MA–561: GRUPOS y ANILLOS

Joseph C. Várilly

Escuela de Matemática, Universidad de Costa Rica

I Ciclo Lectivo del 2014

Introducción

El creciente predominio del enfoque abstracto en las matemáticas ha resaltado el papel del álgebra y de los métodos algebraicos. La palabra *álgebra*, originalmente concebido como el estudio y la resolución de las ecuaciones polinomiales, hoy en día significa más bien el manejo detallado de ciertas *estructuras*: grupos, anillos, cuerpos, retículos, etc. Este curso es una introducción a la teoría de grupos y de anillos, con énfasis en los ejemplos más concretos: grupos finitos y matriciales; anillos de matrices y polinomios; y las representaciones de grupos sobre espacios vectoriales de dimensión finita.

Los estudiantes que emprenden este curso tendrán conocimiento de los rudimentos del álgebra lineal: la teoría de espacios vectoriales y el manejo de cálculos matriciales. De hecho, buena parte de los grupos y anillos de uso cotidiano en la matemáticas están formados por matrices. Además, aunque se suele presentar un grupo o anillo de manera abstracta, se obtiene mucha información al identificarlo con un juego concreto de matrices (dícese que *se representa* el grupo o anillo en forma matricial).

Por otro lado, la teoría de cuerpos y sus extensiones, que juega un papel predominante en la resolución de ecuaciones, queda para un curso subsiguiente. Un aspecto clave de la teoría de cuerpos, la llamada correspondencia de Galois, le asocia a cada extensión de cuerpos un grupo de automorfismos (el "grupo de Galois" de la extensión). Por lo tanto, la materia de este curso es una preparación indispensable para abordar dicha teoría.

Un aspecto característico del álgebra, tan prominente que a veces se identifica con toda la disciplina, es la repetición de ciertos rasgos estructurales: una colección de "objetos" conectados por juegos de "morfismos" que obedecen una ley de composición asociativa. Estas estructuras suelen llamarse *categorías*. Hoy en día, gran parte del álgebra, para no decir de todas las matemáticas, se expresan en el lenguaje de las categorías. Este curso también servirá como una introducción a este lenguaje.

Temario

Grupos Ejemplos de grupos y monoides. Subgrupos, coclases, el teorema de Lagrange; subgrupos normales, grupos cocientes. Homomorfismos de grupos, los teoremas de isomorfismo. Acciones de grupos sobre conjuntos, órbitas, grupos de isotropía, el teorema de Cayley. Productos directos y semidirectos de grupos. Grupos resolubles y nilpotentes. La estructura de grupos finitos, los teoremas de Sylow.

Grupoides y categorías Ejemplos de grupoides. Categorías pequeñas como generalización del concepto de grupoide, morfismos y funtores. La categoría de grupos finitos.

Anillos Ejemplos: anillos de polinomios y matrices. Algebras sobre un cuerpo. Anillos enteros, cuerpos de cocientes. Ideales, homomorfismos de anillos, los teoremas de isomorfismo. Módulos sobre un anillo, categorías de módulos, la estructura de grupos abelianos finitos. El algoritmo euclidiano de división, anillos factoriales, factorización única de polinomios en factores irreducibles.

Representaciones de grupos finitos Anillos de grupos, G-módulos irreducibles, el lema de Schur. Caracteres de un grupo, funciones de clase, relaciones de ortogonalidad, el anillo de caracteres. Ejemplos de representaciones. Representaciones inducidas, la fórmula de reciprocidad de Frobenius.

Bibliografía

El curso seguirá mayormente los lineamientos del libro *Basic Algebra I* de Nathan Jacobson. Otros libros de mucha utilidad son los siguientes.

[1] Paolo Aluffi, *Algebra: Chapter 0*, American Mathl. Society, Providence, RI, 2009.

[2] Morton L. Curtis, *Matrix Groups*, Springer, New York, 1984.

[3] John Dauns, *Modules and Rings*, Cambridge University Press, Cambridge, 1994.

[4] William Fulton and Joseph Harris, *Representation Theory: A First Course*, Springer, New York, 2004.

[5] Isadore N. Herstein, *Topics in Algebra*, Blaisdell, New York, 1964.

[6] Nathan Jacobson, *Basic Algebra I*, 2ª edición, W. H. Freeman, New York, 1985.

[7] Nathan Jacobson, *Basic Algebra II*, 2ª edición, W. H. Freeman, New York, 1989.

[8] Mijail I. Kargapolov y Urii I. Merzliakov, *Fundamentals of the Theory of Groups*, Springer, Berlin, 1979.

[9] Aleksandr G. Kurosh, *The Theory of Groups*, 2ª edición, Chelsea, New York, 1960.

[10] Serge Lang, *Algebra*, 3ª edición, Springer, New York, 2002.

[11] Walter Ledermann, *Introduction to the Theory of Finite Groups*, Oliver & Boyd, Edinburgh, 1953.

[12] Saunders MacLane y Garrett Birkhoff, *Algebra*, Macmillan, New York, 1967.

[13] Joseph J. Rotman, *The Theory of Groups: an Introduction*, Allyn & Bacon, Boston, 1978.

[14] Jean-Pierre Serre, *Linear Representations of Finite Groups*, Springer, New York, 1977.

[15] Barry Simon, *Representations of Finite and Compact Groups*, American Mathl. Society, Providence, RI, 1996.

[16] Bartel L. van der Waerden, *Modern Algebra 1*, Frederick Ungar, New York, 1953.

Notaciones y convenios

Las notaciones usados en este curso serán mayormente compatibles con las del libro de Jacobson, *Basic Algebra I* y las del libro de Aluffi, *Algebra: Chapter 0*. En particular, los conjuntos usuales de números serán denotados por

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ es el conjunto de los *números naturales*, es decir, los números enteros no negativos.
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ es el conjunto de los *números enteros*.
- $\mathbb{Q}$ es el conjunto de los *números racionales*.
- $\mathbb{R}$ es el conjunto de los *números reales*.
- $\mathbb{C}$ es el conjunto de los *números complejos*.

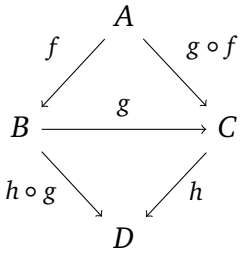
Fíjese que aquí se usa el convenio de contar 0 como número natural. Los *números enteros positivos* se denotarán por $\mathbb{P} = \{1, 2, 3, \dots\} = \mathbb{N} \setminus \{0\}$, como hace Jacobson.[1]

[1] Los autores franceses usan $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ y escriben $\mathbb{N}^* = \{1, 2, 3, \dots\}$. En cambio, los autores alemanes suelen poner $\mathbb{N} = \{1, 2, 3, \dots\}$ y $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$. Por lo general, el lector debe cerciorarse si un determinado libro considera 0 como número natural o no.

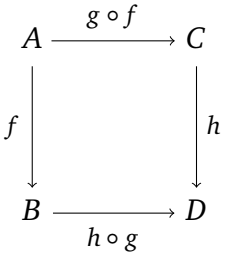
► Se usarán las notaciones usuales $A \cup B$, $A \cap B$, $A \backslash B$ para la unión, intersección o diferencia de conjuntos A y B. En el caso de que $A \cap B = \emptyset$, es decir, si los conjuntos A y B no tienen elementos en común, se escribirá $A \uplus B$ para denotar la *unión disjunta* de A y B.

Si $f : A \to B$ y $g : B \to C$ son dos funciones tales que el dominio B de g coincide con el codominio de f, la *composición* de estas dos funciones se denotará por $g \circ f$; en otras palabras, $g \circ f(x) := g(f(x))$ para $x \in A$. En algunas ocasiones, se omitirá el símbolo circular, dejando $gf(x) := g(f(x))$.

La composición de funciones es *asociativa*, es decir, el orden de formación de la composición de tres funciones es inmaterial: $h \circ (g \circ f) = (h \circ g) \circ f : x \mapsto h(g(f(x)))$. Esta regla puede ser ilustrada de la siguiente manera:



La asociatividad $h \circ (g \circ f) = (h \circ g) \circ f$ dice que en este diagrama, todas las maneras de seguir las flechas desde A hasta D producen el mismo resultado. En tal caso, dícese que el diagrama *conmuta*. Si se omite la flecha g, la asociatividad toma la forma de un *diagrama conmutativo*:



Por otro lado, la composición de funciones *no es conmutativo*: $f \circ g \neq g \circ f$ en general.

► La notación algebraica emplea muchas relaciones de orden: inclusión de conjuntos $A \subseteq B$, inclusión de subespacios vectoriales $V \leqslant W$, inclusión de un subgrupo normal $H \trianglelefteq K$ (este último concepto se verá oportunamente). En cada caso, la omisión de la barra inferior significa una *inclusión sin igualdad*: $A \subset B$ cuando $A \subseteq B$ pero $A \neq B$; $V < W$ cuando $V \leqslant W$ pero $V \neq W$; $H \lhd K$ cuando $H \trianglelefteq K$ pero $H \neq K$.

1 Grupos

Antes de abordar el tema de los grupos, vale la pena recordar una estructura algebraica bien conocido: la de un **cuerpo**,[2] es decir, un sistema de "escalares" que aparecen como coeficientes de las combinaciones lineales de vectores en un espacio vectorial. Los ejemplos mejor conocidos de cuerpos son los números racionales $\mathbb{Q}$ y los números reales $\mathbb{R}$. (Los números complejos $\mathbb{C}$ también forman un cuerpo.) Un cuerpo es entonces un conjunto $\mathbb{F}$ con dos operaciones binarias: la *suma* y el *producto*. Conviene hacer una lista de sus propiedades algebraicas, para fijar algunos términos de vocabulario.

- ◇ *Ley asociativa* de sumas: $(a+b)+c = a+(b+c)$.
- ◇ *Ley conmutativa* de sumas: $a+b = b+a$.
- ◇ *Ley de cancelación* de sumas: $a+c = b+c \implies a = b$.
- ◇ *Ley asociativa* de productos: $(ab)c = a(bc)$.
- ◇ *Ley conmutativa* de productos: $ab = ba$.
- ◇ *Ley de cancelación* de productos: $ac = bc \implies a = b$ si $c \neq 0$.
- ◇ *Ley distributiva* de productos sobre sumas: $a(b+c) = ac+bc$.
- ◇ *Existencia de un cero*: hay un (único) elemento $0 \in \mathbb{F}$ tal que $0+a = a$ para todo $a \in \mathbb{F}$.
- ◇ *Existencia de negativos*: si $a \in \mathbb{F}$, hay un (único) elemento $-a \in \mathbb{F}$ tal que $a+(-a) = 0$.
- ◇ *Existencia de un "uno"*: hay un (único) elemento $1 \in \mathbb{F}$ tal que $1a = a$ para todo $a \in \mathbb{F}$.
- ◇ *Existencia de recíprocos*: si $a \in \mathbb{F}$, $a \neq 0$, hay un (único) elemento $a^{-1} \in \mathbb{F}$ tal que $aa^{-1} = 1$.

Dejando de lado la ley distributiva, que relaciona las dos operaciones, se puede observar una analogía interesante entre el conjunto $\mathbb{F}$ con la operación de suma; y el conjunto $\mathbb{F} \setminus \{0\}$ con la operación de producto. Estos son dos ejemplos de *grupos abelianos*.

[2] El término **cuerpo** viene del alemán *Körper*, un término introducido por Richard Dedekind en 1871; se llama *corps* en francés, *corp* en rumano, etc., pero en inglés se usa la palabra *field*. En español, no debe usarse la traducción secundaria *campo*, que denota campos vectoriales, campos magnéticos, etc.

1.1 Definición y ejemplos de grupos

Una *operación binaria* sobre un conjunto A es simplemente una función $m\colon A\times A\to A$. En lugar de denotar un elemento de su imagen como $m(a,b)\in A$, se puede escribir en forma abreviada $ab := m(a,b)$.

Definición 1.1. Un **grupo** es un conjunto G con un **producto** $G\times G\to G\colon (g,h)\mapsto gh$ tal que:

(a) el producto es *asociativo*: $(gh)k = g(hk)$ para todo $g,h,k\in G$;

(b) hay un *elemento neutro* $1\in G$ tal que $1g = g1 = g$, para todo $g\in G$;

(c) para todo $g\in G$, hay un *elemento inverso* $g^{-1}\in G$ tal que $gg^{-1} = g^{-1}g = 1$.

Dícese que G es un **grupo abeliano** si además:

(d) el producto es *conmutativo*: $gh = hg$ para todo $g,h\in G$. ◊

A veces conviene denotar la operación binaria con un símbolo explícito, al escribir $m(g,h) = g*h$, por ejemplo. En tal caso, las fórmulas que definen las propiedades de grupo se escriben así:

(a) $(g*h)*k = g*(h*k)$; (b) $1*g = g*1 = g$; (c) $g*g^{-1} = g^{-1}*g = 1$;

y también (d) $g*h = h*g$, si el grupo es abeliano. De hecho, cuando el grupo es abeliano, se suele emplear una *notación aditiva*: $m(g,h) =: g+h$. En tal caso, el elemento neutro aditivo se denota por 0 (el *cero* del grupo abeliano) y el inverso aditivo de g se denota por $-g$.

Es útil, para poder apreciar que estas reglas no siempre se cumplen, escribir estas condiciones en términos de la función m.

(a) asociatividad: $m(m(g,h),k) = m(g,m(h,k))$ para todo $g,h,k\in G$;

(b) elemento neutro: $m(1,g) = m(g,1) = g$ para todo $g\in G$;

(c) invertibilidad: $m(g,g^{-1}) = m(g^{-1},g) = 1$ para todo $g\in G$;

(d) conmutatividad: $m(g,h) = m(h,g)$ para todo $g,h\in G$.

Proposición 1.2. *En un grupo G:*

(a) el elemento neutro es único;

(b) el inverso de cualquier elemento es único;

(c) $(g^{-1})^{-1} = g$*, para todo* $g \in G$*;*

(d) $(gh)^{-1} = h^{-1}g^{-1}$*, para todo* $g, h \in G$*;*

(e) $gh = gk \implies h = k$ *y también* $hg = kg \implies h = k$.

Demostración. Ad(a): Si e, f son elementos de G tales que $eg = g$ y $gf = g$ para todo $g \in G$, entonces $f = ef = e$. (En palabras: una identidad a la izquierda y una identidad a la derecha son necesariamente iguales.) En particular, si e y f son identidades (bilaterales) en G, entonces $f = e$. ⟦ En adelante, este elemento neutro se denotará por 1. ⟧

Ad(b): Si $h, k \in G$ son tales que $hg = 1$ y $gk = 1$, entonces

$$h = h1 = h(gk) = (hg)k = 1k = k.$$

(En palabras: un inverso a la izquierda y un inverso a la derecha para el elemento g son necesariamente iguales.) En particular, si h y k son inversos (bilaterales) para g, entonces $h = k$. ⟦ En adelante, el elemento inverso de g se denotará por g^{-1}. ⟧

Ad(c): Las igualdades $g^{-1}g = gg^{-1} = e$ muestran que g es un inverso para g^{-1}. Por la parte (b), este inverso es único.

Ad(d): La asociatividad del producto implica que

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

De hecho, la asociatividad del producto muestra que las paréntesis en este cálculo son redundantes: se podría escribir $ghh^{-1}g^{-1} = g1g^{-1} = gg^{-1} = 1$. De igual manera, se ve que $h^{-1}g^{-1}gh = h^{-1}1h = h^{-1}h = 1$. En fin, $h^{-1}g^{-1}$ es el inverso del elemento gh.

Ad(e): Estas *leyes de cancelación* siguen de la multiplicación, a la izquierda o a la derecha respectivamente, por el elemento g^{-1}, tomando en cuenta la asociatividad:

$$\begin{aligned} gh = gk &\implies g^{-1}gh = g^{-1}gk \implies h = k, \\ hg = kg &\implies hgg^{-1} = kgg^{-1} \implies h = k. \end{aligned}$$

□

La notación 1 para el elemento neutro no es universal: muchos autores lo denotan por e. (En contextos específicos, tiene otros nombres: en un grupo de matrices se suele denotar la matriz identidad por I; en un grupo de funciones se escribe $\underline{\mathrm{id}}$ para la función idéntica $x \mapsto x$; etc.) En estos apuntes, se seguirá el siguiente convenio en lo posible (con algunas excepciones): *cualquier cero* (elemento neutro aditivo) *se denotará por* 0 y

cualquier identidad (elemento neutro multiplicativo) *se denotará por* 1. Así, por ejemplo, la matriz unidad $n \times n$ se escribe 1_n en vez de I_n; la aplicación idéntica del conjunto A en sí mismo se denota por 1_A en vez de id_A; etcétera.

Definición 1.3. Una estructura más general que un grupo es un **monoide**: este es un conjunto M con una operación binaria asociativa y un elemento neutro 1, en donde no es necesaria que todo elemento posee un inverso. En otras palabras:

(a) el producto es *asociativo*: $(x * y) * z = x * (y * z)$ para todo $x, y, z \in M$;

(b) hay un *elemento neutro* $1 \in M$ tal que $1 * x = x * 1 = x$, para todo $x \in M$.

Todo grupo, desde luego, es un monoide. De hecho, un grupo es un monoide en donde cada elemento es invertible. ◊

En un monoide, el elemento neutro es único, porque la parte (a) de la Proposición 1.2 es aplicable al caso. Debido a la posible ausencia de elementos inversos, las leyes de cancelación de la parte (e) no estarán garantizadas en monoides: algunos monoides las cumplen pero otros no.

Ejemplo 1.4. Un conjunto con un sólo elemento, $G = \{1\}$, admite una única operación binaria, dada por $1 * 1 = 1$. Es evidente que esta operación cumple trivialmente las condiciones (a), (b) y (c) de la Definición 1.1. De este modo se define el **grupo trivial** de un elemento; se suele escribir $\mathbf{1} := \{1\}$. ◊

Ejemplo 1.5. El conjunto de *números enteros* $\mathbb{Z}$, con la suma usual, es un grupo abeliano $(\mathbb{Z}, +)$. Su elemento neutro es 0 y el inverso aditivo de n es $(-n)$ en cada caso.

Los *números naturales* forman un monoide $(\mathbb{N}, +)$, el cual no es un grupo. Este es un monoide que *admite cancelación*: si $m + k = n + k$ en $\mathbb{N}$, entonces $m = n$.

Los *números enteros positivos* $(\mathbb{P}, +)$ están cerrados bajo la operación (asociativa) de suma, pero carecen del elemento neutro: dícese que $(\mathbb{P}, +)$ es un *semigrupo*.[3] ◊

Ejemplo 1.6. Otros ejemplos de grupos abelianos, con la operación de suma usual, son $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$: los números racionales, reales y complejos. ◊

Ejemplo 1.7. Si $\mathbb{F}$ es un cuerpo cualquiera, escríbase $\mathbb{F}^\times := \mathbb{F} \setminus \{0\}$ para denotar la totalidad de sus elementos no nulos. Entonces $\mathbb{F}^\times$ es un grupo con la operación de multiplicación. En particular, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$ y $(\mathbb{C}^\times, \cdot)$ son grupos multiplicativos, con elemento neutro 1. En estos casos, el inverso multiplicativo de x es $x^{-1} := 1/x$.

[3] En esta terminología, un monoide es un semigrupo que posee un elemento neutro. Sin embargo, hay que advertir que tal nomenclatura no es universal: muchos autores, particularmente en libros de análisis, dicen "semigrupo" como sinónimo de "monoide", es decir, asumen que posee un elemento neutro.

Los números enteros positivos $(\mathbb{P}, \cdot)$ forman un monoide bajo multiplicación. Los enteros no nulos $(\mathbb{Z}^\times, \cdot)$ también forman un monoide. ◊

Ejemplo 1.8. Tómese $m \in \mathbb{P}$ con $m > 1$. Entonces cada número entero $n \in \mathbb{Z}$ puede escribirse de manera única como $n = qm + r$ donde $q \in \mathbb{Z}$ y $r \in \{0, 1, 2, \ldots, m-1\}$. Este r es el *residuo* de n bajo división por m. Si $n' = q'm + s$, entonces

$$n + n' = \begin{cases} (q + q')m + (r + s) & \text{si } r + s < m, \\ (q + q' + 1)m + (r + s - m) & \text{si } r + s \geqslant m. \end{cases}$$

Es evidente que la relación "$n \equiv n'$ mod m si y sólo si $(n - n')$ es un múltiplo entero de m" es una relación de equivalencia sobre $\mathbb{Z}$; las clases de equivalencia corresponden con los posibles residuos bajo división por m. Al denotar por $\overline{r} := \{qm + r : q \in \mathbb{Z}\}$ la clase de equivalencia de r, se obtiene el "conjunto cociente"[4]

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

La *suma* de dos clases de residuos está bien definida por la receta $\overline{r} + \overline{s} := \overline{r+s}$, porque $(r+s) \equiv (r+s-m)$ mod m. Fíjese que esta "suma de residuos" es asociativa, con elemento neutro $\overline{0}$. Es también evidente que $\overline{r} + \overline{m-r} = \overline{0}$, así que $(\mathbb{Z}_m, +)$ es un grupo abeliano finito, con m elementos. ◊

Ejemplo 1.9. Obsérvese que la parte no nula $\mathbb{Z}_m \setminus \{0\} = \{\overline{1}, \overline{2}, \ldots, \overline{m-1}\}$ generalmente no queda cerrada bajo el "producto de residuos" definido por $\overline{r} \cdot \overline{s} := \overline{rs}$. Por ejemplo, si $m = 6$, entonces $\overline{2} \cdot \overline{3} = \overline{0}$ en $\mathbb{Z}_6$. (Este fenómeno de "divisores de cero" se presenta toda vez que m sea un número entero compuesto.)

En cambio, si $m = p$ es un *número primo*, entonces para cada $r \in \{1, 2, \ldots, p-1\}$ es posible encontrar $q \in \mathbb{Z}$ y $s \in \{1, 2, \ldots, p-1\}$ que cumplen $qp + rs = 1$. (Esta es una propiedad conocida del par de números "relativamente primos" p y r.) En consecuencia, $\overline{r} \cdot \overline{s} = \overline{1}$ en $\mathbb{Z}_p \setminus \{0\}$. Escríbase $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ para p primo. Se ha comprobado que $(\mathbb{Z}_p^\times, \cdot)$ es un grupo multiplicativo, con elemento neutro $\overline{1}$.

La ley distributiva $\overline{r} \cdot (\overline{s} + \overline{t}) = \overline{r} \cdot \overline{s} + \overline{r} \cdot \overline{t}$ también es válida en $\mathbb{Z}_p$, porque $r(s+t) = rs + rt$ en $\mathbb{Z}$. Entonces, si p es un número primo, el conjunto finito $\mathbb{Z}_p$ de residuos es un **cuerpo finito** de p elementos. Este cuerpo se denota también por $\mathbb{F}_p$, como sinónimo de $\mathbb{Z}_p$. ◊

[4] El conjunto de residuos módulo m se denota por $\mathbb{Z}_m$ en estos apuntes, como también en los libros de geometría diferencial. Sin embargo, en la teoría de números el nombre $\mathbb{Z}_p$ significa otra cosa (los elementos enteros del cuerpo $\mathbb{Q}_p$ de números p-ádicos) y los libros de álgebra tienden a usar notaciones menos cómodas, como $\mathbb{Z}/m\mathbb{Z}$ [Aluffi] o bien $\mathbb{Z}/\mathbb{Z}m$ [Jacobson I] o inclusive $\mathbb{Z}/(m)$[Jacobson II].

Ejemplo 1.10. Si V es un *espacio vectorial* cualquiera sobre un cuerpo $\mathbb{F}$, se puede hacer caso omiso de la multiplicación por escalares en $\mathbb{F}$; con sólo la operación de suma de vectores, $(V,+)$ es un grupo abeliano. ◊

Ejemplo 1.11. Una *rotación* por un ángulo θ en el plano $\mathbb{R}^2$ es una aplicación $(x,y) \mapsto (\bar{x},\bar{y})$ dado por la fórmula:

$$\bar{x} = x\cos\theta - y\,\mathrm{sen}\,\theta,$$
$$\bar{y} = x\,\mathrm{sen}\,\theta + y\cos\theta.$$

Esta aplicación es lineal en las coordenadas (x,y); entonces queda representada por su matriz de coeficientes

$$\rho_\theta := \begin{pmatrix} \cos\theta & -\mathrm{sen}\,\theta \\ \mathrm{sen}\,\theta & \cos\theta \end{pmatrix}.$$

Es fácil verificar, con un poco de trigonometría, que $\rho_\theta\,\rho_\phi = \rho_{\theta+\phi}$. Se ve que $\rho_0 = 1_2$ es la matriz unidad 2×2 y $\rho_\theta^{-1} = \rho_{-\theta}$. Estas matrices forman un **grupo de rotaciones**, que se denota por SO(2). Sólo hay que recordar que la composición de transformaciones lineales corresponde con el producto de matrices. ◊

Ejemplo 1.12. Considérese la *reflexión* en el plano $\mathbb{R}^2$ dado por

$$\left\{ \begin{array}{l} \bar{x} = x\cos\theta + y\,\mathrm{sen}\,\theta \\ \bar{y} = x\,\mathrm{sen}\,\theta - y\cos\theta \end{array} \right\}, \quad \text{con matriz} \quad \mu_\theta := \begin{pmatrix} \cos\theta & \mathrm{sen}\,\theta \\ \mathrm{sen}\,\theta & -\cos\theta \end{pmatrix}.$$

Obsérvese que

$$\begin{aligned} \mu_\theta\,\mu_\phi &= \begin{pmatrix} \cos\theta & \mathrm{sen}\,\theta \\ \mathrm{sen}\,\theta & -\cos\theta \end{pmatrix}\begin{pmatrix} \cos\phi & \mathrm{sen}\,\phi \\ \mathrm{sen}\,\phi & -\cos\phi \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta\cos\phi + \mathrm{sen}\,\theta\,\mathrm{sen}\,\phi & \cos\theta\,\mathrm{sen}\,\phi - \mathrm{sen}\,\theta\cos\phi \\ \mathrm{sen}\,\theta\cos\phi - \cos\theta\,\mathrm{sen}\,\phi & \mathrm{sen}\,\theta\,\mathrm{sen}\,\phi + \cos\theta\cos\phi \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta-\phi) & -\mathrm{sen}(\theta-\phi) \\ \mathrm{sen}(\theta-\phi) & \cos(\theta-\phi) \end{pmatrix} = \rho_{\theta-\phi}\,. \end{aligned}$$

En particular, $\mu_\theta^2 = \rho_0 = 1_2$; además, esta transformación lineal deja fija la recta que pasa por el origen y por el punto $(\cos\frac{\theta}{2}, \mathrm{sen}\,\frac{\theta}{2})$ —esta recta fija es el *eje* de la reflexión.

