_1) \cdot (f_2 \circ f_1)(g_2).\end{aligned}$$

■

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.

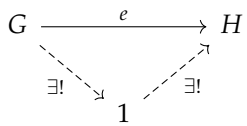
$$f(g^{-1}) \cdot f(g) = f(g^{-1}\,g) = f(1) = 1.$$

■

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 $\emptyset \to X$ y una aplicación única $X \to \{\bullet\}$. Los conjuntos $\emptyset$ 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 $e^z = e^{z+2\pi k\sqrt{-1}}$. ▲

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

$$\begin{aligned} f^{-1}(h_1h_2) = f^{-1}\Big(f(f^{-1}(h_1)) \cdot f(f^{-1}(h_2))\Big) = f^{-1}\Big(f\big(f^{-1}(h_1) \cdot f^{-1}(h_2)\big)\Big) \\ = f^{-1}(h_1) \cdot f^{-1}(h_2), \end{aligned}$$

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

$$\operatorname{im} f := \{f(g) \mid g \in G\}$$

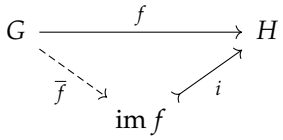
se llama la **imagen** de f.

5.4.2. Observación. *Para todo homomorfismo $f\colon G \to H$ la imagen $\operatorname{im} f$ es un subgrupo de H.*

Demostración. Como hemos notado en 5.2.2, tenemos $1_H \in \operatorname{im} f$. Luego, si $f(g_1), f(g_2) \in \operatorname{im} f$, entonces $f(g_1)\,f(g_2) = f(g_1 g_2) \in \operatorname{im} f$. En fin, gracias a 5.2.3, si $f(g) \in \operatorname{im} f$, entonces $f(g)^{-1} = f(g^{-1}) \in \operatorname{im} f$. ■

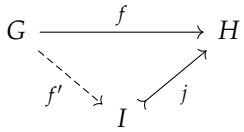
5.4.3. Proposición (Propiedad universal de la imagen). *Sea $f\colon G \to H$ un homomorfismo de grupos.*

1) *Existe una factorización de f por el monomorfismo canónico $i\colon \operatorname{im} f \rightarrowtail H$ (inclusión de subgrupo):*



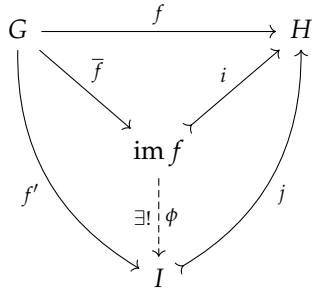
$$f = i \circ \overline{f}.$$

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:

$$A_n := \ker(S_n \xrightarrow{\mathrm{sgn}} \{\pm 1\}).$$

▲

5.5.4. Ejemplo. Tenemos

$$\ker(\mathbb{R}^\times \xrightarrow{\mathrm{sgn}} \{\pm 1\}) = \mathbb{R}_{>0}.$$

▲

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

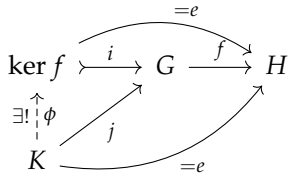
$$\ker(\exp\colon \mathbb{C} \to \mathbb{C}^\times) = 2\pi\sqrt{-1}\,\mathbb{Z} = \{2\pi n\sqrt{-1} \mid n \in \mathbb{Z}\} \subset \mathbb{C}.$$

Por esto en el caso complejo, el logaritmo es más sutil: la exponencial toma el mismo valor en $z + 2\pi n\sqrt{-1}$ 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*

$$\begin{array}{ccccc} \ker f & \rightarrowtail & G & \xrightarrow{f} & H \\ \vdots\exists! & & {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ \ker f' & \rightarrowtail & G' & \xrightarrow[f']{} & H' \end{array}$$

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

f es un homomorfismo inyectivo $\iff$ f es cancelable por la izquierda
($f \circ g = f \circ g' \Rightarrow g = g'$ para homomorfismos g, g'),
f es un homomorfismo biyectivo $\iff$ f es invertible (existe homomorfismo f^{-1}).

El lector puede adivinar que también existe otra equivalencia

f es un homomorfismo sobreyectivo $\iff$ f es cancelable por la derecha
($g \circ f = g' \circ f \Rightarrow g = g'$ para homomorfismos g, g').

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 $f\colon G \to H$ un homomorfismo de grupos y sea $K \subset H$ un subgrupo. Demuestre que $f^{-1}(K)$ es un subgrupo de G.*

Ejercicio 5.2. *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 5.3. *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 5.4.

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 5.5. *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 5.6. *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 5.7. *Demuestre que los grupos $\mathbb{R}^\times$ y $\mathbb{C}^\times$ no son isomorfos.*

Ejercicio 5.8. *Asociemos a cada elemento del grupo de cuaterniones Q_8 una matriz compleja de la siguiente manera:*

$$\pm 1 \mapsto \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \quad \pm i \mapsto \begin{pmatrix} \pm\sqrt{-1} & 0 \\ 0 & \mp\sqrt{-1} \end{pmatrix},$$
$$\pm j \mapsto \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}, \quad \pm k \mapsto \begin{pmatrix} 0 & \pm\sqrt{-1} \\ \pm\sqrt{-1} & 0 \end{pmatrix}.$$

Demuestre que esta correspondencia es un monomorfismo $Q_8 \rightarrowtail \mathrm{SL}_2(\mathbb{C}) \subset \mathrm{GL}_2(\mathbb{C})$.

Ejercicio 5.9. *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 5.10. *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 5.11. *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 $\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$.*

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 $B\,A$ 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,

$$\langle X\rangle = \Big\{ n_1 \frac{a_1}{b_1} + \cdots + n_k \frac{a_k}{b_k} \;\Big|\; n_1, \ldots, n_k \in \mathbb{Z} \Big\}.$$

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,

$$\begin{aligned}\operatorname{ord}(\sigma) = \min\{k \mid \tau_1^k = \mathrm{id},\ \ldots,\ \tau_s^k = \mathrm{id}\} = \min\{k \mid \operatorname{ord}\tau_1 \mid k,\ \ldots,\ \operatorname{ord}\tau_s \mid k\} \\ = \operatorname{mcm}(\tau_1, \ldots, \tau_s).\end{aligned}$$

Por ejemplo, para la permutación $\sigma = (1\ 2)\ (3\ 4)\ (5\ 6\ 7)$ tenemos

$$\sigma^2 = (5\ 7\ 6),\ \sigma^3 = (1\ 2)\ (3\ 4),\ \sigma^4 = (5\ 6\ 7),\ \sigma^5 = (1\ 2)\ (3\ 4)\ (5\ 7\ 6),\ \sigma^6 = \mathrm{id}.$$

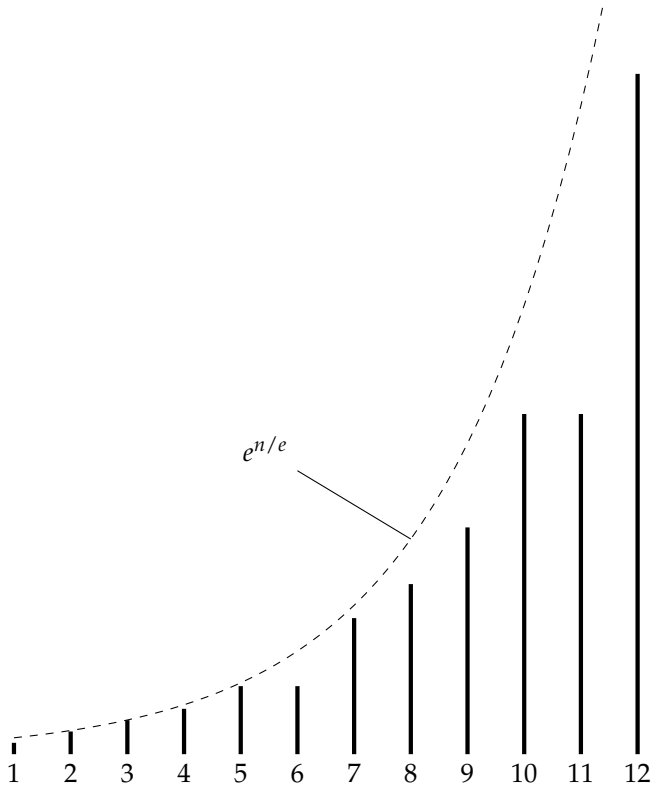
El número

$$g(n) := \max\{\operatorname{ord}\sigma \mid \sigma \in S_n\} = \max\{\operatorname{mcm}(n_1, \ldots, n_s) \mid n_1 + \cdots + n_s = n\}$$

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
$g(n)$:	1	2	3	4	6	6	12	15	20	30	30	60

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

$$\operatorname{ord} g^k = \operatorname{mín}\{m \mid (g^k)^m = 1\} = \operatorname{mín}\{m \mid n \mid km\} = \operatorname{mín}\{m \mid n' \mid m\} = n' = n/d.$$

■

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

$$G \to \mathbb{Z},$$
$$g^n \mapsto n$$

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

$$\mu_n(\mathbb{C}) \to \mathbb{Z}/n\mathbb{Z},$$
$$\zeta_n^k \mapsto [k]_n.$$

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

$$n\mathbb{Z} := \{0, \pm n, \pm 2n, \pm 3n, \ldots\}.$$

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. *Encuentre el orden de cada uno de los elementos del grupo diédrico D_n.*

Ejercicio 6.4. *Encuentre los órdenes de las siguientes matrices en* $\mathrm{SL}_2(\mathbb{Z})$*:*

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}.$$

Ejercicio 6.5. *Exprese la matriz* $\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$ *como un producto de matrices*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad y \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Ejercicio 6.6. *Demuestre que las matrices*

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad y \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

generan un subgrupo de $\mathrm{GL}_3(\mathbb{Z})$ *que es isomorfo a S_3.*

Ejercicio 6.7. *Demuestre que el subgrupo de* $\mathrm{GL}_2(\mathbb{Z})$ *generado por las matrices*

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad y \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

es isomorfo al grupo diédrico D_4,

Ejercicio 6.8. *Demuestre que el conjunto*

$$X = \{1/p^k \mid p \text{ primo}, k = 0, 1, 2, 3, \ldots\}$$

genera el grupo aditivo $\mathbb{Q}$.

Ejercicio 6.9. *Encuentre los elementos de orden finito en el grupo de isometrías del plano euclidiano* $\mathbb{R}^2 \to \mathbb{R}^2$.

Ejercicio 6.10. *Supongamos que G es un grupo finito de orden par. Demuestre que G tiene un elemento de orden* 2.

Ejercicio 6.11. *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 6.12. *Sea A un grupo abeliano (escrito en la notación aditiva).*

1) *Sea $m = 1, 2, 3, \ldots$ 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 6.13. *Consideremos $\mathbb{Q}$, el grupo de los números racionales respecto a la adición. Demuestre que todo subgrupo finitamente generado de $\mathbb{Q}$ es cíclico.*

Ejercicio 6.14. *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*

$$\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, A) \to A[m], \quad f \mapsto f([1]_m)$$

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 $m, n = 2, 3, 4, 5, \ldots$

Ejercicio 6.15. *Encuentre todos los homomorfismos entre el grupo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo n respecto a la adición y el grupo $\mathbb{C}^\times$ de los números complejos no nulos respecto a la multiplicación.*

Ejercicio 6.16. *Demuestre que* $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

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

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

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.

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

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

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

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

■

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

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

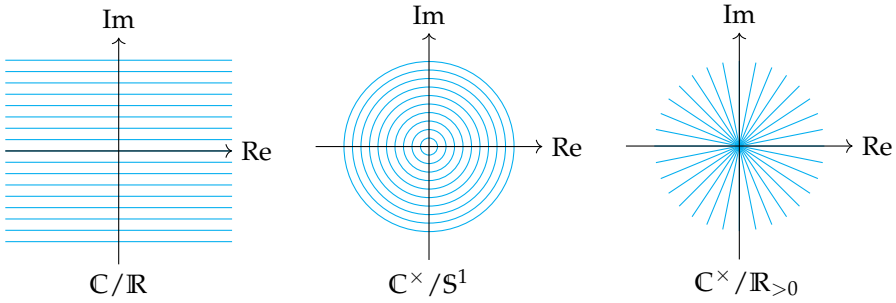
(el grupo del círculo) y

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

Los dibujos de abajo representan las clases laterales

$$\mathbb{C}/\mathbb{R} = \{z + \mathbb{R} \mid z \in \mathbb{C}\},$$
$$\mathbb{C}^\times/\mathbb{S}^1 = \{z\mathbb{S}^1 \mid z \in \mathbb{C}^\times\},$$
$$\mathbb{C}^\times/\mathbb{R}_{>0} = \{z\mathbb{R}_{>0} \mid z \in \mathbb{C}^\times\}$$

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,

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

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.

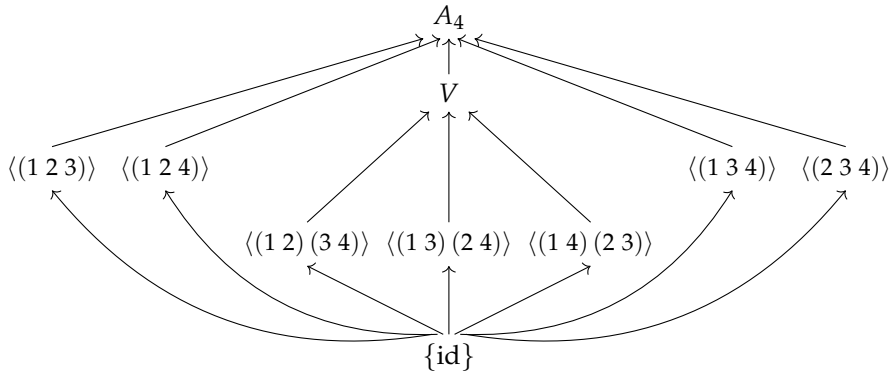
Si G es un subgrupo de orden 6, sus elementos necesariamente tienen orden 2 o 3; es decir, son 3-ciclos o permutaciones de la forma $(\bullet\ \bullet)\,(\bullet\ \bullet)$. Junto con cada 3-ciclo G debe contener su inverso. Las posibles opciones son

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

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.

3. Tenemos la siguiente tabla de multiplicación:

[*]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.

$\cdot$	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.

7.3 Aplicación seria: subgrupos finitos de $k^\times$

Terminemos esta sección por el siguiente resultado importante.

7.3.1. 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.

7.3.2. 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 7.3.1 [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 7.3.2. ■

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

7.3.4. 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 7.3.1 nos dice que todos los subgrupos finitos de $\mathbb{C}^\times$ son cíclicos. ▲

7.3.5. Ejemplo. Si $k = \mathbb{F}_q$ es un cuerpo finito (donde $q = p^k$ para algún primo p), 7.3.1 implica que el grupo $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ es cíclico de orden $q - 1$. Note que la demostración de 7.3.1 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

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

▲

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

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 o simplemente un **cuadrado módulo** p. Para un entero a tal que $p \nmid a$ el **símbolo de Legendre** se define mediante

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & a \text{ es un cuadrado,} \\ -1, & a \text{ no es un cuadrado,} \end{cases}$$

y si $p \mid a$, se pone $\left(\frac{a}{p}\right) := 0$.

7.3.6. Proposición. *Sea p un primo impar.*

1) *El producto de dos no-cuadrados es un cuadrado.*
2) *Hay precisamente $\frac{p+1}{2}$ cuadrados módulo p.*
3) *El **criterio de Euler**: para cualquier entero a se cumple la congruencia*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

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.

Para probar 3), notamos que si $p \mid a$ la congruencia es obvia. Si $p \nmid a$, tenemos $[a]_p = x^k$ para algún k, y esto es un cuadrado en $\mathbb{F}_p^\times$ si y solamente si k es par. Luego,

$$[a]_p^{(p-1)/2} = x^{k(p-1)/2}.$$

Si k es par, entonces $k(p-1)/2$ es divisible por $p-1 = \#\mathbb{F}_p^\times$, así que

$$x^{k(p-1)/2} = 1$$

gracias a 7.2.9. Si k es impar, entonces $k\frac{p-1}{2}$ no es divisible por $p-1$ y por ende

$$x^{k(p-1)/2} \neq 1.$$

Sin embargo,

$$\left(x^{k(p-1)/2}\right)^2 = x^{k(p-1)} = 1,$$

lo que nos permite concluir que

$$x^{k(p-1)/2} = -1.$$

(El polinomio $X^2 - 1$ tiene precisamente dos raíces en $\mathbb{F}_p$: son ± 1.) ■

7.3.7. Corolario (Primera ley suplementaria de reciprocidad cuadrática). *Para $p \neq 2$ se cumple*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases}$$

Demostración. Basta sustituir $a = -1$ en el criterio de Euler. ■

7.4 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**.

7.4.1. 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.

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

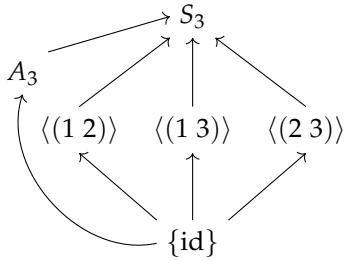
7.4.3. Ejemplo. Los subgrupos $\{1\}$ y G son normales. ▲

7.4.4. 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

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

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

7.4.5. 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. ▲

7.4.6. 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 $\sigma = \mathrm{id}$. ▲

7.4.7. 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

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

■

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

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

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

7.4.11. 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.

7.5 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.

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

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

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 $g_1, g_1', g_2, g_2' \in G$

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

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. ■

7.5.2. 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

$$g_1 H \cdot g_2 H = (g_1 g_2) H.$$

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

Como acabamos de ver, la fórmula de arriba tiene sentido: si H es normal, entonces la clase lateral $(g_1 g_2)H$ no depende de g_1 y g_2, sino de las clases laterales $g_1 H$ y $g_2 H$. 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 $(gH)^{-1} = g^{-1} H$.

7.5.3. 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.

7.5.4. Ejemplo. Todos los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$. 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. ▲

7.5.5. 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. ▲

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

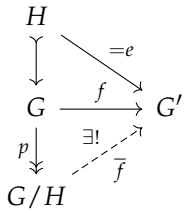
$$|A_4/V| = |A_4|/|V| = \frac{4!/2}{4} = 3,$$

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

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

$$\begin{aligned} p\colon G &\twoheadrightarrow G/H, \\ g &\mapsto gH \end{aligned}$$

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

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

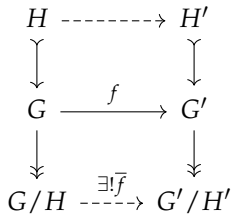
Es una aplicación bien definida: si $gH = g'H$ para algunos $g, g' \in G$, entonces $g^{-1}g' \in H$, luego $g^{-1}g' \in \ker f$ y

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

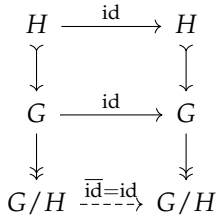
La aplicación $\overline{f}$ es un homomorfismo de grupos, puesto que f lo es. ■

7.5.8. Corolario (Funtorialidad del cociente).

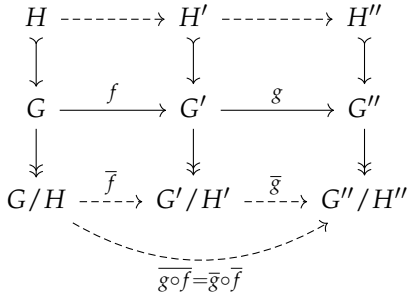
1) *Sea $f\colon G \to G'$ un homomorfismo de grupos. Sean $H \subseteq G$ y $H' \subseteq G'$ subgrupos normales. Supongamos que $f(H) \subseteq H'$. Entonces f induce un homomorfismo canónico $\widetilde{f}\colon G/H \to G'/H'$ que conmuta con las proyecciones canónicas:*



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. ■

7.6 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.

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

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

7.6.3. 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 lineal especial 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.

7.6.4. 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

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

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

7.6.5. 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.

7.6.6. 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. ■

7.6.7. 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 $H = A_n$. ■

7.6.8. 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. ■

7.6.9. 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. ■

7.6.10. 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 $(\bullet\ \bullet)\ (\bullet\ \bullet)$.

7.7 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.

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

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

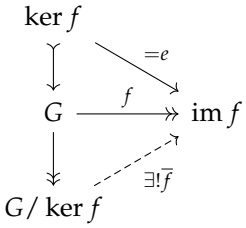
que hace parte del diagrama conmutativo

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

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 $G/\ker f$:



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.

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

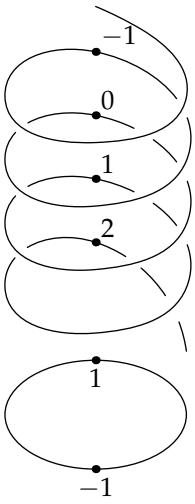
$$|G| = |\operatorname{im} f| \cdot |\ker f|.$$

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.

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

	epimorfismo	núcleo	conclusión
1)	$\mathbb{R}^\times \xrightarrow{x\mapsto\lvert x\rvert} \mathbb{R}_{>0}$	$\{\pm 1\}$	$\mathbb{R}^\times/\{\pm1\} \cong \mathbb{R}_{>0}$
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)	$\mathbb{R} \xrightarrow{x\mapsto e^{2\pi i x}} \mathbb{S}^1$	$\mathbb{Z}$	$\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$
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)	$S_n \xrightarrow{\mathrm{sgn}} \{\pm1\}$	A_n	$S_n/A_n \cong \{\pm1\}$
6)	$\mathrm{GL}_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^\times \xrightarrow{\mathrm{sgn}} \{\pm1\}$	$\mathrm{GL}_n(\mathbb{R})^+$	$\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{R})^+ \cong \{\pm1\}$
7)	$\mathbb{C}^\times \xrightarrow{z\mapsto\lvert z\rvert} \mathbb{R}_{>0}$	$\mathbb{S}^1$	$\mathbb{C}^\times/\mathbb{S}^1 \cong \mathbb{R}_{>0}$
8)	$\mathbb{C}^\times \xrightarrow{z\mapsto z/\lvert z\rvert} \mathbb{S}^1$	$\mathbb{R}_{>0}$	$\mathbb{C}^\times/\mathbb{R}_{>0} \cong \mathbb{S}^1$

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 $0 \leq \phi < 2\pi$. ▲

7.7.4. 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

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

▲

7.8 Ejercicios

Ejercicio 7.1. *Sea G un grupo y N su subgrupo normal. Sea $K \subset G/N$ un subgrupo del grupo cociente. Demuestre que $K = H/N$ donde H es un subgrupo de G que contiene a N.*
Sugerencia: considere el homomorfismo canónico $p\colon G \twoheadrightarrow G/N$ y $p^{-1}(K) \subset G$.

Ejercicio 7.2. *Demuestre que si $H \subset G$ es un subgrupo de índice $|G : H| = 2$, entonces H es normal.*

Ejercicio 7.3. *Demuestre que todo cociente de un grupo cíclico es cíclico.*

Ejercicio 7.4 (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.*

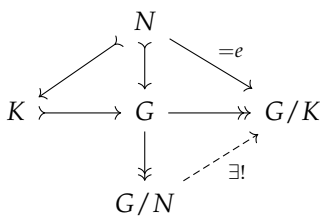
3) *Demuestre que la aplicación*
$$H \to HK/K, \quad h \mapsto hK$$
es un homomorfismo sobreyectivo de grupos y su núcleo es $H \cap K$.

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

Ejercicio 7.5. *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 7.6 (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 $K/N \subset G/N$.
Indicación: se puede usar la propiedad universal de G/N:



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

Ejercicio 7.7. *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 $y \in A$ (no necesariamente único) tal que $ny = x$. Si todos los elementos de A son divisibles, se dice que A es un **grupo divisible**.

Ejercicio 7.8.

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 7.9. *Sea p un número primo. El **p-grupo de Prüfer** es el grupo de las raíces de la unidad de orden p^n para $n \in \mathbb{N}$:*

$$\mu_{p^\infty}(\mathbb{C}) := \bigcup_{n \geq 0} \mu_{p^n}(\mathbb{C}) = \{z \in \mathbb{C}^\times \mid z^{p^n} = 1 \text{ para algún } n = 0, 1, 2, \ldots\}$$

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 7.10. *Sea A un grupo abeliano. Demuestre que $x \in A$ es divisible si y solamente es divisible por cualquier* número primo *$p = 2, 3, 5, 7, 11, \ldots$*

Ejercicio 7.11. *Usando el ejercicio anterior, demuestre que el grupo de Prüfer $\mu_{p^\infty}(\mathbb{C}) \cong \mathbb{Z}[1/p]/\mathbb{Z}$ es divisible.*

Ejercicio 7.12.

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

Capítulo 8
Conmutadores y abelianización

En este breve capítulo vamos a estudiar la relación entre los grupos abelianos y no abelianos. A cada grupo G se puede asociar de modo canónico un grupo abeliano G^{ab}, llamado la **abelianización** de G, que es el máximo cociente abeliano de G.

8.1 El subgrupo conmutador $[G, G]$

8.1.1. Definición. Sea G un grupo. Para dos elementos $g, h \in G$ el **conmutador** es el elemento

$$[g, h] := ghg^{-1}h^{-1}.$$

Note que g y h conmutan ($gh = hg$) si y solamente si $[g, h] = 1$.

Los conmutadores no siempre forman un subgrupo de G. A saber, para un conmutador tenemos obviamente

$$[g, h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h, g],$$

pero el producto de dos conmutadores no tiene por qué ser un conmutador. Sin embargo, se puede considerar el subgrupo *generado* por los conmutadores.

8.1.2. Definición. Para un grupo G el **subgrupo conmutador** $[G, G]$ (también conocido como el **subgrupo derivado**) es el subgrupo generado por todos los conmutadores:

$$[G, G] := \langle [g, h] \mid g, h \in G \rangle.$$

Obviamente, un grupo G es abeliano si y solamente si todos los conmutadores son iguales a 1, si y solamente si $[G, G] = 1$. Así que todo esto es de interés para grupos no abelianos.

8.1.3. Proposición. *$[G, G]$ es un subgrupo normal en G.*

Demostración. $h \in [G, G]$ y $g \in G$ tenemos

$$ghg^{-1} = ghg^{-1}h^{-1}h = [g, h]\, h \in [G, G].$$

■

La demostración de arriba es bastante lista: por la definición, los elementos de $[G, G]$ son productos de conmutadores, pero no son necesariamente conmutadores. Sin embargo, en el argumento de arriba no necesitamos considerar un elemento genérico de $[G, G]$, que sería $[g_1, h_1] \cdots [g_n, h_n]$.

8.1.4. Observación. *Homomorfismos preservan conmutadores: si $f\colon G \to H$ es un homomorfismo de grupos, entonces*

$$f([g_1, g_2]) = [f(g_1), f(g_2)].$$

8.1.5. Corolario. *Para todo homomorfismo $f\colon G \to H$ tenemos $f([G, G]) \subseteq [H, H]$.*

$$\begin{array}{ccc} [G,G] & \rightarrowtail & G \\ \vdots & & \downarrow f \\ [H,H] & \rightarrowtail & H \end{array}$$

8.1.6. Comentario. El centro $Z(G)$ tiene una propiedad parecida a la propiedad del subgrupo conmutador:

1) $Z(G) = G$ si y solamente si G es abeliano,

2) $[G, G] = 1$ si y solamente si G es abeliano.

Sin embargo, el centro no se comporta bien respecto a homomorfismos: una aplicación $f\colon G \to H$ no tiene por qué restringirse a $Z(G) \to Z(H)$. Por ejemplo, para el grupo simétrico S_n se tiene $Z(S_n) = \{\mathrm{id}\}$ para $n \geq 3$, pero S_n puede contener subgrupos abelianos $G \subset S_n$ donde $Z(G) = G \neq \{\mathrm{id}\}$. Un ejemplo específico nos da $A_3 \subset S_3$.

8.1.7. Observación. *Sea $H \subseteq G$ un subgrupo normal tal que G/H es abeliano. Entonces, $[G, G] \subseteq H$.*

Demostración. Para todo conmutador $[g_1, g_2] \in G$ se tiene necesariamente $[g_1, g_2] \equiv 1$ (mód H), ya que G/H es abeliano. En otras palabras, $[g_1, g_2] \in H$. ■

Ya se puede notar que $[G, G]$ es el *mínimo* subgrupo normal en G tal que $G/[G, G]$ es un grupo abeliano. Volveremos a esto un poco más adelante, pero primero calculemos $[G, G]$ para algunos grupos específicos.

8.2 Algunos cálculos de $[G, G]$

8.2.1. Ejemplo. Para el grupo diédrico

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

Tenemos

$$[D_n, D_n] = \langle r^2 \rangle.$$

Dejo este cálculo al lector (véase el ejercicio 8.9 abajo). Note que si n es impar, este grupo consiste en todas las rotaciones; si n es impar, este grupo contiene solo la mitad de las rotaciones. ▲

Conmutadores en S_n y A_n

8.2.2. Teorema. *Para el grupo simétrico tenemos*

$$[S_n, S_n] = A_n \quad \textit{para } n \geq 3.$$

Demostración. Para cualesquiera $\sigma, \tau \in S_n$ se cumple

$$\operatorname{sgn}[\sigma, \tau] = \operatorname{sgn}(\sigma\tau\sigma^{-1}\tau^{-1}) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau) = +1,$$

entonces $[S_n, S_n] \subseteq A_n$. Ya que S_n no es un grupo abeliano para $n \geq 3$, sabemos que $[S_n, S_n] \neq \{\mathrm{id}\}$. Sin embargo, A_n es el único subgrupo normal propio no trivial de S_n, así que $[S_n, S_n] = A_n$. ■

8.2.3. Comentario. Otro modo de ver que $[S_n, S_n] = A_n$, sin recurrir al resultado sobre los subgrupos normales de S_n, es de expresar cada 3-ciclo como un conmutador

$$[(i\ j), (i\ k)] = (i\ j)\ (i\ k)\ (i\ j)\ (i\ k) = (i\ j\ k)$$

para diferentes i, j, k. Los 3-ciclos generan todo A_n, así que $[S_n, S_n] = A_n$.

8.2.4. Teorema. *Para $n \geq 5$ tenemos*

$$[A_n, A_n] = A_n,$$

mientras que para $n = 4$

$$[A_4, A_4] = V.$$

Demostración. Hay varios modos de verlo. En general, hemos visto que A_n es simple para $n \geq 5$; es decir, no tiene subgrupos normales propios. El conmutador $[A_n, A_n]$ es un subgrupo normal y no es trivial, puesto que el grupo no es abeliano, así que $[A_n, A_n] = A_n$.

En el caso de A_4 notamos que no es abeliano, y por lo tanto su conmutador no es trivial. Un buen candidato sería el único subgrupo normal propio

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

El cociente $A_4/V \cong \mathbb{Z}/3\mathbb{Z}$ es abeliano, lo que implica que $[A_4, A_4] \subseteq V$. Ya que A_4 no es abeliano, tenemos $[A_4, A_4] \neq \{\mathrm{id}\}$. Los únicos subgrupos normales en A_4 son $\{\mathrm{id}\}$, V y todo A_4. ■

8.2.5. Comentario. Otro modo de ver que $[A_n, A_n] = A_n$ para $n \geq 5$, sin usar la simplicidad de A_n, es de calcular que

$$[(i\ j\ a), (i\ k\ b)] = (i\ j\ a)\ (i\ k\ b)\ (i\ a\ j)\ (i\ b\ k) = (i\ j\ k)$$

para diferentes i, j, k, a, b, y luego recordar que los 3-ciclos generan A_n.

En en caso de $[A_4, A_4] = V$, podemos calcular que

$$[(i\ j\ k), (i\ j\ \ell)] = (i\ j\ k)\ (i\ j\ \ell)\ (i\ k\ j)\ (i\ \ell\ j) = (i\ j)\ (k\ \ell)$$

para diferentes i, j, k, ℓ.

8.2.6. Comentario. Para un grupo G, su **serie derivada** es la sucesión de subgrupos

$$G \supseteq G' \supseteq G'' \supseteq G''' \supseteq \cdots$$

donde

$$G' := [G, G],\ G'' := [G', G'],\ G''' := [G'', G''],\ \ldots$$

Si esta serie termina en algún punto por el grupo trivial, entonces se dice que G es un grupo **resoluble**. El grupo simétrico S_n es resoluble para $n \leq 4$. De hecho, tenemos

$$[S_3, S_3] = A_3,\ [A_3, A_3] = 1$$

y

$$[S_4, S_4] = A_4,\ [A_4, A_4] = V,\ [V, V] = 1.$$

El resultado de 8.2.4 dice que S_n no es resoluble para $n \geq 5$: en este caso

$$[S_n, S_n] = A_n,\ [A_n, A_n] = A_n.$$

De la irresolubilidad de S_n para $n \geq 5$ Galois demostró la imposibilidad de expresar las soluciones de la ecuación general de grado $n \geq 5$

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

aplicando únicamente las operaciones básicas y extracción de raíces a los coeficientes a_i. Este célebre resultado es conocido como el **teorema de Abel–Ruffini** ya que el matemático italiano Paolo Ruffini (1765–1822) obtuvo una demostración incompleta en 1799 y Abel proporcionó una prueba en 1823. Galois encontró su demostración de manera independiente, pero esta fue publicada póstumamente en 1846. La teoría desarrollada por Galois motivó muchos conceptos de la teoría de grupos, y por sí mismo, es una piedra angular de la teoría de números.

En este curso no vamos a hablar más de grupos resolubles, ni, lamentablemente, de la teoría de Galois.

Conmutadores en $\mathrm{GL}_n(k)$ y $\mathrm{SL}_n(k)$

Ahora nos gustaría calcular el subgrupo conmutador para el grupo lineal general $\mathrm{GL}_n(k)$ y el grupo lineal especial $\mathrm{SL}_n(k)$ donde k es un cuerpo. Primero, necesitamos algunos resultados auxiliares sobre las matrices elementales. Para $1 \leq i \neq j \leq n$ y $\lambda \in k$ una **matriz elemental** viene dada por

$$E_{ij}(\lambda) := I + \lambda\, e_{ij}.$$

En otras palabras, es la matriz que tiene 1 en la diagonal, λ en la posición (i, j) afuera de la diagonal, y ceros en las demás entradas.

Dejo el siguiente cálculo al lector.

8.2.7. Lema. *Las matrices elementales satisfacen las siguientes propiedades.*

1) *La multiplicación de una matriz $A \in M_n(k)$ por la matriz elemental $E_{ij}(\lambda)$ por la izquierda (donde $i \neq j$) tiene el siguiente efecto: a la fila i se le suma la fila j multiplicada por λ:*

$$E_{ij}(\lambda) \cdot \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1,n-1} & x_{1n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{i1} & x_{i2} & \cdots & x_{i,n-1} & x_{in} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{j1} & x_{j2} & \cdots & x_{j,n-1} & x_{jn} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{n,n-1} & x_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1,n-1} & x_{1n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{i1} + \lambda x_{j1} & x_{i2} + \lambda x_{j2} & \cdots & x_{i,n-1} + \lambda x_{j,n-1} & x_{in} + \lambda x_{jn} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{j1} & x_{j2} & \cdots & x_{j,n-1} & x_{jn} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{n,n-1} & x_{nn} \end{pmatrix}.$$

2) *Toda matriz elemental es invertible, y su inversa viene dada por $E_{ij}(\lambda)^{-1} = E_{ij}(-\lambda)$.*

3) *Si i, j, k son índices diferentes, entonces*

$$[E_{ij}(\lambda), E_{jk}(\mu)] = E_{ik}(\lambda\mu).$$

8.2.8. Lema. *El grupo $\mathrm{SL}_n(k)$ puede ser generado por las matrices elementales $E_{ij}(\lambda)$ donde $1 \leq i \neq j \leq n$, $\lambda \in k$.*

Demostración. Esto es esencialmente el método de eliminación gaussiana. Sea $A = (x_{ij}) \in \mathrm{SL}_n(k)$. Primero, multiplicando A por matrices elementales, podemos lograr que $x_{11} = 1$. En efecto, si $x_{i1} \neq 0$ para algún $i = 2, 3, \ldots, n$, entonces podemos sumar a la primera fila la i-ésima fila multiplicada por el coeficiente λ apropiado. Si $x_{i1} = 0$ para todo $i = 2, 3, \ldots, n$, entonces tenemos $x_{11} \neq 0$ y podemos sumar a la i-ésima fila para algún $i = 2, 3, \ldots, n$ la primera fila, lo que nos deja en la situación considerada.

Ahora cuando $x_{11} = 1$, podemos restar de las otras filas la primera fila multiplicada por los coeficientes λ apropiados y obtener $x_{i1} = 0$ para todo $i = 2, 3, \ldots, n$. Repitiendo este proceso para las filas $i = 2, 3, \ldots, n$, podemos reducir A a una matriz de la forma

$$A' = \begin{pmatrix} 1 & x'_{12} & x'_{13} & \cdots & x'_{1,n-1} & x'_{1n} \\ 0 & 1 & x'_{23} & \cdots & x'_{2,n-1} & x'_{2n} \\ 0 & 0 & 1 & \cdots & x'_{2,n-1} & x'_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & x'_{n-1,n} \\ 0 & 0 & 0 & \cdots & 0 & x'_{nn} \end{pmatrix}.$$

Ya que $\det E_{ij}(\lambda) = 1$, nuestras operaciones no afectan el determinante de la matriz, así que $\det A' = \det A = 1$ y necesariamente $x'_{nn} = 1$. Entonces A' es una matriz triangular superior con 1 en la diagonal.

Ahora, podemos restar de las primeras $n-1$ filas la última fila multiplicada por los coeficientes apropiados y obtener $x'_{1n} = x'_{2n} = \cdots = x'_{n-1,n} = 0$. De la misma manera, restando la fila $n-1$, podemos obtener $x'_{1,n-1} = x'_{2,n-1} = \cdots = x'_{n-2,n-1} = 0$, etcétera. Esto nos dejará con la matriz identidad.

Podemos concluir que $E \cdot A = I$, donde E es un producto de matrices elementales que corresponden a las operaciones con las filas. Luego, $A = E^{-1}$. ■

8.2.9. Teorema. *Si k es un cuerpo, entonces tenemos para $n \geq 2$*

$$[\mathrm{GL}_n(k), \mathrm{GL}_n(k)] = \mathrm{SL}_n(k), \quad [\mathrm{SL}_n(k), \mathrm{SL}_n(k)] = \mathrm{SL}_n(k)$$

con las siguientes excepciones:

1) *si $n = 2$ y $k = \mathbb{F}_2$, entonces*

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

y $[S_3, S_3] = A_3$;

2) *si $n = 2$, $k = \mathbb{F}_3$, entonces*

$$[\mathrm{SL}_2(\mathbb{F}_3), \mathrm{SL}_2(\mathbb{F}_3)] \cong Q_8.$$

Demostración. Primero notamos que para cualesquiera $A, B \in \mathrm{GL}_n(k)$ se tiene

$$\det[A, B] = \det(A\,B\,A^{-1}\,B^{-1}) = \det(A)\,\det(B)\,\det(A)^{-1}\,\det(B)^{-1} = 1,$$

así que $[A, B] \in \mathrm{SL}_n(k)$. Esto significa que $[\mathrm{GL}_n(k), \mathrm{GL}_n(k)] \subseteq \mathrm{SL}_n(k)$. Ya que el grupo $\mathrm{SL}_n(k)$ está generado por las matrices elementales, para concluir que $[\mathrm{GL}_n(k), \mathrm{GL}_n(k)] = [\mathrm{SL}_n(k), \mathrm{SL}_n(k)] = \mathrm{SL}_n(k)$, sería suficiente expresar toda matriz elemental como un conmutador. Si $n \geq 3$, entonces para todo $1 \leq i \neq k \leq n$ podemos escoger otro índice diferente j y luego

$$[E_{ij}(\lambda), E_{jk}(1)] = E_{ik}(\lambda).$$

Esto establece el teorema para cualquier $n \geq 3$ y cualquier k.

Ahora si $n = 2$ y si $|k| > 3$, entonces existe un elemento $\mu \in k^\times$ tal que $\mu^2 \neq 1$[*]. Luego, un cálculo directo nos dice que toda matriz elemental $E_{12}(\lambda)$ es un conmutador de matrices en $\mathrm{SL}_n(k)$:

$$E_{12}(\lambda) = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = [A, B], \quad \text{donde } A = \begin{pmatrix} \mu & 0 \\ 0 & 1/\mu \end{pmatrix},\ B = \begin{pmatrix} 1 & \lambda/(\mu^2 - 1) \\ 0 & 1 \end{pmatrix},$$

y de la misma manera,

$$E_{21}(\lambda) = E_{12}(\lambda)^t = [A, B]^t = [B^{-t}, A^{-t}].$$

[*]En efecto, en un cuerpo la ecuación $x^2 = 1$ tiene a lo sumo dos soluciones y son ± 1. En el cuerpo $\mathbb{F}_2$ es una sola solución $1 = -1$; en el cuerpo $\mathbb{F}_3$ tenemos $\mathbb{F}_3^\times = \{1, 2\} = \{1, -1\}$, y cuando $|k| > 3$, habrá algún $x \neq 0$ tal que $x \neq \pm 1$.

Si $|k| = 3$; es decir, si $k = \mathbb{F}_3$, toda matriz elemental todavía puede ser expresada como un conmutador *de matrices en* $\mathrm{GL}_n(k)$:

$$E_{12}(\lambda) = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = [A, B], \quad \text{donde } A = \begin{pmatrix} 1 & \lambda/2 \\ 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

(en $\mathbb{F}_3$ tenemos $2 \neq 0$, así que el término $\lambda/2$ tiene sentido). Notemos que $B \notin \mathrm{SL}_2(\mathbb{F}_3)$, y de hecho para $\mathrm{SL}_2(\mathbb{F}_3)$ las matrices elementales salvo $E_{12}(0) = E_{21}(0) = I$ no son conmutadores. Nos quedan entonces dos casos excepcionales.

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

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

y $[S_3, S_3] = A_3$. En términos de matrices,

$$[\mathrm{GL}_2(\mathbb{F}_2), \mathrm{GL}_2(\mathbb{F}_2)] = [\mathrm{SL}_2(\mathbb{F}_2), \mathrm{SL}_2(\mathbb{F}_2)] = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}.$$

2) Si $n = 2$ y $k = \mathbb{F}_3$, entonces para calcular $[\mathrm{SL}_2(\mathbb{F}_3), \mathrm{SL}_2(\mathbb{F}_3)]$, notamos que

$$|\mathrm{SL}_2(\mathbb{F}_3)| = \frac{1}{2} \cdot |\mathrm{GL}_2(\mathbb{F}_3)| = \frac{1}{2} \cdot (3^2 - 1)\,(3^2 - 3) = 24.$$

En $\mathrm{SL}_2(\mathbb{F}_3)$ hay un subgrupo normal H generado por las matrices

$$I = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},\ J = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix},\ K = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$$

que es isomorfo al grupo de cuaterniones Q_8.

$$IJ = K, \quad JK = I, \quad KI = J, \quad I^2 = J^2 = K^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Luego,

$$|\mathrm{SL}_2(\mathbb{F}_3)/H| = |\mathrm{SL}_2(\mathbb{F}_3)|/|H| = 24/8 = 3, \text{ así que } \mathrm{SL}_2(\mathbb{F}_3)/H \cong \mathbb{Z}/3\mathbb{Z},$$

el cual es un grupo abeliano; esto demuestra que

$$[\mathrm{SL}_2(\mathbb{F}_3), \mathrm{SL}_2(\mathbb{F}_3)] \subseteq H.$$

Además, los generadores de H pueden ser expresados como conmutadores:

$$I = \left[\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix} \right], \quad J = \left[\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right], \quad K = \left[\begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \right],$$

y por lo tanto

$$[\mathrm{SL}_2(\mathbb{F}_3), \mathrm{SL}_2(\mathbb{F}_3)] \cong Q_8.$$

■

8.2.10. Comentario. Hemos encontrado un isomorfismo excepcional $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) \cong S_3$. Podemos preguntarnos si otros grupos $\mathrm{GL}_m(\mathbb{F}_q)$ pueden ser isomorfos a S_n para algunos m, q, n. La respuesta es negativa.

1) Primero, para $q \neq 2$ el centro $Z(\mathrm{GL}_m(\mathbb{F}_q))$ consiste en las matrices escalares y no es trivial, mientras que $Z(S_n) = \{\mathrm{id}\}$. Esto implica que $\mathrm{GL}_m(\mathbb{F}_q) \ncong S_n$ para $q \neq 2$.

2) Si $q = 2$, podemos calcular los subgrupos conmutadores: si $m \neq 2$, entonces

$$[\mathrm{GL}_m(\mathbb{F}_2), \mathrm{GL}_m(\mathbb{F}_2)] = \mathrm{SL}_m(\mathbb{F}_2) = \mathrm{GL}_m(\mathbb{F}_2),$$

mientras que

$$[S_n, S_n] = A_n \neq S_n.$$

De hecho, en la parte 2) también se puede acudir a un argumento elemental aritmético y probar que $|\mathrm{GL}_m(\mathbb{F}_2)|$ no es un factorial para $m \geq 3$ (por ejemplo, bastaría considerar la valuación 2-ádica y 3-ádica de $|\mathrm{GL}_m(\mathbb{F}_2)|$ y compararlas con las correspondientes valuaciones de $n!$).

8.2.11. Ejemplo. He aquí un ejemplo curioso[*] de cuándo un elemento del subgrupo conmutador no se expresa como un conmutador. Tenemos $-I \in [\mathrm{SL}_2(\mathbb{R}), \mathrm{SL}_2(\mathbb{R})] = \mathrm{SL}_2(\mathbb{R})$. Supongamos que

$$-I = [A, B] = ABA^{-1}B^{-1}.$$

Para algunos $A, B \in \mathrm{SL}_2(\mathbb{R})$. Entonces,

$$-B = ABA^{-1},$$

y luego

$$-\operatorname{tr}(B) = \operatorname{tr}(-B) = \operatorname{tr}(ABA^{-1}) = \operatorname{tr}(B),$$

así que $\operatorname{tr} B = 0$. Puesto que $\det B = 1$ y $\operatorname{tr} B = 0$, tenemos

$$C\,B\,C^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} =: B'$$

para alguna matriz C. Podemos reemplazar A por la matriz

$$A' := C\,A\,C^{-1}.$$

Ya que $AB = -BA$, tenemos también $A'B' = -B'A'$; es decir, $[A', B'] = -I$. Escribamos

$$A' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Luego,

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

[*] https://mathoverflow.net/questions/44269

y se calcula que

$$[A', B'] = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix}.$$

Pero esta matriz no puede ser igual a $-I$. ▲

8.2.12. Comentario. Si en lugar de un cuerpo k se considera un anillo conmutativo R, el cálculo de $[\mathrm{GL}_n(R), \mathrm{GL}_n(R)]$ y $[\mathrm{SL}_n(R), \mathrm{SL}_n(R)]$ pertenece al terreno de la **teoría** K **algebraica**, una rama de las matemáticas que nació en los años 50 del siglo pasado.

8.3 Abelianización

Ya que el subgrupo conmutador $[G, G]$ es normal, podemos considerar el cociente correspondiente $G/[G, G]$.

8.3.1. Definición. El grupo $G/[G, G]$ se llama la **abelianización** de G y se denota por G^{ab}.

Note que si G ya es abeliano, entonces $[G, G] = 1$ y $G^{ab} \cong G$.

8.3.2. Observación. *Para todo grupo G, su abelianización $G^{ab} := G/[G, G]$ es un grupo abeliano.*

Demostración. Los elementos G^{ab} son de la forma

$$\overline{g} := g \mod [G, G] \quad \text{para algún } g \in G.$$

Luego, $\overline{g}, \overline{h}$ conmutan si y solamente si $[\overline{g}, \overline{h}] = \overline{1}$, pero tenemos siempre $[\overline{g}, \overline{h}] = \overline{[g, h]}$ donde $[g, h] \in [G, G]$, así que $[\overline{g}, \overline{h}] = \overline{1}$ para cualesquiera $\overline{g}, \overline{h} \in G^{ab}$. ■

8.3.3. Proposición (Propiedad universal de la abelianización). *Sea $f\colon G \to A$ un homomorfismo entre un grupo G y un grupo abeliano A. Entonces, f se factoriza de modo único por el epimorfismo canónico $G \twoheadrightarrow G^{ab} := G/[G, G]$:*

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & A \\ {\scriptstyle p}\downarrow & \overset{\exists!}{\nearrow}_{\overline{f}} & \\ G^{ab} & & \end{array}$$

$$f = \overline{f} \circ p.$$

Demostración. Como notamos en 8.1.5, tenemos $f([G, G]) \subseteq [A, A]$. Ya que A es abeliano, el grupo $[A, A]$ es trivial y luego $[G, G] \subset \ker f$. La factorización canónica por $G^{ab} := G/[G, G]$ existe gracias a la propiedad universal del cociente. ■

8.3.4. Corolario (Funtorialidad de la abelianización). *Todo homomorfismo de grupos $f\colon G \to H$ desciende de modo único a un homomorfismo de grupos $f^{ab}\colon G^{ab} \to H^{ab}$.*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow & & \downarrow \\ G^{ab} & \xrightarrow[f^{ab}]{\exists!} & H^{ab} \end{array}$$

Además,

$$\mathrm{id}_G^{ab} = \mathrm{id}_{G^{ab}},$$

y para homomorfismos $f\colon G \to H$ *y* $g\colon H \to K$ *tenemos*

$$(g \circ f)^{ab} = g^{ab} \circ f^{ab}.$$

Demostración. La flecha punteada existe y es única gracias a la propiedad universal de G^{ab} aplicada a la composición $G \xrightarrow{f} H \twoheadrightarrow H^{ab}$.

Para el homomorfismo identidad $\mathrm{id}\colon G \to G$ en el diagrama conmutativo

$$\begin{array}{ccc} G & \xrightarrow{\mathrm{id}} & G \\ \downarrow & & \downarrow \\ G^{ab} & \xrightarrow{\exists!} & G^{ab} \end{array}$$

la flecha punteada tiene que ser el homomorfismo identidad $\mathrm{id}\colon G^{ab} \to G^{ab}$ por la unicidad. De la misma manera, en el diagrama conmutativo

$$\begin{array}{ccccc} G & \xrightarrow{f} & H & \xrightarrow{g} & K \\ \downarrow & & \downarrow & & \downarrow \\ G^{ab} & \xrightarrow{\exists! f^{ab}} & H^{ab} & \xrightarrow{\exists! g^{ab}} & K^{ab} \\ & \searrow^{\exists!(g\circ f)^{ab}} & & & \end{array}$$

gracias a la unicidad, necesariamente $(g \circ f)^{ab} = g^{ab} \circ f^{ab}$. ■

8.3.5. Ejemplo.

1) Para el grupo diédrico tenemos

$$(D_n)^{ab} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{si } n \text{ es impar,} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong V, & \text{si } n \text{ es par.} \end{cases}$$

—haga el ejercicio 8.9.

2) Puesto que $[S_n, S_n] = A_n$ para $n \geq 3$ (véase 8.2.2), la abelianización del grupo simétrico S_n viene dada por

$$(S_n)^{ab} = \begin{cases} \{\mathrm{id}\}, & \text{si } n = 0, 1, \\ S_n/A_n \cong \{\pm 1\}, & \text{si } n \geq 2. \end{cases}$$

3) Puesto que $[A_n, A_n] = A_n$ para $n \geq 5$ y $[A_4, A_4] = V$, la abelianización del grupo alternante A_n es

$$(A_n)^{ab} \cong \begin{cases} \{\mathrm{id}\}, & \text{si } n = 0, 1, 2, \\ A_3 \cong \mathbb{Z}/3\mathbb{Z}, & \text{si } n = 3, \\ \cong \mathbb{Z}/3\mathbb{Z}, & \text{si } n = 4, \\ \{\mathrm{id}\}, & \text{si } n \geq 5. \end{cases}$$

4) Para el grupo lineal general $\mathrm{GL}_n(k)$ el resultado de 8.2.9 nos da

$$\mathrm{GL}_n(k)^{ab} \cong k^{\times},$$

salvo el caso especial de

$$\mathrm{GL}_2(\mathbb{F}_2)^{ab} \cong \mathbb{Z}/2\mathbb{Z}.$$

5) De la misma manera, para $\mathrm{SL}_n(k)$ tenemos

$$\mathrm{SL}_n(k)^{ab} = \{I\},$$

salvo los casos excepcionales

$$\mathrm{SL}_2(\mathbb{F}_2)^{ab} = \mathrm{GL}_2(\mathbb{F}_2)^{ab} \cong \mathbb{Z}/2\mathbb{Z}, \quad \mathrm{SL}_2(\mathbb{F}_3)^{ab} \cong \mathbb{Z}/3\mathbb{Z}.$$

▲

8.4 Ejercicios

Ejercicio 8.1. *Para un grupo G y su subgrupo H denotemos por $[G,H]$ el subgrupo generado por los conmutadores $[g,h]$ donde $g \in G$ y $h \in H$. Demuestre que $[G,H] \subseteq H$ si y solamente si H es un subgrupo normal.*

Ejercicio 8.2. *En A_5 tenemos $[(1\,2\,4),(1\,3\,5)] = (1\,2\,3)$. De modo similar, exprese las permutaciones $(1\,2)\,(3\,4)$ y $(1\,2\,3\,4\,5)$ como conmutadores.*

Ejercicio 8.3. *Para las matrices elementales $E_{ij}(\lambda) := I + \lambda\, e_{ij}$ demuestre que*

$$[E_{ij}(\lambda), E_{jk}(\mu)] = E_{ik}(\lambda\mu)$$

donde i,j,k son índices diferentes.

Ejercicio 8.4. *Encuentre todos los homomorfismos $S_n \to \mathbb{Z}/m\mathbb{Z}$.*

Ejercicio 8.5. *Sea $f\colon G \twoheadrightarrow H$ un epimorfismo de grupos. Demuestre que $f^{ab}\colon G^{ab} \to H^{ab}$ es también un epimorfismo. Demuestre que si $f\colon G \rightarrowtail H$ es un monomorfismo, entonces $f^{ab}\colon G^{ab} \to H^{ab}$ no es necesariamente un monomorfismo (encuentre un contraejemplo especifico).*

Ejercicio 8.6. *Consideremos la aplicación*

$$\begin{aligned} \mathrm{Hom}(G,H) &\to \mathrm{Hom}(G^{ab},H^{ab}),\\ f &\mapsto f^{ab}. \end{aligned}$$

Demuestre que no es ni inyectiva, ni sobreyectiva en general (encuentre contraejemplos).
Indicación: para ver que no es sobreyectiva, considere $G = \{\pm 1\}$ y $H = Q_8$.

Ejercicio 8.7. *Sea k un cuerpo. Consideremos el grupo*

$$G := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a,b,c \in k \right\}.$$

1) *Calcule el subgrupo conmutador $[G,G]$.*
2) *Demuestre que la abelianización G^{ab} es isomorfa al grupo aditivo*

$$k^2 = \{(a,c) \mid a,c \in k\}.$$

Ejercicio 8.8. *Calcule la abelianización del grupo de cuaterniones Q_8.*

Ejercicio 8.9. *Para el grupo diédrico*

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

1) *calcule que $[D_n, D_n] = \langle r^2 \rangle$;*
2) *calcule $(D_n)^{ab}$.*

Ejercicio 8.10. *El grupo diédrico D_n permuta los vértices del n-ágono regular y esto nos da un monomorfismo natural $f\colon D_n \to S_n$. Calcule el homomorfismo correspondiente $f^{ab}\colon (D_n)^{ab} \to (S_n)^{ab}$.*

Capítulo 9
Acciones de grupos

Por sus obras los conoceréis.

Normalmente los grupos surgen junto con su acción sobre algún conjunto. En general, el concepto de acción es fundamental en las matemáticas.

9.1 Definiciones y primeros ejemplos

9.1.1. Definición. Sea G un grupo y X un conjunto. Se dice que G **actúa sobre** X **(por la izquierda)** si está definida una aplicación

$$\begin{aligned} \alpha\colon G \times X &\to X, \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

que satisface las siguientes propiedades.

A1) La identidad del grupo actúa como la identidad: para cualesquiera $x \in X$ se cumple

$$1 \cdot x = x.$$

A2) La acción es compatible con la multiplicación en G: para cualesquiera $h, g \in G$ y $x \in X$ se cumple

$$(hg) \cdot x = h \cdot (g \cdot x).$$

También se dice que X es un G**-conjunto (izquierdo)**.

9.1.2. Comentario. También hay una noción de acción por la derecha: es una aplicación

$$\begin{aligned} X \times G &\to X, \\ (x, g) &\mapsto x \cdot g \end{aligned}$$

que satisface

A1) $x \cdot 1 = x$ para todo $x \in X$,

A2) $x \cdot (gh) = (x \cdot g) \cdot h$ para cualesquiera $x \in X$, $g, h \in G$.

A toda acción por la derecha se puede asociar *de manera canónica* una acción por la izquierda definida por

$$g \cdot x := x \cdot g^{-1}.$$

Necesitamos tomar el inverso de g para que se cumpla el axioma A2): si la acción por la derecha cumple $x \cdot (gh) = (x \cdot g) \cdot h$, entonces

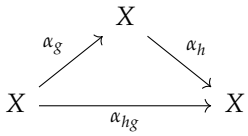
$$(gh) \cdot x := x \cdot (gh)^{-1} = x \cdot (h^{-1} g^{-1}) = (x \cdot h^{-1}) \cdot g^{-1} =: g \cdot (h \cdot x).$$

Vamos a trabajar exclusivamente con las acciones por la izquierda.

Dado una acción $\alpha \colon G \times X \to X$, fijando $g \in G$ se obtiene la aplicación de la acción por g

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

La condición A1) de arriba significa que $\alpha_1 = \mathrm{id}_X$ y la condición A2) nos dice que $\alpha_{hg} = \alpha_h \circ \alpha_g$:



Notamos que de A1) y A2) se sigue que $\alpha_g \colon X \to X$ es una biyección y su aplicación inversa es $\alpha_{g^{-1}} \colon X \to X$:

$$\alpha_{g^{-1}} \circ \alpha_g = \alpha_{g^{-1}g} = \mathrm{id}_X, \quad \alpha_g \circ \alpha_{g^{-1}} = \alpha_{gg^{-1}} = \mathrm{id}_X.$$

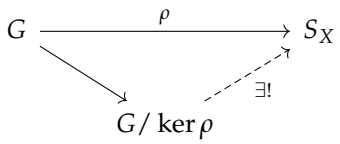
La identidad $\alpha_{hg} = \alpha_h \circ \alpha_g$ significa que tenemos un homomorfismo de grupos

$$\begin{aligned} \rho \colon G &\to S_X, \\ g &\mapsto \alpha_g, \end{aligned} \tag{9.1}$$

donde S_X es el grupo simétrico que consiste en las biyecciones $f \colon X \to X$ respecto a la composición $\circ$. Viceversa, cualquier homomorfismo de grupos (9.1) define una acción de G sobre X mediante $g \cdot x := (\rho(g))(x)$.

9.1.3. Definición. Se dice que la acción de G sobre X es **fiel** si diferentes elementos de G actúan de manera diferente; es decir, si el homomorfismo correspondiente $G \to S_X$ es mono. En general, $\ker(G \to S_X)$ se llama el **núcleo** de la acción.

9.1.4. Observación. *Toda acción $\rho\colon G \to S_X$ da lugar a una acción fiel $G/\ker\rho \to S_X$:*



Demostración. Esto es el teorema de isomorfía. ■

9.1.5. Ejemplo. El ejemplo primordial: el grupo simétrico S_X actúa sobre X de manera evidente ($f \cdot x = f(x)$). Esta acción es fiel. En particular, el grupo S_n actúa sobre el conjunto $\{1, 2, \ldots, n\}$.

De la misma manera,

- el grupo de isometrías del plano $\mathbb{R}^2$ actúa sobre $\mathbb{R}^2$,
- el grupo diédrico actúa sobre un n-ágono regular,
- etcétera.

▲

9.1.6. Ejemplo. El grupo $\mathrm{GL}(V)$ actúa sobre un espacio vectorial V. Si G es cualquier grupo, entonces un homomorfismo

$$\rho\colon G \to \mathrm{GL}(V)$$

da lugar a una acción de G sobre V **por aplicaciones lineales**. En este caso se dice que ρ es una **representación lineal** de G sobre V. El estudio de representaciones lineales ayuda descubrir muchas propiedades de G. Es una herramienta muy poderosa de la teoría de grupos.

De la misma manera, se dice que un homomorfismo

$$\rho\colon G \to S_X$$

(que corresponde a un G-conjunto X) es una **representación por permutaciones** de G sobre X. ▲

9.1.7. Ejemplo. He aquí una variante sobre el tema de la acción de $\mathrm{GL}(V)$ sobre V. Sea R un anillo conmutativo y $\mathrm{GL}_n(R)$ el grupo de las matrices invertibles de $n \times n$. Consideremos los elementos de

$$R^n := \underbrace{R \times \cdots \times R}_{n}$$

como vectores columna; es decir, matrices de $n \times 1$

$$v = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Para $A \in \mathrm{GL}_n(R)$ el producto de matrices $A \cdot v$ es también un vector columna. Esto define una acción de $\mathrm{GL}_n(R)$ sobre el espacio de vectores columna R^n por la izquierda.

Ahora si trabajamos con vectores fila

$$v = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix},$$

el producto $v \cdot A$ es también un vector fila. El grupo $\mathrm{GL}_n(R)$ actúa sobre el espacio de vectores fila R^n por la derecha. ▲

9.1.8. Ejemplo. Consideremos el **semiplano superior** que es el subconjunto de $\mathbb{C}$ dado por

$$\mathcal{H} := \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}.$$

El grupo

$$\mathrm{SL}_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{R},\ ad - bc = 1 \right\}$$

actúa sobre $\mathcal{H}$ mediante las **transformaciones de Möbius**:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az + b}{cz + d}.$$

Esta fórmula tiene sentido, ya que $z \in \mathcal{H}$ es un número complejo con la parte imaginaria estrictamente positiva, así que $cz + d \neq 0$ si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$. Además, verificamos que $\frac{az+b}{cz+d} \in \mathcal{H}$:

$$\operatorname{Im} \frac{az + b}{cz + d} = \operatorname{Im} \frac{(az + b)\,(c\overline{z} + d)}{|cz + d|^2} = \operatorname{Im} \frac{ac\,|z|^2 + ad\,z + bc\,\overline{z} + bd}{|cz + d|^2} > 0,$$

puesto que $ad > bc$.

Comprobemos que se cumplen los axiomas A1) y A2). La matriz identidad nos da

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot z := \frac{1 \cdot z + 0}{0 \cdot z + 1} = z.$$

Para el producto de matrices se tiene

$$\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \cdot z = \begin{pmatrix} a'a + b'c & a'b + b'd \\ c'a + d'c & c'b + d'd \end{pmatrix} \cdot z = \frac{(a'a + b'c)\,z + a'b + b'd}{(c'a + d'c)\,z + c'b + d'd}$$

y

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z \right) = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot \frac{az + b}{cz + d} = \frac{a' \dfrac{az + b}{cz + d} + b'}{c' \dfrac{az + b}{cz + d} + d'} = \frac{a'\,(az + b) + b'\,(cz + d)}{c'\,(az + b) + d'\,(cz + d)},$$

y las últimas dos expresiones coinciden.

La acción de $\mathrm{SL}_2(\mathbb{R})$ no es fiel: las matrices

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

actúan de la misma manera. Dejo al lector como un pequeño ejercicio calcular que el núcleo de la acción es precisamente

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \;\middle|\; \frac{az+b}{cz+d} = z \text{ para todo } z \in \mathcal{H} \right\} = Z(\mathrm{SL}_2(\mathbb{R})) = \{\pm I\}$$

y por ende hay una acción fiel del grupo cociente

$$\mathrm{PSL}_2(\mathbb{R}) := \mathrm{SL}_2(\mathbb{R})/Z(\mathrm{SL}_2(\mathbb{R})) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$$

sobre el semiplano superior.

La acción de $\mathrm{SL}_2(\mathbb{R})$ sobre $\mathcal{H}$ se restringe a una acción de

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z},\ ad-bc = 1 \right\}.$$

Hemos visto que el grupo $\mathrm{SL}_2(\mathbb{Z})$ puede ser generado por dos matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Entonces, todas las acciones de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathcal{H}$ pueden ser escritas como composiciones de las aplicaciones

$$z \mapsto -1/z, \quad z \mapsto z+1$$

y sus inversas.

Para obtener una acción fiel normalmente se considera la acción correspondiente del grupo

$$\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\} = \mathrm{SL}_2(\mathbb{Z})/Z(\mathrm{SL}_2(\mathbb{Z})).$$

▲

9.1.9. Definición. Para dos G-conjuntos X e Y se dice que una aplicación $f\colon X \to Y$ es **G-equivariante** si esta conmuta con las acciones de G:

$$f(g \cdot x) = g \cdot f(x)$$

para cualesquiera $g \in G$, $x \in X$.

En otras palabras, si las acciones de G vienen dadas por aplicaciones $\alpha\colon G \times X \to X$ y $\beta\colon G \times Y \to Y$, entonces $f\colon X \to Y$ es equivariante precisamente cuando el diagrama de abajo conmuta:

$$\begin{array}{ccc} G \times X & \xrightarrow{\mathrm{id}\times f} & G \times Y \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ X & \xrightarrow[f]{} & Y \end{array}$$

9.1.10. Definición. Si X es un G-conjunto y $X_0 \subseteq X$ es un subconjunto tal que para cualesquiera $g \in G$ y $x \in X_0$ se cumple $g \cdot x \in X_0$, se dice que X_0 es un subconjunto **G-invariante**.

En este caso la acción de G sobre X se restringe a X_0 y el último también puede ser visto como un G-conjunto. En la siguiente sección vamos a estudiar cómo un G-conjunto puede ser descompuesto en subconjuntos G-invariantes.

9.1.11. Ejemplo. Sea k un cuerpo. El **espacio afín** n-dimensional sobre k es nada más el conjunto

$$\mathbb{A}^n(k) := k^n = \{(x_1, \ldots, x_n) \mid x_i \in k\}.$$

El grupo $k^\times$ actúa sobre $\mathbb{A}^n(k)$ mediante la multiplicación: para $\lambda \in k^\times$

$$\lambda \cdot (x_1, \ldots, x_n) := (\lambda x_1, \ldots, \lambda x_n).$$

El subconjunto $\mathbb{A}^n(k) \setminus \{(0, \ldots, 0)\}$ es $k^\times$-equivariante: multiplicando un punto no nulo por un escalar no nulo, se obtiene un punto no nulo. ▲

9.2 Órbitas y estabilizadores

9.2.1. Definición. Sea X un G-conjunto. Para un punto $x \in X$ su **órbita** $O_x \subseteq X$ es el conjunto de sus imágenes respecto a las acciones de G:

$$O_x := \{g \cdot x \mid g \in G\}$$

(este es visiblemente un subconjunto G-equivariante).

Se dice que x es un **punto fijo** si $g \cdot x = x$ para todo $g \in G$; es decir, si

$$O_x = \{x\}.$$

El conjunto de los puntos fijos se denota por X^G.

El **estabilizador** de x viene dado por todos los elementos de G que dejan x fijo:

$$G_x := \{g \in G \mid g \cdot x = x\} \subseteq G.$$

9.2.2. Observación. *G_x es un subgrupo de G.*

Demostración. Primero, $1 \cdot x = x$. Luego, si $g \cdot x = x$, entonces actuando por g^{-1} se obtiene $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$, donde en la parte izquierda está $g^{-1} \cdot (g \cdot x) = 1 \cdot x = x$. Por fin, si $g \cdot x = x$ y $h \cdot x = x$, entonces $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$. ■

A veces se dice que G_x es el **grupo de isotropía** de x.

9.2.3. Definición. Se dice que una acción de G sobre X es **transitiva** si todos los puntos de X están en la misma órbita; es decir, si para cualesquiera $x, y \in X$ existe $g \in G$ tal que $x = g \cdot y$.

En este caso también se dice que X es un G-conjunto **homogéneo**.

9.2.4. Ejemplo. La acción del grupo simétrico S_X sobre X es transitiva. En particular, la acción de S_n sobre $\{1, 2, \ldots, n\}$ es transitiva. El estabilizador de $1 \leq i \leq n$ es el subgrupo

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

▲

9.2.5. Ejemplo. La acción de $\mathrm{SL}_2(\mathbb{R})$ sobre $\mathcal{H}$ es transitiva. Para verlo, sería suficiente probar que para todo $z \in \mathcal{H}$ existe $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ tal que

$$z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \sqrt{-1}.$$

Luego, la matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ aplica z en $\sqrt{-1}$. Dados dos puntos $z_1, z_2 \in \mathcal{H}$, para enviar z_1 en z_2, sería suficiente aplicar z_1 a $\sqrt{-1}$ y luego $\sqrt{-1}$ en z_2.

Ahora para cualesquiera $z = x + y\sqrt{-1}$ con $y > 0$ tenemos

$$\begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}), \quad \begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix} \cdot \sqrt{-1} = \frac{\sqrt{y}\sqrt{-1} + x/\sqrt{y}}{1/\sqrt{y}} = x + y\sqrt{-1}.$$

▲

9.2.6. Ejemplo. Para la acción de $k^\times$ sobre $\mathbb{A}^n(k)$ el punto $(0, \ldots, 0)$ es fijo. Para un punto $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ su órbita consiste en todos los puntos no nulos que están en la recta que pasa por $(0, \ldots, 0)$ y $(x_1, \ldots, x_n)$:

$$\{(\lambda x_1, \ldots, \lambda x_n) \mid \lambda \in k^\times\}.$$

▲

El siguiente resultado nos dice que todo G-conjunto se descompone en una unión disjunta de G-conjuntos homogéneos.

9.2.7. Observación. *Sea X un G-conjunto. La relación*

$$x \sim_G y \iff x = g \cdot y \text{ para algún } g \in G$$

es una relación de equivalencia sobre X. Las clases de equivalencia son las órbitas. En particular, X se descompone en la union disjunta de las órbitas:

$$X = \bigsqcup_{[x] \in X/G} O_x,$$

donde X/G denota el conjunto de las órbitas.

Demostración. $x \sim_G x$, puesto que $1 \cdot x$. Ahora, si $x \sim_G y$, entonces $x = g \cdot y$ y luego $g^{-1} \cdot x = g^{-1} \cdot (g \cdot y) = y$. Por fin, si $x \sim_G y$ e $y \sim_G z$, tenemos $x = g \cdot y$ e $y = h \cdot z$, así que $x = g \cdot (h \cdot z) = (gh) \cdot z$. ■

9.2.8. Ejemplo. El grupo multiplicativo $k^\times$ actúa sobre $\mathbb{A}^{n+1} \setminus \{\underline{0}\}$. El conjunto de las órbitas correspondiente

$$\mathbb{P}^n(k) := (\mathbb{A}^{n+1} \setminus \{\underline{0}\})/k^\times = \{[x_0 : x_1 : \cdots : x_n] \mid x_i \in k,\ (x_0, x_1, \ldots, x_n) \neq (0, 0, \ldots, 0)\}$$

se llama el **espacio proyectivo** de dimensión n sobre k. Sus elementos son las rectas en el espacio $\mathbb{A}^{n+1}$ que pasan por el origen. Para más información sobre el espacio proyectivo, el lector puede consultar Wikipedia y libros de texto de geometría.

Consideremos el caso $n = 1$. La definición nos dice que hay que considerar los elementos $(x, y) \in \mathbb{A}^2 \setminus \{(0, 0)\}$ módulo la relación de equivalencia

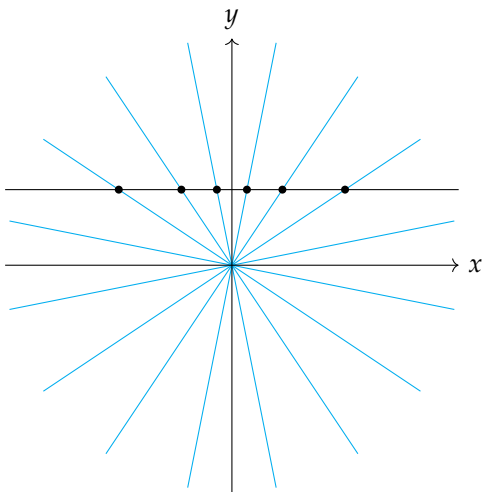
$$(x, y) \sim (\lambda x, \lambda y) \quad \text{para } \lambda \in k^\times.$$

Ahora si $y \neq 0$, tenemos $(x, y) \sim (x/y, 1)$. Si $y = 0$, entonces $x \neq 0$ y $(x, 0) \sim (1, 0)$. Esto nos dice que

$$\mathbb{P}^1(k) = \{[x : 1] \mid x \in k\} \sqcup \{[1 : 0]\}.$$

El conjunto $\{[x : 1] \mid x \in k\}$ está en una biyección natural con la recta afín $\mathbb{A}^1(k)$, y además hay un punto extra $[1 : 0]$ que se llama el **punto al infinito** y normalmente se denota por ∞.

Geométricamente, lo que está pasando es lo siguiente. La recta proyectiva es el conjunto de las rectas en el plano que pasan por el origen. Para parametrizar estas rectas, podemos tomar la proyección sobre una recta paralela a x, por ejemplo $y = 1$:



La recta que corresponde a $[x : y]$ con $y \neq 0$ interseca a la recta $y = 1$ en el punto $(x/y, 1)$. Nos queda la recta $y = 0$ que no tiene intersecciones con $y = 1$. Esta recta corresponde al punto al infinito. ▲

9.2.9. Proposición. *Hay una biyección natural entre la órbita O_x y el conjunto de las clases laterales G/G_x.*

Demostración. Definamos

$$O_x \to G/G_x,$$
$$g \cdot x \mapsto g\,G_x.$$

Esta aplicación está bien definida y es biyectiva:

$$g \cdot x = h \cdot x \iff h^{-1}g \cdot x = x \iff h^{-1}g \in G_x \iff g\,G_x = h\,G_x.$$

■

Los estabilizadores de los elementos de la misma órbita están relacionados de la siguiente manera.

9.2.10. Observación. *Sea X un G-conjunto. Para los estabilizadores se cumple*

$$G_{g\cdot x} = g\,G_x\,g^{-1}.$$

Demostración. Tenemos

$$G_{g\cdot x} = \{h \in G \mid h \cdot g \cdot x = g \cdot x\} = \{h \in G \mid g^{-1} \cdot h \cdot g \cdot x = x\} = g\,G_x\,g^{-1}.$$

■

En general, G_x no es un subgrupo normal de G. Por ejemplo, para el grupo simétrico S_3 que actúa sobre $\{1,2,3\}$ el estabilizador de 3 es el subgrupo $\{\mathrm{id}, (1\ 2)\} \cong S_2$ que no es normal en S_3. Sin embargo, se puede hablar de las clases laterales G/G_x.

9.2.11. Teorema (Ecuación de clase). *Sea X un G-conjunto finito. Sea X^G el subconjunto de puntos fijos y $O_{x_1}, \ldots, O_{x_n}$ las órbitas de la acción que contienen más de un elemento. Entonces,*

$$|X| = |X^G| + \sum_{1\le i\le n} |G : G_{x_i}|.$$

Demostración. Sigue del resultado anterior y la descomposición en la unión disjunta de clases de equivalencia

$$X = \bigsqcup_{x\in X^G} \{x\} \sqcup \bigsqcup_{1\le i\le n} O_{x_i}.$$

■

9.3 Acción de G sobre sí mismo por multiplicación

Algunos conceptos y resultados de la teoría de grupos pueden ser investigados en términos de acciones específicas de G sobre $X = G$.

Para $g, x \in G$ la fórmula

$$g \cdot x := gx$$

define una acción de G: los axiomas A1) y A2) son evidentes. Se dice que G actúa sobre sí mismo por multiplicación (por la izquierda).

9.3.1. Proposición. *La acción de G sobre sí mismo por multiplicación es fiel.*

Demostración. Esta acción corresponde a un homomorfismo

$$\begin{aligned} L\colon G &\to S_G, \\ g &\mapsto (L_g\colon x \to gx). \end{aligned}$$

Tenemos $L_g(1) = g \cdot 1 = g$, así que $L_g = \mathrm{id}_G$ si y solamente si $g = 1$. ■

9.3.2. Corolario (Teorema de Cayley). *Para todo grupo G existe un monomorfismo $G \rightarrowtail S_G$.*

Entonces, todo grupo G es isomorfo a un subgrupo de S_G. En particular, todo grupo finito es isomorfo a un subgrupo de S_n para algún n.

9.3.3. Comentario. La teoría de grupos surgió del estudio de permutaciones de raíces de polinomios en los trabajos de Lagrange (1770) y Galois (1831). De hecho, la palabra "grupo" viene de la expresión "grupo de permutaciones". La primera definición axiomática de grupo dio Cayley*. El último resultado nos dice que todos los grupos pueden ser realizados como subgrupos de grupos de permutaciones.

9.3.4. Ejemplo. La construcción de arriba no es muy efectiva: el grupo simétrico S_G es mucho más grande que G. El ejemplo mínimo no trivial sería de

$$G = \mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}.$$

La aplicación $x \mapsto [0] + x$ es la permutación identidad de los elementos de G. Luego, $x \mapsto [1] + x$ es la permutación

$$\begin{pmatrix} [0] & [1] & [2] \\ [1] & [2] & [0] \end{pmatrix}$$

e $x \mapsto [2] + x$ es la permutación

$$\begin{pmatrix} [0] & [1] & [2] \\ [2] & [0] & [1] \end{pmatrix}$$

La biyección $\{[0], [1], [2]\} \leftrightarrow \{1, 2, 3\}$ nos da un isomorfismo entre $S_{\mathbb{Z}/3\mathbb{Z}}$ y S_3 respecto al cual la imagen de G en S_3 puede ser identificada con

$$\left\{ \mathrm{id},\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3),\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2) \right\}.$$

De hecho, es A_3, el único subgrupo de orden 3 en S_3. ▲

9.3.5. Comentario. En general, si $H \subseteq G$ es un subgrupo, entonces G actúa sobre el conjunto de las clases laterales izquierdas G/H mediante multiplicación:

$$g_1 \cdot g_2 H := g_1 g_2 H.$$

Esta acción es transitiva.

*Arthur Cayley (1821–1895), uno de los fundadores de la escuela británica moderna de matemáticas puras.

9.4 Acción de G sobre sí mismo por conjugación

9.4.1. Definición. Para $g, x \in G$ la **conjugación** de x por g viene dada por

$$^{g}x := g\,x\,g^{-1}.$$

Notamos que para la identidad se tiene $^{1}x = x$ y para cualesquiera $g, h, x \in G$

$$^{h}(^{g}x) = h\,(g\,x\,g^{-1})\,h^{-1} = (hg)\,x\,(hg)^{-1} = {}^{hg}x. \tag{9.2}$$

Entonces, lo que tenemos es una acción de G sobre sí mismo. La notación "^{g}x" es una especie de "potencia", pero con el exponente escrito a la izquierda, puesto que la acción es por la izquierda.

9.4.2. Definición. Para la acción de G sobre sí mismo por conjugación la órbita

$$^{G}x := \{^{g}x = g\,x\,g^{-1} \mid g \in G\}$$

se llaman la **clase de conjugación** de x. El estabilizador

$$C_G(x) := \{g \in G \mid {}^{g}x := g\,x\,g^{-1} = x\} \subseteq G$$

se llama el **centralizador** de x.

9.4.3. Ejemplo. Como todo estabilizador, $C_G(x)$ no es necesariamente un subgrupo normal. Por ejemplo, en $G = S_3$ tenemos

$$C_{S_3}((1\ 2)) = \{\mathrm{id}, (1\ 2)\}.$$

De todos modos, podemos considerar las clases laterales $S_3/C_{S_3}((1\ 2))$. Estas están representadas por $(1\ 2), (1\ 3), (2\ 3)$ que son los elementos de la clase de conjugación de $(1\ 2)$. ▲

Notamos que $x \in G$ es un punto fijo si y solamente si x pertenece al centro de G:

$$^{g}x := g\,x\,g^{-1} = x \text{ para todo } g \in G \iff x \in Z(G).$$

9.4.4. Observación. *Un subgrupo $H \subseteq G$ es normal si y solamente si H es una unión de clases de conjugación en G.*

Demostración. $H \subseteq G$ es normal si y solamente si para todo elemento $h \in H$ se tiene $^{G}h \subseteq H$. ■

9.4.5. Ejemplo. Prometí que íbamos a demostrar directamente que el grupo alternante A_5 es simple. En efecto, las clases de conjugación son las siguientes.

clase:	$^{G}\mathrm{id}$	$^{G}(1\,2)\,(3\,4)$	$(1\,2\,3)$	$^{G}(1\,2\,3\,4\,5)$	$^{G}(1\,2\,3\,5\,4)$
tamaño:	1	15	20	12	12

Ya que todo subgrupo normal es una unión de clases de conjugación y contiene id, un cálculo tedioso nos dice que los posibles órdenes de subgrupos normales son

$$1,\ 13,\ 16,\ 21,\ 25,\ 28,\ 33,\ 36,\ 40,\ 45,\ 48,\ 60.$$

Ningún número de estos, salvo 1 y 60, divide a $|A_5| = 60$, y gracias al teorema de Lagrange podemos concluir que A_5 es un grupo simple. ▲

9.4.6. Teorema (Ecuación de clase). *Para un grupo finito G sean $x_1, \dots, x_n$ los representantes de las clases de conjugación no triviales. Entonces*

$$|G| = |Z(G)| + \sum_{1 \le i \le n} |G : C_G(x_i)|.$$

Demostración. Es un caso particular de 9.2.11. ■

Notamos que para cualesquiera $g, x, y \in G$ se tiene

$$^g(xy) = g\,(xy)\,g^{-1} = (g\,x\,g^{-1})\,(g\,y\,g^{-1}) = {}^g x\,{}^g y,$$

así que las aplicaciones

$$I_g \colon x \mapsto {}^g x$$

no son simplemente biyecciones $G \to G$ sino automorfismos. Tenemos entonces un homomorfismo de grupos

$$\begin{aligned} I \colon G &\to \operatorname{Aut}(G) \subset S_G, \\ g &\mapsto (I_g \colon x \mapsto {}^g x). \end{aligned}$$

El núcleo de I coincide con el centro de G:

$$\ker I = \{g \in G \mid I_g = \mathrm{id}_G\} = \{g \in G \mid {}^g x := g\,x\,g^{-1} = x \text{ para todo } x \in G\} = Z(G).$$

Entonces, la acción de G sobre sí mismo por conjugación es fiel si y solamente si $Z(G) = \{1\}$.

De la misma manera, se ve que $x \in G$ es un punto fijo de la acción por conjugación si y solamente si $x \in Z(G)$.

9.4.7. Digresión. Los automorfismos de la forma

$$\begin{aligned} I_g \colon G &\to G, \\ x &\mapsto {}^g x \end{aligned}$$

se llaman los **automorfismos internos** de G. Estos forman un grupo (es la imagen del homomorfismo I) que se denota por $\operatorname{Inn}(G)$. El teorema de isomorfía nos dice que

$$G/Z(G) \cong \operatorname{Inn}(G).$$

Por ejemplo, $Z(S_n) = \{\mathrm{id}\}$ para $n \ge 3$, entonces todos los automorfismos de S_n son internos.

Notamos que $\mathrm{Inn}(G)$ es un subgrupo normal en $\mathrm{Aut}(G)$. De hecho, tenemos para cualquier automorfismo $f\colon G \to G$

$$f \circ I_g \circ f^{-1}(x) = f(g\, f^{-1}(x)\, g^{-1}) = f(g)\, x\, f(g)^{-1} = I_{f(g)}(x).$$

Así que $f \circ I_g \circ f^{-1} = I_{f(g)} \in \mathrm{Inn}(G)$. El grupo cociente

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$$

se llama el **grupo de automorfismos externos**.

Para terminar esta sección, notamos que la conjugación es una acción sobre el conjunto de subgrupos.

9.4.8. Observación. *Sea G un grupo y H su subgrupo. Entonces para todo $g \in H$ el conjunto*

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\}$$

es también un subgrupo de G.

Demostración. Por supuesto, tenemos $1 = g \cdot 1 \cdot g^{-1}$. Ahora para $g\,h_1\,g^{-1}, g\,h_2\,g^{-1} \in gHg^{-1}$ se tiene

$$(g\,h_1\,g^{-1})\,(g\,h_2\,g^{-1}) = g\,(h_1h_2)\,g^{-1} \in gHg^{-1}.$$

Por fin, para $ghg^{-1} \in gHg^{-1}$ se tiene

$$(ghg^{-1})^{-1} = g\,h^{-1}\,g^{-1} \in gHg^{-1}.$$

■

Esto quiere decir que la acción de G sobre sí mismo por conjugación induce una acción sobre el conjunto de los subgrupos de G. Los puntos fijos de esta acción son precisamente los subgrupos normales.

9.5 Isomorfismos excepcionales: $\mathrm{PGL}_2(\mathbb{F}_3)$ y $\mathrm{PGL}_2(\mathbb{F}_5)$

En el capítulo 7 durante la discusión de grupos simples mencioné los isomorfismos excepcionales $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$ y $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$. Ahora tenemos las herramientas adecuadas para deducirlos. Esta sección es opcional.

9.5.1. Ejemplo. El grupo $\mathrm{GL}_2(k)$ actúa sobre el plano afín $\mathbb{A}^2(k)$ mediante aplicaciones lineales. Toda aplicación lineal preserva cada recta que pasa por el origen, así que esta acción da lugar a una acción de $\mathrm{GL}_2(k)$ sobre la recta proyectiva $\mathbb{P}^1(k)$. Esta acción no es fiel: dos matrices actúan de la misma manera si y solamente si una es un múltiplo escalar de la otra. Esto quiere decir que el núcleo de la acción es el subgrupo de las matrices escalares $Z(\mathrm{GL}_2(k)) \cong k^\times$. Luego, el cociente de $\mathrm{GL}_2(k)$ por este subgrupo:

$$\mathrm{PGL}_2(k) := \mathrm{GL}_2(k)/Z(\mathrm{GL}_2(k))$$

actúa sobre $\mathbb{P}^1(k)$ de manera fiel. Esto significa que existe un monomorfismo

$$\mathrm{PGL}_2(k) \rightarrowtail S_{\mathbb{P}^1(k)}.$$

Nos interesa el caso cuando $k = \mathbb{F}_p$ es un cuerpo finito. El orden de $\mathrm{PGL}_2(\mathbb{F}_p)$ viene dado por

$$|\mathrm{PGL}_2(\mathbb{F}_p)| = |\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times| = |\mathrm{GL}_2(\mathbb{F}_p)|/|\mathbb{F}_p^\times| = \frac{(p^2-1)(p^2-p)}{p-1} = p^3 - p.$$

Luego,

$$|S_{\mathbb{P}^1(\mathbb{F}_p)}| = (|\mathbb{P}^1(\mathbb{F}_p)|)! = (p+1)!$$

—la descomposición de $\mathbb{P}^1(\mathbb{F}_p)$ en $\mathbb{A}^1(\mathbb{F}_p)$ y ∞ nos dice que

$$|\mathbb{P}^1(\mathbb{F}_p)| = p + 1.$$

Ya que hay un monomorfismo $\mathrm{PGL}_2(\mathbb{F}_p) \rightarrowtail S_{\mathbb{P}^1(\mathbb{F}_p)}$, podemos comparar los órdenes de estos grupos para diferentes p. El factorial crece mucho más rápido que $p^3 - p$, así que solamente para valores pequeños de p se puede esperar algo interesante. Y en efecto, tenemos lo siguiente:

p	$\lvert\mathrm{PGL}_2(\mathbb{F}_p)\rvert$	$\lvert S_{\mathbb{P}^1(\mathbb{F}_p)}\rvert$
2	6	$3! = 6$
3	24	$4! = 24$
5	120	$6! = 720$
7	336	$8! = 40\,320$

Las primeras dos filas nos dicen que hay isomorfismos

$$\mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) \cong S_3, \quad \mathrm{PGL}_2(\mathbb{F}_3) \cong S_4.$$

Notamos que para $p \neq 2$ se tiene

$$\begin{aligned}|\mathrm{PSL}_2(\mathbb{F}_p)| = |\mathrm{SL}_2(\mathbb{F}_p)/Z(\mathrm{SL}_2(\mathbb{F}_p))| = |\mathrm{SL}_2(\mathbb{F}_p)/\{\pm I\}| &= \frac{1}{2}|\mathrm{SL}_2(\mathbb{F}_p)| \\ &= \frac{1}{2}\cdot\frac{1}{p-1}|\mathrm{GL}_2(\mathbb{F}_p)| = \frac{1}{2}|\mathrm{PGL}_2(\mathbb{F}_p)|,\end{aligned}$$

así que $\mathrm{PSL}_2(\mathbb{F}_p)$ es un subgrupo de índice 2 en $\mathrm{PGL}_2(\mathbb{F}_p)$. Siendo un subgrupo de índice 2, es normal. En $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$ hay un subgrupo único de índice 2: es isomorfo al grupo alternante. Podemos concluir que

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

▲

Ya que $|\mathrm{PGL}_2(\mathbb{F}_5)| = 120 = 5!$, esto nos da esperanzas de encontrar un isomorfismo $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$. Sin embargo, las consideraciones de arriba nos dicen nada más que $\mathrm{PGL}_2(\mathbb{F}_5)$ puede ser realizado como un subgrupo de índice 6 en S_6, y hay que usar otro argumento.

9.5.2. Ejemplo. Los puntos de $\mathbb{P}^1(\mathbb{F}_5)$ son

$$0 = [0:1], \quad 1 = [1:1], \quad 2 = [2:1], \quad 3 = [3:1], \quad 4 = [4:1], \quad \infty = [1:0].$$

En $S_{\mathbb{P}^1(\mathbb{F}_5)}$ hay 15 permutaciones de orden 2 sin puntos fijos (en otras palabras, permutaciones de tipo $(\bullet\ \bullet)\,(\bullet\ \bullet)\,(\bullet\ \bullet)$):

$$\begin{array}{lll}
(0\,1)\,(2\,3)\,(4\,\infty), & (0\,1)\,(2\,4)\,(3\,\infty), & (0\,1)\,(2\,\infty)\,(3\,4),\\
(0\,2)\,(1\,3)\,(4\,\infty), & (0\,2)\,(1\,4)\,(3\,\infty), & (0\,2)\,(1\,\infty)\,(3\,4),\\
(0\,3)\,(1\,2)\,(4\,\infty), & (0\,3)\,(1\,4)\,(2\,\infty), & (0\,3)\,(1\,\infty)\,(2\,4),\\
(0\,4)\,(1\,2)\,(3\,\infty), & (0\,4)\,(1\,3)\,(2\,\infty), & (0\,4)\,(1\,\infty)\,(2\,3),\\
(0\,\infty)\,(1\,2)\,(3\,4), & (0\,\infty)\,(1\,3)\,(2\,4), & (0\,\infty)\,(1\,4)\,(2\,3).
\end{array}$$

Solamente 10 de estas permutaciones vienen de la acción de $\mathrm{PGL}_2(\mathbb{F}_5)$:

$$\begin{array}{ll}
\begin{pmatrix}1&4\\4&4\end{pmatrix} \mapsto (0\,1)\,(2\,3)\,(4\,\infty), & \begin{pmatrix}1&4\\3&4\end{pmatrix} \mapsto (0\,1)\,(2\,\infty)\,(3\,4),\\
\begin{pmatrix}1&3\\4&4\end{pmatrix} \mapsto (0\,2)\,(1\,3)\,(4\,\infty), & \begin{pmatrix}1&3\\2&4\end{pmatrix} \mapsto (0\,2)\,(1\,4)\,(3\,\infty),\\
\begin{pmatrix}1&2\\3&4\end{pmatrix} \mapsto (0\,3)\,(1\,4)\,(2\,\infty), & \begin{pmatrix}1&2\\1&4\end{pmatrix} \mapsto (0\,3)\,(1\,\infty)\,(2\,4),\\
\begin{pmatrix}1&1\\2&4\end{pmatrix} \mapsto (0\,4)\,(1\,2)\,(3\,\infty), & \begin{pmatrix}1&1\\1&4\end{pmatrix} \mapsto (0\,4)\,(1\,\infty)\,(2\,3),\\
\begin{pmatrix}0&1\\3&0\end{pmatrix} \mapsto (0\,\infty)\,(1\,2)\,(3\,4), & \begin{pmatrix}0&1\\2&0\end{pmatrix} \mapsto (0\,\infty)\,(1\,3)\,(2\,4).
\end{array}$$

Y otras 5 permutaciones no vienen de la acción de $\mathrm{PGL}_2(\mathbb{F}_5)$:

$$(0\,1)\,(2\,4)\,(3\,\infty), \quad (0\,2)\,(1\,\infty)\,(3\,4), \quad (0\,3)\,(1\,2)\,(4\,\infty), \quad (0\,4)\,(1\,3)\,(2\,\infty), \quad (0\,\infty)\,(1\,4)\,(2\,3).$$

El grupo $S_{\mathbb{P}^1(\mathbb{F}_5)}$, y en particular su subgrupo $\mathrm{PGL}_2(\mathbb{F}_5)$, actúa por conjugación sobre las 15 permutaciones de tipo $(\bullet\ \bullet)\,(\bullet\ \bullet)\,(\bullet\ \bullet)$. La acción de $\mathrm{PGL}_2(\mathbb{F}_5)$ se restringe a una acción fiel sobre las 5 permutaciones de arriba. Esto nos da un monomorfismo $\mathrm{PGL}_2(\mathbb{F}_5) \rightarrowtail S_5$. Ya que $|\mathrm{PGL}_2(\mathbb{F}_5)| = |S_5|$, podemos concluir que

$$\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5.$$

Además, $\mathrm{PSL}_2(\mathbb{F}_5)$ es un subgrupo de índice 2 en $\mathrm{PGL}_2(\mathbb{F}_5)$, así que

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

▲

9.6 Ejercicios

Ejercicio 9.1. *Consideremos la acción del grupo* $\mathrm{SL}_2(\mathbb{R})$ *sobre el semiplano superior* $\mathcal{H}$*. Demuestre que el estabilizador para el punto* $\sqrt{-1} \in \mathcal{H}$ *es el grupo*

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\phi & -\operatorname{sen}\phi \\ \operatorname{sen}\phi & \cos\phi \end{pmatrix} \;\middle|\; 0 \leq \phi < 2\pi \right\} = O_2(\mathbb{R}) \cap \mathrm{SL}_2(\mathbb{R}).$$

Ejercicio 9.2. *Consideremos la acción del grupo* $\mathrm{SL}_2(\mathbb{Z})$ *sobre el semiplano superior* $\mathcal{H}$*. Calcule el estabilizador para los puntos* $\sqrt{-1}$ *y* $\omega := -\frac{1}{2} + \frac{\sqrt{3}}{2}\sqrt{-1}$*.*

Ejercicio 9.3. *Demuestre que el núcleo de la acción de* $\mathrm{SL}_2(\mathbb{R})$ *sobre* $\mathcal{H}$ *es el subgrupo* $Z(\mathrm{SL}_2(\mathbb{R})) = \{\pm I\}$*.*

Ejercicio 9.4. *Sea* p *un número primo y sea* X *un* G*-conjunto finito. Supongamos que para todo subgrupo* $H \subsetneq G$ *su índice es divisible por* p*:*

$$p \;\mid\; |G : H|.$$

Deduzca que el número de los puntos fijos es congruente módulo p *al número de los elementos de* X*:*

$$|X| \equiv |X^G| \pmod{p}.$$

Indicación: considere la ecuación de clase.

Ejercicio 9.5. *Supongamos que* G *es un grupo finito de orden* p^k *donde* p *es primo. Demuestre que* $p \mid |Z(G)|$*, y en particular* $Z(G) \neq \{1\}$*.*

Ejercicio 9.6. *Demuestre que si* G *es un grupo finito de orden* p^2*, entonces* G *es abeliano.*

Ejercicio 9.7 (Teorema de Cayley). *Sea* G *un grupo finito y sea* p *un número primo tal que* $p \mid |G|$*. En este ejercicio vamos a probar que en* G *hay un elemento de orden* p*. Para esto consideremos el conjunto*

$$X := \{(g_0, g_1, \ldots, g_{p-1}) \mid g_i \in G,\ g_0 g_1 \cdots g_{p-1} = 1\}.$$

1) *Demuestre que* $|X| = |G|^{p-1}$*.*

2) *Para* $[n]_p \in \mathbb{Z}/p\mathbb{Z}$ *sea* $[n]_p \cdot (g_0, g_1, \ldots, g_{p-1}) := (g_{[0+n]}, g_{[1+n]}, \ldots, g_{[p-1+n]})$*. Demuestre que esto define una acción de* $\mathbb{Z}/p\mathbb{Z}$ *sobre* X *y sus puntos fijos son* $(g, g, \ldots, g)$ *donde* $g^p = 1$*.*

3) *Demuestre que el número de elementos* $g \in G$ *tales que* $g^p = 1$ *es divisible por* p*. Concluya que existe* $g \neq 1$ *tal que* $g^p = 1$*.*

Ejercicio 9.8. *Supongamos que un grupo finito* G *actúa sobre un conjunto finito* X*. Para un elemento* $g \in G$ *denotemos por* X^g *el conjunto de todos los puntos fijos por* g*:*

$$X^g := \{x \in X \mid g \cdot x = x\}.$$

Demuestre que

$$\sum_{x \in X} |G_x| = \sum_{g \in G} |X^g|.$$

Deduzca la siguiente identidad combinatoria[*]*:*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

(en palabras: el número de órbitas es igual al número promedio de puntos fijos).
Indicación: use las biyecciones $O_x \cong G/G_x$.

Ejercicio 9.9. *Verifique la descripción de las clases de conjugación en* A_5.

Ejercicio 9.10. *Hemos probado que en* A_n *para* $n \geq 5$ *todos los* 3*-ciclos forman una clase de conjugación. Demuestre que en* A_4 *no todos los* 3*-ciclos son conjugados entre sí.*

Ejercicio 9.11. *Encuentre las clases de conjugación en el grupo de cuaterniones* Q_8.

Ejercicio 9.12. *En este ejercicio encontraremos las clases de conjugación del grupo diédrico* D_n.

1) *Demuestre que cada rotación* r^i *está conjugada con* r^{-i} *y consigo misma.*
2) *Demuestre que la clase de conjugación de la reflexión* fr^i *viene dada por las reflexiones* fr^{i-2j} *para* $j \in \mathbb{Z}$.
3) *Termine la descripción de las clases de conjugación. (La respuesta depende de la paridad de n.)*

Ejercicio 9.13. *Hemos visto que* $\mathbb{P}^1(k) = \mathbb{A}^1(k) \sqcup \{\infty\}$.

1) *Demuestre que en general* $\mathbb{P}^n(k) = \mathbb{A}^n(k) \sqcup \mathbb{P}^{n-1}(k)$.
2) *Deduzca que* $\mathbb{P}^n(k) = \mathbb{A}^n(k) \sqcup \mathbb{A}^{n-1}(k) \sqcup \cdots \sqcup \mathbb{A}^0(k)$.
3) *Calcule el número de puntos en el espacio proyectivo* $\mathbb{P}^n(\mathbb{F}_p)$ *usando 2).*
4) *Calcule el mismo número a partir de la definición* $\mathbb{P}^n(\mathbb{F}_p) := (\mathbb{A}^{n+1}(\mathbb{F}_p) \setminus \{\underline{0}\})/\mathbb{F}_p^\times$.

Ejercicio 9.14. *Describa la permutación de* $\{0, 1, 2, 3, 4, \infty\}$ *que corresponde a la acción de* $\begin{pmatrix} 1 & 3 \\ 1 & 0 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_5)$ *sobre* $\mathbb{P}^1(\mathbb{F}_5)$.

[*]Este identidad se conoce como el **lema de Burnside** y es muy común en combinatoria y matemáticas recreativas.

Capítulo 10
Productos de grupos

En este capítulo vamos a investigar la construcción del producto directo y semidirecto de grupos. Este es un modo de construir un grupo G a partir de dos grupos H y K. Luego, en §10.3 vamos a definir la noción de extensión de un grupo por otro. Resulta que los productos directos y semidirectos son casos muy especiales de extensiones. En §10.4 vamos a probar que todo grupo abeliano finitamente generado es isomorfo a un producto de grupos cíclicos. Finalmente, la sección §10.5 presenta un ejemplo muy importante de grupos abelianos finitamente generados: el grupo de puntos racionales de una curva elíptica.

10.1 Productos directos

10.1.1. Definición. Para dos grupos H y K su **producto directo** (o simplemente **producto**) es el conjunto

$$H \times K := \{(h,k) \mid h \in H, k \in K\}$$

dotado de la operación

$$(h_1,k_1) \cdot (h_2,k_2) := (h_1h_2, k_1k_2).$$

Ya que H y K son grupos, $H \times K$ es también un grupo. La identidad es $(1_H, 1_K)$ y los elementos inversos son $(h,k)^{-1} = (h^{-1}, k^{-1})$.

De la misma manera, para una familia de grupos $(H_i)_{i\in I}$, se define el producto

$$\prod_{i\in I} H_i := \{(h_i)_{i\in I} \mid h_i \in H_i\}$$

respecto a la operación

$$(h_i)_{i\in I} \cdot (h'_i)_{i\in I} := (h_i \cdot h'_i)_{i\in I}.$$

Si A y B son grupos abelianos, está claro que el producto $A \times B$ es también un grupo abeliano. En general, si $(A_i)_{i\in I}$ es una familia de grupos abelianos, entonces su producto $\prod_{i\in I} A_i$ es abeliano.

10.1.2. Ejemplo. Para el producto

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0),(0,1),(1,0),(1,1)\}$$

la tabla de adición viene dada por

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Recordemos la tabla de multiplicación del grupo

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

$\circ$	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

Podemos convencernos a simple vista de que

$$V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

▲

10.1.3. Ejemplo. ¿Cuándo el producto de dos grupos cíclicos finitos es también cíclico? Para un elemento $(a,b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tenemos

$$\begin{aligned}\operatorname{ord}(a,b) = \min\{k \mid k\cdot(a,b) = (k\cdot a, k\cdot b) = (0,0)\} &= \min\{k \mid k \mid \operatorname{ord} a,\ k \mid \operatorname{ord} b\} \\ &= \operatorname{mcm}(\operatorname{ord} a, \operatorname{ord} b) = \frac{\operatorname{ord} a \cdot \operatorname{ord} b}{\operatorname{mcd}(\operatorname{ord} a, \operatorname{ord} b)}.\end{aligned}$$

Luego, el grupo $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ es cíclico si y solamente si este posee un elemento de orden

$$|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn.$$

Este elemento tiene que ser de la forma (a,b) donde a es un generador de $\mathbb{Z}/m\mathbb{Z}$ (es decir, $\operatorname{ord} a = m$) y b es un generador de $\mathbb{Z}/n\mathbb{Z}$ (es decir, $\operatorname{ord} a = n$) y además necesitamos tener $\operatorname{mcd}(m,n) = 1$. Entonces, el producto de dos grupos cíclicos es también cíclico si y solamente si los ordenes de grupos son coprimos:

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z} \iff \operatorname{mcd}(m,n) = 1.$$

Por ejemplo,

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \ncong \mathbb{Z}/4\mathbb{Z}.$$

▲

De hecho, las consideraciones de arriba pueden ser resumidas de manera más precisa.

10.1.4. Proposición (Teorema chino del resto). *Sean m y n dos números naturales coprimos. Entonces existe un isomorfismo canónico*

$$\begin{aligned}\mathbb{Z}/mn\mathbb{Z} &\xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\\ [a]_{mn} &\mapsto ([a]_m, [a]_n).\end{aligned}$$

Demostración. Consideremos el homomorfismo canónico

$$\begin{aligned}f\colon \mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\\ a &\mapsto ([a]_m, [a]_n)\end{aligned}$$

inducido por las proyecciones canónicas $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$. Tenemos

$$\ker f = m\mathbb{Z} \cap n\mathbb{Z} = \operatorname{mcm}(m,n)\mathbb{Z}.$$

Ya que m y n son coprimos, $\operatorname{mcm}(m,n) = mn$. Luego, f induce un monomorfismo

$$\overline{f}\colon \mathbb{Z}/mn\mathbb{Z} \xrightarrow{\cong} \operatorname{im} f \rightarrowtail \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Pero

$$|\mathbb{Z}/mn\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn,$$

así que $\overline{f}$ tiene que ser un isomorfismo. ■

10.1.5. Corolario. *La función ϕ de Euler es multiplicativa en el sentido de que*

$$\phi(mn) = \phi(m) \cdot \phi(n), \quad \textit{si } \operatorname{mcd}(m,n) = 1.$$

Demostración. $\phi(mn), \phi(m), \phi(n)$ representan el número de generadores de $\mathbb{Z}/mn\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ respectivamente. Bajo el isomorfismo

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

se ve que $[a]_{mn}$ es un generador de $\mathbb{Z}/mn\mathbb{Z}$ si y solamente si $[a]_m$ es un generador de $\mathbb{Z}/m\mathbb{Z}$ y $[a]_n$ es un generador de $\mathbb{Z}/n\mathbb{Z}$. ■

10.1.6. Proposición. *Si n es un número natural cuya factorización en primos es*

$$n = p_1^{k_1} \cdots p_\ell^{k_\ell},$$

entonces

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\ell}\right).$$

Demostración. Gracias a la multiplicatividad, tenemos

$$\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_\ell^{k_\ell}).$$

Luego de esto, se puede calcular directamente

$$\phi(p_i^{k_i}) = p_i^{k_i} \left(1 - \frac{1}{p_i}\right)$$

(véase el capítulo 4). ■

10.1.7. Ejemplo. Tenemos

$$\phi(198) = \phi(2 \cdot 3^2 \cdot 11) = \phi(2) \cdot \phi(3^2) \cdot \phi(11) = 1 \cdot 6 \cdot 10 = 60.$$

Otro ejemplo: $2018 = 2 \cdot 1009$ donde 1009 es primo, y por lo tanto $\phi(2018) = 1008$. ▲

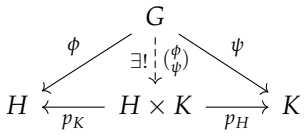
El producto directo está dotado de dos homomorfismos canónicos (proyecciones)

$$\begin{array}{ccccc} H & \xleftarrow{p_H} & H \times K & \xrightarrow{p_K} & K \\ h & \longleftarrow & (h,k) & \longmapsto & k \end{array}$$

10.1.8. Observación (Propiedad universal del producto). *Sea G un grupo junto con dos homomorfismos $\phi\colon G \to H$ y $\psi\colon G \to K$. Entonces, existe una única aplicación $\binom{\phi}{\psi}\colon G \to H \times K$ tal que*

$$p_H \circ \binom{\phi}{\psi} = \phi, \quad p_K \circ \binom{\phi}{\psi} = \psi.$$

(10.1)



Demostración. A nivel de conjuntos, la única opción posible es

$$\begin{aligned} \binom{\phi}{\psi}\colon G &\to H \times K, \\ g &\mapsto (\phi(g), \psi(g)), \end{aligned}$$

y es un homomorfismo de grupos, puesto que ϕ y ψ lo son. ■

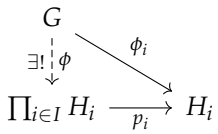
La propiedad universal del producto nos dice que los homomorfismos $G \to H \times K$ corresponden a pares de homomorfismos $G \to H$ y $G \to K$: existe una biyección *natural*

$$\begin{aligned} \mathrm{Hom}(G, H \times K) &\xrightarrow{\cong} \mathrm{Hom}(G,H) \times \mathrm{Hom}(G,K), \\ \phi &\mapsto (p_H \circ \phi, p_K \circ \phi). \end{aligned}$$

La misma propiedad universal se cumple para productos infinitos. A saber, tenemos homomorfismos canónicos de proyección

$$\begin{aligned} p_i\colon \prod_{i \in I} H_i &\to H_i, \\ (h_i)_{i \in I} &\mapsto h_i \end{aligned}$$

Si G es un grupo dotado de homomorfismos $\phi_i\colon G \to H_i$, entonces existe un homomorfismo único $\phi\colon G \to \prod_{i \in I} H_i$ tal que $p_i \circ \phi = \phi_i$:



En otras palabras, hay una biyección natural

$$\mathrm{Hom}(G, \prod_{i\in I} H_i) \cong \prod_{i\in I} \mathrm{Hom}(G, H_i).$$

10.1.9. Observación. *El producto de grupos es asociativo en el sentido de que para tres grupos H_1, H_2, H_3 hay isomorfismos naturales*

$$(H_1 \times H_2) \times H_3 \cong H_1 \times (H_2 \times H_3) \cong H_1 \times H_2 \times H_3.$$

Demostración. Sería instructivo probarlo usando únicamente las propiedades universales. Por ejemplo, el grupo

$$(H_1 \times H_2) \times H_3$$

está dotado de dos homomorfismos

$$H_1 \times H_2 \xleftarrow{p_{12}} (H_1 \times H_2) \times H_3 \xrightarrow{p_3} H_3$$

que satisfacen la propiedad universal correspondiente. Por otro lado, el grupo $H_1 \times H_2$ está dotado de dos homomorfismos

$$H_1 \xleftarrow{p_1} H_1 \times H_2 \xrightarrow{p_2} H_2$$

que satisfacen la propiedad universal correspondiente. Ahora dado un grupo G y tres homomorfismos $\phi_1 \colon G \to H_1$, $\phi_2 \colon G \to H_2$, $\phi_3 \colon G \to H_3$, existe un homomorfismo único $\phi_{12} = \binom{\phi_1}{\phi_2} \colon G \to H_1 \times H_2$ que satisface

$$p_1 \circ \phi_{12} = \phi_1, \quad p_2 \circ \phi_{12} = \phi_2$$

y luego un homomorfismo único $\phi = \binom{\phi_{12}}{\phi_3} \colon G \to (H_1 \times H_2) \times H_3$ que satisface

$$p_{12} \circ \phi = \phi_{12}, \quad p_3 \circ \phi = \phi_3.$$

En este caso

$$p_1 \circ p_{12} \circ \phi = \phi_1, \quad p_2 \circ p_{12} \circ \phi = \phi_2, \quad p_3 \circ \phi = \phi_3.$$

Entonces, $(H_1 \times H_2) \times H_3$ junto con los homomorfismos

$$p_1 \circ p_{12} \colon (H_1 \times H_2) \times H_3 \to H_1, \quad p_2 \circ p_{12} \colon (H_1 \times H_2) \times H_3 \to H_2, \quad p_3 \colon (H_1 \times H_2) \times H_3 \to H_3$$

satisface la propiedad universal de $H_1 \times H_2 \times H_3$. Por ende hay un isomorfismo

$$(H_1 \times H_2) \times H_3 \cong H_1 \times H_2 \times H_3.$$

■

10.1.10. Observación. *Existe un isomorfismo canónico $H \times K \cong K \times H$.*

Demostración. Este isomorfismo viene dado por $(h,k) \mapsto (k,h)$. También se puede notar que $H \times K$ y $K \times H$ satisfacen la misma propiedad universal (es simétrica en H y K). ■

10.1.11. Comentario. Cuando se trata de grupos *abelianos*, normalmente se habla de la **suma directa** que se denota por

$$A \oplus B = \{(a,b) \mid a \in A,\ b \in B\}.$$

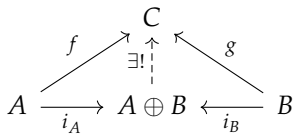
Esta viene con las inclusiones

$$\begin{aligned} i_A \colon A &\to A \oplus B, \\ a &\mapsto (a,0) \end{aligned}$$

y

$$\begin{aligned} i_B \colon B &\to A \oplus B, \\ b &\mapsto (0,b) \end{aligned}$$

que satisfacen la propiedad universal



(donde C es también un grupo abeliano). Lo vamos a estudiar en el contexto más general para **módulos sobre anillos**.

10.1.12. Observación. *H y K se identifican con los subgrupos normales*

$$H \times \{1_K\} := \{(h,1_K) \mid h \in H\} \quad y \quad \{1_H\} \times K := \{(1_H,k) \mid k \in K\}$$

de $H \times K$.

Demostración. Evidente de la definición del producto sobre $H \times K$. ■

10.1.13. Proposición. *Supongamos que G es un grupo y $H, K \subset G$ son dos subgrupos normales tales que $H \cap K = \{1\}$ y todo elemento de G puede ser escrito como hk donde $h \in H$ y $k \in K$. Entonces,*

$$G \cong H \times K.$$

Demostración. Primero, notamos que $hk = kh$. En efecto, usando que H y K son normales,

$$hkh^{-1}k^{-1} = h\,(\underbrace{kh^{-1}k^{-1}}_{\in H}) = (\underbrace{hkh^{-1}}_{\in K})\,k^{-1} \in H \cap K = \{1\}.$$

Esto significa que

$$(h_1k_1) \cdot (h_2k_2) = (h_1h_2) \cdot (k_1k_2)$$

para cualesquiera $h_1, h_2 \in H$, $k_1, k_2 \in K$. También podemos comprobar que todo elemento de G se expresa *de modo único* como hk. Si tenemos $hk = h'k'$, entonces

$$h'^{-1}h = k'k^{-1} \in H \cap K = \{1\},$$

y luego $h = h'$ y $k = k'$. Todo esto significa que

$$\begin{aligned} H \times K &\to G, \\ (h, k) &\mapsto hk \end{aligned}$$

es un isomorfismo de grupos. ■

10.1.14. Comentario. Cuando G tiene dos subgrupos H y K que satisfacen las condiciones de 10.1.13, a veces se dice que G es el producto directo **interno**, mientras que la construcción de $H \times K$ de 10.1.1 se llama el producto directo **externo** de H y K.

10.1.15. Ejemplo. Todo número complejo no nulo puede ser escrito de modo único como $r\, e^{\phi\sqrt{-1}}$ donde $r > 0$ es un número real y $0 \leq \phi < 2\pi$. De aquí sigue que

$$\mathbb{C}^\times \cong \mathbb{R}_{>0} \times \mathbb{S}^1,$$

donde $\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$ es el grupo del círculo. ▲

10.1.16. Ejemplo. Consideremos el grupo $\mathrm{GL}_n^+(\mathbb{R})$ de matrices reales invertibles de determinante positivo. Este contiene como sus subgrupos normales el grupo $\mathrm{SL}_n(\mathbb{R})$ y el grupo de matrices escalares

$$\mathbb{R}_{>0} = \{\lambda I \mid \lambda > 0\}.$$

Toda matriz $A \in \mathrm{GL}_n^+(\mathbb{R})$ puede ser escrita como $\lambda A'$ donde $A' \in \mathrm{SL}_n(\mathbb{R})$ y $\lambda > 0$ (tomemos $\lambda = \sqrt[n]{\det A}$ y $A' = \lambda^{-1} A$). Notamos que $\mathbb{R}_{>0} \cap \mathrm{SL}_n(\mathbb{R}) = \{I\}$. Entonces,

$$\mathrm{GL}_n^+(\mathbb{R}) \cong \mathbb{R}_{>0} \times \mathrm{SL}_n(\mathbb{R}).$$

▲

10.2 Productos semidirectos

Hemos visto que un grupo G es un producto directo si y solamente si en G hay subgrupos normales H y K tales que $H \cap K = \{1\}$ y $G = HK$. Podemos considerar una colección más debil de condiciones:

1) sean N y H dos subgrupos de G donde N es normal,

2) supongamos que $N \cap H = \{1\}$,

3) supongamos que $G = NH$.

Entonces, usando el mismo argumento de 10.1.13, se deduce que todo elemento de G puede ser escrito de modo único como nh donde $n \in N$ y $h \in H$. Véamos cómo se multiplican estos elementos. Tenemos

$$(n_1h_1) \cdot (n_2h_2) = n_1\,(h_1n_2h_1^{-1}) \cdot (h_1h_2),$$

donde $h_1n_2h_1^{-1} \in N$, puesto que N es normal. Esta fórmula puede ser escrita como

$$(n_1h_1) \cdot (n_2h_2) = (n_1 \cdot I_{h_1}(n_2)) \cdot (h_1h_2), \tag{10.2}$$

donde I_{h_1} es el automorfismo de conjugación $x \mapsto h\,x\,h^{-1}$ que se restringe a N gracias a su normalidad. La fórmula (10.2) se generaliza a la siguiente construcción.

10.2.1. Definición. Sean N y H dos grupos y sea

$$\begin{aligned} \phi\colon H &\to \operatorname{Aut}(N), \\ \phi &\mapsto \phi_h \end{aligned}$$

un homomorfismo. Entonces, el **producto semidirecto** $N \rtimes_\phi H$ es el conjunto

$$N \times H = \{(n,h) \mid n \in N, h \in H\}$$

dotado de la operación

$$(n_1,h_1) \cdot (n_2,h_2) := (n_1\,\phi_{h_1}(n_2), h_1h_2). \tag{10.3}$$

10.2.2. Observación. *Respecto a la operación de arriba, $N \rtimes_\phi H$ es un grupo.*

Demostración. Primero, hay que ver que la operación es asociativa. Tenemos

$$\begin{aligned} \Big((n_1,h_1) \cdot (n_2,h_2)\Big) \cdot (n_3,h_3) &= (n_1\,\phi_{h_1}(n_2), h_1h_2) \cdot (n_3,h_3) = (n_1\,\phi_{h_1}(n_2)\,\phi_{h_1h_2}(n_3), h_1h_2h_3) \\ &= (n_1\,\phi_{h_1}(n_2)\,\phi_{h_1} \circ \phi_{h_2}(n_3), h_1h_2h_3) = (n_1\,\phi_{h_1}(n_2\,\phi_{h_2}(n_3)), h_1h_2h_3) \\ &= (n_1,h_1) \cdot (n_2\,\phi_{h_2}(n_3), h_2h_3) = (n_1,h_1) \cdot \Big((n_2,h_2) \cdot (n_3,h_3)\Big). \end{aligned}$$

Aquí hemos usado las identidades

$$\phi_{hk} = \phi_h \circ \phi_k \quad \text{y} \quad \phi_h(mn) = \phi_h(m)\,\phi_h(n)$$

para cualesquiera $h,k \in H$ y $m,n \in N$, que provienen del hecho de que $h \mapsto \phi_h$ es un homomorfismo y cada $\phi_h\colon N \to N$ es también un homomorfismo .

La identidad en $N \rtimes_\phi H$ es $(1_N, 1_H)$:

$$(n,h) \cdot (1_N,1_H) = (n\,\phi_h(1_N), h \cdot 1_H) = (n,h),$$

y de la misma manera

$$(1_N,1_H) \cdot (n,h) = (1_N \cdot \phi_{1_H}(n), 1_H \cdot h) = (1_N \cdot \mathrm{id}(n), h) = (n,h).$$

Los elementos inversos vienen dados por

$$(n,h)^{-1} = (\phi_{h^{-1}}(n^{-1}), h^{-1}).$$

En efecto,

$$\begin{aligned}(n,h)\cdot(\phi_{h^{-1}}(n^{-1}),h^{-1}) = (n\,\phi_h(\phi_{h^{-1}}(n^{-1})), h\,h^{-1}) = (n\,\phi_{h\,h^{-1}}(n^{-1}), h\,h^{-1}) \\ = (n\,n^{-1}, h\,h^{-1}) = (1_N, 1_H)\end{aligned}$$

y también

$$\begin{aligned}(\phi_{h^{-1}}(n^{-1}),h^{-1})\cdot(n,h) = (\phi_{h^{-1}}(n^{-1})\,\phi_{h^{-1}}(n), h\,h^{-1}) = (\phi_{h^{-1}}(n^{-1}\,n), 1_H) \\ = (\phi_{h^{-1}}(1_N), 1_H) = (1_N, 1_H).\end{aligned}$$

■

10.2.3. Comentario. Cuando el homomorfismo $\phi\colon H \to \mathrm{Aut}(N)$ es trivial (es decir, $\phi_h = \mathrm{id}_N$ para todo $h \in H$), entonces $N \rtimes_\phi H$ es el producto directo $N \times H$.

10.2.4. Observación. *N y H se identifican con subgrupos $N \times \{1_H\}$ y $\{1_N\} \times H$ de $N \rtimes_\phi H$. El subgrupo $N \times \{1_H\}$ es normal, y se tiene*

$$N \rtimes_\phi H / N \times \{1_H\} \cong H.$$

Demostración. Todo está claro de la fórmula del producto (10.3). Para calcular el grupo cociente $N \rtimes_\phi H/N \times \{1_H\}$, podemos considerar el homomorfismo

$$\begin{aligned}N \rtimes_\phi H &\to H,\\ (n,h) &\mapsto h\end{aligned}$$

que es sobreyectivo y tiene $N \times \{1_H\}$ como su núcleo. ■

10.2.5. Proposición. *Sea G un grupo y sean N, H sus subgrupos. Supongamos que N es normal, $N \cap H = \{1\}$ y $G = NH$. Entonces, $G \cong N \rtimes_I H$, donde $I\colon H \to \mathrm{Aut}(N)$ asocia a cada $h \in H$ el automorfismo $I_h\colon n \mapsto h\,n\,h^{-1}$.*

Demostración. De la discusión al inicio de esta sección sigue que

$$\begin{aligned}N \rtimes_I H &\to G,\\ (n,h) &\mapsto nh\end{aligned}$$

es un isomorfismo de grupos. ■

10.2.6. Ejemplo. En el grupo diédrico D_n todo elemento es de la forma r^i o bien $fr^i = r^{-i}f$. El subgrupo de rotaciones $\langle r\rangle$ es normal, siendo un subgrupo de índice 2. Además $\langle r\rangle \cap \langle f\rangle = \{\mathrm{id}\}$. En vista de lo anterior, se concluye que $D_n \cong \langle r\rangle \rtimes \langle f\rangle$, donde f actúa sobre $\langle r\rangle$ por la conjugación $r^i \mapsto frf^{-1} = r^{-i}$. ▲

10.2.7. Ejemplo. Sea V un espacio vectorial. El **grupo afín** $\mathrm{Aff}(V)$ es el grupo de aplicaciones

$$\begin{aligned} \phi_{A,u} \colon V &\to V, \\ x &\mapsto Ax + u, \end{aligned}$$

donde $A \in \mathrm{GL}(V)$ y $u \in V$. Es un subgrupo del grupo de biyecciones $V \to V$: tenemos

$$\phi_{B,v} \circ \phi_{A,v}(x) = B\,(A\,x + u) + v = BA\,x + B\,u + v = \phi_{BA,Bu+v}(x).$$

Luego, la identidad es la aplicación $\phi_{I,0}$ y los inversos vienen dados por

$$\phi_{A,u}^{-1} = \phi_{A^{-1},-A^{-1}\,u}.$$

Notamos que $\mathrm{GL}(V)$ se identifica con el subgrupo $H := \{\phi_{A,0} \mid A \in \mathrm{GL}(V)\}$ y el grupo aditivo V se identifica con el subgrupo $N := \{\phi_{I,u} \mid u \in V\}$. El último es normal. Tenemos $N \cap H = \{\phi_{I,0}\}$, y todo elemento de $\mathrm{Aff}(V)$ puede ser escrito como una composición de N y H. Se sigue que

$$\mathrm{Aff}(V) \cong V \rtimes \mathrm{GL}(V).$$

Aquí $\mathrm{GL}(V)$ actúa sobre V de la manera habitual:

$$\phi_{A,0} \circ \phi_{I,u} \circ \phi_{A,0}^{-1} = \phi_{A,0} \circ \phi_{I,u} \circ \phi_{A^{-1},0} = \phi_{I,Au}.$$

▲

10.2.8. Ejemplo. Toda matriz en el grupo $\mathrm{GL}_n(k)$ puede ser escrita como

$$A \cdot \begin{pmatrix} x & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} =: A \cdot \mathrm{diag}(x, 1, \ldots, 1)$$

donde $\det A = 1$ y $x \in k^\times$. Las matrices de determinante 1 forman un subgrupo normal $\mathrm{SL}_n(k)$, mientras que las matrices $\mathrm{diag}(x, 1, \ldots, 1)$ forman un subgrupo isomorfo a $k^\times$ (que no es normal). La intersección de estos dos subgrupos es trivial. Se sigue que

$$\mathrm{GL}_n(k) \cong \mathrm{SL}_n(k) \rtimes k^\times.$$

Aquí $x \in k^\times$ actúa sobre $\mathrm{SL}_n(k)$ mediante la conjugación por $\mathrm{diag}(x, 1, \ldots, 1)$. ▲

10.3 Sucesiones exactas cortas y extensiones

10.3.1. Definición. Una **sucesión exacta corta** de grupos es una sucesión de homomorfismos

$$1 \to H \xrightarrow{i} G \xrightarrow{p} K \to 1$$

donde

1) i es un monomorfismo,

2) p es un epimorfismo,

3) $\operatorname{im} i = \ker p$.

En este caso se dice que G es una **extensión** de K por H.

10.3.2. Comentario. En una sucesión exacta corta "1" denota el grupo trivial $\{1\}$. Los homomorfismos triviales $1 \to H$ y $K \to 1$ significan que $\ker(H \to G) = \operatorname{im}(1 \to H) = \{1\}$ e $\operatorname{im}(G \to K) = \ker(K \to 1) = K$. Cuando se trata de grupos abelianos aditivos, en lugar de "1" se escribe "0".

10.3.3. Ejemplo. Cuando hay un monomorfismo $i\colon H \rightarrowtail G$, el grupo H puede ser identificado con su imagen $i(H) \subseteq G$. Además, la condición $\operatorname{im} i = \ker p$ significa que $i(H)$ es un subgrupo normal, siendo un núcleo. El primer teorema de isomorfía implica que $G/\ker p = G/i(H) \cong K$. Entonces, esencialmente, toda sucesión exacta corta corresponde a la situación cuando H es un subgrupo normal en G, el homomorfismo $i\colon H \rightarrowtail G$ es la inclusión y el homomorfismo p es la proyección canónica sobre el grupo cociente:

$$1 \to H \xrightarrow{i} G \xrightarrow{p} G/H \to 1$$

(Note que en este caso $\operatorname{im} i = \ker p$.) ▲

10.3.4. Ejemplo. Para un producto semidirecto $N \rtimes_\phi H$ tenemos una sucesión exacta corta

$$1 \to N \xrightarrow{n \mapsto (n,h)} N \rtimes_\phi H \xrightarrow{(n,h) \mapsto h} H \to 1$$

Un caso particular es cuando ϕ es trivial y se trata del producto directo $N \times H$. ▲

10.3.5. Ejemplo. Tenemos la siguiente sucesión exacta corta:

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{[1]_2 \mapsto [2]_4} \mathbb{Z}/4\mathbb{Z} \xrightarrow{[1]_4 \mapsto [1]_2} \mathbb{Z}/2\mathbb{Z} \to 0$$

▲

10.3.6. Ejemplo. Tenemos una sucesión exacta corta

$$0 \to \mathbb{Z}/3\mathbb{Z} \xrightarrow{[1]_3 \mapsto [2]_6} \mathbb{Z}/6\mathbb{Z} \xrightarrow{[1]_6 \mapsto [1]_2} \mathbb{Z}/2\mathbb{Z} \to 0$$

y la sucesión exacta corta

$$1 \to A_3 \to S_3 \to \{\pm 1\} \to 1$$

Dado que $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ y $\{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$, ambas sucesiones exactas cortas representan extensiones de $\mathbb{Z}/2\mathbb{Z}$ por $\mathbb{Z}/3\mathbb{Z}$, pero son muy diferentes: la primera es abeliana y la segunda no lo es. ▲

10.3.7. Lema. *Consideremos un diagrama conmutativo de homomorfismos de grupos*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{p} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \xrightarrow{i'} & G' & \xrightarrow{p'} & K & \longrightarrow & 1 \end{array}$$

donde las filas son sucesiones exactas cortas. Luego, $f\colon G \to G'$ es un isomorfismo.

Demostración ("caza de diagramas"). Primero comprobemos que f es inyectivo. Si para algún $g \in G$ se cumple $f(g) = 1$, entonces $p(g) = p'(f(g)) = 1$, y por lo tanto $g \in \ker p = \operatorname{im} i$. Tenemos entonces $g = i(h)$ para algún $h \in H$. Entonces, $i'(h) = f(i(h)) = 1$. La inyectividad de h' implica que $h = 1$. En fin, $g = i(h) = 1$.

Para ver que f es sobreyectiva, tomemos $g' \in G'$. Necesitamos encontrar un elemento $g \in G$ que $f(g) = g'$. Consideremos $p'(g') \in K$. Ya que p es sobreyectivo, existe $g_1 \in G$ tal que $p(g_1) = p'(g')$. Luego,

$$p'(g' \cdot f(g_1)^{-1}) = p'(g') \cdot p' \circ f(g_1)^{-1} = p'(g') \cdot p(g_1)^{-1} = p'(g') \cdot p'(g')^{-1} = 1.$$

Podemos concluir que $g' \cdot f(g_1)^{-1} \in \ker p' = \operatorname{im} i'$ y que existe $h \in H$ tal que $i'(h) = g' \cdot f(g_1)^{-1}$. Tomemos $g := i(h) \cdot g_1$. Luego,

$$f(g) = f \circ i(h) \cdot f(g_1) = i'(h) \cdot f(g_1) = g' \cdot f(g_1)^{-1} \cdot f(g_1) = g'.$$

■

10.3.8. Comentario. El resultado de arriba tiene la siguiente generalización: en el diagrama conmutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{p} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 1 & \longrightarrow & H' & \xrightarrow{i'} & G' & \xrightarrow{p'} & K' & \longrightarrow & 1 \end{array}$$

1) si f y h son monomorfismos, entonces g es también un monomorfismo;

2) si f y h son epimorfismos, entonces g es también un epimorfismo.

En particular, si f y h son isomorfismos, g es también un isomorfismo. Esto lo he probado solo para el caso de $H' = H$, $K' = K$, $f = \mathrm{id}_H$, $h = \mathrm{id}_K$ para simplificar la notación. La versión general no nos va a servir.

10.3.9. Proposición. *Consideremos una sucesión exacta corta de grupos*

$$1 \to H \xrightarrow{i} G \xrightarrow{p} K \to 1$$

Las siguientes condiciones son equivalentes.

1) Existe un homomorfismo de grupos $r\colon G \to H$ tal que $r \circ i = \mathrm{id}_H$.

2) *Existe un isomorfismo* $f\colon G \xrightarrow{\cong} H \times K$ *que forma parte del diagrama conmutativo*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{p} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \cong\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \xrightarrow[h\mapsto(h,1)]{} & H\times K & \xrightarrow[(h,k)\mapsto k]{} & K & \longrightarrow & 1 \end{array} \tag{10.4}$$

Demostración. En la implicación 1) $\Rightarrow$ 2) el isomorfismo f viene dado por

$$\begin{aligned} f\colon G &\to H\times K,\\ g &\mapsto (r(g), p(g)). \end{aligned}$$

Es un homomorfismo, puesto que r y p son homomorfismos. Es fácil comprobar que $f\colon g \mapsto (r(g), p(g))$ hace conmutar el diagrama (10.4). En fin, el lema 10.3.7 implica que f es un isomorfismo.

Para probar 2) $\Rightarrow$ 1), notamos primero que la conmutatividad del segundo cuadrado significa que $f(g) = (h, p(g))$ para algún $h \in H$. Pongamos $r(g) = h$. Dado que f es un homomorfismo, r es también un homomorfismo $G \to H$. Luego, la conmutatividad del primer cuadrado significa que $r(i(h)) = h$ para todo $h \in H$. ■

10.3.10. Ejemplo. La sucesión exacta corta

$$0 \to \mathbb{Z}/3\mathbb{Z} \xrightarrow{i\colon [1]_3\mapsto[2]_6} \mathbb{Z}/6\mathbb{Z} \xrightarrow{[1]_6\mapsto[1]_2} \mathbb{Z}/2\mathbb{Z} \to 0$$

admite un homomorfismo $r\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ tal que $r \circ i = \mathrm{id}_{\mathbb{Z}/3\mathbb{Z}}$. Esta viene dada por $[1]_6 \mapsto [2]_3$. Esto nos da un isomorfismo $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. ▲

10.3.11. Ejemplo. Se ve que la sucesión exacta corta

$$0 \to \mathbb{Z} \xrightarrow{i\colon 1\mapsto n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

no admite un homomorfismo $r\colon \mathbb{Z} \to \mathbb{Z}$ tal que $r \circ i = \mathrm{id}_{\mathbb{Z}}$. Y de hecho, si tal aplicación existiera, tendríamos $\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ lo que es falso (a diferencia de $\mathbb{Z}$, el grupo $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tiene elementos no triviales de orden finito). ▲

10.3.12. Proposición. *Consideremos una sucesión exacta corta de grupos*

$$1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$$

Las siguientes condiciones son equivalentes.

1) *Existe un homomorfismo de grupos* $s\colon H \to G$ *tal que* $p \circ s = \mathrm{id}_H$.

2) *Existe un homomorfismo* $\phi\colon H \to \mathrm{Aut}(N)$ *y un isomorfismo* $f\colon N \rtimes_\phi N \xrightarrow{\cong} G$ *que hace parte del diagrama conmutativo*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{n\mapsto(n,1)} & N\rtimes_\phi H & \xrightarrow{(n,h)\mapsto h} & H & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \cong\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & N & \xrightarrow{i} & G & \xrightarrow{p} & H & \longrightarrow & 1 \end{array} \tag{10.5}$$

Cuando se cumplen estas condiciones, se dice que la sucesión exacta corta es ***escindida***[*].

Demostración. Para ver la implicación 1) ⇒ 2) notamos que H actúa sobre N por la conjugación en el siguiente sentido. Se puede identificar N con el subgrupo $i(N) \subseteq G$, que es normal, siendo el núcleo de p. Luego, dado que $p \circ s = \mathrm{id}_H$, se ve que $s\colon H \to G$ es un monomorfismo, y gracias a esto H se identifica con el subgrupo $s(H) \subseteq G$. Ya que $i(N)$ es normal, conjugando sus elementos por los elementos de $s(H)$, se obtienen elementos de $i(N)$.

La acción de $s(h) \in s(H)$ sobre $i(N)$ viene dada por

$$i(n) \mapsto s(h) \cdot i(n) \cdot s(h)^{-1} =: i(\phi_h(n)), \tag{10.6}$$

donde $\phi_h(n) \in N$. Esto define un homomorfismo

$$\begin{aligned} \phi\colon H &\to \mathrm{Aut}(N), \\ h &\mapsto \phi_h \end{aligned}$$

—el lector puede verificar todos los detalles usando la fórmula (10.6), pero salvo la identificación de N con $i(N)$ y H con $s(H)$, se trata de la acción habitual por la conjugación, y hemos comprobado en el capítulo anterior que en este caso la acción es por automorfismos. Ahora usando ϕ, podemos construir la suma semidirecta $N \rtimes_\phi H$, y luego considerar la aplicación

$$\begin{aligned} f\colon N \rtimes_\phi H &\to G, \\ (n,h) &\mapsto i(n) \cdot s(h). \end{aligned}$$

Esto es un homomorfismo: en G se cumple

$$\begin{aligned} i(n_1) \cdot s(h_1) \cdot i(n_2) \cdot s(h_2) &= i(n_1) \cdot s(h_1) \cdot i(n_2) \cdot s(h_1)^{-1} \cdot s(h_1) \cdot s(h_2) \\ &= i(n_1) \cdot i(\phi_{h_1}(n_2)) \cdot s(h_1 h_2) = i(n_1\, \phi_{h_1}(n_2)) \cdot s(h_1 h_2), \end{aligned}$$

lo que corresponde a la multiplicación en $N \rtimes_\phi H$. Se ve que el homomorfismo f que acabamos de definir hace conmutar el diagrama (10.5), y el lema 10.3.7 nos dice que f es necesariamente un isomorfismo.

Para probar 2) ⇒ 1), definamos $s(h) := f(1,h)$. Esto es un homomorfismo $s\colon H \to G$, dado que f lo es. Luego, de la conmutatividad del segundo cuadrado se sigue que $p \circ s(h) = p \circ f(1,h) = h$ para todo $h \in H$. ■

10.3.13. Ejemplo. Tenemos una sucesión exacta corta

$$1 \to \langle r \rangle \to D_n \xrightarrow{p} \langle f \rangle \to 1$$

Donde el subgrupo $\langle f \rangle = \{\mathrm{id}, f\}$ se identifica con el grupo cociente $D_n / \langle r \rangle$. La inclusión de subgrupo $s\colon \langle f \rangle \rightarrowtail D_n$ satisface $p \circ s = \mathrm{id}$. ▲

[*] "split" en inglés.

10.3.14. Ejemplo. Tenemos una sucesión exacta corta

$$1 \to \mathrm{SL}_n(k) \to \mathrm{GL}_n(k) \xrightarrow{\det} k^\times \to 1$$

Luego, hay un homomorfismo

$$\begin{aligned} k^\times &\to \mathrm{GL}_n(k), \\ x &\mapsto \begin{pmatrix} x & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \end{aligned}$$

y el determiante de la última matriz es igual a x. ▲

Notamos que cuando el grupo G que está en el medio es abeliano (y por ende N y H, siendo su subgrupo y grupo cociente), la fórmula (10.6) que define a ϕ_h implica que $\phi_h(n) = n$ para cualesquiera $h \in H$ y $n \in N$. Esto nos lleva al siguiente resultado.

10.3.15. Corolario. *Consideremos una sucesión exacta corta de grupos abelianos*

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

Las siguientes condiciones son equivalentes.

1) *Existe un homomorfismo de grupos $r\colon B \to A$ tal que $r \circ i = \mathrm{id}_A$.*
2) *Existe un homomorfismo de grupos $s\colon C \to B$ tal que $p \circ s = \mathrm{id}_C$.*
3) *Existe un isomorfismo $f\colon B \xrightarrow{\cong} A \times C$ que forma parte del diagrama conmutativo*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \cong} f & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A & \xrightarrow[a\mapsto(a,0)]{} & A \times C & \xrightarrow[(a,c)\mapsto c]{} & C & \longrightarrow & 0 \end{array}$$

10.3.16. Digresión. Se puede definir una equivalencia de extensiones de grupos

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0 \quad \text{y} \quad 0 \to A \xrightarrow{i'} B' \xrightarrow{p'} C \to 0$$

como un homomorfismo $B \to B'$ que hace conmutar el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A & \xrightarrow{i'} & B' & \xrightarrow{p'} & C & \longrightarrow & 0 \end{array}$$

Como sabemos, en este caso $B \to B'$ es automáticamente un isomorfismo, y en particular se ve que se trata de una relación de equivalencia sobre las extensiones de C por A.

Cuando se trata de grupos abelianos, las extensiones módulo esta equivalencia también forman un grupo abeliano que se denota por $\mathrm{Ext}(C, A)$ y se denomina el **grupo de extensiones** de C por A. El elemento nulo de este grupo corresponde a la clase de equivalencia de la sucesión exacta escindida

$$0 \to A \xrightarrow{a \mapsto (a,0)} A \times C \xrightarrow{(a,c) \mapsto c} C \to 0$$

El cálculo de los grupos $\mathrm{Ext}(C, A)$ pertenece a la rama de las matemáticas conocida como **álgebra homológica**.

10.4 Grupos abelianos finitamente generados

Recordemos que un grupo abeliano (aditivo) A es **finitamente generado** si existe una colección finita $x_1, \ldots, x_k \in A$ de generadores:

$$A = \langle x_1, \ldots, x_k \rangle = \Big\{ \sum_{1 \le i \le k} n_i x_i \;\Big|\; n_i \in \mathbb{Z} \Big\}.$$

10.4.1. Definición. Digamos que $x_1, \ldots, x_k$ es una **base** de A si $A = \langle x_1, \ldots, x_k \rangle$ y

$$n_1 x_1 + \cdots + n_k x_k = 0,$$

para algunos $n_i \in \mathbb{Z}$, entonces $n_i x_i = 0$ para todo i.

10.4.2. Comentario. Esta condición es más débil que tener $n_i = 0$ para todo i. La última sería la definición correcta de una base, pero para esta sección vamos a usar la definición provisional de arriba.

10.4.3. Observación. *Si $x_1, \ldots, x_k$ es una base de A, entonces*

$$A \cong \langle x_1 \rangle \times \cdots \times \langle x_k \rangle.$$

Demostración. Consideremos el homomorfismo

$$\begin{aligned} \langle x_1 \rangle \times \cdots \times \langle x_k \rangle &\to A, \\ (n_1 x_1, \ldots, n_k x_k) &\mapsto \sum_{1 \le i \le k} n_i x_i. \end{aligned}$$

Es sobreyectivo, dado que $x_1, \ldots, x_k$ son generadores de A. Luego, es inyectivo por la definición de la base:

$$\sum_{1 \le i \le k} n_i x_i - \sum_{1 \le i \le k} n_i' x_i \iff \sum_{1 \le i \le k} (n_i - n_i')\, x_i = 0 \iff n_i x_i = n_i' x_i \text{ para todo } i.$$

■

10.4.4. Proposición. *Todo grupo abeliano finitamente generado posee una base y por lo tanto es isomorfso a un producto directo de grupos cíclicos.*

Para la prueba, vamos a usar el siguiente resultado auxiliar.

10.4.5. Lema. *Supongamos que $x_1, \dots, x_k$ son generadores de A. Entonces para cualesquiera $c_1, \dots, c_k \in \mathbb{N}$ tales que $\operatorname{mcd}(c_1, \dots, c_k) = 1$ existen generadores $y_1, \dots, y_k$ de A tales que*

$$y_1 = c_1 x_1 + \cdots + c_k x_k.$$

Demostración. Usemos inducción sobre $c := c_1 + \cdots + c_k$. La base de inducción es $c = 1$. En este caso, sin pérdida de generalidad, $c_1 = 1$ y $c_2 = \cdots = c_k = 0$, así que podemos tomar $y_i = x_i$.

Ahora si $c > 1$, entonces existen dos c_i que no son nulos. Sin pérdida de generalidad, $c_1 \geq c_2 > 0$. Notamos que

1) $A = \langle x_1, x_1 + x_2, x_3, \dots, x_k \rangle$,

2) $\operatorname{mcd}(c_1 - c_2, c_2, c_3, \dots, c_k) = 1$,

3) $(c_1 - c_2) + c_2 + c_3 + \cdots + c_k < c$.

Luego, por la hipótesis de inducción, existen generadores $y_1, \dots, y_k$ tales que

$$y_1 = (c_1 - c_2)\, x_1 + c_2\, (x_1 + x_2) + c_3 x_3 + \cdots + c_k x_k = c_1 x_1 + \cdots + c_k x_k.$$

■

Demostración de 10.4.4. Usemos inducción sobre el número de generadores de A. La base es el caso cuando A puede ser generado por un elemento y es cíclico.

Supongamos que A puede ser generado por $k > 1$ elementos. Escojamos generadores $x_1, \dots, x_k$ donde $\operatorname{ord} x_1$ es el mínimo posible. Vamos a probar que $A \cong \langle x_1 \rangle \times \langle x_2, \dots, x_k \rangle$. Supongamos que

$$A \ncong \langle x_1 \rangle \times \langle x_2, \dots, x_k \rangle.$$

Esto significa que $\langle x_1 \rangle \cap \langle x_2, \dots, x_k \rangle \neq \{0\}$ y que existe una relación

$$n_1 x_1 + n_2 x_2 + \cdots + n_k x_k = 0$$

donde $n_1 x_1 \neq 0$. Reemplazando x_i por $-x_i$ si necesario, podemos suponer que $n_i \geq 0$. Además, sin pérdida de generalidad, $n_1 < \operatorname{ord} x_1$. Consideremos

$$d := \operatorname{mcd}(n_1, \dots, n_k) > 0, \quad c_i := n_i / d.$$

Luego, $\operatorname{mcd}(c_1, \dots, c_k) = 1$ y por el lema de arriba existen generadores $y_1, \dots, y_k$ tales que $y_1 = c_1 x_1 + \cdots + c_k x_k$; es decir,

$$d y_1 = n_1 x_1 + \cdots + n_k x_k = 0.$$

Esto significa que

$$\operatorname{ord} y_1 \leq d \leq n_1 < \operatorname{ord} x_1.$$

Esto contradice nuestra elección de $x_1, \dots, x_k$.

Entonces,

$$A \cong \langle x_1 \rangle \times \langle x_2, \dots, x_k \rangle.$$

Procediendo por inducción de esta manera, podemos descomponer $\langle x_2, \dots, x_k \rangle$ en un producto directo de grupos cíclicos. ■

10.4.6. Comentario. Hay muchas pruebas diferentes de 10.4.4. El argumento de arriba tiene ventaja de ser muy breve, pero no es constructivo. La fuente que seguí son los apuntes de J.S. Milne sobre la teoría de grupos: http://jmilne.org/math/CourseNotes/gt.html

Podemos formular un resultado más preciso.

10.4.7. Teorema. *Todo grupo abeliano finitamente generado no nulo A es isomorfo a un producto directo de grupos cíclicos*

$$\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}.$$

*El número r está bien definido y se llama el **rango** de A. Los números $p_i^{k_i}$ son potencias de números primos (no necesariamente distintos) y también están definidos de modo único para A.*

Demostración. Según 10.4.4, todo grupo abeliano finitamente generado es un producto directo de grupos cíclicos. Cada uno de los factores cíclicos finitos es isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Tomando la factorización en números primos $n = p_1^{k_1} \cdots p_s^{k_s}$ y aplicando el teorema chino del resto, se obtiene

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z}.$$

Esto establece la existencia de isomorfismo

$$A \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r} \tag{10.7}$$

para todo grupo abeliano finitamente generado A. Nos falta ver que los números r y $p_i^{k_i}$ están bien definidos.

Sería útil separar la parte finita $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z}$ de la parte infinita $\underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}$.

Para esto podemos considerar el **subgrupo de torsión**

$$A_{tors} := \{a \in A \mid n \cdot a = 0 \text{ para algún } n = 1, 2, 3, \ldots\}.$$

Tenemos

$$A_{tors} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z}, \quad A_{tf} := A/A_{tors} \cong \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}$$

("tf" significa "torsion free", "libre de torsión"). Ahora sea p cualquier número primo. Consideremos el grupo

$$pA_{tf} := \{p \cdot a \mid a \in A_{tf}\} \subset A_{tf}.$$

El grupo cociente

$$A_{tf}/pA_{tf} \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}}_{r} = \underbrace{\mathbb{F}_p \times \cdots \times \mathbb{F}_p}_{r}$$

es un espacio vectorial sobre $\mathbb{F}_p$ y

$$\dim_{\mathbb{F}_q}(A_{tf}/pA_{tf}) = r.$$

Entonces, r no depende de un isomorfismo particular (10.7), sino es un invariante de A.

Para ver la unicidad de los números $p_i^{k_i}$, podemos analizar por separado cada primo. A saber, para cada primo p consideremos el **subgrupo de p-torsión**

$$A[p^\infty] := \{a \in A \mid p^n \cdot a = 0 \text{ para algún } n = 0, 1, 2, 3, \ldots\}.$$

Será suficiente ver que en

$$A[p^\infty] \cong \mathbb{Z}/p^{\ell_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\ell_t}\mathbb{Z}$$

los números p^{ℓ_i} están bien definidos. Procedamos por inducción sobre $\ell = \ell_1 + \cdots + \ell_t$. Si $\ell = 1$, entonces $A[p^\infty] \cong \mathbb{Z}/p\mathbb{Z}$. Para el paso inductivo, podemos considerar el subgrupo $pA[p^\infty] \subset A[p^\infty]$. Luego,

$$A[p^\infty]/pA[p^\infty] \cong \mathbb{Z}/p^{\ell_1-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\ell_t-1}\mathbb{Z}.$$

Por la hipótesis de inducción, los números $\ell_i - 1$ están bien definidos. La única excepción son los factores $\mathbb{Z}/p\mathbb{Z}$ que corresponden a $\ell_i = 1$ que van a desaparecer. El número de estos factores puede ser recuperado de la relación $\sum_i \ell_i = \ell$. ■

10.4.8. Corolario. *Todo subgrupo de un grupo abeliano finitamente generado es finitamente generado.*

Para grupos no abelianos, el último resultado no se cumple. Un grupo no abeliano finitamente generado puede tener subgrupos que no son finitamente generados.

10.4.9. Ejemplo. Hay tres grupos abelianos no isomorfos de orden 8:

$$\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Para encontrar los grupos abelianos de orden 100, podemos factorizar $100 = 2^2 \cdot 5^2$. Entonces, tenemos

$$\mathbb{Z}/100\mathbb{Z} \cong \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

▲

10.4.10. Comentario. En la expresión

$$A \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}$$

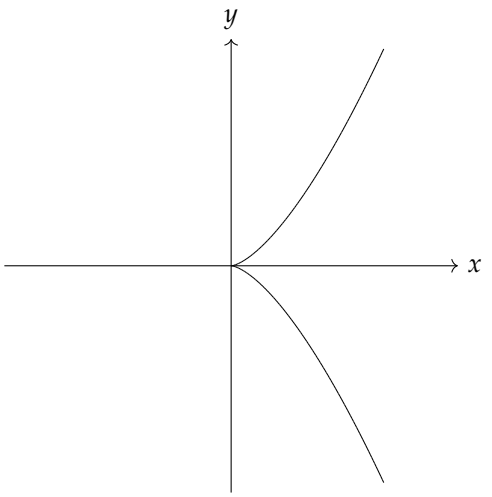
los números $p_i^{k_i}$ y r están bien definidos, pero el mismo isomorfismo depende de una base particular y por lo tanto no es canónico en ningún sentido.

10.5 Perspectiva: el grupo de Mordell–Weil

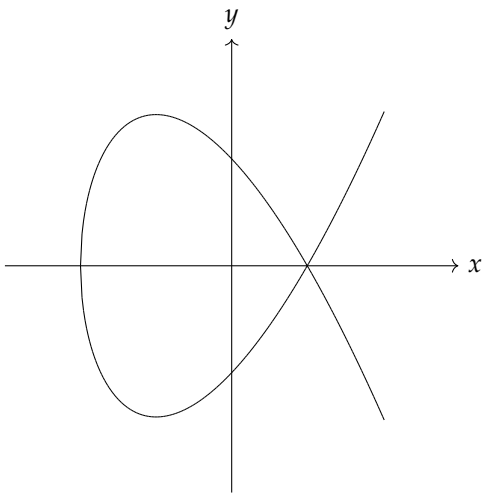
Finalizamos nuestra discusión de grupos abelianos finitamente generados con un ejemplo muy importante y no trivial. Sea E la curva plana definida por una ecuación cúbica

$$y^2 = x^3 + A\,x + B,$$

donde A y B son algunos coeficientes racionales. Esta curva puede tener una **cúspide** o un **nodo** como las curvas en el dibujo de abajo; en este caso se dice que E es **singular**.



cúbica singular $y^2 = x^3$

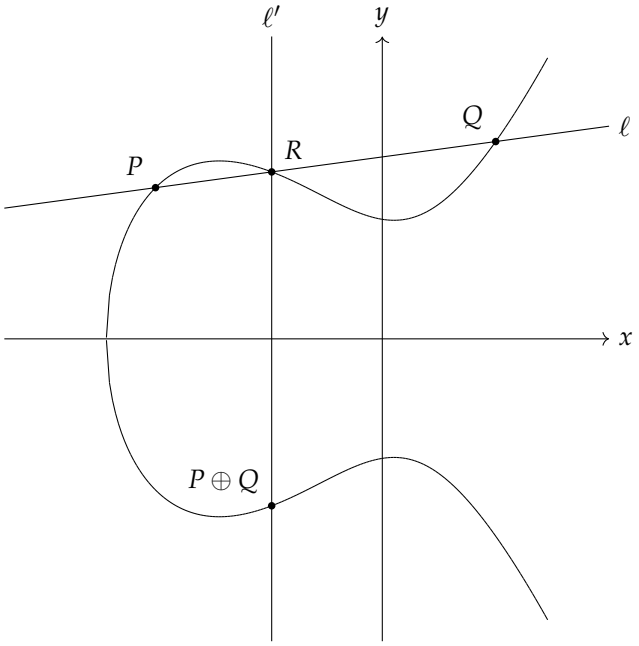


cúbica singular $y^2 = x^3 - 3x + 2$

La curva no será singular precisamente cuando

$$4\,A^3 + 27\,B^2 \neq 0.$$

En este caso se dice que E es una **curva elíptica**. Sobre los puntos de E se puede definir la siguiente operación. Para dos puntos $P, Q \in E$, sea ℓ la recta que pasa por P y Q (si $P = Q$, se considera la tangente que pasa por P) y sea R el tercer punto de intersección de ℓ con E. Sea ℓ' la recta vertical que pasa por R. Entonces, el punto $P \oplus Q$ es el otro punto de intersección de E con ℓ'.



Un caso excepcional es cuando $P = (x, y)$ y $Q = (x, -y)$. En este caso se dice que el tercer punto de intersección "está al infinito" y se escribe $P \oplus Q = O$. Aquí O es un punto que se añade al plano afín; para este punto se define

$$P \oplus O = O \oplus P = P$$

para todo P. En el resto de casos, las coordenadas del tercer punto de intersección R pueden ser calculadas directamente.

1. Si $P = (x_P, y_P)$ y $Q = (x_Q, y_Q)$ donde $x_P \neq x_Q$, entonces se puede calcular que el tercer punto de intersección $R = (x_R, y_R)$ tiene coordenadas

$$x_R = \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_P - x_Q, \quad y_R = \frac{y_P - y_Q}{x_P - x_Q}\,(x_R - x_Q) + y_Q.$$

2. Si $P = Q = (x_P, y_P)$, entonces

$$x_R = \frac{(3\,x_P^2 + A)^2}{4\,y_P^2} - 2\,x_P, \quad y_R = \frac{3\,x_P^2 + A}{2\,y_P}\,(x_R - x_P) + y_P.$$

10.5.1. Teorema. *Sea E una curva elíptica definida por la ecuación*

$$y^2 = x^3 + A\,x + B,$$

donde $4\,A^3 + 27\,B^2 \neq 0$. Denotemos por $E(\mathbb{Q})$ los puntos con coordenadas racionales que están en la curva, junto con el punto O:

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + A\,x + B\} \cup \{O\}.$$

Este se llama el ***grupo de Mordell–Weil*** *de la curva elíptica E.*

Entonces, $E(\mathbb{Q})$ es un grupo abeliano respecto a la operación $\oplus$.

Bosquejo de demostración. De las fórmulas de arriba se ve que si P y Q tienen coordenadas racionales, entonces $P \oplus Q$ también tiene coordenadas racionales.

Por la definición, O es el elemento neutro. El elemento opuesto a $P = (x_P, y_P)$ es $-P = (x_P, -y_P)$. La operación es simétrica en P y Q, así que $P \oplus Q = Q \oplus P$ para cualesquiera $P, Q \in E(\mathbb{Q})$.

La única cosa que no está clara es la asociatividad: $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$. La única prueba comprensible y convincente usa geometría algebraica y la omitiré. ■

Un teorema clásico de Siegel dice que una curva elíptica tiene un número finito de puntos enteros. El número de puntos racionales puede ser infinito. Sin embargo, tenemos el siguiente resultado, conocido como el **teorema de Mordell–Weil**[*].

10.5.2. Teorema. *El grupo $E(\mathbb{Q})$ es finitamente generado.*

Esto significa que

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{tors},$$

donde r es un número natural, llamado el **rango** de la curva elíptica, y $E(\mathbb{Q})_{tors}$ es algún grupo finito. En otras palabras, existen algunos puntos

$$P_1, \ldots, P_r, Q_1, \ldots, Q_s$$

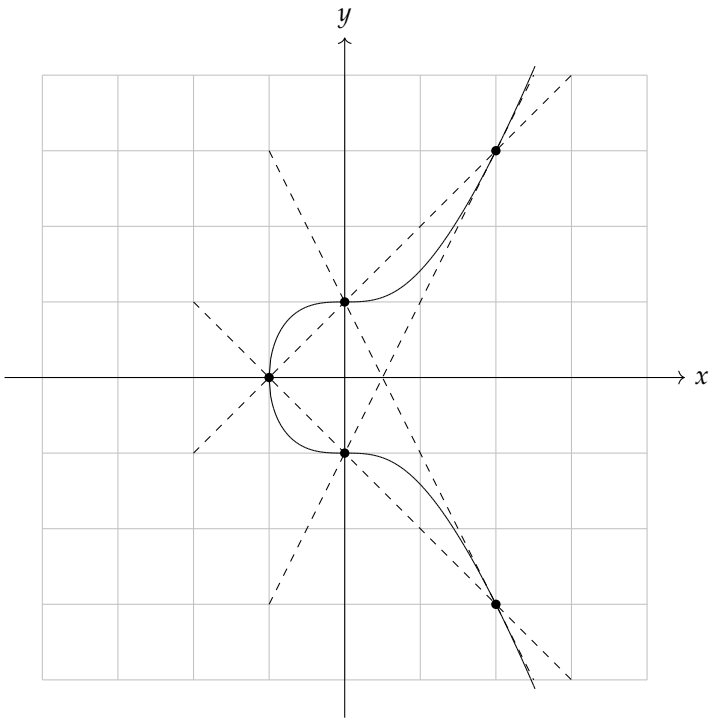
tales que todos los puntos racionales de la curva pueden ser obtenidas a partir de estas usando la operación $\oplus$.

10.5.3. Ejemplo. Para la curva $y^2 = x^3 + 1$ podemos calcular que el punto $(2, 3)$ es de orden 6:

$$2 \cdot (2,3) = (0,1),\ 3 \cdot (2,3) = (-1,0),\ 4 \cdot (2,3) = (0,-1),\ 5 \cdot (2,3) = (2,-3),\ 6 \cdot (2,3) = O.$$

Todo esto se ve del dibujo de abajo. Note que $(0, \pm 1)$ son puntos de inflexión.

[*] Louis J. Mordell (1888–1972) probó el resultado en 1922 y André Weil (1906–1998) obtuvo una generalización en 1928.



curva elíptica $y^2 = x^3 + 1$

De hecho, no hay otros puntos racionales y el grupo $E(\mathbb{Q})$ es cíclico de orden 6. ▲

10.5.4. Ejemplo. Resulta que para la curva $y^2 = x^3 - 4x + 4$ el grupo $E(\mathbb{Q})$ es isomorfo a $\mathbb{Z}$. Su generador es $P = (2, -2)$. Tenemos, por ejemplo

$$2 \cdot P = (0, -2), \quad 3 \cdot P = (-2, 2), \quad 4 \cdot P = (1, 1), \quad 5 \cdot P = (6, 14), \quad 6 \cdot P = (8, -22).$$

▲

En 1978 el matemático estadounidense Barry Mazur demostró que el subgrupo $E(\mathbb{Q})_{tors}$ es isomorfo a uno de los siguientes grupos:

$$\mathbb{Z}/n\mathbb{Z}, \text{ donde } n = 1, 2, 3, \ldots, 9, 10, 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \text{ donde } m = 2, 4, 6, 8,$$

y además, cada uno de los grupos mencionados surge como el subgrupo de torsión de alguna curva elíptica.

El número r es más misterioso. Una curva elíptica aleatoria suele tener rango 0 o 1. Una conjetura dice que r puede ser arbitrariamente grande, pero es muy difícil construir ejemplos particulares. El último récord pertenece al matemático estadounidense Noam Elkies: es una curva de rango ≥ 28.

Aparte del interés teórico, el grupo abeliano $E(\mathbb{Q})$ tiene aplicaciones en criptografía.

10.6 Ejercicios

Ejercicio 10.1. *Enumere todos los grupos abelianos de orden* 666 *salvo isomorfismo.*

Ejercicio 10.2. *Sea $n \geq 3$ un número natural impar. Consideremos el grupo diédrico*

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

(las simetrías del $2n$-ágono regular) y sus subgrupos $H := \langle r^2, f\rangle$ y $K := \{1, r^n\}$.

1) *Demuestre que $H \cong D_n$ y $K \cong \mathbb{Z}/2\mathbb{Z}$.*

2) *Demuestre que $D_{2n} \cong H \times K$.*

3) *Si n es par, demuestre que $D_{2n} \ncong D_n \times \mathbb{Z}/2\mathbb{Z}$.*

Ejercicio 10.3. *Demuestre que la sucesión*

$$0 \to \mathbb{Z} \xrightarrow{n\mapsto(n,-n)} \mathbb{Z}[1/p] \times \mathbb{Z}_{(p)} \xrightarrow{(x,y)\mapsto x+y} \mathbb{Q} \to 0$$

es exacta. Aquí $\mathbb{Z}[1/p]$ es el subgrupo de $\mathbb{Q}$ formado por las fracciones con potencias de p en el denominador y $\mathbb{Z}_{(p)}$ es el subgrupo de fracciones con el denominador no divisible por p.

Ejercicio 10.4. *Demuestre que si $\mathbb{Q} \cong A \times B$ para algunos grupos abelianos A y B, entonces $A = 0$ o $B = 0$.*

Sugerencia: supongamos que A y B son subgrupos no triviales de $\mathbb{Q}$. Demuestre que $A \cap B \neq \{0\}$.

Ejercicio 10.5. *Demuestre que $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Z}[1/p]/\mathbb{Z} \times \mathbb{Z}_{(p)}/\mathbb{Z}$.*

Ejercicio 10.6. *Consideremos el grupo alternante A_4 y sus subgrupos*

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

y $H := \langle(1\,2\,3)\rangle$. Demuestre que A_4 es el producto semidirecto de V y H.

Ejercicio 10.7. *Demuestre que para $n \geq 5$ el grupo alternante A_n no puede ser isomorfo a un producto semidirecto $N \rtimes_\phi H$ donde N y H no son triviales.*

Ejercicio 10.8. *Sea* $\mathrm{Isom}(\mathbb{R}^2)$ *el grupo de isometrías del plano euclidiano. Demuestre que*

$$\mathrm{Isom}(\mathbb{R}^2) \cong \mathbb{R}^2 \rtimes_\phi O_2(\mathbb{R}),$$

donde $\mathbb{R}^2$ es el grupo aditivo $\mathbb{R} \times \mathbb{R}$ y el homomorfismo

$$\phi\colon O_2(\mathbb{R}) \to \mathrm{Aut}(\mathbb{R}^2)$$

viene dado por la multiplicación de vectores $\binom{x}{y} \in \mathbb{R}^2$ por matrices $A \in O_2(\mathbb{R})$:

$$\phi_A \binom{x}{y} := A \cdot \binom{x}{y}.$$

Ejercicio 10.9. *Demuestre que* $O_n(\mathbb{R}) \cong SO_n(\mathbb{R}) \rtimes_\phi \{\pm 1\}$ *para algún homomorfismo* $\phi\colon \{\pm 1\} \to \mathrm{Aut}(SO_n(\mathbb{R}))$. *Indicación: demuestre que la sucesión exacta corta*

$$1 \to SO_n(\mathbb{R}) \xrightarrow{i} O_n(\mathbb{R}) \xrightarrow{p} \{\pm 1\} \to 1$$

(donde i *es la inclusión de subgrupo y* p *es la proyección sobre el grupo cociente) admite un homomorfismo* $s\colon \{\pm 1\} \to O_n(\mathbb{R})$ *tal que* $i \circ s = \mathrm{id}$.

Ejercicio 10.10. *Encuentre todas las posibles extensiones de* $\mathbb{Z}/2\mathbb{Z}$ *por* $\mathbb{Z}/2\mathbb{Z}$

$$0 \to \mathbb{Z}/2\mathbb{Z} \to A \to \mathbb{Z}/2\mathbb{Z} \to 0$$

salvo isomorfismo.

Ejercicio 10.11. *Demuestre que toda sucesión exacta corta de grupos abelianos*

$$0 \to A \to B \to \mathbb{Z} \to 0$$

es equivalente a la extensión

$$0 \to A \xrightarrow{a \mapsto (a,0)} A \times \mathbb{Z} \xrightarrow{(a,n) \mapsto n} \mathbb{Z} \to 0$$

Indicación: demuestre que todo epimorsifmo $p\colon B \twoheadrightarrow \mathbb{Z}$ *admite un homomorfismo* $s\colon \mathbb{Z} \to B$ *tal que* $p \circ s = \mathrm{id}_{\mathbb{Z}}$.

Ejercicio 10.12. *Sea* A *un grupo abeliano que satisface la siguiente propiedad: todo monomorfismo de grupos abelianos* $i\colon A \rightarrowtail B$ *admite un homomorfismo* $r\colon B \to A$ *tal que* $r \circ i = \mathrm{id}_A$. *En este ejercicio vamos a demostrar que* A *es divisible.*

Sea $n = 1, 2, 3, \ldots$ *y* $a \in A$.

1) *Demuestre que* $C := \{m \cdot a, -mn) \mid m \in \mathbb{Z}\}$ *es un subgrupo de* $A \times \mathbb{Z}$.

2) *Consideremos el grupo cociente* $(A \times \mathbb{Z})/C$ *y el homomorfismo*

$$\begin{aligned} i\colon A &\to (A \times \mathbb{Z})/C, \\ x &\mapsto (x, 0) + C \end{aligned}$$

(esto es la composición de la inclusión de A *como un subgrupo* $A \times 0 \subset A \times \mathbb{Z}$ *con la proyección sobre el grupo cociente). Demuestre que* i *es un monomorfismo.*

3) *Demuestre que*

$$i(a) = (0, n) + C = n \cdot ((0, 1) + C) \quad \text{en } (A \times \mathbb{Z})/C.$$

4) *Por la hipótesis sobre* A, *existe un homomorfismo* $r\colon (A \times \mathbb{Z})/C \to A$ *tal que* $r \circ i = \mathrm{id}_A$. *Usando esto, encuentre un elemento* $b \in A$ *tal que* $a = n \cdot b$. *Concluya que* A *es divisible.*

Ejercicio 10.13. *Recordemos que dos sucesiones exactas cortas (extensiones de grupos)*

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0 \quad y \quad 0 \to A \xrightarrow{i'} B' \xrightarrow{p'} C \to 0$$

son ***equivalentes*** *si existe un homomorfismo $f\colon B \to B'$ tal que el diagrama*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & A & \xrightarrow{i'} & B' & \xrightarrow{p'} & C & \longrightarrow & 1 \end{array}$$

es conmutativo (hemos probado que en este caso f es un isomorfismo).

Sea p un número primo. Consideremos una sucesión de homomorfismos

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{[1]_p \mapsto [p]_{p^2}} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{[1]_{p^2} \mapsto [n]_p} \mathbb{Z}/p\mathbb{Z} \to 0$$

1) *Demuestre que para todo $n = 1, 2, \ldots, p-1$ es una sucesión exacta corta.*

2) *Demuestre que estas sucesiones no son equivalentes para diferentes $n = 1, 2, \ldots, p-1$.*

Ejercicio 10.14. *Sea*

$$1 \to H \to G \to K \to 1$$

una sucesión exacta corta de grupos finitos. Demuestre que $|G| = |H| \cdot |K|$.

Ejercicio 10.15. *Se dice que una sucesión de homomorfismos*

$$1 \xrightarrow{f_n} G_{n-1} \xrightarrow{f_{n-1}} G_{n-2} \xrightarrow{f_{n-2}} G_{n-3} \to \cdots \to G_1 \xrightarrow{f_1} G_0 \xrightarrow{f_0} 1$$

es ***exacta*** *si $\operatorname{im} f_i = \ker f_{i-1}$ para todo $i = 1, \ldots, n$. Es una generalización de la noción de sucesión exacta corta*

$$1 \xrightarrow{f_3} G_2 \xrightarrow{f_2} G_1 \xrightarrow{f_1} G_0 \xrightarrow{f_0} 1$$

Demuestre que para una sucesión exacta de grupos finitos se cumple

$$\prod_{0 \le i \le n-1} |G_i|^{(-1)^i} = 1.$$

Esto generaliza la fórmula del ejercicio precedente.

Parte III
Teoría de anillos

Capítulo 11
Anillos

Ya introducimos anillos y cuerpos en el capítulo 3. Ahora vamos a estudiar otros conceptos relacionados y ver más detalles. Recordemos del capítulo 3 que 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 aditivo $0 \in R$ (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**. Al estudio de algunas propiedades especiales de anillos conmutativos estará dedicado el siguiente capítulo.

Advertencia para el lector: algunos libros de texto consideran anillos sin identidad (anillos que no satisfacen el axioma R4)), pero en este curso la palabra "anillo" siempre significa "anillo con identidad".

Recordemos algunos ejemplos de anillos que hemos visto.

1) Los números enteros $\mathbb{Z}$, racionales $\mathbb{Q}$, reales $\mathbb{R}$, complejos $\mathbb{C}$. Los últimos tres son **cuerpos**.

2) Para $n = 1, 2, 3, \ldots$ y para p un número primo los conjuntos

$$\mathbb{Z}\Big[\frac{1}{n}\Big] := \Big\{ \frac{a}{n^k} \in \mathbb{Q} \;\Big|\; a \in \mathbb{Z},\ k = 0, 1, 2, \ldots \Big\}, \quad \mathbb{Z}_{(p)} := \Big\{ \frac{a}{b} \in \mathbb{Q} \;\Big|\; p \nmid b \Big\}$$

son anillos. Esto es un ejemplo de **localización** que vamos a estudiar más adelante en el curso.

3) El anillo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo n. Cuando $n = p$ es primo, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ es un **cuerpo**.

4) Los anillos aritméticos como los **enteros de Gauss**

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

los **enteros de Eisenstein**

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

(donde $\zeta_3 := e^{2\pi\sqrt{-1}/3}$) y el anillo

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

5) El anillo de polinomios $R[X]$, donde R es un anillo conmutativo.

Esta construcción puede ser generalizada al **anillo de polinomios en n variables** $R[X_1, \ldots, X_n]$. En este caso los elementos son las expresiones formales de la forma

$$f = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n},$$

donde $a_{i_1, \ldots, i_n} = 0$, salvo un número finito de $(i_1, \ldots, i_n)$. Las sumas y productos están definidos por

$$\left(\sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n} \right) + \left(\sum_{i_1, \ldots, i_n \geq 0} b_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n} \right) := \sum_{i_1, \ldots, i_n \geq 0} (a_{i_1, \ldots, i_n} + b_{i_1, \ldots, i_n})\, X_1^{i_1} \cdots X_n^{i_n}$$

y

$$\left(\sum_{i_1,\ldots,i_n\geq 0} a_{i_1,\ldots,i_n} X_1^{i_1}\cdots X_n^{i_n}\right)\cdot\left(\sum_{j_1,\ldots,j_n\geq 0} b_{j_1,\ldots,j_n} X_1^{j_1}\cdots X_n^{j_n}\right)$$
$$:=\sum_{k_1,\ldots,k_n\geq 0}\left(\sum_{\substack{(k_1,\ldots,k_n)=\\(i_1,\ldots,i_n)+(j_1,\ldots,j_n)}} a_{i_1,\ldots,i_n}\, b_{j_1,\ldots,j_n}\right) X_1^{k_1}\cdots X_n^{k_n}.$$

6) Si quitamos la condición que $a_{i_1,\ldots,i_n}=0$, salvo un número finito de $(i_1,\ldots,i_n)$, se obtiene el **anillo de las series formales de potencias en** n **variables** $R[\![X_1,\ldots,X_n]\!]$.

7) Los anillos de matrices $M_n(R)$, donde R es un anillo conmutativo.

Todos los anillos de arriba son conmutativos, salvo el anillo de matrices $M_n(R)$ para $n>1$.

11.1 Subanillos

11.1.1. Definición. Sea R un anillo. Se dice que un subconjunto $S\subseteq R$ es un **subanillo** de R si

1) S es un subgrupo abeliano de R respecto a la adición,

2) $1\in S$,

3) S es cerrado respecto a la multiplicación: $xy\in S$ para cualesquiera $x,y\in S$.

El lector puede comprobar que en este caso S es también un anillo respecto a las mismas operaciones que R.

11.1.2. Ejemplo. Sea R un anillo conmutativo. Identificándolo con los polinomios constantes

$$\sum_{i_1,\ldots,i_n\geq 0} a_{i_1,\ldots,i_n} X_1^{i_1}\cdots X_n^{i_n},\quad a_{i_1,\ldots,i_n}=0 \text{ para } (i_1,\ldots,i_n)\neq(0,\ldots,0),$$

podemos decir que R es un subanillo de $R[X_1,\ldots,X_n]$. De la misma manera, por la definición, los polinomios forman un subanillo de $R[\![X_1,\ldots,X_n]\!]$.

$$R\subset R[X_1,\ldots,X_n]\subset R[\![X_1,\ldots,X_n]\!].$$

▲

11.1.3. Ejemplo. Tenemos una cadena de subanillos

$$\mathbb{Z}\subset\mathbb{Z}[\sqrt{5}]\subset\mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big]\subset\mathbb{R}\subset\mathbb{C},$$

donde

$$\mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}, \quad \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big] := \Big\{a + b\,\frac{1+\sqrt{5}}{2} \;\Big|\; a, b \in \mathbb{Z}\Big\}.$$

▲

11.1.4. Ejemplo. Para $n = 1, 2, 3, \ldots$ y para p un número primo los conjuntos

$$\mathbb{Z}\Big[\frac{1}{n}\Big] := \Big\{\frac{a}{n^k} \in \mathbb{Q} \;\Big|\; a \in \mathbb{Z},\ k = 0, 1, 2, \ldots\Big\}, \quad \mathbb{Z}_{(p)} := \Big\{\frac{a}{b} \in \mathbb{Q} \;\Big|\; a, b \in \mathbb{Z},\ p \nmid b\Big\}$$

son subanillos de $\mathbb{Q}$. ▲

11.1.5. Ejemplo. Consideremos el anillo de las aplicaciones $f\colon \mathbb{R} \to \mathbb{R}$ respecto a las operaciones **punto por punto**

$$(f + g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

Las aplicaciones continuas $\mathbb{R} \to \mathbb{R}$ forman un subanillo. ▲

11.1.6. Ejemplo. Para un anillo R consideremos el subconjunto de los elementos que conmutan con todos los elementos:

$$Z(R) := \{x \in R \mid xy = yx \text{ para todo } y \in R\}.$$

Es un subanillo de R, llamado el **centro**. Notamos que R es conmutativo si y solamente si $R = Z(R)$. ▲

11.1.7. Ejemplo. $\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$ no tienen subanillos propios. En efecto, si $R \subseteq \mathbb{Z}$ es un subanillo, entonces $1 \in R$, y el mínimo subgrupo abeliano de $\mathbb{Z}$ que contiene a 1 es todo $\mathbb{Z}$. De la misma manera, para un subanillo $R \subseteq \mathbb{Z}/n\mathbb{Z}$ tenemos necesariamente $[1]_n \in R$, pero para todo $a = 1, 2, 3, 4, \ldots$ se cumple

$$[a]_n = \underbrace{[1]_n + \cdots + [1]_n}_{n}.$$

▲

11.1.8. Observación. *Sea R un anillo. Si $R_i \subseteq R$ son subanillos, entonces $\bigcap_i R_i$ es un subanillo.*

11.2 Homomorfismos de anillos

Un homomorfismo de anillos es una aplicación que preserva las operaciones de adición y multiplicación. Ya que no todos los elementos de R son invertibles, de la identidad $f(xy) = f(x)\,f(y)$ en general no se puede deducir que $f(1_R) = 1_S$. La última condición hace parte de la definición de homomorfismo de anillos.

11.2.1. Definición. Sean R y S anillos. Se dice que una aplicación $f\colon R \to S$ es un **homomorfismo** si se cumplen las siguientes condiciones:

1) f es un homomorfismo de grupos abelianos respecto a la adición; es decir, $f(x+y) = f(x)+f(y)$ para cualesquiera $x, y \in R$;

2) f preserva la identidad: $f(1_R) = 1_S$;

3) f preserva la multiplicación: $f(xy) = f(x)\,f(y)$ para cualesquiera $x, y \in R$.

Un homomorfismo $f\colon R \to R$ se llama un **endomorfismo** de R.

11.2.2. Ejemplo. La proyección canónica

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad a \mapsto [a]_n$$

es un homomorfismo de anillos. De hecho, $\mathbb{Z}/n\mathbb{Z}$ es un ejemplo de **anillo cociente** que vamos a introducir más adelante. ▲

11.2.3. Ejemplo. Para todo anillo R existe un homomorfismo único $R \to 0$ al anillo nulo. ▲

11.2.4. Ejemplo. Para todo anillo R existe un homomorfismo único $f\colon \mathbb{Z} \to R$ desde el anillo de los enteros. En efecto, por la definición, $f(1) = 1_R$, y luego para todo $n \in \mathbb{Z}$ se tiene

$$f(n) = \begin{cases} \underbrace{1_R + \cdots + 1_R}_{n}, & n > 0, \\ -(\underbrace{1_R + \cdots + 1_R}_{-n}), & n < 0, \\ 0, & f = 0. \end{cases}$$

El elemento $f(n) \in R$ por abuso de notación también se denota por n. ▲

11.2.5. Ejemplo. Sea R un anillo conmutativo. Para $\underline{c} = (c_1, \ldots, c_n)$ donde $c_i \in R$ tenemos el **homomorfismo de evaluación**

$$\begin{aligned} \mathrm{ev}_{\underline{c}}\colon R[X_1, \ldots, X_n] &\to R, \\ f &\mapsto f(c_1, \ldots, c_n). \end{aligned}$$

Aquí si $f = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n}\, X_1^{i_1} \cdots X_n^{i_n}$, entonces

$$f(c_1, \ldots, c_n) := \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n}\, c_1^{i_1} \cdots c_n^{i_n}.$$

▲

11.2.6. Observación. *Sea $f\colon R \to S$ un homomorfismo de anillos. Se cumplen las siguientes propiedades.*

1) $f(0_R) = 0_S$,

2) $f(-x) = -f(x)$ para todo $x \in R$,

3) *se cumple* $f(x^{-1}) = f(x)^{-1}$ *para todo* $x \in R^\times$, *y de este modo* f *se restringe a un homomorfismo de grupos* $f^\times \colon R^\times \to S^\times$*:*

$$\begin{array}{ccc} R^\times & \overset{f^\times}{\dashrightarrow} & S^\times \\ \downarrow & & \downarrow \\ R & \xrightarrow{f} & S \end{array}$$

Demostración. Las partes 1) y 2) ya las probamos para homomorfismos de grupos. La parte 3) es un análogo multiplicativo de 2) y se demuestra de la misma manera:

$$f(x^{-1})\,f(x) = f(x^{-1}\,x) = f(1_R) = 1_S, \quad f(x)\,f(x^{-1}) = f(x\,x^{-1}) = f(1_R) = 1_S.$$

■

11.2.7. Definición. Se dice que un homomorfismo de anillos $f \colon R \to S$ es un **isomorfismo** si existe un homomorfismo de anillos $f^{-1} \colon S \to R$ tal que $f^{-1} \circ f = \mathrm{id}_R$ y $f \circ f^{-1} = \mathrm{id}_S$.

Un isomorfismo $f \colon R \to R$ se llama un **automorfismo** de R.

11.2.8. Ejemplo. La conjugación compleja

$$z = x + y\sqrt{-1} \mapsto \overline{z} := x - y\sqrt{-1}$$

es un automorfismo de $\mathbb{C}$. ▲

11.2.9. Observación. *Todo homomorfismo de anillos* $f \colon R \to S$ *es un isomorfismo si y solamente si es biyectivo.*

Demostración. Si f es un isomorfismo, entonces f admite un homomorfismo inverso $f^{-1} \colon S \to R$, así que es una biyección.

Viceversa, supongamos que f es un homomorfismo biyectivo. En este caso existe una aplicación inversa $f^{-1} \colon S \to R$ y hay que comprobar que es un homomorfismo de anillos. Dado que $f(1_R) = 1_S$, tenemos $f^{-1}(1_S) = 1_R$. Luego, para $x, y \in S$

$$f^{-1}(xy) = f^{-1}(f \circ f^{-1}(x) \cdot f \circ f^{-1}(y)) = f^{-1}(f(f^{-1}(x) \cdot f^{-1}(y))) = f^{-1}(x) \cdot f^{-1}(y).$$

Con el mismo truco se demuestra que $f^{-1}(x + y) = f^{-1}(x) + f^{-1}(y)$. ■

11.2.10. Observación (Imagen y preimagen). *Sea* $f \colon R \to S$ *un homomorfismo de anillos.*

1) *La* ***imagen*** $\operatorname{im} f := \{f(x) \mid x \in R\}$ *es un subanillo de* S*.*

2) *Si* $S' \subseteq S$ *es un subanillo, entonces su preimagen*

$$f^{-1}(S') := \{x \in R \mid f(x) \in S'\}$$

es un subanillo de R*.*

Demostración. La parte 1) se sigue de las identidades

$$f(x+y) = f(x) + f(y), \quad f(1_R) = 1_S, \quad f(xy) = f(x)\,f(y).$$

En la parte 2), si $x \pm y \in f^{-1}(S')$, entonces $f(x), f(y) \in S'$. Luego, $x \pm y \in f^{-1}(S')$, dado que $f(x \pm y) = f(x) \pm f(y) \in S'$. De la misma manera, $xy \in f^{-1}(S')$, dado que $f(xy) = f(x)\,f(y) \in S'$. Tenemos $f(0_R) = 0_S \in S'$ y $f(1_R) = 1_S \in S'$, y por lo tanto $0_R, 1_R \in f^{-1}(S')$. ■

11.2.11. Proposición. *Sea R un anillo. Consideremos el homomorfismo $f\colon \mathbb{Z} \to R$. Entonces,* $\operatorname{im} f$ *es el mínimo subanillo de R. Hay dos posibilidades.*

1) $\operatorname{im} f \cong \mathbb{Z}$. *En este caso se dice que R es un anillo de* ***característica*** 0.

2) $\operatorname{im} f \cong \mathbb{Z}/n\mathbb{Z}$ *para algún $n = 1, 2, 3, \ldots$ En este caso se dice que R es un anillo de* ***característica*** n.

Demostración. Tenemos

$$\operatorname{im} f = \{\underbrace{1_R + \cdots + 1_R}_{m} \mid m = 0, 1, 2, 3, \ldots\}.$$

Notamos que todo subanillo $S \subseteq R$ necesariamente contiene 0_R y 1_R, y siendo cerrado respecto a la suma, también contiene todos los elementos $\pm\underbrace{1 + \cdots + 1}_{m}$. Entonces, $\operatorname{im} f \subseteq S$ para cualquier subanillo $S \subseteq R$. Hay dos posibilidades.

1) El orden de 1_R en el grupo aditivo de R es infinito. En este caso $\operatorname{im} f \cong \mathbb{Z}$ y el isomorfismo viene dado por

$$\mathbb{Z} \to \operatorname{im} f, \quad 1 \mapsto 1_R.$$

2) El orden de 1_R en el grupo aditivo de R es finito y es igual a algún número $n = 1, 2, 3, \ldots$ En este caso $\operatorname{im} f \cong \mathbb{Z}/n\mathbb{Z}$ y el isomorfismo viene dado por

$$\mathbb{Z}/n\mathbb{Z} \to \operatorname{im} f, \quad [1]_n \mapsto 1_R.$$

■

11.2.12. Ejemplo. Los anillos $\mathbb{Q}$, $\mathbb{Q}[X]$, $M_m(\mathbb{Z})$ y $\mathbb{Z}[X_1, \ldots, X_m]$ son de característica 0. Los anillos $M_m(\mathbb{Z}/n\mathbb{Z})$ y $\mathbb{Z}/n\mathbb{Z}[X_1, \ldots, X_m]$ son de característica n. El cuerpo finito $\mathbb{F}_p$ tiene característica p. ▲

11.2.13. Observación. *Si R es un anillo no nulo sin divisores de cero ($xy = 0$ implica que $x = 0$ o $y = 0$), entonces la característica de R es igual a 0 o es un número primo p.*

Demostración. El anillo $\mathbb{Z}/n\mathbb{Z}$ tiene divisores de cero si y solamente si n es un número compuesto. ■

11.3 Álgebras sobre anillos

11.3.1. Definición. Sea R un anillo. Una **R-álgebra** es un anillo A junto con un homomorfismo de anillos $\alpha\colon R \to A$. En este caso por abuso de notación para $r \in R$ y $x \in A$

(11.1) en lugar de "$\alpha(r) \cdot x$" se escribe simplemente "$r \cdot x$".

Para dos R-álgebras $\alpha\colon R \to A$ y $\beta\colon R \to B$ un **homomorfismo** es un homomorfismo de anillos $f\colon R \to B$ que hace conmutar el diagrama

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ & {\scriptstyle\alpha}\nwarrow \quad \nearrow{\scriptstyle\beta} & \\ & R & \end{array}$$

Notamos que la última condición $f \circ \alpha = \beta$ implica que para todo $r \in R$ y $x \in A$ se cumple

$$f \circ \alpha(r) \cdot f(x) = \beta(r) \cdot f(x).$$

Puesto que f es un homomorfismo, esto es equivalente a $f(\alpha(r) \cdot x) = \beta(r) \cdot f(x)$ o, usando la notación (11.1),

$$f(r \cdot x) = r \cdot f(x).$$

11.3.2. Ejemplo. Todo anillo tiene una estructura única de $\mathbb{Z}$-álgebra: existe un homomorfismo único $\mathbb{Z} \to R$. Un homomorfismo de $\mathbb{Z}$-álgebras es la misma cosa que homomorfismo de anillos:

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & S \\ & {\scriptstyle\exists!}\nwarrow \quad \nearrow{\scriptstyle\exists!} & \\ & \mathbb{Z} & \end{array}$$

De nuevo, usando la notación (11.1), para $n \in \mathbb{Z}$ y $r \in R$ tenemos

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

▲

11.3.3. Ejemplo. Los números complejos forman una $\mathbb{R}$-álgebra: tenemos un homomorfismo

$$\begin{aligned} \alpha\colon \mathbb{R} &\rightarrowtail \mathbb{C}, \\ x &\mapsto x + 0\sqrt{-1}. \end{aligned}$$

Notamos que para $x \in \mathbb{R}$ se tiene

$$x \cdot (u + v\sqrt{-1}) = xu + xv\sqrt{-1}.$$

▲

11.3.4. Ejemplo. Sea R un anillo conmutativo. Los anillos de polinomios $R[X_1, \ldots, X_n]$ y series formales de potencias $R[\![X_1, \ldots, X_n]\!]$ son R-álgebras. En el caso de polinomios, el homomorfismo

$$\alpha\colon R \to R[X_1, \ldots, X_n]$$

asocia a los elementos de R los polinomios constantes correspondientes. En este caso

$$r \cdot \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} = \sum_{i_1,\ldots,i_n} (r \cdot a_{i_1,\ldots,i_n}) X_1^{i_1} \cdots X_n^{i_n}.$$

De modo similar, tenemos para las series de potencias

$$\alpha\colon R \to R[\![X_1, \ldots, X_n]\!].$$

▲

11.3.5. Ejemplo. Sea R un anillo conmutativo. El homomorfismo

$$\alpha\colon R \to M_n(R), \quad r \mapsto \begin{pmatrix} r & & & \\ & r & & \\ & & \ddots & \\ & & & r \end{pmatrix}$$

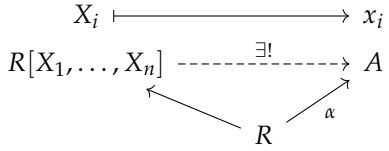
que asocia a los elementos de R las matrices escalares correspondientes define estructura de R-álgebra sobre $M_n(R)$. En este caso

$$r \cdot (x_{ij}) = (r x_{ij}).$$

▲

Ahora podemos finalmente aclarar qué es el anillo de polinomios $R[X_1, \ldots, X_n]$.

11.3.6. Proposición (Propiedad universal del álgebra de polinomios). *Sea R un anillo conmutativo y sea A una R-álgebra conmutativa. Consideremos elementos $x_1, \ldots, x_n \in A$. Existe un homomorfismo único de R-álgebras $f\colon R[X_1, \ldots, X_n] \to A$ tal que $f(X_i) = x_i$ para $i = 1, \ldots, n$.*



Demostración. Si $f\colon R[X_1, \ldots, X_n] \to A$ es un homomorfismo de R-álgebras, entonces para todo polinomio tenemos

$$\begin{aligned} f\left(\sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}\right) &= \sum_{i_1,\ldots,i_n \geq 0} f\left(a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}\right) \\ &= \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} \cdot f(X_1^{i_1} \cdots X_n^{i_n}) = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} \cdot f(X_1)^{i_1} \cdots f(X_n)^{i_n}. \end{aligned}$$

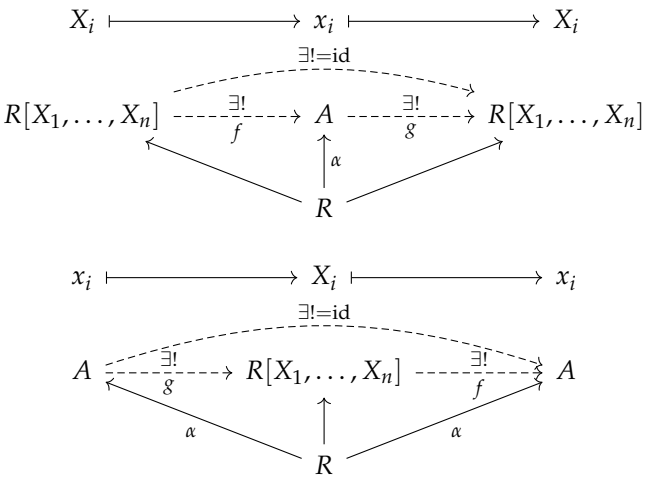
Esto significa que f está definido de modo único por las imágenes $f(X_i) \in A$. Además, se ve que especificando $f(X_i) = x_i$ para elementos arbitrarios $x_1, \ldots, x_n \in A$ se obtiene un homomorfismo de R-álgebras $f\colon R[X_1, \ldots, X_n] \to A$. ■

11.3.7. Corolario. *Sea R un anillo conmutativo. Consideremos elementos $x_1, \ldots, x_n \in R$. Existe un homomorfismo único de anillos $f\colon \mathbb{Z}[X_1, \ldots, X_n] \to R$ tal que $f(X_i) = x_i$ para $i = 1, \ldots, n$.*

$$\begin{array}{ccc} X_i & \longmapsto & x_i \\ \mathbb{Z}[X_1, \ldots, X_n] & \overset{\exists!}{\dashrightarrow} & R \end{array}$$

Demostración. Recordemos que anillos son $\mathbb{Z}$-álgebras. ■

Como siempre, las palabras "propiedad universal" significan que $R[X_1, \ldots, X_n]$ está definido de modo único salvo isomorfismo único por esta propiedad. En efecto, supongamos que A es una R-álgebra con algunos elementos $x_1, \ldots, x_n$ que satisface la misma propiedad universal. Entonces, existe un único homomorfismo de R-álgebras $f\colon R[X_1, \ldots, X_n] \to A$ tal que $X_i \mapsto x_i$ y un único homomorfismo de R-álgebras $g\colon A \to R[X_1, \ldots, X_n]$ tal que $x_i \mapsto X_i$. Luego, necesariamente $g \circ f = \mathrm{id}_{R[X_1,\ldots,X_n]}$ y $f \circ g = \mathrm{id}_A$:



11.3.8. Comentario. Es importante que A sea conmutativa. En el caso contrario, los elementos $f(X_i)$ no necesariamente conmutan entre sí, mientras que X_i conmutan en $R[X_1, \ldots, X_n]$. La propiedad universal similar respecto a álgebras no conmutativas caracteriza a los "polinomios en variables no conmutativas" (aunque suena exótico, es un objeto natural e importante).

Sin embargo, para polinomios *en una variable* tenemos la siguiente propiedad universal: si A es una R-álgebra, *no necesariamente conmutativa* y $x \in A$, entonces existe un homomorfismo único de R-álgebras $f\colon R[X] \to A$ tal que $f(X) = x$:

$$f\Big(\sum_{i\geq 0} a_i X^i\Big) = \sum_{i\geq 0} a_i \cdot f(X)^i.$$

11.3.9. Comentario. El anillo de series formales $R[\![X_1, \ldots, X_n]\!]$ también se caracteriza por cierta propiedad universal, pero es un poco más complicada y por esto la omitimos.

11.3.10. Proposición. *Sea R un anillo conmutativo y sea $n = 2, 3, 4, \ldots$ Tenemos isomorfismos*

$$R[X_1, \ldots, X_{n-1}][X_n] \cong R[X_1, \ldots, X_n],$$
$$R[\![X_1, \ldots, X_{n-1}]\!][\![X_n]\!] \cong R[\![X_1, \ldots, X_n]\!].$$

Idea de la demostración. Todo elemento $\sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}$ puede ser escrito como $\sum_{i \geq 0} f_i X_n^i$, donde en f_i aparecen las variables $X_1, \ldots, X_{n-1}$. Dejo los detalles al lector. ■

11.4 El álgebra de grupo

11.4.1. Definición. Sea G un grupo y sea R un anillo conmutativo. Definamos

$$R[G] := \Big\{ \text{sumas formales } \sum_{g \in G} a_g\, g \;\Big|\; a_g \in R,\ a_g = 0 \text{ salvo un número finito de } g \in G \Big\}.$$

Definamos la suma mediante

$$\Big(\sum_{g \in G} a_g\, g\Big) + \Big(\sum_{g \in G} b_g\, g\Big) := \sum_{g \in G} (a_g + b_g)\, g$$

y el producto mediante la multiplicación en G y la distributividad formal:

$$\begin{aligned}\Big(\sum_{h \in G} a_h\, h\Big) \cdot \Big(\sum_{k \in G} b_k\, k\Big) := \sum_{h \in G} a_h \Big(\sum_{k \in G} b_k\, hk\Big) &= \sum_{h \in G} a_h \Big(\sum_{g \in G} b_{h^{-1}g}\, h(h^{-1}g)\Big) \\ &= \sum_{h \in G} \Big(\sum_{h \in G} a_h\, b_{h^{-1}g}\Big)\, g = \sum_{g \in G} \Big(\sum_{hk = g} a_h b_k\Big)\, g.\end{aligned}$$

Aquí la segunda igualdad sigue del hecho de que el conjunto $\{h^{-1}g \mid g \in G\}$ está en biyección con los elementos de G. Entonces, podemos tomar como la definición la identidad[*]

$$\Big(\sum_{h \in G} a_h\, h\Big) \cdot \Big(\sum_{k \in G} b_k\, k\Big) := \sum_{g \in G} \Big(\sum_{hk = g} a_h b_k\Big)\, g.$$

Se puede comprobar que $R[G]$ es un anillo. El cero es la suma $\sum_{g \in G} a_g\, g$ donde $a_g = 0$ para todo $g \in G$ y la identidad es la suma donde $a_e = 1$ (donde $e \in G$ es el elemento neutro de G) y $a_g = 0$ para $g \neq e$. Notamos que el anillo $R[G]$ es conmutativo si y solamente si G es un grupo abeliano. El homomorfismo

$$\begin{aligned} &R \to R[G], \\ &r \mapsto \sum_{g \in G} a_g\, g, \quad a_g := \begin{cases} r, & g = e, \\ 0, & g \neq e \end{cases}\end{aligned}$$

[*]Note que es parecida a la fórmula

$$\Big(\sum_{i \geq 0} a_i\, X^i\Big) \cdot \Big(\sum_{j \geq 0} b_j\, X^j\Big) := \sum_{k \geq 0} \Big(\sum_{i+j=k} a_i b_j\Big)\, X^k.$$

(No es una coincidencia.)

define una estructura de R-álgebra sobre $R[G]$. Tenemos

$$r \cdot \sum_{g\in G} a_g\, g = \sum_{g\in G} (r\, a_g)\, g.$$

El álgebra $R[G]$ se llama el **álgebra de grupo** asociada a G.