Dos cálculos similares muestran que $\mu_\theta\,\rho_\phi = \mu_{\theta-\phi}$ y $\rho_\theta\,\mu_\phi = \mu_{\theta+\phi}$. Por lo tanto, el conjunto de matrices

$$\mathrm{O}(2) = \{\,\rho_\theta : -\pi < \theta \leqslant \pi\,\} \cup \{\,\mu_\theta : -\pi < \theta \leqslant \pi\,\}$$

está cerrado bajo multiplicación. Este es el **grupo ortogonal** de matrices 2×2. El grupo SO(2) del ejemplo anterior es un *subgrupo* de O(2). ◊

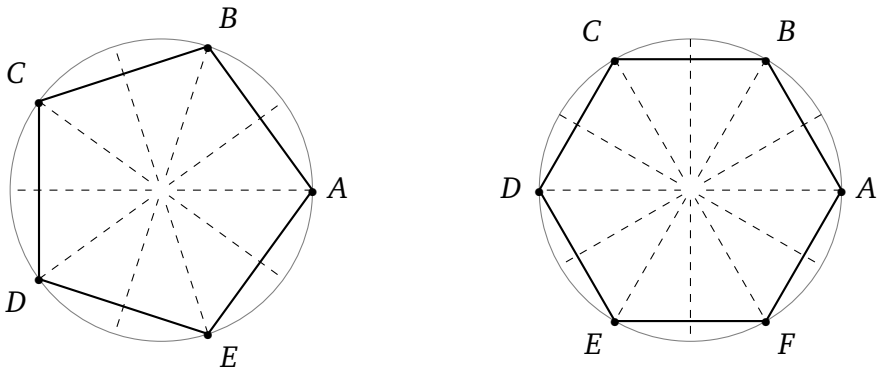


Figura 1.1: Poliedros regulares convexos y sus ejes de simetría

Ejemplo 1.13. Tómese $n \in \mathbb{N}$ con $n \geqslant 3$. Los puntos del plano $\mathbb{R}^2$ cuyos coordenados son $(\cos\theta, \operatorname{sen}\theta)$, para $\theta = 0, 2\pi/n, 4\pi/n, \ldots, 2(n-1)\pi/n$, son los vértices de un polígono regular de n vértices, inscrito en un círculo de radio 1. El conjunto de rotaciones

$$C_n := \left\{ \rho_\theta : \theta = 0, \frac{2\pi}{n}, \frac{4\pi}{n}, \ldots, \frac{2(n-1)\pi}{n} \right\} \tag{1.1a}$$

forma un grupo finito de n elementos, con elemento neutro $1 = \rho_0$, que permuta los vértices del polígono en orden cíclico. Este C_n es el **grupo cíclico** de n elementos.

El polígono regular de n vértices tiene n ejes de simetría (véase la Figura 1.1). Al agregar a las n rotaciones de C_n las n *reflexiones* en estos ejes, se obtiene un grupo de $2n$ elementos:

$$D_n := C_n \uplus \left\{ \mu_\theta : \theta = 0, \frac{2\pi}{n}, \frac{4\pi}{n}, \ldots, \frac{2(n-1)\pi}{n} \right\}. \tag{1.1b}$$

Este D_n es el **grupo diedral** de $2n$ elementos, formado por *todas* las transformaciones ortogonales del plano que permutan los n vértices de un polígono regular. El grupo cíclico C_n aparece como subgrupo del grupo diedral D_n.

Si $n = 2m+1$ es impar, cada reflexión deja fija un vértice y transpone m pares de los otros vértices; pero si $n = 2m$ es par, hay m reflexiones que dejan dos vértices opuestos fijos y las otras m reflexiones no tiene vértice fijo alguno. ◊

Ejemplo 1.14. Estas cuatro matrices 2×2:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad P = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad R = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

forman un grupo abeliano de 4 elementos,[5] denotado por V. El elemento neutro es 1_2 y cada matriz A del grupo satisface $A^2 = 1$.

Este grupo V coincide con el grupo diedral D_2. En efecto, se ve que $1 = \rho_0$, $P = \rho_\pi$, $Q = \mu_0$, $R = \mu_\pi$ en las notaciones de los Ejemplos anteriores. ◊

Ejemplo 1.15. El conjunto de todas las *matrices $n \times n$ invertibles* con entradas en un cuerpo $\mathbb{F}$ forman un grupo, llamado $\mathrm{GL}(n, \mathbb{F})$, un **grupo general lineal** sobre $\mathbb{F}$. (En el caso trivial $n = 1$, se ve que $\mathrm{GL}(1, \mathbb{F}) = \mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.)

Si dos matrices $n \times n$ sobre $\mathbb{F}$ tienen determinante 1, son invertibles y tanto su producto como sus matrices inversas también tienen determinante igual a 1. Tales matrices forman un subgrupo,

$$\mathrm{SL}(n, \mathbb{F}) := \{ A \in \mathrm{GL}(n, \mathbb{F}) : \det A = 1 \}.$$

Este grupo se llama un **grupo especial lineal** sobre $\mathbb{F}$.

Aunque $\mathbb{Z}$ no es un cuerpo, una matriz A de determinante 1 con entradas en $\mathbb{Z}$ tiene matriz inversa A^{-1} con entradas en $\mathbb{Z}$; además, vale $\det A^{-1} = 1/\det A = 1$ también. Tales matrices forman un grupo, llamado $\mathrm{SL}(n, \mathbb{Z})$. ◊

Definición 1.16. Si G es un grupo y si $g \in G$, se escribe $g^2 := gg$, $g^3 := ggg$, etcétera; también $g^1 := g$ y $g^0 := 1$. Además, se escribe $g^{-n} := (g^{-1})^n$, notando que $g^{-n} = (g^n)^{-1}$.

El menor entero positivo m tal que $g^m = 1$ se llama el **período del elemento** g en el grupo G. Si no existe $m \in \mathbb{P}$ alguno con $g^m = 1$, dícese que el período de g es infinito.[6]

El **orden** del grupo G, escrito $|G|$, es el número de elementos (es decir, la cardinalidad) del conjunto G.

Si hay un entero positivo $m \in \mathbb{P}$ tal que $g^m = 1$ para *todo* $g \in G$, el menor m con esta propiedad se llama el **exponente** del grupo G. El exponente es entonces el mínimo común múltiplo de los períodos de los elementos individuales de G. ◊

Los grupos C_4 y V tiene 4 elementos cada uno. Sin embargo, C_4 posee dos elementos de período 4 (las rotaciones $\rho_{\pi/2}$ y $\rho_{3\pi/2}$) y un elemento de período 2 (la mediavuelta ρ_π), aparte del elemento neutro, de período 1. En cambio, el grupo V posee tres elementos de período 2, aparte del elemento neutro. Así, C_4 tiene exponente 4 mientras V tiene exponente 2. Este ejercicio de conteo permite distinguir entre los dos grupos; para anticipar un poco la terminología, esto muestra que C_4 y V *no son isomorfos*.

[5] El nombre V para este grupo le fue otorgado por Félix Klein, quien lo llamo *Vierergruppe* en alemán (es decir, "grupo de cuatro").

[6] Algunos libros hablan del *orden de un elemento* g como sinónimo de su período. Al preferir el término *período*, aquí se sigue el libro de Lang, que también usa $\#(G)$ en vez de $|G|$ para denotar el orden del grupo.

1.2 Subgrupos y coclases

En algunos de los ejemplos anteriores, se ha usado el término "subgrupo" de manera informal, para denotar un grupo que aparece como una parte de otro grupo. He aquí la definición formal.

Definición 1.17. Si G es un grupo, una parte no vacía $H \subseteq G$ se llama un **subgrupo** de G si H también es un grupo, con el producto heredado de G. En otras palabras, H es un subgrupo de G si:

(i) $h_1, h_2 \in H \implies h_1 h_2 \in H$; y

(ii) $h \in H \implies h^{-1} \in H$.

Obsérvese que cualquier subgrupo de G necesariamente contiene el elemento neutro 1.

Se escribe $H \leqslant G$ para denotar que H sea un subgrupo de G. Si $H \leqslant G$ y $H \neq G$, se escribe $H < G$.

Si $K \subseteq G$ y $L \subseteq G$ son dos *partes* de G que no necesariamente son subgrupos, conviene usar las notaciones

$$KL := \{\, kl : k \in K,\, l \in L \,\}, \qquad K^{-1} := \{\, k^{-1} : k \in K \,\}.$$

Entonces $H \leqslant G$ si y sólo si $HH = H$ y $H^{-1} = H$. ◊

Las dos condiciones (i) y (ii) de la definición son equivalentes a una sola condición alternativa:

$$h, k \in H \implies hk^{-1} \in H. \tag{1.2}$$

En efecto, la condición (ii) es inmediato, al aplicar esta propiedad al par de elementos $1, h \in H$; luego, la condición (i) sigue al aplicarla a los elementos $h_1, h_2^{-1} \in H$.

Ejemplo 1.18. En el grupo aditivo $\mathbb{C} = (\mathbb{C}, +)$, hay una cadena de subgrupos:

$$\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}.$$

En el grupo multiplicativo $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, hay otra cadena de subgrupos:

$$(\mathbb{Q}^\times \cap (0, \infty)) \leqslant \mathbb{Q}^\times \leqslant \mathbb{R}^\times \leqslant \mathbb{C}^\times.$$ ◊

En el Ejemplo 1.12, las rotaciones de $\mathbb{R}^2$ alrededor del origen forman un subgrupo propio del grupo ortogonal: $\mathrm{SO}(2) < \mathrm{O}(2)$.

En el Ejemplo 1.13, el grupo cíclico de rotaciones del n-gono regular forman un subgrupo propio del grupo diedral de sus simetrías: $C_n < D_n$.

En el Ejemplo 1.15, el grupo especial lineal de matrices $n \times n$ es un subgrupo propio del grupo general lineal: $\mathrm{SL}(n, \mathbb{F}) < \mathrm{GL}(n, \mathbb{F})$.

Cualquier grupo G posee al menos *dos subgrupos triviales*: G mismo y el singulete $\mathbf{1} = \{1\}$.

Si $H \leqslant G$ y $K \leqslant G$, la intersección $H \cap K$ es otro subgrupo de G. (Sin embargo, la parte $HK \subseteq G$ no es necesariamente un subgrupo, si G no es abeliano.) Más generalmente, si $\{ H_j : j \in J \}$ es una familia de subgrupos de G, su intersección $H := \bigcap_{j\in J} H_j$ es también un subgrupo de G. De hecho, si $h, k \in H$, entonces $h, k \in H_j$ para todo j, así que $hk^{-1} \in h_j$ para todo j y por ende $hk^{-1} \in H$: la intersección H cumple el criterio (1.2).

Definición 1.19. Sea S una parte de un grupo G. Denótese por $\langle S \rangle$ el menor subgrupo que incluye S, esto es,

$$\langle S \rangle := \bigcap \{ H \leqslant G : S \subseteq H \}.$$

Dícese que $\langle S \rangle$ es el **subgrupo generado por** S.

Si $S = \{a_1, a_2, \ldots, a_m\}$ es un conjunto finito, se puede escribir $\langle S \rangle = \langle a_1, a_2, \ldots, a_m \rangle$. Un grupo G se llama *finitamente generado* si $G = \langle a_1, \ldots, a_m \rangle$ para una cantidad finita de elementos $a_1, \ldots, a_m \in G$, en cuyo caso estos elementos son un juego de *generadores* para G.

Un **grupo cíclico** es un grupo generado por un solo elemento. ◊

Ejemplo 1.20. El grupo aditivo $\mathbb{Z} = \langle 1 \rangle$ es un grupo cíclico infinito. El grupo aditivo de residuos $\mathbb{Z}_m = \langle \overline{1} \rangle$ es un grupo cíclico finito de m elementos, para cada $m \in \mathbb{N}$ con $m \geqslant 2$.

El grupo de rotaciones C_n del Ejemplo 1.13 es un grupo cíclico finito de n elementos (de ahí su nombre) si $n \in \mathbb{N}$ con $n \geqslant 3$. La rotación con ángulo $2\pi/n$ es un generador: $C_n = \langle \rho_{2\pi/n} \rangle$.

La *mediavuelta* ρ_π cumple $\rho_\pi^2 = 1_2$, así que $C_2 := \{1_2, \rho_\pi\}$ es un grupo cíclico de dos elementos, con generador ρ_π.

El grupo trivial $\mathbf{1} = \{1\}$ es también cíclico, porque obviamente $\mathbf{1} = \langle 1 \rangle$. (En este caso, también se podría tomar $S = \emptyset$: el menor subgrupo que incluye S debe contener el elemento neutro, así que $\mathbf{1} = \langle \emptyset \rangle$.) ◊

Ejemplo 1.21. El grupo diedral D_n del Ejemplo 1.13 no es cíclico. Cualquier elemento ρ_θ del subgrupo C_n genera C_n o bien un subgrupo de C_n, que no es todo D_n. Cualquier reflexión μ_θ de la lista (1.1b) cumple $\mu_\theta^2 = 1_2$ y por tanto genera un subgrupo de orden 2, que tampoco es todo D_n.

Sin embargo, es fácil comprobar que $D_n = \langle \rho_{2\pi/n}, \mu_{2\pi/n} \rangle$; el grupo diedral es generado por una rotación y una reflexión. ◊

El grupo $\mathbb{Q} = \langle 1/n : n = 1, 2, \ldots \rangle$ es un ejemplo de un grupo abeliano que no es finitamente generado.

Todo grupo cíclico es abeliano. En efecto, si $G = \langle a \rangle$, entonces $G = \{ a^n : n \in \mathbb{Z} \}$ —fíjese que esta lista tiene muchas repeticiones si $|G|$ es finito— y está claro (por la asociatividad del producto) que $a^m a^n = a^{m+n} = a^n a^m$ si $m, n \in \mathbb{Z}$.

Proposición 1.22. *Cualquier subgrupo de un grupo cíclico $G = \langle a \rangle$ es también cíclico.*

Si G es infinito, cada subgrupo es de la forma $H = \langle a^m \rangle$ para algún m y H es infinito.

Si $|G| = n$ es finito y $H \leqslant G$, entonces $|H|$ divide n; y si q divide n, hay exactamente un subgrupo $H \leqslant G$ con $|H| = q$.

Demostración. Sea $H \leqslant G$ un subgrupo no trivial (es decir, $\mathbf{1} < H < G$) y sea $m \in \mathbb{P}$ el menor entero positivo tal que $a^m \in H$. Entonces $\langle a^m \rangle \subseteq H$. Si $a^k \in H$ y si k no fuera un múltiplo de m, entonces $k = qm + r$ donde $q \in \mathbb{Z}$ y $r \in \{1, 2, \ldots, m-1\}$. Pero en ese caso, sería $a^r = a^{k-qm} = a^k((a^m)^{-1})^q \in H$, contrario a la minimalidad de m. Esto demuestra que $H = \langle a^m \rangle$ así que H es cíclico.

Si $\langle a \rangle$ es infinito, las potencias a^n, para $n \in \mathbb{Z}$, son distintas; en particular, las potencias $a^{qm} = (a^m)^q$, para $q \in \mathbb{Z}$, son distintas y $\langle a^m \rangle$ es infinito.

Si $|G| = n$ es finito, entonces $G = \langle a \rangle = \{ 1, a, a^2, \ldots, a^{n-1} \}$ porque a^n debe estar en esa lista, lo cual obliga que $a^n = 1$. Si $H = \langle a^m \rangle$ es un subgrupo y si $n = qm + r$ donde ahora $r \in \{0, 1, \ldots, m-1\}$, entonces $1 = a^n = (a^m)^q a^r$, así que $a^r = (a^m)^{-q} \in H$ y por tanto $r = 0$. Se ha comprobado que m divide n y que $H = \{1, a^m, a^{2m}, \ldots, a^{(q-1)m}\}$.

Inversamente, si q divide n, sea $m := n/q$; entonces $H := \{1, a^m, a^{2m}, \ldots, a^{(q-1)m}\}$ es un subgrupo de G con $|H| = q$.

Además, si $K = \langle b \rangle$ es un subgrupo con $|K| = q$, entonces $b = a^k$ para algún k, con $k = pm + s$ para $s \in \{0, 1, \ldots, m-1\}$. Como $1 = b^q = a^{qk} = a^{pn+qs} = a^{qs}$, se obtiene $s = 0$, luego $k = pm$ y $b = a^{pm} \in H$. Esto muestra que $K \subseteq H$, de donde $K = H$ ya que $|K| = q = |H|$. □

Notación. En la demostración anterior, se ha usado ciertas propiedades de divisibilidad de los números enteros. Conviene introducir un símbolo de divisibilidad. En adelante, se escribe $m \mid n$ (en palabras, "*m divide n*") si $n = qm$ para algún $q \in \mathbb{Z}$.

El generador de un grupo cíclico G no es único (si $|G| > 2$). En efecto, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$; y si $|G| = n$ es finito, con $G = \langle a \rangle$, entonces $G = \langle b \rangle$ también si $b = a^k$ donde *los enteros k y m son relativamente primos*. Se sabe que esto ocurre si y sólo hay $p, q \in \mathbb{Z}$ con $pk + qn = 1$. En tal caso, $b^p = a^{pk} = a^{pk+qn} = a$, lo cual muestra que $\langle b \rangle \supseteq \langle a \rangle$ a la vez que $\langle a \rangle \supseteq \langle b \rangle$ pues $a^k = b$. Por ejemplo, $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$ es un grupo cíclico con dos generadores distintos.

Notación. El último párrafo muestra la conveniencia de otra notación para los números enteros: se puede escribir $m \perp n$ (en palabras: "*m es primo con n*") cuando m y n son relativamente primos.[7]

► La existencia de subgrupos no triviales de un grupo finito da lugar a un importante principio de conteo: los elementos del grupo pueden organizarse en ciertas clases de equivalencia determinadas por un subgrupo dado.

Definición 1.23. Sea G un grupo y sea $H \leqslant G$ uno de sus subgrupos. Si $g \in G$, considérese los dos conjuntos

$$gH := \{\, gh : h \in H \,\}, \qquad Hg := \{\, hg : h \in H \,\}. \tag{1.3}$$

Estos conjuntos se llaman **clases laterales** o bien **coclases**[8] del subgrupo H. En más detalle: el conjunto gH es la **coclase a izquierda** y Hg es la **coclase a derecha** del elemento g, con respecto al subgrupo H. ◊

Lema 1.24. *Las coclases a izquierda para un determinado subgrupo $H \leqslant G$ forman una* partición *de los elementos de G. Dos coclases coinciden, $g_1H = g_2H$, si y sólo si $g_1^{-1}g_2 \in H$.*

Demostración. Es evidente que $G = \bigcup\{\, gH : g \in G \,\}$, porque cada $g \in G$ pertenece a una coclase: $g = g\,1 \in gH$.

Si $k \in H$, entonces $kH = \{\, kh : h \in H \,\} \subseteq H$, mientras $H = \{\, kk^{-1}h : h \in H \,\} \subseteq kH$; en consecuencia, $kH = H$ para todo $k \in H$.

Si $g_1H \cap g_2H \neq \emptyset$, entonces hay elementos $h_1, h_2 \in H$ con $g_1h_1 = g_2h_2$. Como

$$g_1h_1 = g_2h_2 \iff h_1 = g_1^{-1}g_2h_2 \iff h_1h_2^{-1} = g_1^{-1}g_2,$$

se obtiene $g_1^{-1}g_2 \in H$. Por lo tanto, $g_1^{-1}g_2H = H$, así que

$$g_1H = \{\, g_1h' : h' \in H \,\} = \{\, g_1g_1^{-1}g_2h : h \in H \,\} = \{\, g_2h : h \in H \,\} = g_2H.$$

En resumen, $g_1H \cap g_2H \neq \emptyset$ implica $g_1H = g_2H$. De forma contrapositiva, $g_1H \neq g_2H$ implica $g_1H \cap g_2H = \emptyset$; es decir, las coclases gH son disjuntos. □

[7] La notación "$m \perp n$" fue introducida, un poco tardíamente, en el influyente libro: Ronald L. Graham, Donald E. Knuth y Oren Patashnik, *Concrete Mathematics*, Addison-Wesley, Reading, MA, 1989. (Véase la proclamación en la página 115.)

[8] La terminología "clases laterales" es muy apropiada y se usa en los idiomas romances (en francés, por ejemplo: *classes à gauche*, *classes à droite*). Sin embargo, en inglés el término usual es *coset*. Dado que el vocablo *set* se traduce como "conjunto", esto ha dado lugar a una execrable traducción mexicana "coconjunto". Aparte de su cacofonía, este juego de sílabas no comunica idea alguna. Aquí se emplea el término *coclase* como sinónimo de "clase lateral" con una sola palabra.

Para las coclases a derecha, hay una afirmación similar: ellas forman otra partición de G, con $Hg_1 = Hg_2$ si y sólo si $g_1 g_2^{-1} \in H$.

La totalidad de coclases a izquierda con respecto a H forman un **conjunto cociente**, denotado por G/H. *El número* (es decir, la cardinalidad) *de tales coclases a izquierda* se denota por $[G\colon H]$, el **índice** de H en G.

La inversión $g \mapsto g^{-1}$ es una biyección de G en G y lleva la coclase a izquierda gH en la coclase a derecha Hg^{-1}. Esto establece una correspondencia biunívoca entre coclases a izquierda y coclases a derecha. Por lo tanto, el índice $[G\colon H]$ es también *el número de coclases a derecha* del subgrupo H.

Obsérvese que la partición en coclases a izquierda corresponde a una *relación de equivalencia* sobre G. Por el lema anterior, $g_1 \sim g_2$ para esta equivalencia si y sólo si $g_1^{-1} g_2 \in H$. ⟦ La transitividad de esta relación se obtiene de $g_1^{-1} g_3 = (g_1^{-1} g_2)(g_2^{-1} g_3) \in H$. ⟧

Teorema 1.25 (Lagrange)**.** *Si G es un grupo finito y $H \leqslant G$ es un subgrupo, entonces vale $|G| = |H|\,[G\colon H]$, así que $|H|$ divide $|G|$.*

Demostración. Si $|G| = n$, $[G\colon H] = r$, entonces G es una unión disjunta de coclases,[9]

$$G = g_1 H \uplus g_2 H \uplus \cdots \uplus g_r H,$$

porque estas coclases forman una *partición* del conjunto finito G.

Además, para cada $g \in G$, la aplicación $h \mapsto gh$ es una biyección entre H y gH, por la ley de cancelación —véase la Proposición 1.2(e)— así que $|gH| = |H|$ para cualquier $g \in G$. Luego $n = r|H|$. □

Corolario 1.26. *Si G es un grupo finito con $|G| = n$, entonces $g^n = 1$ para todo $g \in G$.*

Demostración. Si el elemento $g \in G$ tiene período m, entonces $\langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$ es un subgrupo de G de orden m. Luego $n = qm$ para $q = [G\colon \langle g \rangle]$, por el teorema de Lagrange. Ahora es inmediato que $g^n = (g^m)^q = 1^q = 1$. □

1.3 Elementos conjugados y subgrupos normales

Si G es un grupo y $H \leqslant G$ es un subgrupo, es natural preguntar si el conjunto cociente G/H es también un grupo. Para contestar, habría que definir una operación de producto entre coclases (a izquierda) de H. A primera vista, un candidato para tal producto sería tomar $(g'H)(g''H) := g'g''H$, donde $(g', g'') \mapsto g'g''$ denota el producto en el grupo G. Sin

[9] El símbolo ⊎ denota **unión disjunta**. (Algunos libros usan otro símbolo ⊔ para el mismo propósito.)

embargo, no está claro si esa operación estaría bien definida: dados elementos $g'h' \in g'H$ y $g''h'' \in g''H$, habría que encontrar $h''' \in H$ tal que $(g'h')(g''h'') = g'g''h'''$ en G.

Para un grupo abeliano G, es suficiente tomar $h''' := h'h''$, porque

$$(g'h')(g''h'') = (g'g'')(h'h'') \quad \text{si } G \text{ es abeliano.}$$

Por lo tanto, la falta de conmutatividad $h'g'' \neq g''h'$ —en el caso no abeliano— obstruye la definición de un producto entre coclases en el conjunto G/H. Sin embargo, esa obstrucción se podría vencer si, para g y h' dados, siempre fuera posible hallar algún $h \in H$ tal que $h'g = gh$. Al notar que $gh \in gH$ mientras $h'g \in Hg$, la condición esencial para definir productos de coclases es la coincidencia de coclases a derecha con coclases a izquierda, es decir, $Hg = gH$ para todo $g \in G$. (En el caso de grupos finitos, el Teorema 1.25 de Lagrange garantiza que los conjuntos Hg y gH tiene el mismo número de elementos, $[G : H]$, porque su demostración se aplica de igual manera a coclases a derecha.)

Definición 1.27. Un subgrupo H de un grupo G es un **subgrupo normal** si $gH = Hg$ para todo $g \in G$. Se usa la notación $H \trianglelefteq G$ para denotar que H sea un subgrupo normal de G; o bien $H \triangleleft G$ si H es un subgrupo normal propio de G.

Una definición equivalente de subgrupo normal es el siguiente. Dado $g \in G$ y $H \leq G$, considérese el conjunto de elementos

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

Este conjunto es también un *subgrupo* de G, porque

$$(gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1} \quad \text{y} \quad (ghg^{-1})^{-1} = gh^{-1}g^{-1}$$

por asociatividad. Está claro que la ecuación $h'g = gh$ es equivalente a $h' = ghg^{-1}$, así que $Hg = gH$ si y sólo si $gHg^{-1} = H$. En resumen: un subgrupo H es G es **normal** si y sólo si $gHg^{-1} = H$ para todo $g \in G$. ◊

Definición 1.28. Dos elementos $x, y \in G$ son **conjugados** en el grupo G si existe $g \in G$ tal que $y = gxg^{-1}$; lo cual es lo mismo que $x = g^{-1}yg$. Si y, z son conjugados con $z = hyh^{-1}$, entonces $z = hgxg^{-1}h^{-1} = (hg)x(hg)^{-1}$, así que x, z son también conjugados. Es evidente, entonces, que la conjugación en G es una *relación de equivalencia* sobre G.