Notamos que cada elemento $g \in G$ corresponde a un elemento

$$\sum_{h\in G} a_h\, g \in R[G], \quad a_h := \begin{cases} 1, & h = g, \\ 0, & h \neq g, \end{cases}$$

y esto nos da una aplicación inyectiva $G \hookrightarrow R[G]$. Respecto a esta inclusión, $G \subseteq R[G]^\times$.

Tenemos

$$h \sum_{g\in G} a_g\, g = \sum_{g\in G} a_g\, hg = \sum_{g\in G} a_{h^{-1}g}\, g, \quad \Big(\sum_{g\in G} a_g\, g\Big)\, h = \sum_{g\in G} a_g\, gh = \sum_{g\in G} a_{gh^{-1}}\, g.$$

Comparando estas dos expresiones, se puede calcular el centro de $R[G]$ (haga el ejercicio 11.10).

11.4.2. Ejemplo. En el álgebra $\mathbb{Z}[S_3]$ calculamos

$$\begin{aligned}(1\cdot(1\,2) + 2\cdot(2\,3))^2 &= 1\cdot\underbrace{(1\,2)^2}_{=\mathrm{id}} + 2\cdot\underbrace{(1\,2)\,(2\,3)}_{=(1\,2\,3)} + 2\cdot\underbrace{(2\,3)\,(1\,2)}_{=(1\,3\,2)} + 4\cdot\underbrace{(2\,3)^2}_{=\mathrm{id}} \\ &= 5\cdot\mathrm{id} + 2\cdot(1\,2\,3) + 2\cdot(1\,3\,2).\end{aligned}$$

Si $C_3 = \{e, g, g^2\}$ es el grupo cíclico de orden 3, entonces tenemos en $\mathbb{Z}[C_3]$

$$(e+g+g^2)^2 = e+g+g^2+g+g^2+\underbrace{g^3}_{=e} + g^2 + \underbrace{g^3}_{=e} + \underbrace{g^4}_{=g} = 3\cdot(e+g+g^2).$$

(Para una generalización, de este cálculo, haga el ejercicio 11.9.) ▲

11.4.3. Proposición (Propiedad universal del álgebra de grupo o adjunción con $A \rightsquigarrow A^\times$). *Sea R un anillo conmutativo, G un grupo y A una R-álgebra. Todo homomorfismo de grupos $f\colon G \to A^\times$ se extiende de modo único a un homomorfismo de R-álgebras $\widetilde{f}\colon R[G] \to A$:*

$$\begin{array}{ccc} G & \hookrightarrow & R[G] \\ {\scriptstyle f}\downarrow & & \vdots\,{\scriptstyle \exists!\widetilde{f}} \\ A^\times & \hookrightarrow & A \end{array}$$

En otras palabras, hay una biyección natural

$$\{\text{homomorfismos de } R\text{-álgebras } R[G] \to A\} \cong \{\text{homomorfismos de grupos } G \to A^\times\}.$$

En particular, para todo anillo R hay una biyección natural

$$\{\text{homomorfismos de anillos } \mathbb{Z}[G] \to R\} \cong \{\text{homomorfismos de grupos } G \to R^\times\}.$$

Demostración. Sea $\alpha\colon R \to A$ el homomorfismo que define la estructura de R-álgebra. Sea $\widetilde{f}\colon R[G] \to A$ un homomorfismo de R-álgebras. Puesto que $G \subseteq R[G]^\times$, este homomorfismo se restinge a un homomorfismo de grupos $f\colon G \to A^\times$. Luego,

$$\widetilde{f}\Big(\sum_{g\in G} a_g\, g\Big) = \sum_{g\in G} \widetilde{f}(a_g\, g) = \sum_{g\in G} \alpha(a_g)\, f(g).$$

■

11.4.4. Corolario. *Sea R un anillo conmutativo. Todo homomorfismo de grupos $f\colon G \to H$ se extiende de manera canónica a un homomorfismo de R-álgebras $\widetilde{f}\colon R[G] \to R[H]$.*

Demostración. El homomorfismo de R-álgebras en cuestión viene dado por

$$\widetilde{f}\Big(\sum_{g\in G} a_g\, g\Big) = \sum_{g\in G} a_g\, f(g),$$

y es un caso particular del resultado anterior:

$$\begin{array}{ccc} G & \hookrightarrow & R[G] \\ {\scriptstyle f}\downarrow & & \\ H & & \exists!\widetilde{f}\,\big\downarrow \\ \big\downarrow & & \\ R[H]^\times & \hookrightarrow & R[H] \end{array}$$

■

El álgebra $R[G]$ juega papel importante en la teoría de representación de grupos finitos.

11.5 Monomorfismos y epimorfismos de anillos

11.5.1. Proposición. *Sea $f\colon R \to S$ un homomorfismo de anillos. Las siguientes condiciones son equivalentes.*

1) *f es inyectivo.*
2) *Si S' es otro anillo y hay homomorfismos $g, g'\colon R' \to R$ tales que $f \circ g = f \circ g'$, entonces $g = g'$.*

En este caso se dice que f es un ***monomorfismo****.*

Demostración. La implicación 1) $\Rightarrow$ 2) se cumple para cualquier aplicación inyectiva f. Para ver que 2) $\Rightarrow$ 1), supongamos que f no es inyectiva y existen diferentes $x, x' \in R$ tales que $f(x) = f(x')$. Primero recordemos que para todo anillo R un homomorfismo $f\colon \mathbb{Z}[X] \to R$ está definido de modo único por $f(X) \in R$ (véase el comentario 11.3.9). Consideremos los homomorfismos

$$g\colon \mathbb{Z}[X] \to R, \quad X \mapsto x$$

y

$$g\colon \mathbb{Z}[X] \to R, \quad X \mapsto x'.$$

Ahora $f \circ g = f \circ g'$, aunque $g \neq g'$. ■

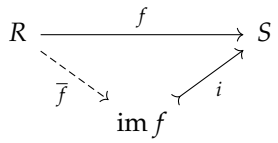
11.5.2. Ejemplo. Consideremos la propiedad dual para un homomorfismo $f\colon R \to S$: *si S' es otro anillo y hay homomorfismos $g, g'\colon S \to S'$ tales que $g \circ f = g' \circ f$, entonces $g = g'$*. Esto se cumple si f es sobreyectivo. Sin embargo, esta propiedad no necesariamente implica que f es sobreyectivo. Por ejemplo, consideremos la inclusión $i\colon \mathbb{Z} \to \mathbb{Q}$. Supongamos que $g \circ i = g' \circ i$. Luego, para todo $\frac{a}{b} \in \mathbb{Q}$ se tiene

$$\begin{aligned} g\left(\frac{a}{b}\right) &= g(a) \cdot g\left(\frac{1}{b}\right) = g'(a) \cdot g\left(\frac{1}{b}\right) = g'\left(\frac{a}{b} \cdot b\right) \cdot g\left(\frac{1}{b}\right) = g'\left(\frac{a}{b}\right) \cdot g'(b) \cdot g\left(\frac{1}{b}\right) \\ &= g'\left(\frac{a}{b}\right) \cdot g(b) \cdot g\left(\frac{1}{b}\right) = g'\left(\frac{a}{b}\right) \cdot g\left(b \cdot \frac{1}{b}\right) = g'\left(\frac{a}{b}\right) \cdot g(1) = g'\left(\frac{a}{b}\right). \end{aligned}$$

Entonces, $g = g'$. ▲

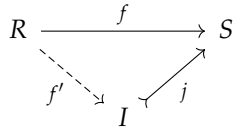
11.5.3. Proposición (Propiedad universal de la imagen). *Sea $f\colon R \to S$ un homomorfismo de anillos.*

1) *Existe una factorización de f por el monomorfismo canónico $i\colon \operatorname{im} f \rightarrowtail S$ (inclusión de subanillo):*



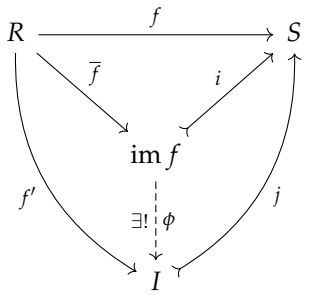
$$f = i \circ \overline{f}.$$

2) *Supongamos que hay otro anillo I junto con un monomorfismo $j\colon I \rightarrowtail S$ 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 $\operatorname{im} f \subset S$, en realidad f puede ser vista como una aplicación $\overline{f}\colon R \to \operatorname{im} f$. Es un homomorfismo, puesto que f es un homomorfismo. Su composición con la inclusión del subanillo $i\colon \operatorname{im} f \rightarrowtail S$ coincide con f.

En 2), la única opción para ϕ para que se cumpla $\phi \circ \overline{f} = f'$ es definir

$$\begin{aligned} \phi\colon \operatorname{im} f &\to I, \\ f(x) &\mapsto f'(x). \end{aligned}$$

Esta aplicación está bien definida: si tenemos $f(x_1) = f(x_2)$, entonces

$$j(f'(x_1)) = f(x_1) = f(x_2) = j(f'(x_2)) \Rightarrow f'(x_1) = f'(x_2).$$

También se cumple $i = j \circ \phi$. En efecto, para $h = f(x) \in \operatorname{im} f$ tenemos

$$j(\phi(h)) = j(f'(x)) = f(x).$$

■

11.6 Ideales

El la teoría de grupos, el grupo cociente se construye a partir de un subgrupo *normal*. Para anillos, los cocientes se definen a partir de un *ideal*.

11.6.1. Definición. Sea R un anillo y sea $I \subseteq R$ un subgrupo abeliano de R respecto a la adición.

1) Si $rx \in I$ para cualesquiera $r \in R$ y $x \in I$, se dice que I es un **ideal izquierdo** en R.

2) Si $xr \in I$ para cualesquiera $r \in R$ y $x \in I$, se dice que I es un **ideal derecho** en R.

3) Si se cumplen las condiciones 2) y 3), entonces se dice que I es un **ideal bilateral** en R. Esto es equivalente a asumir que $rxr' \in I$ para cualesquiera $r, r' \in R$ y $x \in I$.

11.6.2. Comentario. Tenemos $-x = (-1) \cdot x = x \cdot (-1)$, así que para comprobar que un subconjunto $I \subseteq R$ es un ideal, es suficiente comprobar que I no es vacío, cerrado respecto a la adición, y cumple una de las propiedades 1)–3) de la definición de arriba.

11.6.3. Comentario. Si R es un anillo *conmutativo*, entonces las condiciones 1)–3) son equivalentes. En este caso se dice simplemente que I es un **ideal** en R.

11.6.4. Observación. *Sea R un anillo.*

1) *Si $I_k \subseteq R$ es una familia de ideales izquierdos (resp. derechos, bilaterales), entonces $\bigcap_k I_k$ es un ideal izquierdo (resp. derecho, resp. bilateral).*

2) *Si*
$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq R$$
es una cadena de ideales izquierdos (resp. derechos, bilaterales), entonces $\bigcup_k I_k$ es un ideal izquierdo (resp. derecho, resp. bilateral).

Demostración. Ejercicio para el lector. ■

11.6.5. Ejemplo. 0 y R son ideales bilaterales para cualquier anillo R. ▲

11.6.6. Ejemplo. Consideremos el anillo de los números enteros $\mathbb{Z}$. Como sabemos, sus subgrupos abelianos son de la forma
$$n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\}$$
para $n = 0, 1, 2, 3, \ldots$ Se puede comprobar que $n\mathbb{Z}$ son ideales (al multiplicar un múltiplo de n por cualquier número entero se obtiene un múltiplo de n). ▲

11.6.7. Observación. *Sea R un anillo.*

1) *Para un ideal izquierdo (resp. derecho, resp. bilateral) $I \subseteq R$ se tiene $I = R$ si y solo si $u \in I$ para algún elemento invertible $u \in R^\times$.*

2) *Si R es un anillo conmutativo, entonces R es un cuerpo si y solo si 0 y R son los únicos ideales en R.*

Demostración. En 1), notamos que si $I = R$, entonces $1 \in I$ y $1 \in R^\times$. Viceversa, si $u \in R^\times$ es un elemento tal que $u \in I$, entonces para todo $r \in R$
$$r = r \cdot 1 = r\,(u^{-1}\,u) = (r\,u^{-1})\,u \in I.$$
Este argumento funciona si I es un ideal izquierdo. Para un ideal derecho, tenemos
$$r = 1 \cdot r = (u\,u^{-1})\,r = u\,(u^{-1}\,r) \in I.$$

En 2), si R es un cuerpo, entonces para todo ideal no nulo I si $x \in I$ y $x \neq 0$, entonces $x \in R^\times$ y por ende $I = R$ según la parte 1). Viceversa, si 0 y R son los únicos ideales en R, para $x \neq 0$ podemos considerar el ideal
$$Rx := \{rx \mid r \in R\}.$$
Tenemos $Rx \neq 0$, así que $Rx = R$. En particular, $rx = 1$ para algún $r \in R$, y este elemento r es el inverso de x. ■

11.6.8. Ejemplo. Sea X un conjunto no vacío y sea R un anillo. Entonces, las aplicaciones $f\colon X \to R$ forman un anillo $Fun(X,R)$ respecto a las operaciones punto por punto. Para un punto $x \in X$ sea I_x el conjunto de las aplicaciones tales que $f(x) = 0$:

$$I_x := \{f\colon X \to R \mid f(x) = 0\}.$$

Esto es un ideal en $Fun(X,R)$. En general, para un subconjunto $Y \subseteq X$, tenemos un ideal

$$I(Y) = \bigcap_{x\in Y} I_x = \{f\colon X \to R \mid f(x) = 0 \text{ para todo } x \in Y\} \subseteq Fun(X,R).$$

▲

El último ejemplo tiene muchas variaciones. Por ejemplo, se puede tomar $R = \mathbb{R}$ y X un subconjunto de $\mathbb{R}$ y considerar las funciones continuas $f\colon X \to \mathbb{R}$. También se puede tomar un cuerpo k y el **espacio afín**

$$\mathbb{A}^n(k) := \{(x_1, \ldots, x_n) \mid x_i \in k\}$$

y en lugar de todas las funciones $f\colon \mathbb{A}^n(k) \to k$ considerar los polinomios $f \in k[X_1, \ldots, X_n]$ que también pueden ser evaluados en los puntos de $\mathbb{A}^n(k)$.

11.6.9. Ejemplo. Sea k un cuerpo. Para todo subconjunto $X \subseteq \mathbb{A}^n(k)$ consideremos el conjunto de los polinomios en n variables con coeficientes en k que se anulan en todos los puntos de X:

$$I(X) := \{f \in k[X_1, \ldots, X_n] \mid f(x) = 0 \text{ para todo } x \in X\} = \bigcap_{x\in X} I(\{x\}).$$

Esto es un ideal en el anillo de polinomios $k[X_1, \ldots, X_n]$. En efecto, si $f_i(x) = 0$ para todo $x \in X$, entonces todas las sumas finitas $\sum_i g_i f_i$ se anulan sobre X. ▲

En este curso no vamos a ver muchos resultados sobre anillos no conmutativos, pero es bueno conocer algunas definiciones básicas. El lector interesado puede consultar el libro [Lam2001].

11.6.10. Ejemplo. Las matrices de la forma $\begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}$ forman un ideal izquierdo en $M_2(R)$ que no es un ideal derecho. Viceversa, las matrices $\begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}$ forman un ideal derecho que no es izquierdo. ▲

11.6.11. Observación. *Sea k un cuerpo. Entonces, los únicos ideales bilaterales en el anillo de matrices $R = M_n(k)$ son 0 y R.*

Demostración. Denotemos por e_{ij} la matriz que tiene ceros en todas las entradas y 1 en la entrada (i,j). Notamos que

$$e_{ij}\, A\, e_{k\ell} = a_{jk}\, e_{i\ell}.$$

Supongamos que $I \subseteq R$ es un ideal bilateral no nulo. Sea $A \in I$ donde A es una matriz tal que $a_{jk} \neq 0$ para algunos $1 \leq j,k \leq n$. Luego, la fórmula de arriba nos dice que para todo $1 \leq i,\ell \leq n$ se tiene

$$e_{i\ell} = a_{jk}^{-1}\, e_{ij}\, A\, e_{k\ell}.$$

Puesto que I es un ideal bilateral, podemos concluir que todas las matrices $e_{i\ell}$ pertenecen a I. Luego, para cualquier matriz $B = (b_{i\ell}) \in M_n(k)$ tenemos

$$B = \sum_{1\leq i,\ell\leq n} b_{i\ell}\, e_{i\ell},$$

y esta matriz pertenece a I, siendo una suma de $b_{i\ell}\, e_{i\ell} \in I$. Entonces, acabamos de probar que un ideal bilateral no nulo en $M_n(k)$ necesariamente coincide con todo $M_n(k)$. ■

Para una generalización del último resultado, haga el ejercicio 11.15.

11.6.12. Observación. *Sea $f\colon R \to S$ un homomorfismo de anillos.*

1) *Si $I \subseteq S$ es un ideal izquierdo (resp. ideal derecho, resp. ideal bilateral), entonces $f^{-1}(I)$ es un ideal izquierdo (resp. ideal derecho, resp. ideal bilateral) en R.*

2) *Si f es sobreyectivo e $I \subseteq R$ es un ideal izquierdo (resp. ideal derecho, resp. ideal bilateral), entonces $f(I)$ es un ideal izquierdo (resp. ideal derecho, resp. ideal bilateral) en S.*

Demostración. Veamos el caso de ideales izquierdos; el caso de ideales derechos y bilaterales es similar.

Tenemos $f(0_R) = 0_S \in I$, así que $0_R \in f^{-1}(I)$. Si $x,y \in f^{-1}(I)$, esto significa que $f(x), f(y) \in I$. Luego, $f(x+y) = f(x) + f(y) \in I$, así que $x+y \in f^{-1}(I)$. Ahora si $x \in f^{-1}(I)$, entonces $f(x) \in I$, y luego $f(r\,x) = f(r)\,f(x) \in I$ para cualesquiera $r \in R$, así que $r\,x \in f^{-1}(I)$.

En la parte 2), tenemos $0_S = f(0_R)$ donde $0_R \in I$, así que $0_S \in f(I)$. Para $x,y \in I$ tenemos $x+y \in I$, así que $f(x), f(y) \in f(I)$ implica que $f(x) + f(y) = f(x+y) \in f(I)$. Para $x \in I$ y $s \in S$, dado que f es una aplicación sobretectiva, se tiene $s = f(r)$ para algún $r \in R$. Luego, $s\,f(x) = f(r)\,f(x) = f(rx) \in f(I)$. ■

11.6.13. Comentario. Si $f\colon R \to S$ es un homomorfismo que no es sobreyectivo e $I \subseteq R$ es un ideal, entonces $f(I)$ no tiene por qué ser un ideal en S. Considere por ejemplo la inclusión $f\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$.

11.7 Ideales generados

11.7.1. Definición. Sea R un anillo y $A \subset R$ un subconjunto.

1) El **ideal izquierdo generado por** A es el mínimo ideal izquierdo que contiene a A:

$$RA := \bigcap_{\substack{I\subseteq R \\ \text{izquierdo} \\ A\subseteq I}} I.$$

2) El **ideal derecho generado por** A es el mínimo ideal derecho que contiene a A:

$$AR := \bigcap_{\substack{I \subseteq R \\ \text{derecho} \\ A \subseteq I}} I.$$

3) El **ideal bilateral generado por** A es el mínimo ideal bilateral que contiene a A:

$$RAR := \bigcap_{\substack{I \subseteq R \\ \text{bilateral} \\ A \subseteq I}} I.$$

11.7.2. Comentario. Si $A = \{x_1, \ldots, x_n\}$ es un conjunto finito, se usa la notación

$$RA = Rx_1 + \cdots + Rx_n, \quad AR = x_1R + \cdots + x_nR, \quad RAR = Rx_1R + \cdots + Rx_nR.$$

11.7.3. Comentario. Notamos que cuando R es un anillo conmutativo, se tiene $RA = AR = RAR$, y normalmente este ideal se denota por (A), o por $(x_1, \ldots, x_n)$ cuando $A = \{x_1, \ldots, x_n\}$ es un conjunto finito.

11.7.4. Definición. Si $I \subseteq R$ es un ideal (izquierdo, derecho, bilateral) que puede ser generado por un número finito de elementos, se dice que I es **finitamente generado**. Si I puede ser generado por un elemento (es decir, $I = Rx$, xR, RxR respectivamente), se dice que I es un **ideal principal**.

11.7.5. Ejemplo. Todo ideal en $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ para algún $n = 0, 1, 2, 3, \ldots$ El ideal $n\mathbb{Z}$ es el mínimo ideal que contiene a n, así que es exactamente el ideal generado por n. Entonces, todos los ideales en $\mathbb{Z}$ son principales. ▲

Más adelante vamos a estudiar los anillos conmutativos donde todos los ideales son finitamente generados o donde todos los ideales son principales.

11.7.6. Observación. *Sea R un anillo y $A \subset R$ un subconjunto.*

1) El ideal RA consiste en todas las sumas finitas $\sum_i r_i\, a_i$ donde $r_i \in R$ y $a_i \in A$.

2) El ideal AR consiste en todas las sumas finitas $\sum_i a_i\, r_i$ donde $r_i \in R$ y $a_i \in A$.

3) El ideal RAR consiste en todas las sumas finitas $\sum_i r_i\, a_i\, r_i'$ donde $r_i, r_i' \in R$ y $a_i \in A$.

Demostración. Verifiquemos, por ejemplo, la parte 1). Si I es un ideal izquierdo tal que $A \subseteq I$, entonces $\sum_i r_i a_i \in I$ para cualesquiera $r_i \in R$, $a_i \in A$. Además, se ve que

$$\left\{ \sum_i r_i\, a_i \;\middle|\; r_i \in R,\ a_i \in A \right\}$$

es un ideal izquierdo: es cerrado respecto a las sumas: si $\sum_i r_i\, a_i$ y $\sum_j r_j'\, a_j'$ son sumas finitas con $r_i, r_j' \in R$ y $a_i, a_j' \in A$, entonces $\sum_i r_i\, a_i + \sum_j r_j'\, a_j'$ es una suma finita de la misma forma. Además, para todo $r \in R$

$$r \sum_i r_i\, a_i = \sum_i (r\, r_i)\, a_i,$$

así que el conjunto es cerrado respecto a la multiplicación por los elementos de R por la izquierda.

Las partes 2) y 3) se verifican de la misma manera. ■

11.7.7. Corolario (Sumas de ideales). *Sea R un anillo y sea $I_k \subseteq R$ una familia de ideales izquierdos (resp. derechos, resp. bilaterales). Entonces, el ideal izquierdo (resp. derecho, resp. bilateral) generado por los elementos de I_k coincide con el conjunto*

$$\sum_k I_k := \{\text{sumas finitas } \sum_k x_k \mid x_k \in I_k\}$$

*y se llama la **suma** de los ideales I_k. Es el mínimo ideal izquierdo (resp. derecho, resp. bilateral) en R tal que $I_k \subseteq \sum_k I_k$ para todo k.*

Demostración. Por ejemplo, en el caso de ideales izquierdos, la observación anterior nos dice que hay que tomar las sumas finitas $\sum_i r_i a_i$ donde $r_i \in R$ y $a_i \in I_k$ para algún k. Puesto que cada I_k es un ideal izquierdo, en este caso se tiene $r_i a_i \in I_k$. Las sumas de elementos del mismo ideal I_k también pertenecen a I_k. Entonces, el conjunto de las sumas finitas $\sum_i r_i a_i$ coincide con el conjunto de las sumas finitas $\sum_k x_k$ donde $x_k \in I_k$. ■

11.7.8. Observación (Productos de ideales). *Sea R un anillo y sean $I_1, \ldots, I_n \subseteq R$ ideales izquierdos (resp. derechos, bilaterales).*

1) *El ideal izquierdo (resp. derecho, bilateral) generado por los productos $x_1 \cdots x_n$ donde $x_k \in I_k$ coincide con el conjunto*

$$I_1 \cdots I_n := \{\text{sumas finitas } \sum_i x_{i_1} \cdots x_{i_n} \mid x_{i_k} \in I_k\}$$

*y se llama el **producto** de los ideales $I_1, \ldots, I_n$.*

2) *Si $I_1, \ldots, I_n$ son ideales bilaterales, entonces*

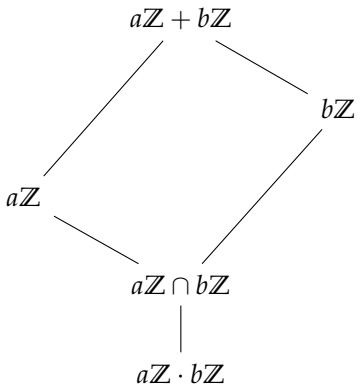
$$I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n.$$

Demostración. Por ejemplo, en el caso de ideales izquierdos, hay que considerar las sumas $\sum_i r_i\, x_{i_1} \cdots x_{i_n}$ donde $r_i \in R$, pero I_1 es un ideal, así que $r_i\, x_{i_1} \in I_1$.

Si todo I_k es un ideal bilateral, tenemos $x_{i_1} \cdots x_{i_k} \cdots x_{i_n} \in I_k$ para todo $k = 1, \ldots, n$, así que $I_1 \cdots I_n \subseteq I_k$ para todo k. ■

11.7.9. Ejemplo. Para dos ideales $a\mathbb{Z}, b\mathbb{Z} \subseteq \mathbb{Z}$ tenemos

$$\begin{aligned} a\mathbb{Z} + b\mathbb{Z} &= d\mathbb{Z}, \quad d = \operatorname{mcd}(a,b), \\ a\mathbb{Z} \cdot b\mathbb{Z} &= ab\mathbb{Z}, \\ a\mathbb{Z} \cap b\mathbb{Z} &= m\mathbb{Z}, \quad m = \operatorname{mcm}(a,b). \end{aligned}$$



▲

11.7.10. Definición. Sea R un anillo y sea $I \subseteq R$ un ideal bilateral. Para $n = 1, 2, 3, \ldots$ la n-ésima potencia de I se define mediante

$$I^n := \underbrace{I \cdots I}_{n} = \{\text{sumas finitas } \sum_i x_{i_1} \cdots x_{i_n} \mid x_{i_k} \in I\}$$

que es equivalente a la definición inductiva

$$I^1 := I, \quad I^n := I \cdot I^{n-1}.$$

11.7.11. Ejemplo. Sea k un cuerpo y sea $k[X]$ el anillo de polinomios correspondiente. El ideal generado por X en $k[X]$ viene dado por

$$I := (X) = \{f \in k[X] \mid \deg f \geq 1\} \cup \{0\}.$$

Luego, se ve que

$$I^n = (X^n) = \{f \in k[X] \mid \deg f \geq n\} \cup \{0\}.$$

▲

11.7.12. Ejemplo. En el anillo $\mathbb{Z}[X]$ consideremos el ideal $I := (2, X)$ generado por los elementos 2 y X. Es el ideal de los polinomios con el término constante par:

$$(2, X) = \{2f + Xg \mid f, g \in \mathbb{Z}[X]\} = \{a_n X^n + a_{n-1} X + \cdots + a_1 X + a_0 \mid n \geq 0,\ a_i \in \mathbb{Z},\ a_0 \text{ es par}\}.$$

Luego,

$$I^2 = \Big\{\text{sumas finitas } \sum_i f_i g_i \;\Big|\; f_i, g_i \in I\Big\}.$$

En particular, dado que $2 \in I$ y $X \in I$, tenemos $4, X^2 \in I^2$, y por lo tanto $X^2 + 4 \in I^2$. Notamos que el polinomio $X^2 + 4$ no puede ser escrito como un producto fg donde $f, g \in I$. ▲

11.7.13. Ejemplo. Sea k un cuerpo. Para una colección de polinomios $f_i \in k[X_1, \ldots, X_n]$ consideremos el conjunto de sus ceros comunes en $\mathbb{A}^n(k)$:

$$V(\{f_i\}_{i\in I}) := \{x \in \mathbb{A}^n(k) \mid f_i(x) = 0 \text{ para todo } i \in I\}.$$

Diferentes colecciones $\{f_i\}_{i\in I}$ pueden dar el mismo conjunto de los ceros. Para resolver este problema, podemos definir para todo ideal $J \subseteq k[X_1, \ldots, X_n]$

$$V(J) := \{x \in \mathbb{A}^n(k) \mid f(x) = 0 \text{ para todo } f \in J\}.$$

Ahora

$$V(\{f_i\}_{i\in I}) = V((f_i)_{i\in I})$$

donde $(f_i)_{i\in I}$ denota el ideal en $k[X_1, \ldots, X_n]$ generado por los polinomios f_i. En efecto, en general, la inclusión $\{f_i\}_{i\in I} \subseteq (f_i)_{i\in I}$ implica que $V(\{f_i\}_{i\in I}) \supseteq V((f_i)_{i\in I})$. Viceversa, si $x \in V(\{f_i\}_{i\in I})$, entonces $f_i(x) = 0$ para todo i, y por ende todas las sumas finitas $\sum_i g_i f_i$ se anulan en x. ▲

Los ejemplos 11.6.9 y 11.7.13 nos dan dos operaciones I y V:

$$\{\text{ideales } J \subseteq k[X_1, \ldots, X_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{subconjuntos } X \subseteq \mathbb{A}^n(k)\}$$

Vamos a ver algunas relaciones entre ellas en los ejercicios 11.19 y 11.20. Su estudio pertenece al terreno de la geometría algebraica. Para una introducción, el lector puede consultar el libro [Ful2008].

11.8 El núcleo de un homomorfismo de anillos

Un ejemplo importante de ideales bilaterales es el núcleo de un homomorfismo de anillos.

11.8.1. Observación. *Sea $f\colon R \to S$ un homomorfismo de anillos. Entonces, el conjunto*

$$\ker f := \{x \in R \mid f(x) = 0\}$$

*es un ideal bilateral en R, llamado el **núcleo** de f.*

Note que en la teoría de grupos, si $f\colon G \to H$ es un homomorfismo, entonces $\ker f$ es un *subgrupo normal* de G. Para un homomorfismo de anillos $f\colon R \to S$, el núcleo $\ker f$ no es un *subanillo* de R, sino un *ideal*.

Demostración. Un homomorfismo de anillos es en particular de los grupos abelianos correspondientes, y ya sabemos que el núcleo es un subgrupo abeliano. Falta comprobar que para cualesquiera $x \in \ker f$ y $r \cdot R$ se cumple $rx, xr \in \ker f$. En efecto, si $f(x) = 0$, entonces

$$f(rx) = f(r)\,f(x) = f(r) \cdot 0 = 0, \quad f(xr) = f(x)\,f(r) = 0 \cdot f(r) = 0.$$

■

11.8.2. Observación. *Un homomorfismo de anillos $f\colon R \to S$ es inyectivo (es decir, un monomorfismo) si y solo si* $\ker f = 0$.

Demostración. Ya lo verificamos para homomorfismos de grupos abelianos. ■

11.8.3. Observación. *Sea k un cuerpo y R un anillo no nulo. Entonces, todo homomorfismo $f\colon k \to R$ es inyectivo.*

Demostración. Si $R \neq 0$, entonces $f(1_k) = 1_R \neq 0$ y $1_k \notin \ker f$. Pero las únicas opciones son $\ker f = 0$ y $\ker f = k$. Entonces, $\ker f = 0$. ■

11.9 Anillos cociente

11.9.1. Definición. Sea R un anillo y sea $I \subseteq R$ un ideal bilateral. El **anillo cociente** correspondiente R/I es el grupo abeliano cociente R/I con la multiplicación definida por

$$(x + I) \cdot (y + I) := (xy + I).$$

Hay que verificar que el producto está bien definido. Supongamos que $x + I = x' + I$; es decir, $x - x' \in I$. Luego, $xy - x'y = (x - x')\, y \in I$, dado que I es un ideal derecho, y esto implica que $xy + I = x'y + I$. De la misma manera, si $y + I = y' + I$, esto significa que $y - y' \in I$. Esto implica que $xy - xy' = x\,(y - y') \in I$, puesto que I es un ideal izquierdo. De aquí se sigue que $xy + I = xy' + I$. Notamos que en este argumento es importante que I sea un ideal *bilateral*[*].

Dejo al lector verificar que los axiomas de anillo para el cociente R/I se siguen de los axiomas correspondientes para R.

11.9.2. Ejemplo. En todo anillo R hay dos ideales evidentes: $I = 0$ e $I = R$. Al desarrollar las definiciones, se ve que $R/0 \cong R$ y $R/R = 0$. ▲

11.9.3. Ejemplo. El cociente del anillo $\mathbb{Z}$ por el ideal $n\mathbb{Z}$ es el anillo $\mathbb{Z}/n\mathbb{Z}$ de los restos módulo n. ▲

11.9.4. Ejemplo. Tenemos $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$. En efecto, puesto que $X^2 \equiv -1 \pmod{X^2 + 1}$ en el cociente, se ve que los elementos de $\mathbb{R}[X]/(X^2 + 1)$ pueden ser representados por los polinomios $b\,X + a$, donde $a, b \in \mathbb{R}$. Luego,

$$(b\,X + a)\,(d\,X + c) = bd\,X^2 + (bc + ad)\,X + ac \equiv (ac - bd) + (bc + ad)\,X \pmod{X^2 + 1}.$$

Esta fórmula corresponde a la multiplicación compleja, y por ende se tiene un isomorfismo

$$\begin{aligned} \mathbb{R}[X]/(X^2 + 1) &\xrightarrow{\cong} \mathbb{C} \\ b\,X + a &\mapsto a + b\sqrt{-1}. \end{aligned}$$

▲

[*] De la misma manera, el producto sobre el grupo cociente G/H está bien definido solo cuando H es un subgrupo normal (véase el capítulo 7).

11.9.5. Ejemplo (El cuerpo de cuatro elementos). Calculemos $\mathbb{F}_2[X]/(X^2+X+1)$. Puesto que $X^2 \equiv X+1 \pmod{X^2+X+1}$, todos los elementos del cociente pueden ser representados por los polinomios de grado ≤ 1 en $\mathbb{F}_2[X]$:

$$\overline{0}, \quad \overline{1}, \quad \overline{X}, \quad \overline{X+1}.$$

La tabla de adición correspondiente viene dada por

$+$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{X+1}$	$\overline{X}$
$\overline{X}$	$\overline{X}$	$\overline{X+1}$	$\overline{0}$	$\overline{1}$
$\overline{X+1}$	$\overline{X+1}$	$\overline{X}$	$\overline{1}$	$\overline{0}$

Notamos que este grupo es isomorfo al grupo de Klein $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. La tabla de multiplicación viene dada por

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{X}$	$\overline{0}$	$\overline{X}$	$\overline{X+1}$	$\overline{1}$
$\overline{X+1}$	$\overline{0}$	$\overline{X+1}$	$\overline{1}$	$\overline{X}$

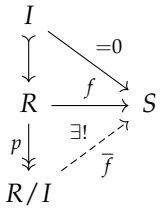
Se ve que todo elemento no nulo es invertible, así que $\mathbb{F}_2[X]/(X^2+X+1)$ es un cuerpo de cuatro elementos. Su grupo de elementos no nulos es de orden 3 y en particular es cíclico. Esto coincide con el resultado del capítulo 7 que dice que si k es un cuerpo, entonces todo subgrupo finito de $k^\times$ es necesariamente cíclico. ▲

Más adelante en el curso vamos a construir todos los cuerpos finitos.

11.9.6. Proposición (Propiedad universal del anillo cociente). *Sea $I \subseteq R$ un ideal bilateral. Sea*

$$\begin{aligned} p\colon R &\twoheadrightarrow R/I, \\ x &\mapsto x+I \end{aligned}$$

la proyección canónica sobre el anillo cociente. Si $f\colon R \to S$ es un homomorfismo de anillos tal que $I \subseteq \ker f$, entonces f se factoriza de modo único por R/I: existe un homomorfismo único $\overline{f}\colon R/I \to S$ tal que $f = \overline{f} \circ p$.



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

$$x + I \mapsto f(x).$$

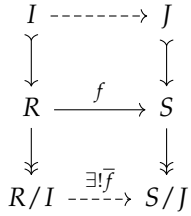
Es una aplicación bien definida: si $x + I = x' + I$ para algunos $x, x' \in R$, entonces $x - x' \in I$, luego $x - x' \in \ker f$ y

$$f(x - x') = 0 \iff f(x) = f(x').$$

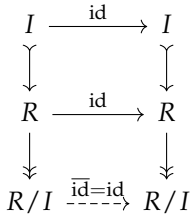
La aplicación $\overline{f}$ es un homomorfismo de anillos, puesto que f lo es. ■

11.9.7. Corolario (Funtorialidad del cociente).

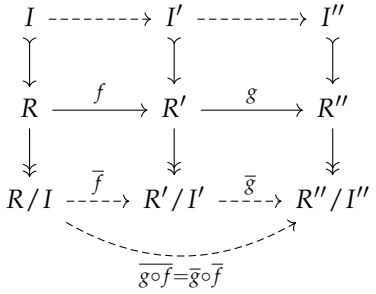
1) *Sea $f\colon R \to S$ un homomorfismo de anillos. Sean $I \subseteq R$ y $J \subseteq S$ ideales bilaterales. Supongamos que $f(I) \subseteq J$. Entonces f induce un homomorfismo canónico $\overline{f}\colon R/I \to S/J$ que conmuta con las proyecciones canónicas:*



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



3) *Sean $f\colon R \to R'$ y $g\colon R' \to R''$ dos homomorfismos de anillos y sean $I \subseteq R$, $I' \subseteq R'$, $I'' \subseteq R''$ ideales bilaterales tales que $f(I) \subseteq I'$ y $g(I') \subseteq I''$. Entonces, $\overline{g \circ f} = \overline{g} \circ \overline{f}$:*

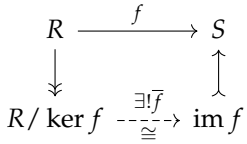


Demostración. En 1) la flecha $\overline{f}$ existe y es única gracias a la propiedad universal de R/I aplicada a la composición $R \xrightarrow{f} S \twoheadrightarrow S/J$. Los resultados de 2) y 3) siguen de la unicidad del homomorfismo inducido sobre los grupos cociente. ■

11.9.8. Proposición (Primer teorema de isomorfía). *Sea $f\colon R \to S$ un homomorfismo de anillos. Entonces, existe un isomorfismo canónico*

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

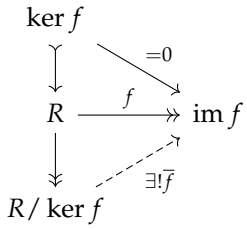
que hace parte del diagrama conmutativo



Descifremos el diagrama: la flecha $R \twoheadrightarrow R/\ker f$ es la proyección canónica $x \mapsto x + \ker f$ y la flecha $\operatorname{im} f \rightarrowtail S$ es la inclusión de subanillo, así que el isomorfismo $\overline{f}$ necesariamente viene dado por

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

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



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

$$f(x) = f(y) \iff x - y \in \ker f \iff x + \ker f = y + \ker f.$$

■

11.9.9. Ejemplo. Consideremos el homomorfismo de evaluación

$$\begin{aligned} f\colon \mathbb{R}[X] \hookrightarrow \mathbb{C}[X] &\to \mathbb{C}, \\ f &\mapsto f(\sqrt{-1}). \end{aligned}$$

Es visiblemente sobreyectivo. Su núcleo consiste en los polinomios en $\mathbb{R}[X]$ que tienen $\sqrt{-1}$ como su raíz; es decir, los polinomios divisibles por X^2+1. Entonces, $\ker f = (X^2+1)$. Podemos concluir que $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$. ▲

11.9.10. Ejemplo. Sea p un número primo. Consideremos el anillo

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; p \nmid b \right\}.$$

Este es un subanillo de $\mathbb{Q}$. Consideremos la aplicación

$$\begin{aligned} f \colon \mathbb{Z}_{(p)} &\to \mathbb{Z}/p^k\mathbb{Z}, \\ \frac{a}{b} &\mapsto [a]_{p^k} [b]_{p^k}^{-1} \end{aligned}$$

que a una fracción $\frac{a}{b} \in \mathbb{Z}_{(p)}$ asocia el producto del resto $[a]_{p^k}$ por el inverso multiplicativo $[b]_{p^k}^{-1}$ (que existe, dado que $p \nmid b$). Notamos que la aplicación está bien definida: si $\frac{a}{b} = \frac{a'}{b'}$, entonces $[a]_{p^k} [b]_{p^k}^{-1} = [a']_{p^k} [b']_{p^k}^{-1}$. Esto es un homomorfismo de anillos: tenemos

$$f\left(\frac{1}{1}\right) = [1]_{p^k} [1]_{p^k}^{-1} = [1]_{p^k},$$

$$\begin{aligned} f\left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) = f\left(\frac{a_1 b_2 + a_2 b_1}{b_1 b_2}\right) &= [a_1 b_2 + a_2 b_1]_{p^k} [b_1 b_2]_{p^k}^{-1} = \left([a_1]_{p^k} [b_2]_{p^k} + [a_2]_{p^k} [b_1]_{p^k}\right) [b_1]_{p^k}^{-1} [b_2]_{p^k}^{-1} \\ &= [a_1]_{p^k} [b_1]_{p^k}^{-1} + [a_2]_{p^k} [b_2]_{p^k}^{-1} = f\left(\frac{a_1}{b_1}\right) + f\left(\frac{a_2}{b_2}\right), \end{aligned}$$

$$f\left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}\right) = f\left(\frac{a_1\, a_2}{b_1\, b_2}\right) = [a_1\, a_2]_{p^k} [b_1\, b_2]_{p^k}^{-1} = [a_1]_{p^k} [b_1]_{p^k}^{-1} [a_2]_{p^k} [b_2]_{p^k}^{-1} = f\left(\frac{a_1}{b_1}\right) \cdot f\left(\frac{a_2}{b_2}\right).$$

Este homomorfismo es sobreyectivo: para $[a]_{p^k} \in \mathbb{Z}/p^k\mathbb{Z}$ tenemos $f\left(\frac{a}{1}\right) = [a]_{p^k} [1]_{p^k}^{-1} = [a]_{p^k}$.
El núcleo viene dado por

$$\ker f = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} \;\middle|\; [a]_{p^k} [b]_{p^k}^{-1} = 0 \right\} = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} \;\middle|\; [a]_{p^k} = 0 \right\} = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} \;\middle|\; p^k \mid a \right\}.$$

Este es precisamente el ideal $p^k\mathbb{Z}_{(p)}$ generado por p^k. El primer teorema de isomorfía nos dice que

$$\mathbb{Z}_{(p)}/p^k\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^k\mathbb{Z}.$$

▲

Ahora vamos a formular el segundo y el tercer teorema de isomorfía, pero los dejo como un ejercicio.

11.9.11. Teorema (Segundo teorema de isomorfía). *Sean R un anillo, $S \subseteq R$ un subanillo y $I \subseteq R$ un ideal bilateral. Entonces,*

1) *$S + I := \{x + y \mid x \in S, y \in I\}$ es un subanillo de R;*

2) *I es un ideal bilateral en $S + I$;*

3) la aplicación

$$S \to (S+I)/I,$$
$$x \mapsto x+I$$

es un homomorfismo de anillos sobreyectivo que tiene como núcleo a $S \cap I$.

Luego, gracias al primer teorema de isomorfía,

$$S/(S \cap I) \cong (S+I)/I.$$

11.9.12. Teorema (Tercer teorema de isomorfía). *Sea R un anillo y sean $I \subseteq J \subseteq R$ ideales bilaterales. Entonces, la aplicación*

$$R/I \to R/J,$$
$$x+I \mapsto x+J$$

está bien definida y es un homomorfismo sobreyectivo que tiene como núcleo a

$$J/I := \{x+I \mid x \in J\} \subseteq R/I.$$

Luego, gracias al primer teorema de isomorfía,

$$(R/I)/(J/I) \cong R/J.$$

En fin, vamos a describir los ideales en el anillo cociente.

11.9.13. Teorema. *Sea R un anillo y sea $I \subseteq R$ un ideal bilateral. Denotemos por $p\colon R \to R/I$ la proyección sobre el anillo cociente dada por $x \mapsto x+I$. Hay una biyección*

$$\{\text{ideales bilaterales } J \subseteq R \text{ tales que } I \subseteq J\} \leftrightarrow \{\text{ideales bilaterales } \overline{J} \subseteq R/I\},$$
$$J \mapsto p(J) = J/I,$$
$$p^{-1}(\overline{J}) \leftarrow\!\shortmid \overline{J}.$$

Esta biyección preserva las inclusiones:

1) si $I \subseteq J_1 \subseteq J_2$, entonces $J_1/I \subseteq J_2/I$;

2) si $\overline{J_1} \subseteq \overline{J_2} \subseteq R/I$, entonces $p^{-1}(\overline{J_1}) \subseteq p^{-1}(\overline{J_2})$.

Demostración. El hecho de que las aplicaciones estén bien definidas sigue de 11.6.12. El homomorfismo $p\colon R \to R/I$ es sobreyectivo, así que para todo ideal $J \subseteq R$ su imagen $p(J)$ es un ideal en R/I. Para todo ideal $\overline{J} \subseteq R/I$ la preimagen $p^{-1}(\overline{J})$ es un ideal en R. Además, tenemos $0_{R/I} \in \overline{J}$ para todo ideal $\overline{J} \subseteq R/I$ y $p^{-1}(0_{R/I}) = I$, así que $I \subseteq p^{-1}(\overline{J})$.

Hay que ver que las aplicaciones $J \mapsto J/I$ y $\overline{J} \mapsto p^{-1}(\overline{J})$ son mutualmente inversas. Tenemos

$$p^{-1}(\overline{J})/I = \{x+I \mid x \in p^{-1}(\overline{J})\} = \{p(x) \mid p(x) \in \overline{J}\} = \overline{J}$$

y

$$p^{-1}(J/I) = \{x \in R \mid p(x) \in J/I\} = \{x \in R \mid x+I \in J/I\} = J.$$

Está claro que las dos aplicaciones preservan las inclusiones (esto es teoría de conjuntos elemental). ■

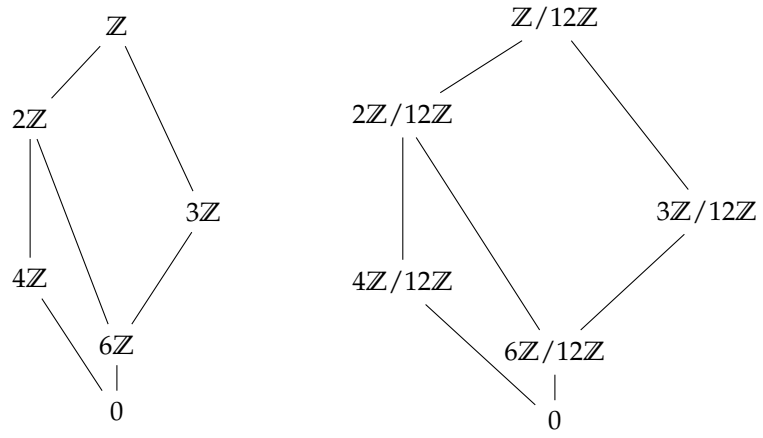
11.9.14. Ejemplo. Describamos los ideales en el anillo cociente $\mathbb{Z}/12\mathbb{Z}$. Según el teorema, estos corresponden a los ideales en $\mathbb{Z}$ que contienen a $12\mathbb{Z}$:

$$12\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}.$$

Dado que $12\mathbb{Z} \subseteq n\mathbb{Z}$ significa que $n \mid 12$, tenemos $n = 1, 2, 3, 4, 6, 12$. Entonces, los ideales en el cociente son

$$\begin{aligned}
\mathbb{Z}/12\mathbb{Z} &= \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\},\\
2\mathbb{Z}/12\mathbb{Z} &= \{[0], [2], [4], [6], [8], [10]\},\\
3\mathbb{Z}/12\mathbb{Z} &= \{[0], [3], [6], [9]\},\\
4\mathbb{Z}/12\mathbb{Z} &= \{[0], [4], [8]\},\\
6\mathbb{Z}/12\mathbb{Z} &= \{[0], [6]\},\\
12\mathbb{Z}/12\mathbb{Z} &= 0.
\end{aligned}$$

Tenemos las siguientes inclusiones de ideales:



▲

11.10 Productos de anillos

11.10.1. Definición. Sea R_i, $i \in I$ una familia anillos. El **producto** $\prod_{i\in I} R_i$ es el conjunto

$$\prod_{i\in I} R_i := \{(x_i)_{i\in I} \mid x_i \in R_i\}$$

con la suma y producto definidos término por término:

$$\begin{aligned}
(x_i)_{i\in I} + (y_i)_{i\in I} &:= (x_i + y_i)_{i\in I},\\
(x_i)_{i\in I} \cdot (y_i)_{i\in I} &:= (x_i\, y_i)_{i\in I}.
\end{aligned}$$

Ya que las operaciones se definen término por término, los axiomas de anillos para los R_i implican los axiomas correspondientes para el producto $\prod_{i\in I} R_i$. El cero es el elemento donde $x_i = 0$ para todo $i \in I$ y la identidad es el elemento donde $x_i = 1$ para todo $i \in I$. Notamos que las proyecciones naturales sobre cada uno de los R_i:

$$\begin{aligned} p_i \colon \prod_{i\in I} R_i &\twoheadrightarrow R_i, \\ (x_i)_{i\in I} &\mapsto x_i \end{aligned}$$

son homomorfismos de anillos[*].

Cuando $I = \{1, \dots, n\}$ es un conjunto finito, se usa la notación $R_1 \times \cdots \times R_n$.

11.10.2. Observación (Propiedad universal del producto). *Sea R_i, $i \in I$ una familia de anillos y S cualquier otro anillo. Para toda familia de homomorfismos de anillos $\{f_i \colon S \to R_i\}_{i\in I}$ existe un único homomorfismo de anillos $f \colon S \to \prod_{i\in I} R_i$ tal que $p_i \circ f = f_i$ para todo $i \in I$.*

$$\begin{array}{ccc} S & & \\ {\scriptstyle \exists!}\,\vdots\,{\scriptstyle f}\downarrow & \searrow^{f_i} & \\ \prod_{i\in I} R_i & \xrightarrow[p_i]{} & R_i \end{array}$$

En otras palabras, hay una biyección natural entre conjuntos

$$\begin{aligned} \left\{ \textit{homomorfismos } S \to \prod_{i\in I} R_i \right\} &\xrightarrow{\cong} \prod_{i\in I} \{\textit{homomorfismos } S \to R_i\}, \\ f &\mapsto p_i \circ f. \end{aligned}$$

Demostración. La condición $p_i \circ f = f_i$ implica que f viene dado por

$$s \mapsto (f_i(s))_{i\in I}.$$

Puesto que cada uno de los f_i es un homomorfismo de anillos, esta fórmula define un homomorfismo de anillos. ■

11.10.3. Observación. *Sean R_1, R_2, R_3 anillos.*

1) *Hay un isomorfismo natural de anillos $R_1 \times R_2 \cong R_2 \times R_1$.*
2) *Hay isomorfismos naturales $(R_1 \times R_2) \times R_3 \cong R_1 \times (R_2 \times R_3) \cong R_1 \times R_2 \times R_3$.*

Demostración. Ejercicio para el lector. Esto se puede deducir de la propiedad universal del producto (véase las pruebas correspondientes para los productos de grupos en el capítulo 10). ■

11.10.4. Observación ($R \rightsquigarrow R^\times$ preserva productos). *Sea R_i, $i \in I$ una familia de anillos. Hay un isomorfismo natural de grupos*

$$\left(\prod_{i\in I} R_i\right)^\times \cong \prod_{i\in I} R_i^\times.$$

[*]Note que las inclusiones $R_i \rightarrowtail \prod_{i\in I} R_i$ no son homomorfismos de anillos: la identidad no se preserva.

Demostración. Dado que el producto en el anillo $\prod_{i\in I} R_i$ está definido término por término, un elemento $(x_i)_{i\in I}$ es invertible en $\prod_{i\in I} R_i$ si y solo si cada x_i es invertible en R_i. ■

11.10.5. Digresión (*). Otra prueba más general y abstracta puede ser obtenida de 11.4.3. Para cualquier grupo G y anillo R hay una biyección natural

$$\{\text{homomorfismos de anillos } \mathbb{Z}[G] \to R\} \cong \{\text{homomorfismos de grupos } G \to R^\times\}.$$

Junto con la propiedad universal del producto de grupos y de anillos, esto nos da biyecciones *naturales* para cualquier grupo G

$$\begin{aligned}\left\{\text{homom. de grupos } G \to \prod_{i\in I} R_i^\times\right\} &\cong \prod_{i\in I}\{\text{homom. de grupos } G \to R_i^\times\}\\ \cong \prod_{i\in I}\{\text{homom. de anillos } \mathbb{Z}[G] \to R_i\} &\cong \left\{\text{homom. de anillos } \mathbb{Z}[G] \to \prod_{i\in I} R_i\right\}\\ &\cong \left\{\text{homom. de grupos } G \to \left(\prod_{i\in I} R_i\right)^\times\right\}.\end{aligned}$$

Esto es suficiente para concluir que $\prod_{i\in I} R_i^\times \cong \left(\prod_{i\in I} R_i\right)^\times$, pero omitiré los detalles. El punto es que el isomorfismo de 11.10.4 puede ser obtenido como una consecuencia formal de 11.4.3.

En el capítulo 10 hemos probado que si m y n son coprimos, entonces hay un isomorfismo de *grupos abelianos* $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. En realidad, esto es un isomorfismo de *anillos*, y ahora estamos listos para probar una generalización.

11.10.6. Teorema chino del resto. *Sea R un anillo conmutativo y sean $I_1, \ldots, I_n \subseteq R$ ideales tales que $I_k + I_\ell = R$ para $k \neq \ell$. Luego, hay un isomorfismo natural*

$$R/(I_1 \cdots I_n) \cong R/I_1 \times \cdots \times R/I_n.$$

Demostración. Denotemos por $p_k \colon R \to R/I_k$ las proyecciones canónicas $x \mapsto x + I_k$. Estas inducen un homomorfismo de anillos

$$\begin{aligned} R &\to R/I_1 \times \cdots \times R/I_n,\\ x &\mapsto (x + I_1, \ldots, x + I_n).\end{aligned}$$

Vamos a probar que es sobreyectivo y su núcleo es igual al producto de ideales $I_1 \cdots I_n$.

Escribamos $x \equiv y \pmod{I}$ para $x + I = y + I$. Para ver la sobreyectividad, necesitamos probar que para cualesquiera $x_1, \ldots, x_n \in R$ existe $x \in I$ tal que $x \equiv x_k \pmod{I_k}$ para todo $k = 1, \ldots, n$. Tenemos

$$R = R \cdots R = (I_1 + I_2)(I_1 + I_3) \cdots (I_1 + I_n) = I + I_2 I_3 \cdots I_n,$$

donde $I \subseteq I_1$. De hecho, al desarrollar el producto de sumas de ideales (vése el ejercicio 11.13), se ve que todos los términos pertenecen a I_1, salvo el último término $I_2 I_3 \cdots I_n$. Podemos concluir que

$$I_1 + I_2 I_3 \cdots I_n = R \tag{11.2}$$

En particular, existen $z_1 \in I_1$ e $y_1 \in I_2\, I_3 \cdots I_n$ tales que $z_1 + y_1 = 1$. Tenemos entonces $y_1 \equiv 1 \pmod{I_1}$ e $y_1 \equiv 0 \pmod{I_k}$ para $k \neq 1$. Usando el mismo argumento, podemos ver que existen $y_2, \ldots, y_n$ que satisfacen

$$y_k \equiv 1 \pmod{I_k}, \quad y_k \equiv 0 \pmod{I_\ell} \text{ si } \ell \neq k.$$

El elemento

$$x := x_1\, y_1 + \cdots + x_n\, y_n$$

cumple la condición deseada $x \equiv x_k \pmod{I_k}$ para todo $k = 1, \ldots, n$.

Ahora necesitamos calcular el núcleo del homomorfismo $x \mapsto (x + I_1, \ldots, x + I_n)$. Está claro que

$$\ker(x \mapsto (x + I_1, \ldots, x + I_n)) = I_1 \cap \cdots \cap I_n.$$

Vamos a probar que la hipótesis de que $I_k + I_\ell = R$ para $k \neq \ell$ implica que

$$I_1 \cap \cdots \cap I_n = I_1 \cdots I_n.$$

La inclusión que se cumple en cualquier caso es $I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n$, y hay que probar la inclusión inversa.

Procedamos por inducción sobre n. Supongamos que $n = 2$ e $I_1 + I_2 = R$. Luego, existen $y \in I_1$ y $z \in I_2$ tales que $y + z = 1$. Para todo $x \in I_1 \cap I_2$ se tiene

$$x = x\,(y + z) = xy + xz \in I_1\, I_2,$$

así que $I_1 \cap I_2 \subseteq I_1\, I_2$.

Para $n > 2$, supongamos que el resultado se cumple para $n - 1$ ideales. Entonces,

$$I_1 \cap \cdots \cap I_n = I_1 \cap (I_2 \cap I_3 \cap \cdots \cap I_n) = I_1 \cap I_2\, I_3 \cdots I_n.$$

Sin embargo, $I_1 + I_2\, I_3 \cdots I_n = R$ (véase (11.2)), así que $I_1 \cap I_2\, I_3 \cdots I_n = I_1\, I_2\, I_3 \cdots I_n$ por el caso de dos ideales. ■

11.10.7. Corolario. *Si $a_1, \ldots, a_n$ son números coprimos dos a dos, entonces hay un isomorfismo de anillos*

$$\mathbb{Z}/a_1 \cdots a_n\mathbb{Z} \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}.$$

Demostración. Para dos ideales $m\mathbb{Z}$ y $n\mathbb{Z}$ en $\mathbb{Z}$ tenemos $m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z}$ y $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, donde $d = \operatorname{mcd}(m, n)$. En particular, si m y n son coprimos, $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Se cumplen las condiciones del teorema anterior y se obtiene un isomorfismo

$$\mathbb{Z}/a_1 \cdots a_n\mathbb{Z} \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}.$$

■

11.10.8. Corolario.

1) *La función de Euler $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ es multiplicativa: si m y n son coprimos, entonces*

$$\phi(mn) = \phi(m)\,\phi(n).$$

2) *Si n se factoriza en números primos como $p_1^{k_1} \cdots p_\ell^{k_\ell}$, entonces*

$$\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_\ell^{k_\ell}) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\ell}\right).$$

Demostración. Si m y n son coprimos, el isomorfismo de anillos

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

induce un isomorfismo de grupos

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times,$$

como notamos en 11.10.4. De aquí sigue 1). La parte 2) se demuestra de la misma manera o por inducción usando la parte 1). La fórmula

$$\phi(p^k) = p^k \left(1 - \frac{1}{p}\right)$$

fue obtenida en el capítulo 4. ■

En el capítulo 10 hemos probado la multiplicatividad de la función ϕ de Euler usando que los elementos de $(\mathbb{Z}/n\mathbb{Z})^\times$ son los generadores del grupo cíclico $\mathbb{Z}/n\mathbb{Z}$. La prueba de arriba es más natural.

11.11 Ejercicios

Subanillos

Corto 1
23.08.18

Ejercicio 11.1. *Verifique que hay una cadena de subanillos*

$$\mathbb{Z}[\sqrt{5}] \subset \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big] \subset \mathbb{R}$$

donde

$$\mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}, \quad \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big] := \Big\{a + b\,\frac{1+\sqrt{5}}{2} \;\Big|\; a, b \in \mathbb{Z}\Big\}.$$

Ejercicio 11.2. *Consideremos el anillo de las funciones $f\colon \mathbb{R} \to \mathbb{R}$ respecto a las operaciones* ***punto por punto***

$$(f+g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

Demuestre que hay una cadena de subanillos

$$\begin{aligned}\{\textit{funciones constantes } \mathbb{R} \to \mathbb{R}\} &\subset \{\textit{funciones polinomiales } \mathbb{R} \to \mathbb{R}\} \\ &\subset \{\textit{funciones continuas } \mathbb{R} \to \mathbb{R}\} \subset \{\textit{funciones } \mathbb{R} \to \mathbb{R}\}.\end{aligned}$$

Homomorfismos de anillos

Ejercicio 11.3. *Sea R un anillo conmutativo y $M_n(R)$ el anillo de las matrices de $n \times n$ con coeficientes en R. ¿Cuáles aplicaciones de abajo son homomorfismos?*

1) *La proyección*

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \mapsto x_{11}.$$

2) *La traza*

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \mapsto x_{11} + x_{22} + \cdots + x_{nn}.$$

3) *El determinante $A \mapsto \det A$.*

Ejercicio 11.4. *Sea $f\colon R \to S$ un homomorfismo de anillos conmutativos y sea $n = 1, 2, 3, \ldots$*

1) *Demuestre que f induce un homomorfismo de los anillos de matrices correspondientes $f_*\colon M_n(R) \to M_n(S)$ dado por*

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \mapsto \begin{pmatrix} f(x_{11}) & f(x_{12}) & \cdots & f(x_{1n}) \\ f(x_{21}) & f(x_{22}) & \cdots & f(x_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ f(x_{n1}) & f(x_{n2}) & \cdots & f(x_{nn}) \end{pmatrix}.$$

2) *Demuestre que f induce un homomorfismo de grupos $\mathrm{GL}_n(f)\colon \mathrm{GL}_n(R) \to \mathrm{GL}_n(S)$.*

3) *Demuestre que el diagrama de homomorfismos de grupos*

$$\begin{array}{ccc} \mathrm{GL}_n(R) & \xrightarrow{\det} & R^\times \\ {\scriptstyle \mathrm{GL}_n(f)}\downarrow & & \downarrow{\scriptstyle f^\times} \\ \mathrm{GL}_n(S) & \xrightarrow[\det]{} & S^\times \end{array}$$

conmuta.

(Sugerencia: use la fórmula $\det(x_{ij}) = \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot x_{1\sigma(1)} \cdots x_{n\sigma(n)}$.)

Ejercicio 11.5. *Sea R un anillo conmutativo. Calcule $Z(M_n(R))$, el centro del anillo de las matrices de $n \times n$ con coeficientes en R.*
(Véanse los ejercicios donde calculamos el centro del grupo lineal general $\mathrm{GL}_n(R)$.)

Ejercicio 11.6.

1) *Demuestre que un isomorfismo de anillos $R \to S$ se restringe a un isomorfismo de grupos $R^\times \to S^\times$.*

2) *Demuestre que los anillos de polinomios $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$ no son isomorfos.*

Ejercicio 11.7. *Sea $f\colon R \to S$ un homomorfismo sobreyectivo de anillos. Demuestre que $f(Z(R)) \subseteq Z(S)$.*

Álgebra de grupo

Ejercicio 11.8. *Sea R un anillo conmutativo y G un grupo. Demuestre que*

$$\epsilon\colon R[G] \twoheadrightarrow R, \quad \sum_{g\in G} a_g\, g \mapsto \sum_{g\in G} a_g$$

es un homomorfismo sobreyectivo de anillos.

Ejercicio 11.9. *Sea R un anillo conmutativo y G un grupo finito. Consideremos $t := \sum_{g\in G} 1\cdot g \in R[G]$. Demuestre que $t^2 = |G|\, t$.*

Ejercicio 11.10. *En este ejercicio vamos a calcular el centro del álgebra de grupo $R[G]$. Consideremos*

$$x = \sum_{g\in G} a_g\, g \in R[G].$$

1) *Demuestre que $x \in Z(R[G])$ si y solamente si $h\,x = x\,h$ para todo $h \in G$.*

2) *Deduzca que $x \in Z(R[G])$ si y solamente si $a_g = a_{hgh^{-1}}$ para cualesquiera $g, h \in G$.*

Entonces, el centro de $R[G]$ consiste en los elementos $\sum_{g\in G} a_g\, g$ cuyos coeficientes a_g son constantes sobre las clases de conjugación de G.

Corto 2
30.08.18

Ejercicio 11.11. *Sea R un anillo conmutativo y G un grupo. Consideremos el homomorfismo*

$$\epsilon\colon R[G] \twoheadrightarrow R, \quad \sum_{g\in G} a_g\, g \mapsto \sum_{g\in G} a_g.$$

1) *Demuestre que el ideal $I_G := \ker\epsilon$ está generado por los elementos $g - e$ para $g \in G$. Este se llama el **ideal de aumento**.*

2) *En particular, si $G = C_n = \{e, g, \ldots, g^{n-1}\}$ es el grupo cíclico de orden n generado por g, demuestre que $\ker\epsilon$ está generado por el elemento $g - e$.*

Ideales

Ejercicio 11.12. *Sea R un anillo y $S \subseteq R$ un subanillo.*

1) *Demuestre que para todo ideal $I \subseteq R$ (izquierdo, derecho, bilateral) la intersección $I \cap S$ es un ideal en S (izquierdo, derecho, bilateral).*

2) *Encuentre un ejemplo de $S \subseteq R$ donde no todos los ideales de S son de la forma $I \cap S$.*

Ejercicio 11.13. *Sea R un anillo y sean I, J, K ideales bilaterales. Demuestre que $I(J + K) = IJ + IK$ y $(I + J)K = IK + JK$.*

Ejercicio 11.14. *Sea R un anillo. Para un ideal izquierdo $I \subseteq R$ definamos el **aniquilador** por*

$$\operatorname{Ann} I := \{r \in R \mid rx = 0 \text{ para todo } x \in I\}.$$

Demuestre que esto es un ideal bilateral en R.

Ejercicio 11.15. *Sea R un anillo conmutativo y $M_n(R)$ el anillo de matrices correspondiente.*

1) *Sea $I \subseteq R$ un ideal. Denotemos por $M_n(I)$ el conjunto de las matrices que tienen como sus entradas elementos de I. Verifique que $M_n(I)$ es un ideal bilateral en $M_n(R)$.*

2) *Sea $J \subseteq M_n(R)$ un ideal bilateral. Sea I el conjunto de los coeficientes que aparecen en la entrada $(1,1)$ de las matrices que pertenecen a J. Demuestre que I es un ideal en R.*

3) *Demuestre que $J = M_n(I)$. (Use las mismas ideas de 11.6.11.)*

Entonces, todo ideal en el anillo de matrices $M_n(R)$ es de la forma $M_n(I)$ para algún ideal $I \subseteq R$. Esto generaliza el resultado de 11.6.11.

Nilradical y radical

Ejercicio 11.16. *Sea R un anillo conmutativo.*

1) *Demuestre que el conjunto de nilpotentes*

$$N(R) := \{x \in R \mid x^n = 0 \text{ para algún } n = 1, 2, 3, \ldots\}$$

*es un ideal en R. Este se llama el **nilradical** de R.*

2) Demuestre que en el anillo no conmutativo $M_n(R)$ los nilpotentes no forman un ideal.

Ejercicio 11.17. *Sea R un anillo conmutativo. Supongamos que el nilradical de R es finitamente generado; es decir, $N(R) = (x_1, \ldots, x_n)$ donde x_i son algunos nilpotentes. Demuestre que en este caso $N(R)$ es un **ideal nilpotente**:*

$$N(R)^m := \underbrace{N(R) \cdots N(R)}_{m} = 0$$

para algún $m = 1, 2, 3, \ldots$

Ejercicio 11.18. *Sea R un anillo conmutativo y sea $I \subseteq R$ un ideal. Demuestre que*

$$\sqrt{I} := \{x \in R \mid x^n \in I \text{ para algún } n = 1, 2, 3, \ldots\}$$

*es también un ideal en R, llamado el **radical** de I. (Note que el nilradical $N(R) = \sqrt{(0)}$ es un caso particular.)*

Operaciones I y V

Ejercicio 11.19 (*). *Sea k un cuerpo. Sean J, J_1, J_2 ideales en $k[X_1, \ldots, X_n]$ y sean X, Y subconjuntos de $\mathbb{A}^n(k)$. Demuestre las siguientes relaciones.*

0) $I(\emptyset) = k[X_1, \ldots, X_n]$, $V(0) = \mathbb{A}^n(k)$, $V(1) = V(k[X_1, \ldots, X_n]) = \emptyset$.

1) Si $J_1 \subseteq J_2$, entonces $V(J_2) \subseteq V(J_1)$.

2) Si $X \subseteq Y$, entonces $I(Y) \subseteq I(X)$.

3) $V(J) = V(\sqrt{J})$.

4) $J \subseteq \sqrt{J} \subseteq IV(J)$. Demuestre que la inclusión es estricta para $J = (X^2 + 1) \subset \mathbb{R}[X]$.

5) $X \subseteq VI(X)$.

6) $VIV(J) = V(J)$ y $IVI(X) = I(X)$.

Ejercicio 11.20 (**).

1) Demuestre que $I(\mathbb{A}^n(k)) = (0)$ si k es un cuerpo infinito.

2) Note que $X^p - X \in I(\mathbb{A}^1(\mathbb{F}_p))$, así que esto es falso para cuerpos finitos.

Anillos cociente

Corto 3
06.09.18

Ejercicio 11.21. *Sea R un anillo conmutativo y sea $N(R)$ su nilradical. Demuestre que el anillo cociente $R/N(R)$ no tiene nilpotentes; es decir, $N(R/N(R)) = 0$.*

Ejercicio 11.22. *Sea R un anillo conmutativo y sea $I \subseteq R$ un ideal. Demuestre que $M_n(R)/M_n(I) \cong M_n(R/I)$.*

Ejercicio 11.23. *Sea k un cuerpo y $c \in k$. Consideremos el homomorfismo de evaluación*

$$ev_c \colon k[X] \to k, \quad f \mapsto f(c).$$

1) *Demuestre que $\ker ev_c = (X - c)$ es el ideal generado por el polinomio lineal $X - c$.*

2) *Deduzca del primer teorema de isomorfía que $k[X]/(X - c) \cong k$.*

3*) *De modo similar, demuestre que para $c_1, \ldots, c_n \in k$ se tiene $k[X_1, \ldots, X_n]/(X_1 - c_1, \ldots, X_n - c_n) \cong k$.*

Sugerencia: considere el automorfismo de $k[X_1, \ldots, X_n]$ dado por $X_i \mapsto X_i + c_i$.

Ejercicio 11.24. *Demuestre que el cociente $\mathbb{Q}[X]/(X^2 + 5)$ es isomorfo al cuerpo*

$$\mathbb{Q}(\sqrt{-5}) := \{x + y\sqrt{-5} \mid x, y \in \mathbb{Q}\}$$

(en particular, verifique que $\mathbb{Q}(\sqrt{-5})$ es un cuerpo).

Ejercicio 11.25. *Para el anillo de los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ demuestre que*

$$\mathbb{Z}[\sqrt{-1}]/(1 + \sqrt{-1}) \cong \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}[\sqrt{-1}]/(1 + 2\sqrt{-1}) \cong \mathbb{Z}/5\mathbb{Z}.$$

Ejercicio 11.26. *Consideremos el anillo de los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ y los ideales*

$$I = (1 + \sqrt{-1}), \quad J = (1 + 2\sqrt{-1}).$$

1) *Demuestre que $I + J = \mathbb{Z}[\sqrt{-1}]$.*

2) *Demuestre que $IJ = (1 - 3\sqrt{-1})$.*

Sugerencia: note que en cualquier anillo conmutativo, se tiene $(x) \cdot (y) = (xy)$ para cualesquiera $x, y \in R$.

3) *Demuestre que $\mathbb{Z}[\sqrt{-1}]/(1 - 3\sqrt{-1}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ usando el teorema chino del resto.*

Ejercicio 11.27. *Demuestre el segundo teorema de isomorfía para anillos.*

Ejercicio 11.28. *Demuestre el tercer teorema de isomorfía para anillos.*

Productos de anillos

Ejercicio 11.29. *Sean R y S anillos y sean $I \subseteq R$, $J \subseteq S$ ideales bilaterales.*

1) *Demuestre que*

$$I \times J := \{(x, y) \mid x \in I,\ y \in J\}$$

es un ideal bilateral en el producto $R \times S$.

2) *Demuestre que todos los ideales bilaterales en $R \times S$ son de esta forma.*
Sugerencia: para un ideal bilateral $A \subseteq R \times S$ considere $I = p_1(A)$ y $J = p_2(A)$ donde

$$\begin{array}{ccccc} R & \xleftarrow{p_1} & R \times S & \xrightarrow{p_2} & S \\ r & \longleftarrow\!\shortmid & (r,s) & \shortmid\!\longrightarrow & s \end{array}$$

son las proyecciones canónicas.

Ejercicio 11.30.

1) *Sean R y S dos anillos no nulos. Demuestre que el producto $R \times S$ tiene divisores de cero.*

2) *Demuestre que el producto de dos anillos no nulos nunca es un cuerpo.*
Sugerencia: para un ideal bilateral $A \subseteq R \times S$ considere $I = p_1(A)$ y $J = p_2(A)$ donde

$$\begin{array}{ccccc} R & \xleftarrow{p_1} & R \times S & \xrightarrow{p_2} & S \\ r & \longleftarrow\!\shortmid & (r,s) & \shortmid\!\longrightarrow & s \end{array}$$

son las proyecciones canónicas.

Capítulo 12
Anillos conmutativos

En este capítulo vamos a ver algunas nociones básicas del **álgebra conmutativa**, la rama de álgebra que se dedica al estudio de anillos conmutativos.

12.1 Ideales primos y maximales

12.1.1. Definición. Sea R un anillo conmutativo.
Se dice que un ideal $\mathfrak{p} \subset R$ es **primo** si se cumplen las siguientes condiciones:

1) $\mathfrak{p}$ es un ideal propio: $\mathfrak{p} \neq R$,

2) para cualesquiera $x, y \in R$ si $xy \in \mathfrak{p}$, entonces $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$.

Se dice que un ideal $\mathfrak{m} \subset R$ es **maximal** si se cumplen las siguientes condiciones:

1) $\mathfrak{m}$ es un ideal propio: $\mathfrak{m} \neq R$,

2) $\mathfrak{m}$ es **maximal** respecto a la inclusión: para todo ideal $I \subseteq R$ tal que $\mathfrak{m} \subseteq I \subseteq R$ se cumple $I = \mathfrak{m}$ o $I = R$.

12.1.2. Comentario. Las letras $\mathfrak{p}$ y $\mathfrak{m}$ son p y m *góticas*. Esta notación es común en álgebra conmutativa y viene de la tradición alemana.

12.1.3. Notación. Sea R un anillo conmutativo. El conjunto de los ideales primos en R se llama el **espectro** de R y se denota por $\operatorname{Spec} R$:

$$\operatorname{Spec} R := \{\mathfrak{p} \subset R \mid \mathfrak{p} \text{ ideal primo}\}.$$

El conjunto de los ideales maximales se llama el **espectro maximal** y lo vamos a denotar por[*]

$$\operatorname{Specm} R := \{\mathfrak{m} \subset R \mid \mathfrak{m} \text{ ideal maximal}\}.$$

12.1.4. Ejemplo. El anillo nulo 0 no tiene ideales propios y entonces $\operatorname{Spec} 0 = \operatorname{Specm} 0 = \emptyset$. Más adelante vamos a ver que si $R \neq 0$, entonces $\operatorname{Spec} R \neq \emptyset$ y $\operatorname{Specm} R \neq \emptyset$. ▲

[*] A diferencia de $\operatorname{Spec} R$, esta notación no es estándar. En la literatura también aparece Spec-max R y $\operatorname{Max} R$.

12.1.5. Ejemplo. En el anillo $\mathbb{Z}$ los ideales son de la forma $n\mathbb{Z}$ para $n = 0, 1, 2, 3, \ldots$ Tenemos $x \in n\mathbb{Z}$ si y solamente si $n \mid x$. Luego, $n\mathbb{Z}$ es un ideal primo si

1) $n \neq 1$,

2) para cualesquiera $x, y \in \mathbb{Z}$ si $n \mid xy$, entonces $n \mid x$ o $n \mid y$.

Estas condiciones se cumplen para $n = 0$. Si $n \neq 0$, estas condiciones se cumplen si y solo si $n = p$ es un número primo. Entonces,

$$\operatorname{Spec} \mathbb{Z} = \{0\} \cup \{p\mathbb{Z} \mid p \text{ primo}\}.$$

Un ideal $n\mathbb{Z}$ es maximal si

1) $n \neq 1$,

2) para todo ideal $m\mathbb{Z} \subseteq \mathbb{Z}$ tal que $n\mathbb{Z} \subseteq m\mathbb{Z} \subseteq \mathbb{Z}$ se cumple $n\mathbb{Z} = m\mathbb{Z}$ o $m\mathbb{Z} = \mathbb{Z}$.

Recordamos que $n\mathbb{Z} \subseteq m\mathbb{Z}$ si y solo si $m \mid n$. Entonces, la condición 2) dice que si $m \mid n$, entonces $m = n$ o $m = 1$. Esto significa precisamente que $n = p$ es un número primo. Entonces,

$$\operatorname{Specm} \mathbb{Z} = \{p\mathbb{Z} \mid p \text{ primo}\}.$$

▲

En particular, este ejemplo demuestra que los ideales primos generalizan la noción de números primos. Tenemos la siguiente caracterización de ideales primos.

12.1.6. Proposición. *Sea R un anillo conmutativo. Las siguientes condiciones son equivalentes:*

1) $\mathfrak{p} \subset R$ es un ideal primo,

2) el anillo cociente $R/\mathfrak{p}$ es un dominio de integridad.

Demostración. Por la definición, $\mathfrak{p} \subset R$ es un ideal primo si y solo si 1) $\mathfrak{p} \neq R$ y 2) $xy \in \mathfrak{p}$ implica $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$. En términos del anillo cociente $R/\mathfrak{p}$, esto es equivalente a

1) $R/\mathfrak{p} \neq 0$,

2) si $(x + \mathfrak{p})(y + \mathfrak{p}) := xy + \mathfrak{p} = \overline{0}$[*], entonces $x + \mathfrak{p} = \overline{0}$ o $y + \mathfrak{p} = \overline{0}$.

En otras palabras, $R/\mathfrak{p}$ es un anillo conmutativo no nulo que no tiene divisores de cero. Es precisamente la definición de dominio de integridad. ■

Los ideales maximales tienen una caracterización parecida.

12.1.7. Proposición. *Sea R un anillo conmutativo. Las siguientes condiciones son equivalentes:*

1) $\mathfrak{m} \subset R$ es un ideal maximal,

[*] Aquí $\overline{0}$ denota la clase lateral $0 + \mathfrak{p}$ en el cociente $R/\mathfrak{p}$.

2) *el anillo cociente* $R/\mathfrak{m}$ *es un cuerpo.*

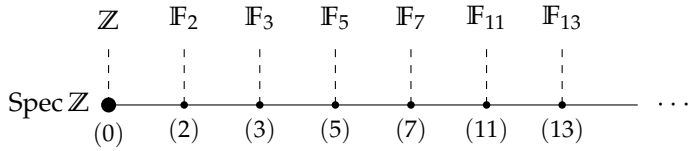
Demostración. Recordemos que un anillo conmutativo S es un cuerpo si y solo si sus únicos ideales son 0 y S. Además, tenemos la siguiente descripción de los ideales en el anillo cociente $R/\mathfrak{m}$:

$$\{\text{ideales } \overline{I} \subseteq R/\mathfrak{m}\} \xrightarrow{\cong} \{\text{ideales } \mathfrak{m} \subseteq I \subseteq R\},$$
$$\overline{I} \mapsto \pi^{-1}(\overline{I}),$$

donde $\pi\colon R \to R/\mathfrak{m}$ denota la proyección canónica $x \mapsto x + \mathfrak{m}$.

En particular, los ideales $\overline{0}$ y $R/\mathfrak{m}$ en el cociente corresponden a los ideales $I = \mathfrak{m}$ e $I = R$ en R. El anillo $R/\mathfrak{m}$ no tiene otros ideales si y solamente si $\mathfrak{m} \subseteq I \subseteq R$ implica $I = \mathfrak{m}$ o $I = R$. Esto es precisamente la condición de la definición de ideales maximales. ■

12.1.8. Ejemplo. El anillo cociente $\mathbb{Z}/n\mathbb{Z}$ es un dominio de integridad si y solo si $n = 0$ o $n = p$ es un número primo y es un cuerpo si y solo si $n = p$. Esto coincide con nuestra descripción de los ideales primos y maximales en $\mathbb{Z}$.



El espectro de $R = \mathbb{Z}$ con los anillos cociente correspondientes $R/\mathfrak{p}$

▲

12.1.9. Corolario. *Sea* R *un anillo conmutativo. Todo ideal maximal* $\mathfrak{m} \subset R$ *es un ideal primo.*

Demostración. Si $R/\mathfrak{m}$ es un cuerpo, en particular es un dominio de integridad. ■

12.1.10. Corolario. *Sea* R *un anillo conmutativo.*

1) *El ideal nulo* 0 *es primo en* R *si y solo si* R *es un dominio de integridad,*

2) *El ideal nulo* 0 *es maximal en* R *si y solo si* R *es un cuerpo.*

Demostración. $R/0 \cong R$. ■

12.1.11. Observación. *Sea* $f\colon R \to S$ *un homomorfismo de anillos conmutativos.*

1) *Si* $\mathfrak{p} \subset S$ *es un ideal primo, entonces* $f^{-1}(\mathfrak{p})$ *es un ideal primo en* R*. En otras palabras, un homomorfismo de anillos* $f\colon R \to S$ *induce una aplicación entre los espectros*

$$\operatorname{Spec} S \to \operatorname{Spec} R, \quad \mathfrak{p} \mapsto f^{-1}(\mathfrak{p}).$$

2) *Si* f *es sobreyectivo y* $\mathfrak{m} \subset S$ *es un ideal maximal, entonces* $f^{-1}(\mathfrak{m})$ *es un ideal maximal en* R*.*

Demostración. Para un ideal $I \subseteq S$ podemos considerar el homomorfismo

$$R \xrightarrow{f} S \xrightarrow{\pi} S/I$$

donde $\pi\colon s \mapsto s + I$ es la proyección sobre el anillo cociente. Tenemos

$$\ker(\pi \circ f) = \{r \in R \mid f(r) \in I\} = f^{-1}(I).$$

Luego, el primer teorema de isomorfía implica que

$$R/f^{-1}(I) \cong \operatorname{im}(\pi \circ f) \subseteq S/I.$$

Ahora en la parte 1), si $I = \mathfrak{p}$ es un ideal primo, entonces $S/\mathfrak{p}$ es un dominio de integridad, y luego $\operatorname{im}(\pi \circ f) \cong R/f^{-1}(\mathfrak{p})$ es también un dominio de integridad, siendo un subanillo. Esto implica que $f^{-1}(\mathfrak{p})$ es un ideal primo en R.

En la parte 2), si f es un homomorfismo sobreyectivo, entonces $\operatorname{im}(\pi \circ f) = S/I$. Si $I = \mathfrak{m}$ es un ideal maximal, entonces $S/\mathfrak{m}$ es un cuerpo, y luego $S/\mathfrak{m} \cong R/f^{-1}(\mathfrak{m})$ es también un cuerpo y por lo tanto el ideal $f^{-1}(\mathfrak{m})$ es maximal en R. ■

12.1.12. Comentario. En general, para un homomorfismo de anillos $f\colon R \to S$, si $\mathfrak{m} \subset S$ es un ideal maximal, entonces $f^{-1}(\mathfrak{m})$ no tiene por qué ser un ideal maximal en R. Considere por ejemplo la inclusión $f\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$. El ideal nulo 0 es maximal en $\mathbb{Q}$, pero $0 = f^{-1}(0)$ no es un ideal maximal en $\mathbb{Z}$. En este sentido los ideales primos se comportan mejor que los maximales.

12.1.13. Proposición. *Sean R un anillo conmutativo, $I \subseteq R$ un ideal y $\pi\colon R \to R/I$ la proyección correspondiente sobre el anillo cociente. La biyección*

$$\begin{aligned} \{\textit{ideales } \overline{J} \subseteq R/I\} &\leftrightarrow \{\textit{ideales } I \subseteq J \subseteq R\}, \\ \overline{J} &\mapsto \pi^{-1}(\overline{J}), \\ J &\leftarrow\!\shortmid J/I \end{aligned}$$

se restringe a las biyecciones

$$\begin{aligned} \operatorname{Spec} R/I &\leftrightarrow \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\}, \\ \operatorname{Specm} R/I &\leftrightarrow \{\mathfrak{m} \in \operatorname{Specm} R \mid I \subseteq \mathfrak{m}\}. \end{aligned}$$

Demostración. Para los ideales primos, ya vimos en 12.1.11 que si $\overline{\mathfrak{p}} \subset R/I$ es un ideal primo, entonces $\pi^{-1}(\overline{\mathfrak{p}}) \subset R$ es un ideal primo. Además, notamos que para un ideal primo $I \subseteq \mathfrak{p} \subset R$ el ideal $\mathfrak{p}/I \subset R/I$ es también primo. En efecto,

$$\mathfrak{p} \text{ es primo} \iff R/\mathfrak{p} \text{ es un dominio;} \quad \mathfrak{p}/I \text{ es primo} \iff (R/I)/(\mathfrak{p}/I) \text{ es un dominio,}$$

pero según el tercer teorema de isomorfía,

$$(R/I)/(\mathfrak{p}/I) \cong R/\mathfrak{p}.$$

De la misma manera, si $\overline{\mathfrak{m}} \subset R/I$ es un ideal maximal, entonces $\pi^{-1}(\overline{\mathfrak{m}})$ es un ideal maximal en R como notamos en 12.1.11 (usando que $\pi\colon R \to R/I$ es un homomorfismo sobreyectivo). Luego, para un ideal $I \subseteq \mathfrak{m} \subseteq R$ tenemos

$$\mathfrak{m} \text{ es maximal} \iff R/\mathfrak{m} \text{ es un cuerpo}; \quad \mathfrak{m}/I \text{ es maximal} \iff (R/I)/(\mathfrak{m}/I) \text{ es un cuerpo},$$

y de nuevo, es suficiente aplicar el tercer teorema de isomorfía

$$(R/I)/(\mathfrak{m}/I) \cong R/\mathfrak{m}.$$

■

El siguiente resultado establece la existencia de ideales maximales.

12.1.14. Proposición. *Todo anillo conmutativo no nulo posee un ideal maximal.*

Para probarlo, necesitamos el lema de Zorn. El lector puede consultar el apéndice B para revisar el enunciado.

Demostración de 12.1.14. Sea R un anillo conmutativo no nulo y sea $\mathcal{P}$ el conjunto de los ideales propios $I \subsetneq R$. Esto es un conjunto parcialmente ordenado respecto a la inclusión $I \subseteq J$. Por la hipótesis, $R \neq 0$, así que $0 \in \mathcal{P}$ y por lo tanto $\mathcal{P} \neq \emptyset$. Un elemento maximal en $\mathcal{P}$ sería precisamente un ideal maximal en R. Para deducir la existencia de un elemento maximal, tenemos que probar que toda cadena en $\mathcal{P}$ es acotada.

Una cadena en $\mathcal{P}$ es una colección de ideales propios $\mathcal{S} = \{I_\alpha\}$ donde $I_\alpha \subseteq I_\beta$ o $I_\beta \subseteq I_\alpha$ para cualesquiera α, β. Se ve que la unión $I := \bigcup_\alpha I_\alpha$ es también un ideal en R[*]. Dado que $1 \notin I_\alpha$ para todo α, tenemos $1 \notin I$, así que I es también un ideal propio e $I \in \mathcal{P}$. Tenemos $I_\alpha \subseteq I$ para todo α. Este ideal I es una cota superior para $\mathcal{S}$. ■

12.1.15. Corolario. *Sea R un anillo conmutativo y sea $I \subsetneq R$ un ideal propio. Entonces, R posee un ideal maximal $\mathfrak{m} \subset R$ tal que $I \subseteq \mathfrak{m}$.*

Demostración. Si $I \neq R$, entonces el anillo R/I no es nulo y según 12.1.14 posee un ideal maximal $\overline{\mathfrak{m}} \subset R/I$. Luego, como vimos en 12.1.13, este ideal corresponde a un ideal maximal $\mathfrak{m} = \pi^{-1}(\overline{\mathfrak{m}}) \subset R$ tal que $I \subseteq \mathfrak{m}$. ■

He aquí otro resultado sobre los ideales que puede ser demostrado mediante el lema de Zorn.

12.1.16. Proposición. *Sea R un anillo conmutativo. Entonces, su nilradical coincide con la intersección de los ideales primos en R:*

$$N(R) := \{r \in R \mid r^n = 0 \text{ para algún } n = 1, 2, 3, \ldots\} = \bigcap_{\mathfrak{p} \subset R \text{ primo}} \mathfrak{p}.$$

[*]De hecho, $0 \in I_\alpha$ para todo α, así que $0 \in I$. Para $x, y \in I$ tenemos $x \in I_\alpha$ e $y \in I_\beta$ para algunos α, β. Sin pérdida de generalidad, $I_\alpha \subseteq I_\beta$, así que $x + y \in I_\beta$, dado que I_β es un ideal. Para todo $r \in R$ y $x \in I$ se tiene $x \in I_\alpha$ para algún α, y luego $rx \in I_\alpha \subseteq I$.

Demostración. Sea $r \in N(R)$ un nilpotente. Luego, $r^n = 0$ para algún n y por ende $r^n \in \mathfrak{p}$ para cualquier ideal primo $\mathfrak{p} \subset R$, lo que implica que $r \in \mathfrak{p}$. Entonces, r pertenece a cualquier ideal primo. Esto demuestra la inclusión

$$N(R) \subseteq \bigcap_{\mathfrak{p} \subset R \text{ primo}} \mathfrak{p}.$$

Para probar la otra inclusión, vamos a ver que si $r \notin N(R)$, entonces existe un ideal primo $\mathfrak{p} \subset R$ tal que $r \notin \mathfrak{p}$. Supongamos entonces que $r \in R$ satisface $r^n \neq 0$ para todo $n = 1, 2, 3, \ldots$ Sea $\mathcal{P}$ el conjunto de los ideales $I \subset R$ que no contienen ninguna potencia de r:

$$U \cap I = \emptyset, \quad \text{donde } U := \{r^n \mid n = 1, 2, 3, \ldots\}.$$

Esto es un conjunto parcialmente ordenado respecto a la inclusión. Notamos que $0 \in \mathcal{P}$, así que $\mathcal{P} \neq \emptyset$. Sea $\{I_\alpha\}$ una cadena en $\mathcal{P}$. Entonces, $I := \bigcup_\alpha I_\alpha$ es también un ideal, como ya notamos en la demostración en 12.1.14. Dado que $U \cap I_\alpha = \emptyset$ para todo α, tenemos $U \cap I = \emptyset$. Esto significa que $I \in \mathcal{P}$. El ideal I es una cota superior para la cadena $\{I_\alpha\}$. Ahora el lema de Zorn implica que existe un elemento maximal en $\mathcal{P}$; es decir, un ideal $\mathfrak{p} \subset R$ tal que[*]

1) $U \cap \mathfrak{p} = \emptyset$,

2) si $I \subset R$ es otro ideal que satisface $U \cap I = \emptyset$ y $\mathfrak{p} \subseteq I$, entonces $I = \mathfrak{p}$.

La notación "$\mathfrak{p}$" no es una coincidencia: ahora vamos a probar que esto es un ideal primo. Primero, $r \notin \mathfrak{p}$, así que esto es un ideal propio. Además, si $xy \in \mathfrak{p}$ para algunos $x, y \in R$, necesitamos probar que $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$. Supongamos que $x \notin \mathfrak{p}$ e $y \notin \mathfrak{p}$ para obtener una contradicción. En este caso

$$(x) + \mathfrak{p} \supsetneq \mathfrak{p}, \quad (y) + \mathfrak{p} \supsetneq \mathfrak{p},$$

lo que implica que

$$U \cap ((x) + \mathfrak{p}) \neq \emptyset, \quad U \cap ((y) + \mathfrak{p}) \neq \emptyset;$$

es decir, que existen algunas potencias

$$r^m = sx + p \in (x) + \mathfrak{p}, \quad r^n = ty + q \in (y) + \mathfrak{p}$$

para algunos $m, n \geq 1$, $s, t \in R$, $p, q \in \mathfrak{p}$. Tenemos

$$r^{m+n} = (sx + p)(st + q) = stxy + sxq + tyq + pq.$$

Dado que $\mathfrak{p}$ es un ideal y $xy \in \mathfrak{p}$, este elemento pertenece a $\mathfrak{p}$. Sin embargo, esto contradice la propiedad que $U \cap \mathfrak{p} = \emptyset$. Podemos concluir que $\mathfrak{p}$ es un ideal primo.

Entonces, existe un ideal primo $\mathfrak{p} \subset R$ tal que $U \cap \mathfrak{p} = \emptyset$, y en particular $r \notin \mathfrak{p}$. ■

[*]Cuidado: es un ideal maximal *respecto a la propiedad* $U \cap I = \emptyset$, pero no es necesariamente un ideal maximal en el anillo R.

12.1.17. Ejemplo. Los ideales en el anillo $\mathbb{Z}/12\mathbb{Z}$ corresponden a los ideales en $\mathbb{Z}$ que contienen a $12\mathbb{Z}$:

$$\mathbb{Z},\ 2\mathbb{Z},\ 3\mathbb{Z},\ 4\mathbb{Z},\ 6\mathbb{Z},\ 12\mathbb{Z}.$$

Los ideales primos en $\mathbb{Z}/12\mathbb{Z}$ corresponden a los ideales primos en la lista de arriba, así que son

$$2\mathbb{Z}/12\mathbb{Z} = \{[0],[2],[4],[6],[8],[10]\},$$
$$3\mathbb{Z}/12\mathbb{Z} = \{[0],[3],[6],[9]\}.$$

Su intersección es

$$2\mathbb{Z}/12\mathbb{Z} \cap 3\mathbb{Z}/12\mathbb{Z} = 6\mathbb{Z}/12\mathbb{Z} = \{[0],[6]\}$$

y se ve que $[0]$ y $[6]$ son precisamente los nilpotentes en $\mathbb{Z}/12\mathbb{Z}$. ▲

12.1.18. Ejemplo. Si R es un dominio de integridad, entonces (0) es un ideal primo y la intersección de todos los ideales primos $\mathfrak{p} \subset R$ es necesariamente nula. Esto coincide con el hecho de que un dominio de integridad no pueda tener nilpotentes. ▲

12.1.19. Corolario. *Sea R un anillo conmutativo y sea $I \subseteq R$ un ideal. Entonces, el radical de I coincide con la intersección de todos los ideales primos que contienen a I:*

$$\sqrt{I} := \{r \in R \mid r^n \in I \text{ para algún } n = 1,2,3,\ldots\} = \bigcap_{\substack{\mathfrak{p} \subset R \text{ primo} \\ I \subseteq \mathfrak{p}}} \mathfrak{p}.$$

Demostración. Si $r^n \in I$ para algún n e $I \subseteq \mathfrak{p}$ para un ideal primo $\mathfrak{p} \subset R$, entonces $r \in \mathfrak{p}$. Esto demuestra que $\sqrt{I}$ pertenece a la intersección. Viceversa, supongamos que $r \in \mathfrak{p}$ para todo ideal primo $\mathfrak{p}$ tal que $I \subseteq \mathfrak{p}$. Recordemos que los ideales primos $I \subseteq \mathfrak{p} \subset R$ están en biyección con los ideales primos en el anillo cociente R/I. Esta biyección implica que $r + I \in \overline{\mathfrak{p}}$ para todo ideal primo $\overline{\mathfrak{p}} \subset R/I$. Entonces,

$$r + I \in \bigcap_{\overline{\mathfrak{p}} \subset R/I \text{ primo}} \overline{\mathfrak{p}} = N(R/I).$$

Pero para $r + I$ ser nilpotente en R/I significa precisamente que $r \in \sqrt{I}$. ■

He aquí otra aplicación más del lema de Zorn.

12.1.20. Teorema (I.S. Cohen). *Sea R un anillo conmutativo. Supongamos que todo ideal primo en R es finitamente generado. Entonces, todos los ideales en R son finitamente generados.*

Demostración. Vamos a ver que si en R hay un ideal que no es finitamente generado, entonces en R hay un ideal primo que no es finitamente generado.

Sea $\mathcal{P}$ el conjunto de los ideales que no son finitamente generados, parcialmente ordenado respecto a la inclusión. Por nuestra hipótesis, $\mathcal{P} \neq \emptyset$. Para una cadena de tales ideales $\{I_\alpha\}$ la unión $I := \bigcup_\alpha I_\alpha$ es también un ideal y no es finitamente generado. De hecho, si $I = (x_1,\ldots,x_n)$ para $x_1,\ldots,x_n \in R$, entonces $x_1,\ldots,x_n \in I_\alpha$ para algún α (usando que $\{I_\alpha\}$ es una cadena), lo que implicaría que el ideal $I_\alpha = I$ es finitamente generado.

Ahora según el lema de Zorn, existe un ideal $\mathfrak{p} \subset R$ que es maximal respecto a la propiedad de no ser finitamente generado:

1) $\mathfrak{p}$ no es finitamente generado,

2) si $\mathfrak{p} \subseteq I \subset R$ para otro ideal I que no es finitamente generado, entonces $I = \mathfrak{p}$.

Vamos a probar que $\mathfrak{p}$ es un ideal primo. Primero, es un ideal propio, puesto que $R = (1)$ es finitamente generado. Supongamos que $xy \in \mathfrak{p}$ para algunos $x, y \in R$, pero $x \notin \mathfrak{p}$ e $y \notin \mathfrak{p}$. Luego,

$$(x) + \mathfrak{p} \supsetneq \mathfrak{p},$$

así que $(x) + \mathfrak{p}$ es un ideal finitamente generado:

$$(x) + \mathfrak{p} = (y_1, \ldots, y_n)$$

para algunos $y_1, \ldots, y_n \in (x) + \mathfrak{p}$. En particular, tenemos

$$y_i = r_i\, x + p_i$$

para algunos $r_i \in R$, $p_i \in \mathfrak{p}$. Notamos que

$$(x) + \mathfrak{p} = (x, p_1, \ldots, p_n).$$

De hecho, dado que $y_i \in (x, p_1, \ldots, p_n)$ para todo i, se cumple $(y_1, \ldots, y_n) \subseteq (x, p_1, \ldots, p_n)$. Viceversa, $x \in (x) + \mathfrak{p}$ y $p_i \in \mathfrak{p} \subsetneq (x) + \mathfrak{p}$ para todo $i = 1, \ldots, n$, así que $(x, p_1, \ldots, p_n) \subseteq (x) + \mathfrak{p} = (y_1, \ldots, y_n)$.

Para un elemento arbitrario $p \in \mathfrak{p}$ tenemos en particular $p \in (x) + \mathfrak{p} = (x, p_1, \ldots, p_n)$, y por ende

$$p = r\, x + r_1\, p_1 + \cdots + r_n\, p_n \tag{12.1}$$

para algunos $r, r_1, \ldots, r_n \in R$. Luego,

$$r\, x = p - (r_1\, p_1 + \cdots + r_n\, p_n),$$

así que

$$r \in \{s \in R \mid sx \in \mathfrak{p}\}.$$

Notamos que el último conjunto es un ideal y denotémoslo por I. Tenemos $\mathfrak{p} \subsetneq I$, dado que $\mathfrak{p}$ es un ideal e $y \in I$, pero $y \notin \mathfrak{p}$ por nuestra hipótesis. Entonces, por la maximalidad de $\mathfrak{p}$, el ideal I debe ser finitamente generado:

$$I = (z_1, \ldots, z_k)$$

para algunos $z_1, \ldots, z_k \in I$. Esto significa que todo elemento de $\mathfrak{p}$ puede ser escrito como

$$p = (a_1\, z_1 + \cdots + a_k\, z_k)\, x + (r_1\, p_1 + \cdots + r_n\, p_n),$$

y por ende

$$\mathfrak{p} \subseteq (z_1 x, \ldots, z_k x, p_1, \ldots, p_n).$$

Pero por la definición de I, aquí $z_i x \in \mathfrak{p}$ para todo $i = 1, \ldots, k$ puesto que $z_i \in I$, así que

$$\mathfrak{p} = (z_1 x, \ldots, z_k x, p_1, \ldots, p_n).$$

Esto contradice el hecho de que $\mathfrak{p}$ no sea finitamente generado. Entonces, $\mathfrak{p}$ debe ser un ideal primo. ■

La prueba de arriba de que $\mathfrak{p}$ sea primo usa cierto truco, pero el argumento general es una aplicación típica del lema de Zorn.

12.2 Localización

En esta sección vamos a estudiar una construcción importante para anillos conmutativos llamada **localización**. La idea es bien sencilla y puede ser motivada por la construcción de los números racionales $\mathbb{Q}$ a partir de los números enteros $\mathbb{Z}$. Los elementos de $\mathbb{Q}$ son fracciones $\frac{a}{b}$, donde $a, b \in \mathbb{Z}$ y $b \neq 0$. Tenemos

$$\frac{a}{b} = \frac{a'}{b'} \iff ab' - a'b = 0. \tag{12.2}$$

La suma y producto de fracciones se definen mediante las fórmulas

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{12.3}$$

Notamos que si $\frac{a}{b} = \frac{a'}{b'}$, entonces

$$\frac{ad + cb}{bd} = \frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c}{d} = \frac{a'd + cb'}{b'd}.$$

En efecto,

$$(ad + cb)\, b'd - (a'd + cb')\, bd = ab'd^2 + \cancel{cbb'd} - a'bd^2 - \cancel{cb'bd} = d^2 \underbrace{(ab' - a'b)}_{=0} = 0.$$

De la misma manera, si $\frac{a}{b} = \frac{a'}{b'}$, entonces

$$\frac{ac}{bd} = \frac{a'c}{b'd}.$$

En efecto,

$$ac\, b'd - a'c\, bd = dc \underbrace{(ab' - a'b)}_{=0} = 0.$$

Esto verifica que las operaciones (12.3) están bien definidas: son compatibles con (12.2). Se ve que $\mathbb{Q}$ es un anillo conmutativo respecto a (12.3), y de hecho es un cuerpo.

Otro ejemplo relevante es el anillo

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ p \nmid b \right\}$$

para un primo fijo p. Este anillo consiste en las fracciones donde p no divide al denominador. Se ve que $\mathbb{Z}_{(p)}$ es un subanillo de $\mathbb{Q}$. Los elementos invertibles en $\mathbb{Z}_{(p)}$ son las fracciones $\frac{a}{b}$ donde $p \nmid a$ y $p \nmid b$. En este caso $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Nuestro objetivo es generalizar el cálculo de fracciones a cualquier anillo conmutativo R. Supongamos que queremos invertir ciertos elementos $u \in R$. En este caso hay que "extender" R a las fracciones $\frac{r}{u}$ donde u aparece en el denominador, así que $\left(\frac{u}{1}\right)^{-1} = \frac{1}{u}$. Antes de dar la construcción general, recordamos que si u y v son invertibles, entonces $u^{-1} v^{-1}$ es el inverso de uv, así que todo producto de elementos invertibles es también invertible.

12.2.1. Construcción. Sea R un anillo conmutativo y sea $U \subseteq R$ un **conjunto multiplicativo**; es decir, que satisface

a) $1 \in U$,

b) si $u, v \in U$, entonces $uv \in U$.

1) Consideremos la siguiente relación sobre el conjunto $R \times U$, motivada[*] por (12.2):

$$(r,u) \sim (r',u') \iff v\,(ru' - r'u) = 0 \text{ para algún } v \in U.$$

Esto es una relación de equivalencia: de hecho, tenemos $(r,u) \sim (r,u)$, puesto que

$$1 \cdot (ru - ru) = 0,$$

así que la relación es reflexiva. Si $(r,u) \sim (r',u')$, entonces $v\,(ru' - r'u) = 0$ para algún $v \in U$, y multiplicando esta identidad por -1, se obtiene $v\,(r'u - ru') = 0$, lo que significa que la relación es simétrica. En fin, supongamos que $(r,u) \sim (r',u')$ y $(r',u') \sim (r'',u'')$; es decir, que existen algunos $v, v' \in U$ tales que

$$v\,(ru' - r'u) = 0, \quad v'\,(r'u'' - r''u') = 0.$$

Ahora

$$\begin{aligned} 0 = v'u'' \cdot v\,(ru' - r'u) + uv \cdot v'\,(r'u'' - r''u') &= ru'u''vv' - \cancel{r'uu''vv'} + \cancel{r'uu''vv'} - r''uu'vv' \\ &= vv'u'\,(ru'' - r''u), \end{aligned}$$

donde $vv'u' \in U$, puesto que $v, v', u' \in U$, y luego $(r,u) \sim (r'',u'')$. Esto demuestra que la relación es transitiva.

2) Denotemos por $\frac{r}{u}$ la clase de equivalencia de (r,u) y sea

$$R[U^{-1}] := R \times U / \sim = \left\{ \frac{r}{u} \;\middle|\; r \in R,\ u \in U \right\}$$

el conjunto de las clases de equivalencia. Definamos el producto y la suma en $R[U^{-1}]$ mediante

$$\frac{r_1}{u_1} + \frac{r_2}{u_2} := \frac{r_1u_2 + r_2u_1}{u_1u_2}, \quad \frac{r_1}{u_1} \cdot \frac{r_2}{u_2} := \frac{r_1r_2}{u_1u_2}.$$

Comprobemos que estas operaciones están bien definidas sobre las clases de equivalencia. Supongamos que

$$\frac{r_1}{u_1} = \frac{r_1'}{u_1'} \iff v\,(r_1u_1' - r_1'u_1) = 0 \text{ para algún } v \in U.$$

Luego,

$$\begin{aligned} &v\,((r_1u_2 + r_2u_1)\,u_1'u_2 - (r_1'u_2 + r_2u_1')\,u_1\,u_2) \\ &\qquad = r_1u_1'u_2^2v + \cancel{r_2u_1u_1'u_2v} - r_1'u_1u_2^2v - \cancel{r_2u_1u_1'u_2v} = u_2^2\,v\,(r_1u_1' - r_1'u_1) = 0, \end{aligned}$$

[*] En (12.2) no aparece el múltiplo v, pero este será necesario para probar la transitividad de la relación. Sin embargo, si R es un dominio de integridad y $0 \notin U$, este múltiplo siempre puede ser cancelado.

lo que significa que

$$\frac{r_1u_2 + r_2u_1}{u_1u_2} = \frac{r_1'u_2 + r_2u_1'}{u_1'u_2}.$$

De la misma manera,

$$v\left(r_1r_2u_1'u_2 - r_1'r_2u_1u_2\right) = r_2\, u_1 \underbrace{v\left(r_1u_1' - r_1'u_1\right)}_{=0} = 0,$$

así que

$$\frac{r_1r_2}{u_1u_2} = \frac{r_1'r_2}{u_1'u_2}.$$

3) Notamos que $R[U^{-1}]$ es un anillo conmutativo respecto a estas dos operaciones, puesto que R es un anillo conmutativo (el lector que está convencido de que los números racionales forman un anillo conmutativo puede saltar estos cálculos).

   - La adición es asociativa: para cualesquiera $\frac{r_1}{u_1}, \frac{r_2}{u_2}, \frac{r_3}{u_3} \in R[U^{-1}]$ tenemos

   $$\left(\frac{r_1}{u_1} + \frac{r_2}{u_2}\right) + \frac{r_3}{u_3} = \frac{r_1u_2 + r_2u_1}{u_1u_2} + \frac{r_3}{u_3} = \frac{\left(r_1u_2 + r_2u_1\right)u_3 + r_3u_1u_2}{u_1u_2u_3} = \frac{r_1u_2u_3 + r_2u_1u_3 + r_3u_1u_2}{u_1u_2u_3},$$

   y

   $$\frac{r_1}{u_1} + \left(\frac{r_2}{u_2} + \frac{r_3}{u_3}\right) = \frac{r_1}{u_1} + \frac{r_2u_3 + r_3u_2}{u_2u_3} = \frac{r_1u_2u_3 + \left(r_2u_3 + r_3u_2\right)u_1}{u_1u_2u_3} = \frac{r_1u_2u_3 + r_2u_3u_1 + r_3u_2u_1}{u_1u_2u_3},$$

   así que

   $$\left(\frac{r_1}{u_1} + \frac{r_2}{u_2}\right) + \frac{r_3}{u_3} = \frac{r_1}{u_1} + \left(\frac{r_2}{u_2} + \frac{r_3}{u_3}\right).$$

   - La multiplicación es asociativa: para cualesquiera $\frac{r_1}{u_1}, \frac{r_2}{u_2}, \frac{r_3}{u_3} \in R[U^{-1}]$ tenemos

   $$\left(\frac{r_1}{u_1} \cdot \frac{r_2}{u_2}\right) \cdot \frac{r_3}{u_3} = \frac{r_1}{u_1} \cdot \left(\frac{r_2}{u_2} \cdot \frac{r_3}{u_3}\right) = \frac{r_1r_2r_3}{u_1u_2u_3}.$$

   - La adición es conmutativa: para cualesquiera $\frac{r_1}{u_1}, \frac{r_2}{u_2} \in R[U^{-1}]$ se cumple

   $$\frac{r_1}{u_1} + \frac{r_2}{u_2} = \frac{r_2}{u_2} + \frac{r_1}{u_1} = \frac{r_1u_2 + r_2u_1}{u_1u_2}.$$

   - La multiplicación es conmutativa: para cualesquiera $\frac{r_1}{u_1}, \frac{r_2}{u_2} \in R[U^{-1}]$ se cumple

   $$\frac{r_1}{u_1} \cdot \frac{r_2}{u_2} = \frac{r_2}{u_2} \cdot \frac{r_1}{u_1} = \frac{r_1r_2}{u_1u_2}.$$

- La fracción $\frac{0}{1}$ es el elemento nulo: para todo $\frac{r}{u} \in R[U^{-1}]$ se cumple

$$\frac{0}{1} + \frac{r}{u} = \frac{0 \cdot u + r \cdot 1}{u} = \frac{r}{u}.$$

  Notamos que

$$\frac{r}{u} = \frac{0}{1} \iff v\,r = 0 \text{ para algún } v \in U.$$

  En particular, $\frac{0}{u} = \frac{0}{1}$ para cualquier $u \in U$.

- La fracción $\frac{1}{1}$ es la identidad: para todo $\frac{r}{u} \in R[U^{-1}]$ se cumple

$$\frac{1}{1} \cdot \frac{r}{u} = \frac{1 \cdot r}{1 \cdot u} = \frac{r}{u}.$$

  Notamos que

$$\frac{r}{u} = \frac{1}{1} \iff v\,(r - u) = 0 \text{ para algún } v \in U.$$

  En particular, $\frac{u}{u} = \frac{1}{1}$ para cualquier $u \in U$, y funciona la cancelación habitual en las fracciones:

$$\frac{ru'}{uu'} = \frac{r}{u}$$

  para cualesquiera $r \in R, u, u' \in U$.

- Para todo $\frac{r}{u} \in R[U^{-1}]$ existe el elemento opuesto que es la fracción $\frac{-r}{u}$:

$$\frac{r}{u} + \frac{-r}{u} = \frac{ru - ru}{ru} = \frac{0}{ru} = \frac{0}{1}.$$

- la multiplicación es distributiva respecto a la adición: para cualesquiera $\frac{r_1}{u_1}, \frac{r_2}{u_2}, \frac{r_3}{u_3} \in R[U^{-1}]$ se cumple

$$\frac{r_1}{u_1} \cdot \left(\frac{r_2}{u_2} + \frac{r_3}{u_3}\right) = \frac{r_1}{u_1} \cdot \frac{r_2}{u_2} + \frac{r_1}{u_1} \cdot \frac{r_3}{u_3}.$$

  En efecto,

$$\frac{r_1}{u_1} \cdot \left(\frac{r_2}{u_2} + \frac{r_3}{u_3}\right) = \frac{r_1}{u_1} \cdot \left(\frac{r_2 u_3 + r_3 u_2}{u_2 u_3}\right) = \frac{r_1 r_2 u_3 + r_1 r_3 u_2}{u_1 u_2 u_3}$$

  y

$$\frac{r_1 r_2}{u_1 u_2} + \frac{r_1 r_3}{u_1 u_3} = \frac{r_1 r_2 u_1 u_3 + r_1 r_3 u_1 u_2}{u_1^2 u_2 u_3} = \frac{u_1\,(r_1 r_2 u_3 + r_1 r_3 u_2)}{u_1\,(u_1 u_2 u_3)} = \frac{r_1 r_2 u_3 + r_1 r_3 u_2}{u_1 u_2 u_3}.$$

12.2.2. Definición. Para un anillo conmutativo R y un conjunto multiplicativo $U \subseteq R$, el anillo conmutativo $R[U^{-1}]$ se llama la **localización** de R en U.

Aunque la construcción de arriba no excluye las fracciones $\frac{r}{0}$, la presencia de 0 en los denoninadores implica que $R[U^{-1}] = 0$.

12.2.3. Observación. $R[U^{-1}] = 0$ *es el anillo trivial si y solo si* $0 \in U$.

Demostración. La localización es trivial si y solo si $\frac{1}{1} = \frac{0}{1}$; es decir, si $v\,(1 \cdot 1 - 0 \cdot 1) = 0$ para algún $v \in U$. Pero esto significa que $v = 0$. ■

12.2.4. Observación. *Supongamos que R es un dominio de integridad. Entonces, hay dos posibilidades:*

1) $0 \in U$, *y entonces* $R[U^{-1}] = 0$;

2) $0 \notin U$, *y entonces* $R[U^{-1}]$ *es también un dominio de integridad.*

Demostración. Supongamos que para $\frac{r_1}{u_1}, \frac{r_2}{u_2} \in R[U^{-1}]$ se tiene

$$\frac{r_1}{u_1}\,\frac{r_2}{u_2} = \frac{r_1 r_2}{u_1 u_2} = \frac{0}{1}.$$

Esto quiere decir que $v\,r_1\,r_2 = 0$ para algún $v \in U$. Si $0 \notin U$, entonces esto implica $r_1 = 0$ o $r_2 = 0$. ■

Es natural asociar a los elementos $r \in R$ las fracciones $\frac{r}{1} \in R[U^{-1}]$, pero en general la aplicación $r \mapsto \frac{r}{1}$ no es inyectiva.

12.2.5. Observación.

1) *La aplicación*

$$\phi\colon R \to R[U^{-1}], \quad r \mapsto \frac{r}{1}$$

es un homomorfismo de anillos.

2) *Tenemos*

$$\ker\phi = \left\{ r \in R \;\middle|\; \frac{r}{1} = \frac{0}{1} \right\} = \{ r \in R \mid v\,r = 0 \text{ para algún } v \in U \}.$$

3) *Si U no contiene divisores de cero, entonces* ϕ *es un monomorfismo y R es isomorfo al subanillo*

$$\operatorname{im}\phi = \left\{ \frac{r}{1} \;\middle|\; r \in R \right\} \subset R[U^{-1}].$$

4) *En particular, si R es un dominio de integridad y* $0 \notin U$, *entonces* ϕ *es un monomorfismo y R es isomorfo al subanillo* $\operatorname{im}\phi \subset R[U^{-1}]$.

Demostración. 1) y 2) está claro de las definiciones de arriba. La parte 3) sigue de 2). En fin, 4) es un caso especial de 3). ■

12.2.6. Ejemplo. Sea R un anillo conmutativo.

1) Para un elemento $x \in R$ consideremos

$$U := \{1, x, x^2.x^3, \ldots\}.$$

Este es un conjunto multiplicativo. La localización correspondiente se denota por

$$R[U^{-1}] =: R\Big[\frac{1}{x}\Big] \text{ o } R[x^{-1}] = \Big\{ \frac{r}{x^n} \;\Big|\; r \in R,\ n = 0, 1, 2, 3, \ldots \Big\}.$$

Por ejemplo, tenemos

$$\mathbb{Z}\Big[\frac{1}{n}\Big] := \Big\{ \frac{a}{n^k} \mid a \in \mathbb{Z},\ k = 0, 1, 2, 3, \ldots \Big\}.$$

Esta es la localización de $\mathbb{Z}$ en el conjunto de las potencias de n.

El resultado de 12.2.3 nos dice que $R[x^{-1}] = 0$ si y solo si x es un nilpotente.

2) Para un ideal $I \subseteq R$ consideremos $U := R \setminus I$. Entonces, U es un conjunto multiplicativo si $1 \in U$ y $u, v \in U$ implica $uv \in U$. Esto es equivalente a $I \neq R$ y que si $xy \in I$ para algunos $x, y \in R$, entonces $x \in I$ o $y \in i$; es decir, que $I = \mathfrak{p}$ es un ideal primo. En este caso la localización se denota por

$$R[(R \setminus \mathfrak{p})^{-1}] =: R_{\mathfrak{p}} = \Big\{ \frac{r}{u} \;\Big|\; r, u \in R,\ u \notin \mathfrak{p} \Big\}.$$

Por ejemplo, $\mathbb{Z}_{(p)}$ es la localización de $\mathbb{Z}$ en $U := \mathbb{Z} \setminus (p)$.

En general, si tomamos un subconjunto multiplicativo $U \subset R$, entonces $R \setminus U$ no tiene por qué ser un ideal (las condiciones sobre U se tratan de la multiplicación y no dicen nada sobre la adición), pero el ejercicio 12.8 nos dice que si $0 \notin U$, entonces existe un ideal primo $\mathfrak{p} \subset R$ tal que $U \cap \mathfrak{p} = \emptyset$.

3) Si R es un dominio de integridad, entonces el conjunto

$$U := R \setminus \{0\}$$

es multiplicativo. En este caso todo elemento no nulo en $R[U^{-1}]$ es invertible y este cuerpo se denota por

$$R[U^{-1}] =: K(R) = \Big\{ \frac{r}{s} \;\Big|\; r, s \in R, s \neq 0 \Big\}$$

y se llama el **cuerpo de fracciones** de R. La aplicación

$$\phi \colon R \to K(R), \quad r \mapsto \frac{1}{r}$$

es un monomorfismo. Notamos que R es un dominio de integridad si y solamente si el ideal nulo (0) es primo, y en este caso $K(R) = R_{\mathfrak{p}}$ donde $\mathfrak{p} = 0$, así que se trata de un caso muy particular de 2),

Por ejemplo, $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$.

▲

12.2.7. Proposición. *Sea R un dominio de integridad. Para todo ideal maximal $\mathfrak{m} \subset R$ identifiquemos R con el subanillo*

$$\left\{ \frac{r}{1} \;\middle|\; r \in R \right\}$$

de la localización

$$R_{\mathfrak{m}} := R[(R \setminus \mathfrak{m})^{-1}] = \left\{ \frac{r}{u} \;\middle|\; r, u \in R,\ u \notin \mathfrak{m} \right\}$$

y $R_{\mathfrak{m}}$ con el subanillo del cuerpo de fracciones

$$K(R) = \left\{ \frac{r}{s} \;\middle|\; r, s \in R,\ s \neq 0 \right\}.$$

Entonces,

$$\bigcap_{\substack{\mathfrak{m} \subset R \\ \text{maximal}}} R_{\mathfrak{m}} = R.$$

Demostración. Dado que $R \subseteq R_{\mathfrak{m}}$ para todo $\mathfrak{m} \subset R$, el anillo R está incluido en la intersección. En la otra dirección, sea $x \in K(R)$ un elemento tal que $x \notin R$. Consideremos el ideal

$$I := \{ r \in R \mid rx \in R \}.$$

Tenemos $1 \notin I$, así que I es un ideal propio. Luego, existe un ideal maximal $\mathfrak{m} \subset R$ tal que $I \subseteq \mathfrak{m}$. Supongamos que $x \in R_{\mathfrak{m}}$. Luego, $x = \frac{r}{u}$ para algunos $r, u \in R$, $u \notin \mathfrak{m}$. Tenemos entonces $u\,x = \frac{u}{1}\,\frac{r}{u} = \frac{r}{1} \in R$ y $u \in I$. Pero esto contradice nuestra elección de $\mathfrak{m}$. Entonces, $x \notin R_{\mathfrak{m}}$. ■

12.2.8. Ejemplo. Tenemos

$$\begin{aligned} \bigcap_{p \text{ primo}} \mathbb{Z}_{(p)} &= \bigcap_{p \text{ primo}} \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0,\ p \nmid b \right\} \\ &= \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0,\ p \nmid b \text{ para ningún primo } p \right\} = \mathbb{Z}. \end{aligned}$$

▲

Ahora vamos a ver otro ejemplo más de cuerpos de fracciones.

12.2.9. Ejemplo. Para un cuerpo k el anillo de polinomios $k[X]$ tiene como su cuerpo de fracciones el cuerpo de las **funciones racionales**

$$k(X) := \left\{ \frac{f}{g} \;\middle|\; f, g \in k[X],\ g \neq 0 \right\}$$

Recordemos que en el anillo de las series formales $k[\![X]\!]$ una serie $g = \sum_{i \geq 0} a_i\, X^i$ es invertible si y solamente si $a_0 \neq 0$. Sin embargo, para una serie no nula $\sum_{i \geq 0} a_i\, X^i$ donde $a_n \neq 0$ es el primer coeficiente no nulo se puede escribir

$$\sum_{i \geq 0} a_i\, X^i = X^n \sum_{i \geq n} a_i\, X^{i-n} =: X^n\, h,$$

donde h es invertible: existe $h^{-1} \in k[\![X]\!]$ tal que $h\,h^{-1} = 1$. Luego, en el cuerpo de fracciones de $k[\![X]\!]$ para $f, g \in k[\![X]\!]$, $g \neq 0$ se tiene

$$\frac{f}{g} = \frac{f}{X^n\,h} = \frac{f\,h^{-1}}{X^n\,h\,h^{-1}} = \frac{f\,h^{-1}}{X^n}.$$

Esto quiere decir que en el cuerpo de fracciones de $k[\![X]\!]$ todo elemento puede ser representado como una fracción $\frac{f}{X^n}$ donde $f \in k[\![X]\!]$ y $n = 0, 1, 2, 3, \ldots$ Se ve que el cuerpo formado por estas fracciones es isomorfo al cuerpo

$$k((X)) := \Big\{ \sum_{i \geq -n} a_i\,X^i \;\Big|\; a_i \in k,\ n = 0, 1, 2, 3, \ldots \Big\}$$

(con las operaciones de suma y producto definidas de la manera habitual) que se llama el **cuerpo de las series de Laurent**. Tenemos inclusiones naturales de subanillos

$$\begin{array}{ccc} k[\![X]\!] & \hookrightarrow & k((X)) \\ \uparrow & & \uparrow \\ k[X] & \hookrightarrow & k(X) \end{array}$$

Las series de Laurent $\mathbb{C}((X))$ tienen mucha importancia en análisis complejo. ▲

La localización $R[U^{-1}]$ es la "extensión mínima" de R donde los elementos de U se vuelven invertibles.

12.2.10. Proposición (Propiedad universal de la localización). *Sea R un anillo conmutativo y $U \subseteq R$ un subconjunto multiplicativo. Consideremos el homomorfismo canónico*

$$\phi\colon R \to R[U^{-1}], \quad r \mapsto \frac{r}{1}.$$

Entonces

1) *para todo $u \in U$ el elemento $\phi(u) = \frac{u}{1}$ es invertible en $R[U^{-1}]$;*
2) *si S es otro anillo junto con un homomorfismo $f\colon R \to S$ tal que $f(u)$ es invertible en S para todo $u \in U$, entonces f se factoriza de modo único por ϕ:*

$$\begin{array}{ccc} R & \xrightarrow{\ f\ } & S \\ {\scriptstyle\phi}\downarrow & \nearrow_{\exists!\widetilde{f}} & \\ R[U^{-1}] & & \end{array}$$

Demostración. La parte 1) está clara: se tiene $\left(\frac{u}{1}\right)^{-1} = \frac{1}{u}$.

En la parte 2), sea $\widetilde{f}$ un homomorfismo que hace conmutar el diagrama; entonces

$$\widetilde{f}\left(\frac{r}{1}\right) = f(r)$$

para todo $r \in R$. Además, si $f(u)$ es invertible para todo $u \in U$, entonces

$$\widetilde{f}\left(\frac{1}{u}\right) = \widetilde{f}\left(\left(\frac{u}{1}\right)^{-1}\right) = \widetilde{f}\left(\frac{u}{1}\right)^{-1} = f(u)^{-1},$$

y para todo $\frac{r}{u} \in R[U^{-1}]$ se tiene necesariamente

$$\widetilde{f}\left(\frac{r}{u}\right) = \widetilde{f}\left(\frac{r}{1} \cdot \frac{1}{u}\right) = \widetilde{f}\left(\frac{r}{1}\right)\, \widetilde{f}\left(\frac{1}{u}\right) = f(r)\, f(u)^{-1}.$$

Esto demuestra la unicidad de $\widetilde{f}$.

Para la existencia, notamos que dado un homomorfismo $f\colon R \to S$ tal que $f(u)$ es invertible para todo $u \in U$, la aplicación

$$\widetilde{f}\colon R[U^{-1}] \to S, \quad \frac{r}{u} \mapsto f(r)\, f(u)^{-1}$$

es un homomorfismo de anillos que hace conmutar el diagrama. Evidentemente,

$$\widetilde{f}\left(\frac{1}{1}\right) = f(1)\, f(1)^{-1} = 1.$$

Para las sumas, se cumple

$$\begin{aligned}\widetilde{f}\left(\frac{r_1}{u_1} + \frac{r_2}{u_2}\right) = \widetilde{f}\left(\frac{r_1u_2 + r_2u_1}{u_1u_2}\right) &= f(r_1u_2 + r_2u_1)\, f(u_1u_2)^{-1} \\ &= f(r_1)\, f(u_1)^{-1} + f(r_2)\, f(u_2)^{-1} = \widetilde{f}\left(\frac{r_1}{u_1}\right) + \widetilde{f}\left(\frac{r_2}{u_2}\right),\end{aligned}$$

y para los productos,

$$\begin{aligned}\widetilde{f}\left(\frac{r_1}{u_1} \cdot \frac{r_2}{u_2}\right) = \widetilde{f}\left(\frac{r_1r_2}{u_1u_2}\right) = f(r_1r_2)\, f(u_1u_2)^{-1} &= f(r_1)\, f(u_1)^{-1}\, f(r_2)\, f(u_2)^{-1} \\ &= \widetilde{f}\left(\frac{r_1}{u_1}\right) \cdot \widetilde{f}\left(\frac{r_2}{u_2}\right).\end{aligned}$$

■

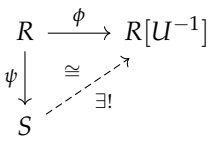
Como siempre, la propiedad universal caracteriza a $R[U^{-1}]$ de modo único salvo isomorfismo.

12.2.11. Proposición. *Supongamos que $\psi\colon R \to S$ es un homomorfismo de anillos que satisface la misma propiedad universal que el homomorfismo canónico de localización $\phi\colon R \to R[U^{-1}]$:*

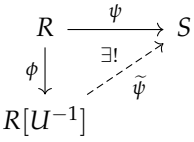
1) *para todo $u \in U$ el elemento $\psi(u)$ es invertible en S;*
2) *si S' es otro anillo junto con un homomorfismo $f\colon R \to S'$ tal que $f(u)$ es invertible en S' para todo $u \in U$, entonces f se factoriza de modo único por ψ:*

$$\begin{array}{ccc} R & \xrightarrow{\ f\ } & S' \\ {\scriptstyle\psi}\downarrow & \nearrow_{\exists!\widetilde{f}} & \\ S & & \end{array}$$

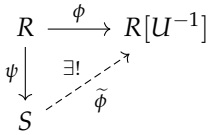
Entonces, existe un isomorfismo único $S \to R[U^{-1}]$ que hace conmutar el diagrama



Demostración. Podemos aplicar la propiedad universal de ϕ a ψ



y viceversa, aplicar la propiedad universal de ψ a ϕ:

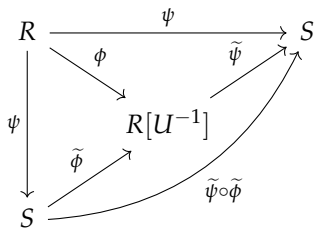


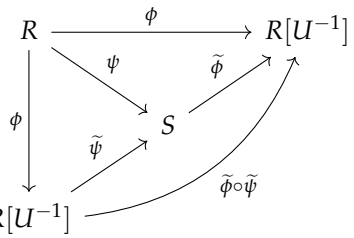
De esta manera se obtienen homomorfismos de anillos

$$\widetilde{\phi}\colon R[U^{-1}] \to S, \quad \widetilde{\phi}\colon S \to R[U^{-1}], \quad \psi = \widetilde{\psi} \circ \phi, \quad \phi = \widetilde{\phi} \circ \psi.$$

Ahora tenemos

$$\widetilde{\psi} \circ \widetilde{\phi} \circ \psi = \widetilde{\psi} \circ \phi = \psi, \quad \widetilde{\phi} \circ \widetilde{\psi} \circ \phi = \widetilde{\phi} \circ \psi = \phi.$$





Pero la propiedad universal de ψ en el primer diagrama de arriba postula que hay un homomorfismo *único* $f\colon S \to S$ tal que $f \circ \psi = \psi$. Funciona el homomorfismo identidad id_S, así que necesariamente

$$\widetilde{\psi} \circ \widetilde{\phi} = \mathrm{id}_S.$$

De la misma manera, la propiedad universal de ϕ implica que

$$\widetilde{\phi} \circ \widetilde{\psi} = \mathrm{id}_{R[U^{-1}]}.$$

Podemos concluir que los homomorfismos $\widetilde{\phi}$ y $\widetilde{\psi}$ son mutualmente inversos. ■

El siguiente resultado nos dice que invertir un producto xy es lo mismo que invertir x y luego invertir y.

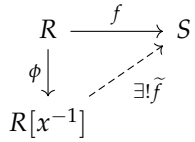
12.2.12. Proposición. *Sea R un anillo conmutativo y sean $x, y \in R$ algunos elementos. Entonces, hay un isomorfismo natural*[*]

$$R[x^{-1}][y^{-1}] \cong R[(xy)^{-1}].$$

Demostración. Consideremos la propiedad universal de $R[x^{-1}]$. Notamos que si $f\colon R \to S$ es un homomorfismo tal que $f(x)$ es invertible en S, entonces $f(x^n) = f(x)^n$ es invertible para cualquier $n = 0, 1, 2, 3, \ldots$, así que es suficiente decir que

1) el elemento $\phi(u) = \frac{u}{1}$ es invertible en $R[x^{-1}]$;

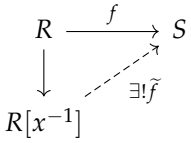
2) si S es otro anillo junto con un homomorfismo $f\colon R \to S$ tal que $f(x)$ es invertible en S, entonces f se factoriza de modo único por ϕ:



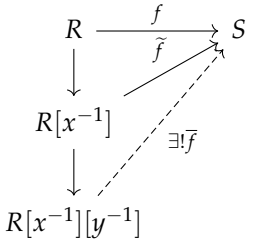
Ahora supongamos que $f\colon R \to S$ es un homomorfismo de anillos tal que $f(xy)$ es invertible en S. Entonces, $f(x)$ y $f(y)$ son también invertibles:

$$f(x)^{-1} = f(y)\, f(xy)^{-1}, \quad f(y)^{-1} = f(x)\, f(xy)^{-1},$$

así que f se factoriza de modo único por el homomorfismo canónico $R \to R[x^{-1}]$:



En este caso $\widetilde{f}\left(\frac{y}{1}\right) = f(y)$ es invertible en S, así que $\widetilde{f}$ se factoriza de modo único por el homomorfismo canónico $R[x^{-1}] \to R[x^{-1}][y^{-1}]$:



Acabamos de probar que la composición $R \to R[x^{-1}] \to R[x^{-1}][y^{-1}]$ satisface la propiedad universal de la localización $R \to R[(xy)^{-1}]$. Entonces, $R[x^{-1}][y^{-1}] \cong R[(xy)^{-1}]$. ■

[*]Aquí $R[x^{-1}][y^{-1}]$ denota dos localizaciones consecutivas: primero $R \to R[x^{-1}]$, y luego $R[x^{-1}] \to R[x^{-1}][(y/1)^{-1}]$, donde $\frac{y}{1} \in R[x^{-1}]$.

El siguiente resultado interpreta la localización $R[x^{-1}]$ como un cociente del anillo de polinomios $R[T]$.

12.2.13. Proposición. *Sea R un anillo conmutativo y $x \in R$. Entonces, la composición de homomorfismos canónicos*

$$\phi\colon R \rightarrowtail R[T] \twoheadrightarrow R[T]/(xT-1)$$

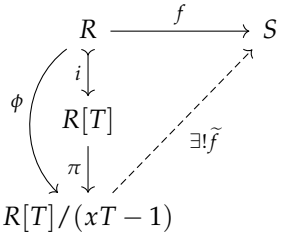
(donde $R[T]$ es el anillo de polinomios en T con coeficientes en R) satisface la propiedad universal de la localización $R \to R[x^{-1}]$, y por ende hay un isomorfismo natural

$$R[x^{-1}] \cong R[T]/(xT-1).$$

Demostración. Tenemos

$$x\,T \equiv 1 \pmod{xT-1},$$

así que $\phi(x)$ es invertible en $R[T]/(xT-1)$. Sea $f\colon R \to S$ otro homomorfismo de anillos tal que $f(x)$ es invertible en S. Supongamos que f se factoriza por ϕ:



Esto implica que para todo $a \in R$ se tiene

$$\widetilde{f}(\overline{a}) = f(a),$$

donde $\overline{a}$ denota el elemento representado por a en el cociente $R[T]/(xT-1)$. Además, para $\overline{T} \in R[T]/(xT-1)$ se tiene

$$\widetilde{f}(\overline{T}) = \widetilde{f}(\overline{x}^{-1}) = \widetilde{f}(\overline{x})^{-1} = f(x)^{-1}.$$

Pero esto ya define a $\widetilde{f}$ de modo único:

$$\begin{aligned}\widetilde{f}(\overline{a_n\,T^n + \cdots + a_1\,T + a_0}) &= \widetilde{f}(\overline{a_n}\cdot\overline{T}^n + \cdots + \overline{a_1}\cdot\overline{T} + \overline{a_0}) \\ &= \widetilde{f}(\overline{a_n})\,\widetilde{f}(\overline{T})^n + \cdots + \widetilde{f}(\overline{a_1})\cdot\widetilde{f}(\overline{T}) + \widetilde{f}(\overline{a_0}) \\ &= f(a_n)\,f(x)^{-1} + \cdots + f(a_1)\,f(x)^{-1} + f(a_0).\end{aligned}$$

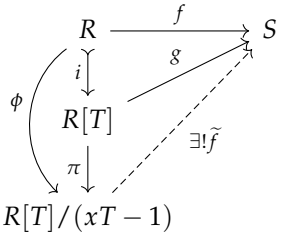
Viceversa, dado un homomorfismo $f\colon R \to S$ tal que $f(x)$ es invertible en S, se ve que

$$\begin{aligned}&g\colon R[T] \to S,\\ &\sum_i a_i\,T^i \mapsto \sum_i f(a_i)\,x^{-i}\end{aligned}$$

es un homomorfismo de anillos que cumple $g(a) = f(a)$ para todo $a \in R$ y $xT - 1 \in \ker g$, así que g induce un homomorfismo único

$$\widetilde{f}\colon R[T]/(xT-1) \to S, \quad \overline{p} \mapsto g(p)$$

tal que $\widetilde{f} \circ \pi = g$.



■

En general, para cualquier conjunto multiplicativo $U \subset R$, se puede probar que

$$R[U^{-1}] \cong R[T_u \mid u \in U]/(u\,T_u - 1 \mid u \in U),$$

donde $R[T_u \mid u \in U]$ es el anillo de polinomios en las variables T_u indexadas por los elementos de U y $(u\,T_u - 1 \mid u \in U)$ es el ideal generado por los polinomios $u\,T_u - 1$. Algunos autores *definen* la localización $R[U^{-1}]$ como el anillo cociente $R[T_u \mid u \in U]/(u\,T_u - 1 \mid u \in U)$. Esta construcción es más concisa pero probablemente menos intuitiva para los principiantes que nuestra construcción con fracciones.

12.3 Ideales en la localización

En esta sección R denota un anillo conmutativo, $U \subseteq R$ un subconjunto multiplicativo y

$$\phi\colon R \to R[U^{-1}], \quad r \mapsto \frac{r}{1}$$

es el homomorfismo canónico de localización.

Notamos que la localización conmuta con los cocientes en el siguiente sentido.

12.3.1. Proposición. *Sea $I \subseteq R$ un ideal. Definamos el conjunto*

$$\overline{U} := \{\overline{u} := u + I \mid u \in U\} \subseteq R/I$$

y sea

$$IR[U^{-1}] := \phi(I)\,R[U^{-1}] := \textit{el ideal en } R[U^{-1}] \textit{ generado por } \frac{x}{1},\ x \in I.$$

Entonces,

1) *$\overline{U}$ es un subconjunto multiplicativo en R/I;*

2) se tiene

$$IR[U^{-1}] = \left\{ \frac{x}{u} \;\middle|\; x \in I,\ u \in U \right\};$$

3) hay un isomorfismo natural

$$(R/I)[\overline{U}^{-1}] \cong R[U^{-1}]/IR[U^{-1}].$$

La notación "$IR[U^{-1}]$" es un poco abusiva: en general R no puede ser encajado en $R[U^{-1}]$, tenemos solamente el homomorfismo canónico $\phi\colon R \to R[U^{-1}]$ que no es siempre inyectivo. Sería más correcto escribir "$\phi(I)\, R[U^{-1}]$", pero lo encuentro un poco incómodo.

Demostración. Tenemos $1 \in U$, así que $\overline{1} \in \overline{U}$. Si $u, v \in U$, entonces $uv \in U$, y luego $\overline{u} \cdot \overline{v} = \overline{uv} \in \overline{U}$. Esto verifica que $\overline{U}$ es un subconjunto multiplicativo en R/I.

Notamos que los elementos de la forma $\frac{x}{u}$ con $x \in I$ y $u \in U$ forman un ideal en $R[U^{-1}]$. En efecto, este conjunto contiene $\frac{0}{1}$. Para las sumas tenemos

$$\frac{x_1}{u_1} + \frac{x_2}{u_2} = \frac{x_1 u_2 + x_2 u_1}{u_1 u_2},$$

donde $x_1 u_2 + x_2 u_1 \in I$, puesto que I es un ideal, y para los productos por los elementos de $R[U^{-1}]$,

$$\frac{r}{u}\,\frac{x}{v} = \frac{rx}{uv},$$

donde $rx \in I$.

Todos los elementos $\frac{x}{1}$ están en este ideal, así que $IR[U^{-1}] \subseteq \left\{ \frac{x}{u} \;\middle|\; x \in I,\ u \in U \right\}$. Viceversa, todo elemento $\frac{x}{u}$ puede ser escrito como $\frac{1}{u} \cdot \frac{x}{1}$ y por ende pertenece al ideal $IR[U^{-1}]$.

Para obtener el isomorfismo $(R/I)[\overline{U}^{-1}] \cong R[U^{-1}]/IR[U^{-1}]$, se puede usar la propiedad universal de la localización, pero se puede definirlo de modo explícito. Consideremos la aplicación[*]

$$\begin{aligned} f\colon R[U^{-1}] &\to (R/I)[\overline{U}^{-1}], \\ r/u &\mapsto \overline{r}/\overline{u}. \end{aligned}$$

Esta aplicación está bien definida: si $r/u = r'/u'$, entonces $v\,(r\,u' - r'\,u) = 0$ para algún $v \in U$. Luego, reduciendo esta identidad módulo I, se obtiene $\overline{v}\,(\overline{r}\,\overline{u'} - \overline{r'}\,\overline{u}) = 0$, lo que significa que $\overline{r}/\overline{u} = \overline{r'}/\overline{u'}$ en $(R/I)[\overline{U}^{-1}]$. Este es un homomorfismo de anillos: la identidad en $(R/I)[\overline{U}^{-1}]$ es $\overline{1}/\overline{1}$; la adición viene dada por

$$\overline{r_1}/\overline{u_1} + \overline{r_2}/\overline{u_2} = (\overline{r_1}\,\overline{u_2} + \overline{r_2}\,\overline{u_1})/(\overline{u_1}\,\overline{u_2}) = (\overline{r_1 u_2 + r_2 u_1})/(\overline{u_1 u_2})$$

y la multiplicación viene dada por

$$(\overline{r_1}/\overline{u_1}) \cdot (\overline{r_2}/\overline{u_2}) = (\overline{r_1}\,\overline{r_2})/(\overline{u_1}\,\overline{u_2}) = \overline{r_1 r_2}/\overline{u_1 u_2}.$$

[*]Voy a escribir r/u en lugar de $\frac{r}{u}$, dado que $\overline{r}/\overline{u}$ se ve mejor que $\frac{\overline{r}}{\overline{u}}$.

Este homomorfismo es visiblemente sobreyectivo. Su núcleo viene dado por

$$\begin{aligned}\ker f = \{r/u \in R[U^{-1}] \mid \overline{r}/\overline{u} = \overline{0}/\overline{1} \text{ en } (R/I)[\overline{U}^{-1}]\} &= \{r/u \mid \overline{v}\,\overline{r} = \overline{0} \text{ para algún } \overline{v} \in \overline{U}\} \\ &= \{r/u \mid v\,r \in I \text{ para algún } v \in U\} = IR[U^{-1}].\end{aligned}$$

Para la última igualdad, notamos que si $vr \in I$, entonces $\frac{r}{u} = \frac{vr}{vu} \in IR[U^{-1}]$, y viceversa, para todo elemento $\frac{x}{u} \in IR[U^{-1}]$ se cumple claramente $f(x/u) = \overline{0}/\overline{u} = \overline{0}/\overline{1}$.

El primer teorema de isomorfía nos dice que f induce un isomorfismo

$$R[U^{-1}]/IR[U^{-1}] \xrightarrow{\cong} (R/I)[\overline{U}^{-1}].$$

■

12.3.2. Ejemplo. Consideremos el anillo $\mathbb{Z}/12\mathbb{Z}$. Tenemos

$$(\mathbb{Z}/12\mathbb{Z})_{(3)} \cong (\mathbb{Z}_{(3)}/12\mathbb{Z}_{(3)}),$$

donde $(\mathbb{Z}/12\mathbb{Z})_{(3)}$ denota la localización de $\mathbb{Z}/12\mathbb{Z}$ afuera del ideal maximal $3\mathbb{Z}/12\mathbb{Z}$, mientras que $\mathbb{Z}_{(3)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ 3 \nmid b \right\}$ es la localización de $\mathbb{Z}$ afuera del ideal maximal $3\mathbb{Z}$. Tenemos $4 \in \mathbb{Z}_{(3)}^{\times}$, así que $12\mathbb{Z}_{(3)} = 4^{-1} \cdot 12\mathbb{Z} = 3\mathbb{Z}$. Luego,

$$(\mathbb{Z}_{(3)}/12\mathbb{Z}_{(3)}) = \mathbb{Z}_{(3)}/3\mathbb{Z}_{(3)} \cong \mathbb{Z}/3\mathbb{Z}.$$

De la misma manera, se tiene

$$(\mathbb{Z}/12\mathbb{Z})_{(2)} \cong (\mathbb{Z}_{(2)}/12\mathbb{Z}_{(2)}) \cong (\mathbb{Z}_{(2)}/4\mathbb{Z}_{(2)}) \cong \mathbb{Z}/4\mathbb{Z}.$$

En general, para el anillo $\mathbb{Z}/n\mathbb{Z}$ con $n = p_1^{k_1} \cdots p_s^{k_s}$ tenemos la siguiente forma del teorema chino del resto:

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})_{(p_1)} \times \cdots \times (\mathbb{Z}/n\mathbb{Z})_{(p_s)}.$$

▲

Ahora una pregunta muy natural es qué sucede con los ideales de R al pasar a la localización $R[U^{-1}]$. Resulta que todos los ideales de $R[U^{-1}]$ provienen de los ideales de R en el siguiente sentido.

12.3.3. Proposición.

1) *Todo ideal $J \subseteq R[U^{-1}]$ es de la forma $IR[U^{-1}]$ para algún ideal $I \subseteq R$; específicamente,*

$$J = \phi^{-1}(J)\, R[U^{-1}].$$

2) *Un ideal $I \subseteq R$ es de la forma $\phi^{-1}(J)$ para algún $J \subseteq R[U^{-1}]$ si y solamente si los elementos de U no son divisores de cero en R/I. En otras palabras, si $ur \in I$ para algunos $u \in U$, $r \in R$, entonces $r \in I$. Específicamente, cuando se cumple esta condición, se tiene*

$$I = \phi^{-1}(IR[U^{-1}]).$$

Demostración. Consideremos un ideal $J \subseteq R[U^{-1}]$. Para todo elemento $\frac{r}{u} \in J$ se cumple $\frac{r}{1} = \frac{u}{1} \cdot \frac{r}{u} \in J$, así que $r \in \phi^{-1}(J)$, y luego $\frac{r}{u} = \frac{1}{u} \cdot \frac{r}{1} \in \phi^{-1}(U)$. Viceversa, todo elemento de $\phi^{-1}(J)R[U^{-1}]$ es de la forma $\frac{x}{u}$ donde $x \in \phi^{-1}(J)$ y $u \in U$; es decir, $\frac{x}{1} \in J$. Luego, $\frac{x}{u} = \frac{1}{u} \cdot \frac{x}{1}$. Esto establece la parte 1).

En la parte 2), consideremos un ideal $J \subseteq R[U^{-1}]$ y su preimagen

$$I := \phi^{-1}(J) = \left\{ r \in R \;\middle|\; \frac{r}{1} \in J \right\}.$$

Supongamos que para $u \in U$ y $r \in R$ se cumple $ur \in I$. Esto significa que $\frac{ur}{1} \in J$. Pero luego $\frac{1}{u} \cdot \frac{ur}{1} = \frac{r}{1} \in J$, así que $r \in I$.

Viceversa, asumamos que $I \subseteq R$ es un ideal tal que $ur \in I$ implica $r \in I$ para cualesquiera $u \in U$ y $r \in R$. Consideremos el ideal correspondiente

$$IR[U^{-1}] = \left\{ \frac{x}{u} \;\middle|\; x \in I,\ u \in U \right\}.$$

Luego,

$$\begin{aligned} \phi^{-1}(IR[U^{-1}]) &= \left\{ r \in R \;\middle|\; \frac{r}{1} = \frac{x}{u} \text{ para algunos } x \in I,\ u \in U \right\} \\ &= \left\{ r \in R \;\middle|\; vur = vx \text{ para algunos } x \in I,\ u, v \in U \right\}. \end{aligned}$$

Si $vur = vx$ donde $x \in I$, $u, v \in U$, entonces $vur \in I$, donde $vu \in U$, y por nuestra hipótesis $r \in I$, así que $\phi^{-1}(IR[U^{-1}]) \subseteq I$. La otra inclusión $I \subseteq \phi^{-1}(IR[U^{-1}])$ es evidente. ■

12.3.4. Comentario. Las biyecciones del resultado anterior preservan las inclusiones: si $J_1 \subseteq J_2 \subseteq R[U^{-1}]$, entonces $\phi^{-1}(J_1) \subseteq \phi^{-1}(J_2)$. De la misma manera si $I_1 \subseteq I_2 \subseteq R$, entonces $I_1 R[U^{-1}] \subseteq I_2 R[U^{-1}]$.

12.3.5. Corolario. *Hay una biyección entre los ideales primos*

$$\begin{aligned} \operatorname{Spec} R[U^{-1}] &\cong \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap U = \emptyset\}, \\ \mathfrak{q} &\mapsto \phi^{-1}(\mathfrak{q}), \\ \mathfrak{p}R[U^{-1}] &\hookleftarrow \mathfrak{p}. \end{aligned}$$

Demostración. Para un ideal primo $\mathfrak{q} \subset \operatorname{Spec} R[U^{-1}]$ su preimagen $\mathfrak{p} := \phi^{-1}(\mathfrak{q})$ es también un ideal primo, como para cualquier homomorfismo de anillos. La condición 2) del resultado anterior dice que los elementos de U no son divisores de cero en el anillo cociente $R/\mathfrak{p}$. Pero este cociente es un dominio de integridad y por lo tanto la condición nos dice precisamente que $\mathfrak{p} \cap U = \emptyset$. Esto verifica que la aplicación $\mathfrak{q} \mapsto \phi^{-1}(\mathfrak{q})$ está bien definida.

Sea $\mathfrak{p} \subset R$ un ideal primo. Como vimos en 12.3.1, se cumple

$$R[U^{-1}]/\mathfrak{p}R[U^{-1}] \cong (R/\mathfrak{p})[\overline{U}^{-1}].$$

Puesto que $R/\mathfrak{p}$ es un dominio de integridad, para la localización $(R/\mathfrak{p})[\overline{U}^{-1}]$ hay dos posibilidades (véase 12.2.4):

a) $\overline{0} \in \overline{U}$ (es decir, $\mathfrak{p} \cap U \neq \emptyset$), y entonces $(R/\mathfrak{p})[\overline{U}^{-1}] = 0$ (es decir, $\mathfrak{p}R[U^{-1}] = R[U^{-1}]$);

b) $\overline{0} \notin \overline{U}$ (es decir, $\mathfrak{p} \cap U = \emptyset$), y entonces $(R/\mathfrak{p})[\overline{U}^{-1}]$ es un dominio de integridad (es decir, $\mathfrak{p}R[U^{-1}] \subset R[U^{-1}]$ es un ideal primo).

Entonces, la aplicación $\mathfrak{p} \mapsto \mathfrak{p}R[U^{-1}]$ también está bien definida.

La parte 1) de la proposición anterior nos dice que para cualquier ideal $\mathfrak{q} \subset R[U^{-1}]$ se cumple

$$\mathfrak{q} = \phi^{-1}(\mathfrak{q})\, R[U^{-1}].$$

La parte 2) nos dice que si para un ideal primo $\mathfrak{p} \subset R$ se cumple $\mathfrak{p} \cap U = \emptyset$, entonces

$$\mathfrak{p} = \phi^{-1}(\mathfrak{p}R[U^{-1}]).$$

■

12.3.6. Comentario. El lector que no esté satisfecho con el argumento de arriba siempre puede escribir su propia demostración usando la definición de ideales primos de 12.1.1, sin considerar los cocientes $R[U^{-1}]/\mathfrak{p}R[U^{-1}]$ y $R/\phi^{-1}(\mathfrak{q})$.

12.3.7. Corolario. *Sea $\mathfrak{p} \subset R$ un ideal primo. Hay una biyección natural*

$$\begin{aligned} \operatorname{Spec} R_{\mathfrak{p}} &\cong \{\mathfrak{q} \in \operatorname{Spec} R \mid \mathfrak{q} \subseteq \mathfrak{p}\}, \\ \mathfrak{P} &\mapsto \phi^{-1}(\mathfrak{P}), \\ \mathfrak{q}R_{\mathfrak{p}} &\hookleftarrow \mathfrak{q}. \end{aligned}$$

En particular, el anillo $R_{\mathfrak{p}}$ tiene un único ideal maximal dado por $\mathfrak{p}R_{\mathfrak{p}}$.

Demostración. Por la definición, $R_{\mathfrak{p}} = R[U^{-1}]$ donde $U := R \setminus \mathfrak{p}$. Entonces, la condición $\mathfrak{q} \cap U = \emptyset$ es equivalente a $\mathfrak{q} \subseteq \mathfrak{p}$. Respecto al ideal maximal, basta notar que $\mathfrak{q} \subseteq \mathfrak{p}$ implica $\mathfrak{q}R_{\mathfrak{p}} \subseteq \mathfrak{p}R_{\mathfrak{p}}$. ■

12.3.8. Ejemplo. Los ideales primos en $\mathbb{Z}_{(p)}$ corresponden a los ideales primos $(q) \subseteq \mathbb{Z}$ tales que $(q) \subseteq (p)$. Esto implica que

$$\operatorname{Spec} \mathbb{Z}_{(p)} = \{(0), (p)\}.$$

▲

12.3.9. Definición. Un anillo que tiene un único ideal maximal se llama un **anillo local**.

Acabamos de probar que para cualquier ideal primo $\mathfrak{p} \subset R$ la localización $R_{\mathfrak{p}}$ es un anillo local. Los anillos locales son mucho más sencillos que los anillos conmutativos en general. Muy a menudo problemas se resuelven considerando diferentes localizaciones $R_{\mathfrak{p}}$ para $\mathfrak{p} \subset R$.

12.4 Anillos noetherianos

En practica, para especificar un ideal, es conveniente considerar una lista de elementos que lo generan. En este sentido mucha importancia tienen ideales finitamente generados. Notemos primero que algunas operaciones con ideales pueden ser expresadas en términos de los generadores.

12.4.1. Observación. *Sean $I = (x_1, \ldots, x_m)$ y $J = (y_1, \ldots, y_n)$ dos ideales finitamente generados. Entonces, su suma y producto son también finitamente generados; específicamente*

1) *$I + J$ está generado por los elementos $x_1, \ldots, x_m, y_1, \ldots, y_n$*

2) *IJ está generado por los productos $x_i y_j$ donde $i = 1, \ldots, m$ y $j = 1, \ldots, n$,*

Demostración. Para la suma, tenemos

$$I + J = \Big((x_1) + \cdots + (x_m)\Big) + \Big((y_1) + \cdots + (y_n)\Big) = (x_1, \ldots, x_m, y_1, \ldots, y_n)$$

y para el producto,

$$IJ = \Big((x_1) + \cdots + (x_m)\Big) \cdot \Big((y_1) + \cdots + (y_n)\Big) = \sum_{1 \le i \le m} \sum_{1 \le j \le n} (x_i) \cdot (y_j) = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} (x_i y_j).$$

Aquí hemos usado el hecho de que el producto de dos ideales principales (x) e (y) es el ideal generado por xy. ■

12.4.2. Observación. *Sea $f\colon R \to S$ un homomorfismo sobreyectivo de anillos conmutativos. Si $I = (x_1, \ldots, x_n) \subseteq R$ es un ideal finitamente generado, entonces $f(I) = (f(x_1), \ldots, f(x_n)) \subseteq S$ es también finitamente generado.*

En particular, si R es un anillo conmutativo y $I \subseteq R$ es un ideal, entonces para todo ideal finitamente generado $J \subseteq R$ el ideal correspondiente $J/I \subseteq R/I$ es también finitamente generado.

Demostración. Tenemos

$$I = \{r_1 x_1 + \cdots + r_n x_n \mid r_i \in R\}$$

y luego

$$\begin{aligned} f(I) = \{f(r_1) f(x_1) + \cdots + f(r_n) f(x_n) \mid r_i \in R\} &= \{s_1 f(x_1) + \cdots + s_n f(x_n) \mid s_i \in S\} \\ &= (f(x_1), \ldots, f(x_n)), \end{aligned}$$

dado que f es un homomorfismo sobreyectivo. ■

Resulta que la *intersección* de dos ideales finitamente generados no tiene por qué ser un ideal finitamente generado.

12.4.3. Ejemplo. Consideremos el anillo[*]

$$R := \mathbb{Z} + X^2\,\mathbb{Q}[X] := \{a_0 + a_2\,X^2 + \cdots + a_n\,X^n \mid a_0 \in \mathbb{Z},\ a_1 = 0,\ a_2, \ldots, a_n \in \mathbb{Q}\} \subset \mathbb{Q}[X].$$

Sea I el ideal generado por X^2 y sea J el ideal generado por X^3. Los elementos de I son los polinomios

$$a_2\,X^2 + a_4\,X^4 + a_5\,X^5 + \cdots + a_n\,X^n,$$

donde $a_2 \in \mathbb{Z}$ y $a_4, a_5, \ldots, a_n \in \mathbb{Q}$. Los elementos de J son los polinomios

$$a_3\,X^3 + a_5\,X^5 + a_6\,X^6 + \cdots + a_n\,X^n,$$

donde $a_3 \in \mathbb{Z}$ y $a_5, a_6, \ldots, a_n \in \mathbb{Q}$. Notamos que

$$I \cap J = X^5\,\mathbb{Q}[X] := \{a_5\,X^5 + a_6\,X^6 + \cdots + a_n\,X^n \mid a_i \in \mathbb{Q}\}.$$

Este ideal no es finitamente generado en R. En efecto, supongamos que $I \cap J = (f_1, \ldots, f_n)$ para algunos polinomios $f_1, \ldots, f_n \in I \cap J$. Escribamos $f_i = X^5\,g_i$ donde $g_i \in \mathbb{Q}[X]$. Podemos escribir el término constante de cada uno de estos polinomios como $g_i(0) = \frac{a_i}{b_i}$ donde a_i, b_i son números enteros coprimos. Consideremos el polinomio $g := \frac{1}{b_1 \cdots b_n + 1}\,X^5$. Tenemos $g \in I \cap J$. Sin embargo, $g \notin (f_1, \ldots, f_n)$. En efecto, si lo último fuera cierto, tendríamos algunos polinomios $h_1, \ldots, h_n \in R$ tales que

$$g = f_1 h_1 + \cdots + f_n h_n.$$

Aquí g y $f_1, \ldots, f_n$ son divisibles por X^5. Cancelando X^5 y poniendo $X = 0$ se obtiene

$$\frac{1}{b_1 \cdots b_n + 1} = \frac{a_1}{b_1}\,h_1(0) + \cdots + \frac{a_n}{b_n}\,h_n(0)$$

donde $h_i(0) \in \mathbb{Z}$. Esto es imposible, puesto que $b_i \nmid (b_1 \cdots b_n + 1)$ para ningún $i = 1, \ldots, n$.

Este ejemplo también demuestra que la preimagen de un ideal finitamente generado no es necesariamente un ideal finitamente generado. En efecto, tenemos el homomorfismo de inclusión $R \hookrightarrow \mathbb{Q}[X]$ y como acabamos de ver, el ideal $X^5\,\mathbb{Q}[X]$ no es finitamente generado en R. ▲

Entonces, aunque es cómodo trabajar con ideales finitamente generados, en general es fácil salir de su clase. Por esto sería interesante estudiar los anillos donde todos los ideales son finitamente generados.

12.4.4. Definición. Si en un anillo conmutativo R todo ideal es finitamente generado, se dice que R es **noetheriano**.

12.4.5. Ejemplo. En todo cuerpo k los únicos ideales son (0) y $(1) = k$, así que k es noetheriano.

El anillo $\mathbb{Z}$ es noetheriano: sus ideales son (n) para $n = 0, 1, 2, 3, \ldots$ ▲

[*]Este ejemplo curioso fue sugerido por un usuario del foro *Mathematics Stack Exchange*: http://math.stackexchange.com/questions/295875/

El término "noetheriano" conmemora las contribuciones de la matemática alemana EMMY NOETHER (1882–1935) que fue una de los fundadores del álgebra moderna y entre otras cosas reconoció la importancia de anillos noetherianos. He aquí una condición equivalente.

12.4.6. Observación. *Un anillo R es noetheriano si y solamente si para toda cadena de ideales*

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq R$$

se tiene $I_n = I_{n+1}$ para n suficientemente grande.

Demostración. Supongamos que R es noetheriano y consideremos el ideal $I := \bigcup_{n\geq 0} I_n$. Tenemos $I = (x_1, \ldots, x_m)$ para algunos $x_1, \ldots, x_m \in I$, pero estos elementos necesariamente pertenecen a I_n para algún n. Luego, $I_n = I_{n+1} = I_{n+2} = \cdots = I$.

Viceversa, supongamos que R no es noetheriano y existe algún ideal $I \subset R$ que no es finitamente generado. Escojamos $x_0 \in I$. Tenemos $I \neq (x_0)$, así que se puede escoger $x_1 \in I \setminus (x_0)$. Luego, $I \neq (x_0, x_1)$ y existe $x_2 \in I \setminus (x_0, x_1)$, etcétera. De esta manera se obtiene una cadena

$$(x_0) \subsetneq (x_0, x_1) \subsetneq (x_0, x_1, x_2) \subsetneq \cdots \subset R.$$

■

12.4.7. Ejemplo. Sea R un anillo conmutativo. El anillo de polinomios $R[X_1, \ldots, X_n]$ puede ser visto como un subanillo de $R[X_1, \ldots, X_n, X_{n+1}]$. Tenemos una cadena de anillos

$$R[X_1] \subset R[X_1, X_2] \subset R[X_1, X_2, X_3] \subset \cdots$$

La unión nos da el anillo de polinomios en un número infinito de variables:

$$S := R[X_1, X_2, \ldots] := \bigcup_{n\geq 1} R[X_1, \ldots, X_n].$$

En cierto sentido, este anillo es demasiado grande para ser noetheriano: por ejemplo, se tiene una cadena de ideales

$$(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \cdots \subset S$$

Sin embargo, notamos que S es un dominio de integridad, y entonces S puede ser encajado en su cuerpo de fracciones $K(S)$. Siendo un cuerpo, $K(S)$ es noetheriano. Esto es un ejemplo tonto que demuestra que un subanillo de un anillo noetheriano no tiene por qué ser noetheriano. ▲

12.4.8. Ejemplo. Sea $\mathcal{C}(\mathbb{R})$ el anillo de las funciones continuas $f\colon \mathbb{R} \to \mathbb{R}$. Para $n = 0, 1, 2, 3, \ldots$ consideremos

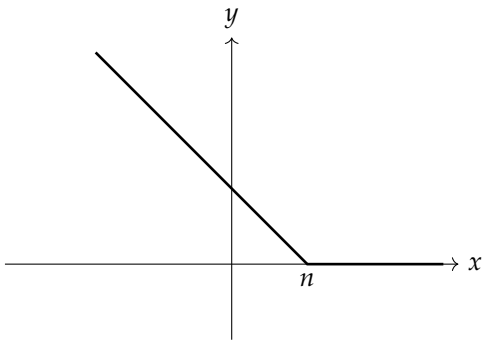
$$I_n := \{f \in \mathcal{C}(\mathbb{R}) \mid f(x) = 0 \text{ para } x \geq n\}.$$

Esto es un ideal en $\mathcal{C}(\mathbb{R})$ y se tiene una cadena infinita ascendente

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subset \mathcal{C}(\mathbb{R}).$$

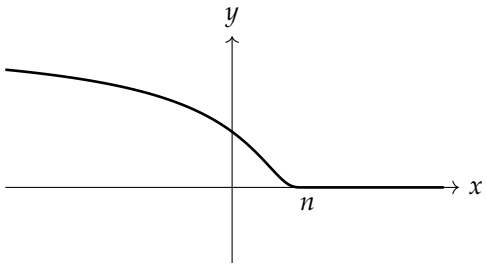
En efecto, es fácil encontrar una función continua $f_n\colon \mathbb{R} \to \mathbb{R}$ tal que $f_n \in I_n$, pero $f_n \notin I_{n-1}$. Por ejemplo, basta poner

$$f_n(x) := \begin{cases} n - x, & x < n, \\ 0, & x \geq n. \end{cases}$$



Podemos considerar el subanillo $\mathcal{C}^\infty(\mathbb{R}) \subset \mathcal{C}(\mathbb{R})$ cuyos elementos son las funciones infinitamente diferenciables. Las funciones que acabamos de definir no son diferenciables en $x = n$, pero se puede tomar

$$g_n(x) := \begin{cases} e^{1/(x-n)}, & x < n, \\ 0, & x \geq n. \end{cases}$$



Es un ejercicio de cálculo comprobar que g_n es infinitamente diferenciable en todos los puntos. Podemos tomar

$$J_n := \{f \in \mathcal{C}^\infty(\mathbb{R}) \mid f(x) = 0 \text{ para } x \geq n\} = I_n \cap \mathcal{C}^\infty(\mathbb{R}),$$

y luego $g_n \in J_n \setminus J_{n-1}$, lo que demuestra que existe una cadena infinita ascendente

$$J_0 \subsetneq J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots \subset \mathcal{C}^\infty(\mathbb{R}).$$

De la misma manera, las funciones holomorfas $\mathbb{C} \to \mathbb{C}$ forman un anillo $O(\mathbb{C})$. Este anillo tampoco es noetheriano. Podemos considerar los ideales

$$I_n := \{f \in O(\mathbb{C}) \mid f(k) = 0 \text{ para todo } k = n+1, n+2, \ldots\}.$$

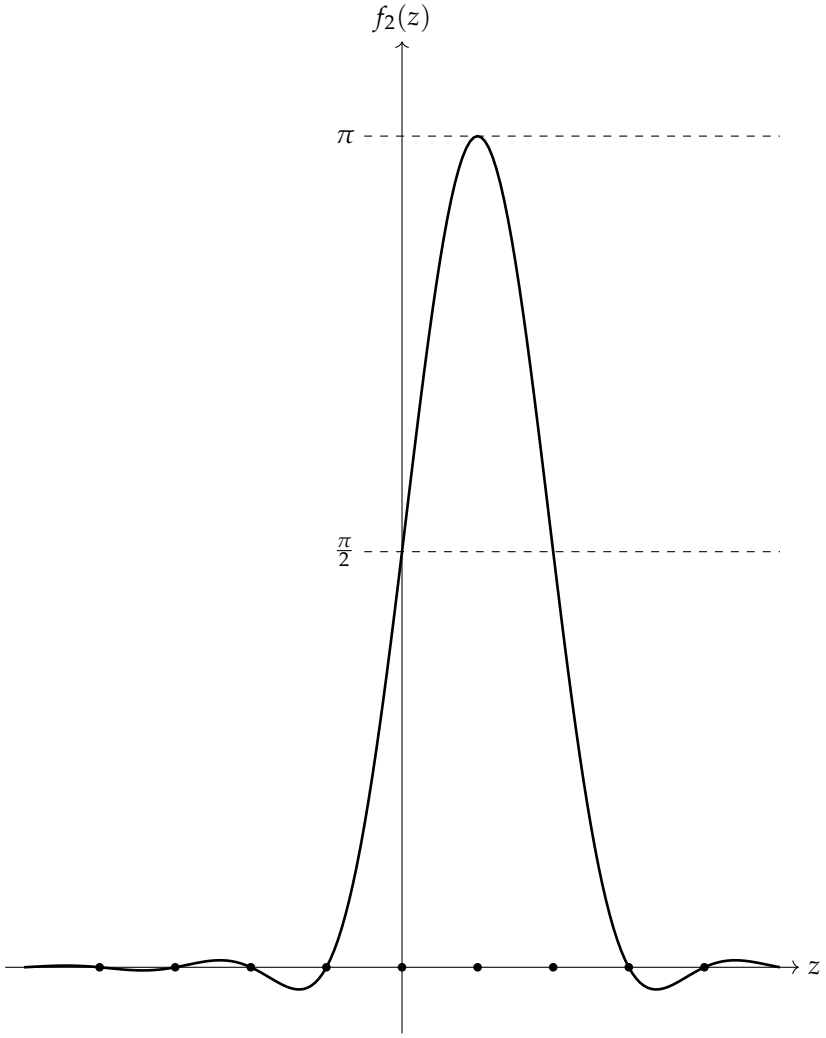
Estos forman una cadena

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \cdots \subset O(\mathbb{C}).$$

Para las funciones

$$f_n := \frac{\sin \pi z}{z\,(z-1)\,(z-2)\cdots(z-n)}$$

se tiene $f_n \in I_{n+1} \setminus I_n$ (para entender este ejemplo, hay que conocer el análisis complejo).



La función $f_2(z) := \frac{\sin \pi z}{z\,(z-1)\,(z-2)}$

▲

Intuitivamente, los anillos $\mathcal{C}(\mathbb{R})$, $\mathcal{C}^\infty(\mathbb{R})$, $\mathcal{O}(\mathbb{C})$ son demasiado grandes para ser noetherianos: hay demasiadas funciones continuas, diferenciables, holomorfas. Intuitivamente, todos estos ejemplos se obtienen del hecho de que este tipo de funciones pueden tener muchos ceros. Las funciones polinomiales no constantes (en una variable) tienen un número finito de ceros. Aunque los anillos como $\mathcal{C}(\mathbb{R})$, $\mathcal{C}^\infty(\mathbb{R})$, $\mathcal{O}(\mathbb{C})$ tienen mucha importancia en análisis, en álgebra muy a menudo se trabaja con los anillos de polinomios $k[X_1, \ldots, X_n]$ donde k es un cuerpo, o en general con los anillos cociente $k[X_1, \ldots, X_n]/I$. Resulta que todos son noetherianos, y así se establece el siguiente hecho.

12.4.9. Teorema (El teorema de la base de Hilbert). *Si R es un anillo noetheriano, entonces el anillo de polinomios $R[X]$ es también noetheriano.*

12.4.10. Corolario. *Si R es un anillo noetheriano, entonces $R[X_1, \ldots, X_n]$ es también un anillo noetheriano.*

Demostración. Podemos usar el teorema de la base junto con la inducción sobre n y los isomorfismos $R[X_1, \ldots, X_n] \cong R[X_1, \ldots, X_{n-1}][X_n]$. ■

Demostración de 12.4.9. Consideremos una cadena ascendente de ideales

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq R[X].$$

Necesitamos ver que esta se estabiliza; es decir, que existe un índice k tal que $I_k = I_{k'}$ para todo $k' \geq k$.

Sea $I_{k,d}$ el ideal de los elementos de R que aparecen como los coeficientes mayores de los polinomios de grado d en I_k; específicamente,

$$I_{k,d} := \{a \in R \mid \text{existe un polinomio } a\,X^d + \cdots \in I_k\} \cup \{0\}.$$

1) Verifiquemos que $I_{k,d}$ es un ideal.

   Para $a, b \in I_{k,d}$ hay que ver que $a + b \in I_{k,d}$. Esto es obvio si $a = 0$ o $b = 0$ o $a + b = 0$ y podemos descartar estos casos. Entonces, $a, b \in I_{k,d}$ significa que en I_k existen polinomios $f = a\,X^d + \cdots$ y $g = b\,X^d + \cdots$. Luego, $f + g = (a + b)\,X^d + \cdots \in I_k$ y $\deg(f + g) = d$ (asumiendo que $a + b \neq 0$), así que $a + b \in I_{k,d}$.

   Para los productos, si $f = a\,X^d + \cdots \in I_k$, entonces para cualquier elemento $c \in R$ el polinomio $cf = ca\,X^d + \cdots$ también está en I_k. Si $ca \neq 0$, entonces $\deg(cf) = d$ y $ca \in I_{k,d}$. Si $ca = 0$, tenemos $0 \in I_{k,d}$.

2) Verifiquemos que

   $$I_{k,d} \subseteq I_{k',d'} \quad \text{si } k \leq k' \text{ y } d \leq d'.$$

   Notamos que en nuestra cadena de ideales $I_k \subseteq I_{k'}$ para $k \leq k'$. Ahora si $a \in I_{k,d}$ y $a \neq 0$, esto significa que existe un polinomio $f = a\,X^d + \cdots \in I_k \subseteq I_{k'}$. Luego, $X^{d'-d} f = a\,X^{d'} + \cdots \in I_{k'}$, lo que demuestra que $a \in I_{k',d'}$.

3) Probemos que entre los $I_{k,d}$ hay solo un número finito de ideales distintos. En efecto, supongamos lo contrario. En este caso una familia infinita de ideales distintos corresponde a un subconjunto infinito de los índices dobles $(k, d) \in \mathbb{N} \times \mathbb{N}$ y entre ellos se puede escoger una cadena infinita* (k_ℓ, d_ℓ) con

   $$k_0 \leq k_1 \leq k_2 \leq \cdots, \quad d_0 \leq d_1 \leq d_2 \leq \cdots$$

   De aquí se obtiene una cadena ascendente

   $$I_{k_0,d_0} \subsetneq I_{k_1,d_1} \subsetneq I_{k_2,d_2} \subsetneq \cdots \subset R$$

   pero esto contradice nuestra hipótesis que R es noetheriano.

*Ejercicio 12.28.

4) Entonces, hay solo un número finito de ideales distintos $I_{k,d}$. Esto significa que existe un índice k tal que
$$I_{k,d} = I_{k+1,d} = I_{k+2,d} = \cdots$$
para todo d.

Supongamos que $k' \geq k$. Vamos a probar que $I_k = I_{k'}$. Tenemos una inclusión $I_k \subseteq I_{k'}$ y hay que ver que todo elemento de $I_{k'}$ pertenece a I_k. Para $f \in I_{k'}$ podemos proceder por inducción sobre $d = \deg f$. Como la base de inducción se puede considerar el caso de $d = -\infty$; es decir, $f = 0$. Para el paso inductivo, supongamos que todos los polinomios de $I_{k'}$ de grado $< d$ pertenecen a I_k. Luego, si $f = a\,X^d + \cdots \in I_{k'}$, entonces $a \in I_{k',d}$. Pero acabamos de ver que $I_{k',d} = I_{k,d}$, lo que implica que existe un polinomio $g = a\,X^d + \cdots \in I_k$. Ahora $\deg(f-g) < d$ y por ende $f - g \in I_k$ por la hipótesis de inducción. Pero en este caso $f = (f-g) + g \in I_k$. ■

Un poco de la historia. En el siglo XIX muchos algebristas se dedicaban a la **teoría de invariantes** que trata de encontrar generadores de ciertos ideales en casos particulares. Hilbert probó el teorema de arriba para deducir la existencia de un número finito de generadores en un caso general abstracto. Luego el matemático alemán Paul Gordan (1837–1912), conocido como *el rey de la teoría de invariantes* no aceptó el articulo de Hilbert a la revista *Mathematische Annalen*, diciendo que su argumento estaba poco claro y que "no era matemáticas, sino teología".

12.4.11. Digresión. Si R es un anillo noetheriano, entonces el anillo de series formales $R[\![X_1, \ldots, X_n]\!]$ es también noetheriano. Sin embargo, esto se demuestra de otra manera (a saber, $R[\![X_1, \ldots, X_n]\!]$ es una **completación** del anillo noetheriano $R[X_1, \ldots, X_n]$; la completación es otra construcción interesante, pero no la vamos a definir en este curso).

12.4.12. Proposición. *Si R es un anillo noetheriano, entonces toda localización $R[U^{-1}]$ es también un anillo noetheriano.*

Demostración. Como vimos en §12.3, para todo ideal $J \subseteq R[U^{-1}]$ se cumple $J = \phi^{-1}(J)\,R[U^{-1}]$ y la correspondencia $J \mapsto \phi^{-1}(J)$ es inyectiva y preserva inclusiones. Entonces, toda cadena de ideales
$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots \subset R[U^{-1}]$$
nos da una cadena de ideales
$$\phi^{-1}(J_0) \subseteq \phi^{-1}(J_1) \subseteq \phi^{-1}(J_2) \subseteq \cdots \subset R$$
que se estabiliza, puesto que R es noetheriano. Pero esto significa que la cadena en $R[U^{-1}]$ se estabiliza.

Otro modo de probar el resultado es notar que si todo ideal en R es finitamente generado, entonces para todo ideal $J \subseteq R[U^{-1}]$ se tiene
$$\phi^{-1}(J) = (x_1, \ldots, x_n),$$
para algunos $x_1, \ldots, x_n \in R$, y luego
$$J = \phi^{-1}(J)\,R[U^{-1}] = \left(\frac{x_1}{1}, \ldots, \frac{x_n}{1}\right).$$

■

12.4.13. Ejemplo. Sea k un cuerpo. Para una colección de polinomios $f_i \in k[X_1, \ldots, X_n]$ consideremos el conjunto de sus ceros comunes en $\mathbb{A}^n(k)$:

$$V(\{f_i\}_{i\in I}) := \{x \in \mathbb{A}^n(k) \mid f_i(x) = 0 \text{ para todo } i \in I\}.$$

Este se llama un **conjunto algebraico**. Luego,

$$V(\{f_i\}_{i\in I}) = V(J) := \{x \in \mathbb{A}^n(k) \mid f(x) = 0 \text{ para todo } f \in J\},$$

donde $J \subseteq k[X_1, \ldots, X_n]$ es el ideal generado por los polinomios f_i. El teorema de la base nos dice que J es necesariamente finitamente generado: $J = (g_1, \ldots, g_m)$ y luego

$$V(\{f_i\}_{i\in I}) = V(J) = V(g_1, \ldots, g_m).$$

Esto significa que todo sistema de ecuaciones polinomiales en $k[X_1, \ldots, X_n]$ siempre equivale a un sistema de un número finito de ecuaciones polinomiales.

Lamentablemente, la prueba del teorema de la base no es constructiva: no sabemos cuáles son los generadores. Para hacer cálculos con conjuntos algebraicos, se usan sistemas especiales de generadores, llamados **bases de Gröbner**. ▲

12.4.14. Observación. *Sea $f\colon R \to S$ un homomorfismo sobreyectivo. Si R es noetheriano, entonces S es también noetheriano. De manera equivalente, todo cociente de un anillo noetheriano es noetheriano.*

Demostración. Véase 12.4.2. ■

12.4.15. Definición. Sean R un anillo conmutativo y A una R-álgebra conmutativa; es decir, un anillo A dotado de un homomorfismo $f\colon R \to A$. Se dice que A es una **R-álgebra finitamente generada** si existen elementos $x_1, \ldots, x_n$ tales que todo elemento de A puede ser expresado como un polinomio en $x_1, \ldots, x_n$ con coeficientes en R; es decir, como una suma finita

$$\sum_{i_1,\ldots,i_n\geq 0} r_{i_1,\ldots,i_n} \cdot x_1^{i_1} \cdots x_n^{i_n} := \sum_{i_1,\ldots,i_n\geq 0} f(r_{i_1,\ldots,i_n})\, x_1^{i_1} \cdots x_n^{i_n}.$$

El anillo de polinomios $R[X_1, \ldots, X_n]$ es una R-álgebra finitamente generada. En general, las R-álgebras finitamente generadas son precisamente los cocientes de estos anillos de polinomios.

12.4.16. Observación. *Una R-álgebra A es finitamente generada si y solo si existe un homomorfismo sobreyectivo $R[X_1, \ldots, X_n] \twoheadrightarrow A$ para algún n; es decir, si y solo si $A \cong R[X_1, \ldots, X_n]/I$ para algún n y algún ideal I.*

Demostración. Por la propiedad universal del álgebra de polinomios, la asignación $X_i \mapsto x_i$ define un homomorfismo único de R-álgebras:

$$\begin{aligned} f\colon R[X_1, \ldots, X_n] &\to A, \\ X_i &\mapsto x_i. \end{aligned}$$

El hecho de que los x_i generan a A como una R-álgebra significa precisamente que esto es una sobreyección. Luego, por el primer teorema de isomorfía

$$A \cong R[X_1, \ldots, X_n]/\ker f.$$

■

12.4.17. Observación. *Si R es un anillo noetheriano, entonces toda R-álgebra finitamente generada A es también un anillo noetheriano.*

Demostración. Se tiene $A \cong R[X_1, \ldots, X_n]/I$ donde $R[X_1, \ldots, X_n]$ es noetheriano por el teorema de la base, y luego todo cociente de un anillo noetheriano es también noetheriano. ■

En la geometría algebraica elemental, las propiedades de conjuntos algebraicos $X \subseteq \mathbb{A}^n(k)$ se estudian a través de las k-álgebras finitamente generadas $k[X_1, \ldots, X_n]/I(X)$, llamadas las **álgebras de funciones polinomiales sobre** X. Véase [Ful2008] para una introducción amigable a este tema. La geometría algebraica es una área inmensa de las matemáticas que ha sido una de las más influyentes a partir del siglo XX.

En este capítulo no hemos tocado ni siquiera la punta del iceberg del álgebra conmutativa. El lector interesado puede consultar [Sha2001], [Rei1995], [AM1969] (un libro de texto clásico) o [Eis2004] (una enciclopedia de 800 páginas).

12.5 Ejercicios

Ideales primos y maximales

Ejercicio 12.1. *Sea $\mathcal{C}(\mathbb{R})$ el anillo de las funciones continuas $f\colon \mathbb{R} \to \mathbb{R}$ con operaciones punto por punto. Demuestre que para cualquier $x \in \mathbb{R}$*

$$\mathfrak{m}_x := \{\text{funciones continuas } f\colon \mathbb{R} \to \mathbb{R} \mid f(x) = 0\}$$

es un ideal maximal en $\mathcal{C}(\mathbb{R})$.

Ejercicio 12.2. *Determine si el ideal generado por el polinomio $X^2 + 1$ es primo o maximal en el anillo*

$$\mathbb{R}[X], \quad \mathbb{C}[X], \quad \mathbb{Z}[X], \quad \mathbb{F}_2[X].$$

Ejercicio 12.3. *Sea R un anillo conmutativo y sea $\mathfrak{p} \subset R$ un ideal primo. Demuestre que si $x^n \in \mathfrak{p}$ para algún $x \in R$ y $n = 1, 2, 3, \ldots$, entonces $x \in \mathfrak{p}$.*

Ejercicio 12.4. *Sea $f\colon R \to S$ un homomorfismo de anillos conmutativos. Para un ideal primo $\mathfrak{p} \subset S$ verifique directamente que $f^{-1}(\mathfrak{p})$ es un ideal primo en R.*

Ejercicio 12.5. *Sea R un anillo conmutativo y sea $\mathfrak{p} \subset R$ un ideal primo.*

1) *Demuestre que para dos ideales $I, J \subseteq R$, si $IJ \subseteq \mathfrak{p}$, entonces $I \subseteq \mathfrak{p}$ o $J \subseteq \mathfrak{p}$.*
2) *Demuestre que si para un ideal $I \subseteq R$ se tiene $I^n \subseteq \mathfrak{p}$ para algún $n = 1, 2, 3, \ldots$, entonces $I \subseteq \mathfrak{p}$.*

Ejercicio 12.6. *Sea R un anillo conmutativo. Para un subconjunto $S \subseteq R$ sea $V(S)$ el conjunto de los ideales primos que contienen a S:*

$$V(S) := \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq S\}.$$

1) *Demuestre que para $S_1 \subseteq S_2 \subseteq R$ se tiene $V(S_2) \subseteq V(S_1)$.*
2) *Demuestre que $V(S) = V(I)$ donde $I = (S)$ es el ideal generado por S.*
3) *Demuestre que $V(0) = \operatorname{Spec} R$ y $V(1) = \emptyset$.*
4) *Demuestre que $V(I) \cup V(J) = V(IJ)$ para ideales $I, J \subseteq R$.*
5) *Demuestre que $\bigcap_k V(I_k) = V(\sum_k I_k)$ para ideales $I_k \subseteq R$.*

Ejercicio 12.7. *Sean R y S anillos conmutativos. Consideremos el producto $R \times S$ con las proyecciones canónicas*

$$\begin{array}{ccccc} R & \xleftarrow{\pi_1} & R \times S & \xrightarrow{\pi_2} & S \\ r & \longleftarrow\!\shortmid & (r, s) & \longmapsto & s \end{array}$$

1) *Si $\mathfrak{p} \subset R$ y $\mathfrak{q} \subset S$ son ideales primos, demuestre que*

$$\mathfrak{p} \times S := \pi_1^{-1}(\mathfrak{p}) = \{(x,s) \mid x \in \mathfrak{p},\ s \in S\}, \quad R \times \mathfrak{q} = \pi_2^{-1}(\mathfrak{q}) := \{(r,y) \mid r \in R,\ y \in \mathfrak{q}\}$$

son ideales primos en el producto $R \times S$.

2) *Demuestre que si $\mathfrak{P} \subset R \times S$ es un ideal primo, entonces $\mathfrak{P}$ es de la forma $\mathfrak{p} \times S$ o $R \times \mathfrak{q}$ como en 1).*

Indicación: para $e_1 := (1_R, 0_S)$ y $e_2 := (0_R, 1_S)$ note que $e_1 e_2 \in \mathfrak{P}$, así que $e_1 \in \mathfrak{P}$ o $e_2 \in \mathfrak{P}$.

Ensto nos da una biyección natural $\operatorname{Spec}(R \times S) \cong \operatorname{Spec} R \sqcup \operatorname{Spec} S$.

Lema de Zorn

Ejercicio 12.8. *Sea R un anillo conmutativo. Sea $U \subset R$ un subconjunto no vacío tal que $0 \notin U$ y si $x, y \in U$, entonces $xy \in U$.*

1) *Deduzca del lema de Zorn que existe un ideal $\mathfrak{p} \subset R$ que satisface las siguientes propiedades:*

   - $U \cap \mathfrak{p} = \emptyset$,
   - *Si $\mathfrak{p} \subseteq I$ para otro ideal I que satisface $U \cap I = \emptyset$, entonces $I = \mathfrak{p}$.*

2) *Demuestre que $\mathfrak{p}$ es un ideal primo.*

Indicación: basta revisar y entender nuestra prueba de que $N(R) = \bigcap_{\mathfrak{p} \subset R \text{ primo}} \mathfrak{p}$.

Ejercicio 12.9. *Sean R un anillo conmutativo no nulo e $I \subset R$ un ideal propio.*

1) *Sea $R \supset \mathfrak{p}_0 \supseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq I$ una cadena descendente de ideales primos que contienen a I. Demuestre que $\mathfrak{p} := \bigcap_i \mathfrak{p}_i$ es un ideal primo que contiene a I.*

2) *Deduzca del lema de Zorn que en R existen **ideales primos minimales sobre** I; es decir, ideales primos $I \subseteq \mathfrak{p} \subset R$ tales que si $\mathfrak{q} \subseteq \mathfrak{p}$ para otro ideal primo $I \subseteq \mathfrak{q} \subset R$, entonces $\mathfrak{q} = \mathfrak{p}$.*

Ejercicio 12.10. *Sea R un anillo conmutativo noetheriano. En este ejercicio vamos a probar que para todo ideal propio no nulo $I \subset R$ (es decir, $I \neq R$, $I \neq 0$)*

(*) *existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \neq 0$ tales que $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq I$.*

Para llegar a una contradicción, asumamos que esto es falso y existen ideales propios no nulos que no cumplen la propiedad (*).

1) *Demuestre usando el lema de Zorn que en este caso existe un ideal propio no nulo I que es maximal entre los ideales que no cumplen la propiedad (*). Demuestre que I no es primo, así que existen $x, y \in R$ tales que $xy \in I$, pero $x \notin I$ e $y \notin I$.*

2) *Demuestre que para los ideales $A := I + (x)$ y $B := I + (y)$ se tiene $AB \subseteq I$ y son ideales propios no nulos.*

3) *Demuestre que A y B cumplen la propiedad (*): se tiene*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_m \subseteq A, \quad \mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq B$$

para algunos ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}_1, \ldots, \mathfrak{q}_n \subset R$. Deduzca que $\mathfrak{p}_1 \cdots \mathfrak{p}_m \, \mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq I$.

Concluya que hemos obtenido una contradicción.

Localización

Ejercicio 12.11. *En el cuerpo de las series de Laurent $\mathbb{Q}((X))$, encuentre el elemento inverso de $X - X^2$.*

Ejercicio 12.12. *Describa los cuerpos de fracciones $K(R)$ para los anillos*

$$R = \mathbb{Z}[\sqrt{-1}],\ \mathbb{Z}[\sqrt{5}],\ \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big].$$

Ejercicio 12.13. *Sea $R \times S$ un producto de anillos conmutativos no nulos. Consideremos $e := (1,0)$. Demuestre que $(R \times S)[e^{-1}] \cong R$.*
Sugerencia: nota que $\frac{(r,s)}{(1,0)} = \frac{(r,s)}{(1,1)} = \frac{(r,0)}{(1,1)}$ para cualesquiera $r \in R$ y $s \in S$.

Ejercicio 12.14. *Consideremos el anillo finito $R = \mathbb{Z}/n\mathbb{Z}$ donde $n = p_1^{k_1} \cdots p_s^{k_s}$.*

1) *Demuestre que los ideales maximales en R son $\mathfrak{m}_i = p_i\,\mathbb{Z}/n\mathbb{Z}$ para $i = 1, \ldots, s$.*

2) *Demuestre que $R \cong R_{\mathfrak{m}_1} \times \cdots \times R_{\mathfrak{m}_s}$.*

Sugerencia: demuestre que la aplicación canónica $\mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p_i^{k_i}\mathbb{Z}$ satisface la propiedad universal de la localización $\mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})_{\mathfrak{m}_i}$.

Ejercicio 12.15. *Sean R un anillo conmutativo, $U \subseteq R$ un subconjunto multiplicativo y $\phi\colon R \to R[U^{-1}]$ el homomorfismo canónico de localización.*

1) *Para un ideal primo $\mathfrak{p} \subset R$ tal que $\mathfrak{p} \cap U = \emptyset$ compruebe directamente que el ideal $\mathfrak{p}R[U^{-1}] \subset R[U^{-1}]$ (es decir, que $\mathfrak{p}R[U^{-1}] \neq R[U^{-1}]$ y $\frac{r}{u} \cdot \frac{s}{v} \in \mathfrak{p}R[U^{-1}]$ implica $\frac{r}{u} \in \mathfrak{p}R[U^{-1}]$ o $\frac{s}{v} \in \mathfrak{p}R[U^{-1}]$).*

2) *Para un ideal primo $\mathfrak{q} \subset R[U^{-1}]$ compruebe directamente que $\phi^{-1}(\mathfrak{q}) \cap U = \emptyset$ (use la definición original de ideales primos).*

Ejercicio 12.16. *He aquí una generalización de las ideas que hemos ocupado para caracterizar los ideales en $R[U^{-1}]$. Para un homomorfismo de anillos $f\colon R \to S$ e ideales $I \subseteq R$, $J \subseteq S$ definamos*

$$I^e := f(I)\,S \subseteq S, \quad J^c := f^{-1}(J) \subseteq R$$

*(el ideal I^e se llama la **extensión** de I y el ideal J^c se llama la **contracción** de J). Verifique las siguientes propiedades de estas operaciones:*

1) *Si* $I_1 \subseteq I_2$, *entonces* $I_1^e \subseteq I_2^e$.

2) *Si* $J_1 \subseteq J_2$, *entonces* $J_1^c \subseteq J_2^c$.

3) $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$.

4) $I \subseteq I^{ec}$, $J \supseteq J^{ce}$. *Encuentre ejemplos cuando las inclusiones son estrictas.*

5) $J^c = J^{cec}$, $I^e = I^{ece}$.

Ejercicio 12.17. *Sea* $n = p_1^{k_1} \cdots p_s^{k_s}$. *Describa los ideales primos en el anillo*

$$\mathbb{Z}\Big[\frac{1}{n}\Big] := \Big\{ \frac{a}{n^k} \;\Big|\; a \in \mathbb{Z},\ k = 0, 1, 2, 3, \ldots \Big\}.$$

Ejercicio 12.18. *Sea* R *un anillo conmutativo y* $U \subseteq R$ *un subconjunto multiplicativo.*

1) *Para un ideal* $I \subseteq R$ *y un elemento* $x \in R$ *verifique que* $(I : x) := \{r \in R \mid xr \in I\}$ *es un ideal en* R.

2) *Demuestre que hay una biyección entre los ideales en la localización* $R[U^{-1}]$ *y los ideales en* R *tales que* $(I : u) = I$ *para todo* $u \in U$.

Ejercicio 12.19. *Sea* R *un anillo conmutativo. Denotemos por*

$$N(R) := \{x \in R \mid x^n = 0 \text{ para algún } n = 1, 2, 3, \ldots\}$$

el nilradical. Demuestre que para todo subconjunto multiplicativo $U \subseteq R$ *se tiene*

$$N(R[U^{-1}]) = N(R)R[U^{-1}].$$

Ejercicio 12.20. *Sean* R *un anillo conmutativo y* $x \in R$ *algún elemento no nulo.*

1) *Demuestre que* $\operatorname{Ann}(x) := \{r \in R \mid rx = 0\}$ *es un ideal propio en* R.

2) *Demuestre que existe un ideal maximal* $\mathfrak{m} \subset R$ *tal que* $\frac{x}{1} \neq \frac{0}{1}$ *en la localización* $R_{\mathfrak{m}}$.

Anillos locales

Ejercicio 12.21. *Sea* R *un anillo local y sea* $\mathfrak{m}$ *su único ideal maximal. Demuestre que para cualquier* $x \in R$ *se cumple* $x \in R^\times$ *o* $1 - x \in R^\times$.

Ejercicio 12.22. *Demuestre que un anillo es local si y solo si todos los elementos no invertibles en* R *forman un ideal.*

Ejercicio 12.23. *Sea* k *un cuerpo.*

1) *Demuestre que el anillo de series formales* $k[\![X]\!]$ *es local y su ideal maximal es* (X).

   Indicación: véase el ejercicio anterior.

2) *Demuestre que si* R *es un anillo local con ideal maximal* $\mathfrak{m}$, *entonces* $R[\![X]\!]$ *es también local con ideal maximal* $\mathfrak{m} + (X)$.

3) *Use la parte anterior para probar que $k[\![X_1, \ldots, X_n]\!]$ es local y su ideal maximal es $(X_1, \ldots, X_n)$.*

Ejercicio 12.24. *Demuestre que si R es un anillo local, entonces el cociente R/I por cualquier ideal $I \subsetneq R$ es también un anillo local.*

Ejercicio 12.25.

1) *Demuestre que para cualquier cuerpo k el anillo de polinomios $k[X]$ no es local.*

2) *Demuestre que el anillo de series de potencias $\mathbb{Z}[\![X]\!]$ no es local.*

Anillos noetherianos

Ejercicio 12.26. *Sea R un anillo conmutativo noetheriano y $U \subseteq R$ un subconjunto multiplicativo. Demuestre que la localización $R[U^{-1}]$ es también un anillo noetheriano.*

Ejercicio 12.27. *Se dice que un anillo es* ***artiniano***[*] *si toda cadena* descendente *de ideales*

$$R \supseteq I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$$

se estabiliza. Note que $\mathbb{Z}$ es un anillo noetheriano, pero no es artiniano.