Si $x \in G$, el conjunto $\{\, gxg^{-1} : g \in G \,\}$, la *clase conjugada* de x, es la clase de equivalencia de x bajo esta relación. Si $H \leqslant G$, entonces el subgrupo $gHg^{-1} = \{\, ghg^{-1} : h \in H \,\}$ se llama un *subgrupo conjugado* de H. (Está claro que el subgrupo H es normal si y sólo si coincide con todos sus conjugados.) ◊

En un grupo abeliano, la relación de conjugación es trivial, porque $gxg^{-1} = xgg^{-1} = x$ para todo $g, x \in G$; la clase conjugada de x es el conjunto solitario $\{x\}$ y cada clase de equivalencia posee un solo elemento. En cambio, si G no es abeliano, hay al menos una clase de equivalencia con más de un elemento.

Fíjese que un subgrupo $H \leqslant G$ es normal si y sólo si H es una unión de clases conjugadas. En particular, todo subgrupo de un grupo abeliano es automáticamente normal.

Es importante notar que

$$(gxg^{-1})^m = gxg^{-1}\,gxg^{-1}\cdots gxg^{-1} = gxx\cdots xg^{-1} = gx^m g^{-1}.$$

Luego $(gxg^{-1})^m = 1$ si y sólo si $x^m = 1$. Por lo tanto, los elementos conjugados x y gxg^{-1} tienen el mismo período. Por lo tanto, todos los miembros de una clase conjugada tienen el mismo período.

Ejemplo 1.29. En el grupo $GL(n,\mathbb{F})$ de matrices invertibles $n \times n$ sobre un cuerpo $\mathbb{F}$, los conjugados de una matriz A son las matrices de la forma PAP^{-1} con P invertible. En otras palabras, dos matrices (invertibles) son conjugadas en $GL(n,\mathbb{F})$ si y sólo si son *semejantes* como matrices.

En álgebra lineal, hay algoritmos que construyen una *forma canónica* de una matriz: está puede ser la "forma canónica racional", o bien, en el caso $\mathbb{F} = \mathbb{C}$, la llamada "forma canónica de Jordan". Dos matrices son semejantes si y sólo sus formas canónicas (de una determinada especie) coinciden. De esta manera, se puede identificar todas las clases conjugadas del grupo $GL(n,\mathbb{F})$.

Si $g \in GL(n,\mathbb{F})$ y $x \in SL(n,\mathbb{F})$, una propiedad conocida de determinantes muestra que

$$\det(gxg^{-1}) = (\det g)(\det x)(\det g^{-1}) = (\det g)(1)(\det g)^{-1} = 1,$$

así que $gxg^{-1} \in SL(n,\mathbb{F})$ también. Esto demuestra que $SL(n,\mathbb{F}) \lhd GL(n,\mathbb{F})$. ◊

Ejemplo 1.30. Sea S_3 el grupo de todas las permutaciones del conjunto $\{1,2,3\}$. Escríbase (12) para denotar la **transposición** $1 \leftrightarrow 2$ (con $3 \mapsto 3$); escríbase (123) para denotar el **ciclo** $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$. El grupo S_3 tiene 6 elementos:[10]

$$S_3 = \{\underline{1}, (12), (13), (23), (123), (132)\}$$

(donde $\underline{1}$ denota la permutación idéntica $x \mapsto x$). Al agrupar los elementos en juegos con períodos 1, 2 y 3:

$$S_3 = \{\underline{1}\} \uplus \{(12), (13), (23)\} \uplus \{(123), (132)\},$$

[10] Una **permutación** de un conjunto X es una *biyección* $\sigma : X \to X$; la operación de grupo es la composición de estas biyecciones. En la permutación compuesta $\sigma\tau := \sigma \circ \tau$, primero τ permuta los elementos de X y luego σ permuta el resultado.

se obtienen las tres clases conjugadas de S_3. En efecto, obsérvese que

$$(23)(12)(23)^{-1} = (23)(12)(23) = (23)(123) = (13),$$
$$(13)(12)(13)^{-1} = (13)(12)(13) = (13)(132) = (23),$$

así que $\{(12),(13),(23)\}$ es una clase conjugada: no hay otros elementos de período 2. Además, como $(12)(123)(12)^{-1} = (12)(123)(12) = (12)(13) = (132)$, los dos elementos de período 3 forman otra clase conjugada $\{(123),(132)\}$.

Nótese también que el subgrupo $H = \{\underline{1},(12)\}$ de S_3 *no es normal*: si $g = (23)$, entonces $gHg^{-1} = \{\underline{1},(13)\} \neq H$. ◊

Ejemplo 1.31. Sea S_n el grupo de todas las permutaciones del conjunto $\{1,2,\ldots,n\}$ para $n \in \mathbb{N}$ con $n \geqslant 2$. El ***k*-ciclo** $a_1 \mapsto a_2$, $a_2 \mapsto a_3$,..., $a_{k-1} \mapsto a_k$, $a_k \mapsto a_1$ se denota por $(a_1 a_2 \ldots a_k)$. Cualquier $\sigma \in S_n$ es un producto de ciclos disjuntos (contando la identidad $\underline{1}$ como ciclo trivial); y dos ciclos disjuntos conmutan. Si $(b_1 b_2 \ldots b_k)$ es otro k-ciclo, entonces

$$\sigma\,(a_1 a_2 \ldots a_k)\,\sigma^{-1} = (b_1 b_2 \ldots b_k) \quad \text{si} \quad \sigma(a_j) = b_j \quad \text{para} \quad j = 1,2,\ldots,k,$$

porque el término al lado izquierdo lleva $b_j \mapsto a_j \mapsto a_{j+1} \mapsto b_{j+1}$ para $j = 1,2,\ldots,k-1$, lleva $b_k \mapsto a_k \mapsto a_1 \mapsto b_1$ y deja fijo los otros elementos de $\{1,2,\ldots,n\}$. De este modo, se ve que dos k-ciclos cualesquiera son conjugados en S_n. Por otro lado, está claro que cualquier permutación de la forma $\tau\,(a_1 a_2 \ldots a_k)\,\tau^{-1}$ es un k-ciclo.

En consecuencia, las clases conjugadas en S_n corresponden a los diversos *patrones de productos de ciclos disjuntos*. En S_4, por ejemplo, hay 5 clases conjugados: las permutaciones

$$\underline{1}, \quad (12), \quad (123), \quad (1234), \quad (12)(34)$$

son representantes de cada clase: la identidad, un 2-ciclo o transposición, un 3-ciclo, un 4-ciclo, un producto de dos transposiciones disjuntas. Obsérvese que hay $\binom{4}{2} = 6$ transposiciones, hay ocho 3-ciclos, hay seis 4-ciclos y hay tres productos de dos transposiciones. Como $1+6+8+6+3 = 24 = |S_4|$, no hay otras clases conjugadas. ◊

Lema 1.32. *Si $H \leqslant G$ con $[G:H] = 2$, entonces H es un subgrupo* normal *de G.*

Demostración. Como $[G:H] = 2$, hay exactamente dos coclases a izquierda en el conjunto G/H. Uno de ellas es el propio H (la coclase del elemento neutro 1) y el otro es gH para algún $g \in G \setminus H$. Fíjese que $gH = G \setminus H$ en tal caso.

De igual manera, hay exactamente dos coclases a derecha, el propio H y Hk para algún $k \in G \setminus H$ (en cuyo caso $Hk = G \setminus H$).

Para cualquier elemento $g \in G$, entonces, sólo hay dos posibilidades: o bien $g \in H$, en cuyo caso $gH = H = Hg$, o bien $g \notin H$, en cuyo caso $gH = G \setminus H = Hg$. Por lo tanto, la igualdad $gH = Hg$ es válida para todo g, así que $H \lhd G$. □

► Si $H \leqslant G$ es un subgrupo, no necesariamente normal, el conjunto cociente no tiene otra estructura *a priori*. Sin embargo, el cociente por un subgrupo *normal* hereda la operación de grupo de G.

Lema 1.33. *Si $N \trianglelefteq G$, el conjunto cociente G/N es un* grupo*, cuya operación de producto es $(gN)(hN) := ghN$.*

Demostración. Si $n', n'' \in N$, entonces $(gn')(hn'') = gh(h^{-1}n'h)n'' = ghn \in ghN$. De hecho, $h^{-1}n'h \in h^{-1}Nh = N$ porque el subgrupo N es normal, así que $n := (h^{-1}n'h)n'' \in N$. Dicho de otra manera, el producto (elemento por elemento) de los coclases gN y hN coincide con la coclase ghN. Entonces la operación $(gN)(hN) := ghN$ sobre las coclases está bien definida.

Como esta operación está heredada de la operación de producto en G, su asociatividad está clara: $(ghN)(kN) = (gN)(hkN) = ghkN$. El elemento neutro de G/N es el subgrupo N, visto como la coclase de $1 \in G$. Además, como $(gN)(g^{-1}N) = N = (g^{-1}N)(gN)$, el inverso de la coclase gN es la coclase $g^{-1}N$.

También, como $gN = Ng$ para cualquier $g \in G$, la operación de grupo en G/N puede escribirse con la fórmula alternativa $(Ng)(Nh) := Ngh$. □

Definición 1.34. Si $x \in G$, el **centralizador** de x en G es el subgrupo

$$Z_G(x) := \{\, g \in G : gx = xg \,\} = \{\, g \in G : gxg^{-1} = x \,\}.$$

Más generalmente, Si $S \subseteq G$, el centralizador de S en G es el subgrupo

$$\begin{aligned} Z_G(S) &:= \{\, g \in G : gx = xg \text{ para todo } x \in S \,\} \\ &= \{\, g \in G : gxg^{-1} = x \text{ para todo } x \in S \,\} = \bigcap_{x \in S} Z_G(x). \end{aligned}$$

El **centro** de un grupo G es el subgrupo $Z(G) := \{\, g \in G : gx = xg \text{ para todo } x \in G \,\}$. Es evidente que $Z(G)$ es un *grupo abeliano* y que $Z(G) \trianglelefteq G$. Además, está claro que $Z(G) = G$ si y sólo si G es abeliano. ◊

Definición 1.35. Si $S \subseteq G$, el **normalizador** de S es el subgrupo

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

Si $H \leqslant G$, entonces $H \trianglelefteq N_G(H)$. Además, $H \trianglelefteq G$ si y sólo si $N_G(H) = G$. ◊

Ejemplo 1.36. En el grupo S_3, se verifica por cálculos directos que $Z_G((12)) = \{\underline{1}, (12)\}$ y $Z_G((13)) = \{\underline{1}, (13)\}$. Como $Z(G) = \bigcap_{x\in G} Z_G(x)$, se sigue que $Z(S_3) = \{\underline{1}\} = \mathbf{1}$.

Del mismo modo se verifica que $Z(S_n) = \mathbf{1}$ para cualquier $n \geqslant 3$. ◊

Ejemplo 1.37. En $GL(n, \mathbb{F})$, el centro consta de matrices escalares (múltiplos de la identidad); luego $Z(GL(n, \mathbb{F})) = \{\, a\, 1_n : a \in \mathbb{F}^\times \,\}$. ◊

Lema 1.38. *Si $x \in G$, el número de elementos en la clase conjugada de x es igual al índice $[G : Z_G(x)]$.*

Demostración. Si $gxg^{-1} = hxh^{-1}$ en G, entonces $g^{-1}hxh^{-1}g = g^{-1}gxg^{-1}g = x$, es decir, $g^{-1}h \in Z_G(x)$. Por el Lema 1.24, las coclases $gZ_G(x)$ y $hZ_G(x)$ coinciden.

Por otro lado, si $gxg^{-1} \neq hxh^{-1}$, entonces $g^{-1}hxh^{-1}g \neq x$, así que $g^{-1}h \notin Z_G(x)$: en este caso, las coclases $gZ_G(x)$ y $hZ_G(x)$ son distintas. Luego, el número de elementos distintos en la clase conjugada de x es igual al número de coclases del subgrupo $Z_G(x)$.

(Obsérvese que este número es un divisor de $|G|$ si G es finito, por el teorema de Lagrange.) □

En vista del Lema 1.38, el conjunto solitario $\{x\}$ es una clase conjugada si y sólo si $Z_G(x) = G$, es decir, si y sólo si $x \in Z(G)$. Esta sencilla observación tiene una consecuencia importante.

Proposición 1.39. *Si $|G| = p^m$ donde p es un número primo, entonces $Z(G) \neq \mathbf{1}$.*

Demostración. El grupo G es la unión disjunta de sus clases conjugadas. Por el Lema 1.38 (y el teorema de Lagrange), cada clase tiene p^k elementos con $k \in \{0, 1, \ldots, m-1\}$.

La clase conjugada de 1 es $\{1\}$, que tiene un solo elemento (el caso donde $k = 0$). Luego debe haber al menos $(p-1)$ otros elementos cuyas clases conjugadas tienen un solo elemento. Estos elementos pertenecen a $Z(G)$ y por ende $|Z(G)| \geqslant p$. □

1.4 Homomorfismos e isomorfismos de grupos

Definición 1.40. Si G y K son dos grupos, un **homomorfismo** de G en K es una función $\varphi : G \to K$ tal que:

$$\varphi(gh) = \varphi(g)\,\varphi(h) \quad \text{para todo} \quad g, h \in G. \qquad \text{◊}$$

Un homomorfismo preserva todos los aspectos estructurales de un grupo. No solamente entrelaza los productos; también respeta los elementos neutros y la inversión. En efecto, si se denota por 1 ambos elementos neutros de G y K, entonces

$$1\,\varphi(1) = \varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\,\varphi(1) \quad \text{en } K.$$

Al multiplicar a la derecha por $\varphi(1)^{-1}$, se obtiene $1 = \varphi(1)$ en K. Si $g \in G$, entonces

$$\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(1) = 1 \quad \text{y} \quad \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = 1.$$

La unicidad de inversos entonces implica que $\varphi(g^{-1}) = \varphi(g)^{-1}$ para todo $g \in G$.

Definición 1.41. Si $\varphi : G \to K$ es un homomorfismo de grupos, su **imagen** es el conjunto $\underline{\operatorname{im}\varphi} := \varphi(G) := \{\, \varphi(g) : g \in G \,\} \subseteq K$. Su **núcleo** es

$$\underline{\ker\varphi} := \{\, g \in G : \varphi(g) = 1 \,\} \subseteq G. \qquad \Diamond$$

Proposición 1.42. *Si $\varphi : G \to K$ es un homomorfismo de grupos, entonces su imagen* $\operatorname{im}\varphi$ *es un* subgrupo *de K; su núcleo* $\ker\varphi$ *es un* subgrupo normal *de G.*

Demostración. Las igualdades $\varphi(g)\varphi(h) = \varphi(gh)$ y $\varphi(g)^{-1} = \varphi(g^{-1})$ muestran que $\varphi(G)$ es un subgrupo de K.

Si $g, h \in \ker\varphi$, entonces $\varphi(gh) = \varphi(g)\varphi(h) = 1\,1 = 1$, así que $gh \in \ker\varphi$. Además, si $g \in \ker\varphi$, entonces $\varphi(g^{-1}) = \varphi(g)^{-1} = 1^{-1} = 1$ en K, así que $g^{-1} \in \ker\varphi$ también. Luego $\ker\varphi$ es un subgrupo de G.

Si $x \in \ker\varphi$ y $g \in G$, entonces

$$\varphi(gxg^{-1}) = \varphi(g)\,\varphi(x)\,\varphi(g^{-1}) = \varphi(g)\,1\,\varphi(g)^{-1} = \varphi(g)\,\varphi(g)^{-1} = 1 \quad \text{en } K,$$

así que $gxg^{-1} \in \ker\varphi$. Esto dice que $\ker\varphi \trianglelefteq G$. □

Si $N \trianglelefteq G$, la **aplicación cociente** $\eta : G \to G/N : g \mapsto gN$ es un homomorfismo de grupos, como consecuencia automática de la definición del producto en G/N:

$$\eta(gh) = ghN = (gN)(hN) = \eta(g)\,\eta(h) \quad \text{para todo} \quad g, h \in G. \tag{1.4}$$

Si $\varphi : G \to K$ y $\psi : K \to L$ son homomorfismos, su composición $\psi \circ \varphi : G \to L$ es también un homomorfismo, porque para todo $g, h \in G$, vale

$$\psi \circ \varphi(gh) := \psi(\varphi(gh)) = \psi\big(\varphi(g)\,\varphi(h)\big) = \psi(\varphi(g))\,\psi(\varphi(h)) = \psi \circ \varphi(g)\,\psi \circ \varphi(h).$$

Definición 1.43. Un homomorfismo biyectivo $\varphi : G \to K$ se llama un **isomorfismo**.[11] Dos grupos G y K son **isomorfos** si existe un isomorfismo $\varphi : G \to K$. Esto establece una relación de equivalencia entre grupos: la aplicación inversa $\varphi^{-1} : K \to G : \varphi(g) \mapsto g$ es también un isomorfismo; y si $\psi : K \to L$ es otro isomorfismo, entonces $\psi \circ \varphi : G \to L$ es también un isomorfismo.

Conviene, entonces, escribir $\underline{G \simeq K}$ para decir que los grupos G y K son isomorfos. $\Diamond$

[11] Algunos autores llaman "isomorfismo" a un homomorfismo inyectivo pero no necesariamente sobreyectivo. Eso sería una complicación innecesaria: es preferible hablar de un "isomorfismo sobre su imagen" para referirse a tales homomorfismos.

Ejemplo 1.44. La **función exponencial** $t \mapsto e^t$ es un homomorfismo del grupo aditivo de los números reales $(\mathbb{R}, +)$ en el grupo multiplicativo $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ de los números reales no ceros, porque $e^{s+t} = e^s\, e^t$ para todo $s, t \in \mathbb{R}$. Su imagen es el subgrupo $\mathbb{R}_{>0}$ de los números positivos.

Al considerar $t \mapsto e^t$ como una aplicación $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$, se obtiene un *isomorfismo* de grupos, cuyo isomorfismo inverso es $\log\colon \mathbb{R}_{>0} \to \mathbb{R}$. Las ecuaciones $\exp 0 = 1$, $\log 1 = 0$, $e^{-t} = 1/e^t$ y $\log(1/x) = -\log x$ son instancias de las propiedades generales de homomorfismos. ◊

Ejemplo 1.45. El grupo cíclico C_n de rotaciones de un n-gono regular es isomorfo al grupo aditivo $\mathbb{Z}_n$. La biyección $\varphi : \mathbb{Z}_n \to C_n$ definido por $\varphi(\overline{r}) := \rho_{2r\pi/n}$, para $r \in \{0, 1, \ldots, n-1\}$, es un isomorfismo, porque $\rho_{2r\pi/n}\, \rho_{2s\pi/n} = \rho_{2(r+s)\pi/n} = \rho_{2t\pi/n}$ toda vez que $r+s \equiv t \bmod n$, ya que $\rho_{2n\pi/n} = \rho_{2\pi} = 1$ en el grupo C_n.

Este isomorfismo $\mathbb{Z}_n \simeq C_n$ ejemplifica lo siguiente: *todos los grupos cíclicos de orden n son isomorfos*. En efecto, si $G_n := \{1, g, g^2, \ldots, g^{n-1}\}$ y $K_n := \{1, k, k^2, \ldots, k^{n-1}\}$ son grupos cíclicos de orden n con los generadores respectivos g y k, la biyección $g^r \mapsto k^r$, para $r \in \{0, 1, \ldots, n-1\}$, es un isomorfismo. Por lo tanto, vale $G_n \simeq K_n$. En adelante, se hablará de *el* grupo cíclico de n elementos como grupo abstracto, usualmente denotado por C_n. ◊

Ejemplo 1.46. Los *números complejos* $\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$ forman un cuerpo que incluye el cuerpo real $\mathbb{R}$ (se identifica $x \in \mathbb{R}$ con $x + i0 \in \mathbb{C}$), cuyo producto está determinado por la regla $i^2 = -1$. La función exponencial se define sobre $\mathbb{C}$ por la regla $e^{x+iy} := e^x\, e^{iy}$, donde las exponenciales imaginarias quedan definidas por la *identidad de Euler*:

$$e^{i\theta} := \cos\theta + i \operatorname{sen}\theta, \quad \text{para todo} \quad \theta \in \mathbb{R}.$$

(Es fácil comprobar por trigonometría que $e^{i\theta}\, e^{i\phi} = e^{i(\theta+\phi)}$, para $\theta, \phi \in \mathbb{R}$.)

Obsérvese que $e^{2\pi i} = \cos 2\pi + i \operatorname{sen} 2\pi = 1 + i0 = 1$ y que $e^{i\theta} \neq 1$ si $0 < \theta < 2\pi$. El conjunto de números complejos

$$\mathrm{U}(1) := \{\, e^{i\theta} : 0 \leqslant \theta < 2\pi \,\} = \{\, e^{i\theta} : -\pi < \theta \leqslant \pi \,\}$$

es un grupo multiplicativo, llamado el **grupo unitario** de un parámetro.

No es difícil comprobar que la correspondencia $e^{i\theta} \mapsto \rho_\theta$ es un *isomorfismo* entre los grupos $\mathrm{U}(1)$ y $\mathrm{SO}(2)$.

⟦ El *valor absoluto* del número complejo $z = x + iy \in \mathbb{C}$ es el número real no negativo $|z| := \sqrt{x^2 + y^2}$; es fácil comprobar que $|zw| = |z|\,|w|$ para $z, w \in \mathbb{C}$. La fórmula de Pitágoras $\cos^2\theta + \operatorname{sen}^2\theta = 1$ muestra que $|e^{i\theta}| = 1$ para todo θ; esto muestra que el

grupo unitario uniparamétrico U(1) coincide con $\{z \in \mathbb{C} : |z| = 1\}$, el *círculo unitario* en el plano complejo. El isomorfismo $\mathrm{U}(1) \simeq \mathrm{SO}(2)$ identifica un círculo en el plano $\mathbb{C} \leftrightarrow \mathbb{R}^2$ con el grupo de rotaciones de dicho plano. ⟧ ◊

Ejemplo 1.47. El grupo $V = D_2$ del Ejemplo 1.14, de orden 4, *no es isomorfo* al grupo cíclico C_4.

De hecho, si $\varphi : G \to K$ es un isomorfismo de grupos con inverso $\psi : K \to G$, las relaciones $\varphi(g)^r = \varphi(g^r)$ y $\psi(k)^r = \psi(k^r)$ muestran que los elementos correspondientes $g \in G$ y $\varphi(g) \in K$ tienen el mismo período. Por lo tanto, los grupos G y K tienen el mismo número de elementos de un determinado período r, para cada valor posible de r.

Ahora bien, el grupo V tiene 3 elementos de período 2, junto con el elemento neutro de período 1. Por otro lado, el grupo C_4 tiene un sólo elemento ρ_π de período 2 y dos elementos de período 4 (las rotaciones $\rho_{\pi/2}$ y $\rho_{3\pi/2}$), amén del elemento neutro. Se concluye que $V \not\simeq C_4$. ◊

Ejemplo 1.48. El grupo S_3, de orden 6, *no es isomorfo* al grupo cíclico C_6, porque C_6 es abeliano pero S_3 no es abeliano. ◊

Proposición 1.49. *Un homomorfismo $\varphi : G \to K$ es inyectivo si y sólo si* $\ker \varphi = \{1\}$.

Demostración. Si φ es inyectivo, entonces el conjunto $\ker \varphi = \varphi^{-1}(\{1\})$ tiene un solo elemento, el cual necesariamente es el elemento neutro $1 \in G$.

Por otro lado, si $\ker \varphi = \{1\}$ y si dos elementos $g, h \in G$ satisfacen $\varphi(g) = \varphi(h)$ en K, entonces $\varphi(g^{-1}h) = \varphi(g)^{-1}\varphi(h) = 1$ en K, así que $g^{-1}h \in \ker \varphi$. Luego $g^{-1}h = 1$ en G y por ende $g = h$. En consecuencia, φ es inyectivo. □

► El concepto de isomorfía entre grupos permite pasar de grupos concretos, como $\mathbb{Z}_m$ ó S_n ó $\mathrm{SO}(n)$ a grupos "abstractos", al considerar cualquier grupo particular como un representante de una clase de isomorfía de grupos. Así, por ejemplo, se habla de "el grupo cíclico C_n de orden n" en cualquiera de sus manifestaciones concretos: el grupo de rotaciones del Ejemplo 1.13, o bien el grupo aditivo $(\mathbb{Z}_n, +)$, o bien el grupo de permutaciones generado por el n-ciclo $(123\ldots n)$.

Hay tres criterios importantes que determinan la existencia de isomorfismos entre ciertos grupos. La literatura de la teoría de grupos habla de "los tres teoremas de isomorfía", aunque no hay acuerdo unánime sobre el orden de la lista. Sin embargo, el primer teorema que se enuncia a continuación es el más fundamental.

Teorema 1.50 (Primer teorema de isomorfía)**.** *Sea $\varphi : G \to K$ un homomorfismo de grupos. Entonces*

$$\frac{G}{\ker \varphi} \simeq \varphi(G).$$

Demostración. Escríbase $N := \ker \varphi$; la Proposición 1.42 muestra que $N \trianglelefteq G$. La aplicación cociente $\eta : G \to G/N : g \mapsto gN$ es un homomorfismo sobreyectivo, en vista de (1.4).

Defínase $\psi : G/N \to \varphi(G)$ por $\psi(gN) := \varphi(g)$. Hay que comprobar que ψ está bien definido: si $gN = hN$, entonces $h \in gN$, así que hay $n \in N = \ker \varphi$ con $h = gn$; luego $\varphi(h) = \varphi(g)\varphi(n) = \varphi(g)1 = \varphi(g)$.