Ejercicio 12.28. *Sea X un subconjunto infinito de $\mathbb{N} \times \mathbb{N}$. Demuestre que en X hay un subconjunto infinito de pares (k_ℓ, d_ℓ) para $\ell = 0, 1, 2, 3, \ldots$ tal que*

$$k_0 \leq k_1 \leq k_2 \leq \cdots, \quad d_0 \leq d_1 \leq d_2 \leq \cdots$$

[*] Emil Artin (1898–1962), algebrista y teórico de números alemán.

Capítulo 13
Aritmética

> La matemática es la reina de las ciencias y la aritmética es la reina de las matemáticas.
>
> Gauss

Una gran parte de la teoría de anillos y en general de las matemáticas importantes del fin del siglo XIX fue desarrollada para generalizar la aritmética de los números enteros a los anillos conmutativos, o estudiar las obstrucciones que aparecen en este intento. Esto se estudia en detalles en la teoría de números algebraica, y en este capítulo vamos a ver algunas nociones básicas. En particular, vamos a definir ciertas clases importantes de anillos:

dominios euclidianos $\subsetneq$ dominios de ideales principales $\subsetneq$ dominios de factorización única

y terminar por una breve discusión de anillos de números. Este material generaliza los resultados clásicos sobre los números enteros. El lector puede consultar, por ejemplo, el primer capítulo de [IR1990].

En este capítulo R siempre va a denotar un anillo conmutativo sin divisores de cero; es decir, un dominio de integridad.

13.1 Divisibilidad en dominios de integridad

13.1.1. Definición. Para elementos $x, y \in R$ se dice que x **divide** a y si $y = zx$ para algún $z \in R$. En este caso también se dice que x es un **divisor** de y y que y es un **múltiplo** de x y se escribe "$x \mid y$".

Se dice que x e y son **asociados** si $x \mid y$ e $y \mid x$. En este caso se escribe "$x \sim y$".

Hagamos primero algunas observaciones triviales.

13.1.2. Observación.

1) $1 \mid x$ *para cualquier* $x \in R$,

2) $x \mid 1$ *si y solamente si* $x \in R^\times$,

3) $x \mid 0$ *para cualquier* $x \in R$,

4) $0 \mid x$ *si y solamente si* $x = 0$.

Demostración. En 1) basta notar que $x = 1 \cdot x$. En 2), si $x \mid 1$, entonces $1 = xy$ para algún $y \in R$ y $y = x^{-1}$. En 3), siempre se cumple $0 = 0 \cdot x$ y en 4), si $x = 0 \cdot y$, entonces $x = 0$. ■

La relación $x \sim y$ significa precisamente que son iguales salvo un múltiplo invertible.

13.1.3. Observación. *En un dominio de integridad se cumple* $x \sim y$ *si y solamente si* $y = ux$ *para algún* $u \in R^\times$.

Demostración. Si tenemos $x \sim y$, entonces $x \mid y$ e $y \mid x$; es decir, $x = vy$ e $y = ux$ para algunos $u, v \in R$. Luego, $x = uvx$, así que $x(1 - uv) = 0$. Esto implica que $x = 0$, y en este caso $y = 0$ y se tiene $y = 1 \cdot x$; o $uv = 1$, y en este caso $u \in R^\times$.

Viceversa, si $y = ux$ donde $u \in R^\times$, entonces $x = u^{-1}y$, así que $x \mid y$ e $y \mid x$. ■

13.1.4. Observación. *En un dominio de integridad, si* $z \neq 0$, *entonces* $xz \mid yz$ *implica* $x \mid y$.

Demostración. Si $yz = axz$ para algún a, entonces, puesto que $z \neq 0$, podemos cancelarlo y obtener $y = ax$. ■

Notamos que

1) $x \mid 0$ para todo $x \in R$;

2) si $x \mid y$ e $x \mid z$, entonces $x \mid (y + z)$;

3) si $x \mid y$, entonces $x \mid zy$ para todo $z \in R$.

Esto significa que los múltiplos de x forman un ideal. Es precisamente el ideal generado por x:

$$(x) = \{yx \mid y \in R\}.$$

13.1.5. Definición. Un ideal $I \subseteq R$ tal que $I = (x)$ para algún $x \in R$ se llama un **ideal principal**.

La relación de divisibilidad $x \mid y$ puede ser interpretada en términos de ideales (x) e (y).

13.1.6. Observación (Divisibilidad e ideales principales).

1) $x \mid y$ *si y solamente si* $(x) \supseteq (y)$.

2) $x \sim y$ *si y solamente si* $(x) = (y)$.

3) $x \in R^\times$ *si y solamente si* $(x) = R$.

4) si $x \mid y$, *pero* $y \nmid x$, *entonces* $(x) \supsetneq (y)$.

Demostración. En la parte 1), si $y = z\,x$, entonces $y \in (x)$, y luego $(y) \subseteq (x)$. Viceversa, si $(y) \subseteq (x)$, entonces $y = z\,x$ para algún $z \in R$. La parte 2) sigue inmediatamente de 1). La parte 3) sigue del hecho de que $x \in R^\times$ si y solamente si $x \sim 1$. ■

Notamos que la relación de divisibilidad es reflexiva y transitiva: para cualesquiera $x, y, z \in R$

$$x \mid x,$$
$$x \mid y,\ y \mid z \Longrightarrow x \mid z.$$

La relación $\sim$ es una relación de equivalencia: para cualesquiera $x, y, z \in R$ se cumple

$$x \sim x,$$
$$x \sim y \Longrightarrow y \sim x,$$
$$x \sim y,\ y \sim z \Longrightarrow x \sim z.$$

La relación de divisibilidad es una relación de **preorden** sobre R. Para que esto sea una relación de **orden**, falta la propiedad de antisimetría: $x \mid y$ e $y \mid x$ no implica $x = y$, sino que $x \sim y$ (por la definición). Esto significa que la divisibilidad es una relación de orden sobre las clases $R/\sim$.

Notamos que todo elemento y es divisible por 1 y por sí mismo, y en consecuencia por todo x tal que $x \sim 1$ (es decir, $x \in R^\times$) o $x \sim y$. Estos divisores de y son triviales. Un elemento que no tiene divisores no triviales se llama **irreducible**.

13.1.7. Definición. Un elemento $p \in R$ es **irreducible** si

1) $p \neq 0$ y $p \notin R^\times$,

2) $x \mid p$ implica que $x \in R^\times$ o $x \sim p$.

Se dice que un elemento $x \in R$ tal que $x \neq 0$ y $x \notin R^\times$ es **reducible** si existe un divisor no trivial $y \mid x$; es decir, $y \notin R^\times$ y $y \not\sim x$. Tenemos entonces cuatro clases disjuntas de elementos:

$$R = R^\times \sqcup \{0\} \sqcup \{\text{irreducibles}\} \sqcup \{\text{reducibles}\}.$$

13.1.8. Observación. *Un elemento $p \neq 0$ es irreducible si y solamente si el ideal (p) es **maximal entre los ideales principales**; es decir,*

1) $(p) \neq R$,

2) si $(p) \subseteq (x) \subseteq R$, entonces $(p) = (x)$ o $(x) = R$.

Demostración. Está claro a partir de 13.1.6. ■

El momento delicado de la teoría general es la distinción entre los elementos primos e irreducibles.

13.1.9. Definición. Un elemento $p \in R$ es **primo** si

1) $p \neq 0$ y $p \notin R^\times$,

2) para cualesquiera $x, y \in R$, si $p \mid xy$, entonces $p \mid x$ o $p \mid y$.

13.1.10. Ejemplo. En el anillo de los números enteros $\mathbb{Z}$ los elementos invertibles son ± 1. Se cumple $x \sim y$ si y solo si $y = \pm x$. Las clases de equivalencia en $\mathbb{Z}$ módulo la relación de equivalencia $\sim$ pueden ser representadas por los números no negativos.

Los elementos irreducibles son $\pm p$ donde $p = 2, 3, 5, 7, 11, \ldots$ es primo. Convenientemente, los elementos primos son los mismos. ▲

13.1.11. Observación. *Un elemento $p \neq 0$ es primo si y solamente si el ideal $(p) \subseteq R$ es primo.*

Demostración. La condición $p \notin R^\times$ es equivalente a $(p) \neq R$. La condición $p \mid xy \Rightarrow p \mid x$ o $p \mid y$ es equivalente a $xy \in (p) \Rightarrow x \in (p)$ o $y \in (p)$. ■

13.1.12. Observación. *Todo elemento primo es irreducible.*

Demostración. Supongamos que $p \in R$ es un elemento que no es irreducible. Esto significa que $p = xy$, donde $x, y \notin R^\times$ y $x \not\sim p$, $y \not\sim p$. Entonces, $p \mid xy$, pero $p \nmid x$ y $p \nmid y$, así que p no es primo. ■

En general, un elemento irreducible no tiene por qué ser primo.

13.1.13. Contraejemplo. En el anillo cociente $k[X, Y, Z]/(Z^2 - XY)$ la clase $\overline{Z}$ es irreducible. Sin embargo, se tiene $\overline{Z} \mid \overline{X}\,\overline{Y}$, aunque $\overline{Z} \nmid \overline{X}$ y $\overline{Z} \nmid \overline{Y}$. Esto significa que $\overline{Z}$ es un elemento irreducible, pero no es primo. ▲

13.1.14. Contraejemplo. Si $n \geq 3$ es un entero libre de cuadrados, entonces en el anillo

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

el número 2 es irreducible, pero no es primo. Véase el ejercicio 13.2. ▲

13.1.15. Definición. Para $x_1, \ldots, x_n \in R$ se dice que $d \in R$ es un **máximo común divisor** de $x_1, \ldots, x_n$ si

1) $d \mid x_1$, …, $d \mid x_n$,

2) si para otro elemento $z \in R$ se cumple $z \mid x_1$, …, $z \mid x_n$, entonces $z \mid d$.

(¡Note que la definición no afirma que tal d siempre existe!)

13.1.16. Observación. *Si para $x_1, \ldots, x_n \in R$ existe su máximo común divisor, entonces este está definido de modo único salvo $\sim$. En este caso se escribe por abuso de notación $d = \operatorname{mcd}(x_1, \ldots, x_n)$.*

Demostración. Si d e d' son mcd de $x_1, \ldots, x_n$, entonces la definición implica que $d \mid d'$ y $d' \mid d$. ■

Debido a la última observación, todas las identidades con mcd se entienden salvo $\sim$.

13.1.17. Ejemplo. Para los números enteros $\mathbb{Z}$, normalmente como $\operatorname{mcd}(x_1, \ldots, x_n)$ se toma un número positivo. ▲

13.1.18. Ejemplo. Tenemos $\operatorname{mcd}(x, 0) = x$ para cualquier x. En efecto, $x \mid x$ y $x \mid 0$. La segunda condición de la definición de mcd se cumple trivialmente. De la misma manera, se ve que $\operatorname{mcd}(x, x) = x$ para cualquier x. ▲

13.1.19. Observación. *El mcd tiene las siguientes propiedades.*

1) $\mathrm{mcd}(x,y) = x$ *si y solamente si* $x \mid y$;

2) *si* $\mathrm{mcd}(x,y)$ *existe, entonces* $\mathrm{mcd}(y,x)$ *también existe y se tiene* $\mathrm{mcd}(x,y) = \mathrm{mcd}(y,x)$;

3) $\mathrm{mcd}(\mathrm{mcd}(x,y),z) = \mathrm{mcd}(x,\mathrm{mcd}(y,z)) = \mathrm{mcd}(x,y,z)$, *en el sentido de que si uno de los tres elementos existe, los otros dos también existen y todos son iguales.*

Demostración. Las primeras dos propiedades son evidentes de la definición. Para la tercera, se puede notar que las propiedades que definen a $\mathrm{mcd}(\mathrm{mcd}(x,y),z)$ y $\mathrm{mcd}(x,\mathrm{mcd}(y,z))$ corresponden a la propiedad que define a $\mathrm{mcd}(x,y,z)$. ■

13.1.20. Lema. *Se cumple* $\mathrm{mcd}(zx,zy) = z\ \mathrm{mcd}(x,y)$ *(es decir, si uno de estos elementos existe, entonces el otro también existe y son asociados).*

Demostración. Si $z = 0$, esto es obvio, así que podemos asumir que $z \neq 0$.

Sea $d = \mathrm{mcd}(x,y)$. Entonces, $zd \mid zx$ y $zd \mid zy$, así que $zd \mid \mathrm{mcd}(zx,zy)$. Viceversa, puesto que $z \mid zx$ y $z \mid zy$, se tiene $z \mid \mathrm{mcd}(zx,zy)$, tenemos $\mathrm{mcd}(zx,zy) = zc$ para algún $c \in R$. Esto significa que $zc \mid zx$ y $zc \mid zy$. Pero puesto que $z \neq 0$, esto implica que $c \mid x$ y $c \mid y$, así que $c \mid d$, y luego $zc = \mathrm{mcd}(zx,zy) \mid zd$. ■

De la misma manera se define el mínimo común múltiplo $\mathrm{mcm}(x,y)$.

13.1.21. Definición. Para $x_1,\ldots,x_n \in R$ se dice que $m \in R$ es un **mínimo común múltiplo** de $x_1,\ldots,x_n$ si

1) $x_1 \mid m$, …, $x_n \mid m$,

2) si para otro elemento $z \in R$ se cumple $x_1 \mid z$, …, $x_n \mid z$, entonces $m \mid z$.

De nuevo, estas condiciones definen a m de modo único salvo la relación $\sim$, y normalmente se escribe $m = \mathrm{mcm}(x_1,\ldots,x_n)$.

13.1.22. Ejemplo. Tenemos $\mathrm{mcm}(x,0) = 0$ para todo $x \in R$. En efecto, $x \mid 0$ y $0 \mid 0$. Luego, si hay otro elemento z tal que $x \mid z$ y $0 \mid z$, lo último implica que $z = 0$, y de hecho $0 \mid 0$. ▲

El mcm satisface las mismas propiedades que el mcd.

13.1.23. Observación.

1) $\mathrm{mcm}(x,y) = x$ *si y solamente si* $y \mid x$.
   En particular, $\mathrm{mcm}(x,x) = \mathrm{mcd}(x,1) = x$.

2) *Si* $\mathrm{mcm}(x,y)$ *existe, entonces* $\mathrm{mcm}(y,x)$ *también existe y se tiene* $\mathrm{mcm}(x,y) = \mathrm{mcm}(y,x)$.

3) $\mathrm{mcm}(\mathrm{mcm}(x,y),z) = \mathrm{mcm}(x,\mathrm{mcm}(y,z)) = \mathrm{mcm}(x,y,z)$, *en el sentido de que si uno de los tres elementos existe, los otros dos también existen y todos son iguales.*

13.1.24. Proposición. *Si para* $x,y \in R$ *existe uno de los* $\mathrm{mcd}(x,y)$ *o* $\mathrm{mcm}(x,y)$, *entonces existe el otro y se cumple*

$$\mathrm{mcd}(x,y)\ \mathrm{mcm}(x,y) = xy.$$

Demostración. Supongamos por ejemplo que existe $d = \mathrm{mcd}(x, y)$. El caso de $x = y = 0$ es trivial y podemos descartarlo desde el principio. Entonces, se puede asumir que $d \neq 0$.

En particular, esto significa que $d \mid x$ e $d \mid y$. Escribamos

$$x = d\,x', \quad y = d\,y'$$

para algunos $x', y' \in R$. Definamos

$$m := d\,x'\,y'.$$

Tenemos $dm = xy$ y nos gustaría probar que m satisface la propiedad de $\mathrm{mcm}(x, y)$. Primero,

$$m = x\,y' = x'\,y,$$

así que $x \mid m$ e $y \mid m$. Sea z otro elemento tal que $x \mid z$ e $y \mid z$. Necesitamos deducir que $m \mid z$. Notamos que según 13.1.20

$$d = \mathrm{mcd}(x, y) = \mathrm{mcd}(dx', dy') = d \cdot \mathrm{mcd}(x', y'),$$

y luego

$$\mathrm{mcd}(x', y') = 1.$$

Pero en este caso

$$\mathrm{mcd}(zx', zy') = z\ \mathrm{mcd}(x', y') = z.$$

Luego, $m \mid zx'$ y $m \mid zy'$, y por lo tanto $m \mid z$. ■

13.2 Dominios de ideales principales

13.2.1. Definición. Sea R un dominio de integridad. Se dice que R es un **dominio de ideales principales** si R es un dominio de integridad y todo ideal $I \subseteq R$ es principal; es decir $I = (x)$ para algún $x \in R$.

13.2.2. Ejemplo. Todo cuerpo es obviamente un dominio de ideales principales.

El anillo $\mathbb{Z}$ es un dominio de ideales principales. Esto ya no es tan obvio y se demuestra usando la división con resto; véase el apéndice A. Usando las mismas ideas, vamos a ver un poco más adelante que el anillo de polinomios $k[X]$ (donde k es un cuerpo) y el anillo de los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ son también dominios de ideales principales.

Los anillos $\mathbb{Z}\left[\frac{1}{n}\right]$ y $\mathbb{Z}_{(p)}$ para p primo son también dominios de ideales principales. Esto sigue de la descripción de los ideales en la localización y el hecho de que $\mathbb{Z}$ es un dominio de ideales principales. ▲

13.2.3. Ejemplo. El anillo de polinomios en dos variables $k[X, Y]$ no es un dominio de ideales principales. Por ejemplo, tenemos el ideal (X, Y) que no puede ser generado por un elemento.

En efecto, asumamos que $(X, Y) = (f)$ para algún polinomio $f \in k[X, Y]$. Entonces, $(X) \subseteq (f)$ y $(Y) \subseteq (f)$, pero esto significa que $f \mid X$ y $f \mid Y$. Sin embargo, los elementos X e Y son irreducibles y esto implica que f es invertible en $k[X, Y]$, de donde $(f) = k[X, Y]$. Contradicción. ▲

13.2.4. Ejemplo. El anillo de polinomios $\mathbb{Z}[X]$ no es un dominio de ideales principales. Por ejemplo, el ideal (p, X) donde p es un número primo no puede ser generado por un elemento. Notamos que este ideal es propio:

$$(p, X) = \{p\,f + X\,g \mid f, g \in \mathbb{Z}[X]\} = \{a_0 + a_1\,X + \cdots + a_d\,X^d \mid a_0, a_1, \ldots, a_d \in \mathbb{Z},\ p \mid a_0\}.$$

En efecto, el ideal (p, X) es maximal. De hecho, consideremos el homomorfismo sobreyectivo de anillos

$$\begin{aligned} \mathbb{Z}[X] &\twoheadrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}, \\ f &\mapsto f(0) \pmod{p} \end{aligned}$$

—este homomorfismo primero evalúa un polinomio en 0 y luego reduce el resultado módulo p. El núcleo de este homomorfismo viene dado por los polinomios con el término constante divisible por p, pero esto es precisamente (p, X). El primer teorema de isomorfía nos permite concluir que $\mathbb{Z}[X]/(p, X) \cong \mathbb{Z}/p\mathbb{Z}$, lo que es un cuerpo.

Ahora asumamos que $(p, X) = (f)$ para algún polinomio $f \in \mathbb{Z}[X]$. En particular, esto quiere decir que $(p) \subseteq (f)$ y por ende $f \mid p$, así que $f = \pm 1$ o $\pm p$. Si $f = \pm p$, el ideal $(f) = p\,\mathbb{Z}[X]$ no puede contener a X. Si $f = \pm 1$, entonces $(f) = \mathbb{Z}[X]$. Contradicción. ▲

En general, es muy difícil encontrar el número mínimo posible de generadores para un ideal.

13.2.5. Proposición. *Sea R un dominio de ideales principales que no es un cuerpo. Entonces, los ideales maximales en R son precisamente los ideales primos no nulos.*

(Note que la hipótesis de que R no sea un cuerpo es importante: ¡en un cuerpo el ideal nulo es maximal!)

Demostración. Si $(p) \subset R$ un ideal primo no nulo, entonces $p \in R$ es un elemento primo (véase 13.1.11). Si tenemos $(p) \subseteq (x)$ para otro ideal, entonces $x \mid p$, lo que implica $x \in R^\times$ o $x \sim p$; es decir, $(x) = R$ o $(x) = (p)$. ■

13.2.6. Proposición. *En un dominio de ideales principales todo elemento irreducible es primo.*

Demostración. Si $p \in R$ es irreducible, entonces el ideal (p) es maximal entre los ideales principales. Pero por la hipótesis *todos* los ideales son principales, así que (p) es un ideal maximal en R. Todo ideal maximal es primo, lo que significa que p es un elemento primo. ■

13.2.7. Proposición (Relación de Bézout). *En todo dominio de integridad R tenemos*

1) *si $(x_1, \ldots, x_n) = (d)$, entonces $d = \operatorname{mcd}(x_1, \ldots, x_n)$;*
2) *si $(x_1) \cap \cdots \cap (x_n) = (m)$, entonces $m = \operatorname{mcm}(x_1, \ldots, x_n)$.*

Además, si R es un dominio de ideales principales, entonces mcd *y* mcd *siempre existen. En este caso se tiene*

1) *$(x_1, \ldots, x_n) = (d)$, donde $d = \operatorname{mcd}(x_1, \ldots, x_n)$;*

2) $(x_1) \cap \cdots \cap (x_n) = (m)$, *donde* $m = \operatorname{mcm}(x_1, \ldots, x_n)$.

Demostración. Vamos a ver el caso del mcd; el caso del mcm es parecido.

Si $(x_1, \ldots, x_n) = (d)$, entonces $(x_i) \subseteq (d)$ para todo $i = 1, \ldots, n$, lo que significa que $d \mid x_i$. Supongamos que $z \mid x_i$ para todo i. Tenemos entonces

$$c_1\, x_1 + \cdots + c_n\, x_n = d$$

para algunos c_i y luego $z \mid d$.

Ahora si R es un dominio de ideales principales, sea $d = \operatorname{mcd}(x_1, \ldots, x_n)$. Tenemos $d \mid x_i$ para todo i; es decir, $(x_i) \subseteq (d)$. El ideal $(x_1, \ldots, x_n)$ es el ideal mínimo tal que $(x_i) \subseteq (x_1, \ldots, x_n)$ para todo i, así que $(x_1, \ldots, x_n) \subseteq (d)$. Para ver la otra inclusión, notamos que $(x_1, \ldots, x_n) = (z)$ para algún $z \in R$, puesto que R es un dominio de ideales principales. Luego, $z = \operatorname{mcd}(x_1, \ldots, x_n)$ por la primera parte, así que $(z) = (d)$. ■

La igualdad $(x_1, \ldots, x_n) = (d)$ donde $d = \operatorname{mcd}(x_1, \ldots, x_n)$ significa que en un dominio de ideales principales R, el máximo común divisor de los x_i puede ser expresado como una combinación R-lineal de los x_i. Esto se llama la relación de Bézout.

13.2.8. Corolario (Elementos coprimos). *En un dominio de ideales principales,* $\operatorname{mcd}(x, y) = 1$ *si y solamente si* $(x, y) = R$.

13.2.9. Ejemplo. En el anillo $k[X, Y]$ los elementos X e Y son irreducibles y son divisibles solamente por las constantes no nulas, así que $\operatorname{mcd}(X, Y) = 1$. Sin embargo, $(X, Y) \neq k[X, Y]$. Esto demuestra una vez más que el anillo $k[X, Y]$ no es un dominio de ideales principales.

De la misma manera, en $\mathbb{Z}[X]$ se tiene $\operatorname{mcd}(p, X) = 1$, aunque $(p, X) \neq \mathbb{Z}[X]$. ▲

13.3 Dominios de factorización única

13.3.1. Definición. Se dice que un dominio de integridad R es un **dominio de factorización única** si todo elemento no nulo $x \in R$ puede ser descompuesto en factores irreducibles y esta descomposición es única salvo el orden de los múltiplos y la relación de equivalencia $\sim$.

En otras palabras, para dos descomposiciones

$$x = u\, p_1 \cdots p_s = v\, q_1 \cdots q_t$$

donde $u, v \in R^\times$ y p_i, q_j son irreducibles, se tiene necesariamente $s = t$, y después de una permutación de los múltiplos, se cumple $p_i \sim q_i$ para todo $1 \leq i \leq s$.

13.3.2. Comentario. En la factorización $x = u\, p_1 \cdots p_s$ *no* se supone que entre los p_i no hay repeticiones. Diferentes p_i y p_j pueden ser asociados.

13.3.3. Ejemplo. Todo cuerpo es trivialmente un dominio de factorización única: todo elemento no nulo es invertible y la condición de la definición es vacía. ▲

13.3.4. Ejemplo. El anillo de los enteros $\mathbb{Z}$ es un dominio de factorización única. Este resultado se conoce como el **teorema fundamental de aritmética** y fue probado rigurosamente por primera vez por Gauss. De hecho, eventualmente en este capítulo lo vamos a probar otra vez más. ▲

Para probar que algo es un dominio de factorización única, necesitamos ciertas herramientas especiales. Lo que es fácil es probar es que un anillo específico no posea factorizaciones únicas: basta encontrar dos diferentes factorizaciones del mismo elemento.

13.3.5. Ejemplo. En el anillo $\mathbb{Z}[\sqrt{-5}]$ definamos la norma por

$$N(a+b\sqrt{-5}) := (a+b\sqrt{-5})\,(a-b\sqrt{-5}) = a^2+5\,b^2.$$

Esto es una función multiplicativa:

$$N(xy) = N(x)\,N(y) \quad \text{para cualesquiera } x, y \in \mathbb{Z}[\sqrt{-5}].$$

Ahora si $x \mid y$, entonces $y = zx$ y $N(y) = N(z)\,N(x)$, así que $N(x) \mid N(y)$. Se sigue que los elementos invertibles deben tener norma 1, así que $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$. Notamos que si $x \mid y$ donde $N(x) = N(y)$, entonces $y = zx$ donde $N(z) = 1$, así que $x \sim y$; es decir, $x = \pm y$.

Notamos que los números 2 y 3 no pueden ser expresados como $a^2+5\,b^2$, así que en $\mathbb{Z}[\sqrt{-5}]$ no hay elementos de esta norma. Esto nos lleva a las siguientes conclusiones.

1) $1 \pm \sqrt{-5}$ es irreducible. En efecto, si $x \mid (1 \pm \sqrt{-5})$, entonces $N(x) \mid 6$ y luego $N(x) = 1$ o $N(x) = 6$. En el primer caso, $x \in \mathbb{Z}[\sqrt{-5}]^\times$; en el segundo caso, $x \sim 1 \pm \sqrt{-5}$.

2) 2 es irreducible: si $x \mid 2$, entonces $N(x) \mid 4$ y $N(x) = 1$ o 4 y tenemos dos casos parecidos.

3) 3 es irreducible. Si $x \mid 3$, entonces $N(x) \mid 9$ y $N(x) = 1$ o 9.

Ahora la identidad

$$6 = 2 \cdot 3 = (1+\sqrt{-5})\,(1-\sqrt{-5})$$

significa que 6 puede ser expresado de dos maneras diferentes como un producto de elementos irreducibles. ▲

13.3.6. Ejemplo. Consideremos el anillo $\mathbb{Z}[\sqrt{-3}]$. La norma viene dada por $N(a+b\sqrt{-3}) = a^2+3\,b^2$. Los elementos de norma 1 son ± 1 y enotratonces $\mathbb{Z}[\sqrt{-3}]^\times = \{\pm 1\}$. Está claro que no existen elementos de norma 2.

Ahora 2 es un elemento irreducible: si $x \mid 2$, entonces $N(x) \mid 4$, lo que implica $N(x) = 1$ o 4. El elemento $1 \pm \sqrt{-3}$ también tiene norma 4 y es irreducible por las mismas razones. La identidad

$$4 = 2 \cdot 2 = (1+\sqrt{-3})\,(1-\sqrt{-3}) \tag{13.1}$$

demuestra que $\mathbb{Z}[\sqrt{-3}]$ no es un dominio de factorización única.

Sin embargo, se puede considerar el anillo más grande

$$\mathbb{Z}[\omega], \quad \omega := \frac{1+\sqrt{-3}}{2}.$$

La norma es

$$N\,(a+b\,\omega) = \left(a+b\,\frac{1+\sqrt{-3}}{2}\right)\left(a+b\,\frac{1-\sqrt{-3}}{2}\right) = a^2+ab+b^2.$$

Ahora hay más elementos de norma 1: son

$$\pm 1, \quad \pm\omega, \quad \pm(1-\omega),$$

y de hecho son precisamente las raíces de la unidad de orden 6:

$$(1-\omega)^2 = -\omega, \quad (1-\omega)^3 = -1.$$

Ahora podemos volver a nuestra factorización de 4 en (13.1). La fórmula se vuelve

$$4 = 2 \cdot 2 = 2\,\omega \cdot 2\,(1-\omega).$$

Pero ω y $1-\omega$ son invertibles, así que esta fórmula ya no es un ejemplo de diferentes factorizaciones. En efecto, el anillo $\mathbb{Z}[\omega]$ es un dominio de factorización única, pero lo vamos a ver un poco más adelante usando otras herramientas. ▲

El descubrimiento de anillos que no son dominios de factorización única fue uno de los sucesos más importantes en la matemática del siglo XIX.

13.3.7. Lema. *En un anillo noetheriano, todo elemento no invertible es divisible por un elemento irreducible.*

Demostración. Sea R un anillo noetheriano y $x \in R$ un elemento tal que $x \neq 0$ y $x \notin R^\times$. Si x es irreducible, no hay nada que probar. Si x es reducible, entonces podemos escribir $x = x_1\,y_1$ donde x_1 es un divisor no trivial: $x_1 \notin R^\times$ y $x_1 \not\sim x$. Si x_1 es irreducible, la prueba está terminada. En el caso contrario, podemos escribir $x_1 = x_2\,y_2$ donde $x_2 \notin R^\times$ y $x_2 \not\sim x_1$. Continuando de esta manera, se obtienen elementos $x_1, x_2, x_3, \ldots$ tales que

$$x_1 \mid x, \quad x_2 \mid x_1, \quad x_3 \mid x_2, \quad x_4 \mid x_3, \quad \ldots,$$

lo que nos da una cadena de ideales

$$(x) \subseteq (x_1) \subseteq (x_2) \subseteq (x_3) \subseteq (x_4) \subseteq \cdots \subset R.$$

Pero R es noetheriano por hipótesis, así que en algún momento la cadena se estabiliza, lo que significa que $(x_n) = (x_{n+1})$ para n suficientemente grande; es decir, $x_n \sim x_{n+1}$. Podemos concluir que el proceso siempre termina y nos da un factor irreducible de x. ■

13.3.8. Lema. *Sea R un anillo noetheriano. Todo elemento $x \neq 0$ posee una **factorización en irreducibles**; es decir, puede ser escrito como*

$$x = u\,p_1 \cdots p_n$$

donde $u \in R^\times$ y $p_1, \ldots, p_n \in R$ son elementos irreducibles.

Demostración. Sea R un anillo noetheriano. Si para $x \neq 0$ se tiene $x \in R^\times$ o x es irreducible, no hay que probar nada. En el caso contrario, por el resultado anterior, podemos escribir $x = p_1\,x_1$ donde p_1 es irreducible. Luego, si $x_1 \in R^\times$ o x_1 es irreducible, la prueba está

terminada. En el caso contrario, escribamos $x_1 = p_2\, x_2$, etcétera. Esto nos da una cadena de ideales

$$(x) \subseteq (x_1) \subseteq (x_2) \subseteq (x_3) \subseteq \cdots \subset R.$$

Esta cadena necesariamente se estabiliza, lo que significa que $x_n \sim x_{n+1}$ para n suficientemente grande, así que x_n es irreducible. Tenemos entonces

$$x = p_1 x_1 = p_1 p_2 x_2 = \cdots = p_1 \cdots p_n x_n$$

donde los factores de la última expresión son irreducibles. ■

Para probar que algo es un dominio de factorización única, se puede usar el siguiente criterio.

13.3.9. Teorema. *Sea R un dominio de integridad donde todo elemento admite factorización en elementos irreducibles. Entonces, R es un dominio de factorización única si y solo si todo elemento irreducible es primo.*

Demostración. Supongamos primero que R es un dominio de factorización única. Sea p un elemento irreducible. Hay que probar que p es primo. Si $p \mid xy$, se tiene $xy = pz$ para algún $z \in R$. Factoricemos x, y, z en elementos irreducibles:

$$x = u\, p_1 \cdots p_r, \quad y = v\, p_{r+1} \cdots p_s, \quad z = w\, q_1 \cdots q_t,$$

donde $u, v, w \in R^\times$, $p_1, \ldots, p_s$, $q_1, \ldots, q_t$ son irreducibles. Tenemos

$$uv\, p_1 \cdots p_s = w\, p\, q_1 \cdots q_t.$$

Por la unicidad de factorizaciones, tenemos $p \sim p_i$ para algún $1 \leq i \leq r$. Esto quiere decir que $p \mid x$ o $p \mid y$.

Ahora supongamos que todo elemento irreducible es primo. En este caso la hipótesis nos dice que todo elemento admite una factorización en elementos primos

$$x = u\, p_1 \cdots p_s.$$

Falta ver que estas factorizaciones son únicas. Sea entonces

$$x = v\, q_1 \cdots q_t$$

otra factorización. Sin pérdida de generalidad, asumamos que $s \leq t$ y procedamos por inducción sobre s.

Si $s = 0$, no hay que probar nada: $u = v\, q_1 \cdots q_t$ para $t > 0$ implica que $q_1 \cdots q_t = uv^{-1}$ es invertible, pero luego todo q_i es invertible, lo que no es el caso, puesto que los q_i son primos. Entonces, $t = 0$.

Asumamos que el resultado es cierto para $s - 1$ factores. Consideremos la igualdad

$$u\, p_1 \cdots p_s = v\, q_1 \cdots q_t.$$

Dado que p_s es primo y $p_s \mid v\, q_1 \cdots q_t$, tenemos $p_s \mid q_i$ para algún $1 \leq i \leq t$ (notamos que p_s, siendo primo, no puede dividir al elemento invertible v). Después de una renumeración de los múltiplos, podemos asumir que $p_s \mid q_t$. Pero q_t es también primo, así que $p_s \sim q_t$; es decir, $p_s = w\, q_t$ para algún $w \in R^\times$. Ahora en la identidad

$$u\, p_1 \cdots p_{s-1}\, (w\, q_t) = v\, q_1 \cdots q_{t-1}\, q_t$$

podemos cancelar q_t y obtener

$$uw\, p_1 \cdots p_{s-1} = v\, q_1 \cdots q_{t-1}.$$

Por la hipótesis de inducción, se tiene $s - 1 = t - 1$ y $p_i \sim q_i$ para todo $1 \leq i \leq s - 1$, después de una permutación de los múltiplos. ■

13.3.10. Corolario. *Todo dominio de ideales principales es un dominio de factorización única.*

Demostración. Siendo un dominio de ideales principales, en particular el anillo es noetheriano y por ende admite factorización en elementos irreducibles según 13.3.8. En 13.2.6 hemos probado en que en un dominio de ideales principales todo elemento irreducible es primo. ■

Hay muchos ejemplos de dominios de factorización única que no son dominios de ideales principales. Por ejemplo, el anillo de polinomios en n variables $k[X_1, \ldots, X_n]$ donde k es un cuerpo es un dominio de factorización única. Lo vamos a probar más adelante. Nuestro próximo objetivo es obtener algún método para ver que ciertos anillos son dominios de ideales principales. Para esto nos va a servir la noción de **dominios euclidianos**.

13.4 Dominios euclidianos

Un dominio euclidiano es un dominio de integridad que admite el algoritmo de división con resto.

13.4.1. Definición. Se dice que un dominio de integridad R es un **dominio euclidiano** si sobre R existe una función $\delta\colon R \setminus \{0\} \to \mathbb{N}$ (llamada **norma euclidiana**) que satisface la siguiente propiedad. Para todo $x, y \in R$, $y \neq 0$ existen $q, r \in R$ tales que $x = qy + r$, donde $r = 0$ o $\delta(r) < \delta(y)$.

13.4.2. Comentario. No se supone que los elementos q, r son únicos.

El ejemplo primordial de dominios euclidianos fue estudiado por Euclides en sus "Elementos".

13.4.3. Ejemplo. El anillo de los enteros $\mathbb{Z}$ es un dominio euclidiano respecto al valor absoluto $\delta(x) := |x|$. En efecto, dados $m, n \in \mathbb{Z}$, $n \neq 0$, podemos considerar el conjunto

$$X := \{m - xn \mid x \in \mathbb{Z}\}.$$

Notamos que este conjunto contiene elementos no negativos. Sea $r = m - qn$ el elemento mínimo no negativo en X. Si tenemos $r \geq |n|$, podemos considerar dos casos:

1) si $n > 0$, entonces $r = m - qn \geq n$, así que

$$0 \leq m - (q+1)\, n < r.$$

2) si $n < 0$, entonces $r = m - qn \geq -n$, así que

$$0 \leq m - (q-1)\, n < r.$$

Pero ambos casos contradicen nuestra elección de r. Entonces, necesariamente $0 \leq r < |n|$. ▲

13.4.4. Ejemplo. Sea k un cuerpo. El anillo de polinomios en una variable $k[X]$ es un dominio euclidiano respecto al grado $\delta(f) := \deg f$. Sean $f, g \in k[X]$ dos polinomios, $g \neq 0$. Nos gustaría probar que existen polinomios $q, r \in k[X]$ tales que

$$f = qg + r, \quad r = 0 \text{ o } \deg r < \deg g.$$

Si $\deg f < \deg g$, podemos tomar $q = 0$ y $r = f$. En el caso contrario, procedamos por inducción sobre $\deg f$. Si tenemos

$$f = a_d\, X^d + a_{d-1}\, X^{d-1} + \cdots + a_1\, X + a_0,$$

donde $a_d \neq 0$ y

$$g = b_n\, X^n + b_{n-1}\, X^{n-1} + \cdots + b_1\, X + b_0,$$

donde $b_n \neq 0$ y $d \geq n$, consideremos

$$f' := f - a_d\, b_n^{-1}\, X^{d-n}\, g.$$

Notamos que $\deg f' < \deg f$. Por inducción, podemos escribir

$$f' = q'g + r, \quad r = 0 \text{ o } \deg r < \deg g.$$

Tenemos

$$f = (q' + a_d\, b_n^{-1}\, X^{d-n})\, g + r.$$

De hecho, lo que acabamos de describir es el algoritmo de división habitual. Notamos que es importante que los coeficientes de los polinomios estén en un cuerpo. En general, este argumento funciona si el coeficiente mayor de g es invertible; por ejemplo si es igual a 1 (en este caso se dice que g es un polinomio **mónico**). ▲

13.4.5. Comentario. El ejemplo del anillo $k[X]$ es la única razón por que en la definición el caso de $r = 0$ se considera por separado. Tenemos $\deg(0) = -\infty$, pero nos gustaría usar el grado como la norma euclidiana.

13.4.6. Ejemplo. El anillo de los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ es un dominio euclidiano respecto a la norma

$$N(a + b\sqrt{-1}) := (a + b\sqrt{-1})\,(a - b\sqrt{-1}).$$

En efecto, dados dos elementos $x, y \in \mathbb{Z}[\sqrt{-1}]$, $y \neq 0$, podemos dividir x por y en el cuerpo de fracciones $\mathbb{Q}(\sqrt{-1})$:

$$\frac{x}{y} = s + t\sqrt{-1} \quad \text{para algunos } s, t \in \mathbb{Q}.$$

Ahora podemos escoger $m, n \in \mathbb{Z}$ tales que

$$|s - m| \leq \frac{1}{2}, \quad |t - n| \leq \frac{1}{2}.$$

Pongamos

$$q := m + n\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$$

y

$$r := x - qy = (s + t\sqrt{-1})\, y - y\,(m + n\sqrt{-1}) = y\,(s - m + (t - n)\sqrt{-1}).$$

Por la multiplicatividad de la norma,

$$N(r) = N(y)\, N(s - m + (t - n)\sqrt{-1}) = N(y)\left((s - m)^2 + (t - n)^2\right) \leq \frac{1}{2} N(y).$$

En particular,

$$x = qy + r, \quad 0 \leq N(r) < N(y).$$

▲

La razón de ser de la noción de dominio euclidiano es el siguiente resultado.

13.4.7. Teorema. *Todo dominio euclidiano es un dominio de ideales principales.*

Demostración. Sea R un dominio euclidiano y sea $I \subseteq R$ un ideal. Necesitamos probar que I es un ideal principal. Si $I = (0)$, no hay que probar nada. Si $I \neq (0)$, sea $x \in I$ un elemento con la norma euclidiana $\delta(x)$ mínima posible. Tenemos $(x) \subseteq I$. Supongamos que existe un elemento $y \in I$ tal que $y \notin (x)$. Esto quiere decir que y no puede ser escrito como qx para algún $q \in R$. Podemos dividir y por x con resto: tenemos

$$y = qx + r, \quad r \neq 0,\ \delta(r) < \delta(x)$$

para algunos $q, r \in R$. Sin embargo, $r = y - qx \in I$ y esto contradice nuestra elección de x. Podemos concluir que $I = (x)$. ■

13.4.8. Corolario. *Todo dominio euclidiano es un dominio de factorización única.*

En general, existen dominios de ideales principales que no son dominios euclidianos. Sin embargo, no es fácil encontrar un ejemplo específico: hay que probar que cierto dominio de ideales principales no admite *ninguna* norma euclidiana.

13.4.9. Ejemplo (Para el lector interesado). Sea R un dominio euclidiano que no es un cuerpo. Sea $x \in R$ un elemento no nulo y no invertible con el mínimo posible valor $\delta(x)$. Esto implica que para cualquier elemento $y \in R$ tenemos

$$y = qx + r, \quad \text{donde } r = 0 \text{ o } \delta(r) < \delta(x).$$

Por nuestra elección de x, esto significa que hay dos posibilidades: $x \mid y$ o $r \in R^\times$.

Ahora consideremos el anillo

$$\mathbb{Z}[\omega], \quad \omega := \frac{1+\sqrt{-19}}{2}.$$

Al analizar la norma

$$N(a+b\,\omega) := (a+b\,\omega)\,(a+b\,\overline{\omega}) = a^2+ab+5\,b^2$$

se ve que $\mathbb{Z}[\omega]^\times = \{\pm 1\}$ y que en $\mathbb{Z}[\omega]$ no hay elementos de norma 2 o 3. Esto implica que los números 2 y 3 son irreducibles en $\mathbb{Z}[\omega]$.

Ahora si $\mathbb{Z}[\omega]$ fuera un dominio euclidiano, entonces tendríamos algún elemento no nulo y no invertible $x \in \mathbb{Z}[\omega]$ tal que para todo $y \in \mathbb{Z}[\omega]$ se cumple $x \mid y$, o se puede escribir $y = qx + r$ donde $r = \pm 1$. Es decir, x siempre debe dividir a y o $y \pm 1$. Primero tomemos $y = 2$.

1) Si $x \mid 2$, entonces necesariamente $x = \pm 2$ (como notamos, 2 es irreducible y x no es invertible).

2) Si $x \mid (2+1)$, entonces $x = \pm 3$ (de nuevo, 3 es irreducible y x no es invertible).

3) El caso $x \mid (2-1)$ no es posible, puesto que x no es invertible.

Entonces, necesariamente $x = \pm 2$ o ± 3, así que $N(x) = 4$ o 9. Tomemos ahora $y = \omega$. Hay tres casos, pero cada uno de ellos se descarta:

1) $x \nmid \omega$, puesto que $N(\omega) = 5$;

2) $x \nmid (1+\omega)$, puesto que $N(1+\omega) = 7$;

3) $x \nmid (-1+\omega)$, puesto que $N(-1+\omega) = 5$.

Podemos concluir que $\mathbb{Z}[\omega]$ no es un dominio euclidiano. Sin embargo, se puede probar que es un dominio de ideales principales. Para una prueba directa, véase [DF2004, §8.2], pero esto surge de ciertos cálculos en la teoría de números algebraica que vamos a explicar brevemente un poco más adelante.

En efecto, en lugar de $\frac{1+\sqrt{-19}}{2}$ también funcionaría

$$\omega = \frac{1+\sqrt{-43}}{2}, \quad \frac{1+\sqrt{-67}}{2}, \quad \frac{1+\sqrt{-163}}{2}.$$

▲

Los ejemplos como el de arriba nada más demuestran que la noción de dominio euclidiano no tiene ningún sentido profundo; es puramente utilitaria y se ocupa solo para probar que ciertos anillos son dominios de ideales principales. En práctica no es fácil demostrar que algo es un dominio euclidiano (salvo los casos básicos como $\mathbb{Z}$ y $k[X]$), ni que no lo es.

13.5 Valuaciones p-ádicas

Sea R un dominio de factorización única. Todo elemento no nulo $x \in R$ está definido, salvo un múltiplo invertible, por sus factores primos. Es conveniente juntar factores repetidos y escribir x como $u\, p_1^{k_1} \cdots p_n^{k_n}$ donde los p_i son primos no asociados entre sí (es decir, $p_i \not\sim p_j$ para $i \neq j$). El exponente k de un factor primo p se llama la **valuación p-ádica** de x.

13.5.1. Definición. Sea $p \in R$ un elemento primo. Para un elemento $x \in R$, $x \neq 0$ definamos

$$v_p(x) := \text{máx}\{k \mid p^k \mid x\}$$

y para el elemento nulo pongamos

$$v_p(0) := \infty.$$

El número $v_p(x)$ se llama la **valuación p-ádica** de x.

En otras palabras, para un elemento no nulo se tiene $v_p(x) = n$ precisamente cuando se puede escribir $x = p^n\, x'$, donde $p \nmid x'$. La factorización única en R significa que para todo $x \neq 0$ se cumple

$$x \sim \prod_p p^{v_p(x)},$$

donde el producto es sobre las clases de equivalencia de los elementos primos módulo la relación $\sim$. Notamos que en realidad este producto es finito, puesto que $v_p(x) = 0$ para todo p, salvo un número finito.

13.5.2. Ejemplo. Tenemos

$$v_2(60) = 2, \quad v_3(60) = 1, \quad v_5(60) = 1$$

y $v_p(60) = 0$ para $p \neq 2, 3, 5$. ▲

13.5.3. Proposición. *La valuación p-ádica satisface las siguientes propiedades.*

V1) $v_p(x) = \infty$ *si y solamente si* $x = 0$.

V2) $v_p(xy) = v_p(x) + v_p(y)$.

V3) $v_p(x + y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

Demostración. La parte V1) hace parte de la definición. Para la parte V2), si $x = 0$ o $y = 0$, la igualdad es evidente. Ahora si x e y no son nulos y $v_p(x) = m$ y $v_p(y) = n$, esto significa que

$$x = p^m\, x', \quad y = p^n\, y',$$

donde $p \nmid x'$ y $p \nmid y'$. Luego,

$$xy = p^{m+n}\, x'y',$$

donde $p \nmid x'y'$, así que $v_p(xy) = m + n$. De la misma manera, la parte V3) es evidente cuando $x = 0$ o $y = 0$. Para x e y no nulos, de nuevo podemos asumir que $v_p(x) = m$ y $v_p(y) = n$, donde sin pérdida de generalidad $m \leq n$. Luego,

$$x + y = p^m x' + p^n y' = p^m (x' + p^{n-m} y'),$$

entonces $p^m \mid (x + y)$ y por ende $v_p(x + y) \geq m$. ■

13.5.4. Observación. *Si $u \in R^\times$, entonces $v_p(u) = 0$ y $v_p(ux) = x$ para todo $x \in R$. En particular, $v_p(-x) = v_p(x)$ para todo $x \in R$.*

Demostración. Si $u \in R^\times$, entonces u no es divisible por ningún primo, así que $v_p(u) = 0$ para cualquier p. Luego,

$$v_p(ux) = v_p(u) + v_p(x) = 0 + v_p(x) = v_p(x).$$

■

Nos conviene extender las valuaciones p-ádicas al cuerpo de fracciones de R.

13.5.5. Definición. Sean R un dominio de factorización única, $p \in R$ un elemento primo y K el cuerpo de fracciones de R. Para $\frac{x}{y} \in K$ definamos la valuación p-ádica sobre K mediante

$$v_p\left(\frac{x}{y}\right) := v_p(x) - v_p(y).$$

Hay que verificar que esta definición tiene sentido: si $\frac{x}{y} = \frac{x'}{y'}$, entonces $xy' = x'y$. Luego,

$$v_p(x) + v_p(y') = v_p(x') + v_p(y);$$

es decir,

$$v_p(x) - v_p(y) = v_p(x') - v_p(y').$$

Esto significa que

$$v_p\left(\frac{x}{y}\right) = v_p\left(\frac{x'}{y'}\right).$$

Notamos que para toda fracción no nula se tiene

$$\frac{x}{y} = \prod_p p^{v_p(x/y)},$$

donde el producto se toma sobre todos los primos en R salvo la relación $\sim$, y la igualdad se entiende salvo un múltiplo $u \in R^\times$.

13.5.6. Ejemplo. Para $x = \frac{12}{34} = \frac{2^2 \cdot 3}{2 \cdot 17}$ se tiene

$$v_2(x) = 1, \quad v_3(x) = 1, \quad v_{17}(x) = -1,$$

y $v_p(x) = 0$ para otros p. ▲

13.5.7. Observación. *La valuación p-ádica sobre K satisface las mismas propiedades:*

V1) $v_p\left(\frac{x}{y}\right) = \infty$ *si y solamente si* $\frac{x}{y} = \frac{0}{1}$.

V2) $v_p\left(\frac{x_1}{y_1}\,\frac{x_2}{y_2}\right) = v_p\left(\frac{x_1}{y_1}\right) + v_p\left(\frac{x_2}{y_2}\right)$.

V3) $v_p\left(\frac{x_1}{y_1} + \frac{x_2}{y_2}\right) \geq \text{mín}\left\{v_p\left(\frac{x_1}{y_1}\right), v_p\left(\frac{x_2}{y_2}\right)\right\}$.

Demostración. En V1) basta recordar que $\frac{x}{y} = \frac{0}{1}$ si y solo si $x = 0$.

En V2), tenemos

$$v_p\left(\frac{x_1}{y_1}\,\frac{x_2}{y_2}\right) = v_p\left(\frac{x_1x_2}{y_1y_2}\right) = v_p(x_1x_2) - v_p(y_1y_2) = v_p(x_1) + v_p(x_2) - v_p(y_1) - v_p(y_2)$$
$$= v_p\left(\frac{x_1}{y_1}\right) + v_p\left(\frac{x_2}{y_2}\right).$$

En fin, en V3)

$$\begin{aligned} v_p\left(\frac{x_1}{y_1} + \frac{x_2}{y_2}\right) &= v_p\left(\frac{x_1y_2 + x_2y_1}{y_1y_2}\right) = v_p(x_1y_2 + x_2y_1) - v_p(y_1) - v_p(y_2) \\ &\geq \text{mín}\{v_p(x_1) + v_p(y_2), v_p(x_2) + v_p(y_1)\} - v_p(y_1) - v_p(y_2) \\ &= \text{mín}\{v_p(x_1) - v_p(y_1), v_p(x_2) - v_p(y_2)\} = \text{mín}\left\{v_p\left(\frac{x_1}{y_1}\right), v_p\left(\frac{x_2}{y_2}\right)\right\}. \end{aligned}$$

■

La desigualdad $v_p(x+y) \geq \text{mín}\{v_p(x), v_p(y)\}$ puede ser mejorada de la siguiente manera.

13.5.8. Observación. *Para cualesquiera* $x, y \in R$, *si* $v_p(x) \neq v_p(y)$, *entonces*

$$v_p(x+y) = \text{mín}\{v_p(x), v_p(y)\}.$$

De la misma manera, para cualesquiera $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in K$, *si* $v_p\left(\frac{x_1}{y_1}\right) \neq v_p\left(\frac{x_2}{y_2}\right)$, *entonces*

$$v_p\left(\frac{x_1}{y_1} + \frac{x_2}{y_2}\right) = \text{mín}\left\{v_p\left(\frac{x_1}{y_1}\right), v_p\left(\frac{x_2}{y_2}\right)\right\}.$$

Demostración. La propiedad en cuestión sigue formalmente de las propiedades V1), V2), V3). Asumamos que se cumple la desigualdad estricta

$$v_p(x+y) > \text{mín}\{v_p(x), v_p(y)\}.$$

Entonces, tenemos

$$v_p(x) = v_p(x+y-y) \geq \text{mín}\{v_p(x+y), v_p(y)\} = v_p(y)$$

y de la misma manera

$$v_p(y) = v_p(x+y-x) \geq \text{mín}\{v_p(x+y), v_p(x)\} = v_p(x).$$

■

13.5.9. Comentario. Por inducción, de la última observación se sigue que si $x = x_1 + \cdots + x_n$ y existe $i = 1, \ldots, n$ tal que $v_p(x_i) < v_p(x_j)$ para $i \neq j$, entonces $v_p(x) = v_p(x_i)$.

13.5.10. Observación. *Se tiene*

$$R = \{x \in K \mid v_p(x) \geq 0 \text{ para todo primo } p\},$$

donde se consideran todos los primos en R salvo la relación $\sim$ *y*

$$R^\times = \{x \in K \mid v_p(x) = 0 \text{ para todo primo } p\}.$$

Demostración. Tenemos $x = \prod_p p^{v_p(x)}$ salvo un múltiplo $u \in R^\times$, así que si $v_p(x) \geq 0$ para todo p, se tiene $x \in R$. ■

13.6 Lema de Gauss y factorización de polinomios

El objetivo de esta sección es probar el siguiente resultado: si R es un dominio de factorización única, entonces el anillo de polinomios $R[X]$ es también un dominio de factorización única. El argumento que vamos a ver esencialmente pertenece a Gauss (como una gran parte del resto de esta sección).

Primero, nos va a servir la siguiente extensión de las valuaciones p-ádicas al anillo de polinomios $K[X]$.

13.6.1. Definición. Sean R un dominio de factorización única, K su cuerpo de fracciones y $p \in R$ un elemento primo. Para un polinomio $f = \sum_{i\geq 0} a_i X^i \in K[X]$ definamos

$$v_p(f) := \min_i\{v_p(a_i)\}.$$

En particular,

$$v_p(0) = \infty.$$

De la definición debe estar claro que

$$v_p(f + g) \geq \min\{v_p(f), v_p(g)\}.$$

También tenemos la propiedad deseada para los productos.

13.6.2. Lema. *Para cualesquiera* $f, g \in K[X]$ *se cumple*

$$v_p(fg) = v_p(f) + v_p(g).$$

Demostración. Esto es evidente si $f = 0$ o $g = 0$, así que podemos asumir que $f, g \neq 0$. Tenemos

$$f = \sum_{i\geq 0} a_i X^i, \quad g = \sum_{j\geq 0} b_j X^j, \quad fg = \sum_{k\geq 0} c_k X^k, \quad c_k = \sum_{i+j=k} a_i b_j.$$

Ahora

$$v_p(c_k) \geq \min_{i+j=k}\{v_p(a_i) + v_p(b_j)\} \geq v_p(f) + v_p(g),$$

y por ende

$$v_p(fg) \geq v_p(f) + v_p(g).$$

Para concluir que se tiene la igualdad, hay que ver que algún coeficiente c_k tiene valuación $v_p(f) + v_p(g)$. Asumamos que $v_p(f) = v_p(a_m)$, donde el índice m es el mínimo posible:

$$v_p(a_m) < v_p(a_i) \text{ para } 0 \leq i < m, \quad v_p(a_m) \leq v_p(a_i) \text{ para } i \geq m.$$

De la misma manera, supongamos que $v_p(g) = v_p(b_n)$, donde n es el mínimo posible:

$$v_p(b_n) < v_p(b_i), \text{ para } 0 \leq i < n, \quad v_p(b_n) \leq v_p(b_i), \text{ para } i \geq n.$$

Luego,

$$v_p(c_{m+n}) \geq \max_{i+j=m+n} \{v_p(a_i) + v_p(b_j)\}.$$

Dado que $i + j = m + n$, se tiene $i < m$ o $j < n$, salvo el caso $i = m$, $j = n$. Por nuestra elección de m y n, esto significa que $v_p(a_m) + v_p(b_n)$ es estrictamente menor que otros términos, así que gracias a 13.5.9 se puede concluir que

$$v_p(c_{m+n}) = v_p(a_m) + v_p(b_n) = v_p(f) + v_p(g).$$

■

13.6.3. Definición. Sean R un dominio de factorización única y K su cuerpo de fracciones. Para un polinomio $f \in K[X]$ su **contenido** está definido por

$$\text{cont}(f) := \prod_p p^{v_p(f)},$$

donde el producto se toma sobre todos los primos en R salvo la relación de equivalencia $\sim$. Esto define a $\text{cont}(f)$ salvo un múltiplo invertible $u \in R^\times$.

He aquí algunas observaciones sobre el contenido que serán útiles más adelante.

1) Para un polinomio constante $f = c$ se tiene $\text{cont}(c) = c$, salvo un múltiplo invertible $u \in R^\times$.

2) Si $f \in R[X]$, entonces $\text{cont}(f) \in R$.

3) Si $\text{cont}(f) = 1$, entonces $v_p(f) = 0$ para todo p; es decir, $f \in R[X]$ (véase 13.5.10) y además para todo p existe i tal que $p \nmid a_i$.

4) Para $f \in K[X]$ se tiene $\frac{1}{\text{cont}(f)} f \in R[X]$.

13.6.4. Observación. *Sea R un dominio de factorización única y K su cuerpo de fracciones. Para cualesquiera $f, g \in K[X]$ se tiene*

$$\text{cont}(fg) = \text{cont}(f) + \text{cont}(g).$$

Demostración. Sigue inmediatamente de 13.6.2. ■

13.6.5. Lema (Gauss). *Sea R un dominio de factorización única y sea K su cuerpo de fracciones. Si $f \in R[X]$ es un polinomio irreducible en $K[X]$ y $\operatorname{cont}(f) = 1$, entonces f es irreducible en $R[X]$.*

Demostración. Supongamos que $f = g\,h$ para algunos $g, h \in R[X]$. Vamos a probar que $g \in R[X]^\times$ o $h \in R[X]^\times$. Interpretando $f = g\,h$ como una factorización en $K[X]$, podemos concluir que $g \in K[X]^\times = K^\times$ o $h \in K[X]^\times = K^\times$. Asumamos por ejemplo que $g = c \in K^\times$. Tenemos

$$\operatorname{cont}(c)\ \operatorname{cont}(h) = \operatorname{cont}(f) = 1,$$

lo que significa que $\operatorname{cont}(c) \in R^\times$, así que $c \in R^\times$. Hemos probado entonces que $g = c \in R[X]^\times$. ■

13.6.6. Ejemplo. La condición $\operatorname{cont}(f) = 1$ es necesaria. Por ejemplo, el polinomio $f = 2\,X^2 + 2\,X - 2$ tiene $\operatorname{cont}(f) = 2$. Es irreducible en $\mathbb{Q}[X]$, pero en $\mathbb{Z}[X]$ tenemos una factorización no trivial $f = 2\,(X^2 + X - 1)$. ▲

13.6.7. Teorema. *Si R es un dominio de factorización única, entonces el anillo de polinomios $R[X]$ es también un dominio de factorización única.*

Demostración. Sea K el cuerpo de fracciones de R. El anillo de polinomios $K[X]$ es un dominio euclidiano y en particular un dominio de factorización única.

Sea $f \in R[X]$ un polinomio no nulo. En $K[X]$ tenemos una factorización única

$$f = c\,p_1 \cdots p_s,$$

donde $c \in K^\times$ y $p_1, \ldots, p_s \in K[X]$ son polinomios irreducibles en $K[X]$. Luego,

$$\operatorname{cont}(f) = \operatorname{cont}(c)\ \operatorname{cont}(p_1) \cdots \operatorname{cont}(p_s),$$

así que

$$\frac{1}{\operatorname{cont}(f)}\,f = \frac{1}{\operatorname{cont}(c)}\,c \cdot \frac{1}{\operatorname{cont}(p_1)}\,p_1 \cdots \frac{1}{\operatorname{cont}(p_s)}\,p_s.$$

Notamos que los polinomios $\frac{1}{\operatorname{cont}(f)}\,f$, $\frac{1}{\operatorname{cont}(c)}\,c$, $\frac{1}{\operatorname{cont}(p_i)}\,p_i$ tienen contenido 1 y en particular pertenecen a $R[X]$. Tenemos necesariamente $\frac{1}{\operatorname{cont}(c)}\,c \in R^\times$. Por el lema de Gauss, $\frac{1}{\operatorname{cont}(p_i)}\,p_i$ son polinomios irreducibles en $R[X]$, puesto que son irreducibles en $K[X]$.

Entonces, hemos logrado factorizar el polinomio $\frac{1}{\operatorname{cont}(f)}\,f \in R[X]$ en polinomios irreducibles en $R[X]$. Luego, en R tenemos una factorización única

$$\operatorname{cont}(f) = u\,x_1 \cdots x_t$$

donde $u \in R^\times = R[X]^\times$ y $x_1, \ldots, x_t$ son irreducibles en R, y por ende son irreducibles en $R[X]$ (un polinomio constante puede ser escrito solo como un producto de polinomios constantes).

Entonces,

$$f = \operatorname{cont}(f)\,\frac{1}{\operatorname{cont}(f)}\,f = v\,x_1 \cdots x_t \cdot \frac{1}{\operatorname{cont}(p_1)}\,p_1 \cdots \frac{1}{\operatorname{cont}(p_s)}\,p_s,$$

(donde $v := u \frac{1}{\mathrm{cont}(c)} c \in R^\times$) es una factorización de f en polinomios irreducibles en $R[X]$. Falta ver que estas factorizaciones son únicas.

Asumamos que hay otra factorización

$$f = w\, y_1 \cdots y_{t'} \cdot q_1 \cdots q_{s'}$$

donde $w \in R^\times = R[X]^\times$, $y_1, \ldots, y_{t'}$ son elementos irreducibles en R y $q_1, \ldots, q_{s'}$ son polinomios no constantes irreducibles en $R[X]$. Esta factorización puede ser considerada como una factorización en $K[X]$ que es un dominio de factorización única. Notamos que $w\, y_1 \cdots y_{t'} \in K^\times$. Los polinomios p_i son irreducibles en $K[X]$, así que para todo i existe j tal que $p_i \mid q_j$:

$$q_j = g_{ij}\, p_i$$

para algún polinomio $g_{ij} \in K[X]$. Luego, tenemos una identidad en $R[X]$

$$\frac{1}{\mathrm{cont}(q_j)}\, q_j = \frac{1}{\mathrm{cont}(q_{ij})}\, g_{ij}\, \frac{1}{\mathrm{cont}(p_i)}\, p_i.$$

Pero q_j es irreducible en $R[X]$ por nuestra hipótesis, y el polinomio p_i no es constante, lo que implica que q_j y $\frac{1}{\mathrm{cont}(p_i)}\, p_i$ son asociados en $R[X]$: existe $u_j \in R^\times = R[X]^\times$ tal que

$$q_j = u_j\, \frac{1}{\mathrm{cont}(p_i)}\, p_i. \tag{13.2}$$

En particular, q_j son irreducibles en $K[X]$, y entonces necesariamente $s = s'$, dado que $K[X]$ es un dominio de factorización única. Podemos comparar las dos factorizaciones:

$$f = v\, x_1 \cdots x_t \cdot \frac{1}{\mathrm{cont}(p_1)}\, p_1 \cdots \frac{1}{\mathrm{cont}(p_s)}\, p_s = w\, y_1 \cdots y_{t'} \cdot q_1 \cdots q_s.$$

Gracias a 13.2, podemos cancelar los términos $\frac{1}{\mathrm{cont}(p_i)}\, p_i$ con correspondientes q_j y nos queda una identidad en R

$$v\, x_1 \cdots x_t = w'\, y_1 \cdots y_{t'}$$

donde $w' := w\, u_1 \cdots u_s \in R^\times$. Pero R es un dominio de factorización única y x_i, y_j son irreducibles, así que $t' = t$ y $y_i \sim x_i$ después de una permutación. ■

13.6.8. Comentario. La prueba de arriba revela que los elementos irreducibles en $R[X]$ son las constantes irreducibles en R y los polinomios no constantes $f \in R[X]$ tales que $\mathrm{cont}(f) = 1$ y f es irreducible en $K[X]$.

13.6.9. Comentario. En particular, si $R = k$ es un cuerpo, es trivialmente un dominio de factorización única y $k[X]$ es un dominio de factorización única. Sin embargo, la prueba de arriba no considera este caso, sino está basada en él.

13.6.10. Ejemplo. El anillo de polinomios $\mathbb{Z}[X]$ es un dominio de factorización única. Los elementos irreducibles (primos) en $\mathbb{Z}[X]$ son los primos $p = \pm 2, \pm 3, \pm 5, \pm 7, \pm 1, \ldots$ y los polinomios $\pi \in \mathbb{Z}[X]$ que son irreducibles en $\mathbb{Q}[X]$, por ejemplo

$$\pi = X, \quad 2\,X + 1, \quad X^2 + 2\,X + 2, \quad X^3 + 2.$$

Como vimos en 13.2.4, $\mathbb{Z}[X]$ no es un dominio de ideales principales: hemos observado que (p, X) es un ideal maximal que no puede ser generado por un elemento. En general, tenemos la siguiente descripción de ideales primos en $\mathbb{Z}[X]$:

0) el ideal nulo (0),

1) los ideales principales (p) para $p = 2, 3, 5, 7, 11, \ldots$,

2) los ideales principales (π) donde $\pi \in \mathbb{Z}[X]$ es un polinomio no constante que es irreducible en $\mathbb{Q}[X]$,

3) los ideales maximales (p, π), donde $p = 2, 3, 5, 7, 11, \ldots$ y $\pi \in \mathbb{Z}[X]$ es un polinomio no constante tal que $\overline{\pi} \in \mathbb{F}_p[X]$ es irreducible.

Primero, notemos que los ideales de la lista son primos. La parte 0) es obvia: $\mathbb{Z}[X]$ es un dominio de integridad. Las partes 1) y 2) siguen de la descripción de los elementos irreducibles (primos) en $\mathbb{Z}[X]$. Para la parte 3), notamos que

$$\mathbb{Z}[X]/(p, \pi) \cong \mathbb{F}_p[X]/(\overline{\pi}),$$

donde $\overline{\pi}$ es la imagen de π respecto al homomorfismo canónico $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ (la reducción de los coeficientes módulo p). El anillo $\mathbb{F}_p[X]$ es un dominio euclidiano y por ende es un dominio de ideales principales. Por nuestra hipótesis, $\overline{\pi}$ es irreducible (primo) en $\mathbb{F}_p[X]$, así que el ideal $(\overline{\pi}) \subset \mathbb{F}_p[X]$ es maximal y $\mathbb{F}_p[X]/(\overline{\pi})$ es un cuerpo. Podemos concluir que el ideal $(p, \pi) \subset \mathbb{Z}[X]$ es también maximal.

Para completar la descripción, hay que probar que todo ideal primo $\mathfrak{p} \subset \mathbb{Z}[X]$ es de la forma 0)–3). Si $\mathfrak{p} = (0)$, estamos en el caso 0), así que asumamos que $\mathfrak{p} \neq (0)$.

La intersección $\mathfrak{p} \cap \mathbb{Z}$ es un ideal primo en $\mathbb{Z}$, siendo la preimagen de $\mathfrak{p}$ respecto al homomorfismo canónico $\mathbb{Z} \hookrightarrow \mathbb{Z}[X]$.

Asumamos primero que $\mathfrak{p} \cap \mathbb{Z} \neq (0)$. En este caso existe un número primo p tal que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Luego, $p\mathbb{Z}[X] \subseteq \mathfrak{p}$.

Ahora $\overline{\mathfrak{p}} := \mathfrak{p}/(p\mathbb{Z}[X])$ es un ideal primo en el anillo cociente $\mathbb{Z}[X]/(p) \cong \mathbb{F}_p[X]$. Esto implica que $\overline{\mathfrak{p}} = (0)$ o $\overline{\mathfrak{p}} = \overline{\pi}\mathbb{F}_p[X]$ donde $\overline{\pi} \in \mathbb{F}_p[X]$ es algún polinomio irreducible. Entonces, hay dos posibilidades:

$$\mathfrak{p} = p\mathbb{Z}[X], \quad \mathfrak{p} = p\mathbb{Z}[X] + \pi\,\mathbb{Z}[X],$$

donde $\overline{pi} = \pi \pmod{p}$. Esto corresponde a los casos 1) y 3) de la lista.

Asumamos que $\mathfrak{p} \cap \mathbb{Z} = (0)$. Sea $f \in \mathfrak{p}$ un polinomio no nulo. Tenemos la factorización única

$$f = \pm\pi_1 \cdots \pi_s,$$

donde $\pi_i \in \mathbb{Z}[X]$ son polinomios irreducibles (primos). Puesto que $\mathfrak{p}$ es un ideal primo, se tiene necesariamente $\pi := \pi_i \in \mathfrak{p}$ para algún $i = 1, \ldots, s$. La hipótesis que $\mathfrak{p} \cap \mathbb{Z} = (0)$ implica que este polinomio π no es constante. Nuestro objetivo es probar que $\mathfrak{p} = \pi\mathbb{Z}[X]$. Sea entonces $g \in \mathfrak{p}$ cualquier polinomio no nulo.

Asumamos que π no divide a g en $\mathbb{Q}[X]$. Dado que π es un polinomio no constante que es irreducible en $\mathbb{Z}[X]$, es también irreducible en $\mathbb{Q}[X]$, y por ende $\mathrm{mcd}(\pi, g) = 1$, lo que significa que

$$h_1\,\pi + h_2\,g = 1$$

para algunos $h_1, h_2 \in \mathbb{Q}[X]$. Tomemos n suficientemente grande tal que los polinomios $n\,h_1\,\pi$ y $n\,h_2\,g$ tienen coeficientes enteros. Luego,

$$n\,h_1\,\pi + n\,h_2\,g = n \in \mathfrak{p},$$

pero esto contradice nuestra hipótesis de que $\mathfrak{p} \cap \mathbb{Z} = (0)$.

Entonces, π tiene que dividir en $\mathbb{Q}[X]$ a cualquier polinomio $g \in \mathfrak{p}$: tenemos

$$g = \pi\,r$$

para algún $r \in \mathbb{Q}[X]$. Sin embargo,

$$\mathrm{cont}(g) = \mathrm{cont}(\pi)\ \mathrm{cont}(r),$$

Donde $\mathrm{cont}(\pi) = 1$, dado que π es un polinomio irreducible en $\mathbb{Z}[X]$. Entonces, $\mathrm{cont}(r) = \mathrm{cont}(g) \in \mathbb{Z}$ y $r \in \mathbb{Z}[X]$. Esto demuestra que $g \in \pi\mathbb{Z}[X]$. ▲

13.6.11. Corolario. *Si R es un dominio de factorización única, entonces el anillo de polinomios en n variables $R[X_1, \ldots, X_n]$ es también un dominio de factorización única.*

Demostración. Inducción sobre n, usando isomorfismos $R[X_1, \ldots, X_n] \cong R[X_1, \ldots, X_{n-1}][X_n]$. ■

13.6.12. Comentario. Si R es un dominio de factorización única, el anillo de las series formales $R[\![X_1, \ldots, X_n]\!]$ no tiene por qué ser un dominio de factorización única[*]. Sin embargo, es cierto si $R = k$ es un cuerpo (las palabras claves son "el **teorema de preparación de Weierstrass**").

13.6.13. Comentario. El teorema 13.6.7 puede ser probado sin recurrir a las valuaciones p-ádicas (véase por ejemplo [DF2004, §9.3]); las hemos revisado porque son muy importantes en la teoría de números.

13.7 Criterios de irreducibilidad

Ahora ya que sabemos que para un dominio de factorización única R los polinomios $R[X]$ también forman un dominio de factorización única, sería interesante saber cuándo un polinomio $f \in R[X]$ es irreducible. Esto es un problema profundo desde el punto de vista teórico y algorítmico y aquí vamos a ver solo un par de criterios útiles en práctica.

[*]Véase por ejemplo el artículo de Pierre Samuel https://projecteuclid.org/euclid.ijm/1255629643 para un estudio de este problema.

13.7.1. Lema. *Sean R un anillo conmutativo e $I \subseteq R$ un ideal. Entonces, hay un isomorfismo natural*

$$R[X]/IR[X] \cong (R/I)[X],$$

donde $IR[X]$ es el ideal generado por I en $R[X] \supset R$:

$$IR[X] = \Big\{ \sum_{i\geq 0} a_i\, X^i \;\Big|\; a_i \in I \Big\}.$$

Demostración. Consideremos la aplicación

$$\begin{aligned} R[X] &\to (R/I)[X], \\ \sum_{i\geq 0} a_i\, X^i &\mapsto \sum_{i\geq 0} \overline{a_i}\, X^i \end{aligned}$$

que reduce los coeficientes de un polinomio módulo I. Las fórmulas para la suma y producto de polinomios demuestran que esto es un homomorfismo de anillos. Es visiblemente sobreyectivo, y su núcleo es precisamente $IR[X]$. ■

13.7.2. Proposición. *Sea R un dominio de integridad y sea $f \in R[X]$ un polinomio mónico (con coeficiente mayor igual a 1) no constante. Sea $I \subset R[X]$ un ideal propio tal que la imagen $\overline{f}$ en el cociente $R[X]/IR[X] \cong (R/I)[X]$ no se factoriza como un producto de polinomios de grado $< \deg \overline{f}$. Entonces, f es irreducible en $R[X]$.*

Demostración. Asumamos que f es reducible en $R[X]$; es decir, $f = gh$ donde $g, h \notin R[X]^\times = R^\times$. Si $g = a_m\, X^m + a_{m-1}\, X^{m-1} + \cdots$ y $h = b_n\, X^n + b_{n-1}\, X^{n-1} + \cdots$, entonces el coeficiente mayor de gh es $a_m\, b_n = 1$. Esto implica que $a_m, b_n \in R^\times$, y en particular g y h no son polinomios constantes, y luego $\deg g, \deg h < \deg f$. Gracias a nuestra hipótesis de que $I \neq R$, tenemos $a_m, b_n \notin I$, así que

$$\deg \overline{g} = \deg g, \quad \deg \overline{h} = \deg h.$$

La reducción módulo I nos da entonces una factorización $\overline{f} = \overline{g}\,\overline{h}$, donde $\deg \overline{g}, \deg \overline{h} < \deg \overline{f}$. ■

13.7.3. Ejemplo. Es fácil saber cuándo un polinomio con coeficientes en $\mathbb{F}_p$ es irreducible: hay un número finito de polinomios de grado fijo. Para compilar una lista de polinomios irreducibles en $\mathbb{F}_p[X]$ se puede usar la **criba de Eratóstenes**. Por ejemplo, sea $p = 2$. Los polinomios de grado 1 son siempre irreducibles:

$$X, \quad X + 1.$$

Los polinomios de grado 2 son

$$X^2, \quad X^2 + 1, \quad X^2 + X, \quad X^2 + X + 1.$$

Entre ellos los polinomios reducibles son los productos de polinomios lineales:

$$X^2 = X \cdot X, \quad X^2 + X = X\,(X + 1), \quad X^2 + 1 = (X + 1)^2.$$

Entonces, $X^2 + X + 1$ es irreducible. Luego, los polinomios cúbicos reducibles son los productos de polinomios de grado 1 y 2:

$$\begin{aligned} X^3 &= X^3, \\ X^3 + X^2 + X + 1 &= (X+1)^3, \\ X^3 + X^2 &= X^2\,(X+1), \\ X^3 + X &= X\,(X+1)^2, \\ X^3 + X^2 + X &= (X^2 + X + 1)\,X, \\ X^3 + 1 &= (X^2 + X + 1)\,(X+1). \end{aligned}$$

Los dos polinomios cúbicos que nos quedan son irreducibles:

$$X^3 + X + 1, \quad X^3 + X^2 + 1.$$

Continuando de la misma manera, se puede ver que los polinomios irreducibles de grado cuatro son

$$X^4 + X + 1, \quad X^4 + X^3 + 1, \quad X^4 + X^3 + X^2 + X + 1.$$

El número de polinomios irreducibles en $\mathbb{F}_p[X]$ de grado n crece rápido con p y n. En el siguiente capítulo vamos a ver cómo contarlos. ▲

13.7.4. Ejemplo. El polinomio $f = X^2 + 1$ es irreducible en $\mathbb{Z}[X]$ y $\overline{f}$ se vuelve reducible en $\mathbb{F}_p[X]$ si y solo si -1 es un cuadrado módulo p. Esto sucede precisamente para $p \equiv 1 \pmod 4$. Por ejemplo, en $\mathbb{Z}/5\mathbb{Z}[X]$ se cumple

$$X^2 + 1 = (X+2)\,(X+3).$$

▲

13.7.5. Ejemplo. Consideremos el polinomio

$$f = X^3 + X^2 - 2\,X - 1 \in \mathbb{Z}[X].$$

Al reducirlo módulo 2 nos queda un polinomio irreducible

$$\overline{f} = X^3 + X^2 + 1 \in \mathbb{F}_2[X].$$

Podemos tratar de reducir el mismo polinomio f módulo otros números primos. La tabla de abajo nos da las factorizaciones de $\overline{f} \in \mathbb{F}_p[X]$ en factores irreducibles. He excluido los casos cuando $\overline{f}$ queda irreducible, como para $p = 2$.

$$\begin{aligned} p = 7\colon &\quad (X+5)^3, \\ p = 13\colon &\quad (X+3)\,(X+5)\,(X+6), \\ p = 29\colon &\quad (X+11)\,(X+22)\,(X+26), \\ p = 41\colon &\quad (X+4)\,(X+11)\,(X+27), \\ p = 43\colon &\quad (X+24)\,(X+28)\,(X+35), \\ &\quad \dots \end{aligned}$$

Un experimento numérico demuestra que $\overline{f}$ queda irreducible para $\frac{2}{3}$ de los números primos, y para $\frac{1}{3}$ de los números primos $\overline{f}$ es un producto de tres diferentes polinomios lineales. El caso $p = 7$ es excepcional: se tiene un cubo del mismo polinomio lineal.

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	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997
1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163
1171	1181	1187	1193	1201	1213	1217	1223	1229	1231	1237	1249
1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321
1327	1361	1367	1373	1381	1399	1409	1423	1427	1429	1433	1439
1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601
1607	1609	1613	1619	1621	1627	1637	1657	1663	1667	1669	1693
1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783
1787	1789	1801	1811	1823	1831	1847	1861	1867	1871	1873	1877
1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987

Los primos tales que $X^3 + X^2 - 2X - 1$ es irreducible en $\mathbb{F}_p[X]$

▲

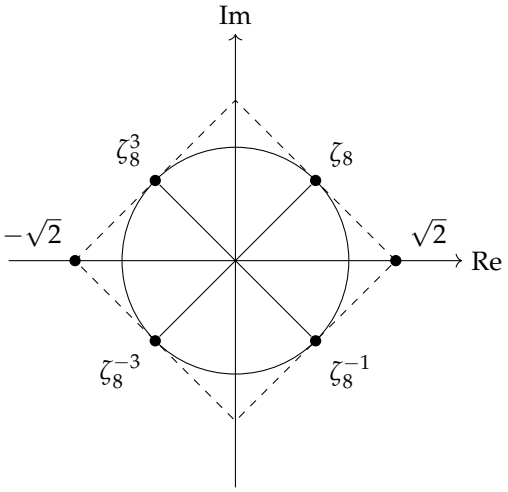
13.7.6. Comentario. En la teoría de números algebraica se estudian los patrones en la factorización de $\overline{f} \in \mathbb{F}_p[X]$ para diferentes p. El "experimentos numérico" mencionado arriba no es una coincidencia; este fenómeno se explica por el famoso **teorema de densidad de Chebotarëv**[*]. Para más detalles, véase el artículo P. Stevenhagen y H. W. Lenstra http://www.math.leidenuniv.nl/~hwl/papers/cheb.pdf

Aunque nuestro criterio de irreducibilidad es muy sencillo, existen polinomios irreducibles $f \in \mathbb{Z}[X]$ tales que $\overline{f} \in \mathbb{F}_p[X]$ es reducible para cualquier primo p.

13.7.7. Ejemplo. El polinomio $f = X^4 + 1$ es irreducible en $\mathbb{Z}[X]$. Lo veremos más adelante usando otro método, pero por el momento podemos presentar una explicación directa. Las raíces complejas de f son

$$\zeta_8 := e^{\frac{1}{8}\cdot 2\pi\sqrt{-1}}, \quad \zeta_8^{-1} = \overline{\zeta_8}, \quad \zeta_8^3, \quad \zeta_8^{-3} = \overline{\zeta_8^3}.$$

[*]Nikolaĭ Chebotarëv (1894–1947), un matemático soviético.



Tenemos entonces una factorización en $\mathbb{C}[X]$

$$f = (X - \zeta_8)\,(X - \overline{\zeta_8})\,(X - \zeta_8^3)\,(X - \overline{\zeta_8^3}).$$

Supongamos que $f = gh$ para algunos $g, h \in \mathbb{Z}[X]$. Dado que f es mónico, el coeficiente mayor de g y h es ± 1. Si $g, h \neq \pm 1$ no son polinomios constantes, entonces $\deg g, \deg h \geq 1$. Es imposible que $\deg g = 1$ o $\deg h = 1$: un polinomio lineal que tiene $\zeta_8^{\pm 1}$ o $\zeta_8^{\pm 3}$ como su raíz no puede tener coeficientes enteros. Entonces, f y g deben ser cuadráticos. Sin embargo, si un polinomio con coeficientes reales (en particular enteros) tiene $z \in \mathbb{C}$ como su raíz, entonces $\overline{z}$ es también una raíz. Pero se tiene

$$\begin{aligned}(X - \zeta_8)\,(X - \overline{\zeta_8}) &= X^2 - (\zeta_8 + \overline{\zeta_8})\,X + \zeta_8\,\overline{\zeta_8} = X^2 - \sqrt{2}\,X + 1,\\ (X - \zeta_8^3)\,(X - \overline{\zeta_8^3}) &= X^2 + \sqrt{2}\,X + 1,\end{aligned}$$

lo que demuestra que un polinomio con raíces $\zeta_8, \overline{\zeta_8}$ o $\zeta_8^3, \overline{\zeta_8^3}$ no puede tener coeficientes enteros.

Ahora se puede probar que el polinomio $X^4 + 1$ se vuelve reducible módulo cualquier primo. Por ejemplo,

$$\begin{aligned}
p = 2\colon&\quad (X+1)^4,\\
p = 3\colon&\quad (X^2 + X + 2)\,(X^2 + 2\,X + 2),\\
p = 5\colon&\quad (X^2 + 2)\,(X^2 + 3),\\
p = 7\colon&\quad (X^2 + 3\,X + 1)\,(X^2 + 4\,X + 1),\\
p = 11\colon&\quad (X^2 + 3\,X + 10)\,(X^2 + 8\,X + 10),\\
p = 13\colon&\quad (X^2 + 5)\,(X^2 + 8),\\
p = 17\colon&\quad (X+2)\,(X+8)\,(X+9)\,(X+15),\\
&\quad \ldots
\end{aligned}$$

En efecto, para $p = 2$ se tiene la factorización $X^4 + 1 = (X+1)^4$. Para p impar tenemos necesariamente $p \equiv 1, 3, 5, 7 \pmod 8$.

1) Si $p \equiv 1$ o $5 \pmod 8$, entonces $p \equiv 1 \pmod 4$, y en este caso -1 es un cuadrado módulo p. Tenemos $-1 = a^2$ para algún $a \in \mathbb{F}_p$ y podemos escribir

$$X^4 + 1 = X^4 - a^2 = (X^2 + a)\,(X^2 - a).$$

2) Si $p \equiv 7 \pmod 8$, entonces 2 es un cuadrado módulo p; se tiene $2 = a^2$ para algún $a \in \mathbb{F}_p$, y luego

$$(X^2 + aX + 1)\,(X^2 - aX + 1) = X^4 + (2 - a^2)\,X + 1 = X^4 + 1.$$

3) Si $p \equiv 3 \pmod 8$, entonces $p \equiv 3 \pmod 4$ y ni -1, ni 2 no es un cuadrado módulo p. En este caso -2 es un cuadrado. Si $-2 = a^2$, entonces

$$(X^2 + aX - 1)\,(X^2 - aX - 1) = X^4 - (2 + a^2)\,X + 1 = X^4 + 1.$$

Un experimento numérico demuestra que para $\frac{3}{4}$ de los primos p el polinomio $X^4 + 1$ se factoriza en $\mathbb{F}_p[X]$ como un producto de dos polinomios cuadráticos irreducibles, y para $\frac{1}{4}$ de los primos la factorización es un producto de cuatro diferentes polinomios lineales (en efecto, estos son los primos tales que $p \equiv 1 \pmod 8$). El primo $p = 2$ es excepcional.

▲

13.7.8. Comentario. El argumento de arriba usa las **leyes suplementarias de reciprocidad cuadrática**: para p impar se cumple

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases} \tag{13.3}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p \equiv 1,7 \pmod 8, \\ -1, & p \equiv 3,5 \pmod 8. \end{cases} \tag{13.4}$$

Ambas leyes pueden ser deducidas del **criterio de Euler**

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

(véase el capítulo 7). Para $a = -1$ se obtiene (13.3). Para $a = 2$, tenemos

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod p.$$

Para identificar el número a la derecha, podemos usar las raíces octavas de la unidad que ya han surgido en 13.7.7. Consideremos el anillo

$$\mathbb{Z}[\zeta_8] = \left\{ \sum_{0 \le i \le 7} n_i\,\zeta_8^i \;\middle|\; n_i \in \mathbb{Z} \right\} \subset \mathbb{C}$$

donde $\zeta_8 := e^{2\pi\sqrt{-1}/8}$. Denotemos

$$\tau := \zeta_8 + \zeta_8^{-1} = \sqrt{2}.$$

Notamos que en $\mathbb{Z}[\zeta_8]$ se cumple

$$\tau^p = (\zeta_8 + \zeta_8^{-1})^p \equiv \zeta_8^p + \zeta_8^{-p} \equiv \begin{cases} \zeta_8 + \zeta_8^{-1} = +\tau, & p \equiv \pm 1 \pmod 8, \\ \zeta_8^3 + \zeta_8^{-3} = -\tau, & p \equiv \pm 3 \pmod 8. \end{cases} \pmod p$$

(usando la identidad $(x+y)^p \equiv x^p + y^p \pmod p$). Puesto que $\tau = \sqrt{2}$, calculamos

$$2^{\frac{p-1}{2}} = \tau^{p-1} = \tau^p \, \tau^{-1} \equiv \begin{cases} +1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases} \pmod p.$$

Esto establece (13.4). Para otra interpretación de este cálculo, véase el siguiente capítulo.

He aquí otro criterio de irreducibilidad útil en práctica.

13.7.9. Teorema (Criterio de Eisenstein). *Sean R un dominio de integridad y $\mathfrak{p} \subset R$ un ideal primo, Sea*

$$f = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

un polinomio mónico con coeficientes en R tal que $a_i \in \mathfrak{p}$ para todo $i = 0, 1, \ldots, n-1$, pero $a_0 \notin \mathfrak{p}^2$. Entonces, f es irreducible.

Demostración. Asumamos que f es reducible y $f = g\,h$ donde $g, h \notin R[X]^\times = R^\times$. Notamos que necesariamente

$$1 \leq \deg g, \deg h < n$$

—si uno de estos polinomios fuera constante, este sería invertible, dado que f es un polinomio mónico. Reduciendo módulo $\mathfrak{p}$, se obtiene una identidad

$$\overline{X^n} = \overline{f} = \overline{g}\,\overline{h} \quad \text{en } (R/\mathfrak{p})[X]$$

por la hipótesis sobre los coeficientes de f. Puesto que $\mathfrak{p}$ es un ideal primo, $R/\mathfrak{p}$ es un dominio de integridad, y podemos encajarlo en su cuerpo de fracciones $K := K(R/\mathfrak{p})$. La identidad de arriba considerada en $K[X]$ implica que

$$\overline{g} = c\,\overline{X^k}, \quad \overline{h} = c^{-1}\,\overline{X^\ell},$$

para algún $c \in K^\times$ y para $k, \ell \geq 0$ tales que $k + \ell = n$. Notamos que $k \leq \deg g$ y $\ell \leq \deg h$, así que $k, \ell < n$, lo que implica que $k, \ell > 0$.

Sin embargo, si ambos g y h se reducen a un polinomio sin término constante, esto significa que los términos constantes de g y h están en $\mathfrak{p}$. Esto implicaría que el término constante de f está en $\mathfrak{p}^2$, pero no es el caso según la hipótesis.

Hemos llegado a una contradicción que significa que f es irreducible. ∎

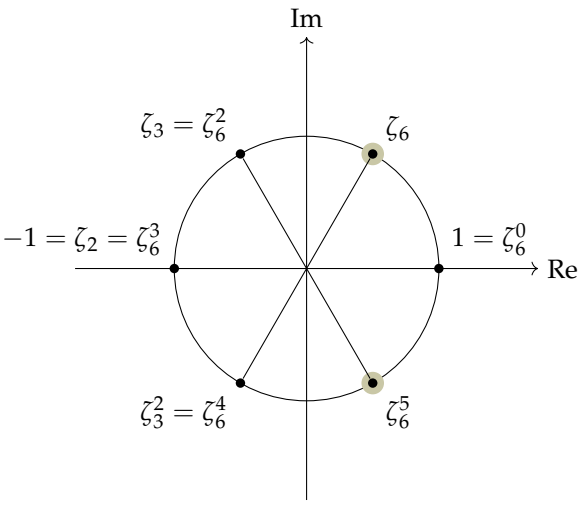
Terminemos por una aplicación importante del criterio de Eisenstein. Recordemos que el grupo de las n-ésimas raíces de la unidad

$$\mu_n(\mathbb{C}) := \{z \in \mathbb{C} \mid z^n = 1\} = \{\zeta_n^k \mid k = 0, \ldots, n-1\}, \quad \zeta_n := e^{2\pi\sqrt{-1}/n},$$

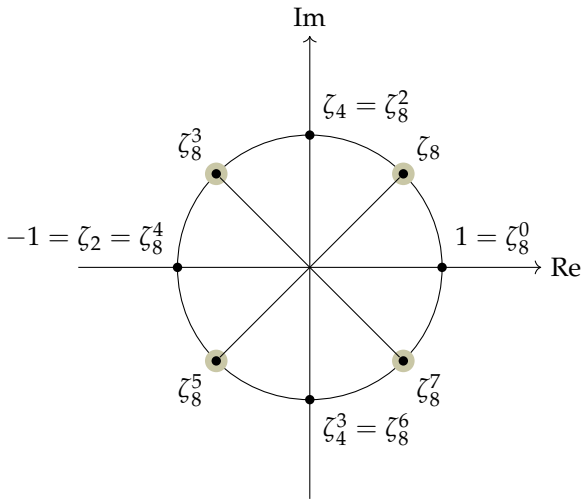
es cíclico de orden n y por ende tiene $\phi(n)$ diferentes generadores. Las raíces n-ésimas que generan a $\mu_n(\mathbb{C})$ se llaman las raíces n-ésimas **primitivas**. Son precisamente ζ_n^k donde k y n son coprimos.

13.7.10. Ejemplo. He aquí una pequeña lista de los grupos $\mu_n(\mathbb{C})$; los elementos subrayados son las raíces primitivas.

$$\mu_1(\mathbb{C}) = \{1\},$$
$$\mu_2(\mathbb{C}) = \{1, \underline{-1}\},$$
$$\mu_3(\mathbb{C}) = \{1, \underline{\zeta_3}, \underline{\zeta_3^2}\} = \left\{1, \underline{\tfrac{-1+\sqrt{-3}}{2}}, \underline{\tfrac{-1-\sqrt{-3}}{2}}\right\},$$
$$\mu_4(\mathbb{C}) = \{1, \underline{\zeta_4}, \zeta_4^2, \underline{\zeta_4^3}\} = \{1, \underline{\sqrt{-1}}, -1, \underline{-\sqrt{-1}}\},$$
$$\mu_5(\mathbb{C}) = \{1, \underline{\zeta_5}, \underline{\zeta_5^2}, \underline{\zeta_5^3}, \underline{\zeta_5^4}\},$$
$$\mu_6(\mathbb{C}) = \{1, \underline{\zeta_6}, \zeta_6^2, \zeta_6^3, \zeta_6^4, \underline{\zeta_6^5}\} = \left\{1, \underline{\tfrac{1+\sqrt{-3}}{2}}, \frac{-1+\sqrt{-3}}{2}, -1, \frac{-1-\sqrt{-3}}{2}, \underline{\tfrac{1-\sqrt{-3}}{2}}\right\},$$
$$\mu_7(\mathbb{C}) = \{1, \underline{\zeta_7}, \underline{\zeta_7^2}, \underline{\zeta_7^3}, \underline{\zeta_7^4}, \underline{\zeta_7^5}, \underline{\zeta_7^6}\},$$
$$\mu_8(\mathbb{C}) = \{1, \underline{\zeta_8}, \zeta_8^2, \underline{\zeta_8^3}, \zeta_8^4, \underline{\zeta_8^5}, \zeta_8^6, \underline{\zeta_8^7}\}$$
$$= \left\{1, \underline{\tfrac{\sqrt{2}+\sqrt{-2}}{2}}, \sqrt{-1}, \underline{\tfrac{-\sqrt{2}+\sqrt{-2}}{2}}, -1, \underline{\tfrac{-\sqrt{2}-\sqrt{-2}}{2}}, -\sqrt{-1}, \underline{\tfrac{-\sqrt{2}+\sqrt{-2}}{2}}\right\}.$$



El grupo $\mu_6(\mathbb{C})$



El grupo $\mu_8(\mathbb{C})$

▲

13.7.11. Definición. El n-ésimo **polinomio ciclotómico**[*] es el polinomio mónico que tiene como sus raíces las raíces n-ésimas primitivas de la unidad:

$$\Phi_n = \prod_{\substack{1 \le k < n \\ \mathrm{mcd}(k,n)=1}} (X - \zeta_n^k).$$

Este polinomio tiene grado $\phi(n) = \#\{k \mid 1 \le k < n,\ \mathrm{mcd}(k,n) = 1\}$.

13.7.12. Ejemplo. Los primeros polinomios ciclotómicos son

$$\begin{aligned}
&\Phi_1 = X - 1,\\
&\Phi_2 = X + 1,\\
&\Phi_3 = (X - \zeta_3)\,(X - \zeta_3^2) = X^2 - (\zeta_3 + \zeta_3^2)\,X + \zeta_3^3 = X^2 + X + 1,\\
&\Phi_4 = (X - \sqrt{-1})\,(X + \sqrt{-1}) = X^2 + 1,\\
&\Phi_5 = \cdots = X^4 + X^3 + X^2 + X + 1,\\
&\Phi_6 = (X - \zeta_6)\,(X - \zeta_6^5) = X^2 - (\zeta_6 + \zeta_6^5)\,X + \zeta_6^6 = X^2 - X + 1,\\
&\Phi_7 = \cdots = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,\\
&\Phi_8 = \cdots = X^4 + 1,\\
&\quad \cdots
\end{aligned}$$

▲

[*] La palabra "ciclotomia" significa "división del círculo".

13.7.13. Comentario. Aunque revisando los primeros Φ_n uno puede pensar que los coeficientes son ± 1, para $n = 105 = 3 \cdot 5 \cdot 7$ en Φ_n aparecen por primera vez coeficientes diferentes:

$$\begin{aligned}\Phi_{105} = X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} + X^{36} + X^{35} + X^{34} \\ + X^{33} + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} + X^{17} + X^{16} + X^{15} \\ + X^{14} + X^{13} + X^{12} - X^9 - X^8 - 2X^7 - X^6 - X^5 + X^2 + X + 1.\end{aligned}$$

13.7.14. Proposición.

1) Para todo primo p se tiene

$$\Phi_p = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + \cdots + X^{p-1}.$$

2) Para todo primo p y $k \geq 1$ se tiene

$$\Phi_{p^k} = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \Phi_p(X^{p^{k-1}}) = 1 + X^{p^{k-1}} + X^{2p^{k-1}} + \cdots + X^{(p-1)\,p^{k-1}}.$$

3) Para todo n se tiene

$$\prod_{d|n} \Phi_d = X^n - 1.$$

4) Todos los polinomios Φ_n tienen coeficientes enteros.

Demostración. En la parte 1), basta notar que entre las raíces p-ésimas, todas son primitivas, salvo la raíz trivial 1.

De la misma manera, en 2) notamos que un número $1 \leq a < p^k$ tal que $a \mid p^k$ necesariamente divide a p^{k-1}, así que las raíces de orden p^k que no son primitivas son precisamente las raíces de orden p^{k-1}.

En la parte 3), basta notar que todas las n-ésimas raíces de la unidad son las raíces complejas del polinomio $X^n - 1$, y cada una de estas raíces aparece una vez como un factor $(X - z)$ en Φ_d para algún d.