Además, ψ es un homomorfismo, porque

$$\psi(gN\, hN) = \psi(ghN) = \varphi(gh) = \varphi(g)\,\varphi(h) = \psi(gN)\,\psi(hN) \quad \text{para} \quad gN, hN \in G/N.$$

Está claro desde su definición que ψ es sobreyectivo. El núcleo de ψ es

$$\ker \psi = \{\, gN : \varphi(g) = 1 \text{ en } K \,\} = \{\, gN : g \in N \,\} = \{N\}.$$

Al recordar que N es el elemento neutro del grupo G/N, la Proposición 1.49 dice que ψ es inyectivo. Entonces ψ es el isomorfismo deseado entre $G/\ker \varphi$ y $\varphi(G)$. □

Corolario 1.51 (Factorización canónica de un homomorfismo)**.** *Cualquier homomorfismo $\varphi : G \to K$ es una composición $\varphi = \iota \circ \psi \circ \eta$ de tres homomorfismos, donde η es sobreyectivo, ψ es un isomorfismo y ι es inyectivo:*

$$\begin{array}{ccc} G & \xrightarrow{\quad\varphi\quad} & K \\ {\scriptstyle\eta}\searrow & & \nearrow{\scriptstyle\iota} \\ & G/\ker\varphi \xrightarrow{\quad\psi\quad} \varphi(G) & \end{array} \tag{1.5}$$

En este diagrama conmutativo, η es la aplicación cociente; ψ es el isomorfismo inducido por φ en el Teorema 1.50; ι es la inclusión de $\varphi(G)$ como subgrupo de K. ⊟

Teorema 1.52 (Segundo teorema de isomorfía)**.** *Sea N un subgrupo normal de un grupo G y sea H un subgrupo de G. Entonces $HN = \{\, hn : h \in H,\ n \in N \,\}$ es un subgrupo de G con $N \trianglelefteq HN$, la intersección $H \cap N$ es un subgrupo normal de H y hay un isomorfismo*

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}.$$

Demostración. La parte $HN \subseteq G$ es un subgrupo puesto que $N \trianglelefteq G$, porque

$$HN = \bigcup_{h\in H} hN = \eta^{-1}(\eta(H)),$$

donde $\eta : G \to G/N$ denota la aplicación cociente. Está claro que $N \leqslant HN$; este subgrupo es normal porque $gNg^{-1} = N$ para todo $g \in G$ y en particular para todo $g \in HN$.

Si $h \in H$ y $x \in H \cap N$, entonces $hxh^{-1} \in H$ obviamente; además, vale $hxh^{-1} \in N$ porque $N \trianglelefteq G$. Se concluye que $(H \cap N) \trianglelefteq H$.

Sea $\varphi := \eta|_H$ la restricción de la aplicación cociente η al subgrupo H. Está claro que $\varphi : H \to G/N$ es un homomorfismo. Su imagen es

$$\varphi(H) = \{\, hN : h \in H \,\} = \{\, hnN : h \in H,\ n \in N \,\} = \frac{HN}{N}$$

y su núcleo es $\ker\varphi = H \cap N$. Al aplicar el Teorema 1.50 a este φ, se obtiene un isomorfismo $\psi : H/(H \cap N) \to HN/N$. □

Teorema 1.53 (Tercer teorema de isomorfía)**.** *Si $N \trianglelefteq G$, sea $\eta : G \to G/N$ la aplicación cociente. La correspondencia $H \mapsto \eta(H) = H/N$ es una biyección entre los subgrupos de G que incluyen N y los subgrupos de G/N. Bajo esta correspondencia, $H/N \trianglelefteq G/N$ si y sólo si $H \trianglelefteq G$; en cuyo caso, hay un isomorfismo*

$$\frac{G}{H} \simeq \frac{G/N}{H/N}.$$

Demostración. Sean H y K dos subgrupos de G que incluyen N tales que $H/N = K/N$. Si $h \in H$, entonces $hN \in H/N = K/N$ así que $h = kn$ con $k \in K$, $n \in N$. Como $N \leqslant K$, se ve que $kn \in K$; luego $H \subseteq K$. De igual manera se obtiene $K \subseteq H$ y por lo tanto $H = K$.

Por otro lado, si $\overline{H}$ es un subgrupo de G/N, sea $H := \eta^{-1}(\overline{H}) = \bigcup\{\, h \in G : hN \in \overline{H} \,\}$. Es fácil comprobar que H es un subgrupo de G; y es evidente que $N \subseteq H$. Por lo tanto, $H \mapsto H/N$ es biyectivo.

Si $H \trianglelefteq G$ con $N \subseteq H$, el homomorfismo cociente $\varphi : G \to G/H$ tiene núcleo H que incluye N. Entonces la aplicación $\tilde{\varphi} : G/N \to G/H$ dado por $\tilde{\varphi}(gN) := \varphi(g) = gH$ es un homomorfismo bien definido. Su núcleo es

$$\ker\tilde{\varphi} = \{\, gN \in G/N : gH = H \,\} = H/N.$$

La Proposición 1.42 entonces dice que $H/N \trianglelefteq G/N$.

Por otro lado, si $H/N \trianglelefteq G/N$, la composición de dos aplicaciones canónicas

$$G \xrightarrow{\ \eta\ } G/N \xrightarrow{\ \tilde{\eta}\ } \frac{G/N}{H/N}$$

es un homomorfismo sobreyectivo $\tilde{\eta} \circ \eta$ cuyo núcleo es H. Luego, $H \trianglelefteq G$.

El Teorema 1.50, aplicado ahora al homomorfismo $\tilde{\varphi}$, produce el isomorfismo deseado $\tilde{\psi} : (G/N)/(H/N) \to G/H$. □

► Muchos isomorfismos permiten identificar dos grupos aparentemente distintos. También son importantes los isomorfismos de un determinado grupo en sí mismo.

Definición 1.54. Sea G un grupo. Un isomorfismo $\varphi : G \to G$ se llama un **automorfismo** del grupo G.

La composición $\psi \circ \varphi$ de dos automorfismos de G es también un automorfismo de G. La función idéntica $1_G : G \to G$ definido por $1_G(g) = g$ es evidentemente un automorfismo. Además, cualquier automorfismo φ, por ser biyectivo, posee un automorfismo inverso φ^{-1} tal que $\varphi^{-1} \circ \varphi = \varphi \circ \varphi^{-1} = 1_G$. Como la composición de funciones es asociativa, se concluye que los automorfismos de G forman un **grupo de automorfismos**, denotado por $\underline{\mathrm{Aut}(G)}$, cuyo elemento neutro es 1_G. ◊

Definición 1.55. Sea G un grupo. Si $g \in G$, la **conjugación** $i_g : G \to G : x \mapsto g\,x\,g^{-1}$ es un automorfismo de G; dícese que las conjugaciones son *automorfismos internos*.

Es evidente que $i_g \circ i_h(x) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = i_{gh}(x)$ y también $i_{g^{-1}}(x) = g^{-1}xg = i_g^{-1}(x)$; los automorfismos internos forman un *subgrupo* $\underline{\mathrm{Inn}(G)}$ de $\mathrm{Aut}(G)$.

Si $\sigma \in \mathrm{Aut}(G)$, entonces

$$\sigma \circ i_g \circ \sigma^{-1}(x) = \sigma(g\,\sigma^{-1}(x)\,g^{-1}) = \sigma(g)\,x\,(\sigma(g)^{-1}) = \sigma(g)\,x\,(\sigma(g))^{-1} = i_{\sigma(g)}(x).$$

De ahí se ve que $\mathrm{Inn}(G)$ es un *subgrupo normal* de $\mathrm{Aut}(G)$. El grupo cociente

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

se denomina, un poco incorrectamente, el *grupo de automorfismos externos* de G. ◊

Proposición 1.56. *Resulta que* $\mathrm{Inn}(G) \simeq G/Z(G)$.

Demostración. Si G es abeliano, cada conjugación es trivial: $i_g = 1_G$. Más generalmente, i_g es trivial si y sólo si el elemento g es central: $g \in Z(G)$.

Defínase una función $\varphi : G \to \mathrm{Inn}(G) : g \mapsto i_g$. Este es un homomorfismo, porque

$$\varphi(gh) : x \mapsto i_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g\,i_h(x)\,g^{-1} = \varphi(g) \circ \varphi(h)(x).$$

Su núcleo es

$$\begin{aligned} \ker\varphi &= \{\, g \in G : g\,x\,g^{-1} = x \text{ para todo } x \in G \,\} \\ &= \{\, g \in G : g\,x = x\,g \text{ para todo } x \in G \,\} = Z(G). \end{aligned}$$

El Teorema 1.50 ahora muestra que $G/Z(G) = G/\ker\varphi \simeq \mathrm{Inn}(G)$. □

Ejemplo 1.57. Si los elementos $\{a_1, \ldots, a_m\}$ generan un grupo G y si $\sigma \in \mathrm{Aut}(G)$, es fácil comprobar que los elementos $\{\sigma(a_1), \ldots, \sigma(a_m)\}$ también generan G. Luego, si $G = \langle a \rangle$ es un grupo cíclico, entonces $\sigma(a)$ es un generador alternativo para G, es decir, $G = \langle \sigma(a) \rangle$.

El grupo cíclico infinito $\mathbb{Z}$ posee exactamente dos generadores (aditivos): los elementos 1 y -1. (Si $m \neq -1, 0, 1$, el subgrupo $\langle m \rangle = m\mathbb{Z}$ consta de los múltiplos enteros de $|m|$ y como tal, es un subgrupo propio de $\mathbb{Z}$.)

En consecuencia, $\mathrm{Aut}(\mathbb{Z}) \simeq C_2$. De hecho, un automorfismo $\alpha \in \mathrm{Aut}(\mathbb{Z})$ queda determinado por el elemento $\alpha(1)$, que debe ser un generador de $\mathbb{Z}$. Si $\alpha(1) = 1$, entonces $\alpha = 1_{\mathbb{Z}}$; si $\alpha(1) = -1$, entonces α es el "cambio de signo" $\sigma : n \mapsto -n$. No hay otras posibilidades. Fíjese que $\sigma^2 = \sigma \circ \sigma = 1_{\mathbb{Z}}$, así que $\mathrm{Aut}(\mathbb{Z}) = \{1_{\mathbb{Z}}, \sigma\}$ es un grupo cíclico de orden 2. ◊

Ejemplo 1.58. Por un argumento similar, se puede identificar el grupo $\mathrm{Aut}(\mathbb{Z}_n)$ para cualquier n finito. De nuevo, $\mathbb{Z}_n = \langle \overline{1} \rangle$ es un grupo cíclico; cada $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$ queda determinado por $\alpha(\overline{1})$, el cual debe ser un generador de $\mathbb{Z}_n$.

Se puede verificar que $\overline{k}$ es un generador para $\mathbb{Z}_n$ si y sólo si k y n son relativamente primos: $k \perp n$ en $\mathbb{Z}$. Si $\sigma_{\overline{k}}$ denota el automorfismo determinado por $\sigma_{\overline{k}}(\overline{1}) = \overline{k}$, se puede notar que

$$\sigma_{\overline{k}} \circ \sigma_{\overline{m}}(1) = \sigma_{\overline{k}}(\overline{m}) = \sigma_{\overline{k}}(\overline{1} + \overline{1} + \cdots + \overline{1}) = \overline{k} + \overline{k} + \cdots + \overline{k} = \overline{km},$$

así que $\sigma_{\overline{k}} \circ \sigma_{\overline{m}} = \sigma_{\overline{km}}$. Esto demuestra que la biyección $\overline{k} \mapsto \sigma_{\overline{k}}$ es un isomorfismo del grupo multiplicativo $\mathbb{Z}_n^\times$ en $\mathrm{Aut}(\mathbb{Z}_n)$. ◊

Ejemplo 1.59. El grupo de cuatro V tiene tres elementos P, Q, R de período 2 (véase el Ejemplo 1.14). No es difícil comprobar que cualquier permutación de P, Q, R define un automorfismo de V (el elemento neutro 1 queda fijo bajo cualquier automorfismo, por supuesto.) Esto muestra que $\mathrm{Aut}(V) \simeq S_3$. ◊

► Un ejemplo importante de un homomorfismo es *el signo de una permutación*. Conviene examinar ahora en más detalle la estructura del grupo de permutaciones S_n.

Una **permutación** $\sigma \in S_n$ es una biyección del conjunto $\{1, 2, \ldots, n\}$ en sí mismo. Es posible expresar σ con una "notación de dos filas":

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

El producto $\sigma\tau$ (o bien $\sigma \circ \tau$) es la composición usual de funciones biyectivas: el efecto de τ sobre $\{1, 2, \ldots, n\}$ seguido por el efecto de σ sobre le resultado. Por ejemplo,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}. \tag{1.6}$$

Para efectuar este cálculo, nótese que

$$1 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 3, \qquad 2 \xrightarrow{\tau} 3 \xrightarrow{\sigma} 2, \qquad 3 \xrightarrow{\tau} 4 \xrightarrow{\sigma} 4, \qquad 4 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 1.$$

Sin embargo, es más eficiente expresar una permutación como un producto de **ciclos**. Denótese por $(i_1 i_2 \dots i_r)$ la permutación cíclica[12]

$$i_1 \mapsto i_2, \quad i_2 \mapsto i_3, \ \dots, \ i_{r-1} \mapsto i_r, \quad i_r \mapsto i_1;$$

con $j \mapsto j$ para $j \notin \{i_1, i_2, \dots, i_r\}$.

Si $(j_1 j_2 \dots j_s)$ es otro ciclo tal que $\{i_1, \dots, i_r\} \cap \{j_1, \dots, j_s\} = \emptyset$, estas dos permutaciones conmutan. Dada una permutación $\sigma \in S_n$ y un número $i_1 \in \{1, 2, \dots, n\}$, tómese $i_2 := \sigma(i_1)$, $i_3 := \sigma(i_2)$, etc., hasta que un elemento de esta lista se repite; entonces σ permuta $\{i_1, i_2, \dots, i_r\}$ cíclicamente y también permuta su complemento en $\{1, 2, \dots, n\}$. Por inducción sobre n, se ve que σ es un producto de ciclos disjuntos:

$$\sigma = (i_1 i_2 \dots i_r)(j_1 j_2 \dots i_s) \cdots (l_1 l_2 \dots l_u), \tag{1.7}$$

cuyos factores conmutan entre sí. El período de σ es el mínimo común múltiplo de $r, s, \dots, u$. Si $\sigma(k) = k$ para algún k, el ciclo trivial $(k) = \underline{1}$ puede ser omitido en la expresión de este producto.

Si dos ciclos no son disjuntos, su producto —leído de derecha a izquierda, por ser una composición de funciones— puede dar lugar a uno o más ciclos nuevos. Por ejemplo, el cálculo (1.6) se escribe de forma más compacta como $(132)(234) = (134)(2) = (134)$.

Una **transposición** es un ciclo (ij) de longitud 2. Obsérvese que

$$(i_1 i_2 \dots i_r) = (i_1 i_r) \cdots (i_1 i_3)(i_1 i_2)$$

así que cualquier ciclo, y luego cualquier permutación, es un producto de transposiciones.

Definición 1.60. Una matriz cuadrada P, de tamaño $n \times n$, es una **matriz de permutación** si cada entrada p_{ij} es 0 ó 1; y si, en cada fila o columna de P, hay exactamente una entrada igual a 1 y $(n-1)$ entradas iguales a 0.

Denótese por $\underline{\mathrm{Perm}(n)}$ el conjunto de todas las matrices de permutación $n \times n$. Este es un *grupo* bajo multiplicación de matrices, con elemento neutro 1_n. Hay exactamente $n!$ elementos en $\mathrm{Perm}(n)$: en las diversas columnas de P, hay que elegir filas distintas en donde colocar la entrada igual a 1.

Defínase una permutación $\pi \in S_n$ por $\pi(j) = k$ si $p_{kj} = 1$. Si $P \in \mathrm{Perm}(n)$ y A es una matriz $n \times n$ cualquiera, entonces en la matriz $AP = B$, la j-ésima columna $\mathbf{b}_j$ de C

[12] Para efectos de la notación, se admiten ciclos triviales $(k) = \underline{1}$.

coincide con la columna $\mathbf{a}_{\pi(j)}$ de A; dicho de otra manera,[13] $b_{ij} = a_{i,\pi(j)}$. Si R es otra matriz de permutación y $\rho \in S_n$ es la permutación asociada a R, y si $C = BR$, entonces $c_{ij} = b_{i,\rho(j)} = a_{i,\pi(\rho(j))}$. Como $C = APR$, se puede observar que la permutación asociada a PR es $\pi\rho \equiv \pi \circ \rho$.

En resumen: la biyección $P \mapsto \pi$ es un *isomorfismo de grupos* $\psi\colon \mathrm{Perm}(n) \to S_n$. ◊

Lema 1.61. *Defínase el* ***signo de una permutación*** $\pi \in S_n$ *así: si* π *es el producto de un número* par *de transposiciones, escríbase* $(-1)^\pi := +1$*; en cambio, si* π *es el producto de un número impar de transposiciones, escríbase* $(-1)^\pi := -1$. *Entonces la asignación* $\Sigma\colon \pi \mapsto (-1)^\pi$ *es un homomorfismo bien definido de* S_n *en el grupo multiplicativo* $\{\pm 1\}$.

Demostración. Si P es una matriz de permutación $n \times n$, resulta que $\det P = \pm 1$. Esto sigue por la expansión del determinante por filas (o por columnas) y una inducción sobre n. Como $\det(PR) = (\det P)(\det R)$, está claro que $\det\colon \mathrm{Perm}(n) \to \{\pm 1\}$ es un isomorfismo de grupos.

Bajo el isomorfismo $S_n \simeq \mathrm{Perm}(n)$, una transposición (ij) corresponde a la matriz $P_{i\leftrightarrow j}$ obtenida de la matriz identidad 1_n al cambiar sus filas $\mathbf{e}_i$ y $\mathbf{e}_j$. Una permutación $\pi = \psi(P)$ es par o impar según sea posible obtener P de 1_n por el intercambio de un número par o impar de columnas. Como los valores $\det P = +1$ y $\det P = -1$ distinguen los dos casos, la paridad del número de transposiciones (o intercambios de columnas) está bien definida. La composición $\det \circ \psi\colon S_n \to \{\pm 1\}$ coincide con la receta $\Sigma\colon \pi \mapsto (-1)^\pi$. Por tanto, Σ es un homomorfismo. □

Definición 1.62. El conjunto de permutaciones pares de $\{1, 2, \ldots, n\}$ es un grupo, el **grupo alternante** A_n. De hecho, $A_n = \ker \Sigma$ es un subgrupo *normal* de S_n.

Del Teorema 1.50, se ve que $[S_n : A_n] = |S_n / \ker \Sigma| = |\operatorname{im} \Sigma| = 2$ para $n \geqslant 2$, porque Σ es sobreyectivo si $n > 1$. Por lo tanto, vale $|A_n| = \frac{1}{2}\, n!$. ◊

Un ciclo $(i_1 i_2 \ldots i_r)$ es par si y sólo si su r es un número impar. El signo del producto (1.7) es $(-1)^\sigma = (-1)^{N(\sigma)}$ donde $N(\sigma) := (r-1) + (s-1) + \cdots + (u-1)$.

[13] Se denotan las *columnas* de una matriz $A = [a_{ij}]$ por $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$.

1.5 Acciones de grupos

El concepto de grupo tomó importancia en la matemática cuando Lagrange y luego Galois consideraron las *sustituciones* de las raíces de una ecuación polinomial: los patrones de intercambios de las raíces aportan información sobre la solubilidad de la ecuación mediante fórmulas explícitas.[14] Posteriormente, Felix Klein enfatizó la importancia de las simetrías admisibles en la clasificación de las geometrías.[15] En los dos casos, los elementos de un grupo aparecen como transformación de otros objetos (raíces de una ecuación algebraica; o puntos de un plano) y los objetos transformados no son menos importantes que las propias transformaciones.

Definición 1.63. Una **acción** (a la izquierda) de un grupo G sobre un conjunto X es una función $\Phi\colon G\times X\to X$ tal que:

(i) $\Phi(g,\Phi(h,x))=\Phi(gh,x)$ para todo $g,h\in G$, $x\in X$;

(ii) $\Phi(1,x)=x$ para todo $x\in X$. ◊

Se acostumbra escribir $\underline{g\cdot x}$ en lugar de $\Phi(g,x)$; con esta notación, las propiedades de una acción son:

$$g\cdot(h\cdot x)=(gh)\cdot x,\qquad 1\cdot x=x. \tag{1.8a}$$

También se escribe $\varphi_g(x):=g\cdot x=\Phi(g,x)$, en cuyo caso las propiedades de una acción son:

$$\varphi_g\circ\varphi_h=\varphi_{gh},\qquad \varphi_1=1_X\,. \tag{1.8b}$$

En otras palabras, $g\mapsto\varphi_g$ es un *homomorfismo* $\varphi\colon G\to S_X$ de G en el grupo S_X de permutaciones del conjunto X.

Definición 1.64. Una acción de grupo define una relación de equivalencia sobre X:

$$x\sim y\quad\text{si y sólo si}\quad x=g\cdot y\text{ para algún }g\in G.$$

[14] Para resolver una ecuación cúbica, Lagrange (1771) consideró otro polinomio de sexto grado —el *resolvente de Lagrange*— empleando las 6 sustituciones (i.e., permutaciones) de las tres raíces originales; el resolvente es fácilmente resoluble y conduce a las fórmulas de Cardano para la ecuación original. Lamentablemente, el método no funciona para las ecuaciones de quinto grado: Évariste Galois (1831) mostró que la dificultad reside en la naturaleza del grupo de sustituciones de las raíces.

[15] Según Klein, una *geometría* se caracteriza por el grupo de sus simetrías; por ejemplo, la geometría del plano euclidiano está determinado por el grupo de *similitudes* del plano: las transformaciones de puntos que conservan la semejanza de triángulos. Esto fue el tema de su discurso inaugural de 1872 en la Universidad de Erlangen (F. Klein, *Vergleichende Betrachtungen über neuere geometrische Forschungen*, publicado en: Mathematische Annalen **43** (1893), 63–100).

⟦ Reflexividad: vale $x \sim x$ porque $x = 1 \cdot x$. Simetría: $x \sim y \implies y \sim x$ porque $x = g \cdot y$ implica $y = g^{-1} \cdot x$. Transitividad: $x \sim y$, $y \sim z \implies x \sim z$ porque $x = g \cdot y$, $y = h \cdot z$ implican $x = g \cdot (h \cdot z) = (gh) \cdot z$. ⟧

La **órbita** de $x \in X$ bajo la acción de G es la *clase de equivalencia* de x bajo esta relación:

$$G \cdot x := \{\, g \cdot x \in X : g \in G \,\} \subseteq X.$$

La acción se llama **transitiva** si $G \cdot x = X$ para algún $x \in X$ (y por ende, para *todo* x). En otras palabras, una acción es transitiva si posee una sola órbita. ◊

Teorema 1.65 (Cayley)**.** *Cualquier grupo G es isomorfo a un grupo de permutaciones. Si G es finito con $|G| = n$, entonces G es isomorfo a un subgrupo de S_n.*

Demostración. Considérese la acción de G sobre sí mismo por *traslaciones a la izquierda*: en cuyo caso se toma $X = G$ y se define $g \cdot h := gh$ para $g, h \in G$. Las propiedades de acción (1.8) son consecuencias de la asociatividad del producto y el papel de 1 como elemento neutro de G. (La existencia de inversos, que implica $g \cdot (g^{-1} \cdot x) = gg^{-1} \cdot x = 1 \cdot x = x$ para $g, x \in G$, indica que la acción es transitiva.) Esta acción se llama la **acción regular a la izquierda** del grupo G.

Fíjese ahora que la función $\lambda_g \colon G \to G : h \mapsto gh$ es una biyección de G en sí mismo, esto es, una permutación del conjunto G. El homomorfismo asociado $\lambda \colon G \to S_G : g \mapsto \lambda_g$ es inyectivo, porque $\lambda_g = \lambda_h$ implica que $gk = hk$ para todo $k \in G$, así que $g = h$ por cancelación. Por lo tanto, λ es un isomorfismo de G en un subgrupo $\lambda(G) \leqslant S_G$.

En particular, si $|G| = n$, de modo que $G = \{g_1, g_2, \ldots, g_n\}$, hay un isomorfismo de grupos $\psi \colon S_G \to S_n$ que lleva cualquier permutación de elementos $g_i \mapsto g_j$ es la permutación correspondiente $i \mapsto j$ del conjunto $\{1, 2, \ldots, n\}$. Luego, $\psi \circ \lambda \colon G \to S_n$ es un homomorfismo inyectivo cuya imagen es un subgrupo de S_n. □

Definición 1.66. Sea $\Phi \colon G \times X \to X$ una acción de grupo. El **subgrupo de isotropía** para un elemento $x \in X$ es el subgrupo

$$G_x := \{\, g \in G : g \cdot x = x \,\} \leqslant G. \qquad \text{◊}$$

Proposición 1.67. *Dada una acción de grupo de G sobre X, el número de elementos de la órbita $G \cdot x$ coincide con el índice $[G \colon G_x]$.*

Demostración. Si $g, h \in G$ y $x \in X$, entonces

$$g \cdot x = h \cdot x \iff g^{-1}h \cdot x = x \iff g^{-1}h \in G_x \iff gG_x = hG_x \text{ en } G/G_x. \tag{1.9}$$

Luego la aplicación $g \cdot x \mapsto gG_x$ es una biyección de la órbita $G \cdot x$ en el conjunto cociente G/G_x. Por lo tanto, sus cardinalidades son iguales: $|G \cdot x| = |G/G_x| = [G \colon G_x]$. □

Ejemplo 1.68. Sea H un subgrupo de G. El grupo G actúa sobre el espacio cociente $X = G/H$ por $g \cdot g'H := (gg')H$. La asociatividad del producto en G establece que $g \cdot (g' \cdot g''H) = gg'g''H = gg' \cdot g''H$.

Esta acción es *transitiva*, porque cada coclase gH es de la forma $g \cdot H$, es decir, está en la órbita de la coclase H. Fíjese que el subgrupo de isotropía de la coclase $H \in G/H$ es el subgrupo H; en efecto, $gH = H$ si y sólo si $g \in H$. (En este caso, la conclusión de la Proposición 1.67 es evidente.)

Un **espacio homogéneo** de un grupo G es, por definición, un conjunto X con una acción transitiva de G. Si H es el subgrupo de isotropía de un determinado punto $x \in X$, la ecuación (1.9) establece una biyección entre X y G/H. ◊

Ejemplo 1.69. El grupo SO(2) de rotaciones del plano actúa sobre el círculo

$$\mathbb{S}^1 := \{ (x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1 \}$$

mediante las transformaciones lineales:[16]

$$\begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix} \begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} x\cos\theta - y\operatorname{sen}\theta \\ x\operatorname{sen}\theta + y\cos\theta \end{bmatrix}.$$

Si $z_\phi := (\cos\phi, \operatorname{sen}\phi)$ denota un punto típico de $\mathbb{S}^1$, esta acción puede escribirse de manera más compacta como $\rho_\theta \cdot z_\phi := z_{\theta+\phi}$.

Esta acción de SO(2) sobre $\mathbb{S}^1$ es *transitiva*; *eficaz* (solo $\rho_\theta = 1$ en SO(2) actúa como $1_{\mathbb{S}^1}$); y *libre* (si $\rho_\theta \cdot z = z$ para algún punto $z \in \mathbb{S}^1$, entonces $\rho_\theta = 1$). En este caso, se dice que $\mathbb{S}^1$ es un *espacio homogéneo principal* de SO(2). Informalmente, el círculo $\mathbb{S}^1$ es una copia biyectiva de SO(2) en donde se "olvida" la ubicación del elemento neutro. ◊

Definición 1.70. Una acción $\Phi\colon G \times X \to X$ es **eficaz** (o **fiel**) si el homomorfismo $\phi : G \to S_X$ es inyectivo. Una acción es eficaz si $g \cdot x = x$ para *todo* $x \in X$ implica $g = 1$ en G.

Una acción $\Phi\colon G \times X \to X$ es **libre** si $g \cdot x = x$ para *algún* $x \in X$ implica $g = 1$ en G.

Si la acción $\Phi\colon G \times X \to X$ es eficaz, libre y transitiva, dícese que X es un **espacio homogéneo principal** de G. ◊

La acción regular de un grupo sobre sí mismo, por "traslaciones a la izquierda" es un ejemplo de una acción eficaz, libre y transitiva. La utilidad del concepto de espacio homogéneo principal consiste en "olvidar" la posición del elemento neutro. En álgebra lineal, por ejemplo, el *espacio afín* $\mathbb{A}^n$ es el mismo conjunto que el espacio vectorial $\mathbb{R}^n$ pero no se declara cuál de sus elementos es el origen.[17]

[16] Aquí se usa la "notación de columnas" $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = (x, y)$ para denotar vectores en $\mathbb{R}^2$.

[17] No es obligatorio que $\mathbb{R}$ sea el cuerpo de base; en la geometría algebraica, se define un espacio afín $\mathbb{A}^n_{\mathbb{F}}$ sobre cualquier cuerpo $\mathbb{F}$, de manera análoga.

El grupo aditivo $\mathbb{R}^n$ actúa sobre el espacio afín $\mathbb{A}^n$ por *traslaciones* $\varphi_x : y \mapsto x + y$ para $x \in \mathbb{R}^n$. De esta manera, $\mathbb{A}^n$ es un espacio homogéneo principal de $\mathbb{R}^n$.

Ejemplo 1.71. El grupo SO(2) también actúa sobre la esfera

$$\mathbb{S}^2 := \{ (x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1 \},$$

mediante transformaciones lineales:

$$\begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} := \begin{bmatrix} x\cos\theta - y\operatorname{sen}\theta \\ x\operatorname{sen}\theta + y\cos\theta \\ z \end{bmatrix}.$$

Esta acción no es transitiva: la órbita del punto (x_0, y_0, z_0) es el círculo horizontal (o "línea de latitud") $\mathbb{S}^2 \cap \{z = z_0\}$, si $-1 < z_0 < 1$. Los polos norte $(0, 0, 1)$ y sur $(0, 0, -1)$ son **puntos fijos** para la acción, es decir, son órbitas con un solo elemento (cada uno). La existencia de puntos fijos muestra que esta acción no es libre. Sin embargo, la acción sí es eficaz: la única rotación alrededor del eje z que deja fija toda la esfera es la identidad. ◊

Ejemplo 1.72. Si $H \leqslant G$, el subgrupo H actúa sobre G por multiplicación, $h \cdot g := hg$. Las órbitas de esta acción son los coclases a derecha Hg.

Hay otra acción de H sobre G dada por $h \triangleright g := gh^{-1}$. Nótese que

$$h \triangleright (k \triangleright g) = gk^{-1}h^{-1} = g(hk)^{-1} = (hk) \triangleright g,$$

así que esta es una acción a la izquierda. Las órbitas de esta segunda acción son los coclases a izquierda gH. ◊

Ejemplo 1.73. Un grupo G actúa sobre sí mismo *por conjugación*:

$$g \cdot x := gxg^{-1} \quad \text{para} \quad g, x \in G.$$

Las órbitas bajo esta acción son precisamente las *clases conjugadas* de G. Todos los elementos del centro $Z(G)$ son puntos fijos bajo conjugación. El subgrupo de isotropía de cualquier $x \in G$ es su centralizador $Z_G(x)$: véase la Definición 1.78 más adelante. ◊

Ejemplo 1.74. Un grupo G también actúa por conjugación sobre el conjunto de todos sus subgrupos, $X := \{ H : H \leqslant G \}$. Esta acción está dada por la fórmula $g \cdot H := gHg^{-1}$.

La órbita de H bajo esta acción es la familia de subgrupos conjugados a H. Una subgrupo H es un punto fijo si y sólo si $H \trianglelefteq G$.

El subgrupo de isotropía de H en este caso es el **normalizador** de H, definido como

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

Obsérvese que $N_G(H) \leqslant G$ es un subgrupo de G, no necesariamente normal, pero H es un subgrupo normal de él: $H \trianglelefteq N_G(H)$.

Para este ejemplo, la Proposición 1.67 tiene un corolario interesante: *el número de subgrupos de G que son conjugados de H es igual al índice* $[G : N_G(H)]$. ◊

Definición 1.75. Dos acciones de un mismo grupo G sobre dos conjuntos X y Y son **acciones equivalentes** si existe una biyección $\sigma : X \to Y$ que *entrelaza* las acciones:

$$\sigma(g \cdot x) = g \triangleright \sigma(x) \quad \text{para todo} \quad g \in G,\ x \in X.$$

Esta biyección entrelazante σ, si existe, se llama una *equivalencia* entre las dos acciones de G. También se dice que σ es una *biyección G-equivariante*. ◊

Por ejemplo, la biyección $h \mapsto h^{-1}$ de G en sí mismo (que es un homomorfismo sólo si G es abeliano) es una equivalencia entre la acción de G por traslaciones a la izquierda, $g \cdot h := gh$; y su acción por traslaciones a la derecha, $g \triangleright h := hg^{-1}$.

► A veces conviene considerar una variante de la Definición 1.63, en donde el grupo actúa *a la derecha*.

Definición 1.76. Una **acción a la derecha** de un grupo G sobre un conjunto X es una función $\Psi : X \times G \to X$ tal que:

(i) $\Psi(\Psi(x,h),g) = \Psi(x,hg)$ para todo $g,h \in G$, $x \in X$;

(ii) $\Psi(x,1) = x$ para todo $x \in X$. ◊

Con las notaciones $\psi_g(x) := \underline{x \triangleleft g} := \Psi(x,g)$, las propiedades de una acción a la derecha son:

$$(x \triangleleft h) \triangleleft g = x \triangleleft (hg), \qquad x \triangleleft 1 = x,$$

o bien $\psi_g \circ \psi_h = \psi_{hg}$, $\psi_1 = 1_X$. En este caso, la correspondencia $g \mapsto \psi_g$ es un homomorfismo de G en el grupo S_X° de permutaciones del conjunto X con el *producto opuesto*: $\sigma * \tau := \tau \circ \sigma$. ◊

Por ejemplo, cada grupo G tiene una *acción regular a la derecha* sobre sí mismo,[18] dada por el producto del grupo, $h \triangleleft g := hg$. Otro ejemplo es la acción a la derecha de G sobre G por conjugación, $x \triangleleft g := g^{-1} x\, g$.

Los conceptos de órbita $x \triangleleft G$; de grupo de isotropía; de acciones eficaz o libre; son completamente análogas al caso de acciones a la izquierda.

[18] Esto no debe confundirse con la receta $g \triangleright h := hg^{-1}$, la cual es una acción a la izquierda!

1.6 El teorema de Sylow

Según el teorema de Lagrange, el orden de un grupo finito G es divisible por el orden de cualquiera de sus subgrupos. Por tanto, la factorización prima $|G| = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ proporciona bastante información sobre la estructura del grupo G y su juego de subgrupos. (Esta información no es completa, porque puede haber varios grupos no isomorfos con el mismo orden.) El detalle de la disposición de los subgrupos fue clarificado por Sylow al analizar el caso de subgrupos cuyos órdenes son potencias de un solo número primo.[19]

Definición 1.77. Sea p un número primo. Un grupo finito G es un ***p*-grupo** si su orden es una potencia de p, es decir, $|G| = p^k$ para algún k. ◊

Definición 1.78. Si G es un grupo y si $x \in G$, el **centralizador** de x es el subgrupo

$$Z_G(x) := \{\, g \in G : gx = xg \,\} = \{\, g \in G : gxg^{-1} = x \,\}.$$

Fíjese que $Z_G(x) = G$ si y sólo si el elemento x es central, es decir, $x \in Z(G)$. Por el Ejemplo 1.73, $Z_G(x)$ es el subgrupo de isotropía de x bajo la acción por conjugación $g \cdot y := gyg^{-1}$. Al contar las cardinalidades de todas las órbitas, a la luz de la Proposición 1.67, se obtiene la **ecuación de clase** para el grupo G:

$$|G| = |Z(G)| + \sum_{x \in J} [G : Z_G(x)], \tag{1.10}$$

donde $J \subset G$ contiene exactamente un representante de cada clase de conjugación con más de un elemento. ◊

Proposición 1.79. *Si G es un p-grupo, su centro no es trivial: $Z(G) \neq \mathbf{1}$.*

Demostración. En la ecuación de clase (1.10), los índices $[G : Z_G(x)]$ para elementos no centrales son divisores no triviales de $|G|$. Luego p divide cada $[G : Z_G(x)]$ al lado derecho de (1.10). Entonces p también divide $|Z(G)|$, lo cual implica $|Z(G)| > 1$. □

El resultado siguiente, descubierto por Cauchy, es un caso especial de la primera parte del teorema de Sylow. Sin embargo, dado su interés propio, vale la pena dar una demostración directa.

Proposición 1.80 (Cauchy)**.** *Si p es un número primo que divide el orden de un grupo finito G, entonces G posee un elemento de período p.*

[19] Ludvig Sylow fue un matemático noruego cuya fama se debe a un solo artículo, en donde mostró tres teoremas sobre subgrupos de un grupo finito. Algunos autores hablan de "los teoremas de Sylow", otros de "el teorema de Sylow", combinando los tres en uno. El artículo original fue: L. Sylow, *Théorèmes sur les groupes de substitutions*, Mathematische Annalen **5** (1872), 584–594.

Demostración. Se procede por inducción sobre el orden de G. En otras palabras (como el caso $|G| = 1$ es trivial), se puede suponer que la proposición es válida para cualquier grupo K con $|K| < |G|$.

Si G es abeliano y no posee subgrupo propio alguno, entonces $\langle g \rangle = G$ para cualquier $g \neq 1$, así que G debe ser cíclico de orden p y cada elemento $g \neq 1$ es un generador, de período p.

Si p divide $|H|$ donde $\mathbf{1} < H < G$, entonces por la hipótesis inductiva hay un elemento $h \in H$, $h \neq 1$, con $h^p = 1$. Este h es también un elemento de G y tiene período p.

Considérese el caso contrario: supóngase (provisionalmente) que no hay subgrupo propio alguno de G que contenga un elemento de período p. Si G es abeliano, cualquier subgrupo propio $H < G$ es un subgrupo normal; por la hipótesis inductiva, el grupo cociente G/H, cuyo orden es $|G/H| = [G\colon H] = |G|/|H|$, posee un elemento gH de período p. En tal caso, vale $g^p H = (gH)^p = H$ en G/H, así que $g^p \in H$ aunque $g \notin H$. El Corolario 1.26 muestra que $g^{p|H|} = (g^p)^{|H|} = 1$. El elemento $k := g^{|H|}$ cumple $k^p = 1$ pero $k \neq 1$ porque $g \notin H$ implica $g^{|H|} \neq 1$, otra vez por el Corolario 1.26. Entonces $k \in G$ es un elemento de período p.

En cambio, si G no es abeliano, la ecuación de clase (1.10) no es trivial: para $x \notin Z(G)$ el centralizador es un subgrupo propio, $Z_G(x) < G$. Ahora, p divide $|G|$ pero no divide $|Z_G(x)|$ por hipótesis, así que p debe dividir cada $[G\colon Z_G(x)] = |G|/|Z_G(x)|$. La ecuación (1.10) entonces implica que p divide $|Z(G)|$. Como $Z(G) < G$, se concluye que $Z(G)$ debe contener un elemento de período p, contrario al supuesto provisional. Por ende, el "caso contrario" es impermisible. □

Teorema 1.81 (Sylow)**.** *Sea G un grupo finito y sea p un primo tal que $|G| = p^r m$ donde p no divide m. Entonces:*

(a) si $s \in \{1, 2, \ldots, r\}$, hay un p-subgrupo $H \leqslant G$ tal que $|H| = p^s$;

(b) si $s < r$, hay otro subgrupo $K \leqslant G$ con $|K| = p^{s+1}$ tal que $H \subseteq K$;

(c) si P y Q son dos subgrupos con $|P| = |Q| = p^r$, hay $g \in G$ tal que $Q = gPg^{-1}$;

(d) el número de subgrupos de orden p^r es $1 + kp$ para algún $k \in \mathbb{N}$; y además divide m.

Demostración. Ad(a): Considérese la siguiente colección de partes de G:

$$\mathscr{X} := \{ S \subseteq G : |S| = p^s \}.$$

Su cardinalidad es

$$|\mathscr{X}| = \binom{p^r m}{p^s} = \frac{(p^r m)!}{(p^s)!(p^r m - p^s)!} = \frac{p^r m}{p^s} \frac{p^r m - 1}{p^s - 1} \frac{p^r m - 2}{p^s - 2} \cdots \frac{p^r m - p^s + 1}{1}.$$

El primer término de este producto de fracciones es $p^r m/p^s = p^{r-s}m$. Si $k = 1, \ldots, p^s - 1$, se puede factorizar k en la forma $k = p^t l$ con $l \perp p$. El término correspondiente del producto anterior es

$$\frac{p^r m - k}{p^s - k} = \frac{p^{r-t} m - l}{p^{s-t} - l}$$

en donde ni el numerador ni el denominador es divisible por p. Luego, después de cancelar factores comunes, la mayor potencia de p que divide $|\mathscr{X}|$ es p^{r-s}.

Ahora G actúa sobre $\mathscr{X}$ por multiplicación a la izquierda: $g \cdot S := gS$ si $S \in \mathscr{X}$. Como $\mathscr{X}$ es la unión de sus órbitas bajo esta acción y p^{r-s+1} no divide $|\mathscr{X}|$, hay al menos una órbita $\{S_1, S_2, \ldots, S_n\} = G \cdot S_1$ tal que p^{r-s+1} no divide n. Sea H el subgrupo de isotropía de S_1.

Por la Proposición 1.67, $n = [G : H]$, así que $p^r m = |G| = n|H| = p^{r-s}k|H|$ donde $k \perp p$; luego, p^s divide $|H|$. Además, si $x \in S_1$, entonces $Hx \subseteq S_1$ por la definición de H, así que $|H| = |Hx| \leqslant |S_1| = p^s$. En consecuencia, vale $|H| = p^s$.

Ad (b): Tómese $H \leqslant G$ con $|H| = p^s$ y considérese la colección de subgrupos

$$\mathscr{Y} := \{\, gHg^{-1} : g \in G \,\}.$$

G actúa transitivamente sobre $\mathscr{Y}$ por conjugación y el subgrupo de isotropía de H es su normalizador $N_G(H)$. La Proposición 1.67 ahora implica que $|\mathscr{Y}| = [G : N_G(H)]$.

Si p no divide $|\mathscr{Y}|$, entonces p^{s+1} debe dividir $|N_G(H)|$. Luego p divide el orden del grupo cociente $N_G(H)/H$ —hay que recordar que $H \trianglelefteq N_G(H)$. Por la Proposición 1.80, o bien por la parte (a) de este teorema, el grupo cociente tiene un subgrupo de orden p. Por el Teorema 1.53, este subgrupo es de la forma K/H, donde $H \leqslant K \leqslant N_G(H)$. El teorema de Lagrange muestra ahora que $|K| = |H|[K : H] = p^{s+1}$.

En cambio, si p divide $|\mathscr{Y}|$, entonces H también actúa sobre $\mathscr{Y}$ por conjugación y cada órbita de H en $\mathscr{Y}$ tiene cardinalidad que divide p^s, por la Proposición 1.67 de nuevo, y por ende es de la forma p^u con $u \in \{0, 1, \ldots, s\}$. El subgrupo H es un punto fijo de esta acción: luego $\{H\}$ es una órbita de cardinalidad $p^0 = 1$. Como $\mathscr{Y}$ es la unión disjunta de sus órbitas, hay al menos otros $(p-1)$ puntos fijos: sea L uno de ellos.

Por su construcción, se ve que $H \leqslant N_G(L)$. Luego HL es un subgrupo de G con $L \trianglelefteq HL$ por el Teorema 1.52, el cual también implica que $HL/L \simeq H/(H \cap L)$. Como $H \cap L$ es un subgrupo propio de H, p divide $[H : H \cap L] = [HL : L]$ y luego p^{s+1} divide $|HL|$, ya que $|L| = |H| = p^s$. Como $L = gHg^{-1}$ para algún g, de $L \trianglelefteq HL$ se obtiene $H \trianglelefteq g^{-1}HLg$. Para terminar, se aplica la Proposición 1.80 para extraer un subgrupo de orden p del grupo cociente $g^{-1}HLg/H$ y de nuevo el Teorema 1.53 produce un subgrupo $K \leqslant G$ con $H \leqslant K \leqslant g^{-1}HLg$ y $|K| = p^{s+1}$.

Ad (c): Tómese ahora $P \leqslant G$ con $|P| = p^r$. Considérese la colección de subgrupos

$$\mathscr{Z} := \{\, gPg^{-1} : g \in G \,\}.$$

Como antes, G actúa transitivamente sobre $\mathscr{Z}$ por conjugación y $|\mathscr{Z}| = [G : N_G(P)]$. Como $P \leqslant N_G(P)$, el teorema de Lagrange dice que p^r divide $|N_G(P)|$ y por ende p no puede dividir $|\mathscr{Z}|$.

Si $Q \leqslant G$ con $|Q| = p^r$, entonces Q también actúa sobre $\mathscr{Z}$ por conjugación; las cardinalidades de sus órbitas dividen $|Q|$ y su suma es $|\mathscr{Z}|$; luego, hay al menos una órbita $\{gPg^{-1}\}$ con un solo elemento. Repitiendo el argumento de la parte (b), esta vez con $H \mapsto Q$ y $L \mapsto gPg^{-1}$, se ve que

$$Q(gPg^{-1}) \leqslant G \quad \text{y} \quad \frac{Q(gPg^{-1})}{gPg^{-1}} \simeq \frac{Q}{Q \cap gPg^{-1}}\,.$$

Por lo tanto, $Q(gPg^{-1})$ es un p-grupo que incluye Q y gPg^{-1} como subgrupos. Por la maximalidad de $|Q| = p^r$, se concluye que $Q = Q(gPg^{-1}) = gPg^{-1}$.

Ad (d): El argumento de la parte (c) muestra que Q es el *único* punto fijo en $\mathscr{Z}$ bajo la acción de Q por conjugación; las órbitas restantes tienen cardinalidades divisibles por p. Al sumar estas cardinalidades, se ve que $|\mathscr{Z}| = 1 + kp$ para algún k. La parte (c) también implica que $|\mathscr{Z}|$ es el número de subgrupos de G de orden p^r.

Además, $|\mathscr{Z}| = [G : N_G(P)]$ divide $|G|$. □

Definición 1.82. Si G es un grupo finito de orden $p^r m$ donde p es un primo que no divide m, cada subgrupo de G de orden p^r se llama un ***p*-subgrupo de Sylow** de G. En otras palabras, un p-subgrupo de Sylow es un p-subgrupo maximal de G. ◊

El Teorema 1.81 puede reformularse como sigue: si un primo p divide $|G|$, entonces:

(i) existe al menos un p-subgrupo de Sylow $P \leqslant G$;

(ii) todos los p-subgrupos de Sylow de G son conjugados entre sí;

(iii) el número de p-subgrupos de Sylow divide $|G|$ y es $\equiv 1 \bmod p$.

En el Teorema 1.81(d), no se excluye la posibilidad de que $k = 0$: a veces ocurre que el p-subgrupo de Sylow $P \leqslant G$ es *único*. En tal caso, la parte (c) del Teorema dice que $gPg^{-1} = P$ para todo $g \in G$. En otras palabras, un p-subgrupo de Sylow único es también *normal*. (Además, *ipso facto*, no es normal si no es único.)

Definición 1.83. Un grupo G es **simple** si no posee subgrupos normales, excepto los subgrupos triviales **1** y G. ◊

Ejemplo 1.84. Un grupo de orden 12 no puede ser simple.

En efecto, un grupo G con $|G| = 12 = 2^2 \cdot 3$ posee uno o más 2-subgrupos de Sylow (de orden 4) y uno o más 3-subgrupos de Sylow (de orden 3).

Si el 3-subgrupo de Sylow no es único, el número de ellos es $1 + 3k$ y divide 4, así que hay 4 de ellos. La intersección $P \cap Q$ de dos de ellos debe ser $\mathbf{1}$ (por el teorema de Lagrange), así que su unión contiene exactamente 8 elementos de período 3. Sobran el elemento neutro y tres elementos de períodos 2 ó 4, que son suficientes para conformar exactamente un subgrupo de orden 4.

Por lo tanto, hay un único 3-subgrupo de Sylow, o bien un único 2-subgrupo de Sylow. En todo caso, G posee un subgrupo normal de orden 3 ó 4.

(Es fácil comprobar, por ejemplo, que el grupo A_4 tiene un 2-subgrupo isomorfo a V y cuatro 3-subgrupos distintos.) ◊

Ejemplo 1.85. Si P es un grupo de orden primo p, por el teorema de Lagrange no tiene subgrupos no triviales: cada elemento $g \neq 1$ es un generador, de período p; y $P \simeq C_p$.

Ahora sea G un grupo finito de orden 15. Tiene un 5-subgrupo de Sylow P y un 3-subgrupo de Sylow Q. Como $(1 + 5k)$ divide 3 sólo si $k = 0$; y además $(1 + 3l)$ divide 5 sólo si $l = 0$, estos subgrupos de Sylow son *únicos* y por tanto *normales*: $P \lhd G$ y $Q \lhd G$. Entonces $PQ = \{\, gh : g \in P,\ h \in Q \,\}$ es un subgrupo de G cuyo orden es divisible por 3 y por 5 (usando el teorema de Lagrange, porque $P \leqslant PQ$ y $Q \leqslant PQ$); por lo tanto, $PQ = G$. También se ve que $|P \cap Q| = 1$ por ser un divisor común de 3 y 5.

Si $g \in P$ y $h \in Q$, considérese el elemento $ghg^{-1}h^{-1} \in G$. Por ser P y Q subgrupos normales, se ve que

$$g(hg^{-1}h^{-1}) \in P \quad \text{mientras} \quad (ghg^{-1})h^{-1} \in Q,$$

así que $ghg^{-1}h^{-1} = 1$ o bien, lo que es lo mismo, $gh = hg$. Conclusión: $G = PQ$ donde los dos subgrupos normales P y Q *conmutan*. En tal caso, se dice que G es el **producto directo** de P y Q, escrito $G = P \times Q$.

Se ha comprobado que $G \simeq C_5 \times C_3$ si $|G| = 15$. En particular, $C_{15} \simeq C_5 \times C_3$. ◊

Ejemplo 1.86. Sea G un grupo finito de orden 6. Tiene un 3-subgrupo de Sylow P; como $(1 + 3k)$ divide 2 sólo si $k = 0$, este P es único, $P \lhd G$ con $P \simeq C_3$ y $G/P \simeq C_2$.

Sea Q un 2-subgrupo de Sylow de G; la condición "$(1 + 2l)$ divide 3" admite dos posibilidades, $l = 0$ y $l = 1$. El caso $l = 0$ sigue el patrón del ejemplo anterior: $G \simeq P \times Q \simeq C_3 \times C_2$ es un grupo abeliano. Por ejemplo, el grupo cíclico C_6 es de este tipo: si $C_6 = \langle g \rangle$, entonces $\{1, g^3\}$ es el único 2-subgrupo porque los demás elementos g, g^2, g^4, g^5 tienen períodos 3 o 6.

En el caso $l = 1$, hay tres conjugados distintos de Q (los tres 2-subgrupos de G) y por tanto G no es abeliano. Escríbase $P = \{1, a, a^2\}$ y $Q = \{1, b\}$, con $a^{-1} = a^2$. Los otros 2-subgrupos de Sylow deben ser $\{1, ab\}$ y $\{1, a^2b\}$, porque $G = \{1, a, a^2, b, ab, a^2b\}$. Ahora $ba \neq ab$ porque G no es abeliano; y es fácil comprobar que $ba \notin \{1, a, a^2, b\}$. Entonces $ba = a^2b$ necesariamente. Estas relación determina la tabla de multiplicación para G: cualquier grupo no abeliano de orden 6 debe ser isomorfo a este caso.

Para la *existencia* de un grupo no abeliano de orden 6, basta recordar que $|S_3| = 6$. La asignación $a \mapsto (123)$, $b \mapsto (12)$ da lugar a un isomorfismo $G \simeq S_3$.