La parte 4) se demuestra fácilmente por inducción. Es cierto, por ejemplo, para $n = 1$. Luego, si $\Phi_m \in \mathbb{Z}[X]$ para todo $m < n$, entonces

$$\prod_{d|n} \Phi_d = \Big(\prod_{\substack{d|n \\ d \neq n}} \Phi_d\Big) \cdot \Phi_n = X^n - 1,$$

así que

$$\Phi_n = \frac{X^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d}.$$

A priori, este polimomio tiene coeficientes en $\mathbb{Q}$, pero

$$\operatorname{cont}\Big(\prod_{\substack{d|n\\ d\neq n}} \Phi_d\Big)\cdot \operatorname{cont}(\Phi_n) = \operatorname{cont}(X^n-1) = 1,$$

así que $\Phi_n \in \mathbb{Z}[X]$. ■

13.7.15. Lema. *Para todo $a \in R$ un polinomio no constante $f \in R[X]$ es irreducible si y solo si $f(X+a)$ es irreducible.*

Demostración. Notamos que $\deg f(X) = \deg f(X+a)$. Una factorización no trivial $f(X+a) = g(X)\,h(X)$ nos daría una factorización $f(X) = g(X-a)\,h(X-a)$. ■

13.7.16. Proposición. *Para todo primo p el polinomio Φ_p es irreducible en $\mathbb{Z}[X]$.*

Demostración. El polinomio $\Phi_p(X)$ es irreducible si y solo si $\Phi_p(X+1)$ es irreducible. Notamos que

$$\begin{aligned}\Phi_p(X+1) = \frac{(X+1)^p-1}{(X+1)-1} &= \frac{1}{X}\sum_{1\le k\le p}\binom{p}{k}X^k\\ &= \binom{p}{p}X^{p-1} + \binom{p}{p-1}X^{p-2} + \cdots + \binom{p}{3}X^2 + \binom{p}{2}X + \binom{p}{1}.\end{aligned}$$

Los coeficientes de arriba satisfacen

$$p \mid \binom{p}{k} \text{ para todo } 1\le k<p \quad \text{y} \quad p^2 \nmid \binom{p}{1} = p.$$

Entonces, se puede aplicar el criterio de Eisenstein respecto al ideal $p\mathbb{Z} \subset \mathbb{Z}$. ■

13.7.17. Proposición. *Para todo primo p y $k \ge 1$ el polinomio Φ_{p^k} es irreducible en $\mathbb{Z}[X]$.*

Demostración. Ya vimos el caso $k = 1$. Podemos asumir entonces que $k \ge 2$. De nuevo, consideremos la sustitución

$$\Phi_{p^k}(X+1) = \frac{(X+1)^{p^k}-1}{(X+1)^{p^{k-1}}-1} = \sum_{0\le i\le p-1}(X+1)^{i\,p^{k-1}}.$$

Tenemos para todo $k \ge 2$

$$(X+1)^{p^{k-1}} \equiv X^{p^{k-1}} + 1 \pmod{p},$$

y luego

$$\begin{aligned}\Phi_{p^k}(X+1) \equiv \sum_{0\le i\le p-1}(X^{p^{k-1}}+1)^i &= \frac{(X^{p^{k-1}}+1)^p-1}{(X^{p^{k-1}}+1)-1}\\ &= \frac{(X^{p^{k-1}}+1)^p-1}{X^{p^{k-1}}} \equiv \frac{X^{p^k}}{X^{p^{k-1}}} = X^{p^{k-1}(p-1)} \pmod{p}.\end{aligned}$$

Todos los coeficientes menores de $\Phi_{p^k}(X+1)$ son divisibles por p. El coeficiente constante es igual a

$$\Phi_{p^k}(1) = \Phi_p(1^{p^{k-1}}) = \Phi_p(1) = p,$$

que no es divisible por p^2. Podemos aplicar el criterio de Eisenstein. ■

13.7.18. Ejemplo. El polinomio $\Phi_8 = X^4 + 1$ es irreducible en $\mathbb{Z}[X]$. Esto sigue del criterio de Eisenstein aplicado a

$$\Phi_8(X+1) = X^4 + 4X^3 + 6X^2 + 4X + 2.$$

▲

En general, Gauss probó que Φ_n es irreducible para cualquier n, pero por el momento nos contentamos con el caso de $n = p^k$ como una aplicación del criterio de Eisenstein.

13.7.19. Ejemplo. Probemos que el polinomio $f = X^2 + Y^2 - Z^2$ es irreducible en $\mathbb{C}[X, Y, Z]$.

Usando la identificación $\mathbb{C}[X, Y, Z] \cong \mathbb{C}[Y, Z][X]$, podemos considerar f como un polinomio en X con término constante $Y^2 - Z^2$. Para aplicar el criterio de Eisenstein, necesitamos encontrar un ideal primo $\mathfrak{p} \subset \mathbb{C}[Y, Z]$ tal que $Y^2 - Z^2 \in \mathfrak{p}$, pero $Y^2 - Z^2 \notin \mathfrak{p}^2$. Sería suficiente tomar $\mathfrak{p} = (p)$ donde $p \in \mathbb{C}[Y, Z]$ es algún polinomio irreducible en $\mathbb{C}[Y, Z]$ tal que $p \mid (Y^2 - Z^2)$, pero $p^2 \nmid (Y^2 - Z^2)$. El mismo $Y^2 - Z^2$ es reducible: se tiene

$$Y^2 - Z^2 = (Y + Z)\,(Y - Z).$$

Sin embargo, cada uno de los factores $Y \pm Z$ es irreducible, siendo un polinomio lineal, y su cuadrado no divide a $Y^2 - Z^2$. Podemos generalizar este argumento al caso de

$$f = X^n + Y^n - Z^n \in \mathbb{C}[X, Y, Z].$$

De la misma manera, bastaría ver que el polinomio $Y^n - Z^n$ no tiene cuadrados en su factorización en $\mathbb{C}[Y, Z]$. Notamos que en el cuerpo de fracciones $\mathbb{C}(Y, Z) = \{f/g \mid f, g \in \mathbb{C}[Y, Z],\ g \neq 0\}$ se tiene

$$\left(\frac{Y}{Z}\right)^n - 1 = \prod_{0 \leq k \leq n-1} \left(\frac{Y}{Z} - \zeta_n^k\right),$$

donde $\zeta_n := e^{2\pi\sqrt{-1}/n}$, y luego

$$Y^n - Z^n = \prod_{0 \leq k \leq n-1} (Y - \zeta_n^k\, Z).$$

Las ecuaciones de la forma $X^n + Y^n - Z^n$ se conocen como las **ecuaciones de Fermat**. El **último teorema de Fermat** (demostrado en 1995 por el matemático inglés Andrew Wiles con ayuda de Richard Taylor) afirma que para $n > 2$ sus únicas soluciones racionales son de la forma

$$\begin{cases} \{(x, 0, x), (0, y, y)\}, & n \text{ impar}, \\ \{(\pm x, 0, \pm x), (0, \pm y, \pm y)\}, & n \text{ par}. \end{cases}$$

▲

13.8 Ejercicios

Ejercicio 13.1. *Hemos notado que el anillo $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única. En este ejercicio vamos a probar que en efecto $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de ideales principales. De nuevo, nos va a servir la norma*

$$N(a+b\sqrt{-5}) := (a+b\sqrt{-5})\,(a-b\sqrt{-5}) = a^2+5\,b^2.$$

Consideremos el ideal $I = (3, 2+\sqrt{-5})$. Supongamos que $I = (\alpha)$ para algún $\alpha \in \mathbb{Z}[\sqrt{-5}]$. En particular, existen $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$ tales que

$$3 = \beta\alpha, \quad 2+\sqrt{-5} = \gamma\alpha.$$

Analice las normas y obtenga una contradicción. Concluya que el ideal I no es principal.

Ejercicio 13.2. *Sea $n \geq 3$ un entero libre de cuadrados. En este ejercicio vamos a probar que el anillo $\mathbb{Z}[\sqrt{-n}]$ no es un dominio de factorización única. (Los anillos $\mathbb{Z}[\sqrt{-1}]$ y $\mathbb{Z}[\sqrt{-2}]$ son dominios euclidianos y por ende sí son dominios de factorización única.) Consideremos la norma*

$$N(a+b\sqrt{-n}) := (a+b\sqrt{-n})\,(a-b\sqrt{-n}) = a^2+n\,b^2.$$

1) *Demuestre que 2 es irreducible en $\mathbb{Z}[\sqrt{-n}]$.*

2) *Demuestre que $1 \pm \sqrt{-n}$ es irreducible en $\mathbb{Z}[\sqrt{-n}]$.*

   Indicación: si $1 \pm \sqrt{-n} = xy$ para $x, y \notin \mathbb{Z}[\sqrt{-n}]^\times$, analice las normas.

3) *Si n es par, demuestre que $2 \mid (\sqrt{-n})^2$, pero $2 \nmid \sqrt{-n}$.*

4) *Si n es impar, demuestre que $2 \mid (1+\sqrt{-n})\,(1-\sqrt{-n})$, pero $2 \nmid (1 \pm \sqrt{-n})$.*

Concluya que 2 es un elemento irreducible, pero no es primo, así que $\mathbb{Z}[\sqrt{-n}]$ no puede ser un dominio de factorización única.

Ejercicio 13.3. *Ya sabemos que los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ forman un dominio de factorización única. En este ejercicio vamos a describir los elementos primos (irreducibles) en $\mathbb{Z}[\sqrt{-1}]$. Para encontrarlos, hay que factorizar los enteros primos $p = 2, 3, 5, 7, 11, \ldots$ en $\mathbb{Z}[\sqrt{-1}]$.*

1) *Demuestre que si para un elemento $\pi = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ la norma $N(\pi) = a^2+b^2 = p$ es un número entero primo, entonces π es un elemento primo en $\mathbb{Z}[\sqrt{-1}]$.*

2) *Sea π un elemento primo en $\mathbb{Z}[\sqrt{-1}]$. Demuestre que $\pi \mid p$ donde p es un número entero primo. Factorice $2, 3, 5$ en elementos primos en $\mathbb{Z}[\sqrt{-1}]$.*

   Sugerencia: note que $\pi \mid N(\pi)$.

3) *Sea $p \in \mathbb{Z}$ un número entero primo. Demuestre que p es compuesto en $\mathbb{Z}[\sqrt{-1}]$ si y solamente si $p = a^2+b^2$ para algunos $a, b \in \mathbb{Z}$, y en este caso p se descompone en dos factores primos conjugados.*

Comentario. En la teoría de números elemental se demuestra que un primo $p \in \mathbb{Z}$ puede ser escrito como una suma de dos cuadrados $a^2 + b^2$ si y solamente si $p = 2$ o $p \equiv 1 \pmod 4$.

Ejercicio 13.4. *Demuestre que el anillo $\mathbb{Z}[\sqrt{-2}]$ es un dominio euclidiano respecto a la norma habitual*

$$N(a + b\sqrt{-2}) := (a + b\sqrt{-2})\,(a - b\sqrt{-2}) = a^2 + 2\,b^2.$$

Ejercicio 13.5. *Demuestre que el anillo $\mathbb{Z}[\omega]$ donde $\omega := \frac{1+\sqrt{-3}}{2}$ es un dominio euclidiano respecto a la norma habitual*

$$N(a + b\,\omega) := (a + b\,\omega)\,(a + b\,\overline{\omega}) = a^2 + ab + b^2.$$

Ejercicio 13.6. *Sea p un número primo. Para el anillo $\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ p \nmid b \right\}$ definamos*

$$v_p\left(\frac{a}{b}\right) := \text{máx}\{k \mid p^k \mid a\}, \quad v_p(0) := +\infty.$$

1) *Demuestre que para cualesquiera $x, y \in \mathbb{Z}_{(p)}$ se cumple*

$$v_p(xy) = v_p(x) + v_p(y).$$

2) *Demuestre que todo elemento no nulo $x \in \mathbb{Z}_{(p)}$ puede ser escrito como up^n donde $u \in \mathbb{Z}_{(p)}^{\times}$ y $n = v_p(x)$.*

3) *Demuestre que todo elemento irreducible en $\mathbb{Z}_{(p)}$ está asociado con p.*

4) *Demuestre que $\mathbb{Z}_{(p)}$ es un dominio euclidiano respecto a v_p.*

Ejercicio 13.7. *Sea k un cuerpo. Consideremos el anillo de las series de potencias $k[\![X]\!]$. Definamos para $f = \sum_{i \geq 0} a_i\, X^i \in k[\![X]\!]$*

$$v_X(f) := \text{máx}\{i \mid a_i = 0\}, \quad v_X(0) := +\infty.$$

1) *Demuestre que para cualesquiera $f, g \in k[\![X]\!]$ se cumple*

$$v_X(fg) = v_X(f) + v_X(g).$$

2) *Demuestre que toda serie no nula $f \in k[\![X]\!]$ puede ser escrita como $g\,X^n$ donde $g \in k[\![X]\!]^{\times}$ y $n = v_X(f)$.*

3) *Demuestre que todo elemento irreducible en $k[\![X]\!]$ está asociado con X.*

4) *Demuestre que $k[\![X]\!]$ es un dominio euclidiano respecto a v_X.*

Comentario. $\mathbb{Z}_{(p)}$ y $k[\![X]\!]$ son ejemplos de **anillos de valuación discreta**.

Ejercicio 13.8. *Sea R un dominio de integridad. Una **norma de Dedekind** es una función $\delta\colon R \setminus \{0\} \to \mathbb{N}$ que satisface la siguiente propiedad: para cualesquiera $x, y \in R \setminus \{0\}$, si $x \nmid y$, entonces existen $a, b \in R$ tales que*

$$ax + by \neq 0, \quad \delta(ax + by) < \delta(x).$$

Demuestre que si sobre R existe una norma de Dedekind, entonces R es un dominio de ideales principales.

Ejercicio 13.9 (H.F. Trotter, The American Mathematical Monthly, Vol. 95, No. 4). *Definamos un **polinomio trigonométrico** como una suma finita*

$$f(x) = a_0 + \sum_{1 \leq k \leq n} (a_k \cos kx + b_k \operatorname{sen} kx),$$

*donde $a_k, b_k \in \mathbb{R}$. Digamos que el **grado** de f es el mayor k tal que $a_k \neq 0$ o $b_k \neq 0$.*

1) *Demuestre que si f y g son polinomios trigonométricos de grado m y n respectivamente, entonces fg es un polinomio trigonométrico de grado $m + n$.*
2) *Demuestre que los polinomios trigonométricos forman un dominio de integridad. Denotémoslo por $Trig_{\mathbb{R}}$.*
3) *Demuestre que los elementos invertibles en $Trig_{\mathbb{R}}$ son los polinomios trigonométricos no nulos de grado 0.*
4) *Demuestre que todo polinomio trigonométrico de grado 1 es irreducible en $Trig_{\mathbb{R}}$.*
5) *Observando la identidad $(\operatorname{sen} x)^2 = (1 + \cos x)(1 - \cos x)$, demuestre que $Trig_{\mathbb{R}}$ no es un dominio de factorización única.*

Valuaciones p-ádicas

Ejercicio 13.10. *Sea $p = 2, 3, 5, 7, \ldots$ un número primo y $k = 1, 2, 3, 4, \ldots$ Calcule que*

$$v_p\left(\binom{p^k}{n}\right) = k - v_p(n) \quad \text{para todo } n = 1, 2, \ldots, p^k.$$

Indicación: calcule las valuaciones p-ádicas de ambos lados de la identidad

$$n!\binom{p^k}{n} = p^k (p^k - 1)(p^k - 2) \cdots (p^k - n + 1).$$

Note que $v_p(p^k - a) = v_p(a)$ para todo $a = 1, 2, \ldots, p^k - 1$

Ejercicio 13.11 (Fórmula de Legendre). *Demuestre que para todo primo p y todo número natural n se tiene*

$$v_p(n!) = \sum_{i \geq 1} \lfloor n / p^i \rfloor.$$

En particular, calcule $v_2(100!)$.

Ejercicio 13.12 (Normas p-ádicas). *Sea R un dominio de factorización única y $p \in R$ un elemento primo. Fijemos un número real $0 < \rho < 1$ y pongamos para todo $x \in R$*

$$|x|_p := \rho^{v_p(x)}.$$

Demuestre que $|\cdot|_p$ cumple las siguientes propiedades.

N1) $|x|_p = 0$ *si y solo si* $x = 0$.

N2) $|xy|_p = |x|_p \cdot |y|_p$.

N3) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$, *y se cumple la igualdad si* $|x|_p \neq |y|_p$.

Factorizaciones de polinomios

Ejercicio 13.13. *Compile una lista de los polinomios cuadráticos irreducibles en $\mathbb{F}_3[X]$.*

Ejercicio 13.14. *Sean k un cuerpo y $f \in k[X]$ un polinomio de grado 2 o 3. Demuestre que f es irreducible en $k[X]$ si y solo si f no tiene raíces en k.*

Ejercicio 13.15. *Consideremos el polinomio $f := X^3 + 2X + 1 \in \mathbb{Z}[X]$.*

1) *Demuestre que $\overline{f} \in \mathbb{F}_2[X]$ es reducible.*
2) *Demuestre que $\overline{f} \in \mathbb{F}_3[X]$ es irreducible.*
   Indicación: use el ejercicio anterior.
3) *Demuestre que f es irreducible en $\mathbb{Z}[X]$.*

Ejercicio 13.16. *Factorice el polinomio $X^4 + 4$ en polinomios irreducibles en $\mathbb{Z}[X]$.*

Ejercicio 13.17. *Consideremos el polinomio $f = X^3 + 8X^2 + 6 \in \mathbb{Z}[X]$.*

1) *Demuestre que f es irreducible usando el criterio de Eisenstein.*
2) *Factorice este polinomio en $\mathbb{F}_p[X]$ para $p = 2, 3, 5, 7$.*
   (En efecto, el primer primo p tal que $\overline{f}$ queda irreducible en $\mathbb{F}_p[X]$ es 29.)

Ejercicio 13.18. *Factorice el polinomio $X^n + Y^n$ en polinomios lineales en $\mathbb{C}[X, Y]$.*

Ejercicio 13.19 (Teorema de las raíces racionales). *Sea*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

un polinomio con coeficientes enteros. Demuestre que si $\frac{a}{b}$ es una raíz racional de f tal que $\mathrm{mcd}(a, b) = 1$, entonces $a \mid a_0$ y $b \mid a_n$.

Ejercicio 13.20. *Sea c un entero no nulo.*

1) *Demuestre que el polinomio $X^3 + n X + c$ es irreducible en $\mathbb{Q}[X]$ para todo $n \in \mathbb{Z}$, salvo un número finito de excepciones.*

2) *En particular, para* $c = 2$ *encuentre las factorizaciones del polinomio* $f = X^3 + nX + 2$ *para todo* n.

Indicación: use el ejercicio anterior.

Ejercicio 13.21. *Encuentre los coeficientes en la expansión de los polinomios ciclotómicos* Φ_{10} *y* Φ_{15}.

Ejercicio 13.22. *Sea* p *un número primo. Factorice el polinomio ciclotómico* Φ_{p^k} *en* $\mathbb{F}_p[X]$.

Parte IV
Teoría de cuerpos

Capítulo 14
Cuerpos

En este capítulo vamos a estudiar algunas propiedades especiales de los cuerpos.

Primero revisemos un par de resultados que ya hemos visto de alguna manera en el capítulo 11.

Para un cuerpo K consideremos el homomorfismo canónico $\phi\colon \mathbb{Z} \to K$.

- Si ϕ es inyectivo, se dice que K tiene **característica** 0. En este caso K contiene un subanillo $\operatorname{im}\phi$ que es isomorfo a $\mathbb{Z}$. Siendo un cuerpo, K también debe contener todos los inversos de los elementos no nulos de $\operatorname{im}\phi$, así que K contiene un *subcuerpo* isomorfo a $\mathbb{Q}$.
- Si ϕ no es inyectivo, entonces $\operatorname{im}\phi \cong \mathbb{Z}/n\mathbb{Z}$. Dado que K no tiene divisores de cero, el número $n = p$ es necesariamente primo. En este caso se dice que K tiene **característica** p. Notamos que $\mathbb{Z}/n\mathbb{Z} = \mathbb{F}_p$ es un cuerpo.

Podemos resumir que la característica de K corresponde al subcuerpo mínimo de K. Si este es isomorfo a $\mathbb{Q}$, entonces la característica es 0; si es isomorfo a $\mathbb{F}_p$, entonces la característica es p.

14.0.1. Ejemplo. Los cuerpos

$$\mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{C}, \quad \mathbb{Q}(X) := \left\{ \frac{f}{g} \;\middle|\; f, g \in \mathbb{Q}[X],\ g \neq 0 \right\}$$

tienen característica 0. Los cuerpos $\mathbb{F}_p$ y $\mathbb{F}_p(X)$ tienen característica p. ▲

Recordemos también que un cuerpo K tiene como sus ideales solamente (0) y K. Esto implica que todos los homomorfismos de cuerpos son inyectivos.

14.0.2. Observación. *Sea $\phi\colon K \to R$ un homomorfismo donde K es un cuerpo y R es un anillo no nulo. Entonces, ϕ es inyectivo.*

Demostración. El núcleo de ϕ es un ideal en K. Puesto que $R \neq 0$, tenemos $\phi(1) = 1 \neq 0$[*], así que $\ker\phi \neq K$. Luego, $\ker\phi = (0)$. ■

[*] Según nuestra convención, un homomorfismo de anillos preserva la identidad 1.

14.1 Extensiones de cuerpos

14.1.1. Definición. Si L es un cuerpo y $K \subseteq L$ es un subcuerpo (un subanillo que es también un cuerpo), se dice que L es una **extensión** de K y se escribe "L/K"* o se dibuja el diagrama

$$\begin{array}{c} L \\ | \\ K \end{array}$$

El lector puede comprobar que en la situación de arriba L satisface los axiomas de espacio vectorial sobre K.

14.1.2. Definición. La dimensión de L como un espacio vectorial sobre K se llama el **grado** de la extensión y se denota por

$$[L : K] := \dim_K L.$$

Si el grado es finito, se dice que L/K es una **extensión finita**. Cuando el grado no es finito, a veces se suele escribir "$[L : K] = \infty$".

14.1.3. Ejemplo. Los números complejos $\mathbb{C}$ es una extensión de grado 2 de los números reales $\mathbb{R}$. Los números 1 y $\sqrt{-1}$ forman una base de $\mathbb{C}$ sobre $\mathbb{R}$. ▲

14.1.4. Ejemplo. Los números reales $\mathbb{R}$ forman una extensión infinita de los números racionales $\mathbb{Q}$. En efecto, para toda extensión finita $K/\mathbb{Q}$ se tiene un isomorfismo $K \cong \mathbb{Q}^n$ de espacios vectoriales sobre $\mathbb{Q}$, donde $n = [K : \mathbb{Q}]$. Luego, $\mathbb{Q}^n$ es numerable, puesto que $\mathbb{Q}$ lo es. Sin embargo, $\mathbb{R}$ no es numerable. De hecho, todo espacio vectorial sobre $\mathbb{Q}$ de dimensión *numerable* es un conjunto numerable, así que este argumento nos dice que la dimensión de $\mathbb{R}$ sobre $\mathbb{Q}$ no es numerable.

Sin analizar las cardinalidades, se puede encontrar un subconjunto infinito de $\mathbb{R}$ que es linealmente independiente sobre $\mathbb{Q}$. Consideremos los números $\log p$ donde $p = 2, 3, 5, 7, 11, \ldots$ son primos. Si tenemos

$$a_1 \log p_1 + \cdots + a_n \log p_n = 0$$

para diferentes primos $p_1, \ldots, p_n$ y algunos $a_1, \ldots, a_n \in \mathbb{Q}$, entonces podemos primero cancelar los denominadores y asumir que $a_1, \ldots, a_n \in \mathbb{Z}$. Luego,

$$p_1^{a_1} \cdots p_n^{a_n} = 1,$$

lo que implica $a_1 = \cdots = a_n = 0$. ▲

14.1.5. Ejemplo. Si $K/\mathbb{F}_p$ es una extensión de grado n del cuerpo finito $\mathbb{F}_p$, entonces $|K| = p^n$. En el siguiente capítulo vamos a describir todas las extensiones finitas de $\mathbb{F}_p$. ▲

14.1.6. Proposición. *Para una cadena de cuerpos $F \subseteq K \subseteq L$ se tiene*

$$[L : F] = [L : K] \cdot [K : F].$$

Específicamente,

*Cuidado: es solamente una notación estándar que no significa ningún tipo de cociente.

1) *si* $[L : K] < \infty$ *y* $[K : F] < \infty$, *entonces* $[L : F] = [L : K] \cdot [K : F]$; *además,* $[L : F] = \infty$ *si y solo si se cumple* $[L : K] = \infty$ *o* $[K : F] = \infty$;

2) *si* $\alpha_1, \ldots, \alpha_m \in K$ *es una base de* K *sobre* F *y* $\beta_1, \ldots, \beta_n \in L$ *es una base de* L *sobre* K, *entonces los productos* $\alpha_i\beta_j$ *forman una base de* L *sobre* F.

$$\begin{array}{cc} L & \beta_1, \ldots, \beta_n \\ {\scriptstyle [L:K]=n}\big| & \\ K & \alpha_1, \ldots, \alpha_m \\ {\scriptstyle [K:F]=m}\big| & \\ F & \end{array}$$

Demostración. Todo elemento de L puede ser escrito como

$$x = \sum_{1 \le j \le n} b_j \beta_j$$

para algunos $b_1, \ldots, b_n \in K$. Luego, los coeficientes b_j pueden ser expresados como

$$b_j = \sum_{1 \le i \le m} a_{ij} \alpha_i$$

para algunos $a_{ij} \in F$. Luego,

$$x = \sum_{1 \le j \le n} \sum_{1 \le i \le m} a_{ij} \alpha_i \beta_j,$$

lo que significa que los productos $\alpha_i\beta_j$ generan a L como un espacio vectorial sobre F. Para ver que esto es una base, hay que ver que los elementos $\alpha_i\beta_j$ son linealmente independientes. Si la combinación lineal de arriba es igual a 0, entonces se tiene $\sum_{1 \le j \le n} b_j \beta_j = 0$, de donde $b_j = 0$ para todo j por la independencia lineal de los β_j. Pero la independencia lineal de los α_i implica entonces que $a_{ij} = 0$ para todo i.

Notamos que si $[K : F] = \infty$, entonces existe un número infinito de elementos $\alpha \in K$ linealmente independientes sobre F. En particular, $\alpha \in L$ y esto significa que $[L : F] = \infty$. De la misma manera, si $[L : K] = \infty$, entonces existe un número infinito de elementos $\beta \in L$ que son linealmente independientes sobre K. En particular, son linealmente independientes sobre F y $[L : F] = \infty$. En fin, si $[L : F] = \infty$, entonces $[L : K] = \infty$ o $[K : F] = \infty$. En efecto, el argumento de arriba nos dice que $[L : K] < \infty$ y $[K : F] < \infty$ implica $[L : F] < \infty$. ■

En práctica muchas extensiones se obtienen "añadiendo" al cuerpo de base K una raíz de algún polinomio irreducible $f \in K[X]$. Por ejemplo, $\mathbb{C}$ es el resultado de añadir a $\mathbb{R}$ una raíz del polinomio $X^2 + 1$ que es irreducible en $\mathbb{R}[X]$. En general, se tiene el siguiente resultado.

14.1.7. Teorema. *Sea* K *un cuerpo y* $f \in K[X]$ *un polinomio irreducible de grado* n. *Entonces,*

1) *el anillo cociente* $L := K[X]/(f)$ *es un cuerpo;*

2) *el homomorfismo canónico* $\phi\colon K \hookrightarrow K[X] \twoheadrightarrow K[X]/(f)$ *es inyectivo e identifica a* K *con un subcuerpo de* L *y entonces a* $K[X]$ *con un subanillo de* $L[X]$;

3) *si* $\alpha := X \mod f \in L$ *es la imagen de la variable* X *en el cociente, entonces* $[L : K] = n$ *y los elementos* $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ *forman una base de* L *sobre* K*; en particular,*

$$L = \{a_0 + a_1\,\alpha + \cdots + a_{n-1}\,\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in K\};$$

4) *considerando a* f *como un elemento de* $L[X]$*, se tiene* $f(\alpha) = 0$*.*

Demostración. Como sabemos, $K[X]$ es un dominio de ideales principales, y entonces si f es irreducible, el ideal $(f) \subset K[X]$ es maximal (si f es irreducible, entonces f es primo, así que el ideal (f) es primo, y luego todo ideal primo no nulo en $K[X]$ es maximal). Esto significa que $K[X]/(f)$ es un cuerpo.

Ahora $\phi\colon K \hookrightarrow K[X] \twoheadrightarrow K[X]/(f)$ es un homomorfismo de cuerpos y por ende es inyectivo.

Todo elemento de $K[X]/(f)$ puede ser representado por algún polinomio $g \in K[X]$ considerado módulo f. La división con resto en $K[X]$ nos permite escribir

$$g = qf + r, \quad \deg r < \deg f,$$

así que $g \equiv r \pmod f$. Esto significa que los elementos del cociente $K[X]/(f)$ se representan por polinomios

$$g = a_0 + a_1\,X + \cdots + a_{n-1}\,X^{n-1}$$

para algunos $a_0, a_1, \ldots, a_{n-1} \in K$. La reducción de g módulo f nos da

$$\begin{aligned}\overline{g} = \overline{a_0 + a_1\,X + \cdots + a_{n-1}\,X^{n-1}} &= a_0 + a_1\,\overline{X} + \cdots + a_{n-1}\,\overline{X}^{n-1} \\ &= a_0 + a_1\,\alpha + \cdots + a_{n-1}\,\alpha^{n-1} \in L.\end{aligned}$$

Entonces, $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ generan a L como un espacio vectorial sobre K y solo falta ver que son linealmente independientes. Si tenemos

$$a_0 + a_1\,\alpha + \cdots + a_{n-1}\,\alpha^{n-1} = 0,$$

esto significa que el polinomio

$$g = a_0 + a_1\,X + \cdots + a_{n-1}\,X^{n-1} \in K[X]$$

se reduce a 0 módulo f; es decir, $f \mid g$. Pero todos los múltiplos no nulos de f tienen grado $\geq n$, mientras que $\deg g \leq n - 1$, así que necesariamente $g = 0$ y $a_0 = a_1 = \cdots = a_{n-1} = 0$.

De la construcción está claro que $f(\alpha) = 0$. ■

14.1.8. Ejemplo. Sea d un número entero libre de cuadrados diferente de 1. El polinomio $X^2 - d$ es irreducible en $\mathbb{Q}[X]$ (por ejemplo, porque sus raíces son irracionales para $d > 1$ o imaginarias para $d < 0$). Por el resultado de arriba, el anillo cociente $K := \mathbb{Q}[X]/(X^2 - d)$ es un cuerpo y $[K : \mathbb{Q}] = 2$. Denotando la imagen de X en el cociente por $\alpha \in K$, se tiene

$$K = \{a + b\,\alpha \mid a, b \in \mathbb{Q}\}.$$

La adición evidentemente viene dada por

$$(a_1 + b_1\,\alpha) + (a_2 + b_2\,\alpha) = (a_1 + a_2) + (b_1 + b_2)\,\alpha.$$

Para la multiplicación, hay que notar que en K se cumple la relación $\alpha^2 = d$:

$$(a_1 + b_1\,\alpha)\cdot(a_2 + b_2\,\alpha) = a_1\,a_2 + (a_1 b_2 + a_2 b_1)\,\alpha + b_1 b_2\,\alpha^2 = (a_1\,a_2 + d\,b_1\,b_2) + (a_1 b_2 + a_2 b_1)\,\alpha.$$

Para invertir un elemento $a + b\,\alpha \neq 0$, se puede primero notar que

$$(a + b\,\alpha)\,(a - b\,\alpha) = a^2 - b^2\,\alpha^2 = a^2 - b^2\,d,$$

y puesto que d es libre de cuadrados, este es un número racional no nulo. Luego,

$$(a + b\,\alpha)^{-1} = \frac{a}{a^2 - b^2\,d} - \frac{b}{a^2 - b^2\,d}\,\alpha.$$

▲

14.1.9. Ejemplo. El polinomio ciclotómico Φ_n es irreducible en $\mathbb{Q}[X]$ y tiene grado $\phi(n)$, así que el cuerpo $K := \mathbb{Q}[X]/(\Phi_n)$ es una extensión de grado $\phi(n)$ de $\mathbb{Q}$. ▲

14.1.10. Ejemplo. El polinomio $X^3 - 2$ es irreducible en $\mathbb{Q}[X]$, por ejemplo, gracias al criterio de Eisenstein para $p = 2$. El cociente $K := \mathbb{Q}[X]/(X^3 - 2)$ es una extensión de grado 3 de $\mathbb{Q}$; tenemos

$$K = \{a + b\,\alpha + c\,\alpha^2 \mid a, b, c \in \mathbb{Q}\},$$

donde como siempre, α denota la imagen de X en el cociente. La multiplicación de los elementos se sigue de la relación $\alpha^3 = 2$, pero la fórmula general no es muy instructiva:

$$\begin{aligned}(a_1 + b_1\,\alpha + c_1\,\alpha^2)\,(a_2 + b_2\,\alpha + c_2\,\alpha^2)&\\ = a_1 a_2 + (a_1 b_2 + a_2 b_1)\,\alpha + (a_1 c_2 + a_2 c_1 + b_1 b_2)\,\alpha^2 + (b_1 c_2 + b_2 c_1)\,\alpha^3 + c_1\,c_2\,\alpha^4&\\ = a_1 a_2 + 2\,(b_1 c_2 + b_2 c_1) + (a_1 b_2 + a_2 b_1 + 2\,c_1\,c_2)\,\alpha + (a_1 c_2 + a_2 c_1 + b_1 b_2)\,\alpha^2.&\end{aligned}$$

▲

14.1.11. Ejemplo. El polinomio $X^2 + X + 1$ es irreducible en $\mathbb{F}_2[X]$. Consideremos el cociente

$$K := \mathbb{F}_2[X]/(X^2 + X + 1).$$

Denotando por α la imagen de X, se ve que

$$K = \{0, 1, \alpha, \alpha + 1\}.$$

Tenemos $[K : \mathbb{F}_2] = 2$ y los elementos 1 y α forman una base de K sobre $\mathbb{F}_2$. Las tablas de adición y multiplicación correspondientes son

$+$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$\times$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

De la misma manera se obtienen todos los cuerpos finitos. Si K es un cuerpo finito, entonces necesariamente $\operatorname{char} K = p$ para algún primo p, lo que significa que K es una extensión finita de $\mathbb{F}_p$. Resulta que $\mathbb{F}_p$ tiene una sola extensión de grado n salvo isomorfismo que se obtiene como $\mathbb{F}_p[X]/(f)$, donde $f \in \mathbb{F}_p[X]$ es un polinomio irreducible de grado n. La existencia de este f es algo que vamos a probar en el siguiente capítulo. ▲

Hemos visto cómo añadir a un cuerpo K una raíz de un polinomio irreducible $f \in K[X]$ de manera formal: hay que pasar al cociente $K[X]/(f)$. En muchos casos estas raíces ya están en una extensión específica de K y pueden ser añadidas en el siguiente sentido.

14.1.12. Definición. Para una extensión de cuerpos L/K y elementos $\alpha_1, \alpha_2, \ldots \in L$ el subcuerpo mínimo de L que contiene a $\alpha_1, \alpha_2, \ldots$ y todos los elementos de K se llama el subcuerpo **generado** por $\alpha_1, \alpha_2, \ldots$ sobre K y se denota por

$$K(\alpha_1, \alpha_2, \ldots) = \bigcap_{\substack{K \subseteq K' \subseteq L \\ \alpha_1, \alpha_2, \ldots \in K'}} K'.$$

Las extensiones de la forma $K(\alpha)/K$ para un solo elemento $\alpha \in L$ se llaman las **extensiones simples** de K. En este caso α se llama un **elemento primitivo** de $K(\alpha)$.

En general, las extensiones de la forma $K(\alpha_1, \ldots, \alpha_n)/K$ se llaman las **extensiones finitamente generadas** de K.

14.1.13. Ejemplo. Para un entero libre de cuadrados $d \neq 1$ consideremos $\sqrt{d} \in \mathbb{C}$ (si $d > 1$, entonces $\sqrt{d} \in \mathbb{R}$). Tenemos entonces

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

En efecto, la parte derecha está contenida en $\mathbb{Q}(\sqrt{d})$. Se ve fácilmente que es un subanillo de $\mathbb{C}$, y de hecho, es un subcuerpo: para $(a, b) \neq (0, 0)$ se tiene

$$\frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - db^2} = \frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2}\sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

(note que $a^2 \neq db^2$, puesto que d es libre de cuadrados). ▲

Toda extensión finita $K/\mathbb{Q}$ es simple: es de la forma $\mathbb{Q}(\alpha)$ para algún $\alpha \in \mathbb{C}$, pero lo veremos más adelante, después de desarrollar la teoría general adecuada. Por el momento, podemos ver algunos ejemplos sencillos.

14.1.14. Ejemplo. Consideremos el cuerpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Denotemos

$$\alpha := \sqrt{2} + \sqrt{3}.$$

Obviamente, tenemos $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Luego, calculamos que

$$\alpha^2 = 5 + 2\sqrt{6}, \quad \alpha^3 = 11\sqrt{2} + 9\sqrt{3}, \quad \alpha^4 = 49 + 20\sqrt{6},$$

de donde

$$\sqrt{2} = \frac{1}{2}(\alpha^3 - 9\alpha), \quad \sqrt{3} = -\frac{1}{2}(\alpha^3 - 11\alpha),$$

así que $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$ y podemos concluir que

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

▲

14.1.15. Ejemplo. Consideremos los elementos

$$\zeta_3 := e^{2\pi\sqrt{-1}/3} = \frac{-1+\sqrt{-3}}{2}, \quad \sqrt[3]{2}, \quad \alpha := \zeta_3 + \sqrt[3]{2}.$$

Tenemos

$$2 = (\alpha - \zeta_3)^3 = \alpha^3 + 3\,\alpha\,\zeta_3^2 - 3\,\alpha^2\,\zeta_3 - \zeta_3^3.$$

Dado que $\zeta_3^3 = 1$ y $\zeta_3^2 = -1 - \zeta_3$, esto nos da la ecuación

$$3 = \alpha^3 - 3\,\alpha - 3\,\alpha\,(1+\alpha)\,\zeta_3,$$

de donde se puede expresar

$$\zeta_3 = \frac{\alpha^3 - 3\,\alpha - 3}{3\,\alpha\,(1+\alpha)},$$

así que $\zeta_3 \in \mathbb{Q}(\alpha)$, y luego $\sqrt[3]{2} = \alpha - \zeta_3 \in \mathbb{Q}(\alpha)$. Podemos concluir que

$$\mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}(\zeta_3 + \sqrt[3]{2}).$$

▲

14.1.16. Comentario. Los últimos dos ejemplos fueron escogidos para facilitar los cálculos. Aunque más adelante vamos a probar que para cualquier extensión finita $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ se tiene $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\gamma)$ para algún número γ, en general este no tiene por qué ser la suma de α y β.

14.1.17. Observación. *Sea L/K una extensión de cuerpos. Para $\alpha,\beta \in L$ se tiene $K(\alpha,\beta) = (K(\alpha))(\beta)$.*

Demostración. Tenemos $K \subset K(\alpha,\beta)$ y $\alpha \in K(\alpha,\beta)$, así que $K(\alpha) \subseteq K(\alpha,\beta)$ por la minimalidad de $K(\alpha)$. Además, $\beta \in K(\alpha,\beta)$ y por ende $(K(\alpha))(\beta) \subseteq K(\alpha,\beta)$.

De la misma manera, $K \subseteq (K(\alpha))(\beta)$ y $\alpha,\beta \in (K(\alpha))(\beta)$, así que $K(\alpha,\beta) \subseteq (K(\alpha))(\beta)$ por la minimalidad de $K(\alpha,\beta)$. ■

Por inducción se sigue que toda extensión finitamente generada $K(\alpha_1,\ldots,\alpha_n)$ se obtiene

como una sucesión de extensiones simples:

$$\begin{array}{rcl} K_n := K_{n-1}(\alpha_n) & = & K(\alpha_1, \ldots, \alpha_n) \\ & & | \\ K_{n-1} := K_{n-2}(\alpha_{n-1}) & = & K(\alpha_1, \ldots, \alpha_{n-1}) \\ & & | \\ & & \vdots \\ & & | \\ K_2 := K_1(\alpha_2) & = & K(\alpha_1, \alpha_2) \\ & & | \\ K_1 & := & K(\alpha_1) \\ & & | \\ & & K \end{array}$$

(En este caso también se dice que $K \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$ es una **torre de extensiones**.)

14.2 Extensiones algebraicas

14.2.1. Definición. Para una extension L/K se dice que un elemento $\alpha \in L$ es **algebraico** sobre K si $f(\alpha) = 0$ para algún polinomio no nulo $f \in K[X]$. Cuando α no es algebraico, se dice que es **trascendente** sobre K.

Se dice que L/K es una extensión algebraica si todo elemento de L es algebraico sobre K.

14.2.2. Ejemplo. Los números $\sqrt[n]{2} \in \mathbb{R}$ y $\zeta_n := e^{2\pi\sqrt{-1}/n} \in \mathbb{C}$ son algebraicos sobre $\mathbb{Q}$: son raíces de los polinomios $X^n - 2$ y $X^n - 1$ respectivamente. ▲

14.2.3. Ejemplo. Los números $e = 2{,}718281828\ldots$ y $\pi = 3{,}1415926\ldots$ son trascendentes sobre $\mathbb{Q}$; es un resultado clásico pero muy difícil. Es mucho más fácil (¡pero tampoco es trivial!) probar que $e, \pi \notin \mathbb{Q}$. ▲

14.2.4. Observación. *Para una cadena de extensiones $F \subseteq K \subseteq L$, si $\alpha \in L$ es algebraico sobre F, entonces es algebraico sobre K.*

Demostración. Si $f(\alpha) = 0$ para algún polinomio no nulo $f \in F[X]$, en particular $f \in K[X]$. ■

14.2.5. Observación. *Toda extensión finita es algebraica.*

Demostración. Si L/K es una extensión finita de grado n, entonces para cualquier $\alpha \in L$ los elementos $1, \alpha, \alpha^2, \ldots, \alpha^n$ son necesariamente linealmente independientes, así que existen algunos coeficientes $a_0, a_1, a_2, \ldots, a_n \in K$, no todos nulos, tales que

$$a_0 + a_1\,\alpha + a_2\,\alpha^2 + \cdots + a_n\,\alpha^n = 0.$$

Esto significa que α es una raíz de un polinomio no nulo

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in K[X].$$

■

Hay extensiones algebraicas infinitas, pero las veremos un poco más adelante. Voy a mencionar un par de extensiones que no son algebraicas.

14.2.6. Ejemplo. Para un cuerpo K la extensión $K(T)/K$, donde

$$K(T) := \left\{ \frac{f}{g} \;\middle|\; f, g \in k[T],\ g \neq 0 \right\}$$

es el cuerpo de las funciones racionales, no es algebraica. Por ejemplo, para cualesquiera $a_0, a_1, a_2, \ldots, a_n$ el elemento

$$a_0 + a_1 T + a_2 T^2 + \cdots + a_n T^n \in K(T)$$

es nulo si y solo si $a_0 = a_1 = a_2 = \cdots = a_n = 0$, lo que significa que T no es algebraico sobre K. ▲

14.2.7. Ejemplo. La extensión $\mathbb{R}/\mathbb{Q}$ no es algebraica. Esto puede ser probado sin construir ningún número trascendente específico. En efecto, todo elemento algebraico $\alpha \in \mathbb{R}$ es una raíz de algún polinomio no nulo $f \in \mathbb{Q}[X]$. El cuerpo $\mathbb{Q}$ es numerable, luego el anillo $\mathbb{Q}[X]$ es numerable, y el conjunto de las raíces de estos polinomios es también numerable (todo polinomio racional de grado n tiene a lo sumo n raíces). Sin embargo, $\mathbb{R}$ no es numerable. Se sigue que hay elementos de $\mathbb{R}$ que no son algebraicos sobre $\mathbb{Q}$. ▲

14.2.8. Teorema (El polinomio mínimo). *Sean L/K una extensión de cuerpos y $\alpha \in L$ un elemento.*

1) *α es algebraico sobre K si y solamente si el homomorfismo de evaluación*

$$\mathrm{ev}_\alpha \colon K[X] \to K(\alpha), \quad f \mapsto f(\alpha)$$

tiene núcleo no trivial.

2) *En este caso $\ker \mathrm{ev}_\alpha = (m_{\alpha,K})$, donde $m_{\alpha,K} \in K[X]$ es un polinomio mónico irreducible definido de modo único; a saber, $m_{\alpha,K}$ es el polinomio mónico de grado mínimo posible que tiene α como su raíz.*

3) *Hay un isomorfismo natural $K[X]/(m_{\alpha,K}) \cong K(\alpha)$.*

4) *Un polinomio $f \in K[X]$ tiene al elemento α como su raíz si y solamente si $m_{\alpha,K} \mid f$. Si f es irreducible, entonces $K[X]/(f) \cong K(\alpha)$.*

5) *Tenemos $[K(\alpha) : K] = \deg m_{\alpha,K}$.*

Demostración. Puesto que $K[X]$ es un dominio de ideales principales, se tiene necesariamente $\ker \mathrm{ev}_\alpha = (f)$ para algún polinomio $f \in K[X]$. Si $f = 0$, entonces α es trascendente. Si $f \neq 0$, entonces de nuestra prueba de que todo dominio euclidiano es un dominio de ideales principales (véase el capítulo anterior) se sigue que f se un polinomio de mínimo grado posible tal que $f(\alpha) = 0$.

Notamos que tal f es necesariamente irreducible: si $f = g\,h$ para algunos $g, h \in K[X]$ de grado menor que f, entonces $g(\alpha)\,h(\alpha) = f(\alpha) = 0$ implica que $g(\alpha) = 0$ o $h(\alpha) = 0$, pero f es un polinomio de mínimo grado posible que tiene a α como su raíz.

Ahora si f_1 y f_2 son dos polinomios que cumplen $(f_1) = (f_2) = \ker \mathrm{ev}_\alpha$, entonces $f_1 \sim f_2$, así que $f_2 = c\,f_1$ para alguna constante $c \in K^\times$. Esto significa que la condición de que f sea mónico lo define de modo único. Denotemos este polinomio mónico por $m_{\alpha,K}$.

Dado que $m_{\alpha,K}$ es irreducible, el ideal $(m_{\alpha,K})$ es primo. El anillo $K[X]$ es un dominio de ideales principales y todo ideal primo no nulo en $K[X]$ es maximal. Esto implica que $K[X]/(m_{\alpha,K})$ es un cuerpo. El primer teorema de isomorfía nos da entonces un isomorfismo de cuerpos

$$K[X]/(m_{\alpha,K}) \cong \mathrm{im}\,\mathrm{ev}_\alpha\,.$$

Calculemos $\mathrm{im}\,\mathrm{ev}_\alpha$. Primero,

$$\mathrm{im}\,\mathrm{ev}_\alpha = \{a_n\,\alpha^n + a_{n-1}\,\alpha^{n-1} + \cdots + a_1\,\alpha + a_0 \mid a_i \in K\} \subseteq K(\alpha).$$

Evaluando los polinomios constantes, se ve que $K \subseteq \mathrm{im}\,\mathrm{ev}_\alpha$. Además, $\alpha \in \mathrm{im}\,\mathrm{ev}_\alpha$. Se sigue que $\mathrm{im}\,\mathrm{ev}_\alpha = K(\alpha)$, puesto que $\mathrm{im}\,\mathrm{ev}_\alpha$ es un cuerpo que contiene a K y α e $\mathrm{im}\,\mathrm{ev}_\alpha$ está contenido en $K(\alpha)$. Entonces,

$$K[X]/(m_{\alpha,K}) \cong K(\alpha).$$

Ahora $f(\alpha) = 0$ si y solamente si $f \in \ker \mathrm{ev}_\alpha = (m_{\alpha,K})$, lo que significa que $m_{\alpha,K} \mid f$. Si f es también irreducible como $m_{\alpha,K}$, entonces $f \sim m_{\alpha,K}$; es decir $(f) = (m_{\alpha,K})$ y

$$K[X]/(f) = K[X]/(m_{\alpha,K}) \cong K(\alpha).$$

En fin, hemos visto en 14.1.7 que el cuerpo $K[X]/(m_{\alpha,K})$ tiene grado $\deg m_{\alpha,K}$ sobre K. ■

14.2.9. Definición. Para una extensión L/K y un elemento $\alpha \in L$ algebraico sobre K, el polinomio mónico $m_{\alpha,K} \in K[X]$ de mínimo grado posible tal que $m_{\alpha,K}$ se llama el **polinomio mínimo** de α sobre K. Como acabamos de notar, $m_{\alpha,K}$ es necesariamente irreducible. El número

$$\deg_K(\alpha) := [K(\alpha) : K] = \deg m_{\alpha,K}$$

se llama el **grado** de α sobre K.

14.2.10. Observación. *Si L/K es una extensión finita, entonces para todo $\alpha \in L$ el grado $\deg_K(\alpha)$ divide al grado $[L : K]$.*

Demostración. Tenemos $[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K]$. ■

14.2.11. Observación. *Sea $F \subseteq K \subseteq L$ una cadena de extensiones y $\alpha \in L$ un elemento algebraico sobre F. Entonces, en el anillo de polinomios $K[X]$ se cumple*

$$m_{\alpha,K} \mid m_{\alpha,F}.$$

En particular,

$$[K(\alpha) : K] = \deg_K(\alpha) \leq \deg_F(\alpha) = [F(\alpha) : F].$$

Demostración. Tenemos $m_{\alpha,F}(\alpha) = 0$. Puesto que $m_{\alpha,F} \in F[X] \subseteq K[X]$, se cumple $m_{\alpha,K} \mid m_{\alpha,F}$. ■

Antes de volver a los resultados generales sobre los elementos algebraicos, veamos algunos ejemplos de polinomios mínimos.

14.2.12. Ejemplo (Trivial). Para una extensión L/K, si $\alpha \in K$, entonces $m_{\alpha,K} = X - \alpha$. ▲

14.2.13. Ejemplo. Para $\sqrt{-1} \in \mathbb{C}$ el polinomio mínimo sobre $\mathbb{Q}$ es $m_{\sqrt{-1},\mathbb{Q}} = X^2 + 1$. Tenemos $\mathbb{Q}(\sqrt{-1}) \cong \mathbb{Q}[X]/(X^2+1)$. De la misma manera, $m_{\sqrt{-1},\mathbb{R}} = X^2 + 1$ y $\mathbb{C} = \mathbb{R}(\sqrt{-1}) \cong \mathbb{R}[X]/(X^2+1)$. ▲

14.2.14. Ejemplo. Sea $d \neq 1$ un entero libre de cuadrados. Para $\sqrt{d} \in \mathbb{C}$ el polinomio mínimo sobre $\mathbb{Q}$ es $X^2 - d$. En efecto, este polinomio tiene a d como su raíz y su grado es igual a $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$. Tenemos $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[X]/(X^2 - d)$. ▲

14.2.15. Ejemplo. Consideremos el número

$$\zeta_3 := e^{2\pi\sqrt{-1}/3} = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}. \tag{14.1}$$

Aunque tenemos $\zeta_3^3 - 1 = 0$, el polinomio $X^3 - 1$ *no es* el polinomio mínimo de ζ_3 sobre $\mathbb{Q}$: se tiene $X^3 - 1 = (X-1)(X^2+X+1)$, donde $f = X^2 + X + 1$ es un polinomio irreducible (por ejemplo, porque $\overline{f} \in \mathbb{F}_2[X]$ es irreducible o porque $f(X+1) = X^3 + 3X + 3$ es irreducible por el criterio de Eisenstein) y $f(\zeta_3) = 0$. Entonces,

$$m_{\zeta_3,\mathbb{Q}} = X^2 + X + 1.$$

Notamos que

$$\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$$

—de la ecuación (14.1) se ve que $\zeta_3 \in \mathbb{Q}(\sqrt{-3})$ y $\sqrt{-3} \in \mathbb{Q}(\zeta_3)$. ▲

Para una generalización de este ejemplo, véase §14.4.

14.2.16. Ejemplo. El polinomio $X^3 - 2$ es irreducible en $\mathbb{Q}[X]$ y tiene tres raíces en $\mathbb{C}$:

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \sqrt[3]{2}\,\frac{-1+\sqrt{-3}}{2} = \sqrt[3]{2}\,\zeta_3, \quad \alpha_3 = \sqrt[3]{2}\,\frac{-1-\sqrt{-3}}{2} = \sqrt[3]{2}\,\overline{\zeta_3} = \sqrt[3]{2}\,\zeta_3^2;$$

donde α_1 es real y α_2 y α_3 son números complejos conjugados. El teorema 14.2.8 nos dice que hay isomorfismos de cuerpos

$$\mathbb{Q}[X]/(X^3 - 2) \cong \mathbb{Q}(\alpha_1) \cong \mathbb{Q}(\alpha_2) \cong \mathbb{Q}(\alpha_3).$$

Sin embargo, $\mathbb{Q}(\alpha_1) \subset \mathbb{R}$, mientras que $\mathbb{Q}(\alpha_2), \mathbb{Q}(\alpha_3) \not\subset \mathbb{R}$, así que hay cierta diferencia entre $\mathbb{Q}(\alpha_1)$ y $\mathbb{Q}(\alpha_2), \mathbb{Q}(\alpha_3)$ que no puede ser expresada en términos de isomorfismos de cuerpos abstractos. ▲

14.2.17. Ejemplo. Volvamos al ejemplo 14.1.14. Para el cuerpo

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

hemos calculado las potencias de $\alpha := \sqrt{2}+\sqrt{3}$:

$$\alpha^2 = 5+2\sqrt{6}, \quad \alpha^3 = 11\sqrt{2}+9\sqrt{3}, \quad \alpha^4 = 49+20\sqrt{6}.$$

Se ve que

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

así que α es una raíz del polinomio $f = X^4 - 10X^2 + 1$. El polinomio mínimo $m_{\alpha,\mathbb{Q}}$ necesariamente divide a f, lo que implica que

$$[\mathbb{Q}(\alpha):\mathbb{Q}] \leq 4.$$

Luego, tenemos

$$[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}],$$

donde $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, así que $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2$ o 4.

Ahora si $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2$, entonces $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})] = 1$ y $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2})$. Sin embargo, esto es imposible: $\sqrt{3} \in \mathbb{Q}(\alpha)$, pero $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. En efecto, si $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, entonces $\sqrt{3} = a + b\sqrt{2}$ para algunos $a, b \in \mathbb{Q}$, pero en este caso $3 = a^2 + 2ab\sqrt{2} + 2b$, lo que demostraría que $\sqrt{2} \in \mathbb{Q}$.

Podemos concluir que $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$, $m_{\alpha,\mathbb{Q}} = f$ y

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) \cong \mathbb{Q}[X]/(X^4 - 10X^2 + 1).$$

Notamos que sin estas consideraciones, no es obvio por qué $f = X^4 - 10X^2 + 1$ es un polinomio irreducible en $\mathbb{Q}[X]$. ▲

* * *

He aquí una caracterización de los elementos algebraicos.

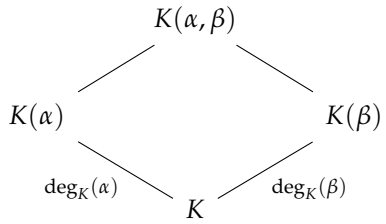
14.2.18. Observación. *Para una extensión L/K un elemento $\alpha \in L$ es algebraico sobre K si y solo si* $\deg_K(\alpha) := [K(\alpha):K] < \infty$.

Demostración. Ya hemos visto que si α es algebraico, entonces existe un polinomio mínimo y $[K(\alpha):K] = \deg m_{\alpha,K} < \infty$. Viceversa, si $[K(\alpha):K] < \infty$, entonces la extensión $K(\alpha)/K$ es algebraica, como notamos en 14.2.5. ■

14.2.19. Observación. *Sea L/K una extensión de cuerpos y $\alpha, \beta \in L$ elementos de grado finito sobre K. Entonces,*

$$[K(\alpha,\beta):K] \leq \deg_K(\alpha)\cdot\deg_K(\beta).$$

Demostración. Consideremos las extensiones



La desigualdad de 14.2.11 aplicada a las extensiones $K \subseteq K(\alpha) \subseteq K(\alpha,\beta)$ y $\beta \in K(\alpha,\beta)$ nos da

$$[(K(\alpha))(\beta) : K(\alpha)] \leq [K(\beta) : K],$$

de donde

$$[K(\alpha,\beta) : K] = [(K(\alpha))(\beta) : K(\alpha)] \cdot [K(\alpha) : K] \leq [K(\beta) : K] \cdot [K(\alpha) : K].$$

■

Por inducción se sigue que en general,

$$[K(\alpha_1,\ldots,\alpha_n) : K] \leq \deg_K(\alpha_1) \cdots \deg_K(\alpha_n).$$

14.2.20. Comentario. Puede suceder que el grado $[K(\alpha,\beta) : K]$ es *estrictamente* menor que el producto $\deg_K(\alpha) \cdot \deg_K(\beta)$. Para un contraejemplo trivial, considere $\alpha = \beta$.

14.2.21. Ejemplo. Volvamos al ejemplo 14.1.15. Hemos visto que

$$\mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}(\zeta_3 + \sqrt[3]{2}).$$

Tenemos

$$[\mathbb{Q}(\zeta_3 + \sqrt[3]{2}) : \mathbb{Q}] \leq \deg_{\mathbb{Q}}(\zeta_3) \cdot \deg_{\mathbb{Q}}(\sqrt[3]{2}) = 2 \cdot 3 = 6.$$

Pero el grado $[\mathbb{Q}(\zeta_3 + \sqrt[3]{2}) : \mathbb{Q}]$ tiene que ser divisible por 2 y 3, así que es exactamente 6. ▲

Tenemos la siguiente caracterización de extensiones finitas.

14.2.22. Proposición. *Una extensión L/K es finita si y solo si $L = K(\alpha_1,\ldots,\alpha_n)$, donde $\alpha_1,\ldots,\alpha_n \in K$ es un número finito de elementos algebraicos sobre K.*

Demostración. Si L/K es una extensión finita de grado n, sea $\alpha_1,\ldots,\alpha_n$ una base de L sobre K. Tenemos $\deg_K(\alpha_i) \leq n$, así que $\alpha_1,\ldots,\alpha_n$ son algebraicos. Está claro que $L = K(\alpha_1,\ldots,\alpha_n)$.

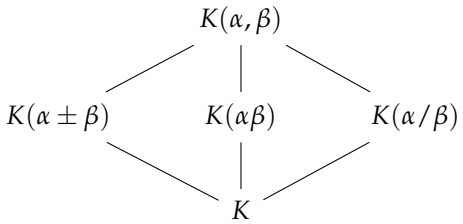
Viceversa, si $L = K(\alpha_1,\ldots,\alpha_n)$ donde $\alpha_1,\ldots,\alpha_n$ son algebraicos sobre K, entonces

$$[L : K] \leq \deg_K(\alpha_1) \cdots \deg_K(\alpha_n),$$

así que la extensión es finita. ■

14.2.23. Proposición. *Para una extensión de cuerpos L/K sean $\alpha, \beta \in L$ elementos algebraicos sobre K. Entonces, $\alpha \pm \beta$, $\alpha\beta$, α/β (donde $\beta \neq 0$) son también algebraicos sobre K.*

Demostración. Si α y β son algebraicos sobre K, entonces la extensión $K(\alpha, \beta)/K$ es finita. Luego, tenemos



así que $K(\alpha \pm \beta)$, $K(\alpha\beta)$, $K(\alpha/\beta)$ son también extensiones finitas de K. Toda extensión finita es algebraica, lo que implica en particular que los números $\alpha \pm \beta$, $\alpha\beta$, α/β son algebraicos sobre K. ■

14.2.24. Comentario. Si α y β son algebraicos, aunque la prueba de arriba nos dice que $\alpha \pm \beta$, $\alpha\beta$, α/β son también algebraicos, esta no revela cómo obtener los polinomios mínimos de $\alpha \pm \beta$, $\alpha\beta$, α/β a partir de los polinomios mínimos $m_{\alpha,K}$ y $m_{\beta,K}$. Veremos esto más adelante.

14.2.25. Corolario. *Para una extensión de cuerpos L/K los elementos de L que son algebraicos sobre K forman un subcuerpo de L.*

Terminemos por un ejemplo de extensiones algebraicas infinitas.

14.2.26. Ejemplo. Según 14.2.25, todos los números complejos que son algebraicos sobre $\mathbb{Q}$ forman un cuerpo. Denotémoslo por $\overline{\mathbb{Q}}$. Notamos que $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ y

$$\deg_{\mathbb{Q}}(\sqrt[n]{2}) = n.$$

Esto implica que la extensión $\overline{\mathbb{Q}}/\mathbb{Q}$ es infinita. En efecto, si $[L : K] < \infty$, entonces $\deg_K(\alpha) \mid [L : K]$ para todo $\alpha \in L$. En nuestro caso, la existencia de elementos $\alpha \in \overline{\mathbb{Q}}$ de grado arbitrariamente grande nos permite concluir que $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Puesto que $\sqrt[n]{2} \in \mathbb{R}$, esto demuestra que el cuerpo $\overline{\mathbb{Q}} \cap \mathbb{R}$ es una extensión algebraica infinita de $\mathbb{Q}$.

De hecho, lo que probamos es que la extensión

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \sqrt[5]{2}, \ldots)/\mathbb{Q}$$

es infinita. Tenemos un cuerpo generado por elementos algebraicos sobre $\mathbb{Q}$, pero el número de estos generadores es infinito. ▲

14.3 Extensiones de grado 2

Sea K un cuerpo y sea L/K una extensión de grado 2. Para un elemento $\alpha \in L$ tal que $\alpha \notin K$ tenemos necesariamente $1 < [K(\alpha) : K] \leq [L : K] = 2$, así que $L = K(\alpha)$ y el polinomio mínimo de α es de grado 2:

$$m_{\alpha,K} = X^2 + b\,X - c$$

para algunos $b, c \in K$. Hay dos casos diferentes.

1) Si $b = 0$, entonces se trata de la extensión
$$K(\alpha) = K(\sqrt{c}) \cong K[X]/(X^2 - c).$$

2) Si $b \neq 0$, podemos hacer un cambio de variables
$$\begin{aligned} K[Y] &\xrightarrow{\cong} K[X], \\ Y &\mapsto X/b, \\ Y^2 + Y - c/b^2 &\mapsto \frac{1}{b^2}\left(X^2 + b\,X - c\right) \end{aligned}$$
que nos da un isomorfismo
$$K[X]/(X^2 + b\,X - c) \cong K[Y]/(Y^2 + Y - c') \cong K(\beta)$$
donde $c' := c/b^2 \in K$ y β denota la imagen de Y en el cociente. Notamos que en este caso $\beta^2 \notin K$, puesto que $\beta = c' - \beta^2 \notin K$.

Cuando $\operatorname{char} K \neq 2$, el caso 2) siempre se reduce al caso 1): se puede hacer un cambio de variables ("completar el cuadrado")
$$\begin{aligned} K[Y] &\xrightarrow{\cong} K[X], \\ Y &\mapsto X + \frac{b}{2}, \\ Y^2 - c - \frac{b^2}{4} &\mapsto \left(X + \frac{b}{2}\right)^2 - c - \frac{b^2}{4} = X^2 + b\,X - c, \end{aligned}$$
así que
$$K[Y]/(Y^2 - c') \cong K[X]/(X^2 + b\,X - c),$$
donde $c' := c + b^2/4 \in K$.

Cuando $\operatorname{char} K = 2$, los casos 1) y 2) son diferentes: en el caso 1) todo cuadrado de $x + y\sqrt{-c} \in K(\sqrt{c})$ pertenece a K:
$$(x + y\sqrt{c})^2 = x^2 + cy^2 \in K$$
(¡usando que $\operatorname{char} K = 2$!), mientras que en el caso 2), tenemos $\beta^2 \notin K$.

Podemos concluir que si $\operatorname{char} K \neq 2$, entonces toda extensión de grado 2 es de la forma $K(\sqrt{d})/K$ para algún $d \in K$ que no es un cuadrado en K.

Si $\operatorname{char} K = 2$, puede haber extensiones distintas de la forma $K[X]/(Y^2 + Y + c)$, donde $c \in K$ e $Y^2 + Y + c \in K[Y]$ es algún polinomio irreducible. Por ejemplo, si $K = \mathbb{F}_2$, el polinomio $Y^2 + Y + 1$ es irreducible en $\mathbb{F}_2[Y]$. De hecho, $\mathbb{F}_2$ no puede tener extensiones de la forma $\mathbb{F}_2(\sqrt{c})$: todos los elementos de $\mathbb{F}_2$ son cuadrados.

En general, si $K = \mathbb{F}_{2^n}$ es un cuerpo finito de 2^n elementos[*], entonces el homomorfismo
$$\mathbb{F}_{2^n}^{\times} \to \mathbb{F}_{2^n}^{\times}, \quad x \mapsto x^2$$
es sobreyecivo. Esto se sigue del hecho de que $\mathbb{F}_{2^n}^{\times}$ sea un grupo cíclico de orden impar $2^n - 1$. Por esto *todos* los elementos de $\mathbb{F}_{2^n}$ son cuadrados.

[*]Véase el siguiente capítulo.

14.4 Cuerpos ciclotómicos

Hemos probado en el capítulo anterior que los polinomios ciclotómicos Φ_{p^k} son irreducibles en $\mathbb{Q}[X]$ usando el criterio de Eisenstein. Para probar el caso general de Φ_n para cualquier n, podemos usar las factorizaciones de Φ_n en $\mathbb{F}_p[X]$. De hecho, sería más fácil considerar las factorizaciones de

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Por ejemplo, para $n = p$ se tiene

$$X^p - 1 = (X-1)^p.$$

Si $n = p-1$, entonces el pequeño teorema de Fermat nos dice que cualquier elemento $x \in \mathbb{F}_p^\times$ satisface $x^{p-1} = 1$, así que se tiene

$$X^{p-1} - 1 = (X-1)\,(X-2)\cdots(X-(p-1)).$$

Normalmente los polinomios $X^n - 1$ y en particular Φ_n se vuelven *reducibles* en $\mathbb{F}_p[X]$.

Primero, necesitamos la siguiente construcción.

14.4.1. Definición. Sea k un cuerpo. Para un polinomio

$$f = a_n\,X^n + a_{n-1}\,X^{n-1} + \cdots + a_1\,X + a_2\,X^2 + a_0 \in k[X]$$

su **derivada** viene dada por

$$f' = n\,a_n\,X^{n-1} + (n-1)\,a_{n-1}\,X^{n-2} + \cdots + a_2\,X + a_1.$$

Dejo al lector como un ejercicio comprobar que esta definición cumple las propiedades habituales: para cualesquiera $f, g \in k[X]$ se cumple

$$(f+g)' = f' + g', \quad (fg)' = f'g + fg'.$$

14.4.2. Lema. *En la factorización de $X^n - 1$ en $\mathbb{F}_p[X]$ hay factores repetidos si y solamente si $p \mid n$.*

Demostración. Primero notamos que si $p \mid n$, entonces $n = pm$ para algún m y luego en $\mathbb{F}_p[X]$ se tiene

$$(X^n - 1) = ((X^m)^p - 1^p) = (X^m - 1)^p.$$

Ahora supongamos que en $\mathbb{F}_p[X]$

$$X^n - 1 = f^2\,g$$

para algunos polinomios no constantes $f, g \in \mathbb{F}_p[X]$. Luego, tomando las derivadas se obtiene

$$n\,X^{n-1} = 2\,f\,f'\,g + f^2\,g' = f\,(2\,f'\,g + f\,g').$$

Entonces, $f \mid (X^n - 1)$ y $f \mid n\,X^{n-1}$. Si $p \nmid n$, esto es imposible: en este caso

$$1 = -1 \cdot (X^n - 1) + \frac{1}{n}\,X \cdot (n\,X^{n-1}),$$

así que

$$\mathrm{mcd}(X^n - 1, n\,X^{n-1}) = 1.$$

■

La siguiente página contiene algunas factorizaciones de $X^n - 1$ en $\mathbb{F}_p[X]$. El lector debe fijarse en los factores repetidos.

Factorizaciones en $\mathbb{Z}[X]$

$$
\begin{aligned}
X^2-1 &= (X-1)(X+1),\\
X^3-1 &= (X-1)(X^2+X+1),\\
X^4-1 &= (X-1)(X+1)(X^2+1),\\
X^5-1 &= (X-1)(X^4+X^3+X^3+X+1).\\
X^6-1 &= (X-1)(X+1)(X^2+X+1)(X^2-X+1),\\
X^7-1 &= (X-1)(X^6+X^5+X^4+X^3+X^2+X+1),\\
X^8-1 &= (X-1)(X+1)(X^2+1)(X^4+1),\\
X^9-1 &= (X-1)(X^2+X+1)(X^6+X^3+1),\\
X^{10}-1 &= (X-1)(X+1)(X^4+X^3+X^2+X+1)(X^4-X^3+X^2-X+1).
\end{aligned}
$$

Factorizaciones en $\mathbb{F}_p[X]$

$\underline{X^2-1}$

$p=2$:	$(X+1)^2$
$p=3$:	$(X-1)(X+1)$
$p=5$:	$(X-1)(X+1)$
$p=7$:	$(X-1)(X+1)$
$p=11$:	$(X-1)(X+1)$

$\underline{X^3-1}$

$p=2$:	$(X+1)(X^2+X+1)$
$p=3$:	$(X-1)^3$
$p=5$:	$(X-1)(X^2+X+1)$
$p=7$:	$(X-1)(X-2)(X-4)$
$p=11$:	$(X-1)(X^2+X+1)$

$\underline{X^4-1}$

$p=2$:	$(X+1)^4$
$p=3$:	$(X-1)(X+1)(X^2+1)$
$p=5$:	$(X-1)(X-2)(X-3)(X-4)$
$p=7$:	$(X-1)(X+1)(X^2+1)$
$p=11$:	$(X-1)(X+1)(X^2+1)$

$\underline{X^5-1}$

$p=2$:	$(X+1)(X^4+X^3+X^2+X+1)$
$p=3$:	$(X-1)(X^4+X^3+X^2+X+1)$
$p=5$:	$(X-1)^5$
$p=7$:	$(X-1)(X^4+X^3+X^2+X+1)$
$p=11$:	$(X-1)(X-3)(X-4)(X-5)(X-9)$

$\underline{X^6-1}$

$p=2$:	$(X+1)^2(X^2+X+1)^2$
$p=3$:	$(X+1)^3(X+2)^3$
$p=5$:	$(X-1)(X+1)(X^2+X+1)(X^2-X+1)$
$p=7$:	$(X-1)(X-2)(X-3)(X-4)(X-5)(X-6)$
$p=11$:	$(X-1)(X+1)(X^2+X+1)(X^2-X+1)$

$\underline{X^7-1}$

$p=2$:	$(X+1)(X^3+X+1)(X^3+X^2+1)$
$p=3$:	$(X-1)(X^6+X^5+X^4+X^3+X^2+X+1)$
$p=5$:	$X^6+X^5+X^4+X^3+X^2+X+1$
$p=7$:	$(X-1)^7$
$p=11$:	$(X-1)(X^3+5X^2+4X-1)(X^3+7X^2+6X-1)$

$\underline{X^8-1}$

$p=2$:	$(X+1)^8$
$p=3$:	$(X-1)(X+1)(X^2+1)(X^2+X-1)(X^2-X-1)$
$p=5$:	$(X-2)(X-3)(X-4)(X^2-2)(X^2-3)$
$p=7$:	$(X-1)(X+1)(X^2+1)(X^2+4X+1)(X^2-4X+1)$
$p=11$:	$(X-1)(X+1)(X^2+1)(X^2+3X-1)(X^2-3X-1)$

$\underline{X^9-1}$

$p=2$:	$(X+1)(X^2+X+1)(X^6+X^3+1)$
$p=3$:	$(X-1)^9$
$p=5$:	$(X-1)(X^2+X+1)(X^6+X^3+1)$
$p=7$:	$(X-1)(X-2)(X-1)(X^3-2)(X^3-4)$
$p=11$:	$(X-1)(X^2+X+1)(X^6+X^3+1)$

$\underline{X^{10}-1}$

$p=2$:	$(X+1)^2(X^4+X^3+X^2+X+1)^2$
$p=3$:	$(X-1)(X+1)(X^4+X^3+X^2+X+1)(X^4-X^3+X^2-X+1)$
$p=5$:	$(X-1)^5(X+1)^5$
$p=7$:	$(X-1)(X+1)(X^4+X^3+X^2+X+1)(X^4-X^3+X^2-X+1)$
$p=11$:	$(X-1)(X-2)(X-3)(X-4)(X-5)(X-6)(X-7)(X-8)(X-9)(X-10)$

14.4.3. Lema. *Para $g \in \mathbb{F}_p[X]$ se cumple $g(X^p) = g^p$.*

Demostración. Usando la fórmula del binomio en característica p y el pequeño teorema de Fermat $a^p = a$ para todo $a \in \mathbb{F}_p$, tenemos

$$(a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0)^p = a_n (X^p)^n + a_{n-1} (X^p)^{n-1} + \cdots + a_1 X^p + a_0.$$

■

14.4.4. Teorema (Gauss). *El polinomio ciclotómico Φ_n es irreducible en $\mathbb{Z}[X]$ para cualquier n.*

Demostración. Escribamos

$$\Phi_n = fg$$

para algunos polinomios $f, g \in \mathbb{Z}[X]$ (necesariamente mónicos), donde f es irreducible. Sea ζ una raíz n-ésima primitiva. Tenemos entonces

$$\Phi_n(\zeta) = f(\zeta)\, g(\zeta) = 0.$$

Esto implica que $f(\zeta) = 0$ o $g(\zeta) = 0$. Puesto que f no es constante, algunas de las raíces n-ésimas primitivas deben ser raíces de f, y nuestro objetivo es probar que todas lo son.

Asumamos entonces que ζ es una raíz de f. Siendo un polinomio mónico irreducible, f debe ser el polinomio mínimo de ζ sobre $\mathbb{Q}$. Sea p un número primo tal que $p \nmid n$. Entonces, ζ^p es también una raíz n-ésima primitiva y

$$\Phi_n(\zeta^p) = f(\zeta^p)\, g(\zeta^p) = 0.$$

Asumamos que $g(\zeta^p) = 0$. Entonces, por las propiedades del polinomio mínimo, el polinomio $g(X^p)$ tiene que ser divisible por f en $\mathbb{Z}[X]$:

$$g(X^p) = f\, h \quad \text{para algún } h \in \mathbb{Z}[X].$$

Luego, reduciendo módulo p y aplicando 14.4.3, se obtiene

$$\overline{g}^p = \overline{f}\,\overline{h} \quad \text{en } \mathbb{F}_p[X].$$

Pero esto significa que $\overline{f}$ y $\overline{h}$ tienen un factor común en su factorización en $\mathbb{F}_p[X]$, así que $\overline{\Phi_n} = \overline{f}\,\overline{g}$ tiene un factor repetido en su factorización. Esto implica que la factorización de

$$X^n - 1 = \prod_{d|n} \overline{\Phi_n}$$

tiene un factor repetido, pero como vimos en 14.4.2, esto es imposible cuando $p \nmid n$. Esta contradicción nos permite concluir que $f(\zeta^p) = 0$.

Entonces, para cualquier primo p tal que $p \nmid n$ se tiene $f(\zeta^p) = 0$. Ahora todas las raíces n-ésimas primitivas son de la forma ζ^k donde $\mathrm{mcd}(n, k) = 1$. Podemos factorizar entonces $k = p_1 \cdots p_s$ donde p_i son primos (no necesariamente diferentes) tales que $p_i \nmid n$, y luego

$$\zeta^k = (((\zeta^{p_1})^{p_2})^{\cdots})^{p_s}.$$

El argumento de arriba nos dice que $f(\zeta^{p_1}) = 0$. Luego, el mismo argumento aplicado a ζ^{p_1} demuestra que $f((\zeta^{p_1})^{p_2}) = 0$, etcétera.

Entonces, todas las raíces n-ésimas primitivas son raíces de f y por ende $g = 1$. ■

14.4.5. Definición. Para $n = 1, 2, 3, 4, \ldots$ el **n-ésimo cuerpo ciclotómico** es el cuerpo $\mathbb{Q}(\zeta_n)$, donde

$$\zeta_n := e^{2\pi\sqrt{-1}/n}.$$

Los cuerpos ciclotómicos tienen mucha importancia en la teoría de números. De los resultados anteriores siguen las siguientes propiedades básicas.

1) Dado que el polinomio ciclotómico $\Phi_n \in \mathbb{Z}[X]$ es un polinomio mónico irreducible y $\Phi_n(\zeta_n) = 0$, tenemos
$$m_{\zeta_n,\mathbb{Q}} = \Phi_n.$$

2) Hay un isomorfismo
$$\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[X]/(\Phi_n).$$

3) El grado de la extensión ciclotómica $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ viene dado por la función ϕ de Euler:
$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \phi(n).$$

14.4.6. Observación. *Si $m \mid n$, entonces $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$.*

Demostración. Si $m \mid n$, entonces $\zeta_m = \zeta_n^{n/m} \in \mathbb{Q}(\zeta_n)$. ■

Una pregunta natural es si los cuerpos $\mathbb{Q}(\zeta_n)$ son diferentes para diferente n. Trivialmente,

$$\mathbb{Q}(\zeta_2) = \mathbb{Q}(\zeta_1) = \mathbb{Q},$$

pero un momento de reflexión nos da otros ejemplos más interesantes: se tiene

$$\zeta_6 = \zeta_6^7 = \zeta_6^3\,\zeta_6^4 = \zeta_2\,\zeta_3^2 = -\zeta_3^2 \in \mathbb{Q}(\zeta_3),$$

así que $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$. En general, tenemos el siguiente resultado.

14.4.7. Observación. *Si m es un número impar, entonces $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$.*

Demostración. Tenemos la inclusión obvia $\zeta_m = \zeta_{2m}^2 \in \mathbb{Q}(\zeta_{2m})$, y por otro lado, escribiendo $m = 2k + 1$,

$$\zeta_{2m} = \zeta_{2m}^{(2k+1)-2k} = \zeta_{2m}^m\,(\zeta_{2m}^2)^{-k} = \zeta_2\,\zeta_m^{-k} = -\zeta_m^{-k} \in \mathbb{Q}(\zeta_m).$$

■

14.4.8. Ejemplo. Tenemos

$$\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3), \quad \mathbb{Q}(\zeta_{10}) = \mathbb{Q}(\zeta_5), \quad \mathbb{Q}(\zeta_{14}) = \mathbb{Q}(\zeta_7), \quad \mathbb{Q}(\zeta_{18}) = \mathbb{Q}(\zeta_9), \quad \ldots$$

▲

14.4.9. Comentario. Esto se refleja de la siguiente manera en los polinomios ciclotómicos: para $m > 1$ impar

$$\Phi_{2m}(X) = \Phi_m(-X),$$

mientras que para $m = 1$, tenemos $\Phi_1 = X - 1$ y $\Phi_2 = X + 1$, así que

$$\Phi_2(X) = -\Phi_1(-X).$$

(Haga el ejercicio 14.8.) Por ejemplo,

$$\begin{aligned} \Phi_3 &= X^2 + X + 1, & \Phi_6 &= X^2 - X + 1, \\ \Phi_5 &= X^4 + X^3 + X^2 + X + 1, & \Phi_{10} &= X^4 - X^3 + X^2 - X + 1, \\ \Phi_7 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, & \Phi_{14} &= X^6 - X^5 + X^4 - X^3 + X^2 - X + 1. \end{aligned}$$

La propiedad 14.4.7 se cumple por la razón banal de que $\zeta_2 = -1 \in \mathbb{Q}$. Resulta que en otras situaciones los cuerpos ciclotómicos no coinciden. Para probarlo, podemos investigar cuáles raíces de la unidad están en $\mathbb{Q}(\zeta_m)$.

14.4.10. Lema. *Si m es par y $m \mid r$, entonces $\phi(r) \leq \phi(m)$ implica $r = m$.*

Demostración. Primero, notamos que para cualesquiera $a, m \geq 1$ se cumple

$$\phi(am) = \frac{\phi(a)\,\phi(m)\,\operatorname{mcd}(a,m)}{\phi(\operatorname{mcd}(a,m))}$$

—esto se sigue de las fórmulas

$$\begin{aligned} \phi(a) &= a \prod_{p \mid a} \left(1 - \frac{1}{p}\right), \\ \phi(m) &= m \prod_{p \mid m} \left(1 - \frac{1}{p}\right), \\ \phi(am) &= am \prod_{p \mid am} \left(1 - \frac{1}{p}\right), \\ \phi(\operatorname{mcd}(a,m)) &= \operatorname{mcd}(a,m) \prod_{p \mid a, p \mid m} \left(1 - \frac{1}{p}\right). \end{aligned}$$

(Notamos que cuando a y m son coprimos, se tiene $\operatorname{mcd}(a,m) = \phi(\operatorname{mcd}(a,m)) = 1$ y se recupera la fórmula conocida.) Ahora para m par y $m \mid r$, asumamos que $m < r$, así que $r = am$ para algún $a > 1$. Tenemos

$$\phi(r) = \phi(am) = \frac{\phi(a)\,\phi(m)\,\operatorname{mcd}(a,m)}{\phi(\operatorname{mcd}(a,m))}.$$

Si $a = 2$, entonces $\phi(a) = \phi(2) = 1$ y $\operatorname{mcd}(a,m) = 2$. Luego,

$$\frac{\phi(a)\,\phi(m)\,\operatorname{mcd}(a,m)}{\phi(\operatorname{mcd}(a,m))} = 2\,\phi(m) > \phi(m).$$

Si $a > 2$, entonces $\phi(a) \geq 2$, y luego

$$\frac{\phi(a)\,\phi(m)\,\operatorname{mcd}(a,m)}{\phi(\operatorname{mcd}(a,m))} \geq \phi(a)\,\phi(m) > \phi(m).$$

En ambos casos, $m < r$ implica $\phi(m) < \phi(r)$. ■

14.4.11. Proposición. *Las raíces de la unidad en el cuerpo $\mathbb{Q}(\zeta_m)$ son precisamente*

$$\mu_\infty(\mathbb{C}) \cap \mathbb{Q}(\zeta_m)^\times = \begin{cases} \mu_m(\mathbb{C}), & \text{si } m \text{ es par,} \\ \mu_{2m}(\mathbb{C}), & \text{si } m \text{ es impar.} \end{cases}.$$

Demostración [Mar1977]. Si $m = 2k+1$ es un número impar, entonces ya notamos en 14.4.7 que $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$. Por esto sería suficiente considerar el caso cuando m es un número par.

Tenemos $\zeta_m \in \mathbb{Q}(\zeta_m)$, y por ende todas las raíces m-ésimas de la unidad, siendo potencias de ζ_m, están en $\mathbb{Q}(\zeta_m)$:

$$\mu_m(\mathbb{C}) \subseteq \mu_\infty(\mathbb{C}) \cap \mathbb{Q}(\zeta_m)^\times.$$

Hay que ver que en $\mathbb{Q}(\zeta_m)$ no hay raíces de la unidad de orden $k \nmid m$. Bastaría considerar las raíces k-ésimas primitivas.

Supongamos que $\zeta_k^\ell \in \mathbb{Q}(\zeta_m)$ donde ζ_k^ℓ es una raíz k-ésima primitiva; es decir, $\operatorname{mcd}(k,\ell) = 1$. Pongamos

$$r := \operatorname{mcm}(k,m) = \frac{km}{d}, \quad d = \operatorname{mcd}(k,m).$$

Luego,

$$\operatorname{mcd}(k,\ell m) = \operatorname{mcd}(k,m) = d,$$

lo que significa que existen $a, b \in \mathbb{Z}$ tales que

$$d = ak + b\ell m.$$

Ahora,

$$\zeta_r = \zeta_{km}^d = \zeta_{km}^{ak+b\ell m} = \zeta_{km}^{ak}\,\zeta_{km}^{b\ell m} = \zeta_m^a\,(\zeta_k^\ell)^b \in \mathbb{Q}(\zeta_m)$$

y

$$\phi(r) \leq \phi(m), \quad m \text{ es par}, \quad m \mid r,$$

así que el lema 14.4.10 nos permite concluir que

$$r = \operatorname{mcd}(k,m) = m,$$

lo que significa que $k \mid m$. ■

14.4.12. Corolario. *Si $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$ para $m < n$, entonces m es impar y $n = 2m$.*

Demostración. Si m es par, entonces las raíces de la unidad en $\mathbb{Q}(\zeta_m)$ son de orden m, mientras que las raíces de la unidad en $\mathbb{Q}(\zeta_n)$ son de orden n o $2n$, dependiendo de la paridad de n. Pero en ambos casos la hipótesis $m < n$ nos lleva a una contradicción.

Entonces, m es impar y las raíces de la unidad en $\mathbb{Q}(\zeta_m)$ son de orden m. La única posibilidad es $n = 2m$. ■

14.4.13. Comentario. Para enumerar los cuerpos ciclotómicos sin redundancias, a veces se consideran $\mathbb{Q}(\zeta_n)$ tales que $n \not\equiv 2 \pmod 4$.

14.5 Perspectiva: números trascendentes

Hasta el momento, hemos estudiado las propiedades de extensiones algebraicas, con énfasis en los ejemplos de números algebraicos sobre $\mathbb{Q}$. Es extremadamente difícil probar que algún número específico es trascendente sobre $\mathbb{Q}$. Voy a mencionar solo algunos resultados clásicos y conjeturas.

1) El primer ejemplo explícito (aunque artificial) de un número trascendente fue construido por Liouville en 1844. Se dice que $\alpha \in \mathbb{R}$ es un **número de Liouville** si para todo entero positivo n existen $p, q \in \mathbb{Z}$, $q > 1$, tales que

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

Se puede demostrar que ningún número algebraico sobre $\mathbb{Q}$ puede cumplir esta propiedad. Por ejemplo, el número

$$\alpha = \sum_{k\geq 1} \frac{1}{10^{k!}} = 0{,}1\,1\,000\,1\,\underbrace{0000000000000000}_{17\text{ ceros}}\,1\,000\cdots$$

es un número de Liouville, y por ende es trascendente.

2) Lindemann[*] probó en 1882 que e^α es trascendente sobre $\mathbb{Q}$ para cualquier número algebraico no nulo α. Para $\alpha = 1$ esto en particular establece la trascendencia de e. Para deducir la trascendencia de π, notamos que si π fuera algebraico, entonces $\pi\sqrt{-1}$ también lo sería y luego $e^{\pi\sqrt{-1}} = -1$ sería trascendente, lo que es absurdo.

De la misma manera del teorema de Lindemann se deduce la trascendencia de $\cos\alpha$, $\operatorname{sen}\alpha$, $\tan\alpha$ para cualquier número algebraico $\alpha \neq 0$ y la trascendencia de $\log\alpha$ para cualquier número algebraico $\alpha \neq 0, 1$.

3) Para la función zeta de Riemann

$$\zeta(s) := \sum_{n\geq 1} \frac{1}{n^s}, \quad (\operatorname{Re} s > 1)$$

Euler calculó que para cualquier $k = 1, 2, 3, \ldots$ se tiene

$$\zeta(2k) := 1 + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \frac{1}{4^{2k}} + \cdots = (-1)^{k+1}\, B_{2k}\, \frac{2^{2k-1}}{(2k)!}\, \pi^{2k},$$

[*] Ferdinand von Lindemann (1852–1939), matemático alemán, conocido principalmente por sus pruebas de la trascendencia de e y π. Director de tesis de Hilbert.

donde B_{2k} son ciertos números racionales, llamados los **números de Bernoulli**. Por ejemplo,

$$\begin{aligned}
\zeta(2) &= \frac{\pi^2}{6} \approx 1{,}644934\ldots,\\
\zeta(4) &= \frac{\pi^4}{90} \approx 1{,}082323\ldots,\\
\zeta(6) &= \frac{\pi^6}{945} \approx 1{,}017343\ldots,\\
\zeta(8) &= \frac{\pi^8}{9450} \approx 1{,}004077\ldots,\\
\zeta(10) &= \frac{\pi^{10}}{93\,555} \approx 1{,}000994\ldots,\\
\zeta(12) &= \frac{691\,\pi^{12}}{638\,512\,875} \approx 1{,}000246\ldots
\end{aligned}$$

Se supone que los números $\zeta(3), \zeta(5), \zeta(7), \zeta(9), \zeta(11), \ldots$ son también trascendentes, pero a diferencia de los $\zeta(2k)$, entre los $\zeta(2k+1)$ no hay ninguna relación algebraica para diferentes k. Sin embargo, hasta el momento no se conoce ni siquiera si los $\zeta(2k+1)$ son irracionales. Para $\zeta(3)$ esto fue establecido en 1977 por el matemático francés Roger Apéry y hay impresionantes resultados más recientes sobre la irracionalidad. Por ejemplo el matemático francés Tanguy Rivoal demostró en 2000 que entre los números $\zeta(3), \zeta(7), \zeta(9), \ldots$ hay una infinidad de irracionales, mientras que el matemático ruso Wadim Zudilin demostró en 2001 que por lo menos un número entre $\zeta(5)$, $\zeta(7)$, $\zeta(9)$ y $\zeta(11)$ es irracional (¡y la prueba no revela cuál!). Sin embargo, parece que la humanidad está muy lejos de probar la trascendencia de los $\zeta(2k+1)$.

4) La serie harmónica $\sum_{k\geq 1} \frac{1}{k}$ diverge lentamente, pero el límite

$$\gamma := \lim_{n\to\infty} \left(\sum_{1\leq k\leq n} \frac{1}{k} - \log n \right)$$

existe. El número $\gamma = 0{,}5772156649\ldots$ se conoce como la **constante de Euler–Mascheroni**[*] y aparece en muchos contextos importantes, inclusive aritméticos. Por ejemplo, el **tercer teorema de Mertens**[**] afirma que

$$\lim_{n\to\infty} \log n \prod_{p\leq n} \left(1 - \frac{1}{p}\right) = e^{-\gamma},$$

donde el producto se toma sobre los primos menores que n.

Otra aparición de la constante de Euler–Mascheroni es la serie de Laurent para la función zeta de Riemann

$$\zeta(s) = \frac{1}{s-1} + \sum_{n\geq 0} \frac{(-1)^n}{n!}\, \gamma_n\, (s-1)^n,$$

[*] Lorenzo Mascheroni (1750–1800), matemático italiano.
[**] Franz Mertens (1840–1927), teórico de números polaco.

donde $\gamma_0 = \gamma$.

Se supone que el número γ es trascendente, pero hasta el momento no ha sido probado ni siquiera que es irracional.

Los números trascendentes se estudian en la **teoría de números trascendente**, mientras que los números algebraicos se estudian en la **teoría de números algebraica**. En este curso, naturalmente, nos van a interesar los números algebraicos. *Para conocer el lado trascendente*, el lector puede consultar el libro de texto [Bak1990].

14.6 La norma, traza y polinomio característico

Para endender mejor esta sección, el lector debe de revisar el apéndice C para las definiciones y resultados relevantes de álgebra lineal. Sea L/K una extensión finita de grado n. Para $\alpha \in L$ consideremos la aplicación de multiplicación por α sobre L:

$$\mu_\alpha \colon L \to L, \quad x \mapsto \alpha x.$$

Esto es un endomorfismo del espacio K-vectorial L. Notamos que para cualesquiera $\alpha, \beta \in L$, $a, b \in K$ se cumple

$$\mu_{\alpha\beta} = \mu_\alpha \circ \mu_\beta, \quad \mu_{a\alpha+b\beta} = a\,\mu_\alpha + b\,\mu_\beta.$$

14.6.1. Definición. Sean L/K una extensión finita de cuerpos y $\alpha \in L$.

1) La **norma** y **traza** de α son el determinante y traza del endomorfismo $\mu_\alpha \colon L \to L$ respectivamente:
$$N_{L/K}(\alpha) := \det \mu_\alpha, \quad T_{L/K}(\alpha) := \operatorname{tr} \mu_\alpha.$$

2) El **polinomio característico** de α es el polinomio característico de μ_α:
$$p_{\alpha,L/K} := p_{\mu_\alpha} := p_A := \det(X\,I_n - A) \in K[X],$$
donde $A \in M_n(K)$ es una matriz que representa a ϕ en alguna base (véase el apéndice C).

14.6.2. Comentario. La norma, traza y el polinomio característico no solamente dependen de α, sino también de la extensión L/K. Cuando la última está clara a partir del contexto, vamos a omitirla por simplicidad y escribir "N, T, p_α" en lugar de "$N_{L/K}$, $T_{L/K}$, $p_{\alpha,L/K}$".