Luego, hay dos grupos no isomorfos de orden 6: C_6 (abeliano) y S_3 (no abeliano). ◊

Ejemplo 1.87. El grupo alternante A_4 tiene ocho 3-ciclos, por ejemplo (123) y tres productos de transposiciones disjuntos, por ejemplo (12)(34). El cálculo

$$(123)\cdot(12)(34)\cdot(123)^{-1} = (123)\cdot(12)(34)\cdot(132) = (14)(23)$$

indica que el subgrupo R generado por (123) y (12)(34) debe incluir el subgrupo $V = \{\underline{1}, (12)(34), (13)(24), (14)(23)\}$ y el subgrupo $Q = \{\underline{1}, (123), (132)\}$. Del teorema de Lagrange se obtiene $|R| = 12$, es decir, $R = A_4$. Ahora bien, un subgrupo de A_4 de orden 6 debe de contener un elemento de período 2 y otro de período 3, por la Proposición 1.80 de Cauchy. Como cualquier par de elementos de períodos 2 y 3 generan todo el grupo, se concluye que *el grupo* A_4, de orden 12, *no incluye subgrupo alguno de orden* 6.

Este contraejemplo indica que no es posible generalizar el teorema de Sylow para obtener subgrupos cuyos órdenes son divisibles por dos primos distintos. ◊

Ejemplo 1.88. Sea $G = \mathrm{GL}(n, p) \equiv \mathrm{GL}(n, \mathbb{F}_p)$, el grupo de matrices invertibles con entradas en el cuerpo finito $\mathbb{F}_p$. Las columnas de una matriz $A \in \mathrm{GL}(n, p)$ son vectores en el espacio vectorial $(\mathbb{F}_p)^n$ y son linealmente independientes porque el rango de A es n. Aparte de dicha independencia lineal, las columnas de A son arbitrarias. La primera columna $\mathbf{a}_1$ puede ser cualquier vector no nulo en $(\mathbb{F}_p)^n$ —recuérdese que $\{0\}$ es linealmente *dependiente* en cualquier espacio vectorial— así que hay $(p^n - 1)$ posibilidades para $\mathbf{a}_1$. La segunda columna $\mathbf{a}_2$ no debe ser proporcional a $\mathbf{a}_1$: hay $(p^n - p)$ posibilidades para $\mathbf{a}_2$. Las primeras j columnas generan un subespacio de dimensión j sobre $\mathbb{F}_p$, con p^j elementos: quedan $(p^n - p^j)$ posibilidades para $\mathbf{a}_{j+1}$. En fin, el número total de elementos de $\mathrm{GL}(n, p)$ es

$$|\mathrm{GL}(n, p)| = \prod_{j=0}^{n-1}(p^n - p^j) = p^{n(n-1)/2}\prod_{j=0}^{n-1}(p^{n-j} - 1).$$

Si P es un p-subgrupo de Sylow de $\mathrm{GL}(n, p)$, el orden de P es $p^{n(n-1)/2}$.

Sea $\mathrm{UT}(n,p) \equiv \mathrm{UT}(n,\mathbb{F}_p)$ el grupo de **matrices unitriangulares**, es decir, matrices con entradas 1 en la diagonal y 0 debajo de la diagonal: $a_{jj} = 1$, $a_{ij} = 0$ si $i > j$. Una matriz unitriangular es invertible: su determinante es 1 y su inverso, calculado por eliminación gaussiana o bien por la regla de Crámer, es también unitriangular. Luego $\mathrm{UT}(n,p)$ es un subgrupo $\mathrm{GL}(n,p)$. Evidentemente, este subgrupo *no es normal*: una conjugación $A \mapsto BAB^{-1}$ ejecuta un *cambio de base* en $\mathbb{F}_p$, que destruye la forma unitriangular de la matriz A en casi todos los casos.

Los entradas supradiagonales de una matriz unitriangular son arbitrarias, porque su invertibilidad está garantizada por las entradas 1 en la diagonal. Ahora, cada una de las $n(n-1)/2$ entradas a_{ij} con $i < j$ es un elemento de $\mathbb{F}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Esto muestra que $|\mathrm{UT}(n,p)| = p^{n(n-1)/2}$ y por ende $\mathrm{UT}(n,p)$ es un p-subgrupo de Sylow de $\mathrm{GL}(n,p)$. ◊

1.7 Productos directos y semidirectos de grupos

Definición 1.89. El **producto directo** de dos grupos H, K es su producto cartesiano $\underline{H \times K}$ con la operación de grupo "por coordenadas": $(h_1,k_1)(h_2,k_2) := (h_1h_2, k_1k_2)$.

Análogamente, se define el producto directo $H_1 \times H_2 \times \cdots \times H_m$ de varios grupos.

Hay un par de homomorfismos canónicos[20] $\pi_1 : H \times K \to H$ y $\pi_2 : H \times K \to K$ dados por $\pi_1(h,k) := h$ y $\pi_2(h,k) := k$.

Se identifican H y K con los subgrupos $\{(h,1) : h \in H\}$ y $\{(1,k) : k \in K\}$ de $H \times K$. Obsérvese que $(h,1)(1,k) = (h,k) = (1,k)(h,1)$: las copias de H y K en el producto directo conmutan. Bajo estas identificaciones, H y K son subgrupos *normales* de $H \times K$, con intersección trivial, $H \cap K = \{(1,1)\}$. ◊

Lema 1.90. *Si un grupo G posee dos subgrupos normales H y K tales que $H \cap K = \{1\}$ y $HK = G$, entonces $G \simeq H \times K$.*

Demostración. Si $g \in G$, es posible escribir $g = hk$ con $h \in H$ y $k \in K$. Si $hk = h'k'$ con $h' \in H$, $k' \in K$, entonces $h^{-1}h' = k(k')^{-1} \in H \cap K = \{1\}$, así que $h' = h$ y $k' = k$. Luego la aplicación $\varphi : G \to H \times K$ dada por $\varphi(hk) := (h,k)$ está bien definida y es biyectiva.

Ahora si $h \in H$, $k \in K$, entonces $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$ porque $K \trianglelefteq G$ y $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$ porque $H \trianglelefteq G$. Luego $hkh^{-1}k^{-1} = 1$ y por ende $hk = kh$.

Esto implica que

$$\varphi(hk\,h'k') = \varphi(hh'\,kk') = (hh', kk') = (h,k)(h',k') = \varphi(hk)\,\varphi(h'k'),$$

así que φ es el isomorfismo deseado entre G y $H \times K$. □

[20] El uso del vocablo *canónico* es informal; quiere decir que los homomorfismos π_1 y π_2 tiene el mismo formato para cada par de grupos dados, H y K.

Algunos autores llaman **producto directo externo** al grupo $H \times K$ de la Definición 1.89; el término **producto directo interno** hace referencia a un subgrupo HK de un grupo dado G que cumple las hipótesis del Lema 1.90. Se trata de una mera distinción de terminología, en vista del isomorfismo del Lema, pero a veces resulta útil en contextos apropiados.

Ejemplo 1.91. Sea G un grupo abeliano finito de orden $|G| = p^r q^s$ donde p, q son números primos distintos. Todos los elementos $h \in G$ de período p^k, para algún $k \leqslant r$, forman un subgrupo $H \leqslant G$. De igual manera, los elementos $k \in G$ de período q^l, para algún $l \leqslant s$, forman otro subgrupo $K \leqslant G$; y es evidente que $H \cap K = \{1\}$. Por ser G abeliano, estos dos subgrupos son automáticamente normales en G.

La conmutatividad de G también implica que $(hk)^m = h^m k^m$ para todo $m \in \mathbb{N}$. Luego, el período del elemento hk es el mínimo común múltiplo de los períodos de h y k. Si un elemento $g \in G$ tiene período $p^k q^l$ —este período es necesariamente un divisor de $|G|$— hay enteros $a, b \in \mathbb{Z}$ con $ap^{r-k} + bq^{s-l} = 1$. Colóquese $h := g^{bq^{s-l}}$ y $k := g^{ap^{r-k}}$; entonces $h \in H$, $k \in K$ y $g = hk$, comprobando así que $G = HK$. El Lema 1.90 entonces muestra que $G \simeq H \times K$.

En particular, $C_{15} \simeq C_5 \times C_3$, como ya se ha observado. ◊

Ejemplo 1.92. Hay tres grupos abelianos no isomorfos de orden 8. Ellos son C_8, $C_4 \times C_2$ y $C_2 \times C_2 \times C_2$. Estos grupos se distinguen por los períodos de sus elementos: C_8 tiene 4 elementos de período 8, sus generadores; $C_4 \times C_2$ tiene 4 elementos de período 4 pero ninguno de período 8; y $C_2 \times C_2 \times C_2$ tiene 7 elementos de período 2.

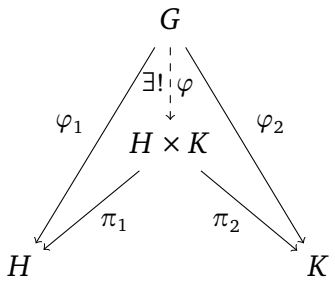
El **exponente** de un grupo finito es el mínimo común múltiplo de los órdenes de sus elementos; dos grupos con exponentes diferentes no pueden ser isomorfos. Para los grupos mencionados: C_8 tiene exponente 8; $C_4 \times C_2$ tiene exponente 4; y $C_2 \times C_2 \times C_2$ tiene exponente 2. ◊

Lema 1.93. *Sea G un grupo cualquiera y sean $\varphi_1 : G \to H$ y $\varphi_2 : G \to K$ dos homomorfismos. Entonces existe un único homomorfismo $\varphi : G \to H \times K$ tal que $\pi_1 \circ \varphi = \varphi_1$ $\pi_2 \circ \varphi = \varphi_2$.*

Demostración. Defínase $\varphi : G \to H \times K$ por $\varphi(g) := (\varphi_1(g), \varphi_2(g))$. Es evidente que φ es un homomorfismo y que $\pi_1 \circ \varphi = \varphi_1$ y $\pi_2 \circ \varphi = \varphi_2$. la unicidad también está clara. □

El resultado del Lema 1.93 es un ejemplo de una **propiedad universal** del producto directo. En el siguiente diagrama conmutativo, la flecha quebrada con la etiqueta $\exists!\, \varphi$

indica *la existencia de un único homomorfismo φ que hace conmutar el diagrama*:



(1.11)

(El triángulo a la izquierda conmuta si $\pi_1 \circ \varphi = \varphi_1$; el triángulo a la derecha conmuta si $\pi_2 \circ \varphi = \varphi_2$.) Dicho de otro modo: entre todos los diagramas de la forma $H \xleftarrow{\varphi_1} G \xrightarrow{\varphi_2} K$, el diagrama especial $H \xleftarrow{\pi_1} H \times K \xrightarrow{\pi_2} K$ es *universal* por ser una imagen homomórfica del primero.

► Cuando se trata de dos *grupos abelianos* A y B con notación aditiva, en vez de *producto* directo $A \times B$ a veces se habla de la **suma directa** $\underline{A \oplus B}$, cuya operación de grupo se denota por $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$. Así, por ejemplo, los tres grupos abelianos del Ejemplo 1.92 se denotan por $\mathbb{Z}_8$; $\mathbb{Z}_4 \oplus \mathbb{Z}_2$; y $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

► El producto directo de dos grupos abelianos es también un grupo abeliano. Hay una variante de esta construcción que es capaz de combinar dos grupos abelianos de tal manera que el resultado sea (muchas veces, aunque no siempre) un grupo no abeliano. De este modo se produce una buena cantidad de ejemplos de grupos no abelianos.

Definición 1.94. Sean dados dos grupos H y K y un homomorfismo $\alpha\colon K \to \mathrm{Aut}(H)$. Entonces K actúa sobre H por automorfismos de H, al definir $k \cdot h := \alpha_k(h)$. El **producto semidirecto** de H por K mediante α es el producto *cartesiano* de los *conjuntos* H y K, dotado de la siguiente operación binaria:

$$(h, k)\,(h', k') := (h\,\alpha_k(h'),\, kk'). \tag{1.12}$$

Esta operación es asociativa porque α es un homomorfismo:

$$\begin{aligned}\big((h, k)\,(h', k')\big)(h'', k'') &= (h\,\alpha_k(h')\,\alpha_{kk'}(h''),\, kk'k'') = (h\,\alpha_k(h'\,\alpha_{k'}(h'')),\, kk'k'') \\ &= (h, k)\,(h'\,\alpha_{k'}(h''),\, k'k'') = (h, k)\big((h', k')\,(h'', k'')\big).\end{aligned}$$

Con el elemento neutro $(1, 1)$ y la inversión dada por $(h, k)^{-1} = (\alpha_{k^{-1}}(h^{-1}),\, k^{-1})$, esta operación binaria es una ley de grupo. Denótese el grupo así formado por $\underline{H \rtimes_\alpha K}$.

Como en el caso de productos directos, se identifican $H \leftrightarrow \{(h,1) : h \in H\}$ y $K \leftrightarrow \{(1,k) : k \in K\}$. Nótese que $(h,1)(1,k) = (h,k)$ pero $(1,k)(h,1) = (\alpha_k(h),k)$, así que *estos subgrupos no conmutan* salvo si la acción de K sobre H es la acción trivial —en cuyo caso se obtiene el producto directo $H \times K$. ◊

Fíjese también que $(1,k)(h,1)(1,k)^{-1} = (\alpha_k(h),k)(1,k^{-1}) = (\alpha_k(h),1)$. Esto muestra que H *es un subgrupo normal* de $H \rtimes_\alpha K$.

Proposición 1.95. *Si un grupo G contiene dos subgrupos N y K tales que $N \trianglelefteq G$, $NK = G$ y $N \cap K = \mathbf{1}$, la conjugación $\alpha_k(h) := khk^{-1}$ define un homomorfismo $\alpha\colon K \to \mathrm{Aut}(N)$; además, hay un isomorfismo $G \simeq N \rtimes_\alpha K$.*

Demostración. La normalidad del subgrupo N implica que $knk^{-1} \in N$ para todo $k \in K$ y está claro que $\alpha_k\colon n \mapsto knk^{-1}$ es un automorfismo de N. También, se ve que la fórmula $\alpha_k(\alpha_{k'}(n)) = kk'nk'^{-1}k^{-1}$ dice que $k \mapsto \alpha_k$ es un *homomorfismo* de K en $\mathrm{Aut}(N)$.

Defínase $\theta : N \rtimes_\alpha K \to G$ por $\theta(n,k) := nk$; entonces

$$\theta(n,k)\theta(n',k') = nk\,n'k' = n(kn'k^{-1})\,kk' = n\alpha_k(n')\,kk' = \theta((n,k)(n',k')),$$

así que θ es un homomorfismo. La condición $G = NK$ muestra que θ es sobreyectivo. Su núcleo es

$$\{(n,k) : nk = 1\} = \{(n,k) : n,k \in N \cap K\} = \{(1,1)\}$$

en vista de la condición $N \cap K = \mathbf{1}$. Entonces θ es un isomorfismo entre $N \rtimes_\alpha K$ y G. □

De nuevo, dícese a veces que un grupo G que cumple las hipótesis de la Proposición 1.95 es un "producto semidirecto interno" de sus subgrupos N y K.

Ejemplo 1.96. El grupo cíclico $C_3 = \{1,a,a^2\}$, con $a^3 = 1$, posee dos automorfismos, la identidad $\underline{1} = 1_{C_3}$ y la transposición $\sigma\colon a \leftrightarrow a^2$. ⟦ Esta σ es un automorfismo de C_3 porque $(a^2)^2 = a$. ⟧ Está claro que $\sigma^2 = \underline{1}$, así que $\mathrm{Aut}(C_3) = \{\underline{1},\sigma\} \simeq C_2$. Por lo tanto, hay dos maneras de formar un producto de C_3 por C_2: si $C_2 = \{1,b\}$, es obligatorio que $\alpha_1 = \underline{1}$ en $\mathrm{Aut}(C_3)$; pero se puede tomar $\alpha_b = \underline{1}$ también, o bien $\alpha_b = \sigma$.

En el caso $\alpha_b = \underline{1}$, el homomorfismo $\alpha\colon C_2 \to \mathrm{Aut}(C_3)$ es trivial y el producto semidirecto dado por (1.12) coincide con el producto *directo* $C_3 \times C_2$, el cual también es isomorfo a C_6 en vista del Ejemplo 1.91.

En el otro caso $\alpha_b = \sigma$, el producto semidirecto $C_3 \rtimes_\alpha C_2$ es un grupo *no abeliano* de orden 6. Por ejemplo, se ve que

$$(1,b)(a,1) = (\sigma(a),b) = (a^2,b) \quad \text{mientras} \quad (a,1)(1,b) = (a,b).$$

La Proposición 1.95 muestra que $C_3 \rtimes_\alpha C_2 \simeq S_3$. En efecto, los subgrupos $N := \langle(123)\rangle$ y $K = \langle(12)\rangle$ de S_3 cumplen las hipótesis de esa Proposición: $N \trianglelefteq S_3$ porque $[S_3 : N] = 2$, $NK = S_3$ y $N \cap K = \mathbf{1}$; y está claro que $N \simeq C_3$ y $K \simeq C_2$. ◊

Definición 1.97. Una sucesión de dos homomorfismos

$$H \xrightarrow{\varphi} G \xrightarrow{\psi} K$$

se llama **exacta** (o "exacta en G") si $\operatorname{im}\varphi = \ker\psi$, es decir, si la composición $\psi \circ \varphi$ es el homomorfismo trivial $H \to K$. Una sucesión de dos o más homomorfismos

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} G_{n+1}$$

es una **sucesión exacta** si es exacta en cada grupo intermedio, es decir, si $\operatorname{im}\varphi_j = \ker\varphi_{j+1}$ para $j = 1, 2, \ldots, n-1$.

Un caso de particular importancia es una **sucesión exacta corta**:

$$\mathbf{1} \longrightarrow H \xrightarrow{\varphi} G \xrightarrow{\psi} K \longrightarrow \mathbf{1}, \tag{1.13}$$

donde las homomorfismos inicial y final son triviales; la exactitud en H dice que φ *es inyectivo*; la exactitud en K dice que ψ *es sobreyectivo*; y también $\operatorname{im}\varphi = \ker\psi$ debido a la exactitud en G. Fíjese que la imagen $\varphi(H)$ es un *subgrupo normal* de G, por ser el núcleo de ψ. Por otro lado, si $N \trianglelefteq G$, la inclusión $\iota : N \to G$ y la aplicación cociente $\eta : G \to G/N$ forman una sucesión exacta corta,

$$\mathbf{1} \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\eta} G/N \longrightarrow \mathbf{1}.$$ ◊

Definición 1.98. Si H y K son dos grupos cualesquiera, una **extensión de** H **por** K es un grupo G que tiene un subgrupo normal N tal que $N \simeq H$ y $G/N \simeq K$. Esta condición es equivalente a la existencia de una sucesión exacta corta (1.13) en donde $H = \ker\varphi$.

Dícese que dos extensiones G y L de H por K son *equivalentes* si y sólo si hay un isomorfismo $\theta : G \to L$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccccccccc}
\mathbf{1} & \longrightarrow & H & \xrightarrow{\varphi} & G & \xrightarrow{\psi} & K & \longrightarrow & \mathbf{1} \\
 & & \downarrow{\scriptstyle 1_H} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle 1_K} & & \\
\mathbf{1} & \longrightarrow & H & \xrightarrow{\varphi'} & L & \xrightarrow{\psi'} & K & \longrightarrow & \mathbf{1}\,.
\end{array}$$

Cada par de grupos H y K posee al menos una extensión, a saber, el producto directo $G = H \times K$, al tomar $\varphi(h) := (h, 1)$ y $\psi(h, k) := k$. ◊

Proposición 1.99. *Un producto semidirecto $H \rtimes_\alpha K$ es una extensión de H por K. Una extensión G de H por K, dada por* (1.13)*, es equivalente a un producto semidirecto si y sólo si hay un homomorfismo $\beta : K \to G$ tal que $\psi \circ \beta = 1_K$.*

Demostración. Defínase $\varphi : H \to H \rtimes_\alpha K$ por $\varphi(h) := (h, 1)$ y $\psi : H \rtimes_\alpha K \to K$ por $\psi(h,k) := k$. Ya se ha observado que $\varphi(H) \trianglelefteq H \rtimes_\alpha K$ y está claro que $(H \rtimes_\alpha K)/\varphi(H) \simeq K$.

Defínase $\tilde{\beta} : K \to H \rtimes_\alpha K$ por $\tilde{\beta}(k) := (1, k)$; entonces $\psi(\tilde{\beta}(k)) = k$ para todo $k \in K$.

Por otro lado, si G es una extensión de H por K y si $\beta : K \to G$ es un homomorfismo tal que $\psi \circ \beta = 1_K$, sea $\alpha_k(h) := \beta(k) h \beta(k)^{-1}$. La condición $\psi \circ \beta = 1_K$ obliga que β sea inyectivo; luego $k \mapsto \alpha_k$ es un homomorfismo bien definido de K en $\mathrm{Aut}(H)$. La receta $\theta(h,k) := h\beta(k)$ define una aplicación $\theta : H \rtimes_\alpha K \to G$ y es fácil verificar que este es un *homomorfismo*. Ahora

$$(h,k) \in \ker\theta \implies h^{-1} = \beta(k) \implies k = \psi(h^{-1}) = 1 \implies h = \beta(k^{-1}) = 1,$$

así que θ es inyectivo. Si ahora $g \in G$, colóquese $k := \psi(g)$; entonces $g\beta(k)^{-1} \in \ker\psi$, así que hay $h \in H$ con $h = g\beta(k)^{-1}$, luego $g = h\beta(k)$: por tanto, θ es sobreyectiva. El isomorfismo θ da la equivalencia de las dos extensiones G y $H \rtimes_\alpha K$. □

En la situación descrita en la Proposición anterior, dícese que la sucesión exacta corta (1.13) **escinde**. Se usa el diagrama

$$\mathbf{1} \longrightarrow H \xrightarrow{\varphi} G \underset{\beta}{\overset{\psi}{\rightleftarrows}} K \longrightarrow \mathbf{1}$$

para denotar la *escisión* de la sucesión por el homomorfismo β.

Ejemplo 1.100. Hay dos extensiones evidentes de C_2 por C_2:

$$\mathbf{1} \longrightarrow C_2 \xrightarrow{\varphi} C_2 \times C_2 \xrightarrow{\psi} C_2 \longrightarrow \mathbf{1} \quad \text{y} \quad \mathbf{1} \longrightarrow C_2 \xrightarrow{\varphi} C_4 \xrightarrow{\psi} C_2 \longrightarrow \mathbf{1}.$$

Como $\mathrm{Aut}(C_2) = \mathbf{1}$, el único producto semidirecto de C_2 por C_2 es el producto directo $C_2 \times C_2$. Como $C_4 \not\simeq C_2 \times C_2$, la Proposición 1.99 muestra que la segunda sucesión exacta corta *no escinde*. ⟦ El único homomorfismo no trivial de $C_2 = \{1, b\}$ en $C_4 = \{1, a, a^2, a^3\}$ está dada por $\beta(b) := a^2$. Pero también $\psi(a) = b$ como única posibilidad, así que $\psi(\beta(b)) = \psi(a^2) = b^2 = 1$, de modo que $\psi \circ \beta \neq 1_K$. ⟧ ◊

1.8 Grupos simples y grupos resolubles

Definición 1.101. Un grupo finito G es **simple** si los únicos subgrupos normales de G son los subgrupos triviales $\mathbf{1}$ y G. ◊

Ejemplo 1.102. Aparte del grupo trivial $\mathbf{1} = \{1\}$, los únicos *grupos abelianos simples* son *los grupos cíclicos* C_p donde p es un número primo. En un grupo abeliano, cada subgrupo es trivialmente normal: un grupo abeliano simple no posee subgrupos no triviales. La Proposición 1.80, de Cauchy, entonces demuestra que su orden es un primo p, en cuyo caso el grupo es isomorfo a C_p. ◊

La identificación y catalogación de los grupos simples no abelianos fue un trabajo de varias décadas, culminando alrededor de 1985 con un consenso de que el catálogo ya estaba completo, aunque la última pieza tuvo que esperar hasta el 2004.[21] Hay varias familias infinitas, entre ellas los grupos alternantes A_n para $n \geqslant 5$; grupos "de tipo de Lie clásicos", del cual el más pequeño es PSL$(2,7)$, de orden 168; y grupos "de tipo de Lie excepcionales". Además, hay unos 26 *grupos esporádicos*, desde el grupo de Mathieu M_{11}, de orden 7920, descubierto en 1861; hasta el grupo de Janko J_4, de orden $86,775,570,046,077,562,880$, descubierto en 1976. El más grande de los grupos esporádicos es el *Monstruo* M, de Fischer y Griess, descubierto en 1973, cuyo orden es

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \sim 8 \times 10^{53} \quad ☺$$

Definición 1.103. Un grupo G es **resoluble** si hay una *torre* finita de subgrupos de G,

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = \mathbf{1} \tag{1.14}$$

tal que $G_j \lhd G_{j-1}$ y cada G_{j-1}/G_j es *abeliano*. (En otras palabras, G es resoluble si puede ser construido por una cantidad finita de extensiones por grupos abelianos.)

Dícese que G es **nilpotente** si además $G_{j-1}/G_j \leqslant Z(G/G_j)$ para todo j. ◊

Algunos autores dicen *serie descendiente* en vez de *torre* para describir el patrón del despliegue (1.14).

Un grupo abeliano es (trivialmente) resoluble. Un grupo simple no abeliano no es resoluble, porque la única torre posible es $G \rhd \mathbf{1}$, cuyo cociente $G/\mathbf{1} = G$ no es abeliano.

[21] El teorema de la clasificación, aunque fácil de enunciar ("Los grupos simples no abelianos son los siguientes: ...") tuvo una demostración repartida en decenas de artículos de investigación. Véase el ensayo descriptivo: Daniel Gorenstein, *The Enormous Theorem*, Scientific American **253** (1985), 104–115. Todavía hay un equipo trabajando en la publicación de una versión simplificada, en varios tomos, cuya longitud total se estima en más de 5000 páginas.

Una torre de tipo (1.14) en donde cada cociente G_{j-1}/G_j es *simple* se llama una **serie de composición** para G. Por ejemplo,

$$C_8 \rhd C_4 \rhd C_2 \rhd \mathbf{1}$$

es una serie de composición para C_8. Por inducción sobre el orden de G, cualquier grupo finito posee una serie de composición; pero el ejemplo $C_4 \times C_2$ indica, puede poseer más de una. Sin embargo, un *teorema de Jordan y Hölder* (no demostrado aquí)[22] dice que dos series de composición para un grupo finito (a) poseen el mismo número de inclusiones estrictas (la *longitud* m de la torre); y (b) poseen los mismos cocientes G_{j-1}/G_j, posiblemente permutados.

Definición 1.104. El **conmutador** de dos elementos $g, h \in G$ es el elemento $ghg^{-1}h^{-1}$. Sea G' el subgrupo de G generado por todos los conmutadores de elementos de G. (Nótese que $G' = \mathbf{1}$ si y sólo si G es abeliano.)

Sea $G'' := (G')'$, $G''' := (G'')'$, etcétera. La **serie derivada** del grupo G es la torre

$$G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq G''' \trianglerighteq \cdots$$

cuyas inclusiones son normales pero no necesariamente estrictas. Por ejemplo, si G es simple y no abeliano, entonces $G = G' = G'' = \cdots$ y la serie queda estancada. ◊

Ejemplo 1.105. Cualquier conmutador en el grupo S_n es una permutación par, así que $S_n' \leqslant A_n$. Para $n = 3$, los 3-ciclos (123) y (132) son conmutadores, usando los cálculos del Ejemplo 1.30; luego, $S_3' = A_3 \simeq C_3$. Además, $S_3'' = C_3' = \mathbf{1}$ porque C_3 es abeliano. La serie derivada de S_3 es entonces $S_3 \rhd C_3 \rhd \mathbf{1}$. El grupo S_3 es resoluble.

En el grupo A_4, algunos conmutadores son

$$(123)\,(124)\,(132)\,(142) = (13)(24)\,(14)(23) = (12)(34),$$
$$(123)\,(12)(34)\,(132)\,(12)(34) = (134)\,(234) = (13)(24),$$

y (por sustituciones de dígitos) se concluye que $A_4' = V$, un subgrupo abeliano. Además, de los cálculos típicos en S_4:

$$(12)\,(23)\,(12)\,(23) = (123)^2 = (132),$$
$$(1234)\,(1243)\,(1432)\,(1342) = (132)\,(124) = (243),$$
$$(1234)\,(123)\,(1432)\,(132) = (1324)\,(1243) = (142),$$
$$(1234)\,(12)(34)\,(1432)\,(12)(34) = (13)(24),$$

[22] La demostración, por inducción sobre m, no es difícil: véase cualquier texto general de álgebra, como por ejemplos los libros recomendados de Aluffi, Jacobson o Lang.

se obtiene $S_4' = A_4$. Entonces la serie derivada de S_4 es

$$S_4 \rhd A_4 \rhd V \rhd \mathbf{1}.$$

Los cocientes sucesivos son C_2, C_3, V, todos abelianos: el grupo S_4 es resoluble. ◊

Proposición 1.106. *Un grupo G es resoluble si y sólo si su serie derivada es una torre finita que termina con* $\mathbf{1}$.

Demostración. La conjugación $g \mapsto kgk^{-1}$ conserva conmutadores, porque

$$k(ghg^{-1}h^{-1})k^{-1} = kgk^{-1}\,khk^{-1}\,kg^{-1}k^{-1}\,kh^{-1}k^{-1} = kgk^{-1}\,khk^{-1}\,(kgk^{-1})^{-1}\,(khk^{-1})^{-1}.$$

Luego G' es siempre un subgrupo normal de G.

El homomorfismo cociente $\eta\colon G \to G/G'$ satisface

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

y el lado derecho es el elemento neutro de G/G'. Esto dice que todos los conmutadores en G/G' son triviales, así que G/G' es abeliano. Luego G es resoluble si la serie derivada termina en un número finito de pasos.

Por el contrario, si G es resoluble, hay una torre (1.14) de subgrupos de G con cocientes abelianos. Por ser G/G_1 abeliano, la aplicación cociente $G \to G/G_1$ lleva cada conmutador al elemento neutro, así todos los conmutadores quedan en G_1; esto dice que $G' \leqslant G_1$. Por inducción, se demuestra que $G'' \leqslant G_2$, $G''' \leqslant G_3$, etc., ya que los grupos cocientes G_1/G_2, G_2/G_3, etc., son abelianos. Después de m pasos de este proceso, la m-ésima subgrupo derivado cumple $G^{(m)} \leqslant G_m = \mathbf{1}$. □

1.9 Generadores y relaciones para un grupo

Cualquier grupo finito admite una *presentación por generadores y relaciones*. Dicha presentación consiste en dar una lista de generadores $a_1, a_2, \ldots, a_r$ y una lista de relaciones entre ellas. Por ejemplo, si el grupo es abeliano las relaciones incluyen las reglas $a_j a_k = a_k a_j$ al menos; el grupo cíclico C_m posee un solo generador a y cumple la sola relación $a^m = 1$. Ahora se pretende mostrar que los grupos finitos —y buena cantidad de grupos infinitos— están determinados hasta isomorfismo por esta clase de presentación.

Definición 1.107. Sea $X = \{x_1, x_2, \ldots, x_r\}$ un conjunto finito y sea $X' = \{x_1', x_2', \ldots, x_r'\}$ otro conjunto de igual cardinalidad, con $X \cap X' = \emptyset$. Sea Y la totalidad de **palabras** en el **alfabeto** $X \uplus X'$, es decir, sucesiones finitas de elementos de $X \uplus X'$. (El conjunto Y

contiene una *palabra vacía*, con cero "letras", denotado por 1.) Dos palabras se declaran equivalentes si se obtiene una de la otra mediante número finito de inserciones o extracciones de uno de los pares $x_j x_j'$ ó $x_k' x_k$; denótase por $F_r := Y/\sim$ el conjunto cociente bajo esa relación de equivalencia.

Defínase una operación de grupo en F_r por yuxtaposición:

$$(y_1 y_2 \dots y_m)(z_1 z_2 \dots z_n) := y_1 y_2 \dots y_m z_1 z_2 \dots z_n,$$

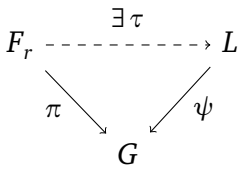
en donde los y_k y z_l son elementos de $X \uplus X'$; al lado derecho se eliminan pares $x_j x_j'$ ó $x_k' x_k$ que aparecen al yuxtaponer las dos palabras originales. Por ejemplo,

$$(x_1 x_2' x_1)(x_1' x_2 x_3' x_1) = x_1 x_2' \not{x}_1 \not{x}_1' x_2 x_3' x_1 = x_1 \not{x}_2' \not{x}_2 x_3' x_1 = x_1 x_3' x_1.$$

La asociatividad de esta operación está clara; el elemento neutro es la palabra vacía 1. El inverso de $y_1 y_2 \dots y_m$ es $y_m' \dots y_2' y_1'$, con el convenio de que $(x_j')' = x_j$. Por ejemplo, $(x_1 x_2' x_1 x_3')^{-1} = x_3 x_1' x_2 x_1'$. El grupo F_r así definido está generado por X: este es el **grupo libre con r generadores**. ◊

Cualquier grupo finitamente generado G es un cociente de un grupo libre; y además, cuando G es un cociente de otro grupo L, hay un homomorfismo del grupo libre en L que respeta los cocientes. Este es contenido de la proposición siguiente.

Proposición 1.108. *Si $G = \langle a_1, a_2, \dots, a_r \rangle$ es un grupo generado por r elementos, hay un único homomorfismo sobreyectivo $\pi\colon F_r \to G$ tal que $\pi(x_j) = a_j$ y $\pi(x_k') = a_k^{-1}$ para $j, k = 1, \dots, r$.*



Además, si L es otro un grupo y si $\psi\colon L \to G$ es un homomorfismo sobreyectivo, entonces hay un homomorfismo $\tau\colon F_r \to L$ tal que $\psi \circ \tau = \pi$.

Demostración. El homomorfismo π, definido sobre generadores por $\pi(x_j) := a_j$, obedece $\pi(x_k') = \pi(x_k)^{-1} = a_k^{-1}$ por ser homomorfismo. La unicidad está clara, porque la imagen de cada palabra $y_1 y_2 \dots y_m \in F_r$ está dada por $\pi(y_1 y_2 \dots y_m) = h_1 h_2 \dots h_m$, en donde $h_i := a_j$ si $y_i = x_j$, $h_i := a_k^{-1}$ si $y_i = x_k'$. Sólo hay que notar que π está bien definida porque $\pi(x_j x_j') = a_j a_j^{-1} = 1$ y $\pi(x_k' x_k) = a_k^{-1} a_k = 1$.

Tómese $b_j \in L$ tal que $\psi(b_j) = a_j$, ya que ψ es sobreyectivo. Sea $\tau\colon F_r \to L$ el homomorfismo determinado, como en el párrafo anterior, por $\tau(x_j) = b_j$ y $\tau(x_k') = b_k^{-1}$.

La igualdad $\psi(\tau(y)) = \pi(y)$, dada inicialmente para $y \in X$, sigue siendo válida para todo $y \in F_r$ porque $F_r = \langle X \rangle$; esto dice que $\psi \circ \tau = \pi$. □

Como $\pi\colon F_r \to G$ es sobreyectivo, el primer teorema de isomorfía (Teorema 1.50) muestra que $G \simeq F_r/\ker\pi$. Si el subgrupo $\ker\pi \trianglelefteq F_r$ es a su vez finitamente generado, es decir, $\ker\pi = \langle R \rangle$ donde R es un conjunto finito de palabras en F_r, dícese que el grupo G está **finitamente presentado** y se escribe $G \simeq \langle X : R \rangle$. La presentación de un grupo no es única: puede haber varias maneras de elegir generadores tanto para G como para $\ker\pi$.

Los elementos de R se llaman **relaciones** (o más correctamente, *relatores*: una palabra $y_1 \dots y_m \in R$ es un relator; la ecuación $\pi(y_1)\dots\pi(y_m) = 1$ es la *relación* correspondiente). Una regla de conmutatividad entre generadores, $a_j a_k = a_k a_j$ puede escribirse en la forma $a_j a_k a_j^{-1} a_k^{-1} = 1$; esta regla es válida si $x_j x_k x_j' x_k' \in \ker\pi$.

Un grupo finito está finitamente presentada por su tabla de multiplicación. Si $G = \langle a_1, a_2, \dots, a_r \rangle$ y si $a_j a_k = g_{jk} \in G$, escríbase el elemento g_{jk} como un producto de los generadores y sus inversos. Hay palabras $y_{jk}' \in F_r$ tales que $\pi(y_{jk}') = g_{jk}^{-1}$; entonces $R = \{\, x_j x_k y_{jk}' : j,k = 1,\dots,m \,\}$ es un conjunto finito que genera $\ker\pi$.

Para aliviar un poco la notación a la hora de dar ejemplos concretos, en una presentación $G \simeq \langle X : R \rangle$, se escribirá la relación $a_j a_k = g_{jk}$ al lado derecho en vez del relator $x_j x_k y_{jk}'$.

Ejemplo 1.109. El *grupo abeliano libre* con r generadores es el grupo

$$\langle a_1, \dots, a_r : a_j a_k = a_k a_j \text{ para todo } i < j \rangle.$$

Como los generadores conmutan, cada elemento de este grupo puede escribirse de forma única como $a_1^{m_1} a_2^{m_2} \dots a_r^{m_r}$ con $m_1, \dots, m_r \in \mathbb{Z}$, con el convenio $a_j^{-m} \equiv (a_j^{-1})^m$. Es preferible, en este caso, emplear una notación aditiva, en cuyo caso el elemento típico del grupo se escribe en la forma

$$m_1 a_1 + m_2 a_2 + \cdots + m_r a_r, \quad \text{con} \quad m_1, \dots, m_r \in \mathbb{Z},$$

De ahí se ve que el grupo abeliano libre es isomorfo a la suma directa $\mathbb{Z}^r = \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ de r copias de $\mathbb{Z}$.

En el caso $r = 1$, el juego de relaciones es vacía y $F_1 \simeq \mathbb{Z}$ es un grupo abeliano. Sin embargo, F_r no es abeliano para $r \geqslant 2$.

Si G es un grupo abeliano finitamente generado, se puede tomar $L = \mathbb{Z}^r$ en la Proposición 1.108: un grupo abeliano con r generadores es una imagen homomórfica de $\mathbb{Z}^r$. ◊

Ejemplo 1.110. El grupo cíclico de m elementos es $C_m \simeq \langle a : a^m = 1 \rangle$. ◊

Ejemplo 1.111. El *grupo de cuatro* tiene las presentaciones

$$V \simeq \langle a, b : a^2 = b^2 = 1,\ ab = ba \rangle \simeq \langle a, b : a^2 = b^2 = (ab)^2 = 1 \rangle.$$

La primera presentación dice que V es abeliana y como tal hay un homomorfismo sobreyectivo $\psi : \mathbb{Z}^2 \to V$ con núcleo $\ker \psi = 2\mathbb{Z} \oplus 2\mathbb{Z}$, así que $V \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \simeq C_2 \times C_2$.

La segunda presentación no es obviamente abeliana; pero de la relación $abab = 1$ se deduce $ba = a^{-1}b^{-1}$ y en la presencia de las relaciones $a^2 = b^2 = 1$ esto se convierte en $ba = ab$. ◊

Ejemplo 1.112. El grupo de permutaciones S_3 tiene las presentaciones

$$S_3 \simeq \langle a, b : a^3 = b^2 = 1,\ ba = a^2 b \rangle \simeq \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle.$$

Las relación $ba = a^2 b$ en S_3 fue observada en el Ejemplo 1.96: la primera presentación describe un producto semidirecto $C_3 \rtimes_\alpha C_2$. La segunda presentación sigue como en el Ejemplo anterior. ◊

Ejemplo 1.113. El *grupo diedral* D_n tiene la presentación

$$D_n \simeq \langle a, b : a^n = b^2 = (ab)^2 = 1 \rangle.$$

Nótese que $D_2 \simeq V$ y $D_3 \simeq S_3$. ◊

Ejemplo 1.114. El **grupo de cuaterniones** $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ fue introducido para generalizar los números complejos al postular la existencia de tres raíces cuadradas independientes de (-1), esto es, $i^2 = j^2 = k^2 = -1$. Su tabla de multiplicación viene del descubrimiento por Hamilton[23] que tales raíces no pueden conmutar. En efecto, valen $jk = i = -kj$; $ki = j = -ik$; $ij = k = -ji$. Este grupo no abeliano tiene la presentación

$$Q \simeq \langle a, b : a^4 = 1,\ a^2 = b^2,\ ba = a^3 b \rangle.$$

El grupo al lado derecho tiene orden 8, porque sus elementos son de la forma $a^k b^l$ con $k = 0, 1, 2, 3$ y $l = 0, 1$. Las asignaciones $a \mapsto i$, $b \mapsto j$ definen un homomorfismo de este grupo en Q (es fácil verificar que este homomorfismo está bien definido y es sobreyectivo). Como los dos grupos tiene 8 elementos, este es un isomorfismo. ◊

[23] William Rowan Hamilton trató durante varios años de generalizar el plano $\mathbb{C} \simeq \mathbb{R}^2$ de los números complejos en algo análogo para $\mathbb{R}^3$. Al agregar un eje más, considerando $\mathbb{R}^3$ como la "parte vectorial" de $\mathbb{R}^4$, tuvo más suerte; pero la regla de multiplicación de los puntos cardinales se le escapaba. Un día (el 16 de octubre de 1843), caminando por Dublín, se le ocurrió la solución: $i^2 = j^2 = k^2 = ijk = -1$. Con un cuchillo, escribió esta fórmula en la madera del puente sobre el Canal Real donde iba caminando.

► Las presentaciones por generadores y relaciones permiten establecer listas exhaustivas de grupos finitos de ciertos órdenes, clasificándoles hasta isomorfismo. Los p-grupos, de ordenes p^k con k primo, son de difícil acceso; por ejemplo, se sabe que hay 14 grupos no isomorfos de orden 16, cinco abelianos y nueve no abelianos.[24]

Teorema 1.115. *Hasta isomorfismo, en grupos de órdenes menor que* 16 *hay:*

- ◇ ***un solo grupo*** *de cada orden* 1*,* 2*,* 3*,* 5*,* 7*,* 11*,* 13 *y* 15*;*
- ◇ ***dos grupos*** *no isomorfos de órdenes* 4*,* 6*,* 9*,* 10*,* 14*;*
- ◇ ***cinco grupos*** *no isomorfos de órdenes* 8 *y* 12*.*

Demostración. El único grupo de orden 1 es el grupo trivial **1**. Un grupo de orden primo es necesariamente cíclico, por el teorema de Lagrange. Luego, en los casos $|G| = p$ con $p \in \{2, 3, 5, 7, 11, 13\}$, hay un isomorfismo $G \simeq C_p$.

En los otros órdenes, $m \in \{4, 6, 8, 9, 10, 12, 14, 15\}$, existe un grupo cíclico C_m. Es posible formar grupos abelianos que son productos directos de grupos cíclicos, pero tales grupos a veces no son nuevos. Del Ejemplo 1.91 se obtiene isomorfismos

$$C_2 \times C_3 \simeq C_6, \quad C_2 \times C_5 \simeq C_{10}, \quad C_3 \times C_4 \simeq C_{12}, \quad C_2 \times C_7 \simeq C_{14}, \quad C_3 \times C_5 \simeq C_{15}.$$

Luego C_6, C_{10}, C_{14} y C_{15} son los únicos grupos *abelianos* de estos órdenes.

Hay otros grupos abelianos de bajo orden:

$$C_2 \times C_2 \simeq V, \quad C_2 \times C_2 \times C_2, \quad C_2 \times C_4, \quad C_3 \times C_3, \quad C_2 \times C_2 \times C_3 \simeq C_2 \times C_6.$$

Los exponentes de estos grupos son respectivamente 2, 2, 4, 3 y 6. Por lo tanto, no son cíclicos (el grupo cíclico C_m es de exponente m).

► Pasando a ejemplos no abelianos, hay una lista de *grupos diedrales*:

$$D_3 \simeq S_3, \quad D_4, \quad D_5, \quad D_6, \quad D_7,$$

de los órdenes respectivos $m = 6, 8, 10, 12, 14$.

El *grupo de cuaterniones* Q, de orden 8, es un grupo no abeliano pero $Q \not\simeq D_4$. De hecho, Q posee un solo elemento de período 2 mientras D_4 contiene cinco.

El *grupo alternante* A_4 es un grupo no abeliano de orden 12, pero $A_4 \not\simeq D_6$. Esto es evidente por cuanto D_6 contiene elementos de período 6 (la rotación $\rho_{\pi/3}$, por ejemplo) mientras A_4 no los tiene.

[24] Para la lista de los grupos finitos de órdenes $|G| \leqslant 16$, se puede consultar la página de la red ⟨`http://es.wikipedia.org/wiki/Anexo:Grupos_finitos_de_orden_bajo`⟩.

El último grupo no abeliano de orden 12 es un *producto semidirecto* $T := C_3 \rtimes_\alpha C_4$ donde $\alpha\colon C_4 \to \mathrm{Aut}(C_3)$ está determinado por $\alpha_t\colon s \longleftrightarrow s^2$, al escribir $C_3 = \{1, s, s^2\}$ y $C_4 = \{1, t, t^2, t^3\}$. Fíjese que $\alpha_{t^2} = (\alpha_t)^2 = 1_{C_3}$ y $\alpha_{t^3} = \alpha_t$; de hecho, como $\mathrm{Aut}(C_3) \simeq C_2$, este α es el único homomorfismo no trivial de C_4 en $\mathrm{Aut}(C_3)$. El elemento $(s, t) \in T$ tiene período 4, así que $T \not\simeq A_4$ y $T \not\simeq D_6$, porque ni A_4 ni D_6 tiene elementos de período 4.

► Falta mostrar que la lista de grupos ya mencionados es exhaustiva.

Si $|G| = p \in \{2, 3, 5, 7, 11, 13, 15\}$, ya se sabe que $G \simeq C_p$.

Si $|G| = p^2 = 4$ ó 9, entonces G es un p-grupo con $Z(G) \neq 1$, por la Proposición 1.79. Si G no fuera abeliano, sería $|Z(G)| = p$ y cada elemento $a \in G \setminus Z(G)$ tendría un centralizador $Z_G(a)$ tal que $Z(G) < Z_G(a) < G$, con lo cual $|Z_G(a)| = p^k$ con $1 < k < 2$, imposible: se concluye que G es abeliano. Entonces, o bien G es cíclico, $G \simeq C_{p^2}$; o bien $G = \langle a, b\rangle$ es generado por dos elementos de período p que conmutan, así que $G \simeq C_p \times C_p$.

Si $|G| = 2p = 6$ ó 10 ó 14 y G es abeliano, entonces G es el producto directo de su p-subgrupo de Sylow y su 2-subgrupo de Sylow, que son cíclicos; luego $G \simeq C_p \times C_2 \simeq C_{2p}$. El mismo argumento muestra que un grupo abeliano de orden 15 es isomorfo a C_{15}.

Si $|G| = 8$ y G es abeliano (véase el Ejemplo 1.92), hay tres posibilidades: (a) G es cíclico, $G \simeq C_8$; o bien (b) $G = \langle a, b\rangle$ con un elemento a de período 4 y otro elemento b de período 2, $b \neq a^2$, en cuyo caso $G =\simeq C_4 \times C_2$; o bien (c) G no posee elementos de período 8 ni 4, así que $G = \langle a, b, c\rangle$ donde a, b, c son elementos distintos de período 2 y por tanto $G \simeq C_2 \times C_2 \times C_2$.

Si $|G| = 12$ y G es abeliano, entonces G es el producto directo de su 2-subgrupo de Sylow y su 3-subgrupo de Sylow. Luego $G \simeq C_4 \times C_3 \simeq C_{12}$ o bien $G \simeq (C_2 \times C_2) \times C_3 \simeq C_2 \times C_6$.

► No hay más grupos abelianos de orden $\leqslant 15$. Supóngase ahora que G no es abeliano.

Si $|G| = 2p = 6$ ó 10 ó 14, el número de p-subgrupos de Sylow es $(1 + kp)$ y divide 2, luego es 1: G posee un p-subgrupo de Sylow *normal* $P = \langle a\rangle$. Sea $Q = \{1, b\}$ algún 2-subgrupo de Sylow. Entonces $bab = ba b^{-1} \in P$, así que $bab = a^m$ con $m \not\equiv 1 \bmod p$. Ahora $a = b^2 a b^2 = b a^m b = (bab)^m = a^{m^2}$, con lo cual $m^2 \equiv 1 \bmod p$; se concluye que $m \equiv -1 \bmod p$, así que $bab = a^{-1}$. De ahí se ve que $ab = b^{-1}a^{-1} = (ab)^{-1}$ y por ende $(ab)^2 = 1$. Se ha mostrado que

$$G \simeq \langle a, b : a^p = b^2 = (ab)^2 = 1\rangle$$

así que $G \simeq D_p$ (véase el Ejemplo 1.113). Para los órdenes 6, 10 y 14, los únicos grupos no abelianos son $D_3 \simeq S_3$, D_5 y D_7 respectivamente.

Si $|G| = 8$, G no contiene un elemento de período 8 y debe tener un elemento con período mayor que 2. Luego hay $a \in G$ de período 4. El subgrupo $N = \langle a\rangle$ es normal

porque $[G\colon N] = 2$. Luego $G = \langle a, b\rangle$ donde $b \notin N$, $b^2 \in N$ porque $[G\colon N] = 2$ y $bab^{-1} \in N$ porque $N \lhd G$. El elemento bab^{-1} tiene período 4 y $bab^{-1} \neq a$ ya que G no es abeliano. Por lo tanto, vale $bab^{-1} = a^3 = a^{-1}$. Como b no es de período 8, se ve que $b^2 \neq a$ y $b^2 \neq a^3$. Si $b^2 = 1$, entonces $G \simeq D_4$ del Ejemplo 1.113. En cambio, si $b^2 = a^2$, el Ejemplo 1.114 muestra que $G \simeq Q$.

► El último paso es la identificación de los grupos no abelianos de orden 12.

Si $|G| = 12$ y G no es abeliano, sea P un 3-subgrupo de Sylow de G. El grupo G actúa sobre el conjunto de coclases G/P por $\varphi_g(hP) := ghP$, permutando así las 4 coclases de P; esta acción define un homomorfismo $\varphi\colon G \to S_4$. Si $g \in \ker\varphi$, entonces $gP = P$, es decir, $g \in P$; por lo tanto, $\ker\varphi = P$ o bien $\ker\varphi = \mathbf{1}$.

Si $\ker\varphi = \mathbf{1}$, entonces $G \simeq \varphi(G) \leqslant S_4$. Resulta que el único subgrupo de S_4 de orden 12 es el grupo alternante A_4. Por lo tanto, en este caso $\underline{G \simeq A_4}$.

En cambio, si $\ker\varphi = P$, entonces $P \trianglelefteq G$. Del Teorema 1.81 (de Sylow), se deduce que P es el *único* 3-subgrupo de Sylow de G. Además, por el mismo teorema hay *tres* 2-subgrupos de Sylow (si hubiera un único 2-subgrupo de Sylow Q, sería $G \simeq P \times Q \simeq C_3 \times C_4$ o bien $C_3 \times V$, abeliano).

Al escribir $P = \{1, c, c^2\}$, los únicos elementos de período 3 en G son c y c^2. La clase conjugada de c es entonces $\{c\}$ o bien $\{c, c^2\}$. En vista del Ejemplo 1.73 y la Proposición 1.67, esto implica que $[G\colon Z_G(c)] = 1$ ó 2.

Si $Z_G(c) = G$, hay un elemento $d \in G$ de período 2, en algún 2-subgrupo de Sylow. Si $|Z_G(c)| = 6$, de nuevo hay un elemento $d \in Z_G(c)$ de período 2, ya que $Z_G(c) \simeq C_6$ ó S_3. En los dos casos, $a := cd = dc$ es un elemento de G de período 6.

Sea $N := \langle a\rangle$, donde $|N| = 6$ y $[G\colon N] = 2$. Del Lema 1.32 se ve que $N \lhd G$. Luego hay $b \in G \setminus N$ con $G = \langle a, b\rangle$, $b^2 = a^k$ y $bab^{-1} = a^m$ para algunos $k, m \in \{0, 1, \ldots, 5\}$. Ahora $m \neq 1$ porque G no es abeliano. Como $a^m = bab^{-1}$ tiene el mismo período que a (es decir, 6), se obtiene $m = 5$ y por ende $bab^{-1} = a^5 = a^{-1}$.