14.6.3. Proposición. *Si $[L : K] = n$, entonces para cualquier $\alpha \in L$ el polinomio característico de α es mónico de grado n:*

$$p_{\alpha,L/K} = X^n + a_{n-1}\,X^{n-1} + \cdots + a_1\,X + a_0.$$

Además,

$$a_{n-1} = -T_{L/K}(\alpha), \quad a_0 = (-1)^n\,N_{L/K}(\alpha).$$

Demostración. Esto es una propiedad general del polinomio característico, probada en el apéndice C: tenemos

$$p_{\alpha,L/K} := p_{\mu_\alpha} = X^n - \operatorname{tr}(\mu_\alpha)\, X^{n-1} + \cdots + a_1\, X + (-1)^n \det(\mu_\alpha).$$

■

14.6.4. Ejemplo. Para $a \in K$ la aplicación $\mu_a \colon L \to L$ se representa en cualquier base por la matriz escalar de $n \times n$

$$\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix},$$

así que

$$N_{L/K}(a) = a^n, \quad T_{L/K}(a) = na, \quad p_{a,L/K} = (X-a)^n.$$

▲

14.6.5. Ejemplo. Para un cuerpo K, sea $d \in K$ un elemento tal que d no es un cuadrado; es decir, el polinomio $X^2 - d$ es irreducible en $K[X]$. Consideremos la extensión

$$K(\sqrt{d}) = K[X]/(X^2 - d),$$

donde $\sqrt{d}$ denota la imagen de X en el cociente. La extensión $K(\sqrt{d})/K$ tiene grado 2 y los elementos $1, \sqrt{d}$ forman una base de $K(\sqrt{d})$ como un espacio vectorial sobre K. Para un elemento fijo $\alpha = a + b\sqrt{d}$ tenemos

$$\alpha \cdot 1 = \alpha = a + b\sqrt{d}, \quad \alpha \cdot \sqrt{d} = db + a\sqrt{d},$$

así que la multiplicación por α sobre $K(\sqrt{d})$ corresponde a la matriz

$$A = \begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

Luego,

$$N(\alpha) = \det A = a^2 - d\, b^2, \quad T(\alpha) = \operatorname{tr} A = 2\, a.$$

El polinomio característico de la matriz de arriba es

$$p_\alpha = \det \begin{pmatrix} X-a & db \\ b & X-a \end{pmatrix} = (X-a)^2 - db^2 = X^2 - 2a\, X + a^2 - db^2 = X^2 - T(\alpha)\, X + N(\alpha).$$

▲

14.6.6. Ejemplo. Consideremos la extensión $K(\sqrt[3]{d})/K$ donde d no es un cubo en K; es decir, el polinomio $X^3 - d$ es irreducible en $K[X]$. Esta es una extensión de grado 3 y como una base de $K(\sqrt[3]{d})$ sobre K se puede tomar

$$1, \quad \sqrt[3]{d}, \quad \sqrt[3]{d^2}.$$

Para el elemento $\sqrt[3]{d}$ calculamos la aplicación $\mu_{\sqrt[3]{d}}\colon K(\sqrt[3]{d}) \to K(\sqrt[3]{d})$:

$$1 \mapsto \sqrt[3]{d}, \quad \sqrt[3]{d} \mapsto \sqrt[3]{d^2}, \quad \sqrt[3]{d^2} \mapsto d.$$

Entonces, $\mu_{\sqrt[3]{d}}$ se representa en la base $1, \sqrt[3]{d}, \sqrt[3]{d^2}$ por la matriz

$$\begin{pmatrix} 0 & 0 & d \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

de donde

$$N(\sqrt[3]{d}) = d, \quad T(\sqrt[3]{d}) = 0.$$

El polinomio característico correspondiente es

$$\det \begin{pmatrix} X & 0 & -d \\ -1 & X & 0 \\ 0 & -1 & X \end{pmatrix} = X \det \begin{pmatrix} X & 0 \\ -1 & X \end{pmatrix} - d \det \begin{pmatrix} -1 & X \\ 0 & -1 \end{pmatrix} = X^3 - d.$$

(Note que la norma y traza de α también pueden extraerse de los coeficientes del polinomio característico.) Por otro lado, la aplicación

$$\mu_{\sqrt[3]{d^2}} = \mu_{\sqrt[3]{d}} \circ \mu_{\sqrt[3]{d}}$$

se representa por la matriz

$$\begin{pmatrix} 0 & 0 & d \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & d \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & d & 0 \\ 0 & 0 & d \\ 1 & 0 & 0 \end{pmatrix},$$

de donde

$$N(\sqrt[3]{d^2}) = d^2, \quad T(\sqrt[3]{d^2}) = 0.$$

El polinomio característico correspondiente es

$$\det \begin{pmatrix} X & -d & 0 \\ 0 & X & -d \\ -1 & 0 & X \end{pmatrix} = X \det \begin{pmatrix} X & -d \\ 0 & X \end{pmatrix} + d \det \begin{pmatrix} 0 & -d \\ -1 & X \end{pmatrix} = X^3 - d^2.$$

▲

14.6.7. Proposición. *Sea L/K una extensión finita. Para todo $\alpha \in L$ el polinomio característico de α tiene a α como su raíz:*

$$p_{\alpha, L/K}(\alpha) = 0.$$

Demostración. Primero notamos que gracias a las identidades

$$\mu_\alpha \circ \mu_\beta = \mu_{\alpha\beta}, \quad a\,\mu_\alpha + b\,\mu_\beta = \mu_{a\,\alpha + b\,\beta}$$

para cualesquiera $\alpha, \beta \in L$, $a, b \in K$, se sigue que para cualquier polinomio

$$f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_1 X + a_0 \in K[X]$$

se cumple

$$f(\mu_\alpha) := a_m \mu_\alpha^m + a_{m-1} \mu_\alpha^{m-1} + \cdots + a_1 \mu_\alpha + a_0 \,\mathrm{id} = \mu_{f(\alpha)}.$$

Por simplicidad, escribamos "p" en lugar de "$p_{\alpha,L/K}$". Tenemos

$$\mu_{p(\alpha)} = p(\mu_\alpha) = 0$$

por el teorema de Cayley–Hamilton (véase el apéndice C). En particular,

$$p(\alpha) = \mu_{p(\alpha)}(1) = 0.$$

■

14.6.8. Corolario. *Si $L = K(\alpha)$, entonces el polinomio característico $p_{\alpha,L/K}$ coincide con el polinomio mínimo $m_{\alpha,K}$.*

Demostración. El polinomio característico es un polinomio mónico de grado $[L : K]$ que, como acabamos de ver, tiene a α como su raíz. Luego, si $L = K(\alpha)$, entonces $[L : K] = \deg_K(\alpha)$ y $p_{\alpha,K}$ debe ser el polinomio mínimo de α sobre K. ■

14.6.9. Ejemplo. Sean m y n dos enteros tales que m, n, mn no son cuadrados. En este caso

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n}), \quad [\mathbb{Q}(\sqrt{m}, \sqrt{n}) : \mathbb{Q}] = 4$$

(véase el ejercicio 14.7). Como una base se puede tomar

$$1, \sqrt{m}, \sqrt{n}, \sqrt{mn}.$$

Calculemos el polinomio característico de $\sqrt{m} + \sqrt{n}$. Tenemos

$$\begin{aligned}
1 \cdot (\sqrt{m} + \sqrt{n}) &= \sqrt{m} + \sqrt{n}, \\
\sqrt{m} \cdot (\sqrt{m} + \sqrt{n}) &= m + \sqrt{mn}, \\
\sqrt{n} \cdot (\sqrt{m} + \sqrt{n}) &= n + \sqrt{mn}, \\
\sqrt{mn} \cdot (\sqrt{m} + \sqrt{n}) &= n\sqrt{m} + m\sqrt{n}.
\end{aligned}$$

Entonces, la multiplicación por $\sqrt{m} + \sqrt{n}$ en la base de arriba corresponde a la matriz

$$A = \begin{pmatrix} 0 & m & n & 0 \\ 1 & 0 & 0 & n \\ 1 & 0 & 0 & m \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Su polinomio característico viene dado por

$$\det \begin{pmatrix} X & -m & -n & 0 \\ -1 & X & 0 & -n \\ -1 & 0 & X & -m \\ 0 & -1 & -1 & X \end{pmatrix} = X^4 - 2\,(m+n)\,X^2 + (m-n)^2$$

(el ejercicio 14.7 da otro modo de obtener el mismo polinomio). Puesto que $\mathbb{Q}(\sqrt{m},\sqrt{n}) = \mathbb{Q}(\sqrt{m}+\sqrt{n})$, lo que acabamos de encontrar es el polinomio mínimo de $\sqrt{m}+\sqrt{n}$ sobre $\mathbb{Q}$. ▲

Multiplicatividad de la norma, linealidad de la traza

14.6.10. Observación.

1) *La norma $N_{L/K}\colon L \to K$ es multiplicativa: para cualesquiera $\alpha, \beta \in L$ se tiene*

$$N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)\cdot N_{L/K}(\beta).$$

2) *La traza $T_{L/K}\colon L \to K$ es K-lineal: para cualesquiera $\alpha, \beta \in L$, $a, b \in K$ se tiene*

$$T_{L/K}(a\alpha + b\beta) = a\,T_{L/K}(\alpha) + b\,T_{L/K}(\beta).$$

Demostración. Se sigue del hecho de que el determinante es multiplicativo y la traza es K-lineal:

$$N_{L/K}(\alpha\beta) = \det(\mu_{\alpha\beta}) = \det(\mu_\alpha \circ \mu_\beta) = \det(\mu_\alpha)\cdot\det(\mu_\beta) = N_{L/K}(\alpha)\cdot N_{L/K}(\beta),$$

y

$$T_{L/K}(a\alpha+b\beta) = T_{L/K}(\mu_{a\alpha+b\beta}) = \operatorname{tr}(a\,\mu_\alpha + b\,\mu_\beta) = a\,\operatorname{tr}(\mu_\alpha) + b\,\operatorname{tr}(\mu_\beta) = a\,T_{L/K}(\alpha) + b\,T_{L/K}(\beta).$$

■

14.6.11. Ejemplo. Probemos que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$. Asumamos que $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{2})$. Dado que

$$[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{6}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3,$$

en este caso tendríamos

$$\mathbb{Q}(\sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{6}) = K.$$

En particular, existen algunos $a, b, c \in \mathbb{Q}$ tales que

$$\sqrt[3]{3} = a + b\,\sqrt[3]{2} + c\,\sqrt[3]{4}.$$

En el ejemplo 14.6.6 hemos calculado que $T_{K/\mathbb{Q}}(\sqrt[3]{2}) = T_{K/\mathbb{Q}}(\sqrt[3]{4}) = 0$. De aquí se sigue que

$$T_{K/\mathbb{Q}}(\sqrt[3]{3}) = T_{K/\mathbb{Q}}(a) + b\,T_{K/\mathbb{Q}}(\sqrt[3]{2}) + c\,T_{K/\mathbb{Q}}(\sqrt[3]{4}) = 3\,a.$$

Luego, tenemos

$$\sqrt[3]{6} = a\,\sqrt[3]{2} + b\,\sqrt[3]{4} + 2c,$$

de donde

$$T_{K/\mathbb{Q}}(\sqrt[3]{6}) = 2\,T_{K/\mathbb{Q}}(c) = 6\,c.$$

Sin embargo, los cálculos de 14.6.6 aplicados a las extensiones $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt[3]{6})/\mathbb{Q}$ nos dicen que

$$T_{K/\mathbb{Q}}(\sqrt[3]{3}) = T_{K/\mathbb{Q}}(\sqrt[3]{6}) = 0.$$

Entonces, $a = c = 0$ y se tiene

$$\sqrt[3]{3} = b\,\sqrt[3]{2}.$$

Esto significa que el número $\sqrt[3]{3/2} = b$ es racional, pero no es el caso. Esta contradicción implica que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$. ▲

14.6.12. Comentario. Para apreciar el argumento de arriba, el lector puede tratar de probar de manera directa que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$, sin usar trazas.

14.6.13. Ejemplo. Consideremos la extensión $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$. Probemos que el número $1 + \sqrt{-5}$ no es un cuadrado en $\mathbb{Q}(\sqrt{-5})$; es decir, no existe $\alpha \in \mathbb{Q}(\sqrt{-5})$ tal que $\alpha^2 = 1 + \sqrt{-5}$. En efecto, en este caso tendríamos

$$N(\alpha)^2 = N(\alpha^2) = N(1 + \sqrt{-5}) = 1^2 + 5 \cdot 1^2 = 6,$$

pero 6 no es un cuadrado en $\mathbb{Q}$. ▲

14.6.14. Comentario. Si para $\alpha \in L$ la norma $N(\alpha)$ es una potencia n-ésima en K, esto *no implica* en general que α es una potencia n-ésima en L.

He aquí un contraejemplo fácil: consideremos la extensión $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$. La norma viene dada por $N(a + b\sqrt{-1}) = a^2 + b^2$. Luego, el número 2 tiene norma 4, pero no es un cuadrado en $\mathbb{Q}(\sqrt{-1})$: si $\alpha^2 = 2$, entonces necesariamente $N(\alpha) = 2$. Sin embargo, los elementos de norma 2 son

$$\pm(1 + \sqrt{-1}), \quad \pm(1 - \sqrt{-1}),$$

y sus cuadrados no son iguales a 2:

$$(1 \pm \sqrt{-1})^2 = \pm 2\sqrt{-1}.$$

Polinomio característico y el polinomio mínimo

En general, el polinomio característico y el polinomio mínimo están relacionados de la siguiente manera.

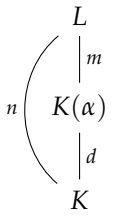
14.6.15. Teorema. *Sean L/K una extensión finita y $\alpha \in L$. Luego,*

$$p_{\alpha,L/K} = m_{\alpha,K}^{n/d},$$

donde

$$n := [L : K], \quad d := \deg_K(\alpha) := [K(\alpha) : K].$$

Demostración. Consideremos las extensiones



Como una base de $K(\alpha)$ sobre K podemos tomar las potencias de α:

$$1, \alpha, \alpha^2, \ldots, \alpha^{d-1}.$$

Sea

$$\beta_1, \beta_2, \ldots, \beta_m$$

una base de L sobre $K(\alpha)$. Entonces, como vimos en 14.1.6, se pueden tomar como una base de L sobre K los productos

$$\alpha^i \beta_j. \quad (0 \leq i \leq d-1,\ 1 \leq j \leq m)$$

Sean c_{ij} los coeficientes de la matriz que representa el endomorfismo $\mu_\alpha \colon K(\alpha) \to K(\alpha)$:

$$\alpha \cdot \alpha^j = \sum_{0 \leq i \leq d-1} c_{ij}\, \alpha^i.$$

Tenemos entonces

$$m_{\alpha,K} = p_{\alpha,K(\alpha)/K} = \det(X \cdot I_d - A),$$

(véase 14.6.8) donde

$$A = \begin{pmatrix} c_{00} & c_{01} & \cdots & c_{0,d-1} \\ c_{10} & c_{11} & \cdots & c_{1,d-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{d-1,0} & c_{d-1,1} & \cdots & c_{d-1,d-1} \end{pmatrix}.$$

Luego,

$$\alpha \cdot \alpha^j \beta_k = \sum_{0 \leq i \leq d-1} c_{ij}\, \alpha^j \beta_k,$$

de donde se ve que la multiplicación por α sobre L se representa en la base $\alpha^j \beta_k$ por la matriz diagonal por bloques

$$\begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix}.$$

Su polinomio característico viene dado por

$$\det \begin{pmatrix} X\, I_d - A & & & \\ & X\, I_d - A & & \\ & & \ddots & \\ & & & X\, I_d - A \end{pmatrix} = \det(X\, I_d - A)^m = m_{\alpha,K}^{n/d}.$$

■

14.6.16. Corolario. *En la situación del teorema anterior, si el polinomio mínimo de α viene dado por*

$$m_{\alpha,K} = X^d + a_{d-1}\, X^{d-1} + \cdots + a_1\, X + a_0,$$

entonces

$$T_{L/K}(\alpha) = -\frac{n}{d}\, a_{d-1}, \quad N_{L/K}(\alpha) = (-1)^n\, a_0^{n/d}.$$

Demostración. Tenemos

$$p_{\alpha,L/K} = m_{\alpha,K}^{n/d} = \left(X^d + a_{d-1}\,X^{d-1} + \cdots + a_1\,X + a_0\right)^{n/d} = X^n + \frac{n}{d}\,a_{d-1}\,X^{n-1} + \cdots + a_0^{n/d}.$$

■

14.6.17. Corolario. *Si en una extensión L/K de grado n para $\alpha \in L$ el polinomio mínimo se descompone en factores lineales*

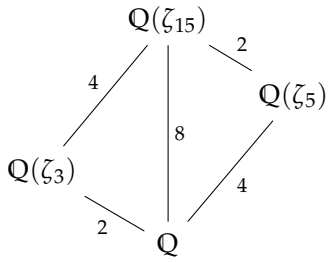
$$m_{\alpha,K} = (X - \alpha_1)\cdots(X - \alpha_d),$$

para algunos $\alpha_1, \ldots, \alpha_d \in L$, entonces

$$T_{L/K}(\alpha) = \frac{n}{d}\,(\alpha_1 + \cdots + \alpha_d), \quad N_{L/K}(\alpha) = (\alpha_1 \cdots \alpha_d)^{n/d}.$$

Demostración. Se sigue inmediatamente del corolario anterior. ■

14.6.18. Ejemplo. Consideremos las extensiones ciclotómicas



Tenemos

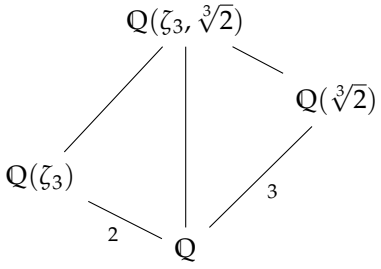
$$m_{\zeta_3,\mathbb{Q}} = \Phi_3 = X^2 + X + 1, \quad m_{\zeta_5,\mathbb{Q}} = \Phi_5 = X^4 + X^3 + X^2 + X + 1.$$

Luego, del resultado de 14.6.15 sabemos que

$$p_{\zeta_3,\mathbb{Q}(\zeta_{15})/\mathbb{Q}} = (X^2 + X + 1)^4, \quad p_{\zeta_5,\mathbb{Q}(\zeta_{15})/\mathbb{Q}} = (X^4 + X^3 + X^2 + X + 1)^2.$$

▲

14.6.19. Ejemplo. Volvamos al ejemplo 14.1.15. Consideremos las extensiones



donde

$$K = \mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}(\zeta_3 + \sqrt[3]{2}).$$

Sabemos que

$$[K : \mathbb{Q}] \leq \deg_{\mathbb{Q}}(\zeta_3) \cdot \deg_{\mathbb{Q}}(\sqrt[3]{2}) = 6,$$

pero este número tiene que ser divisible por 2 y 3, así que es precisamente 6. Como una base se puede tomar

$$1, \quad \zeta_3, \quad \sqrt[3]{2}, \quad \sqrt[3]{2}^2, \quad \zeta_3\sqrt[3]{2}, \quad \zeta_3\sqrt[3]{2}^2.$$

Calculamos

$$\begin{aligned}
1 \cdot (\zeta_3 + \sqrt[3]{2}) &= \zeta_3 + \sqrt[3]{2},\\
\zeta_3 \cdot (\zeta_3 + \sqrt[3]{2}) &= -1 - \zeta_3 + \zeta_3\sqrt[3]{2},\\
\sqrt[3]{2} \cdot (\zeta_3 + \sqrt[3]{2}) &= \sqrt[3]{2}^2 + \zeta_3\sqrt[3]{2},\\
\sqrt[3]{2}^2 \cdot (\zeta_3 + \sqrt[3]{2}) &= 2 + \zeta_3\sqrt[3]{2}^2,\\
\zeta_3\sqrt[3]{2} \cdot (\zeta_3 + \sqrt[3]{2}) &= -\sqrt[3]{2} - \zeta_3\sqrt[3]{2} + \zeta_3\sqrt[3]{2}^2,\\
\zeta_3\sqrt[3]{2}^2 \cdot (\zeta_3 + \sqrt[3]{2}) &= 2\zeta_3 - \sqrt[3]{2}^2 - \zeta_3\sqrt[3]{2}^2.
\end{aligned}$$

La matriz correspondiente es

$$A = \begin{pmatrix}
0 & -1 & 0 & 2 & 0 & 0\\
1 & -1 & 0 & 0 & 0 & 2\\
1 & 0 & 0 & 0 & -1 & 0\\
0 & 0 & 1 & 0 & 0 & -1\\
0 & 1 & 1 & 0 & -1 & 0\\
0 & 0 & 0 & 1 & 1 & -1
\end{pmatrix}.$$

Su polinomio característico es[*]

$$X^6 + 3X^5 + 6X^4 + 3X^3 + 9X + 9.$$

Este polinomio tiene grado 6 y tiene $\zeta_3 + \sqrt[3]{2}$ como su raíz, así que es el polinomio mínimo de $\zeta_3 + \sqrt[3]{2}$ sobre $\mathbb{Q}$.

Tenemos

$$m_{\zeta_3,\mathbb{Q}} = X^2 + X + 1, \quad m_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2,$$

de donde

$$p_{\zeta_3,K/\mathbb{Q}} = (X^2 + X + 1)^3, \quad p_{\sqrt[3]{2},K/\mathbb{Q}} = (X^3 - 2)^2.$$

▲

[*]Se puede hacer este cálculo en el programa PARI/GP (http://pari.math.u-bordeaux.fr/):

```
? charpoly([0,-1,0,2,0,0;1,-1,0,0,0,2;1,0,0,0,-1,0;0,0,1,0,0,-1;0,1,1,0,-1,0;0,0,0,1,1,-1])
% = x^6 + 3*x^5 + 6*x^4 + 3*x^3 + 9*x + 9
```

14.7 Cuerpos de descomposición

Recordemos que un polinomio $f \in K[X]$ tiene una raíz $\alpha \in K$ si y solo si $(X-\alpha) \mid f$. En particular, esto implica que si $\deg f = n > 0$, entonces f tiene a lo sumo n raíces. Si todas las raíces de f están en K, entonces f se descompone en factores lineales en $K[X]$:

$$f = c\,(X-\alpha_1)\cdots(X-\alpha_n).$$

14.7.1. Definición. Para un polinomio $f \in K[X]$ se dice que una extensión L/K es un **cuerpo de descomposición**[*] de f si

1) f se descompone en factores lineales en $L[X]$;

2) ninguna subextensión $K \subseteq L' \subsetneq L$ satisface esta propiedad.

14.7.2. Observación. *Sea $f \in K[X]$ un polinomio de grado n y L/K una extensión tal que en $L[X]$ se tiene una descomposición*

$$f = c\,(X-\alpha_1)\cdots(X-\alpha_n)$$

para algunos $\alpha_1,\ldots,\alpha_n \in L$. Entonces, el subcuerpo

$$K(\alpha_1,\ldots,\alpha_n) = \bigcap_{\substack{K'\subseteq L \\ \alpha_1,\ldots,\alpha_n\in K'}} K'$$

es un cuerpo de descomposición de f.

Demostración. Está claro de la definición. ■

14.7.3. Ejemplo. Sean K un cuerpo y $d \in K$ un elemento que no es un cuadrado en K. Entonces, $K(\sqrt{d}) := K[X]/(X^2-d)$ es un cuerpo de descomposición del polinomio X^2-d. ▲

14.7.4. Ejemplo. Para el polinomio $X^n-1 \in \mathbb{Q}[X]$ el cuerpo ciclotómico $\mathbb{Q}(\zeta_n)$ es un cuerpo de descomposición. En efecto, las raíces complejas de X^n-1 son las raíces n-ésimas de la unidad, generadas por la raíz primitiva $\zeta_n := e^{2\pi\sqrt{-1}/n}$. ▲

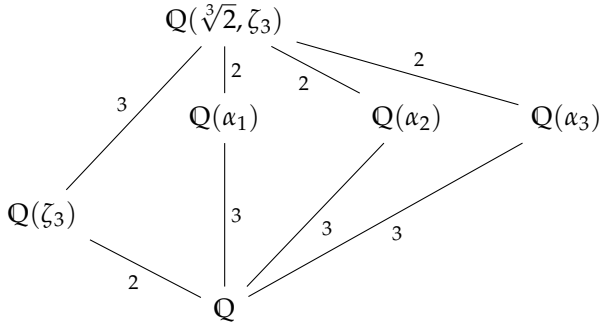
14.7.5. Ejemplo. Consideremos el polinomio $X^3-2 \in \mathbb{Q}[X]$. Sus raíces complejas son

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \zeta_3\sqrt[3]{2}, \quad \alpha_3 = \zeta_3^2\sqrt[3]{2}.$$

El cuerpo de descomposición es el cuerpo

$$\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3) = \mathbb{Q}(\alpha_1,\alpha_2) = \mathbb{Q}(\alpha_1,\alpha_3) = \mathbb{Q}(\sqrt[3]{2},\zeta_3).$$

[*] *Splitting field* en inglés.



▲

Un polinomio $f \in \mathbb{Q}[X]$ siempre tiene raíces complejas $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ y esto nos permite tomar $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ como un cuerpo de descomposición de f. En la situación general abstracta, un cuerpo de descomposición se construye de la siguiente manera.

14.7.6. Proposición. *Para un polinomio $f \in K[X]$ existe un cuerpo de descomposición L/K. Además, $[L : K] \leq n!$ donde $n := \deg f$.*

Demostración. Gracias a la observación 14.7.2, bastaría probar que existe una extensión L/K de grado $\neq n!$ tal que f se descompone en factores lineales en $L[X]$.

Procedamos por inducción sobre n. Si $n = 1$, entonces, siendo un polinomio lineal, f tiene una raíz en K y podemos tomar $L = K$.

Ahora si $n > 1$, sea $p \mid f$ algún factor irreducible de f en $K[X]$. Consideremos el cuerpo $L' := K[X]/(p)$. Denotemos por α la imagen de X en el cociente. Tenemos $[L' : K] = \deg p \leq n$. Además, $p(\alpha) = 0$ y por ende $f(\alpha) = 0$. Se sigue que en $L'[X]$ tenemos una factorización

$$f = (X - \alpha)\, g$$

para algún polinomio $g \in L'[X]$. Tenemos $\deg g = n - 1$, así que por la hipótesis de inducción, existe una extensión L/L' de grado $\leq (n-1)!$ tal que g (y entonces f) se descompone en factores lineales en $L[X]$. Luego,

$$[L : K] = [L : L'] \cdot [L' : K] \leq (n-1)! \cdot n \leq n!$$

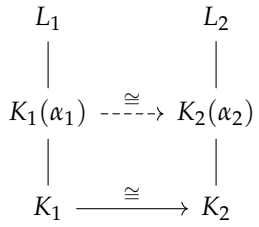
■

Nuestro próximo objetivo es probar que todos los cuerpos de descomposición de f son isomorfos. Empecemos por el siguiente lema.

14.7.7. Lema. *Sea $\phi\colon K_1 \xrightarrow{\cong} K_2$ un isomorfismo de cuerpos y*

$$\begin{aligned} \phi\colon K_1[X] &\to K_2[X], \\ \sum_{i \geq 0} a_i X^i &\mapsto \sum_{i \geq 0} \phi(a_i)\, X^i \end{aligned}$$

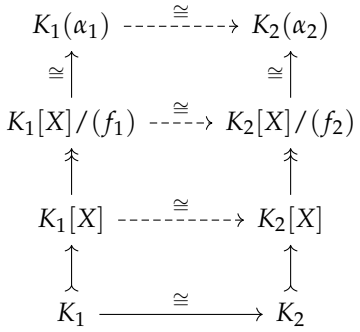
el isomorfismo correspondiente de los anillos de polinomios. Sean $f_1 \in K_1[X]$ y $f_2 \in K_2[X]$ polinomios irreducibles donde $f_2 = \phi(f_1)$ y sean L_1/K_1 y L_2/K_2 extensiones y $\alpha_1 \in L_1$, $\alpha_2 \in L_2$ elementos tales que $f_1(\alpha_1) = 0$ y $f_2(\alpha_2) = 0$. Entonces, el isomorfismo $K_1 \xrightarrow{\cong} K_2$ se extiende de manera canónica a un isomorfismo $K_1(\alpha_1) \xrightarrow{\cong} K_2(\alpha_2)$.



Demostración. El isomorfismo entre $K_1[X]$ y $K_2[X]$ envía el ideal maximal $(f_1) \subset K_1[X]$ al ideal maximal $(f_2) \subset K_2[X]$ y entonces induce un isomorfismo

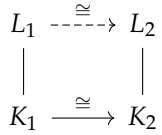
$$K_1[X]/(f_1) \xrightarrow{\cong} K_2[X]/(f_2).$$

Basta considerar el diagrama conmutativo



■

14.7.8. Lema. *Sea $\phi\colon K_1 \xrightarrow{\cong} K_2$ un isomorfismo de cuerpos. Sean $f_1 \in K_1[X]$ un polinomio irreducible y $f_2 \in K_2[X]$ el polinomio que corresponde a f_1 bajo el isomorfismo $K_1[X] \xrightarrow{\cong} K_2[X]$ inducido por ϕ. Sean L_1/K_1 y L_2/K_2 cuerpos de descomposición de f_1 y f_2 respectivamente. Entonces, el isomorfismo entre K_1 y K_2 se extiende a un isomorfismo entre L_1 y L_2:*



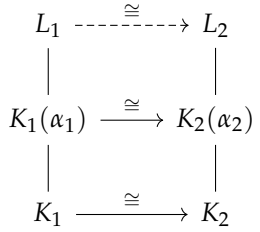
Demostración. Procedamos por inducción sobre $n = \deg f_1$. Notamos que los factores irreducibles de f_1 en $K_1[X]$ corresponden a los factores irreducibles de f_2 en $K_2[X]$.

Si $n = 1$, o en general si f_1 se descompone en factores lineales en $K_1[X]$, se tiene $L_1 = K_1$, $L_2 = K_2$ y no hay que probar nada.

Si $n > 1$, sea $p_1 \in K_1[X]$ un factor irreducible de f y $p_2 \in K_2[X]$ el factor irreducible correspondiente de f_2. Si $\alpha_1 \in L_1$ es una raíz de p_1 y $\alpha_2 \in L_2$ es una raíz de p_2, entonces el lema anterior nos permite extender el isomorfismo $K_1 \xrightarrow{\cong} K_2$ a un isomorfismo $K_1(\alpha_1) \xrightarrow{\cong} K(\alpha_2)$. Ahora

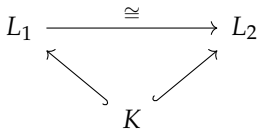
$$f_1 = (X - \alpha_1)\, g_1 \text{ en } K_1(\alpha_1)[X], \quad f_2 = (X - \alpha_2)\, g_2 \text{ en } K_2(\alpha_2)[X].$$

Notamos que L_1 y L_2 son cuerpos de descomposición para g_1 y g_2 sobre $K_1(\alpha_1)$ y $K_2(\alpha_2)$ respectivamente. Puesto que $\deg g_1 = \deg g_2 = n - 1$, por la hipótesis de inducción, el isomorfismo $K_1(\alpha_1) \xrightarrow{\cong} K_2(\alpha_2)$ se extiende a un isomorfismo $L_1 \xrightarrow{\cong} L_2$.



■

14.7.9. Corolario. *Para un polinomio $f \in K[X]$, si L_1/K y L_2/K son dos cuerpos de descomposición, entonces existe un isomorfismo*



Demostración. Basta aplicar el resultado anterior a $K_1 = K_2 = K$, $\phi = \mathrm{id}$ y $f_1 = f_2 = f$. ■

14.8 Extensiones separables

14.8.1. Definición. Sea K un cuerpo y $f \in K[X]$ un polinomio. En un cuerpo de descomposición L/K tenemos

$$f = c\,(X - \alpha_1)^{m_1} \cdots (X - \alpha_k)^{m_k},$$

donde $\alpha_1, \ldots, \alpha_k \in L$ son diferentes elementos y $m_i \geq 1$. Si $m_i = 1$, se dice que α_i es una **raíz simple** de f y si $m_i > 1$, se dice que α_i es una **raíz multiple** de **multiplicidad** m_i. Si todas las raíces de f son simples, se dice que f es un **polinomio separable**.

Notamos que diferentes cuerpos de descomposición son isomorfos y las multiplicidades de las raíces no dependen de la elección de L.

14.8.2. Proposición. *Un polinomio $f \in K[X]$ tiene una raíz múltiple $\alpha \in K$ si y solo si $f'(\alpha) = 0$.*

Demostración. Si α es una raíz multiple, entonces

$$f = (X-\alpha)^2\, g$$

para algún polinomio $g \in K[X]$. Luego, tomando las derivadas, se obtiene

$$f' = 2\,(X-\alpha)\, g + (X-\alpha)^2\, g',$$

de donde $f'(\alpha) = 0$. Viceversa, si $\alpha \in K$ es una raíz común de f y f', entonces tenemos

$$f = (X-\alpha)\, g$$

para algún $g \in K[X]$, y luego

$$f' = g + (X-\alpha)\, g'.$$

De aquí se sigue que $g = f' - (X-\alpha)\, g'$ tiene α como su raíz; es decir, $(X-\alpha) \mid g$. Entonces,

$$f = (X-\alpha)^2\, h$$

para algún $h \in K[X]$. ■

14.8.3. Corolario. *Un polinomio $f \in K[X]$ es separable si y solo si* $\operatorname{mcd}(f, f') = 1$.

Demostración. Sea L/K un cuerpo de descomposición de f.

Si $\operatorname{mcd}(f, f') \neq 1$, entonces existe un polinomio no constante $g \in K[X]$ tal que $g \mid f$ y $g \mid f'$. El polinomio g tiene una raíz $\alpha \in L$, y luego $f(\alpha) = f'(\alpha) = 0$, lo que significa que α es una raíz múltiple de f en L.

Viceversa. si f no es separable, entonces existe $\alpha \in L$ tal que $f(\alpha) = f'(\alpha) = 0$. Esto implica que el polinomio mínimo $m_{\alpha,K}$ divide a f y f', y por ende $\operatorname{mcd}(f, f') \neq 1$. ■

14.8.4. Corolario. *Sea $f \in K[X]$ un polinomio irreducible. Si $f' \neq 0$, entonces f es separable.*

Demostración. Si $g \mid f$ y $g \mid f'$ y f es irreducible, entonces $g \in K^\times$ o $g \sim f$. Sin embargo, en el segundo caso tenemos $\deg f' < \deg f$, así que $g \nmid f'$. Se sigue que $\operatorname{mcd}(f, f') = 1$, y por lo tanto f es separable. ■

14.8.5. Ejemplo. Consideremos el cuerpo

$$K := \mathbb{F}_p(T) := \left\{ \frac{f}{g} \;\middle|\; f, g \in \mathbb{F}_p[T],\ g \neq 0 \right\}.$$

El polinomio $X^p - T$ es irreducible por el criterio de Eisenstein: el elemento T es irreducible en $\mathbb{F}_p[T]$ y $\mathbb{F}_p(T)$ es el cuerpo de fracciones de $\mathbb{F}_p[T]$. Sin embargo, $X^p - T$ no es separable: su derivada es nula, ya que trabajamos en característica p. ▲

14.8.6. Definición. Para una extensión de cuerpos L/K se dice que un elemento $\alpha \in L$ es **separable** sobre K si

1) α es algebraico sobre K,

2) el polinomio mínimo de α sobre K es separable.

Si todo elemento de L es separable sobre K, se dice que L/K es una **extensión separable**.

Para ciertos cuerpos todas las extensiones algebraicas son automáticamente separables.

14.8.7. Definición. Se dice que un cuerpo K es **perfecto** si se cumple una de las siguientes condiciones:

1) $\operatorname{char} K = 0$;

2) $\operatorname{char} K = p$ y todo elemento de K es una p-ésima potencia.

14.8.8. Ejemplo. Todo cuerpo finito es perfecto. En efecto, si K es finito, entonces es una extensión finita de $\mathbb{F}_p$. Consideremos la aplicación

$$\begin{aligned} F\colon K &\to K, \\ \alpha &\mapsto \alpha^p. \end{aligned}$$

Esto es un homomorfismo: tenemos claramente $(\alpha\beta)^p = \alpha^p\,\beta^p$ para cualesquiera $\alpha, \beta \in K$, y luego, dado que estamos en la característica p, tenemos también $(\alpha+\beta)^p = \alpha^p + \beta^p$. Siendo un homomorfismo de cuerpos, F es inyectivo, pero K es finito, así que F es también sobreyectivo. Para más información sobre los cuerpos finitos y la aplicación F, véase el siguiente capítulo. ▲

14.8.9. Ejemplo. El cuerpo $\mathbb{F}_p(T)$ no es perfecto: en este caso $\sqrt[p]{T} \notin \mathbb{F}_p(T)$. ▲

14.8.10. Proposición. *Si K es un cuerpo perfecto, entonces todo polinomio irreducible $f \in K[X]$ es separable.*

Demostración. Gracias a 14.8.4, sería suficiente probar que para todo polinomio irreducible

$$f = a_n\,X^n + a_{n-1}\,X^{n-1} + \cdots + a_1\,X + a_0 \in K[X]$$

donde $a_n \neq 0$ se tiene

$$f' = n\,a_n\,X^{n-1} + (n-1)\,a_{n-1}\,X^{n-2} + \cdots + a_1 \neq 0.$$

Si $\operatorname{char} K = 0$, entonces $n\,a_n \neq 0$ y por ende $f' \neq 0$. Asumamos que $\operatorname{char} K = p$ y todo elemento de K es una p-ésima potencia. Notamos que si $f' = 0$, entonces $i \cdot a_i = 0$ para todo $i = 1, \ldots, n$; es decir, $a_i = 0$ o $p \mid i$. Esto significa que el polinomio tiene forma

$$f = b_m\,X^{mp} + b_{m-1}\,X^{(m-1)\,p} + \cdots + b_1\,X^p + b_0$$

para algunos $b_0, b_1, \ldots, b_m \in K$. Por nuestra hipótesis, todo b_i es una potencia p-ésima en K, así que

$$f = c_m^p\,X^{mp} + c_{m-1}^p\,X^{(m-1)\,p} + \cdots + c_1^p\,X^p + c_0^p = (c_m\,X^m + c_{m-1}\,X^{m-1} + \cdots + c_1\,X + c_0)^p$$

(usando que $\operatorname{char} K = p$). Pero esto contradice la irreducibilidad de f. Entonces, $f' \neq 0$. ■

14.8.11. Corolario. *Si K es un cuerpo perfecto, entonces toda extensión algebraica L/K es separable.*

Teorema del elemento primitivo

El siguiente resultado simplifica mucho el estudio de extensiones de cuerpos K/F: resulta que en muchos casos son **simples**; es decir de la forma $K = F(\theta)$ para algún $\theta \in K$.

14.8.12. Teorema del elemento primitivo. *Sea K/F una extensión finita de cuerpos tal que $K = F(\alpha_1, \ldots, \alpha_n)$, donde $\alpha_2, \ldots, \alpha_n \in K$ son separables*[*]*. Luego, existe un elemento $\theta \in K$ tal que $K = F(\theta)$.*

Demostración [vdW1991, §6.10]. Consideremos primero el caso de $n = 2$. Sea entonces $K = F(\alpha, \beta)$, donde β es separable sobre F. Sea $f := m_{\alpha,F}$ el polinomio mínimo de α sobre F y $g := m_{\beta,F}$ el polinomio mínimo de β sobre F. Sea L/K una extensión donde f y g se descomponen en factores lineales y sean

$$\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_r \in L$$

las raíces diferentes de f en L y sean

$$\beta_1 := \beta, \beta_2, \ldots, \beta_s \in L$$

las raíces de g (son todas diferentes, dado que β es separable).

Notamos que sin pérdida de generalidad, se puede asumir que F es un cuerpo infinito. En el caso contrario, K también sería un cuerpo finito, y luego $K = F(\theta)$ donde θ es un generador del grupo cíclico $K^\times$.

Notamos que $\beta_j \neq \beta_1$ para $j \neq 1$, así que la ecuación

$$\alpha_i + x\,\beta_j = \alpha_1 + x\,\beta_1$$

tiene a lo sumo una raíz $x \in F$ para cualesquiera $i = 1, \ldots, r$ y $j = 2, \ldots, s$. Gracias a nuestra hipótesis de que F sea infinito, existe un elemento $c \in F$ que es distinto de las raíces de las ecuaciones de arriba:

$$\alpha_i + c\,\beta_j \neq \alpha_1 + c\,\beta_1 \quad \text{para } i = 1, \ldots, r,\ j = 2, \ldots, s.$$

Pongamos

$$\theta := \alpha_1 + c\,\beta_1 = \alpha + c\,\beta.$$

Tenemos $\theta = F(\alpha, \beta)$. Si logramos probar que $\beta \in F(\theta)$, entonces también $\alpha = \theta - c\,\beta \in F(\theta)$ y $F(\alpha, \beta) = F(\theta)$. Notamos que

$$g(\beta) = 0, \quad f(\alpha) = f(\theta - c\,\beta) = 0$$

y los polinomios $g \in F[X]$ y $f(\theta - c\,X) \in F(\theta)[X]$ no pueden tener más de una raíz común por nuestra elección de c: se tiene

$$\theta - c\,\beta_j \neq \alpha_i \quad \text{para } i = 1, \ldots, r,\ j = 2, \ldots, s,$$

así que $f(\theta - c\,\beta_j) \neq 0$ para $j \neq 1$. Calculamos

$$\operatorname{mcd}(g, f(\theta - c\,X)) = h \quad \text{en } F(\theta)[X]$$

[*]Sic. La separabilidad de α_1 no será necesaria en la prueba.

para algún polinomio mónico $h \in F(\theta)[X]$. Notamos que $\deg h > 0$: dado que $g(\beta) = f(\theta - c\,\beta) = 0$, ambos polinomios g y $f(\theta - c\,X)$ deben ser divisibles por el polinomio mínimo $m_{\beta,F(\theta)}$. En $L[X]$ el polinomio h se descompone en factores lineales y toda raíz de h es una raíz de g y $f(\theta - c\,X)$. Pero β es la única raíz común de g y $f(\theta - c\,X)$ y g no tiene raíces múltiples, así que necesariamente $h = X - \beta$. Esto nos permite concluir que $\beta \in F(\theta)$.

Esto termina la prueba en el caso de $n = 2$. En el caso general, podemos proceder por inducción sobre n. Asumamos que el resultado es válido para $n - 1$ y se tiene

$$F(\alpha_1, \ldots, \alpha_{n-1}) = F(\eta)$$

para algún $\eta \in K$. Luego,

$$F(\alpha_1, \ldots, \alpha_n) = F(\eta, \alpha_n) = F(\theta)$$

por el caso de dos generadores. ■

14.8.13. Corolario. *Si F es un cuerpo perfecto, entonces toda extensión finita K/F es simple: existe $\theta \in K$ tal que $K = F(\theta)$.*

14.8.14. Ejemplo. Consideremos la extensión $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Los polinomios mínimos de $\sqrt[3]{2}$ y ζ_3 sobre $\mathbb{Q}$ son

$$X^3 - 2 \quad \text{y} \quad X^2 + X + 1$$

respectivamente. Sus raíces complejas son

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \zeta_3\sqrt[3]{2}, \quad \alpha_3 = \zeta_3^2\sqrt[3]{2}, \quad \beta_1 = \zeta_3, \quad \beta_2 = \zeta_3^2.$$

La prueba del teorema nos dice que hay que escoger $c \in \mathbb{Q}$ tal que

$$\begin{aligned}
\sqrt[3]{2} + c\,\zeta_3^2 &\neq \sqrt[3]{2} + c\,\zeta_3,\\
\zeta_3\sqrt[3]{2} + c\,\zeta_3^2 &\neq \sqrt[3]{2} + c\,\zeta_3,\\
\zeta_3^2\sqrt[3]{2} + c\,\zeta_3^2 &\neq \sqrt[3]{2} + c\,\zeta_3.
\end{aligned}$$

Se ve que funciona $c = 1$, y luego

$$\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2} + \zeta_3).$$

▲

14.8.15. Ejemplo. Consideremos la extensión $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ donde m, n y mn no son cuadrados. Tenemos polinomios mínimos $X^2 - m$ y $X^2 - n$ y sus raíces

$$\alpha_1 = \sqrt{m}, \quad \alpha_2 = -\sqrt{m}, \quad \beta_1 = \sqrt{n}, \quad \beta_2 = -\sqrt{n}.$$

Necesitamos encontrar $c \in \mathbb{Q}$ tal que

$$\begin{aligned}
\sqrt{m} - c\,\sqrt{n} &\neq \sqrt{m} + c\,\sqrt{n},\\
-\sqrt{m} - c\,\sqrt{n} &\neq \sqrt{m} + c\,\sqrt{n}.
\end{aligned}$$

Basta tomar $c = 1$, así que

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n}).$$

▲

14.9 Cerradura algebraica

En §14.7 para un polinomio $f \in K[X]$ hemos construido una extensión L/K donde f se descompone en factores lineales; es decir, una extensión que contiene todas las raíces de f. En general, para cualquier cuerpo K se puede construir su **cerradura algebraica** que es una extensión $\overline{K}/K$ que contiene las raíces de *todos* los polinomios $f \in K[X]$.

14.9.1. Proposición. *Sea K un cuerpo. Las siguientes condiciones son equivalentes:*

1) *todo polinomio no constante en $K[X]$ tiene una raíz en K;*

2) *todo polinomio de grado $n > 0$ en $K[X]$ tiene n raíces en K, contándolas con multiplicidades; es decir,*
$$f = c\,(X - \alpha_1) \cdots (X - \alpha_n)$$
para $\alpha_1, \ldots, \alpha_n \in K$;

3) *todo polinomio irreducible en $K[X]$ es lineal;*

4) *K no tiene extensiones algebraicas propias: si L/K es una extensión algebraica, entonces $L = K$.*

Demostración. 1) $\Rightarrow$ 2): si f es un polinomio de grado $n > 0$ y f tiene una raíz $\alpha \in K$, entonces $f = (X - \alpha)\, g$, donde $\deg g = n - 1$. Luego, g también debe tener una raíz, etcétera. Continuando de esta manera, se obtiene una descomposición $f = c\,(X - \alpha_1) \cdots (X - \alpha_n)$.

2) $\Rightarrow$ 3): está claro.

3) $\Rightarrow$ 4): si L/K es una extensión algebraica, entonces para todo $\alpha \in L$ el polinomio mínimo $m_{\alpha,K}$ debe ser lineal según 3), lo que significa que $\alpha \in K$.

4) $\Rightarrow$ 1): para un polinomio no constante f, escribamos $f = g\,h$ donde g es irreducible. Luego, $L := K[X]/(g)$ es una extensión finita de grado $[L : K] = \deg g$, pero según 4), tenemos $L = K$, así que $\deg g = 1$. ■

14.9.2. Definición. Un cuerpo K que satisface las condiciones equivalentes de la proposición anterior se llama **algebraicamente cerrado**.

El siguiente resultado debe de ser conocido al lector.

14.9.3. "Teorema fundamental del álgebra". *El cuerpo de los números complejos $\mathbb{C}$ es algebraicamente cerrado.*

La construcción de los números complejos es *analítica*: primero hay que construir los números reales $\mathbb{R}$ como la completación de los números racionales $\mathbb{Q}$ considerando las sucesiones de Cauchy en $\mathbb{Q}$ respecto a la relación de equivalencia

$$(x_n) \equiv (x'_n) \iff \lim_{n\to\infty} (x_n - x'_n) = 0,$$

y luego pasar al cuerpo $R(\sqrt{-1}) := \mathbb{R}[X]/(X^2 + 1)$. Se conocen muchas pruebas del teorema fundamental del álgebra, y una de estas puede ser encontrada el el apéndice E.

14.9.4. Digresión. Se puede tomar la completación de los números racionales $\mathbb{Q}$ respecto a la **norma p-ádica**

$$\left|\frac{x}{y}\right|_p := v_p(x) - v_p(y)$$

—véase el capítulo anterior para una breve discusión de las valuaciones p-ádicas y mis apuntes

http://cadadr.org/san-salvador/2018-04-topologia-p-adica/topologia-p-adica.pdf

El resultado de esta completación es el cuerpo de los **números p-ádicos** $\mathbb{Q}_p$. Este cuerpo no es algebraicamente cerrado y se puede tomar su cerradura algebraica $\overline{\mathbb{Q}_p}$. Sin embargo, $\overline{\mathbb{Q}_p}$ deja de ser completo (no todas sucesiones de Cauchy convergen en $\overline{\mathbb{Q}_p}$). Luego, se puede tomar de nuevo la completación de $\overline{\mathbb{Q}_p}$ que se denota por $\mathbb{C}_p$. Resulta que $\mathbb{C}_p$ es un cuerpo algebraicamente cerrado.

$$\mathbb{Q} \rightsquigarrow \mathbb{Q}_p \text{ compl., no alg. cerr.} \rightsquigarrow \overline{\mathbb{Q}_p} \text{ no compl., alg. cerr.} \rightsquigarrow \mathbb{C}_p \text{ compl., alg. cerr..}$$

Para los detalles, véase [Kob1984].

14.9.5. Definición. Para un cuerpo K, se dice que una extensión $\overline{K}/K$ es una **cerradura algebraica** de K si

1) $\overline{K}/K$ es una extensión algebraica;

2) el cuerpo $\overline{K}$ es algebraicamente cerrado.

14.9.6. Ejemplo. Los números complejos $\mathbb{C}$ forman una cerradura algebraica de los números reales $\mathbb{R}$. ▲

Existencia de cerradura algebraica

14.9.7. Teorema. *Para todo cuerpo K existe una cerradura algebraica $\overline{K}$.*

Demostración. Consideremos el anillo de polinomios $K[X_f]$, donde cada variable X_f corresponde a un polinomio mónico no constante $f \in K[X]$. (Este anillo es muy grande.)

Sea I el ideal en $K[X_f]$ generado por los polinomios $f(X_f)$ para todo polinomio mónico irreducible $f \in K[X]$. Este ideal es propio. En efecto, en el caso contrario existen algunos polinomios $g_1, \ldots, g_n \in K[X_f]$ y $f_1, \ldots, f_n \in K[X]$ tales que

$$1 = g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}).$$

Sea L/K una extensión finita donde cada uno de los polinomios f_i tiene una raíz $\alpha_i \in L$. Consideremos el homomorfismo de evaluación

$$\begin{aligned} \phi\colon K[X_f] &\to L, \\ X_{f_i} &\mapsto \alpha_i, \text{ para } i = 1, \ldots, n, \\ X_f &\mapsto 0, \text{ si } f \neq f_i \text{ para } i = 1, \ldots, n. \end{aligned}$$

Luego,

$$\phi\Big(g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n})\Big) = 0,$$

pero esto significa que

$$g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) \neq 1.$$

Siendo un ideal propio, I está contenido en un ideal maximal $\mathfrak{m} \subset K[X_f]$. Consideremos el cuerpo $K_1 := K[X_f]/\mathfrak{m}$. Por la construcción, todo polinomio no constante $f \in K[X]$ tiene una raíz en K_1. En efecto, bastaría considerar el caso cuando f es mónico. Denotemos por $\alpha_f \in K_1$ la imagen de X_f en el cociente. Entonces, $f(\alpha_f) = 0$. Notamos que los elementos α_f son algebraicos sobre K, y entonces el cuerpo K_1, siendo generado por los α_f, es una extensión algebraica de K.

De la misma manera, se puede construir una extensión K_2/K_1 tal que todo polinomio no constante $f \in K_1[X]$ tiene una raíz en K_2, etcétera. Esto nos da una torre de extensiones algebraicas

$$K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$$

Pongamos

$$\overline{K} := \bigcup_{i \geq 1} K_i.$$

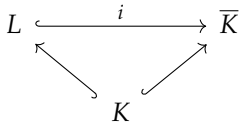
Esto es una extensión algebraica de K. Además, para cualquier polinomio no constante $f \in \overline{K}[X]$ sus coeficientes pertenecen a algún K_n para n suficientemente grande, así que f tiene una raíz en K_{n+1}. Entonces, $\overline{K}$ es un cuerpo algebraicamente cerrado. ■

14.9.8. Comentario. La prueba de arriba pertenece a Emil Artin. En efecto, un análisis más cuidadoso demuestre que no es necesario iterar la construcción y el cuerpo K_1 ya es algebraicamente cerrado. Para los detalles, véase la nota de Keith Conrad

http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/algclosure.pdf

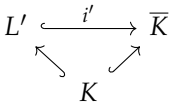
"Unicidad" de cerradura algebraica

14.9.9. Lema. *Sean $\overline{K}/K$ una cerradura algebraica de K y L/K una extensión algebraica. Entonces, existe un encajamiento*



La prueba es una aplicación típica del lema de Zorn*.

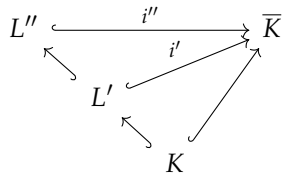
Demostración. Sea $\mathcal{P}$ el conjunto que consiste en pares de elementos (L', i') donde $K \subseteq L' \subseteq L$ es una subextensión e i' es un encajamiento de L' en $\overline{K}$:



*Nuestra construcción de una cerradura algebraica también usa el lema de Zorn, pero escondido en el resultado sobre la existencia de ideales maximales.

Este conjunto no es vacío: $(K, i) \in \mathcal{P}$. Este conjunto es parcialmente ordenado por la relación

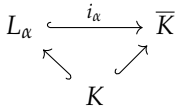
$$(L', i') \preceq (L'', i'') \iff L' \subseteq L'' \text{ y } i''\big|_{L'} = i'.$$



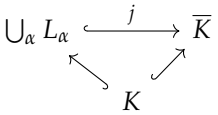
Es fácil comprobar que toda cadena ascendente en $\mathcal{P}$ tiene una cota superior: para una cadena $\{(L_\alpha, i_\alpha)\}_\alpha$ podemos tomar

$$\bigcup_\alpha L_\alpha.$$

Puesto que L_α es una cadena, se ve que la unión es un cuerpo. Las inclusiones



inducen una inclusión



definida por $j(\alpha) := i_\alpha(\alpha)$ si $\alpha \in L_\alpha$ (esta aplicación está bien definida y hace parte del diagrama conmutativo de arriba, dado que $\{(L_\alpha, i_\alpha)\}_\alpha$ es una cadena).

Entonces, el lema de Zorn nos dice que $\mathcal{P}$ tiene un elemento maximal (F, i). Para concluir la prueba, vamos a ver que $F = L$. Todo elemento $x \in L$ es algebraico sobre K, y entonces es algebraico sobre F. Sea $f := m_{x,F} \in F[X]$ el polinomio mínimo de x sobre F. Tenemos

$$F(x) \cong F[X]/(f).$$

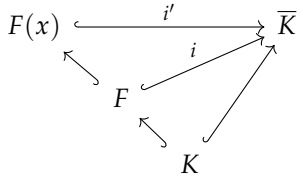
El polinomio f tiene una raíz $\alpha \in \overline{K}$. Consideremos el homomorfismo

$$\begin{aligned} \mathrm{ev}_\alpha \colon F[X] &\to \overline{K}, \\ \sum_{k\geq 0} a_k X^k &\mapsto \sum_{k\geq 0} i(a_k)\, \alpha^k. \end{aligned}$$

Tenemos $f \in \ker \mathrm{ev}_\alpha$, así que este homomorfismo induce un homomorfismo

$$i' \colon F(x) \cong F[X]/(f) \to \overline{K}$$

que es necesariamente inyectivo, dado que $F(x)$ es un cuerpo, y que extiende a i:



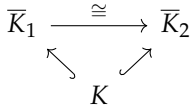
Entonces,

$$(F, i) \preceq (F(x), i').$$

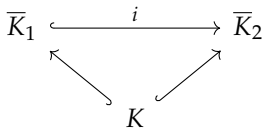
Sin embargo, la maximalidad de (F, i) implica que $F = F(x)$. Esto se cumple para cualquier $x \in L$, así que $F = L$. ■

De este lema se deduce que las cerraduras algebraicas son isomorfas entre sí.

14.9.10. Teorema. *Sean $K \hookrightarrow \overline{K}_1$ y $K \hookrightarrow \overline{K}_2$ dos cerraduras algebraicas. Entonces, existe un isomorfismo*



Demostración. Aplicando el lema anterior a $L = \overline{K}_1$ y $\overline{K} = \overline{K}_2$, se obtiene un encajamiento



Sin embargo, i es necesariamente sobreyectivo. En efecto, un elemento $y \in \overline{K}_2$ es una raíz de algún polinomio mónico irreducible $f \in K[X]$. Luego, f se factoriza como $(X - x_1) \cdots (X - x_n)$ en $\overline{K}_1[X]$, así que $y = i(x_k)$ para algún $k = 1, \ldots, n$. ■

El isomorfismo $\overline{K}_1 \cong \overline{K}_2$ que acabamos de obtener no es único en ningún sentido y por este motivo no hay que hablar de "la cerradura algebraica", sino de elección de *una cerradura algebraica*. De hecho, normalmente una cerradura algebraica $\overline{K}/K$ tiene muchos automorfismos no triviales $\overline{K} \xrightarrow{\cong} \overline{K}$; para un ejemplo particular, véase el siguiente capítulo.

14.10 Ejercicios

Ejercicio 14.1. *Sea K un cuerpo y*

$$f = X^n + a_{n-1}\,X^{n-1} + \cdots + a_1\,X + a_0 \in K[X]$$

un polinomio irreducible. Denotemos por α la imagen de X en el cociente $L := K[X]/(f)$. Encuentre una fórmula explícita para α^{-1} en términos de la base $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.

Ejercicio 14.2. *Consideremos el polinomio $f := X^3 + X^2 + X + 2 \in \mathbb{Q}[X]$.*

1) *Demuestre que f es irreducible.*

2) *Denotemos por α la imagen de X en el cociente $K := \mathbb{Q}[X]/(f)$. Exprese los elementos*

$$(\alpha^2 + \alpha + 1)\,(\alpha^2 + \alpha), \quad (\alpha - 1)^{-1} \in K$$

en términos de la base $1, \alpha, \alpha^2$.

Ejercicio 14.3. *Encuentre un polinomio cúbico irreducible $f \in \mathbb{F}_2[X]$ y considere el cuerpo $k := \mathbb{F}_2[X]/(f)$. Verifique directamente que el grupo $k^\times$ es cíclico mostrando que todos sus elementos son potencias de un generador.*

Ejercicio 14.4. *Sea n un número entero. Encuentre el polinomio mínimo sobre $\mathbb{Q}$ para $n + \sqrt{-1} \in \mathbb{C}$.*

Ejercicio 14.5. *Para una extensión L/K y un elemento algebraico $\alpha \in L$ asumamos que el grado $[K(\alpha) : K]$ es impar. Demuestre que $K(\alpha) = K(\alpha^2)$.*

Ejercicio 14.6. *Para $p = 2, 3$ demuestre que el polinomio $X^3 - p$ es irreducible en $K[X]$ donde $K = \mathbb{Q}(\sqrt{-1})$.*
Sugerencia: considere la extensión $\mathbb{Q}(\sqrt{-1}, \sqrt[3]{p})/\mathbb{Q}$.

Ejercicio 14.7. *Sean $m, n \in \mathbb{Z}$ dos números enteros tales que $\sqrt{m}, \sqrt{n} \notin \mathbb{Q}$. Consideremos $\alpha := \sqrt{m} + \sqrt{n} \in \mathbb{C}$.*

1) *Demuestre que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.*

2) *Para*

$$\alpha_1 := \alpha, \quad \alpha_2 := -\sqrt{m} + \sqrt{n}, \quad \alpha_3 := -\alpha_1, \quad \alpha_4 := -\alpha_2,$$

demuestre que el polinomio $f := (X - \alpha_1)\,(X - \alpha_2)\,(X - \alpha_3)\,(X - \alpha_4)$ tiene coeficientes enteros.

3) *Demuestre que si $\sqrt{mn} \notin \mathbb{Q}$, entonces f es el polinomio mínimo de α sobre $\mathbb{Q}$.*

4) *Demuestre que si $\sqrt{mn} \in \mathbb{Q}$, entonces $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$.*

Polinomios y cuerpos ciclotómicos

Ejercicio 14.8. *Demuestre que si $m > 1$ es impar, entonces $\Phi_{2m} = \Phi_m(-X)$.*
Sugerencia: compare las expresiones

$$\prod_{d|2m} \Phi_d = X^{2m} - 1 = (X^m - 1)\,(X^m + 1) = -(X^m - 1)\,((-X)^m - 1) = -\prod_{d|m} \Phi_d(X)\,\Phi_d(-X)$$

usando la inducción sobre m.

Ejercicio 14.9. *Encuentre un par de cuerpos ciclotómicos $\mathbb{Q}(\zeta_m)$ y $\mathbb{Q}(\zeta_n)$ tales que $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ pero $\mathbb{Q}(\zeta_m) \ncong \mathbb{Q}(\zeta_n)$.*

Ejercicio 14.10. *Demuestre que toda extensión finita $K/\mathbb{Q}$ contiene un número finito de las raíces de la unidad.*

Ejercicio 14.11. *Denotemos por $\mathbb{Q}(\zeta_\infty) = \mathbb{Q}(\zeta_3, \zeta_4, \zeta_5, \zeta_6, \ldots)$ la extensión de $\mathbb{Q}$ generada por todas las raíces de la unidad. Demuestre que $\mathbb{Q}(\zeta_\infty) = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_n)$.*

Derivadas formales

Ejercicio 14.12. *Sea R un anillo conmutativo. Para una serie de potencias $f = \sum_{n\geq 0} a_n\, X^n \in R[\![X]\!]$ definamos su **derivada formal** como la serie*

$$f' := \sum_{n\geq 1} n\, a_n\, X^{n-1}.$$

1) Demuestre que para cualesquiera $f, g \in R[\![X]\!]$ se cumple

$$(f + g)' = f' + g', \quad (fg)' = f'g + fg'.$$

2) Calcule las derivadas de las siguientes series formales en $\mathbb{Q}[\![X]\!]$:

$$\exp(X) := \sum_{n\geq 0} \frac{X^n}{n!}, \quad \log(1 + X) := \sum_{n\geq 0} (-1)^{n+1} \frac{X^n}{n},$$
$$\operatorname{sen}(X) := \sum_{n\geq 0} (-1)^n\, \frac{X^{2n+1}}{(2n+1)!}, \quad \cos(X) := \sum_{n\geq 0} (-1)^n\, \frac{X^{2n}}{(2n)!}.$$

Ejercicio 14.13 (Serie de Taylor). *Demuestre que si $\mathbb{Q} \subseteq R$, entonces para $f \in R[\![X]\!]$ se cumple*

$$f = \sum_{n\geq 0} \frac{f^{(n)}(0)}{n!}\, X^n,$$

donde $f^{(0)} := f$ y $f^{(n)} := (f^{(n-1)})'$ para $n \geq 1$.

Ejercicio 14.14. *Si $\mathbb{Q} \subseteq R$, definamos las **integrales formales** por*

$$\int_0^X \left(\sum_{n\geq 0} a_n\, X^n \right) dX := \sum_{n\geq 0} \frac{a_n}{n+1}\, X^{n+1}.$$

1) *Demuestre que se cumple el* ***teorema fundamental del cálculo****:*

$$\int_0^X f'(X)\,dX = f(X) - f(0) \quad y \quad \left(\int_0^X f(X)\,dX\right)' = f(X),$$

donde $f(0)$ denota el término constante de f.

2) *Demuestre que se cumple la* ***integración por partes****:*

$$f(X)\,g(X) - f(0)\,g(0) = \int_0^X f(X)\,g'(X)\,dX + \int_0^X f'(X)\,g(X)\,dX.$$

3) *Calcule las series*

$$\int_0^X \exp(X)\,dX, \quad \int_0^X \log(1+X)\,dX, \quad \int_0^X X\,\exp(X)\,dX.$$

La traza, norma y el polinomio característico

Ejercicio 14.15. *Consideremos la extensión ciclotómica $\mathbb{Q}(\zeta_3)/\mathbb{Q}$.*

1) *Usando la base $1, \zeta_3$, calcule el polinomio característico para un elemento $\alpha := a + b\,\zeta_3$, donde $a, b \in \mathbb{Q}$.*

2) *Note que $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Verifique que el resultado de 1) coincide con el cálculo para las extensiones cuadráticas que hicimos en clase.*

Ejercicio 14.16. *Demuestre que $1 + \sqrt[3]{2}$ no es una n-ésima potencia en $\mathbb{Q}(\sqrt[3]{2})$ para ningún $n = 2, 3, 4, \ldots$*

Ejercicio 14.17. *Consideremos $\alpha := \zeta_5 + \zeta_5^2$, donde $\zeta_5 := e^{2\pi\sqrt{-1}/5}$.*

1) *Calcule el polinomio característico de α respecto a la extensión ciclotómica $\mathbb{Q}(\zeta_5)/\mathbb{Q}$.*

2) *Demuestre que $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\alpha)$ y el polinomio obtenido es el polinomio mínimo de α.*

Ejercicio 14.18. *Encuentre el polinomio mínimo de $\sqrt{2} + \sqrt[3]{2}$ sobre $\mathbb{Q}$.*

Separabilidad y el teorema del elemento primitivo

Ejercicio 14.19. *Sea p un número primo. Consideremos el polinomio $f := X^2 + X + 1 \in \mathbb{F}_p[X]$.*

1) *Demuestre que f es irreducible si y solo si $p \equiv 2 \pmod 3$.*

   Indicación: use la ley de reciprocidad cuadrática para ver cuándo $\sqrt{-3} \notin \mathbb{F}_p$; otra opción es notar que se trata del tercer polinomio ciclotómico.

2) *¿Para cuáles p el polinomio f es separable?*

Ejercicio 14.20. *¿Para cuáles p el polinomio $f := X^2 + X + 2 \in \mathbb{F}_p[X]$ es irreducible? ¿separable?*

Ejercicio 14.21. *Sean p un número primo y $a \in \mathbb{F}_p$ un elemento no nulo. Consideremos el polinomio*

$$f := X^p - X + a \in \mathbb{F}_p[X].$$

En este ejercicio vamos a probar que f es irreducible.

1) *Demuestre que f es separable.*

2) *Sea L un cuerpo de descomposición de f y sea $\alpha \in L$ un elemento tal que $f(\alpha) = 0$. Demuestre que las raíces de f en L son $\alpha, \alpha + 1, \ldots, \alpha + p - 1$.*

3) *Asumamos que $f = gh$ donde $g, h \in \mathbb{F}_p[X]$ son polinomios mónicos y $\deg g, \deg h < \deg f$. Analizando la suma de las raíces de g o h, concluya que $\alpha \in \mathbb{F}_p$.*

4) *Demuestre que en este caso f se descompone en factores lineales en $\mathbb{F}_p[X]$ y deduzca una contradicción.*

Ejercicio 14.22. *Sean p un primo impar y n un número natural tal que $p \nmid n$. Denotemos por $\Phi_n \in \mathbb{Z}[X]$ el n-ésimo polinomio ciclotómico. Demuestre que si $a \in \mathbb{Z}$ satisface $\Phi_n(a) \equiv 0 \pmod{p}$, entonces $p \nmid a$ y el orden de a en $(\mathbb{Z}/p\mathbb{Z})^\times$ es igual a n.*
Indicación: factorice $X^n - 1 \in \mathbb{Z}[X]$ en polinomios ciclotómicos y note que el polinomio $X^n - 1 \in \mathbb{F}_p[X]$ es separable.

Ejercicio 14.23. *Consideremos la extensión $K := \mathbb{Q}(\sqrt{-1}, \sqrt[3]{2})$. Encuentre $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$.*

Capítulo 15
Cuerpos finitos

> ...as a longtime worker using only real or complex numbers, [Joseph F. Ritt] referred to finite fields as "monkey fields".
>
> Steven Krantz, "Mathematical Apocrypha Redux"

En este capítulo vamos a construir los cuerpos finitos y ver sus propiedades básicas.

15.0.1. Observación. *Todo cuerpo finito tiene p^n elementos donde p es algún número primo y $n = 1, 2, 3, \ldots$*

Demostración. Un cuerpo finito necesariamente tiene característica p para algún número primo p, y entonces es una extensión finita de $\mathbb{F}_p$. En particular, es un espacio vectorial de dimensión finita n sobre $\mathbb{F}_p$ que tiene p^n elementos. ■

15.0.2. Teorema. *Para todo primo p y $n = 1, 2, 3, \ldots$ existe un cuerpo finito de p^n elementos; específicamente, es un cuerpo de descomposición del polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$. En particular, es único salvo isomorfismo.*

Demostración. Consideremos una extensión $\mathbb{F}/\mathbb{F}_p$. Notamos que el polinomio $f := X^{p^n} - X \in \mathbb{F}_p[X]$ no tiene raíces múltiples en $\mathbb{F}$: en efecto, si en $\mathbb{F}[X]$ se tiene

$$X^{p^n} - X = (X - \alpha)^2 \, g$$

para algún X, entonces, tomando las derivadas formales en $\mathbb{F}[X]$, se obtiene

$$-1 = p^n \, X^{p^n - 1} - 1 = 2 \, (X - \alpha) \, g + (X - \alpha)^2 \, g',$$

de donde $(X - \alpha) \mid -1$, lo que es absurdo.

1) Sea $\mathbb{F}/\mathbb{F}_p$ un cuerpo de descomposición de f. Por lo que acabamos de probar, $\mathbb{F}$ contiene p^n raíces distintas de f. Notamos que las raíces de f forman un subcuerpo

de $\mathbb{F}$. En efecto, está claro que $f(0) = f(1) = 0$. Sean $\alpha, \beta \in \mathbb{F}$ elementos tales que $f(\alpha) = f(\beta) = 0$; es decir, $\alpha^{p^n} = \alpha$ y $\beta^{p^n} = \beta$. Luego,

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\,\beta^{p^n} = \alpha\beta,$$

y además

$$(\alpha+\beta)^{p^n} = \sum_{i+j=p^n} \binom{p^n}{i}\,\alpha^i\,\beta^j = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

usando que $p \mid \binom{p^n}{i}$ para todo $i = 1, \ldots, p^n - 1$. En fin, si $\alpha \neq 0$, entonces

$$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}.$$

Por la minimalidad de los cuerpos de descomposición, esto significa que todos los elementos de $\mathbb{F}$ son raíces del polinomio f cuyo grado es p^n, así que $|\mathbb{F}| = p^n$.

2) Viceversa, notamos que si $\mathbb{F}$ es un cuerpo de p^n elementos, entonces $\mathbb{F}$ tiene característica p y $\mathbb{F}_p \subseteq \mathbb{F}$. El grupo multiplicativo $\mathbb{F}^\times$ tiene orden $p^n - 1$, así que todo elemento $\alpha \in \mathbb{F}^\times$ satisface $\alpha^{p^n-1} = 1$ según el teorema de Lagrange, así que $\alpha^{p^n} = \alpha$. Para $\alpha = 0$ esto también trivialmente se cumple. Luego, todos los p^n elementos de $\mathbb{F}$ son raíces del polinomio $f := X^{p^n} - X \in \mathbb{F}_p[X]$ de grado p^n, así que $\mathbb{F}$ es un cuerpo de descomposición de f. Recordemos que un cuerpo de descomposición es único salvo isomorfismo.

■

15.0.3. Notación. En vista del último resultado, se suele hablar de *el cuerpo* de p^n elementos y se usa la notación $\mathbb{F}_{p^n}$, o $\mathbb{F}_q$ donde $q = p^n$.

15.0.4. Comentario. Note que para $n > 1$ el anillo $\mathbb{Z}/p^n\mathbb{Z}$ (los restos módulo p^n) tiene divisores de cero, y en particular no es un cuerpo. Entonces, $\mathbb{F}_{p^n}$ es algo muy diferente de $\mathbb{Z}/p^n\mathbb{Z}$.

Para construir los cuerpos finitos de manera más explícita, notamos que si $\mathbb{F}_{p^n}$ es un cuerpo de p^n elementos, entonces el grupo $\mathbb{F}_{p^n}^\times$ es cíclico (véase el capítulo 7); es decir, existe un generador $\alpha \in \mathbb{F}_{p^n}^\times$ tal que

$$\mathbb{F}_{p^n} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}.$$

Sea $f := m_{\alpha,\mathbb{F}_p}$ el polinomio mínimo de α sobre $\mathbb{F}_p$. Tenemos

$$\mathbb{F}_p[X]/(f) \cong \mathbb{F}_p(\alpha), \quad [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg f.$$

Pero $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$, así que $\deg f = n$. Esto nos da el siguiente resultado.

15.0.5. Teorema. *Para todo primo p y $n = 1, 2, 3, \ldots$ existe un polinomio irreducible $f \in \mathbb{F}_p[X]$ de grado n.*

15.0.6. Comentario. Si f es un polinomio irreducible en $\mathbb{F}_p[X]$ y $\mathbb{F} := \mathbb{F}_p[X]/(f)$, denotemos por α la imagen de X en el cociente. Este α *no tiene por qué* ser un generador del grupo multiplicativo $\mathbb{F}^\times$. Por ejemplo, consideremos un cuerpo finito de 9 elementos $\mathbb{F} := \mathbb{F}_3[X]/(X^2+1)$. En este caso $\alpha^2 = -1$, y luego $\alpha^4 = 1$. Siendo un grupo cíclico de 8 elementos, $\mathbb{F}^\times$ tiene $\phi(8) = 4$ diferentes generadores y son $\alpha+1$, $\alpha+2$, $2\alpha+1$, $2\alpha+2$.

15.0.7. Ejemplo. He aquí algunos polinomios irreducibles en $\mathbb{F}_p[X]$.

$\underline{p=2}$	$\underline{p=3}$	$\underline{p=5}$
X^2+X+1	X^2+X+2	X^2+X+1
X^3+X^2+1	X^3+X^2+X+2	X^3+X^2+3X+4
$X^4+X^3+X^2+X+1$	$X^4+X^3+X^2+X+1$	$X^4+X^3+2X^2+X+3$
$X^5+X^4+X^2+X+1$	$X^5+X^4+2X^3+1$	$X^5+X^4+X^3+2X^2+3X+1$
$X^6+X^5+X^3+X^2+1$	$X^6+X^5+X^4+X^3+X^2+X+1$	$X^6+X^5+X^4+X^3+X^2+X+1$

▲

Entonces, para construir un cuerpo de p^n elementos, se puede tomar un polinomio irreducible $f \in \mathbb{F}_p[X]$ de grado n y pasar al cociente $\mathbb{F}_p[X]/(f)$. Diferentes f dan el mismo resultado, salvo isomorfismo.

15.0.8. Ejemplo. Los polinomios

$$f_1 := X^3+X+1,\ f_2 := X^3+X^2+1 \in \mathbb{F}_2[X]$$

son irreducibles y tiene que haber un isomorfismo entre los cuerpos finitos correspondentes

$$\begin{array}{ccc} \mathbb{F}_2[X]/(f_1) & \xrightarrow{\quad\cong\quad} & \mathbb{F}_2[X]/(f_2) \\ & \nwarrow \quad \nearrow & \\ & \mathbb{F}_2 & \end{array}$$

Vamos a definir un homomorfismo

$$\phi\colon \mathbb{F}_2[X] \to \mathbb{F}_2[X] \twoheadrightarrow \mathbb{F}_2[X]/(f_2)$$

tal que $\ker\phi = (f_1)$. En este caso el primer teorema de isomorfía nos daría un homomorfismo inyectivo

$$\overline{\phi}\colon \mathbb{F}_2[X]/(f_1) \xrightarrow{\cong} \operatorname{im}\phi \hookrightarrow \mathbb{F}_2[X]/(f_2),$$

y dado que $|\mathbb{F}_2[X]/(f_1)| = |\mathbb{F}_2[X]/(f_2)| = 8$, este sería automáticamente sobreyectivo. Necesitamos que se cumpla

$$\phi(f_1) = \phi(X^3+X+1) = \phi(X)^3+\phi(X)+1 \equiv 0 \pmod{X^3+X^2+1}.$$

Se ve que hay tres opciones:

$$\phi_1\colon X \mapsto \overline{X+1},\quad \phi_2\colon X \mapsto \overline{X^2+1},\quad \phi_3\colon X \mapsto \overline{X^2+X}.$$

Cada una de estas aplicaciones induce un isomorfismo $\mathbb{F}_2[X]/(f_1) \cong \mathbb{F}_2[X]/(f_2)$. Notamos que los elementos $\overline{X+1}, \overline{X^2+1}, \overline{X^2+X} \in \mathbb{F}_2[X]/(f_2)$ están relacionados de la siguiente manera:

$$\overline{X^2+1} = (\overline{X+1})^2, \quad \overline{X^2+X} = (\overline{X^2+1})^2 = (\overline{X+1})^4$$

(véase §15.2). ▲

Sería interesante saber cuántas posibilidades hay para escoger al polinomio irreducible f. Denotemos por N_n el número de los polinomios mónicos irreducibles en $\mathbb{F}_p[X]$ de grado n. Nuestro objetivo es deducir una fórmula explícita para N_n.

15.1 La fórmula de Gauss

15.1.1. Lema.

1) *Sea k cualquier cuerpo. El polinomio $X^\ell - 1$ divide a $X^m - 1$ en $k[X]$ si y solo si $\ell \mid m$.*

2) *Sea a un entero ≥ 2. El número $a^\ell - 1$ divide a $a^m - 1$ en $\mathbb{Z}$ si y solo si $\ell \mid m$.*

3) *En particular, para un primo p y $d, n \geq 1$ se tiene $(X^{p^d} - X) \mid (X^{p^n} - X)$ si y solo si $d \mid n$.*

Demostración. En la primera parte, escribamos $m = q\ell + r$ donde $0 \leq r < \ell$. Tenemos en $k(X)$

$$\frac{X^m - 1}{X^\ell - 1} = \frac{(X^{q\ell+r} - X^r) + (X^r - 1)}{X^\ell - 1} = X^r \frac{X^{q\ell} - 1}{X^\ell - 1} + \frac{X^r - 1}{X^\ell - 1} = X^r \sum_{0 \leq i < q} X^{i\ell} + \frac{X^r - 1}{X^\ell - 1}.$$

Esto es un polinomio si y solamente si $\frac{X^r-1}{X^\ell-1}$ lo es. Pero $r < \ell$, así que la única opción es $r = 0$.

La segunda parte se demuestra de la misma manera. La última parte es una combinación de 1) y 2):

$$(X^{p^d} - X) \mid (X^{p^n} - X) \iff (X^{p^d-1} - 1) \mid (X^{p^n-1} - 1) \iff (p^d - 1) \mid (p^n - 1) \iff d \mid n.$$

■

15.1.2. Lema. *Denotemos por f_d el producto de todos los polinomios mónicos irreducibles de grado d en $\mathbb{F}_p[X]$. Luego,*

$$X^{p^n} - X = \prod_{d \mid n} f_d.$$

Demostración. Ya hemos notado en la prueba de 15.0.2 que el polinomio $X^{p^n} - X$ no tiene raíces múltiples en su cuerpo de descomposición. En particular, $X^{p^n} - X$ no puede tener factores irreducubles múltiples en $\mathbb{F}_p[X]$[*]. Sería entonces suficiente comprobar que un polinomio mónico irreducible $f \in \mathbb{F}_p[X]$ es de grado d divide a $X^{p^n} - X$ si y solo si $d \mid n$.

[*]Sin pasar al cuerpo de descomposición, basta notar que si $X^{p^n} - X = f^2 g$, entonces, tomando las derivadas formales en $\mathbb{F}_p[X]$, se obtiene $2f f' g + f^2 g' = -1$, así que $f \mid -1$ y $f \in \mathbb{F}_p^\times$ es una constante invertible.

Consideremos el cuerpo finito

$$\mathbb{F} := \mathbb{F}_p[X]/(f)$$

y denotemos por $\alpha \in \mathbb{F}$ la imagen de X en el cociente. En este caso f es el polinomio mínimo de α sobre $\mathbb{F}_p$. Siendo un cuerpo de p^d elementos, $\mathbb{F}$ es un cuerpo de descomposición del polinomio $X^{p^d} - X \in \mathbb{F}_p[X]$.

1) Si $d \mid n$, entonces, según el lema anterior, $(X^{p^d} - X) \mid (X^{p^n} - X)$. Entonces, todas las raíces de $X^{p^d} - X$ son también raíces de $X^{p^n} - X$, y en particular $\alpha^{p^n} - \alpha = 0$. Tenemos entonces
$$f \mid (X^{p^n} - X).$$

2) Viceversa, si $f \mid (X^{p^n} - X)$, entonces $f(\alpha) = 0$ implica que $\alpha^{p^n} - \alpha = 0$. Además, para cualquier elemento
$$x = a_{d-1}\,\alpha^{d-1} + \cdots + a_1\,\alpha + a_0 \in \mathbb{F},$$
donde $a_0, a_1, \ldots, a_{d-1} \in \mathbb{F}_p$, se tiene
$$x^{p^n} = a_{d-1}\,(\alpha^{p^n})^{d-1} + \cdots + a_1\,(\alpha^{p^n}) + a_0 = x,$$
así que *todos* los elementos de $\mathbb{F}$ son raíces de $X^{p^n} - X$. Se sigue que $(X^{p^d} - X) \mid (X^{p^n} - X)$, y luego $d \mid n$ por el lema anterior.

■

15.1.3. Ejemplo. Se sigue que para obtener todos los polinomios irreducibles de grado $d \mid n$ en $\mathbb{F}_p[X]$, basta factorizar el polinomio $X^{p^n} - X$ en $\mathbb{F}_p[X]$. Por ejemplo, en $\mathbb{F}_2[X]$ se tiene

$$X^{16} - X = X\,(X+1)\,(X^2+X+1)\,(X^4+X+1)\,(X^4+X^3+1)\,(X^4+X^3+X^2+X+1).$$

y en $\mathbb{F}_3[X]$

$$X^9 - X = X\,(X+1)\,(X+2)\,(X^2+1)\,(X^2+X+2)\,(X^2+2X+2).$$

▲

15.1.4. Corolario. *Se cumple*
$$p^n = \sum_{d \mid n} d \cdot N_d.$$

Demostración. Basta comparar grados a ambos lados de la identidad $X^{p^n} - X = \prod_{d \mid n} f_d$ en $\mathbb{F}_p[X]$. ■

Para obtener una fórmula para N_n, se puede usar la fórmula de inversión de Möbius, revisada en el apéndice D.

15.1.5. Teorema (Gauss). *El número de polinomios mónicos irreducibles de grado n en $\mathbb{F}_p[X]$ es igual a*

$$N_n := \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)\, p^d,$$

donde μ denota la ***función de Möbius****;*

$$\mu(1) := 1, \quad \mu(n) = 0 \text{ si } n \text{ no es libre de cuadrados},$$

y para n libre de cuadrados se pone

$$\mu(p_1 \cdots p_k) := (-1)^k,$$

donde k es el número de diferentes números primos que aparecen en la factorización de n.

Demostración. Consideremos la función $f(n) := n\, N_n$. Luego,

$$F(n) := \sum_{d|n} f(d) = \sum_{d|n} d\, N_d = p^n,$$

usando 15.1.4. La fórmula de inversión de Möbius nos da

$$f(n) = n\, N_n = \sum_{d|n}\mu\left(\frac{n}{d}\right)\, F(d) = \sum_{d|n}\mu\left(\frac{n}{d}\right)\, p^d.$$

■

15.1.6. Ejemplo. Hay

$$\frac{1}{6}\left(\mu(1)\cdot 2^6 + \mu(3)\cdot 2^2 + \mu(2)\cdot 2^3 + \mu(6)\cdot 2\right) = \frac{1}{6}\left(64 - 4 - 8 + 2\right) = 9$$

polinomios mónicos irreducibles en $\mathbb{F}_2[X]$ de grado 6. Factorizando el polinomio $X^{2^6} - X$ en $\mathbb{F}_2[X]$, se puede ver que son

$$\begin{array}{lll} X^6 + X + 1, & X^6 + X^4 + X^3 + X + 1, & X^6 + X^5 + X^3 + X^2 + 1, \\ X^6 + X^3 + 1, & X^6 + X^5 + 1, & X^6 + X^5 + X^4 + X + 1, \\ X^6 + X^4 + X^2 + X + 1, & X^6 + X^5 + X^2 + X + 1, & X^6 + X^5 + X^4 + X^2 + 1. \end{array}$$

He aquí algunos valores de N_n para diferentes p y n.

p \ n	1	2	3	4	5	6
2	2	1	2	3	6	9
3	3	3	8	18	48	116
5	5	10	40	150	624	2 580
7	7	21	112	588	3 360	19 544
11	11	55	440	3 630	32 208	295 020
13	13	78	728	7 098	74 256	804 076
17	17	136	1 632	20 808	283 968	4 022 064
19	19	171	2 280	32 490	495 216	7 839 780

El número de los polinomios mónicos irreducibles de grado n en $\mathbb{F}_p[X]$

▲

En particular, la fórmula de Gauss implica que para todo $n \geq 1$ existe un polinomio mónico irreducible $f \in \mathbb{F}_p[X]$ de grado n en $\mathbb{F}_p[X]$. En efecto,

$$N_n = \frac{1}{n}\left(p^n + \sum_{\substack{d|n \\ d\neq n}} \pm p^d\right) \geq \frac{1}{n}\left(p^n - (p^{n-1} + \cdots + p^2 + p)\right) > 0,$$

dado que

$$p^{n-1} + \cdots + p^2 + p = \frac{p^n - 1}{p - 1} - 1 < p^n.$$

15.2 Automorfismos de cuerpos finitos

La construcción de cuerpo finito de p^n elementos depende de una elección de un polinomio irreducible de grado n en $\mathbb{F}_p[X]$. Aunque probamos su existencia, no hay un modo canónico de escogerlo. Sin embargo, sabemos que todos los cuerpos de orden p^n son isomorfos entre sí. Esto nos lleva a la siguiente pregunta: ¿cuántos automorfismos tiene un cuerpo finito $\mathbb{F}_{p^n}$?

Para un cuerpo K los automorfismos $\sigma\colon K \xrightarrow{\cong} K$ forman un grupo $\mathrm{Aut}(K)$ respecto a la composición.

15.2.1. Teorema. *Para un cuerpo finito $\mathbb{F}_{p^n}$ el grupo de automorfismos $\mathrm{Aut}(\mathbb{F}_{p^n})$ es cíclico de orden n. Específicamente,*

$$\mathrm{Aut}(\mathbb{F}_{p^n}) = \langle F \rangle \cong \mathbb{Z}/n\mathbb{Z},$$

donde F denota el ***automorfismo de Frobenius***

$$F\colon x \mapsto x^p.$$

Demostración. Notamos primero que F es un automorfismo. Para cualesquiera $x, y \in \mathbb{F}_{p^n}$ tenemos obviamente

$$(xy)^p = x^p\, y^p.$$

Para las sumas, notamos que $\mathbb{F}_{p^n}$ es un cuerpo de característica p, así que

$$(x+y)^p = \sum_{i+j=p} \binom{p}{i} x^i\, y^j = x^p + y^p,$$

puesto que $p \mid \binom{p}{i}$ para $i = 1, \ldots, p-1$. Esto demuestra que F es un homomorfismo $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. Como todo homomorfismo de cuerpos, F es automáticamente inyectivo. Puesto que $\mathbb{F}_{p^n}$ es finito, F es sobreyectivo.

El grupo multiplicativo $\mathbb{F}_{p^n}^\times$ es cíclico y podemos escoger un generador $\alpha \in \mathbb{F}_{p^n}^\times$. Todo elemento $x \in \mathbb{F}_{p^n}^\times$ es de la forma α^i para $i = 0, 1, \ldots, p^n - 2$, y para cualquier automorfismo $\sigma\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ se tiene

$$\sigma(\alpha^i) = \sigma(\alpha)^i.$$

Esto demuestra que σ está definido por la imagen de α. Consideremos las potencias del automorfismo de Frobenius

$$F^k := \underbrace{F \circ \cdots \circ F}_{k} \colon x \mapsto x^{p^k}.$$

Tenemos $F^k = \mathrm{id}$ si y solo si $\alpha^{p^k} = \alpha$; es decir, $\alpha^{p^k-1} = 1$ en $\mathbb{F}_{p^n}^\times$. Dado que α tiene orden $p^n - 1$ en el grupo $\mathbb{F}_{p^n}^\times$, lo último sucede si y solo si $(p^n - 1) \mid (p^k - 1)$; es decir, si y solo si $n \mid k$. Podemos concluir que

$$F^0 = \mathrm{id},\ F,\ F^2,\ \ldots,\ F^{n-1}$$

son n diferentes automorfismos de $\mathbb{F}_{p^n}$. Para terminar la prueba, hay que ver que $\mathbb{F}_{p^n}$ no tiene otros automorfismos.

Sea $f = m_{\alpha,\mathbb{F}_p}$ el polinomio mínimo de α sobre $\mathbb{F}_p$. Luego,

$$\mathbb{F}_p[X]/(f) \cong \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}.$$

En particular,

$$\deg f = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

Tenemos $f(\alpha) = 0$, y para cualquier automorfismo $\sigma \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ necesariamente

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0,$$

así que $\sigma(\alpha)$ debe ser una raíz de f. Pero f, siendo un polinomio de grado n, tiene a lo sumo n raíces, y esto demuestra que $|\operatorname{Aut}(\mathbb{F}_{p^n})| \leq n$. ■

15.2.2. Corolario. *En un cuerpo finito $\mathbb{F}_{p^n}$ todo elemento es una p-ésima potencia.*

Demostración. Se sigue de la sobreyectividad del automorfismo de Frobenius $F \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. ■

15.2.3. Teorema. *Los subcuerpos de un cuerpo finito $\mathbb{F}_{p^n}$ corresponden a los divisores de n: son precisamente*

$$\mathbb{F}_{p^d} := \{x \in \mathbb{F}_{p^n} \mid x^{p^d} = x\}.$$

Demostración. Primero, si tenemos un subcuerpo $\mathbb{F} \subseteq \mathbb{F}_{p^n}$, entonces necesariamente $\mathbb{F}_p \subseteq \mathbb{F}$ y $|\mathbb{F}| = p^d$ para algún d. Luego,

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}] \cdot d,$$

demuestra que $d \mid n$. Dado que el grupo multiplicativo $\mathbb{F}^\times$ es cíclico de orden $p^d - 1$, los elementos de $\mathbb{F}$ son precisamente las raíces del polinomio $X^{p^d} - X \in \mathbb{F}_p[X]$:

$$\mathbb{F} = \mathbb{F}_d := \{x \in \mathbb{F}_{p^n} \mid x^{p^d} - x = 0\} = \{x \in \mathbb{F}_{p^n} \mid F^d(x) = x\}.$$

donde $F \colon x \mapsto x^p$ denota el automorfismo de Frobenius. Viceversa, para cualquier $d \mid n$ el conjunto $\mathbb{F}_{d^n}$ de arriba tiene p^d elementos: tenemos $(X^{p^d} - X) \mid (X^{p^n} - X)$ y el polinomio

$X^{p^n} - X$ se descompone en factores lineales en $\mathbb{F}_{p^n}[X]$. Además, para cualquier cuerpo K y un endomorfismo $\sigma\colon K \xrightarrow{\cong} K$, el conjunto

$$K^\sigma := \{x \in K \mid \sigma(x) = x\}$$

es un subcuerpo de K: esto se sigue de las identidades

$$\sigma(x+y) = \sigma(x) + \sigma(y), \quad \sigma(1) = 1, \quad \sigma(xy) = \sigma(x)\,\sigma(y), \quad \sigma(x^{-1}) = \sigma(x)^{-1}.$$

■

15.2.4. Ejemplo. Consideremos un cuerpo de $2^6 = 64$ elementos

$$\mathbb{F}_{64} = \mathbb{F}_2[X]/(X^6 + X^5 + X^3 + X^2 + 1).$$

Denotemos por α la imagen de X en el cociente. Tenemos

$$\mathbb{F}_{64} = \{a_5\,\alpha^5 + a_4\,\alpha^4 + a_3\,\alpha^3 + a_2\,\alpha^2 + a_1\,\alpha + a_0 \mid a_i = 0, 1\}.$$

Los elementos fijos bajo el automorfismo de Frobenius $F\colon x \mapsto x^2$ corresponden al subcuerpo

$$\mathbb{F}_2 = \{0, 1\}.$$

Los elementos fijos por $F^2\colon x \mapsto x^4$ corresponden al subcuerpo

$$\mathbb{F}_4 = \{0,\ 1,\ \alpha^4 + \alpha^2 + \alpha,\ \alpha^4 + \alpha^2 + \alpha + 1\}.$$

Los elementos fijos por $F^3\colon x \mapsto x^8$ corresponden al subcuerpo

$$\mathbb{F}_8 = \{0,\ 1,\ \alpha^2 + \alpha,\ \alpha^2 + \alpha + 1,\ \alpha^4 + \alpha,\ \alpha^4 + \alpha + 1,\ \alpha^4 + \alpha^2,\ \alpha^4 + \alpha^2 + 1\}.$$

▲

15.2.5. Comentario. Notamos que $\mathrm{Aut}(\mathbb{F}_{p^n}) = \langle F \rangle$ es el grupo cíclico de orden n generado por el automorfismo de Frobenius $F\colon x \mapsto x^p$. Los subgrupos de $\mathrm{Aut}(\mathbb{F}_{p^n})$ son precisamente $\langle F^d \rangle$ para $d \mid n$, y entonces hemos obtenido una biyección entre los subcuerpos de $\mathbb{F}_{p^n}$ y los subgrupos de $\mathrm{Aut}(\mathbb{F}_{p^n})$. Esto no es una coincidencia: es un caso particular de la **teoría de Galois**.

15.3 Cuerpos finitos y la reciprocidad cuadrática

Recordemos que para un número entero a y un primo p el **símbolo de Legendre** se define mediante

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{si } p \nmid a \text{ y } a \text{ es un cuadrado módulo } p, \\ -1, & \text{si } p \nmid a \text{ y } a \text{ no es un cuadrado módulo } p, \\ 0, & \text{si } p \mid a. \end{cases}$$

Tenemos las siguientes propiedades elementales.

a) El símbolo de Legendre es multiplicativo: se tiene

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

para cualesquiera $a, b \in \mathbb{Z}$.

b) Si p es un primo impar, entonces entre los números $\{1, 2, \ldots, p-1\}$ precisamente la mitad son cuadrados módulo p y la mitad no son cuadrados módulo p; en particular,

$$\sum_{0 \le i \le p-1} \left(\frac{i}{p}\right) = 0. \tag{15.1}$$

c) El símbolo de Legendre puede ser interpretado mediante el **criterio de Euler**: si p es un primo impar, entonces

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Todas estas propiedades se deducen fácilmente del hecho de que $\mathbb{F}_p^\times$ sea un grupo cíclico: existe un generador $\alpha \in \mathbb{F}_p^\times$ tal que todo elemento de $\mathbb{F}_p^\times$ es de la forma α^i para algún $i \in \mathbb{Z}$. Luego, α^i es un cuadrado si y solo si i es par (véase el capítulo 7 para los detalles).

El objetivo de esta sección es presentar una aplicación de cuerpos finitos en una prueba de la **ley de reciprocidad cuadrática** de Gauss.

1) Si p y q son diferentes primos impares, entonces

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right) = \begin{cases} +\left(\frac{p}{q}\right), & \text{si } p \equiv 1 \text{ o } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right), & \text{si } p \equiv 3 \text{ y } q \equiv 3 \pmod 4. \end{cases}.$$

2) La **primera ley suplementaria**: si p es un primo impar, entonces

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{si } p \equiv 1 \pmod 4, \\ -1, & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

3) La **segunda ley suplementaria**: si p es un primo impar, entonces

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{si } p \equiv \pm 1 \pmod 8, \\ -1, & \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

15.3.1. Ejemplo. He aquí una pequeña tabla de los valores de $\left(\frac{p}{q}\right)$.

p \ q	3	5	7	11	13	17	19	23	29	31
-1	$-$	$+$	$-$	$-$	$+$	$+$	$-$	$-$	$+$	$-$
2	$-$	$-$	$+$	$-$	$-$	$+$	$-$	$+$	$-$	$+$
3	0	$-$	$-$	$+$	$+$	$-$	$-$	$+$	$-$	$-$
5	$-$	0	$-$	$+$	$-$	$-$	$+$	$-$	$+$	$+$
7	$+$	$-$	0	$-$	$-$	$-$	$+$	$-$	$+$	$+$
11	$-$	$+$	$+$	0	$-$	$-$	$+$	$-$	$-$	$-$
13	$+$	$-$	$-$	$-$	0	$+$	$-$	$+$	$+$	$-$
17	$-$	$-$	$-$	$-$	$+$	0	$+$	$-$	$-$	$-$
19	$+$	$+$	$-$	$-$	$-$	$+$	0	$-$	$-$	$+$
23	$-$	$-$	$+$	$+$	$+$	$-$	$+$	0	$+$	$-$
29	$-$	$+$	$+$	$-$	$+$	$-$	$-$	$+$	0	$-$
31	$+$	$+$	$-$	$+$	$-$	$-$	$-$	$+$	$-$	0

▲

Notamos que la primera ley suplementaria se deduce inmediatamente del criterio de Euler. Otro modo de verlo: para $\alpha \in \mathbb{F}_p^\times$ se tiene $\alpha^2 = -1$ si y solamente si el orden de α es igual a 4. Entonces, -1 es un cuadrado si y solo si $4 \mid (p-1)$.

Vamos a probar la segunda ley suplementaria y luego la ley principal. Nuestra exposición sigue [IR1990, Chapter 6], pero en lugar de las raíces de la unidad ζ_n usamos los cuerpos finitos, según lo indicado en [IR1990, §7.3].

La segunda ley suplementaria

Antes de probar la ley principal, empecemos por la segunda ley suplementaria. Si p es un primo impar, entonces $p^2 \equiv 1 \pmod 8$, puesto que cualquier cuadrado de un número impar es congruente a 1 módulo 8:

$$1^2 = 1, \quad 3^2 = 9, \quad 5^2 = 25, \quad 7^2 = 49.$$

Consideremos el cuerpo finito $\mathbb{F}_{p^2}$. El grupo multiplicativo $\mathbb{F}_{p^2}^\times$ es cíclico de orden $p^2 - 1$, y dado que $8 \mid (p^2 - 1)$, existe un elemento $\alpha \in \mathbb{F}_{p^2}^\times$ de orden 8. Notamos que

$$(\alpha^4 - 1)(\alpha^4 + 1) = \alpha^8 - 1 = 0.$$

Dado que $\alpha^4 \neq 1$, tenemos $\alpha^4 = -1$, de donde se siguen las identidades

$$\alpha^2 + \alpha^{-2} = 0, \quad \alpha^3 = -\alpha^{-1}.$$

Pongamos

$$\tau := \alpha + \alpha^{-1}.$$

Notamos que $\tau \neq 0$. En efecto, si $\alpha^{-1} = -\alpha$, entonces $\alpha^2 = -1$ y luego $\alpha^4 = 1$, pero no es el caso.

Tenemos

$$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = (\alpha^2 + 2 + \alpha^{-2})^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} = \left(\frac{2}{p}\right),$$

donde la última igualdad se sigue del criterio de Euler. En consecuencia

$$\alpha^p + \alpha^{-p} = (\alpha + \alpha^{-1})^p = \tau^p = \left(\frac{2}{p}\right) \tau.$$

Dado que α tiene orden 8, la expresión a la izquierda depende solamente del residuo de p módulo 8:

$$\alpha^p + \alpha^{-p} = \left\{ \begin{array}{ll} \alpha + \alpha^{-1} = \tau, & p \equiv \pm 1 \pmod 8 \\ \alpha^3 + \alpha^{-3} = -\tau, & p \equiv \pm 3 \pmod 8 \end{array} \right\} = (-1)^{\frac{p^2-1}{8}} \tau.$$

Comparando las últimas dos identidades, se obtiene

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

15.3.2. Comentario. El mismo argumento funciona para la raíz de la unidad ζ_8 en lugar de α y el anillo $\mathbb{Z}[\zeta_8]$ en lugar de $\mathbb{F}_{p^2}$. En este caso hay que considerar identidades en $\mathbb{Z}[\zeta_8]$ módulo p.

La ley principal

Sean p y q dos diferentes primos impares. Podemos escoger un número $n = 1, 2, 3, \ldots$ tal que

$$q^n \equiv 1 \pmod p$$

(por ejemplo, basta tomar $n = p - 1$). Consideremos el cuerpo finito $\mathbb{F}_{q^n}$. El grupo multiplicativo $\mathbb{F}_{q^n}^\times$ es cíclico de orden $q^n - 1$. Por nuestra elección de n, se tiene $p \mid (q^n - 1)$, así que existe un elemento $\alpha \in \mathbb{F}_{q^n}^\times$ de orden p.

Para $a \in \mathbb{Z}$ pongamos

$$\tau_a := \sum_{0 \leq i \leq p-1} \left(\frac{i}{p}\right) \alpha^{ai} \in \mathbb{F}_{q^n}.$$

En particular, definamos

$$\tau := \tau_1.$$

A partir de ahora y hasta el final de esta sección, todos los sumatorios serán entre 0 y $p - 1$, así que por brevedad vamos a escribir "$\sum_i$" en lugar de "$\sum_{0 \leq i \leq p-1}$".

15.3.3. Lema. *Tenemos*

$$\sum_i \alpha^{ai} = \begin{cases} p, & si\ p \mid a, \\ 0, & si\ p \nmid a. \end{cases}$$

Demostración. Si $p \mid a$, entonces $\alpha^{ai} = 1$ para todo $0 \leq i \leq p-1$, así que

$$\sum_i \alpha^{ai} = p.$$

Si $p \nmid a$, entonces $\alpha^a \neq 1$, y luego

$$\sum_i \alpha^{ai} = \frac{\alpha^{ap} - 1}{\alpha^a - 1} = 0.$$

■

15.3.4. Proposición (Gauss). *En $\mathbb{F}_{q^n}$ se cumplen las identidades*

1) $\tau_a = \left(\frac{a}{p}\right) \tau$.

2) $\tau^2 = (-1)^{\frac{p-1}{2}}\, p$.

Demostración. Si $p \mid a$, entonces

$$\left(\frac{a}{p}\right) = 0.$$

Por otro lado, tenemos $\alpha^{ai} = 1$ para todo $0 \leq i \leq p-1$, dado que el orden de α es igual a p, y luego,

$$\tau_a = \sum_i \left(\frac{i}{p}\right) = 0$$

por (15.1). Si $p \nmid a$, entonces calculamos que

$$\left(\frac{a}{p}\right) \tau_a = \sum_i \left(\frac{ai}{p}\right) \alpha^{ai} = \sum_j \left(\frac{j}{p}\right) \alpha^j = \tau$$

—el símbolo de Legendre $\left(\frac{j}{p}\right)$ y el elemento α^j dependen solo del resto de j módulo p y los números ai para $0 \leq i \leq p-1$ nos dan todos los restos módulo p. Ahora $\left(\frac{a}{p}\right) = \pm 1$, así que al multiplicar la identidad de arriba por $\left(\frac{a}{p}\right)$ nos queda la identidad 1)

$$\tau_a = \left(\frac{a}{p}\right) \tau.$$

Probemos la segunda identidad. Notamos que si $p \nmid a$, entonces la identidad 1) nos da

$$\tau_a\, \tau_{-a} = \left(\frac{a}{p}\right) \left(\frac{-a}{p}\right) \tau^2 = \left(\frac{-1}{p}\right) \tau^2,$$

y si $p \mid a$, entonces $\tau_a\,\tau_{-a} = 0$. Luego,

$$\sum_a \tau_a\,\tau_{-a} = \left(\frac{-1}{p}\right)\,(p-1)\,\tau^2. \tag{15.2}$$

Por otro lado, tenemos

$$\tau_a\,\tau_{-a} = \sum_i \sum_j \left(\frac{i}{p}\right)\,\left(\frac{j}{p}\right)\,\alpha^{a\,(i-j)},$$

y sumando estas identidades para $0 \leq a \leq p-1$, se obtiene

$$\sum_a \tau_a\,\tau_{-a} = \sum_i \sum_j \left(\frac{i}{p}\right)\,\left(\frac{j}{p}\right)\,\sum_a \alpha^{a\,(i-j)}.$$

El cálculo del lema 15.3.3 nos dice que

$$\sum_a \alpha^{a\,(i-j)} = \begin{cases} p, & \text{si } i = j, \\ 0, & \text{si } i \neq j. \end{cases}$$

Entonces,

$$\sum_a \tau_a\,\tau_{-a} = \sum_i \left(\frac{i}{p}\right)^2\,p = (p-1)\,p. \tag{15.3}$$

Comparando (15.2) y (15.3), tenemos

$$\left(\frac{-1}{p}\right)\,(p-1)\,\tau^2 = (p-1)\,p,$$

de donde

$$\tau^2 = \left(\frac{-1}{p}\right)\,p = (-1)^{\frac{p-1}{2}}\,p.$$

■

Estamos listos para probar la ley de reciprocidad cuadrática. Denotemos

$$p^* := (-1)^{\frac{p-1}{2}}\,p.$$

La segunda identidad de 15.3.4 nos dice que

$$\tau^2 = p^* \quad \text{en } \mathbb{F}_{q^n}.$$

Entonces,

$$\left(\frac{p^*}{q}\right) = 1 \iff \tau \in \mathbb{F}_q \subset \mathbb{F}_{q^n} \iff \tau^q = \tau.$$

(En efecto, si p^* es un cuadrado en $\mathbb{F}_q$, entonces $p^* = x^2$ para algún $x \in \mathbb{F}_q$. Pero en este caso $\tau = \pm x$, así que $\tau \in \mathbb{F}_q$. Viceversa, si $\tau \in \mathbb{F}_q$, entonces $p^* = \tau^2$ es un cuadrado en $\mathbb{F}_q$.) Luego, tenemos en $\mathbb{F}_{q^n}$

$$\tau^q = \left(\sum_i \left(\frac{i}{p}\right)\,\alpha^i\right)^q = \sum_i \left(\frac{i}{p}\right)^q\,\alpha^{qi} = \sum_i \left(\frac{i}{p}\right)\,\alpha^{qi} = \tau_q = \left(\frac{q}{p}\right)\,\tau,$$

según la primera identidad 15.3.4. Entonces, la condición $\tau^q = \tau$ equivale a

$$\left(\frac{q}{p}\right) = 1.$$

Hemos probado que

$$\left(\frac{p^*}{q}\right) = 1 \iff \left(\frac{q}{p}\right) = 1.$$

Esto equivale a la identidad

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right).$$

15.3.5. Comentario. Estos cálculos se pueden hacer con la raíz de la unidad ζ_p en lugar de α. En este caso la expresión

$$g_a := \sum_{0 \le a \le p-1} \left(\frac{a}{p}\right) \zeta_p^a, \quad g := g_1$$

se conoce como la **suma cuadrática de Gauss**. Muchas pruebas de la reciprocidad cuadrática, incluso una de las pruebas de Gauss, se basan en la identidad

$$g^2 = \left(\frac{-1}{p}\right) p.$$

En el tratado de Gauss "Disquisitiones Arithmeticae" aparecen ocho pruebas diferentes de la reciprocidad cuadrática, y hoy en día se conocen alrededor de 250[*]. Para más información sobre las leyes de reciprocidad en el contexto histórico, véase el libro [Lem2000].

15.4 Perspectiva: ecuaciones sobre cuerpos finitos

> Presently, the topic which amuses me most is counting points on algebraic curves over finite fields. It is a kind of applied mathematics: you try to use any tool in algebraic geometry and number theory that you know of... and you don't quite succeed!
>
> Una entrevista a Jean–Pierre Serre, 1985

Consideremos un cuerpo finito $\mathbb{F}_q$. Sus extensiones finitas son de la forma $\mathbb{F}_{q^k}$ para $k = 1, 2, 3, \ldots$ Denotemos por

$$\mathbb{A}^n(\mathbb{F}_{q^k}) := \mathbb{F}_{q^k}^n$$

el espacio afín de dimensión n sobre $\mathbb{F}_{q^k}$. Para una colección de polinomios $f_1, f_2, \ldots, f_s \in \mathbb{F}_q[X_1, \ldots, X_n]$, consideremos el conjunto de sus ceros en común en $\mathbb{F}_{q^k}^n$:

$$V(\mathbb{F}_{q^k}) := \{\underline{x} = (x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbb{F}_{q^k}) \mid f_1(\underline{x}) = f_2(\underline{x}) = \cdots = f_s(\underline{x}) = 0\}.$$

[*]Véase http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html

Este conjunto es finito, siendo un subconjunto de $\mathbb{A}^n(\mathbb{F}_{q^k})$ que tiene q^{kn} elementos. Entonces, cabe preguntarse, cómo el número de elementos de $V(\mathbb{F}_{q^k})$ depende de k. Este problema fue uno de los más importantes en las matemáticas del siglo XX. A saber, esto se estudia mediante **función zeta** definida por

$$Z(V_{/\mathbb{F}_q}, t) := \exp\left(\sum_{k\geq 1} \#V(\mathbb{F}_{q^k})\,\frac{t^k}{k}\right).$$

Esta expresión también puede ser considerada como una serie formal en $\mathbb{Q}[\![t]\!]$

En 1960 Bernard Dwork probó que $Z(V_{/\mathbb{F}_q}, t)$ es siempre una función racional. En términos de las series formales, esto significa que $Z(V_{/\mathbb{F}_q}, t) = f/g$ para algunos polinomios $f, g \in \mathbb{Q}[t]$. Conociendo esta función racional, se puede considerar los coeficientes de la serie $\log(f/g)$ para recuperar los números $\#V(\mathbb{F}_{q^k})$ para todo $k = 1, 2, 3, \ldots$

La prueba de Dwork está explicada en el libro [Kob1984] y aquí vamos considerar solo un par de casos particulares.

Círculo unitario

El círculo unitario viene dado por la ecuación $X^2 + Y^2 = 1$. Consideremos entonces el conjunto

$$C(\mathbb{F}_q) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_q) \mid x^2 + y^2 = 1\}.$$

Primero, si $q = 2^k$, entonces todo elemento de $\mathbb{F}_{2^k}$ es un cuadrado: para todo $\alpha \in \mathbb{F}_{2^k}$ existe $\beta \in \mathbb{F}_{2^k}$ tal que $\alpha = \beta^2$. Además, este β es único: se tiene

$$X^2 - \alpha = (X - \alpha)^2.$$

Entonces, cualquier $x \in \mathbb{F}_{2^k}$ define un punto único

$$(x, \sqrt{1 - x^2}) \in C(\mathbb{F}_{2^k}).$$

Se sigue que

$$\#C(\mathbb{F}_{2^k}) = 2^k.$$

15.4.1. Ejemplo. Sobre $\mathbb{F}_2$, los puntos del círculo $C(\mathbb{F}_2)$ son

$$(1, 0),\ (0, 1).$$

Sobre el cuerpo

$$\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2 + X + 1) = \{0, 1, \alpha, \alpha + 1\}$$

los puntos del círculo $C(\mathbb{F}_4)$ son

$$(0, 1),\ (1, 0),\ (\alpha, \alpha + 1),\ (\alpha + 1, \alpha).$$

En efecto, tenemos

$$\alpha^2 = \alpha + 1, \quad (\alpha + 1)^2 = \alpha.$$

▲

Ahora si q es impar, el problema se vuelve más interesante. Analicemos algunos ejemplos.

15.4.2. Ejemplo. Tenemos

$$\begin{aligned} C(\mathbb{F}_3) &= \{(0,1),\ (0,2),\ (1,0),\ (2,0)\},\\ C(\mathbb{F}_5) &= \{(0,1),\ (0,4),\ (1,0),\ (4,0)\},\\ C(\mathbb{F}_7) &= \{(0,1),\ (0,6),\ (1,0),\ (2,2),\ (2,5),\ (5,2),\ (5,5),\ (6,0)\}. \end{aligned}$$

En el cuerpo

$$\mathbb{F}_9 := \mathbb{F}_3[X]/(X^2+1) = \{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$$

Los cuadrados son

$$\begin{aligned} 1^2 = 2^2 &= 1,\\ \alpha^2 = (2\alpha)^2 &= 2,\\ (\alpha+1)^2 = (2\alpha+2)^2 &= 2\alpha,\\ (\alpha+2)^2 = (2\alpha+1)^2 &= \alpha. \end{aligned}$$

Luego,

$$\alpha^2+\alpha^2 = (2\alpha)^2+(2\alpha)^2 = \alpha^2+(2\alpha)^2 = 1.$$

Tenemos

$$C(\mathbb{F}_9) = \{(0,1),\ (0,2),\ (1,0),\ (2,0),\ (\alpha,\alpha),\ (\alpha,2\alpha),\ (2\alpha,\alpha),\ (2\alpha,2\alpha)\}.$$

▲

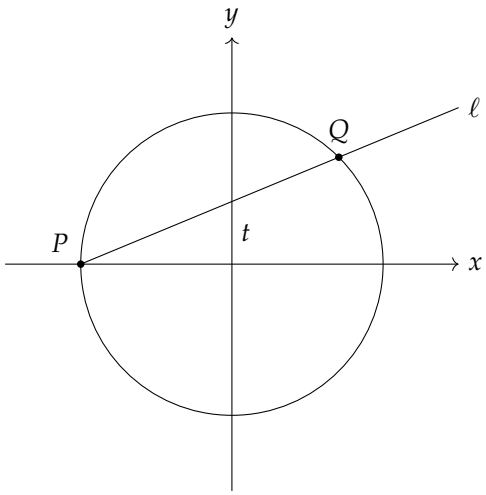
He aquí una pequeña tabla que podemos compilar con ayuda de una computadora:

q:	3	5	7	9	11	13	17	19	23	25	27	29	31	37	41	$\cdots$
q mód 4:	3	1	3	1	3	1	1	3	3	1	3	1	3	1	1	$\cdots$
$\#C(\mathbb{F}_q)$:	4	4	8	8	12	12	16	20	24	24	28	28	32	36	40	$\cdots$

Se nota que $\#C(\mathbb{F}_q) = q \pm 1$. Para explicar qué está pasando, recordemos la parametrización del círculo. Sería instructivo hacer un dibujo del círculo real. El punto $P = (-1,0)$ siempre está en el circulo. Podemos trazar una recta que pasa por P y tiene otra intersección con el círculo. Esta recta necesariamente tendrá ecuación

$$\ell\colon Y = tX + t$$

para algún t.



La intersección de esta recta con el círculo viene dada por[*]

$$Q = (x, y),\ y = t\,x + t,\ x^2 + y^2 = 1 \Longrightarrow (x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right).$$

Viceversa, la recta que pasa por P y $Q = (x, y)$ tiene ecuación

$$Y = t\,X + t, \quad t = \frac{y}{x + 1}.$$

Ahora si trabajamos sobre un cuerpo $\mathbb{F}_q$, puede pasar que $t^2 = -1$. Entonces, lo que tenemos es una aplicación

$$\begin{aligned} \phi\colon \{t \in \mathbb{F}_q \mid t^2 \neq -1\} &\to C(\mathbb{F}_q) \setminus \{(-1, 0)\}, \\ t &\mapsto \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right). \end{aligned}$$

Esta aplicación está bien definida:

$$\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) \neq (-1, 0)$$

si q es impar. Notamos que si para $(x, y) \in C(\mathbb{F}_q)$ tenemos

$$\left(\frac{y}{x + 1}\right)^2 = -1,$$

[*]El lector probablemente reconocerá las identidades trigonométricas

$$\cos\alpha = \frac{\cos^2(\alpha/2) - \operatorname{sen}^2(\alpha/2)}{\cos^2(\alpha/2) + \operatorname{sen}^2(\alpha/2)} = \frac{1 - \tan^2(\alpha/2)}{1 + \tan^2(\alpha/2)}$$

y

$$\operatorname{sen}\alpha = \frac{2\operatorname{sen}(\alpha/2)\cos(\alpha/2)}{\cos^2(\alpha/2) + \operatorname{sen}^2(\alpha/2)} = \frac{2\tan(\alpha/2)}{1 + \tan^2(\alpha/2)}.$$

entonces

$$y^2 = -(x+1)^2,$$

y luego la ecuación

$$x^2 + y^2 = x^2 - (x-1)^2 = -2x - 1 = 1$$

nos dice que $(x, y) = (-1, 0)$. Entonces, tenemos una aplicación bien definida

$$\psi\colon C(\mathbb{F}_q) \setminus \{(-1,0)\} \to \{t \in \mathbb{F}_q \mid t^2 \neq -1\},$$
$$(x, y) \mapsto \frac{y}{x+1}.$$

Las aplicaciones ϕ y ψ son mutualmente inversas:

$$\psi \circ \phi(t) = t, \quad \phi \circ \psi(x, y) = (x, y)$$

para cualesquiera $t \in \mathbb{F}_q$ con $t^2 \neq 1$ y $(x, y) \in C(\mathbb{F}_q)$ con $x \neq -1$. Esta biyección nos permite concluir que

$$\#C(\mathbb{F}_q) - 1 = \#\{t \in \mathbb{F}_q \mid t^2 \neq -1\}.$$

Ahora si -1 es un cuadrado en $\mathbb{F}_q$, la ecuación $t^2 = -1$ tiene dos soluciones. Tenemos entonces

$$\#C(\mathbb{F}_q) = \begin{cases} q+1, & \text{si } -1 \text{ no es un cuadrado en } k, \\ q-1, & \text{si } -1 \text{ es un cuadrado en } k. \end{cases}$$

Falta notar que -1 es un cuadrado en $\mathbb{F}_q^\times$ si y solamente si $q \equiv 1 \pmod 4$ (véase el ejercicio 15.9). Resumamos nuestros resultados.

15.4.3. Proposición. *Se tiene*

$$\#C(\mathbb{F}_q) = \begin{cases} q, & \text{si } q \text{ es par}, \\ q+1, & \text{si } q \equiv 3 \pmod 4, \\ q-1, & \text{si } q \equiv 1 \pmod 4. \end{cases}$$

Calculemos la función zeta correspondiente

$$Z(C_{/\mathbb{F}_q}, t) := \exp\left(\sum_{k\geq 1} \#C(\mathbb{F}_{q^k})\, \frac{t^k}{k}\right).$$

1) Si q es par, enconces $\#C(\mathbb{F}_{q^k}) = q^k$ y tenemos

$$Z(C_{/\mathbb{F}_q}, t) = \exp\left(\sum_{k\geq 1} \frac{(qt)^k}{k}\right).$$

Recordemos la serie para el logaritmo

$$\log(1+t) = \sum_{k\geq 1} (-1)^{k+1}\, \frac{t^k}{k} = t - \frac{t^2}{2} + \frac{t^3}{3} - \frac{t^4}{4} + \cdots$$

Luego,

$$-\log(1-t) = \sum_{k\geq 1} \frac{t^k}{k} = t - \frac{t^2}{2} + \frac{t^3}{3} - \frac{t^4}{4} + \cdots$$

En nuestro caso, tenemos

$$Z(C_{/\mathbb{F}_q}, t) = \exp(-\log(1-qX)) = \frac{1}{1-qX}.$$

2) Si $q \equiv 3 \pmod 4$, entonces $q^k \equiv (-1)^k \pmod 4$, de donde se obtiene

$$\#C(\mathbb{F}_{q^k}) = \begin{cases} q^k + 1, & \text{si } k \text{ es impar,} \\ q^k - 1, & \text{si } k \text{ es par.} \end{cases}$$

Luego,

$$Z(C_{/\mathbb{F}_q}, t) = \exp\left(\sum_{k\geq 1} \frac{(q\,t)^k}{k} + \sum_{k\geq 1} (-1)^{k+1}\,\frac{t^k}{k}\right) = \exp(-\log(1-qt) + \log(1+t)) = \frac{1+t}{1-qt}.$$

3) De la misma manera, si $q \equiv 1 \pmod 4$, entonces $q^k \equiv 1 \pmod 4$ para todo $k = 1, 2, 3, \ldots$ y

$$\#C(\mathbb{F}_{q^k}) = q^k - 1.$$

La función zeta entonces viene dada por

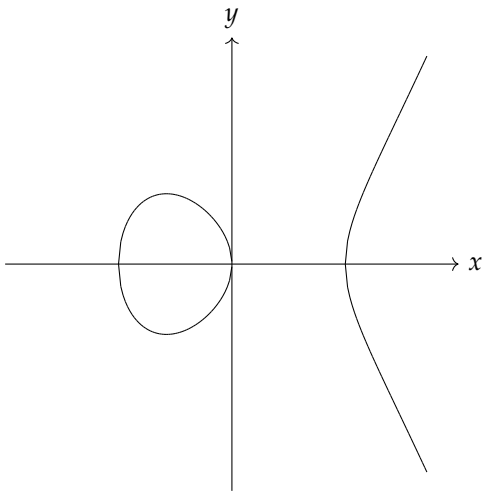
$$Z(C_{/\mathbb{F}_q}, t) = \exp\left(\sum_{k\geq 1} \frac{(q\,t)^k}{k} - \sum_{k\geq 1} \frac{t^k}{k}\right) = \exp(-\log(1-qt) + \log(1-t)) = \frac{1-t}{1-qt}.$$

La curva $Y^2 = X^3 - X$

Consideremos el conjunto

$$E_0(\mathbb{F}_q) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_q) \mid y^2 = x^3 - x\}.$$

He aquí la gráfica de los puntos reales de la curva $y^2 = x^3 - x$:



De nuevo, nuestro objetivo sería investigar cómo la cardinalidad de $E_0(\mathbb{F}_q)$ depende de q. Como en el caso del círculo unitario, si $q = 2^k$, entonces para todo $x \in \mathbb{F}_q$ existe un único y tal que $y^2 = x^3 - x$. Se sigue que

$$\#E_0(\mathbb{F}_{2^k}) = 2^k.$$

En característica diferente de 2, no todo elemento es un cuadrado y el problema es mucho más interesante.

15.4.4. Ejemplo.

$$\begin{aligned}
\#E_0(\mathbb{F}_3) &= \{(0,0),(0,1),(0,2)\},\\
\#E_0(\mathbb{F}_5) &= \{(0,0),(0,1),(0,4),(1,2),(2,3),(3,3),(2,3)\},\\
\#E_0(\mathbb{F}_7) &= \{(0,0),(0,1),(0,6),(1,5),(2,4),(5,4),(6,5)\}.
\end{aligned}$$

▲

Con ayuda de una computadora compilemos una pequeña tabla:

q:	3	5	7	9	11	13	17	19	23	25	27	29	31	37	$\cdots$
q mód 4:	3	1	3	1	3	1	1	3	3	1	3	1	3	1	$\cdots$
$\#E_0(\mathbb{F}_q)$:	3	7	7	15	11	7	15	19	23	31	27	39	31	39	$\cdots$

Aquí se nota un patrón:

$$\#E_0(\mathbb{F}_q) = q, \quad \text{si } q \equiv 3 \pmod 4,$$

y esto es lo que vamos a probar en esta sección.

Usando el hecho de que el grupo $\mathbb{F}_q^\times$ sea cíclico de orden $q-1$, se puede ver que precisamente la mitad de los elementos de $\mathbb{F}_q^\times$ son cuadrados y la mitad no son cuadrados, con la siguiente "tabla de multiplicación"[*]:

$\times$	cuadrado	no-cuadrado
cuadrado	cuadrado	no-cuadrado
no-cuadrado	no-cuadrado	cuadrado

Consideremos la función

$$f(x) := x^3 - x.$$

Primero notamos que la ecuación $f(x) = 0$ tiene tres diferentes soluciones $x = 0, \pm 1$. Esto nos da tres puntos

$$(0,0),\ (1,0),\ (-1,0) \in E_0(\mathbb{F}_q).$$

Asumamos que $q \equiv 3 \pmod 4$. En este caso -1 no es un cuadrado en $\mathbb{F}_q^\times$. Ahora si $x \neq 0, \pm 1$, tenemos $f(x) \neq 0$. Dado que $f(x) = -f(-x)$ y -1 no es un cuadrado, precisamente un elemento entre $f(x)$ y $f(-x)$ es un cuadrado. Se sigue que exactamente para la mitad de los $x \neq 0, \pm 1$, el elemento $f(x)$ es un cuadrado. En este caso la ecuación

$$y^2 = f(x)$$

[*] Véase el ejercicio 15.8.

tiene dos soluciones $y \in \mathbb{F}_q^\times$. Luego,

$$\#E_0(\mathbb{F}_q) = 3 + 2 \cdot \frac{q-3}{2} = q.$$

15.4.5. Proposición. *Si q es par o $q \equiv 3 \pmod 4$, entonces*

$$\#E_0(\mathbb{F}_q) = q.$$

Por otro lado, cuando $q \equiv 1 \pmod 4$, las cosas se vuelven mucho más interesantes. Para formular la respuesta, recordemos que el anillo de los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ es un dominio de factorización única. Recordemos (de los ejercicios del capítulo anterior) que un primo impar p es primo en $\mathbb{Z}[\sqrt{-1}]$ si $p \equiv 3 \pmod 4$ y si $p \equiv 1 \pmod 4$, entonces

$$p = N(\pi) = \pi\,\overline{\pi} = a^2 + b^2$$

para un primo $\pi = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$. Notamos que los números a y b no son nulos y tienen diferente paridad, así que hay ocho diferentes opciones para escoger este π que corresponden al cambio del signo de a y de b y el intercambio de a con b. Se puede escoger uno de estos π que es **primario** en el siguiente sentido.

15.4.6. Definición. Se dice que un entero de Gauss no invertible $\alpha = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ es **primario** si $\alpha \equiv 1 \pmod{2 + 2\sqrt{-1}}$. Esto sucede si y solo si se cumple una de las dos condiciones:

1) $a \equiv 1$ y $b \equiv 0 \pmod 4$;

2) $a \equiv 3$ y $b \equiv 2 \pmod 4$.

15.4.7. Ejemplo. Si pedimos que $N(\pi) = 5$, entonces hay 8 posibilidades:

$$\pi = 2 \pm \sqrt{-1},\ \ -2 \pm \sqrt{-1},\quad 1 \pm 2\sqrt{-1},\ \ -1 \pm 2\sqrt{-1}.$$

Los elementos primarios son $-1 \pm 2\sqrt{-1}$. ▲

15.4.8. Teorema ([IR1990, §18.4, Theorem 5]). *Sean p un número primo tal que $p \equiv 1 \pmod 4$ y $\pi \in \mathbb{Z}[\sqrt{-1}]$ un entero de Gauss tal que $N(\pi) = p$ y π es primario. Entonces,*

$$\#E_0(\mathbb{F}_p) = p - 2\,\mathrm{Re}\,\pi.$$

15.4.9. Ejemplo. He aquí una pequeña tabla de los π como en el teorema y el número de puntos correspondiente en la curva.

p:	5	13	17	29	37	$\cdots$
π:	$-1 \pm 2\sqrt{-1}$	$3 \pm 2\sqrt{-1}$	$1 \pm 4\sqrt{-1}$	$-5 \pm 2\sqrt{-1}$	$-1 \pm 6\sqrt{-1}$	$\cdots$
$\#E_0(\mathbb{F}_p)$:	7	7	15	39	39	$\cdots$

▲

Para obtener los números $\#E_0(\mathbb{F}_{p^k})$ nos puede ayudar la función zeta. Por ciertas razones, es más conveniente añadir a E_0 un punto extra, denotado por O, y trabajar con

$$E := E_0 \cup \{O\}.$$

Entonces,

$$\#E(\mathbb{F}_q) = E_0(\mathbb{F}_q) + 1.$$

15.4.10. Teorema. *Para q impar se tiene*

$$Z(E_{/\mathbb{F}_q}, t) = \frac{1 - at + qt^2}{(1-t)\,(1-qt)} + 1, \quad \textit{donde } a = q + 1 - \#E(\mathbb{F}_q).$$

El lector interesado puede consultar [Sil2009, §V.2] y [Kob1993, §II.1–2] para más detalles. En nuestro caso tenemos

p:	3	5	7	11	13	$\cdots$
$\#E(\mathbb{F}_p)$:	4	8	8	12	8	$\cdots$
$p+1-\#E(\mathbb{F}_p)$:	0	-2	0	0	6	$\cdots$

Las funciones zeta correspondientes son entonces

$$\begin{aligned}
Z(E_{/\mathbb{F}_3}, t) &= \frac{1 + 3t^2}{(1-t)\,(1-3t)}, \\
Z(E_{/\mathbb{F}_5}, t) &= \frac{1 + 2t + 5t^2}{(1-t)\,(1-5t)}, \\
Z(E_{/\mathbb{F}_7}, t) &= \frac{1 + 7t^2}{(1-t)\,(1-7t)}, \\
Z(E_{/\mathbb{F}_{11}}, t) &= \frac{1 + 11t^2}{(1-t)\,(1-11t)}, \\
Z(E_{/\mathbb{F}_{13}}, t) &= \frac{1 - 6t + 13t^2}{(1-t)\,(1-13t)},
\end{aligned}$$

de donde se calculan las series[*]

$$\begin{aligned}
\log Z(E_{/\mathbb{F}_3}, t) &= 4\,t + \frac{16}{2}\,t^2 + \frac{28}{3}\,t^3 + \frac{64}{4}\,t^4 + \frac{244}{5}\,t^5 + \cdots \\
\log Z(E_{/\mathbb{F}_5}, t) &= 8\,t + \frac{32}{2}\,t^2 + \frac{104}{3}\,t^3 + \frac{640}{4}\,t^4 + \frac{3208}{5}\,t^5 + \cdots \\
\log Z(E_{/\mathbb{F}_7}, t) &= 8\,t + \frac{64}{2}\,t^2 + \frac{344}{3}\,t^3 + \frac{2304}{4}\,t^4 + \frac{16\,808}{5}\,t^5 + \cdots \\
\log Z(E_{/\mathbb{F}_{11}}, t) &= 12\,t + \frac{144}{2}\,t^2 + \frac{1332}{3}\,t^3 + \frac{14\,400}{4}\,t^4 + \frac{161\,052}{5}\,t^5 + \cdots \\
\log Z(E_{/\mathbb{F}_{13}}, t) &= 8\,t + \frac{160}{2}\,t^2 + \frac{2216}{3}\,t^3 + \frac{28\,800}{4}\,t^4 + \frac{372\,488}{5}\,t^5 + \cdots
\end{aligned}$$

Tenemos entonces

[*]Un ejemplo de este cálculo en PARI/GP:

```
? log ((1+3*t^2)/((1-t)*(1-3*t)))
% = 4*t + 8*t^2 + 28/3*t^3 + 16*t^4 + 244/5*t^5 + ...
```

p:	3	5	7	11	13	$\cdots$
$\#E(\mathbb{F}_p)$:	4	8	8	12	8	$\cdots$
$\#E(\mathbb{F}_{p^2})$:	16	32	64	144	160	$\cdots$
$\#E(\mathbb{F}_{p^3})$:	28	104	344	1332	2216	$\cdots$
$\#E(\mathbb{F}_{p^4})$:	64	640	2304	14 400	28 800	$\cdots$
$\#E(\mathbb{F}_{p^5})$:	244	3208	16 808	161 052	372 488	$\cdots$

El conteo de soluciones de ecuaciones polinomiales es un tema muy profundo. Por ejemplo, este es el hilo conductor del libro [IR1990].

15.5 Cerradura algebraica de $\mathbb{F}_p$

Consideremos un cuerpo finito $\mathbb{F}_p$. Sus extensiones son cuerpos finitos $\mathbb{F}_{p^n}$. Recordemos que si $m \mid n$, entonces $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$; específicamente, un subcuerpo de p^n elementos contiene un subcuerpo único de p^m elementos. Respecto a estas inclusiones, podemos tomar

$$\mathbb{F}_{p^\infty} := \bigcup_{n \geq 1} \mathbb{F}_{p^n}.$$

A saber, los elementos de $\mathbb{F}_{p^\infty}$ son $x \in \mathbb{F}_{p^m}$ e $y \in \mathbb{F}_{p^n}$, y para calcular $x\,y$ o $x \pm y$, hay que encajar x e y en $\mathbb{F}_{p^{\mathrm{mcm}(m,n)}}$. Se ve que esto es un cuerpo y es una extensión infinita de $\mathbb{F}_p$.

Todo polinomio $f \in \mathbb{F}_{p^\infty}[X]$ tendrá sus coeficientes en algún cuerpo finito $\mathbb{F}_{p^n}$ para n suficientemente grande, y el cuerpo de descomposición de f, siendo una extensión finita de $\mathbb{F}_{p^n}$, también será de la forma $\mathbb{F}_{p^N}$ y será un subcuerpo de $\mathbb{F}_{p^\infty}$. Esto demuestra que $\mathbb{F}_{p^\infty}$ es un cuerpo algebraicamente cerrado. Siendo la unión de extensiones finitas de $\mathbb{F}_p$, es una extensión algebraica de $\mathbb{F}_p$. Entonces, $\mathbb{F}_{p^\infty}$ es una cerradura algebraica de $\mathbb{F}_p$.

Sería interesante calcular el grupo de automorfismos $\mathrm{Aut}(\mathbb{F}_{p^\infty})$. Notamos que para todo automorfismo $\sigma\colon \mathbb{F}_{p^\infty} \xrightarrow{\cong} \mathbb{F}_{p^\infty}$ y todo polinomio $f \in \mathbb{F}_p[X]$ se cumple $f(\sigma(x)) = \sigma(f(x))$ para todo $x \in \mathbb{F}_{p^\infty}$. En particular, σ preserva los subcuerpos

$$\mathbb{F}_{p^n} = \{x \in \mathbb{F}_{p^\infty} \mid x^{p^n} - x = 0\},$$

y la restricción de σ a $\mathbb{F}_{p^n}$ es algún automorfismo de $\mathbb{F}_{p^n}$. Recordemos nuestro cálculo de los automorfismos de $\mathbb{F}_{p^n}$ en 15.2.1:

$$\begin{aligned} \mathrm{Aut}(\mathbb{F}_{p^n}) = \langle F \rangle &\cong \mathbb{Z}/n\mathbb{Z}, \\ F^k &\mapsto [k]_n, \end{aligned}$$

donde $F\colon x \mapsto x^p$ es el automorfismo de Frobenius. Puesto que $\mathbb{F}_{p^\infty}$ es la unión de los $\mathbb{F}_{p^n}$, el automorfismo σ está definido de modo único por sus restricciones a $\mathbb{F}_{p^n}$. Notamos que si $m \mid n$, entonces el automorfismo $F^k\colon \mathbb{F}_{p^n}$ se restringe al automorfismo $F^\ell\colon \mathbb{F}_{p^m} \xrightarrow{\cong} \mathbb{F}_{p^m}$, donde $k \equiv \ell \pmod{m}$. Estas consideraciones nos llevan a la siguiente descripción de grupo de automorfismos de $\mathbb{F}_{p^\infty}$:

$$\mathrm{Aut}(\mathbb{F}_{p^\infty}) \cong \widehat{\mathbb{Z}} := \{(x_n)_{n\geq 1} \in \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z} \mid x_n \equiv x_m \pmod{m} \text{ para todo } m \mid n\}.$$

Este grupo se llama el grupo de los **enteros profinitos** y tiene cardinalidad $2^{\aleph_0}$. (Aunque muy grande, considerado como un **grupo topológico**, el grupo $\widehat{\mathbb{Z}}$ deja de ser tan asombroso; de hecho, es un grupo muy natural e importante en aritmética.)

15.6 Ejercicios

Ejercicio 15.1.

1) *Encuentre polinomios irreducibles de grado* 2

$$f \in \mathbb{F}_2[X] \quad y \quad g \in \mathbb{F}_3[X].$$

2) *Consideremos los cuerpos finitos*

$$\mathbb{F}_4 := \mathbb{F}_2[X]/(f) \quad y \quad \mathbb{F}_9 := \mathbb{F}_3[X]/(g)$$

de orden 4 *y* 9 *respectivamente. Escriba las tablas de adición y multiplicación para* $\mathbb{F}_4$ *y* $\mathbb{F}_9$.

3) *Encuentre el orden de cada elemento del grupo multiplicativo* $\mathbb{F}_4^\times$ *y* $\mathbb{F}_9^\times$.

4) *Consideremos la ecuación*

$$y^2 = x^3 - x.$$

Enumere todas sus soluciones $(x, y) \in R^2$, *donde*

$$R = \mathbb{F}_2,\ \mathbb{F}_3,\ \mathbb{F}_4,\ \mathbb{F}_9,\ \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z}.$$

Ejercicio 15.2. *Sea* $q = p^k$ *donde* p *es primo y* $k = 1, 2, 3, \ldots$ *Demuestre que para cualquier* $n = 1, 2, 3, \ldots$ *existe un polinomio mónico irreducible* $f \in \mathbb{F}_q[X]$ *de grado* n. *(Lo probamos en clase para* $k = 1$.*)*

Ejercicio 15.3. *Encuentre isomorfismos explícitos entre los cuerpos*

$$\mathbb{F}_3[X]/(X^2 + 1), \quad \mathbb{F}_3[X]/(X^2 + X + 2), \quad \mathbb{F}_3[X]/(X^2 + 2X + 2).$$

Ejercicio 15.4. *Encuentre los polinomios mónicos irreducibles de grado* 3 *en* $\mathbb{F}_2[X]$ *factorizando* $X^8 - X$.

Ejercicio 15.5. *Sean* p *un número primo y* $n = 1, 2, 3, \ldots$ *Para* $\alpha \in \mathbb{F}_{p^n}$ *definamos*

$$N(\alpha) := \alpha\, \alpha^p\, \alpha^{p^2} \cdots \alpha^{p^{n-1}}.$$

1) *Demuestre que* $N(\alpha) \in \mathbb{F}_p$ *para todo* $\alpha \in \mathbb{F}_{p^n}$.

2) *Demuestre que*

$$N(\alpha\beta) = N(\alpha)\, N(\beta), \quad N(a\alpha) = a^n\, N(\alpha)$$

para cualesquiera $a \in \mathbb{F}_p$, $\alpha, \beta \in \mathbb{F}_{p^n}$.

3) *Demuestre que el homomorfismo de grupos multiplicativos* $N\colon \mathbb{F}_{p^n}^\times \to \mathbb{F}_p^\times$ *es sobreyectivo.*

Indicación: demuestre que $|\ker N| = \frac{p^n - 1}{p - 1}$ *e use el primer teorema de isomorfía.*

Ejercicio 15.6. *Sean* p *un número primo y* $n = 1, 2, 3, \ldots$ *Para el cuerpo finito* $\mathbb{F}_{p^n}$ *y un elemento* $\alpha \in \mathbb{F}_{p^n}$ *definamos* $T(\alpha) := \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$.

1) *Demuestre que* $T(\alpha) \in \mathbb{F}_p$.

2) *Demuestre que* $T\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ *es una aplicación* $\mathbb{F}_p$*-lineal.*

3) *Demuestre que la aplicación* $T\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ *es sobreyectiva.*

Ejercicio 15.7. *Sean* p *y* q *dos diferentes primos impares. Demuestre que el número de polinomios mónicos irreducibles de grado* q *en* $\mathbb{F}_p[X]$ *es igual a* $\frac{1}{q}(p^q - p)$.

Ejercicio 15.8. *Sea* k *un cuerpo.*

1) *Demuestre que los cuadrados en el grupo multiplicativo* $k^\times$ *forman un subgrupo*

$$(k^\times)^2 := \{\alpha \in k^\times \mid \alpha = x^2 \text{ para algún } x \in k^\times\} \subseteq k^\times.$$

2) *Enumere los cuadrados en el grupo* $\mathbb{F}_9^\times$ *para el cuerpo* $\mathbb{F}_9$ *construido en el ejercicio anterior.*

3) *Calcule el grupo cociente* $k^\times/(k^\times)^2$ *para* $k = \mathbb{R}$ *y* $k = \mathbb{F}_q$*, donde* $q = p^k$ *(considere por separado el caso de* $p = 2$ *y* p *impar).*

Ejercicio 15.9. *Sea* $q = p^k$ *donde* p *es un primo impar y* $k = 1, 2, 3, \ldots$

1) *Demuestre que* -1 *es un cuadrado en* $\mathbb{F}_q$ *si y solamente si* -1 *tiene orden* 4 *en el grupo cíclico* $\mathbb{F}_q^\times$.

2) *Concluya que* -1 *es un cuadrado en* $\mathbb{F}_q$ *si y solamente si* $q \equiv 1 \pmod 4$.

3) *Exprese* -1 *como un cuadrado en* $\mathbb{F}_9$.

Ejercicio 15.10 (generalización de 15.8). *Sea* $q = p^k$ *donde* p *es primo y* $k = 1, 2, 3, \ldots$ *Asumamos que* $q \equiv 1 \pmod n$.

1) *Demuestre que para todo* $\alpha \in \mathbb{F}_q^\times$ *la ecuación* $x^n = \alpha$ *o no tiene soluciones, o tiene* n *soluciones.*

2) *Demuestre que el subconjunto*

$$\{\alpha \in \mathbb{F}_q^\times \mid \alpha = x^n \text{ para algún } x \in \mathbb{F}_q^\times\}$$

es un subgrupo de $\mathbb{F}_q^\times$ *de orden* $\frac{q-1}{n}$.

3) *Por ejemplo, encuentre el subgrupo de cubos en* $\mathbb{F}_{13}^\times$.

Ejercicio 15.11. *Supongamos que* p *es un primo tal que* $p \equiv 3 \pmod 4$. *Demuestre que el anillo cociente* $\mathbb{Z}[\sqrt{-1}]/(p)$ *es un cuerpo de* p^2 *elementos.*

Ejercicio 15.12. *Para un entero de Gauss no invertible* $\alpha = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ *demuestre que*

$$\alpha \equiv 1 \pmod{2 + 2\sqrt{-1}}$$

si y solo si se cumple una de las dos condiciones:

1) $a \equiv 1$ y $b \equiv 0 \pmod 4$;

2) $a \equiv 3$ y $b \equiv 2 \pmod 4$.

Ejercicio 15.13. *Usando los resultados que vimos en clase, encuentre la cardinalidad del conjunto*

$$E_0(\mathbb{F}_p) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_p) \mid y^2 = x^3 - x\}$$

para $p = 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$.

Ejercicio 15.14. *Demuestre que si* $p \equiv 1 \pmod 4$, *entonces el número* $\#E(\mathbb{F}_p) = \#E_0(\mathbb{F}_p) + 1$ *es siempre divisible por* 4.

Ejercicio 15.15. *Consideremos*

$$Z(t) = \frac{1 + 3\,t + 5t^2}{(1 - t)\,(1 - 5\,t)} \in \mathbb{Q}(t).$$

1) *Exprese* $Z(t)$ *como una serie*

$$1 + \underbrace{a_1\,t + a_2\,t^2 + a_3\,t^3 + a_4\,t^4 + \cdots}_{=:f} \in \mathbb{Q}[\![t]\!]$$

(calcule por lo menos los coeficientes a_1 y a_2*).*

2) *Calcule los coeficientes* b_1 y b_2 *de la serie*

$$\log(1 + f) := \sum_{k \geq 1} (-1)^{k+1}\,\frac{f^k}{k} = b_1\,t + \frac{b_2}{2}\,t^2 + \frac{b_3}{3}\,t^3 + \frac{b_4}{4}\,t^4 + \cdots \in \mathbb{Q}[\![t]\!]$$

Ejercicio 15.16. *Consideremos el espacio afín de dimensión* n *sobre el cuerpo finito* $\mathbb{F}_{q^k}$*:*

$$\mathbb{A}^n(\mathbb{F}_{q^k}) = \mathbb{F}_{q^k}^n.$$

Encuentre la expresión racional para la función zeta

$$Z(\mathbb{A}^n_{/\mathbb{F}_q}, t) := \exp\left(\sum_{k \geq 1} \#\mathbb{A}^n(\mathbb{F}_{q^k})\,\frac{t^k}{k}\right).$$

Ejercicio 15.17. *Para los conjuntos*

$$V_1(\mathbb{F}_{q^k}) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_{q^k}) \mid xy = 0\},$$
$$V_2(\mathbb{F}_{q^k}) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_{q^k}) \mid x^2 - y^2 = 0\},$$
$$V_3(\mathbb{F}_{q^k}) := \{(x, y, z) \in \mathbb{A}^3(\mathbb{F}_{q^k}) \mid x^2 = y^2 = z^2\}$$

encuentre la expresión racional para $Z(V_{1/\mathbb{F}_q}, t)$, $Z(V_{2/\mathbb{F}_q}, t)$, $Z(V_{3/\mathbb{F}_q}, t)$.

Ejercicio 15.18. *Demuestre que si* F *es un cuerpo de característica diferente de* 2 *(posiblemente infinito), entonces existe una biyección entre los conjuntos*

$$V_1(F) := \{(x, y) \in \mathbb{A}^2(F) \mid xy = 0\},$$
$$V_2(F) := \{(x, y) \in \mathbb{A}^2(F) \mid x^2 - y^2 = 0\}.$$

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, se mencionan en el 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

$$d := \text{mín}\{x \in A \mid x > 0\}.$$

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 $\pm p$.

[*] 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 $d = 0$.

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, ...

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.*

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 $d := \mathrm{mcd}(a, b)$ caracterizado por las siguientes propiedades:

1) $d \mid a$ y $d \mid b$,

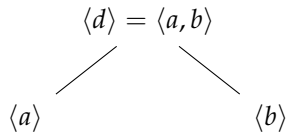
2) si d' es otro número tal que $d' \mid a$ y $d' \mid b$, entonces $d' \mid d$.

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*

$$\langle a, b\rangle = \langle d\rangle \quad \textit{donde } d = \operatorname{mcd}(a, b).$$

En particular, se cumple

$$ax + by = \operatorname{mcd}(a, b) \quad \textit{para algunos } x, y \in \mathbb{Z}$$

y $\operatorname{mcd}(a, b)$ *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 $\operatorname{mcd}(a, b)$.

1) La definición de $d := \operatorname{mcd}(a, b)$ caracteriza a d *salvo signo*. De hecho, si d y d' satisfacen las condiciones de $\operatorname{mcd}(a, b)$, 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 $\operatorname{mcd}(a, b)$ pueden ser interpretadas salvo signo.

2) La definición de $\operatorname{mcd}(a, b)$ es visiblemente simétrica en a y b, así que

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

3) Para todo $a \in \mathbb{Z}$ se tiene

$$\operatorname{mcd}(a, 0) = a.$$

En particular[*],

$$\operatorname{mcd}(0, 0) = 0.$$

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 $a = 0$.

[*]Algunas fuentes insisten que $\operatorname{mcd}(0, 0)$ no está definido, pero como vemos, es lógico poner $\operatorname{mcd}(0, 0) = 0$.

A.3.3. Definición. Si $\mathrm{mcd}(a,b) = 1$, 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, $\mathrm{mcd}(p,b) = 1$ y luego $p \mid c$ por el resultado precedente. En el segundo caso, $\mathrm{mcd}(p,b) = p$, 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 $m := \mathrm{mcm}(a,b)$ caracterizado por las siguientes propiedades:

1) $a \mid m$ y $b \mid m$,

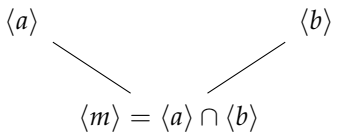
2) si m' es otro número tal que $a \mid m'$ y $b \mid m'$, entonces $m \mid m'$.

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 $\langle m'\rangle \subseteq \langle m\rangle$.

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*

$$\langle a\rangle \cap \langle b\rangle = \langle m\rangle \quad \textit{donde } m = \mathrm{mcm}(a,b).$$

Tenemos las siguientes propiedades.

1) La definición caracteriza a $\mathrm{mcm}(a,b)$ de modo único salvo signo.

2) Para cualesquiera $a, b \in \mathbb{Z}$ se tiene

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

3) Para todo a se cumple

$$\mathrm{mcm}(a,0) = a.$$

En particular,

$$\mathrm{mcm}(0,0) = 0.$$

(De hecho, $0 \mid m$ implica que $m = 0$.)

A.4.3. Proposición. *Para cualesquiera $a, b \in \mathbb{Z}$ tenemos*

$$\mathrm{mcm}(a,b) \cdot \mathrm{mcd}(a,b) = ab.$$

En particular,

$$\mathrm{mcm}(a,b) = ab \text{ si y solamente si } a \text{ y } b \text{ son coprimos}.$$

Primera demostración. El caso de $a = b = 0$ es trivial y podemos descartarlo. Sea $d := \mathrm{mcd}(a,b)$ y $m := ab/d$. Vamos a ver que $m = \mathrm{mcm}(a,b)$.

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

$$d = \mathrm{mcd}(a,b) = \mathrm{mcd}(da', db') = d \cdot \mathrm{mcd}(a', b'),$$

así que

$$\mathrm{mcd}(a', b') = 1$$

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

$$m \mid \mathrm{mcd}(m'b', m'a') = m' \cdot \mathrm{mcd}(a', b') = m'.$$

■

Segunda demostración, usando la teoría de grupos. Consideremos los subgrupos $m\mathbb{Z}$ y $n\mathbb{Z}$ en $\mathbb{Z}$. Luego, el segundo teorema de isomorfía nos dice que

$$a\mathbb{Z}/(a\mathbb{Z}\cap b\mathbb{Z}) \cong (a\mathbb{Z}+b\mathbb{Z})/b\mathbb{Z}$$

(véase el capítulo 7 y los ejercicios). Tenemos $a\mathbb{Z}\cap b\mathbb{Z} = m\mathbb{Z}$ donde $m = \operatorname{mcm}(a,b)$ y $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$ donde $d = \operatorname{mcd}(a,b)$. Entonces,

$$a\mathbb{Z}/m\mathbb{Z} \cong d\mathbb{Z}/b\mathbb{Z}.$$

Lo que nos da la identidad $a/m = d/b$. ■

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

$$x_1a_1+\cdots+x_na_n = \operatorname{mcd}(a_1,\ldots,a_n).$$

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:

$$v_p(n) := \max\{k \mid p^k \mid n\}.$$

(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 $\text{mcm}(a,b)$ y $\text{mcd}(a,b)$ están definidos salvo un múltiplo $u \in R^\times$. Para $R = \mathbb{Z}$ tenemos $\mathbb{Z}^\times = \{\pm 1\}$. Sin embargo, la existencia de $\text{mcm}(a,b)$ y $\text{mcd}(a,b)$ 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 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 estudia en el capítulo 13.

Apéndice B
Lema de Zorn

El lema de Zorn es una versión equivalente del **axioma de elección**[*] que se utiliza muy a menudo en álgebra. Aquí vamos a revisar el enunciado y un par de aplicaciones típicas.

B.1 Lema de Zorn

B.1.1. Definición. Se dice que un conjunto $\mathcal{P}$ es **parcialmente ordenado** si sobre los elementos de $\mathcal{P}$ está definida una relación $\preceq$ que satisface los siguientes axiomas.

1) **Reflexividad**: para todo $x \in \mathcal{P}$ se cumple $x \preceq x$.

2) **Antisimetría**: para cualesquiera $x, y \in \mathcal{P}$ si $x \preceq y$ e $y \preceq x$, entonces $x = y$.

3) **Transitividad**: para cualesquiera $x, y, z \in \mathcal{P}$ si $x \preceq y$ e $y \preceq z$, entonces $x \preceq z$.

Se dice que $m \in \mathcal{P}$ es un elemento **maximal** si no existe otro elemento $x \in \mathcal{P}$ tal que $m \preceq x$.

Se dice que un subconjunto $\mathcal{S} \subseteq \mathcal{P}$ es una **cadena** si para cualesquiera $s, s' \in \mathcal{S}$ se tiene $s \preceq s'$ o $s' \preceq s$.

Se dice que un subconjunto $\mathcal{S} \subseteq \mathcal{P}$ es **acotado** si existe $t \in \mathcal{P}$ (una **cota superior**) tal que $s \preceq t$ para todo $s \in \mathcal{S}$.

B.1.2. Lema de Zorn. *Sea $\mathcal{P}$ un conjunto parcialmente ordenado no vacío. Supongamos que toda cadena en $\mathcal{P}$ es acotada. Entonces, $\mathcal{P}$ posee un elemento maximal.*

B.2 Aplicación: bases de espacios vectoriales

La primera aplicación del lema de Zorn debe de ser conocida al lector. Recordemos primero algunas definiciones de álgebra lineal. Sea k un cuerpo. Para un espacio vectorial V

[*] Esto no es un curso de lógica, así que no voy a probar la equivalencia; el lector puede consultar otras fuentes, por ejemplo [Lan2002, Appendix 2].

sobre k y un subconjunto $S \subset V$ el subespacio vectorial **generado** por S es el subconjunto de las sumas finitas

$$\sum_{1 \leq i \leq n} \lambda_i \, v_i$$

donde $\lambda_i \in k$ y $v_i \in S$. Se dice que los elementos de S son **linealmente independientes** si para cualesquiera $\{v_1, \ldots, v_n\} \subseteq S$, si

$$\sum_{1 \leq i \leq n} \lambda_i \, v_i = 0,$$

entonces $\lambda_1 = \cdots = \lambda_n = 0$. Se dice que S es una **base** de V si $\langle S \rangle = V$ y los elementos de S son linealmente independientes.

B.2.1. Teorema. *Sea V un espacio vectorial no nulo y sea $S \subset V$ un subconjunto linealmente independiente. Entonces, S puede ser completado a una base de V.*

Demostración. Sea $\mathcal{P}$ el conjunto de los subconjuntos linealmente independientes $T \subseteq V$ tales que $S \subseteq T$, parcialmente ordenado respecto a la inclusión. En particular, $S \in \mathcal{P}$, así que $\mathcal{P} \neq \emptyset$.

Sea $\{T_\alpha\}$ una cadena en $\mathcal{P}$; es decir, una colección de conjuntos linealmente independientes $T_\alpha \subset V$ tales que

1) $S \subseteq T_\alpha$ para todo α,

2) para cualesquiera α y β se tiene $T_\alpha \subseteq T_\beta$ o $T_\beta \subseteq T_\alpha$.

Tomemos la unión $T := \bigcup_\alpha T_\alpha$. Tenemos $S \subseteq T_\alpha \subseteq T$ para todo α. Además para una colección finita de vectores $\{v_1, \ldots, v_n\} \subseteq T$ tenemos $v_i \in T_{\alpha_i}$ para algunos α_i, y ya que $\{T_\alpha\}$ es una cadena, todos estos vectores pertenecen a algún conjunto T_α y por ende son linealmente independientes. Esto significa que $T \in \mathcal{P}$ y es una cota superior para la cadena.

Ahora el lema de Zorn implica que existe un elemento maximal en $\mathcal{P}$; es decir, un conjunto linealmente independiente B tal que $S \subseteq B$ y B no está contenido en ningún otro conjunto linealmente independiente. Vamos a probar que los elementos de B generan a V.

Supongamos que $\langle B \rangle \subsetneq V$. En este caso existe un vector $v \in V$, $v \notin \langle B \rangle$. Vamos a ver que esto implica que el conjunto $B \cup \{v\}$ es linealmente independiente. Si $B \cup \{v\}$ fuera linealmente dependiente, entonces existiría una combinación lineal

$$\lambda \, v + \lambda_1 \, v_1 + \cdots + \lambda_n \, v_n = 0$$

donde $\lambda, \lambda_i \in k$ son escalares, no todos nulos, y $v_1, \ldots, v_n \in B$. Dado que los elementos de B son linealmente independientes, tenemos necesariamente $\lambda \neq 0$. Sin embargo, en este caso

$$v = -\left(\frac{\lambda_1}{\lambda} \, v_1 + \cdots + \frac{\lambda_n}{\lambda} \, v_n \right),$$

lo que implica que $v \in \langle B \rangle$. Entonces, el conjunto $B \cup \{v\}$ debe ser linealmente independiente.

Esto contradice el hecho de que B sea un conjunto linealmente independiente maximal, y por lo tanto $\langle B \rangle = V$. ■

B.2.2. Corolario. *Todo espacio vectorial no nulo posee una base.*

Demostración. En el resultado anterior, basta tomar $S = \{v\}$ donde v es cualquier vector no nulo en V. ■

B.2.3. Corolario. *Sea V un espacio vectorial no nulo. Para todo subespacio $U \subset V$ existe otro espacio $W \subset V$ tal que $V = U \oplus W$.*

Demostración. Según el teorema, podemos escoger una base S de U, y luego completarla a una base B de V. Sea W el subespacio generado por $B \setminus S$. Se puede verificar que $V = U + W$ y $U \cap W = \{0\}$. ■

B.3 Aplicación: grupos abelianos divisibles (*)

Recordemos que un grupo abeliano D es **divisible** si para cualesquiera $x \in D$ y $n = 1, 2, 3, \ldots$ existe $y \in D$ tal que $ny = x$. Hemos encontrado estos grupos en los ejercicios. Por ejemplo, los grupos $\mathbb{Q}, \mathbb{R}, \mathbb{Q}/\mathbb{Z}, \mathbb{R}/\mathbb{Z}$ son divisibles. He aquí una caracterización importante de grupos divisibles.

B.3.1. Teorema (Reinhold Baer, 1940). *Sea D un grupo abeliano. Las siguientes condiciones son equivalentes.*

1) *Para todo grupo abeliano A y un subgrupo $B \subseteq A$ cualquier homomorfismo $f\colon B \to D$ se extiende a un homomorfismo $\widetilde{f}\colon A \to D$:*

$$\begin{array}{ccc} B & \hookrightarrow & A \\ {\scriptstyle f}\downarrow & \swarrow_{\exists \widetilde{f}} & \\ D & & \end{array}$$

$$\widetilde{f}\Big|_B = f.$$

2) *D es divisible.*

Demostración. La implicación fácil es 1) $\Rightarrow$ 2). Para $n = 1, 2, 3, \ldots$ consideremos el subgrupo $n\mathbb{Z} \subseteq \mathbb{Z}$. Un elemento $x \in D$ corresponde a un homomorfismo

$$f\colon n\mathbb{Z} \to D, \quad an \mapsto ax.$$

Luego, si D cumple la propiedad 1), entonces f se extiende a $\widetilde{f}$:

$$\begin{array}{ccc} n\mathbb{Z} & \hookrightarrow & \mathbb{Z} \\ {\scriptstyle f}\downarrow & \swarrow_{\exists \widetilde{f}} & \\ D & & \end{array}$$

Tenemos

$$n \cdot \widetilde{f}(1) = \widetilde{f}(n \cdot 1) = f(n) = x.$$

Esto demuestra que x es divisible por n.

Para probar 2) $\Rightarrow$ 1), primero notamos que si D es divisible, entonces la propiedad 1) se cumple para los subgrupos de $\mathbb{Z}$: como arriba, todo homomorfismo $f\colon n\mathbb{Z} \to D$ se extiende a $\widetilde{f}\colon \mathbb{Z} \to D$. De hecho, f está definido por la imagen $f(n) = x \in D$, y por la divisibilidad existe $y \in D$ tal que $n \cdot y = x$. Podemos definir

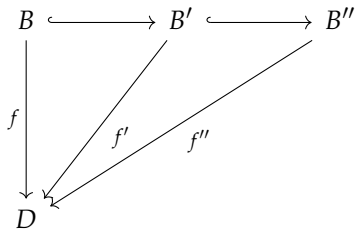
$$\widetilde{f}\colon \mathbb{Z} \to D, \quad 1 \mapsto y.$$

Ahora para todo $an \in n\mathbb{Z}$ se cumple

$$\widetilde{f}(an) = an\,\widetilde{f}(1) = any = ax = a\,f(n) = f(an).$$

Procedamos con la prueba. Sean A un grupo abeliano, $B \subseteq A$ un subgrupo y $f\colon B \to D$ un homomorfismo. Sea $\mathcal{P}$ un conjunto de los pares (B', f') donde $B \subseteq B' \subseteq A$ es un subgrupo que contiene a B y $f'\colon B' \to D$ es un homomorfismo tal que $f = f'|_B$. En particular, $(B, f) \in \mathcal{P}$, así que $\mathcal{P} \neq \emptyset$. Consideremos la siguiente relación sobre $\mathcal{P}$:

$$(B', f') \preceq (B'', f'') \iff B' \subseteq B'' \text{ y } f''|_{B'} = f'.$$



El conjunto $\mathcal{P}$ es parcialmente ordenado respecto a esta relación. Para una cadena $\{(B_\alpha, f_\alpha)\}$ podemos considerar la unión $\bigcup_\alpha B_\alpha$. Puesto que $\{(B_\alpha, f_\alpha)\}$ es una cadena, se ve que $\bigcup_\alpha B_\alpha$ es un subgrupo abeliano de A tal que $B_\alpha \subseteq \bigcup_\alpha B_\alpha$ para todo α. Podemos definir un homomorfismo $\phi\colon \bigcup_\alpha B_\alpha \to D$ de la siguiente manera: para todo $x \in \bigcup_\alpha B_\alpha$ tenemos $x \in B_\alpha$ para algún α, y pongamos $\phi(x) := f_\alpha(x)$. Dado que $\{(B_\alpha, f_\alpha)\}$ es una cadena en $\mathcal{P}$, esto nos da un homomorfismo bien definido. Por la definición, $\phi|_{B_\alpha} = f_\alpha$ para todo α. Entonces, $(\bigcup_\alpha B_\alpha, \phi)$ es una cota superior para la cadena.

El lema de Zorn implica que $\mathcal{P}$ posee un elemento maximal (B', f'). Necesitamos probar que $B' = A$. Supongamos que $B' \subsetneq A$. Entonces, existe algún elemento $x \in A \setminus B'$, y podemos considerar el conjunto

$$C := \{a \in \mathbb{Z} \mid a \cdot x \in B'\} \subseteq \mathbb{Z}.$$

Se ve que esto es un subgrupo de $\mathbb{Z}$. Consideremos el homomorfismo de grupos abelianos

$$g\colon C \to D, \quad a \mapsto f'(a \cdot x).$$

Como hemos notado, dado que D es divisible, el homomorfismo g se extiende a un homomorfismo $\widetilde{g}\colon \mathbb{Z} \to D$:

$$\begin{array}{ccc} C & \hookrightarrow & \mathbb{Z} \\ {\scriptstyle g}\downarrow & \swarrow_{\exists \widetilde{g}} & \\ D & & \end{array}$$

Consideremos ahora el subgrupo $B'' := \langle B' \cup \{x\} \rangle$. Sus elementos son sumas $y + nx$ donde $y \in B'$ y $n \in \mathbb{Z}$. Por nuestra hipótesis que $x \notin B'$, se tiene $B' \subsetneq B'' \subseteq A$. Consideramos la aplicación

$$\begin{aligned} f''\colon B'' &\to A, \\ y + nx &\mapsto \widetilde{g}(n) + f'(y). \end{aligned}$$

Se ve que esto es un homomorfismo de grupos abelianos y $f''|_{B'} = f'$. Entonces, $(B', f') \preceq (B'', f'')$. Pero esto contradice la maximalidad de (B', f'). Podemos concluir que $B' = A$. ■

De aquí podemos deducir otra caracterización de grupos divisibles.

B.3.2. Corolario. *D es un grupo abeliano divisible si y solamente si todo monomorfismo de grupos abelianos $i\colon D \rightarrowtail A$ admite un homomorfismo $r\colon A \to D$ tal que $r \circ i = \mathrm{id}_D$.*

Demostración. Supongamos que D es divisible. Un monomorfismo $i\colon D \rightarrowtail A$ induce un isomorfismo $\bar{i}\colon D \xrightarrow{\cong} \operatorname{im} i$. El teorema anterior nos dice que $\bar{i}^{-1}\colon \operatorname{im} i \xrightarrow{\cong} D$ se extiende al grupo A:

$$\begin{array}{ccc} \operatorname{im} i & \hookrightarrow & A \\ {\scriptstyle \bar{i}^{-1}}\downarrow & \swarrow_{\exists r} & \\ D & & \end{array}$$

Tenemos $r|_{\operatorname{im} i} = \bar{i}^{-1}$, así que $r \circ i = \bar{i}^{-1} \circ \bar{i} = \mathrm{id}_D$.

Viceversa, supongamos que todo monomorfismo $i\colon D \rightarrowtail A$ admite un homomorfismo $r\colon A \to D$ tal que $r \circ i = \mathrm{id}_D$. Para un elemento $x \in D$ y $n = 1, 2, 3, \ldots$ consideremos el conjunto

$$C := \{(a \cdot x, -an) \mid a \in \mathbb{Z}\} \subseteq D \times \mathbb{Z}.$$

Esto es un subgrupo de $D \times \mathbb{Z}$: tenemos $(0,0) = (0 \cdot x, -0 \cdot n) \in C$, y luego para cualesquiera $a, b \in \mathbb{Z}$

$$(a \cdot x, -an) \pm (b \cdot x, -bn) = ((a \pm b) \cdot x, -(a \pm b)\, n).$$

Podemos pasar al grupo cociente $(D \times \mathbb{Z})/C$ y considerar el homomorfismo

$$\begin{aligned} i\colon D &\to (D \times \mathbb{Z})/C, \\ z &\mapsto (z, 0) + C \end{aligned}$$

(esto es la composición de la inclusión de D como un subgrupo de $D \times \mathbb{Z}$ con la proyección sobre el grupo cociente). Notamos que

$$(x, 0) - (0, n) = (x, -n) = (1 \cdot x, -1 \cdot n) \in C,$$

así que

$$i(x) = (0, n) + C \quad \text{en } (D \times \mathbb{Z})/C.$$

Verifiquemos que i es un monomorfismo: si tenemos

$$(z, 0) - (z', 0) \in C,$$

entonces

$$(z - z', 0) = (a \cdot x, -an)$$

para algún $a \in \mathbb{Z}$. Sin embargo, $n \neq 0$, así que esto significa que $a = 0$ y luego $z - z' = 0 \cdot x = 0$, y por ende $z = z'$. Entonces, por nuestra hipótesis, existe un homomorfismo $r\colon (D \times \mathbb{Z})/C \to D$ tal que $r \circ i = \mathrm{id}_D$. En particular,

$$x = r \circ i(x) = r((0, n) + C) = n \cdot r((0, 1) + C).$$

Esto establece la divisibilidad de x por n. ■

Apéndice C
Álgebra lineal

El propósito de este breve apéndice es juntar algunos resultados básicos de álgebra lineal sobre el polinomio característico.

Aquí K denotará un cuerpo y V un espacio K-vectorial de dimensión finita n.

C.1 El determinante y traza de un endomorfismo lineal

Escojamos una base $e_1, \ldots, e_n$ de V. Para toda aplicación K-lineal $\phi\colon V \to V$ (es decir, un **endomorfismo** de V) se tiene

$$\phi(e_j) = \sum_{1 \leq i \leq n} a_{ij}\, e_i$$

para algunos $a_{ij} \in K$. Los elementos a_{ij} forman una matriz de $n \times n$

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

Bajo esta convención, los vectores de V se representan por las matrices columna:

$$v = c_1\, e_1 + c_2\, e_2 + \cdots + c_n\, e_n \leftrightarrow \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$$

y a $\phi(v)$ corresponde la matriz columna se obtiene multiplicando la matriz de arriba por A por la izquierda:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}.$$

Las aplicaciones K-lineales $\phi, \psi\colon V \to V$ forman un anillo (no conmutativo) $\mathrm{End}_K(V)$ respecto a la suma punto por punto y la composición habitual como la multiplicación

$$(\phi + \psi)(v) := \phi(v) + \psi(v), \quad (\phi \circ \psi)(v) := \phi(\psi(v)).$$

A cada elemento $a \in K$ corresponde el endomorfismo

$$\mu_a\colon V \to V, \quad v \mapsto a\,v.$$

La aplicación

$$K \to \mathrm{End}(V), \quad a \mapsto \mu_a$$

es un homomorfismo de anillos que define una estructura de K-álgebra sobre $\mathrm{End}_K(V)$ y en particular de un espacio K-vectorial. La correspondencia

$$\begin{gathered}\mathrm{End}_K(V) \to M_n(K),\\ \phi \mapsto A\end{gathered}$$

define un isomorfismo de K-álgebras, y en particular de espacios vectoriales sobre K.

C.1.1. Definición. El **determinante** y la **traza** de un endomorfismo $\phi\colon V \to V$ se definen como es el determinante y la traza de la matriz correspondiente respecto a alguna base:

$$\det\phi := \det A, \quad \mathrm{tr}\,\phi := \mathrm{tr}\,A = a_{11} + a_{22} + \cdots + a_{nn}.$$

Estas definiciones no dependen de una base particular. En efecto, el determinante es multiplicativo:

$$\det(AB) = \det(A)\cdot\det(B) \quad \text{para cualesquiera } A, B \in M_n(K),$$

mientras que la traza satisface la propiedad

$$\mathrm{tr}(AB) = \mathrm{tr}(BA) \quad \text{para cualesquiera } A, B \in M_n(K).$$

Ahora la matriz de ϕ respecto a otra base $e'_1, \ldots, e'_n$ es de la forma $B = U\,A\,U^{-1}$, donde $U \in \mathrm{GL}_n(K)$ es alguna matriz invertible (la matriz de cambio de base), y luego

$$\det(U\,A\,U^{-1}) = \det(U)\cdot\det(A)\cdot\det(U)^{-1} = \det(A), \quad \mathrm{tr}(U\,A\,U^{-1}) = \mathrm{tr}(A\,U^{-1}\,U) = \mathrm{tr}(A).$$

C.1.2. Observación. *Sean $\phi, \psi\colon V \to V$ aplicaciones K-lineales.*

1) *El determinante es multiplicativo:* $\det(\phi\circ\psi) = \det(\phi)\cdot\det(\psi)$.

2) *La traza es K-lineal:* $\mathrm{tr}(a\,\phi + b\,\psi) = a\ \mathrm{tr}(\phi) + b\ \mathrm{tr}(\psi)$ *para cualesquiera $a, b \in K$.*

Demostración. Se sigue de las identidades $\det(AB) = \det(A)\cdot\det(B)$ y $\mathrm{tr}(a\,A + b\,B) = a\ \mathrm{tr}(A) + b\ \mathrm{tr}(B)$ para las matrices. ■

C.2 El polinomio característico

C.2.1. Definición. Para una matriz

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \in M_n(K)$$

el **polinomio característico** correspondiente viene dado por

$$p_A := \det(X \cdot I_n - A) := \det \begin{pmatrix} X - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & X - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & X - a_{nn} \end{pmatrix} \in K[X].$$

Si V es un espacio vectorial sobre K de dimensión n, entonces para un endomorfismo $\phi\colon V \to V$ el **polinomio característico** se define como

$$p_\phi := p_A,$$

donde A es una matriz que representa a ϕ en alguna base.

Notamos que si $B = U\,A\,U^{-1}$ para alguna matriz invertible U, entonces $p_B = p_A$:

$$p_B = \det(X \cdot I_n - U\,A\,U^{-1}) = \det(U^{-1}\,(X \cdot I_n - U\,A\,U^{-1})\,U) = \det(X \cdot I_n - A) = p_A.$$

Esto significa que el polinomio característico está bien definido para un endomorfismo $\phi\colon V \to V$.

C.2.2. Ejemplo. Para una matriz de 2×2

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

tenemos

$$p_A = \det \begin{pmatrix} X - a & -b \\ -c & X - d \end{pmatrix} = (X - a)\,(X - d) - bc = X^2 - (a + d)\,X + (ad - bc).$$

▲

C.2.3. Proposición. *Sea V un espacio vectorial sobre K de dimensión finita n. Para un endomorfismo $\phi\colon V \to V$ el polinomio característico p_A es un polinomio mónico de grado n:*

$$p_\phi = X^n + a_{n-1}\,X^{n-1} + \cdots + a_1\,X + a_0 \in K[X].$$

Además,

$$a_{n-1} = -\operatorname{tr}\phi, \quad a_0 = (-1)^n\,\det\phi.$$

Demostración. Sea A una matriz de $n \times n$ con coeficientes en K que representa a ϕ en alguna base. Por la definición, $p_\phi := p_A$ es el determinante de la matriz

$$B := \begin{pmatrix} X - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & X - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & X - a_{nn} \end{pmatrix} \in M_n(K[X]).$$

Tenemos entonces

$$p_A = \sum_{\sigma \in S_n} b_{1,\sigma(1)} \cdots b_{n,\sigma(n)}.$$

El único término de la suma que tiene grado n o $n-1$ corresponde a $\sigma = \mathrm{id}$, así que los coeficientes de X^n y X^{n-1} son los mismos que los coeficientes correspondientes en el polinomio

$$(X - a_{11}) \cdots (X - a_{nn}) = X^n - (a_{11} + \cdots + a_{nn})\, X^{n-1} + \cdots .$$

El término constante es

$$p_A(0) = \det(0 \cdot I_n - A) = \det(-A) = \det(-I_n) \cdot \det(A) = (-1)^n \det A.$$

■

Para cualquier polinomio $f = c_m\, X^m + c_{m-1}\, X^{m-1} + \cdots + c_1\, X + c_0 \in K[X]$ y un endomorfismo ϕ pongamos

$$f(\phi) := c_m\, \phi^m + c_{m-1}\, \phi^{m-1} + \cdots + c_1\, \phi + c_0\, \mathrm{id} \in \mathrm{End}_K(V),$$

donde

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

C.2.4. Proposición (Teorema de Cayley–Hamilton). *Sea $\phi\colon V \to V$ un endomorfismo de un espacio vectorial sobre K de dimensión finita. Entonces, el polinomio característico satisface $p_\phi(\phi) = 0$.*

Demostración. Fijemos una base de V. Sea $A \in M_n(K)$ la matriz que representa a ϕ en esta base. Pongamos $B := X \cdot I_n - A$. Tenemos

$$p_A := \det B = X^n + a_{n-1}\, X^{n-1} + \cdots + a_1\, X + a_0$$

para algunos $a_0, a_1, \ldots, a_{n-1} \in K$. Tenemos que probar que

$$p_A(A) = A^n + a_{n-1}\, A^{n-1} + \cdots + a_1\, A + a_0\, I_n = O.$$

La matriz adjunta de B tiene forma

$$\mathrm{adj}\, B = X^{n-1} \cdot B_{n-1} + X^{n-2} \cdot B_{n-2} + \cdots + X \cdot B_1 + B_0$$

para algunas matrices $B_0, B_1, \ldots, B_{n-1} \in M_n(K)$ (note que cada cofactor de B es un polinomio de grado $\leq n-1$). Las entradas de $\operatorname{adj} B$ son algunos polinomios de grado $\leq n-1$. Tenemos

$$\det B \cdot I_n = B \cdot \operatorname{adj} B = (X \cdot I_n - A) \cdot \operatorname{adj} B = X \cdot \operatorname{adj} B - A \cdot \operatorname{adj} B,$$

de donde

$$\begin{aligned} &X^n \cdot I_n + a_{n-1} X^{n-1} \cdot I_n + a_{n-2} X^{n-2} \cdot I_n + \cdots + a_1 X \cdot I_n + a_0 \cdot I_n \\ &= X^n \cdot B_{n-1} + X^{n-1} \cdot B_{n-2} + \cdots + X^2 \cdot B_1 + X \cdot B_0 - (X^{n-1} \cdot AB_{n-1} + \cdots + X \cdot AB_1 + AB_0). \end{aligned}$$

Al igualar los coeficientes de las mismas potencias de X, se obtiene un sistema de ecuaciones

$$\begin{aligned} I_n &= B_{n-1}, \\ a_{n-1} \cdot I_n &= B_{n-2} - AB_{n-1}, \\ a_{n-2} \cdot I_n &= B_{n-3} - AB_{n-2}, \\ &\cdots \\ a_2 \cdot I_n &= B_1 - AB_2, \\ a_1 \cdot I_n &= B_0 - AB_1, \\ a_0 \cdot I_n &= -AB_0. \end{aligned}$$

Multpliquemos la primera ecuación por A^n por la izquierda, la segunda por A^{n-1}, etcétera:

$$\begin{aligned} A^n &= A^n B_{n-1}, \\ a_{n-1} A^{n-1} &= A^{n-1} B_{n-2} - A^n B_{n-1}, \\ a_{n-2} A^{n-2} &= A^{n-2} B_{n-3} - A^{n-1} B_{n-2}, \\ &\cdots \\ a_2 A^2 &= A^2 B_1 - A^3 B_2, \\ a_1 A &= AB_0 - A^2 B_1, \\ a_0 I_n &= -AB_0. \end{aligned}$$

Al sumar todas estas ecuaciones, nos queda

$$p_A(A) = O.$$

■

C.2.5. Comentario. Se conoce la siguiente prueba cómica del teorema de Cayley–Hamilton:

$$p_A(A) = \det(A \cdot I_n - A) = \det(O) = 0.$$

Sin embargo, esto no tiene sentido: $p_A(B)$ es una matriz, mientras que para cualquier matriz B, el determinante $\det(B - A)$ es un elemento de K.

C.2.6. Comentario. El espacio de matrices $M_n(K)$ tiene dimensión n^2 sobre K: como una base se pueden tomar las matrices elementales e_{ij} donde $1 \leq i, j \leq n$. De manera equivalente, el espacio vectorial $\mathrm{End}_K(V)$ tiene dimensión n^2, donde $n = \dim_K(V)$. De aquí está claro que todo endomorfismo $\phi \in \mathrm{End}_K(V)$ satisface algún polinomio no nulo de grado $\leq n^2$: las potencias $\phi^0 = \mathrm{id}, \phi, \phi^2, \ldots, \phi^{n^2}$ son necesariamente linealmente dependientes, así que existen algunos coeficientes $c_0, c_1, \ldots, c_{n^2} \in K$, no todos nulos, tales que

$$c_{n^2}\,\phi^{n^2} + \cdots + c_2\,\phi^2 + c_1\,\phi + c_0\,\mathrm{id} = 0.$$

El teorema de Cayley–Hamilton es un resultado sorprendende porque este nos dice que tal polinomio no nulo puede tener grado n y lo construye de modo explícito.

C.2.7. Comentario. El determinante, traza y polinomio característico eventualmente están bien definidos para endomorfismos $\phi\colon V \to V$, lo que sugiere que debe haber definiciones y pruebas más elegantes y moralmente correctas que no usan elección de base y matrices. Hemos usado las matrices para ahorrar tiempo y también porque eventualmente nos interesan ejemplos y cálculos explícitos.

Apéndice D
Fórmula de inversión de Möbius

En este apéndice vamos a probar la **fórmula de inversión de Möbius** que es una encarnación del principio de inclusión-exclusión.

D.1 Función de Möbius

D.1.1. Definición. Para un entero positivo n la **función de Möbius** se define por

$$\mu(1) := 1, \quad \mu(n) = 0 \text{ si } n \text{ no es libre de cuadrados,}$$

y para n libre de cuadrados se pone

$$\mu(p_1 \cdots p_k) := (-1)^k,$$

donde k es el número de diferentes números primos que aparecen en la factorización de n.

D.1.2. Ejemplo. He aquí los primeros valores de la función de Möbius.

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	$\cdots$
$\mu(n)$:	$+1$	-1	-1	0	-1	$+1$	-1	0	0	$+1$	-1	0	-1	$\cdots$

▲

D.1.3. Lema. *Para todo $n > 0$ se tiene*

$$\sum_{d|n} \mu(d) = 0.$$

Demostración. Escribamos $n = p_1^{k_1} \cdots p_s^{k_s}$. Tenemos

$$\sum_{d|n} \mu(d) = \sum_{(e_1,\ldots,e_s)} \mu(p_1^{e_1} \cdots p_s^{e_s}),$$

donde $e_i = 0$ o 1. Luego,

$$\sum_{d|n} \mu(d) = 1 - s + \binom{s}{2} - \binom{s}{3} + \cdots + (-1)^s = (1-1)^s = 0.$$

■

D.2 Fórmula de inversión

Para dos funciones $f, g\colon \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ definamos su **producto de Dirichlet** mediante

$$(f * g)(n) := \sum_{d_1 d_2 = n} f(d_1)\, g(d_2).$$

Este producto es asociativo:

$$((f * g) * h)(n) = (f * (g * h))(n) = \sum_{d_1 d_2 d_3 = n} f(d_1)\, g(d_2)\, h(d_3).$$

Definamos las funciones $\mathbb{I}$ e I mediante

$$\mathbb{I}(n) := \begin{cases} 1, & n = 1, \\ 0, & n > 1; \end{cases} \qquad I(n) := 1 \text{ para todo } n \geq 1.$$

D.2.1. Lema. *Se tiene $I * \mu = \mu * I = \mathbb{I}$.*

Demostración. Si $n = 1$, entonces

$$(I * \mu)(1) = (\mu * I)(1) = 1.$$

Para $n > 1$, se tiene

$$(\mu * I)(n) = (I * \mu)(n) = \sum_{d \mid n} \mu(d) = 0.$$

■

D.2.2. Proposición (Fórmula de inversión de Möbius). *Para una función $f\colon \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ definamos*

$$F(n) := (f * I) := \sum_{d \mid n} f(d).$$

Luego,

$$f(n) = \sum_{d \mid n} \mu(d)\, F\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right)\, F(d).$$

Demostración. Tenemos

$$F * \mu = (f * I) * \mu = f * (I * \mu) = f * \mathbb{I} = f.$$

Entonces,

$$(F * \mu)(n) = \sum_{d \mid n} \mu(d)\, F\left(\frac{n}{d}\right) = f(n).$$

■

D.2.3. Ejemplo. Para la función ϕ de Euler se tiene $\sum_{d|n} \phi(d) = n$ (por ejemplo, interpretando $\phi(n)$ como el número de los elementos de orden d en el grupo cíclico $\mathbb{Z}/n\mathbb{Z}$). Luego, para $n = p_1^{k_1} \cdots p_s^{k_s}$ la fórmula de inversión de Möbius nos da

$$\begin{aligned}\phi(n) = \sum_{d|n} \mu(d)\, \frac{n}{d} &= n - \sum_{1\le i\le s} \frac{n}{p_i} + \sum_{1\le i<j\le s} \frac{n}{p_i p_j} - \cdots \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right).\end{aligned}$$

▲

Apéndice E
Teorema fundamental del álgebra

El propósito de este apéndice es demostrar el **teorema fundamental del álgebra**.

E.0.1. Teorema. *Sea $f \in \mathbb{C}[X]$ un polinomio no constante. Entonces, existe $z \in \mathbb{C}$ tal que $f(z) = 0$.*

Este resultado aparece en el tratado de d'Alembert[*] "Recherches sur le calcul intégral" (1748) y fue probado de manera rigurosa en la tesis de doctorado de Gauss, publicada en 1799. El nombre "teorema fundamental del álgebra" parece un poco ridículo en un curso del álgebra moderna, pero es histórico y bastante común. Sin duda, es uno de los resultados más importantes en las matemáticas.

Aunque el estudio de raíces de polinomios pertenece al terreno del álgebra, la misma construcción de los números complejos es analítica y por ende cualquier prueba del teorema fundamental del álgebra debe usar análisis. Para una prueba estándar puramente analítica, refiero a [Vin2003, §3.3][**]. El argumento de abajo es *topológico*, basado implícitamente en el **grupo fundamental** del círculo. Para más detalles, véase [May1999, Chapter 1].

E.1 Grado de aplicación $\mathbb{S}^1 \to \mathbb{S}^1$

Consideremos el circulo unitario en el plano complejo

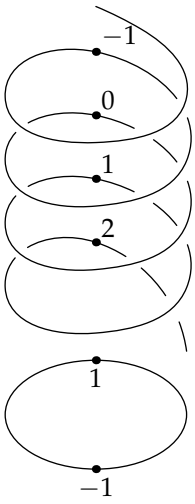
$$\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$$

y la aplicación

$$\exp\colon \mathbb{R} \to \mathbb{S}^1, \quad x \mapsto e^{2\pi i x}.$$

[*] Jean le Rond D'Alembert (1717–1783), matemático, filósofo y enciclopedista francés, conocido por sus contribuciones en análisis, particularmente las ecuaciones diferenciales.

[**] Una buena fuente es [TU1997] donde se encuentran diez diferentes pruebas del teorema. El artículo está en ruso, así que dejo esta referencia más bien para mí mismo.



Esta es una aplicación continua y es un homomorfismo sobreyectivo de grupos $(\mathbb{R}, +)$ y $(\mathbb{S}^1, \times)$. Su núcleo es precisamente $\mathbb{Z} \subset \mathbb{R}$:

$$\exp(x) = e^{2\pi i x} = 1 \iff x \in \mathbb{Z}.$$

Para obtener una aplicación inyectiva, se puede restringir exp al intervalo abierto $\left(-\frac{1}{2}, +\frac{1}{2}\right)$. Como se sabe del análisis complejo, esta restricción tiene una aplicación inversa

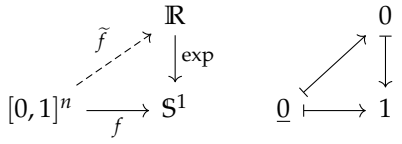
$$\log\colon \mathbb{S}^1 \setminus \{-1\} \to \left(-\frac{1}{2}, +\frac{1}{2}\right)$$

que es también continua.

E.1.1. Lema del levantamiento. *Para toda aplicación continua $f\colon [0,1]^n \to \mathbb{S}^1$ con $f(\underline{0}) = 1$ existe una aplicación continua $\widetilde{f}\colon [0,1]^n \to \mathbb{R}$ que satisface*

$$\exp(\widetilde{f}(\underline{x})) = f(\underline{x}), \quad \widetilde{f}(\underline{0}) = 0.$$

Además, estas condiciones definen a $\widetilde{f}$ de modo único.



Demostración. Primero, probemos la unicidad de $\widetilde{f}$. Supongamos que hay dos aplicaciones continuas $\widetilde{f}_1$ y $\widetilde{f}_2$ que cumplen

$$\exp(\widetilde{f}_1(\underline{x})) = \exp(\widetilde{f}_2(\underline{x})) = f(\underline{x}), \quad \widetilde{f}_1(\underline{0}) = \widetilde{f}_2(\underline{0}) = 0.$$

La primera ecuación implica que

$$\widetilde{f}_1(\underline{x}) - \widetilde{f}_2(\underline{x}) \in \mathbb{Z}.$$

Entonces, la aplicación $\widetilde{f}_1(\underline{x}) - \widetilde{f}_2(\underline{x})$ es continua sobre el conjunto conexo $[0,1]^n$ y toma valores enteros, pero esto significa que es constante. Luego, para cualquier $\underline{x} \in [0,1]^n$

$$\widetilde{f}_1(\underline{x}) - \widetilde{f}_2(\underline{x}) = \widetilde{f}_1(\underline{0}) - \widetilde{f}_2(\underline{0}) = 0.$$

Ahora tenemos que establecer la existencia de $\widetilde{f}$. La aplicación $f\colon [0,1]^n \to \mathbb{S}^1$ es continua y el cubo $[0,1]^n$ es compacto, entonces f es uniformemente continua. Gracias a esto, existe $\delta > 0$ tal que

$$\|\underline{x} - \underline{y}\| < \delta \Longrightarrow |f(\underline{x}) - f(\underline{y})| < 2 \Longrightarrow f(\underline{x}) \neq -f(\underline{y}).$$

Fijemos un número natural N tal que $\frac{1}{N}\|\underline{x}\| < \delta$ para todo $x \in [0,1]^n$ (esto es posible gracias a la compacidad de $[0,1]^n$). Pongamos

$$\widetilde{f}(\underline{x}) := \sum_{0 \leq k \leq N-1} \log\left(\frac{f\left(\frac{k+1}{N}\,\underline{x}\right)}{f\left(\frac{k}{N}\,\underline{x}\right)}\right).$$

Por nuestra elección de N, tenemos

$$\frac{f\left(\frac{k+1}{N}\,\underline{x}\right)}{f\left(\frac{k}{N}\,\underline{x}\right)} \neq -1$$

para ningún $\underline{x} \in [0,1]^n$, así que $\widetilde{f}$ es una aplicación continua bien definida. Luego,

$$\exp(\widetilde{f}(\underline{x})) = \frac{f\left(\frac{1}{N}\,\underline{x}\right)}{f(\underline{0})}\,\frac{f\left(\frac{2}{N}\,\underline{x}\right)}{f\left(\frac{1}{N}\,\underline{x}\right)} \cdots \frac{f\left(\frac{N-1}{N}\,\underline{x}\right)}{f\left(\frac{N-2}{n}\,\underline{x}\right)}\,\frac{f(\underline{x})}{f\left(\frac{N-1}{N}\,\underline{x}\right)} = f(\underline{x}),$$

y claramente,

$$\widetilde{f}(\underline{0}) = \log(f(\underline{0})) = \log(1) = 0.$$

■

E.1.2. Definición. Un **lazo** en $\mathbb{S}^1$ es una aplicacion continua $\gamma\colon \mathbb{S}^1 \to \mathbb{S}^1$ que satisface $\gamma(1) = 1$.

Una **homotopía** entre dos lazos γ_0 y γ_1 es una aplicación continua

$$h\colon [0,1] \times \mathbb{S}^1 \to \mathbb{S}^1$$

tal que

$$h(0,z) = \gamma_0(z), \quad h(1,z) = \gamma_1(z), \quad h(t,1) = 1$$

para cualesquiera $t \in [0,1]$, $z \in \mathbb{S}^1$.

En otras palabras, una homotopía define una familia de lazos $\gamma_t\colon z \mapsto h(t,z)$ que dependen de manera continua del parámetro $t \in [0,1]$.

E.1.3. Definición. Dado un lazo $\gamma\colon \mathbb{S}^1 \to \mathbb{S}^1$, consideremos la aplicación

$$\begin{aligned} f\colon [0,1] &\to \mathbb{S}^1, \\ x &\mapsto \gamma(\exp(x)). \end{aligned}$$

Ahora según E.1.1, existe una aplicación continua única $f\colon [0,1] \to \mathbb{R}$ que satisface

$$\exp(\widetilde{f}(x)) = f(x), \quad \widetilde{f}(0) = 0.$$

En particular,

$$\exp(\widetilde{f}(1)) = f(1) = \gamma(1) = 1,$$

así que $\widetilde{f}(1) \in \mathbb{Z}$. El número $\widetilde{f}(1)$ se llama el **grado** del lazo γ y se denota por $\deg \gamma$.

Intuitivamente, $\deg \gamma$ nos dice cuántas vueltas en el sentido antihorario da γ alrededor del circulo $\mathbb{S}^1$.

E.1.4. Ejemplo. El lazo constante

$$\gamma\colon \mathbb{S}^1 \to \mathbb{S}^1, \quad z \mapsto 1$$

tiene grado nulo: en efecto, a este lazo corresponde la aplicación constante

$$f\colon [0,1] \to \mathbb{S}^1, \quad x \mapsto 1,$$

que se levanta a la aplicación constante

$$\widetilde{f}\colon [0,1] \to \mathbb{R}, \quad x \mapsto 0.$$

▲

E.1.5. Ejemplo. Consideremos el lazo

$$\gamma\colon \mathbb{S}^1 \to \mathbb{S}^1, \quad z \mapsto z^n.$$

A este corresponde la aplicación

$$f\colon [0,1] \to \mathbb{S}^1, \quad x \mapsto e^{2\pi i n x}$$

que se levanta a la aplicación

$$\widetilde{f}(x) = nx.$$

En efecto, tenemos

$$\exp(\widetilde{f}(x)) = e^{2\pi i n x} = f(x), \quad \widetilde{f}(0) = 0.$$

Podemos concluir que

$$\deg \gamma = \widetilde{f}(1) = n.$$

▲

Es fácil convencerse intuitivamente que al deformar un lazo de manera continua, el número de vueltas que este da alrededor del círculo $\mathbb{S}^1$ no cambia. Esto se refleja en el siguiente resultado.

E.1.6. Lema. *Si entre dos lazos γ_0 y $\gamma_1 \colon \mathbb{S}^1 \to \mathbb{S}^1$ existe una homotopía, entonces*

$$\deg \gamma_0 = \deg \gamma_1.$$

Demostración. Consideremos una homotopía

$$h \colon [0,1] \times \mathbb{S}^1 \to \mathbb{S}^1$$

tal que

$$h(0,z) = \gamma_0(z), \quad h(1,z) = \gamma_1(z).$$

Definamos una aplicación

$$\begin{aligned} f \colon [0,1] \times [0,1] &\to \mathbb{S}^1, \\ (t,x) &\mapsto h(t, \exp(x)). \end{aligned}$$

De nuevo, podemos invocar el lema del levantamiento E.1.1 para concluir que existe una aplicación continua

$$\widetilde{f} \colon [0,1] \times [0,1] \to \mathbb{R}$$

que satisface

$$\exp(\widetilde{f}(t,x)) = f(t,x), \quad \widetilde{f}(0,0) = 0.$$

En particular, se tiene

$$\exp(\widetilde{f}(t,0)) = h(t,1) = 1,$$

lo que implica que $\widetilde{f}(t,0) \in \mathbb{Z}$. La aplicación $t \mapsto \widetilde{f}(t,0)$ es continua, definida sobre el intervalo conexo $[0,1]$, y dado que sus valores son enteros, esta debe ser constante. Tenemos $\widetilde{f}(0,0) = 0$, de donde podemos concluir que

$$\widetilde{f}(t,0) = 0 \text{ para todo } t \in [0,1].$$

Además,

$$\exp(\widetilde{f}(0,x)) = \gamma_0(\exp(x)), \quad \exp(\widetilde{f}(1,x)) = \gamma_1(\exp(x)).$$

Esto significa que $\widetilde{f}(0,x)$ y $\widetilde{f}(0,y)$ son levantamientos de los lazos γ_0 y γ_1 respectivamente, y luego

$$\deg \gamma_0 = \widetilde{f}(0,1), \quad \deg \gamma_1 = \widetilde{f}(1,1).$$

Notamos que

$$\exp(\widetilde{f}(t,1)) = h(t, \exp(1)) = h(t,1) = 1,$$

así que $\widetilde{f}(t,1) \in \mathbb{Z}$. De nuevo, se tiene una aplicación continua $t \mapsto \widetilde{f}(t,1)$ definida sobre el intervalo conexo $[0,1]$ que toma valores enteros, entonces es constante. En particular,

$$\deg \gamma_0 = \widetilde{f}(0,1) = \widetilde{f}(1,1) = \deg \gamma_1.$$

■

E.1.7. Comentario. De hecho, se puede probar que si $\deg \gamma_0 = \deg \gamma_1$, entonces entre los lazos γ_0 y γ_1 hay una homotopía. Sin embargo, no lo vamos a necesitar en la prueba de abajo.

E.1.8. Comentario. Para una curva $\gamma\colon \mathbb{S}^1 \to \mathbb{C} \setminus \{0\}$ se puede definir el grado (también conocido como el **índice** o **número de rotación**) mediante la integral

$$\deg \gamma = \frac{1}{2\pi i} \oint_\gamma \frac{dz}{z}.$$

Con esta definición, para deducir que $\deg \gamma \in \mathbb{Z}$ y $\deg \gamma$ es invariante respecto a homotopía, se usa la **fórmula integral de Cauchy**. Véase por ejemplo [Lan1999, Chapter III] para los detalles.

E.2 Prueba del teorema

Consideremos un polinomio complejo

$$f = z^n + a_{n-1}\, z^{n-1} + a_{n-2}\, z^{n-2} + \cdots + a_1\, z + a_0.$$

Asumamos que f no tiene raíces: $f(z) \neq 0$ para ningún $z \in \mathbb{C}$. Definamos un lazo

$$\begin{aligned} \gamma\colon \mathbb{S}^1 &\to \mathbb{S}^1, \\ z &\mapsto \frac{f(z)}{|f(z)|}\, \frac{|f(1)|}{f(1)}. \end{aligned}$$

Para $t \in [0,1]$ pongamos

$$h_1(t,z) := \begin{cases} \dfrac{f(z/t)\, t^n}{|f(z/t)\, t^n|}\, \dfrac{|f(1/t)\, t^n|}{f(1/t)\, t^n}, & t \neq 0, \\ z^n, & t = 0. \end{cases}$$

Notamos que

$$\lim_{t \to 0} h_1(t,z) = z^n$$

y

$$h_1(1,z) = \gamma(z),$$

así que $h_1\colon [0,1] \to \mathbb{S}^1$ es una aplicación continua que define una homotopía entre el lazo $z \mapsto z^n$ y γ. Entonces,

$$\deg \gamma = \deg(z \mapsto z^n) = n.$$

Por otro lado, podemos definir

$$h_2(t,z) := \frac{f(tz)}{|f(tz)|}\, \frac{|f(t)|}{f(t)}.$$

Tenemos

$$h_2(0,z) = \gamma(0) = 1, \quad h_2(1,z) = \gamma(z),$$

así que h_2 define una homotopía entre el lazo constante $z \mapsto 1$ y γ, así que

$$\deg \gamma = 0.$$

Entonces, si $n > 0$, tendríamos una contradicción. Podemos concluir que todo polinomio complejo no constante debe tener una raíz. ■

Bibliografía

[AM1969] Michael Francis Atiyah and I. G. MacDonald, *Introduction to commutative algebra.*, Addison-Wesley-Longman, 1969.

[AW2004] Şaban Alaca and Kenneth S. Williams, *Introductory algebraic number theory*, Cambridge University Press, Cambridge, 2004.

[Bak1990] Alan Baker, *Transcendental number theory*, second ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990. MR1074572

[DF2004] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236

[Eis2004] David Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 2004. http://dx.doi.org/10.1007/978-1-4612-5350-1

[Ful2008] William Fulton, *Algebraic curves. An introduction to algebraic geometry*, 2008. http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[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

[Kob1984] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR754003 http://dx.doi.org/10.1007/978-1-4612-1112-9

[Kob1993] ———, *Introduction to elliptic curves and modular forms*, second ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR1216136 https://doi.org/10.1007/978-1-4612-0909-6

[Lam2001] Tsit-Yuen Lam, *A first course in noncommutative rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag New York, 2001. http://dx.doi.org/10.1007/978-1-4419-8616-0

[Lan1999] Serge Lang, *Complex analysis*, 4 ed., Graduate Texts in Mathematics, vol. 103, Springer-Verlag, New York, 1999.
http://dx.doi.org/10.1007/978-1-4757-3083-8

[Lan2002] ———, *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

[Lem2000] Franz Lemmermeyer, *Reciprocity laws: From Euler to Eisenstein*, Springer-Verlag Berlin Heidelberg, 2000.
http://dx.doi.org/10.1007/978-3-662-12893-0

[Mar1977] Daniel A. Marcus, *Number fields*, Universitext, Springer-Verlag, New York, 1977.
https://doi.org/10.1007/978-1-4684-9356-6

[May1999] J.P. May, *A concise course in algebraic topology*, Chicago Lectures in Mathematics, University of Chicago Press, 1999.
https://www.math.uchicago.edu/~may/CONCISE/ConciseRevised.pdf

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

[Rei1995] Miles Reid, *Undergraduate commutative algebra*, London Mathematical Society Student Texts, Cambridge University Press, 1995.
http://dx.doi.org/10.1017/CBO9781139172721

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

[Sha2001] Rodney Y. Sharp, *Steps in commutative algebra*, 2 ed., London Mathematical Society Student Texts, Cambridge University Press, 2001.
http://dx.doi.org/10.1017/CBO9780511623684

[Sil2009] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094
https://doi.org/10.1007/978-0-387-09494-6

[TU1997] V. M. Tikhomirov and V. V. Uspenskii, Десять доказательств основной теоремы алгебры, Mat. Pros., Ser. 3 **1** (1997), 50–70.
http://mi.mathnet.ru/eng/mp4

[vdW1991] Bartel Leendert van der Waerden, *Algebra*, vol. I, Springer-Verlag, New York, 1991.

[Vin2003] E. B. Vinberg, *A course in algebra*, Graduate Studies in Mathematics, vol. 56, American Mathematical Society, Providence, RI, 2003, Translated from the 2001 Russian original by Alexander Retakh. MR1974508
https://doi.org/10.1090/gsm/056

Índice de símbolos

Índice alfabético de términos