Si el período de b fuera 6, quedarían sólo cinco elementos de períodos 2 ó 4 repartidos entre los tres 2-subgrupos de Sylow. Esto implica que $b^2 \neq a^2$ y $b^2 \neq a^4$. El período de b tampoco es 12 ya que G no es cíclico; luego $b^2 \neq a$ y $b^2 \neq a^5$.

Si $b^2 = 1$, entonces $bab = a^{-1}$ y por tanto $(ab)^2 = 1$. Del Ejemplo 1.113 se obtiene un isomorfismo $\underline{G \simeq D_6}$.

En cambio, si $b^2 = a^3$, de modo que b tenga período 4, es fácil comprobar que la correspondencia $a \mapsto (s, t^2)$, $b \mapsto (s, t)$ determina un isomorfismo $\underline{G \simeq T}$. □

2 Grupoides y Categorías

La *ley de asociatividad* es la propiedad más importante de los grupos. Un *monoide* es asociativo aunque no todos sus elementos tienen inversos; un *semigrupo* es asociativo aunque se prescinde de tener un elemento neutro. Sin embargo, los monoides y semigrupos no constituyen la única manera de generalizar el concepto de grupo. Otra posibilidad, introducida por Brandt[1] y de creciente importancia en años recientes, es el concepto de *grupoide*, donde se conserva la asociatividad y la existencia de inversos pero se permite una pluralidad de elementos neutros. Si se conserva asociatividad y se permiten varios elementos neutros pero no se exige la existencia de inversos, se llega al concepto de *categoría*, que hoy en día forma una estructura organizadora de toda la matemática.

En este capítulo se hace un breve bosquejo introductorio de estas estructuras.

2.1 Grupoides

El concepto de grupoide involucra dos conjuntos, una "base" X y una "cubierta" G: la cubierta generaliza el conjunto subyacente a un grupo, la base sirve como conjunto índice para las unidades. La definición formal es la siguiente.

Definición 2.1. Un **grupoide** sobre un conjunto X es otro conjunto G, con cinco aplicaciones que determinan su estructura:

(a) Hay dos funciones dadas, $s\colon G \to X$ (la **fuente**); y $t\colon G \to X$ (la **meta**). Cuando $s(g) = x$, $t(g) = y$, se escribe $\underline{g\colon x \to y}$ como abreviatura.

(b) Dos elementos $g, h \in G$ son *componibles* si $t(h) = s(g)$. Si

$$G^{(2)} := \{\, (g,h) \in G \times G : s(g) = t(h) \,\}$$

denota el *conjunto de pares componibles*, hay un **producto parcial** $m\colon G^{(2)} \to G$ y se escribe $gh := m(g,h)$. Esta operación debe obedecer:

- $\underline{s(gh) = s(h)}$ y $\underline{t(gh) = t(g)}$ toda vez que $(g,h) \in G^{(2)}$;
- asociatividad $\underline{(gh)k = g(hk)}$: cuando uno de los lados de esta ecuación existe, el otro también existe y son iguales.[2]

[1] El primer uso del vocablo *grupoide*, junto con una definición del concepto, ocurre en el artículo: Heinrich Brandt, *Über eine Verallgemeinerung des Gruppenbegriffes*, Mathematische Annalen **96** (1927), 360–366.

[2] En más detalle: $(gh)k$ existe si $(g,h) \in G^{(2)}$ y $(gh,k) \in G^{(2)}$; en cuyo caso, se afirma que $(h,k) \in G^{(2)}$ y $(g,hk) \in G^{(2)}$ y se postula que $(gh)k = g(hk)$.

(c) Hay una **sección de unidades**[3] inyectiva $u\colon X \to G$, tal que si $g\colon x \to y$ en G, entonces $(u(y), g) \in G^{(2)}$ y $(g, u(x)) \in G^{(2)}$, con $\underline{u(y)g = g = gu(x)}$. ⟦ En particular, $t(u(x)) = x$, $s(u(y)) = y$ para $x, y \in X$, así que las aplicaciones $s, t\colon G \to X$ deben ser *sobreyectivos*. ⟧

(d) Hay una función $i\colon G \to G$, la **inversión**, tal que $i(g)\colon y \to x$ cuando $g\colon x \to y$, que obedece $\underline{i(g)g = u(x)}$ y $\underline{gi(g) = u(y)}$.

Se usa la notación $\underline{G \rightrightarrows X}$ para denotar un grupoide G sobre X. (La doble flecha señala el par de funciones $s, t\colon G \to X$.) ◊

Lema 2.2. *En un grupoide $G \rightrightarrows X$:*

(a) la inversión es involutiva, es decir, $i \circ i = 1_G$;

(b) los inversos son únicos; es decir, para cada $g\colon x \to y$, hay un único $h\colon y \to x$ tal que $gh = u(y)$, $hg = u(x)$.

Demostración. Ad(a): Escríbase $h := i(g)$, $k := i(h) = i(i(g))$; con $x := s(g) = t(h)$, $y := t(g) = s(h)$. Entonces $s(k) = t(h) = x$, así que

$$k = k\,u(x) = k\,i(g)\,g = i(i(g))\,i(g)\,g = i(h)\,h\,g = u(y)\,g = g.$$

Estas expresiones no son ambiguas debido a la asociatividad del producto de un triplete de elementos componibles.

Ad(b): Sean $g, h \in G$ dos elementos tales que $s(g) = t(h)$ y $s(h) = t(g)$. Con la notación $x = s(g)$, $y = t(g)$, supóngase que $gh = u(y)$, $hg = u(x)$. Entonces

$$h = h\,u(y) = h\,g\,i(g) = u(x)\,i(g) = u(t(i(g)))\,i(g) = i(g),$$

lo cual establece la unicidad de h. □

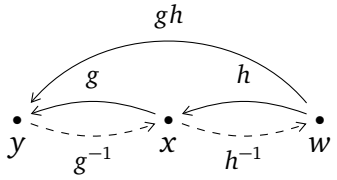
Para aliviar un poco el peso de la notación, se escribe $g^{-1} \equiv i(g)$ y se puede identificar X con su imagen $u(X)$ como parte de G. A veces se escribe $G^{(0)} := u(X)$, $G^{(1)} := G$ y $G^{(3)} := \{(g, h, k) \in G \times G \times G : s(g) = t(h),\ s(h) = t(k)\}$. Entonces cada $u_x \equiv u(x) \in G^{(0)}$ obedece $u_x\colon x \to x$; y las condiciones que definen un grupoide se escriben así:

⋄ $(gh)k = g(hk)$ toda vez que $(g, h, k) \in G^{(3)}$;

[3] Una **sección** de una función $f : A \to B$ es otra función $h\colon B \to A$ tal que $f \circ h = 1_B$. Por ejemplo, en la Proposición 1.99, el homomorfismo $\beta : K \to G$ es una sección del homomorfismo $\psi\colon G \to K$. La igualdad $f \circ h = 1_B$ implica que f debe ser sobreyectiva (una condición necesaria para que exista una sección) y h debe ser inyectiva.

- $u_y g = g = g u_x$ toda vez que $g : x \to y$;
- $g^{-1} g = u_x$, $g g^{-1} = u_y$ toda vez que $g : x \to y$.

Para visualizar la leyes de composición e inversión en un grupoide, es útil dibujar los elementos de G como *flechas* y los elementos de X como *nodos* ligados por las flechas:



Cada flecha procede desde su fuente (la cola de la flecha) hasta su meta (la cabeza de la flecha). Para poder componer dos flechas, la cabeza de la segunda debe coincidir con la cola de la primera —usando el orden de derecha a izquierda, como en la composición de funciones.

Ejemplo 2.3. Un **grupo** es un grupoide sobre un *singulete* (un conjunto $X = \{*\}$ con un solo elemento). El elemento $1 = u(*) \in G$ es el (único) elemento neutro, las funciones s y t son triviales y $G^{(2)}$ es todo $G \times G$, así que el producto es una operación binaria asociativa. El grupoide $G \rightrightarrows \{*\}$ es simplemente el grupo G. ◊

Ejemplo 2.4. Hay un *grupoide trivial* sobre X es $X \rightrightarrows X$, en donde $s = t = 1_X$. ◊

Ejemplo 2.5. El **grupoide de pares** $X \times X \rightrightarrows X$ está definido por las aplicaciones

$$\begin{gathered} s(x,y) := y, \quad t(x,y) := x, \\ m\big((x,y)(y,z)\big) := (x,z), \\ u(x) := (x,x), \quad i(x,y) := (y,x). \end{gathered} \tag{2.1}$$

En este caso $G^{(0)} = u(X)$ es la *diagonal* $\Delta_X = \{\, (x,x) : x \in X \,\} \subset X \times X$. ◊

Ejemplo 2.6. Sea R una **relación de equivalencia** sobre un conjunto X. Por definición, R es una parte del producto cartesiano $X \times X$. Hay un grupoide $R \rightrightarrows X$ definido por las mismas fórmulas (2.1), para pares $(x,y) \in R$ solamente. (En otras palabras: $R \rightrightarrows X$ es un *subgrupoide* de $X \times X \rightrightarrows X$.) Fíjese que $u : X \to R$ está definida porque R es reflexiva, $i : R \to R$ está definida porque R es simétrica, y $m : R^{(2)} \to R$ está definida porque R es transitiva. En resumen: este grupoide permite acceder a la relación de equivalencia sin pasar a su conjunto cociente. ◊

Ejemplo 2.7. Dada una *acción a la izquierda* de un grupo G sobre un conjunto X, hay una **grupoide de acción** $G \times X \rightrightarrows X$ dada por

$$s(g,x) := x \quad \text{y} \quad t(g,x) := g \cdot x.$$

El producto parcial está dado por $(g,x)(h,y) := (gh,y)$ toda vez que $x = h \cdot y$, en cuyo caso $gh \cdot y = g \cdot (h \cdot y) = g \cdot x$: las propiedades de una acción muestran que el producto parcial es compatible con las aplicaciones s y t. El inverso de (g,x) es $(g^{-1}, g \cdot x)$ y la sección de unidades está dada por $u(x) := (1,x)$. ◊

2.2 Categorías y funtores

Los grupoides, introducidos en la sección anterior como una generalización de los grupos que a su vez incluye las acciones de grupos, resultan ser una estructura intermedia que debe ceder su lugar a un concepto más general y poderosa, el de *categoría*.

Definición 2.8. Una **categoría** C es un paquete con tres ingredientes:

(a) Una clase de **objetos** $\underline{\mathrm{Ob}(\mathsf{C})}$;

(b) una familia de conjuntos $\underline{\mathrm{Hom}_{\mathsf{C}}(A,B)}$, uno para cada par de objetos A, B en $\mathrm{Ob}(\mathsf{C})$; los elementos de $\mathrm{Hom}_{\mathsf{C}}(A,B)$ se llaman **morfismos** de A en B;

(c) una **ley de composición** de morfismos, que es una familia de aplicaciones

$$\mathrm{Hom}_{\mathsf{C}}(A,B) \times \mathrm{Hom}_{\mathsf{C}}(B,C) \to \mathrm{Hom}_{\mathsf{C}}(A,C),$$

una para cada tres objetos A, B, C en $\mathrm{Ob}(\mathsf{C})$; la composición de $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ y $g \in \mathrm{Hom}_{\mathsf{C}}(B,C)$ se denotará por $\underline{gf} \in \mathrm{Hom}_{\mathsf{C}}(A,C)$.

Estos datos deben cumplir tres requisitos:

- Los conjuntos de morfismos $\mathrm{Hom}_{\mathsf{C}}(A,B)$ son *disjuntos*: cada morfismo f determina unívocamente dos objetos A, B tales que $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$.
- Para cada objeto $A \in \mathrm{Ob}(\mathsf{C})$ existe un único **morfismo unidad** $1_A \in \mathrm{Hom}_{\mathsf{C}}(A,A)$ tal que $\underline{f\, 1_A = f}$ para todo $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ y $\underline{1_A\, g = g}$ para todo $g \in \mathrm{Hom}_{\mathsf{C}}(C,A)$.
- La composición es *asociativa*: si $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$, $g \in \mathrm{Hom}_{\mathsf{C}}(B,C)$, $h \in \mathrm{Hom}_{\mathsf{C}}(C,D)$, entonces
$$h(gf) = (hg)f \quad \text{en} \quad \mathrm{Hom}_{\mathsf{C}}(A,D).$$ ◊

Históricamente, las categorías fueron inventadas para codificar la idea de "isomorfismo natural" entre objetos matemáticos.[4] La colección de objetos en general no es un conjunto, por ser demasiado amplio: la palabra *clase* es más apropiada.[5]

La totalidad de morfismos, de entre todos los *conjuntos* $\mathrm{Hom}_{\mathsf{C}}(A,B)$, es una clase denotado por $\mathrm{Mor}(\mathsf{C})$. En general, esta clase tampoco es un conjunto; pero los cálculos con morfismos sólo involucran un número finito de los conjuntos $\mathrm{Hom}_{\mathsf{C}}(A,B)$ a la vez.

En muchos de los ejemplos que siguen, aunque no siempre, los morfismos son funciones. En estos casos, se acepta la notación $g \circ f$ como sinónimo de gf. También es cómodo usar la notación $\underline{f : A \to B}$ como abreviatura de "$f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$", aun cuando f no sea una función.

Se habla de una **categoría pequeña** cuando *sus objetos forman un conjunto*. He aquí una definición alternativa de un grupoide: *un grupoide es una categoría pequeña en donde cada morfismo posee un morfismo inverso*. Con la notación de la Definición 2.1, hay que tomar $\mathrm{Ob}(\mathsf{C}) = X$ y $\mathrm{Mor}(\mathsf{C}) = G$.

Ejemplo 2.9. La categoría más sencilla es Set, cuyos objetos son los **conjuntos**. Los morfismos en $\mathrm{Hom}_{\mathsf{Set}}(X,Y)$ son las **funciones** ordinarias $f : X \to Y$. ◊

Ejemplo 2.10. En la categoría Gr, los objetos son los **grupos** y los morfismos en cada $\mathrm{Hom}_{\mathsf{Gr}}(G,K)$ son los **homomorfismos de grupos** $\varphi : G \to K$.

La categoría Ab de los **grupos abelianos** es una *subcategoría* de Gr: los objetos de Ab son objetos de Gr y sus morfismos son morfismos de Gr. Esta es una **subcategoría plena**, por cuanto $\mathrm{Hom}_{\mathsf{Ab}}(G,K) = \mathrm{Hom}_{\mathsf{Gr}}(G,K)$ toda vez que G y K sean grupos abelianos.

En la categoría Ab, cada $\mathrm{Hom}_{\mathsf{Ab}}(G,K)$ es un *grupo abeliano* y no meramente un conjunto. Usando notación aditiva, la **suma de homomorfismos** $\varphi, \psi \in \mathrm{Hom}_{\mathsf{Ab}}(G,K)$ es

$$(\varphi + \psi)(g) := \varphi(g) + \psi(g) \quad \text{para todo} \quad g \in G, \tag{2.2}$$

en donde la suma al lado derecho es la operación de grupo en K. ◊

Ejemplo 2.11. En la categoría Mon, los objetos son los **monoides** y $\mathrm{Hom}_{\mathsf{Mon}}(M,N)$ reúne los **homomorfismos de monoides** $\psi : M \to N$: ellos son las funciones que respetan productos y preservan los elementos neutros.

[4] Los *funtores* aparecieron primeramente, en unos trabajos de Eilenberg y MacLane en 1942, interrumpidos por la guerra mundial. Las categorías nacieron para dar una plataforma para los funtores, en el artículo germinal: Samuel Eilenberg & Saunders MacLane, *General theory of natural equivalences*, Transactions of the American Mathematical Society **58** (1945), 231–294.

[5] En la teoría de conjuntos, se establece una jerarquía de **clases**, en el sentido técnico de la llamada "teoría de clases" de Gödel y Bernays. Cualquier conjunto es una clase, pero no al revés: la colección de todos los conjuntos forma una clase que no es un conjunto (para evitar la paradoja de Russell). En la teoría de Gödel y Bernays, los conjuntos son precisamente las clases que pueden ser miembros de otras clases.

A su vez, Gr es una subcategoría plena de Mon: todo homomorfismo de monoides entre dos grupos respeta inversos, por el comentario después de la Definición 1.40. ◊

Las categorías aparecen en todas las ramas de la matemática. Para dar un solo ejemplo no algebraico, hay una categoría Top cuyos objetos son los *espacios topológicos* y los morfismos en $\mathrm{Hom}_{\mathsf{Top}}(X, Y)$ son las *funciones continuas* $f : X \to Y$.

Ejemplo 2.12. Sea J un **conjunto parcialmente ordenado**.[6] El conjunto J está dotado de una relación $\leqslant$ que es reflexiva, transitiva y antisimétrica. Entonces J da lugar a una categoría pequeña J, con $\mathrm{Ob}(\mathsf{J}) = J$, en donde cada $\mathrm{Hom}_{\mathsf{J}}(i, j) := \{f_{ji}\}$ contiene *un solo morfismo* si $i \leqslant j$, mientras $\mathrm{Hom}_{\mathsf{J}}(i, j) := \emptyset$ si $i \not\leqslant j$. (La ley de composición es entonces automática.)

Fíjese que para $1_k = f_{kk} \in \mathrm{Hom}_{\mathsf{J}}(k, k)$, por reflexividad. Además, vale $f_{kj} f_{ji} = f_{ki}$ si $i \leqslant j \leqslant k$, por transitividad. La asociatividad de esta composición es consecuencia de la unicidad del morfismo f_{li}, si $i \leqslant j \leqslant k \leqslant l$. ◊

► En la medida que una categoría puede ser vista como generalización de un grupo, es legítimo preguntar: ¿cuál sería la generalización de un homomorfismo? Se trataría de definir una aplicación de una categoría en otra (o en sí misma) que preserva la ley de composición y las unidades. Esta idea asume forma concreta en la siguiente definición.

Definición 2.13. Un **funtor** $\mathscr{F}$ de una categoría C en otra categoría D consta de:[7]

(a) una correspondencia $\mathrm{Ob}(\mathsf{C}) \to \mathrm{Ob}(\mathsf{D}) : A \mapsto \mathscr{F}A$;

(b) otra correspondencia $\mathrm{Mor}(\mathsf{C}) \to \mathrm{Mor}(\mathsf{D}) : \varphi \mapsto \mathscr{F}\varphi$, tal que

$$\varphi \in \mathrm{Hom}_{\mathsf{C}}(A, B) \implies \mathscr{F}\varphi \in \mathrm{Hom}_{\mathsf{D}}(\mathscr{F}A, \mathscr{F}B);$$

que cumplen las siguientes condiciones:

(i) $\underline{\mathscr{F}(\psi\varphi) = (\mathscr{F}\psi)(\mathscr{F}\varphi)}$ toda vez que $\varphi \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ y $\psi \in \mathrm{Hom}_{\mathsf{C}}(B, C)$;

(ii) $\underline{\mathscr{F}\, 1_A = 1_{\mathscr{F}A}}$ para todo $A \in \mathrm{Ob}(\mathsf{C})$.

Se escribe $\underline{\mathscr{F} : \mathsf{C} \to \mathsf{D}}$ cuando $\mathscr{F}$ es un funtor de C en D. ◊

[6] Algunos autores lo llaman **poset**, una abreviatura inglesa de *partially ordered set*.

[7] A veces se escribe $\mathscr{F}(A)$ por $\mathscr{F}A$ y $\mathscr{F}(\varphi)$ por $\mathscr{F}\varphi$. Aquí es preferible usar una notación sin adornos para evitar un exceso de paréntesis. Conviene recordar el sabio consejo de William de Ockham: *Entia non sunt multiplicanda praeter necessitatem*.

Ejemplo 2.14. Si C es una categoría cuyos objetos son conjuntos y cuyos morfismos son funciones entre los conjuntos respectivos, se puede definir un funtor $\mathscr{F}\colon \mathsf{C} \to \mathsf{Set}$ por $\mathscr{F}A := A$ y $\mathscr{F}\varphi := \varphi$ para $A \in \mathrm{Ob}(\mathsf{C})$, $\varphi \in \mathrm{Mor}(\mathsf{C})$. El papel de este funtor es simplemente el de "olvidar" cualquier estructura extra de los objetos y morfismos de C, por tanto se llama un **funtor olvidadizo**. Hay funtores olvidadizos $\mathsf{Gr} \to \mathsf{Set}$ y $\mathsf{Ab} \to \mathsf{Set}$ que suprimen las operaciones de producto o suma y dejan de lado la multiplicatividad o aditividad de los homomorfismos. ◊

Ejemplo 2.15. Si X es un conjunto, $\mathscr{P}(X)$ denota el conjunto de todas las partes de X. Si $f : X \to Y$ es un función entre conjuntos, defínase $\mathscr{P}f : A \mapsto f(A) \subseteq Y$ para todo $A \subseteq X$; fíjese que $\mathscr{P}f(\emptyset) = \emptyset$. La correspondencia $X \mapsto \mathscr{P}(X)$, $f \mapsto \mathscr{P}f$ define un funtor $\mathscr{P} : \mathsf{Set} \to \mathsf{Set}$. ◊

Ejemplo 2.16. Si G es un grupo, no necesariamente abeliano, sea G' el *subgrupo derivado*, generado por los conmutadores $ghg^{-1}h^{-1}$ (de la Definición 1.104). Entonces $G' \trianglelefteq G$ y el cociente $\mathscr{A}(G) := G/G'$ es un grupo abeliano. Si $\varphi\colon G \to H$ es un homomorfismo de grupos, está claro que $\varphi(G') \subseteq H'$, lo cual da lugar a un homomorfismo bien definido $\mathscr{A}\varphi\colon G/G' \to H/H' : gG' \mapsto \varphi(g)H'$. Este proceso de **abelianización** es un funtor $\mathscr{A} : \mathsf{Gr} \to \mathsf{Ab}$. ◊

Ejemplo 2.17. Para cualquier categoría C hay un **funtor idéntico** $\mathbf{1}_{\mathsf{C}}\colon \mathsf{C} \to \mathsf{C}$ dado por $\mathbf{1}_{\mathsf{C}}A := A$, $\mathbf{1}_{\mathsf{C}}\varphi := \varphi$ para objeto A en $\mathrm{Ob}(\mathsf{C})$ y cada morfismo φ en $\mathrm{Mor}(\mathsf{C})$. ◊

Definición 2.18. Si C es una categoría cualquiera, C° denota la **categoría opuesta** (o *categoría dual*) definida por

$$\mathrm{Ob}(\mathsf{C}^\circ) := \mathrm{Ob}(\mathsf{C}), \qquad \mathrm{Hom}_{\mathsf{C}^\circ}(A,B) := \mathrm{Hom}_{\mathsf{C}}(B,A). \tag{2.3}$$

Es decir, C° posee los mismos objetos que C pero *las flechas apunten en la dirección contraria*. Si se denota (por esta sola vez) por f° el morfismo $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ visto como elemento de $\mathrm{Hom}_{\mathsf{C}^\circ}(B,A)$, entonces la ley de composición en C° es $\underline{f^\circ g^\circ := (gf)^\circ}$. ◊

A veces se usa la terminología *funtor covariante* para referirse a la condición (i) de la Definición 2.13: un funtor covariante "conserva el orden de las flechas".

Definición 2.19. Un **cofuntor** (a *funtor contravariante*) de una categoría C en otra categoría D se define como un funtor covariante $\mathscr{G}\colon \mathsf{C}^\circ \to \mathsf{D}$. Establece dos correspondencias

(a) $\mathrm{Ob}(\mathsf{C}) \to \mathrm{Ob}(\mathsf{D}) : A \mapsto \mathscr{G}A$; y

(b) $\mathrm{Mor}(\mathsf{C}) \to \mathrm{Mor}(\mathsf{D}) : \varphi \mapsto \mathscr{G}\varphi$ tal que

$$\varphi \in \mathrm{Hom}_{\mathsf{C}}(A,B) \implies \mathscr{G}\varphi \in \mathrm{Hom}_{\mathsf{D}}(\mathscr{G}B, \mathscr{G}A);$$

que cumplen las condiciones:

(i′) $\underline{\mathscr{G}(\psi\varphi) = (\mathscr{G}\varphi)(\mathscr{G}\psi)}$ toda vez que $\varphi \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ y $\psi \in \mathrm{Hom}_{\mathsf{C}}(B,C)$;

(ii) $\underline{\mathscr{G}\,1_A = 1_{\mathscr{G}A}}$ para todo $A \in \mathrm{Ob}(\mathsf{C})$.

Brevemente: un cofuntor "revierte el orden de las flechas". ◊

Ejemplo 2.20. Sea $\mathsf{VectFin}\text{-}\mathbb{F}$ la categoría de *espacios vectoriales de dimensión finita* sobre un cuerpo $\mathbb{F}$, en donde los morfismos $\mathrm{Hom}_{\mathbb{F}}(U,V) \equiv \mathrm{Hom}_{\mathsf{VectFin}\text{-}\mathbb{F}}(U,V)$ son las *aplicaciones* $\mathbb{F}$*-lineales* de U en V. Para cada espacio $\mathbb{F}$-vectorial V de dimensión finita, su **espacio dual**

$$V^* := \mathrm{Hom}_{\mathbb{F}}(V,\mathbb{F})$$

también tiene dimensión finita, porque vale $\dim_{\mathbb{F}} V^* = \dim_{\mathbb{F}} V$. Cada aplicación $\mathbb{F}$-lineal $R\colon U \to V$ posee una **aplicación transpuesta**, dada por

$$R^t : V^* \to U^* : g \mapsto g \circ R.$$

Si $S\colon V \to W$ es otra aplicación $\mathbb{F}$-lineal, entonces $(S\circ R)^t = R^t \circ S^t : h \mapsto h \circ S \circ R$. En otras palabras, las correspondencias $V \mapsto V^*$, $R \mapsto R^t$ definen un **cofuntor de dualidad** $\mathscr{D}\colon (\mathsf{VectFin}\text{-}\mathbb{F})^\circ \to \mathsf{VectFin}\text{-}\mathbb{F}$.

El **espacio bidual** $V^{**} := \mathrm{Hom}_{\mathbb{F}}(V^*,\mathbb{F})$ cumple $\dim_{\mathbb{F}} V^{**} = \dim_{\mathbb{F}} V$; y la segunda transpuesta $S^{tt} := (S^t)^t$ es una aplicación $\mathbb{F}$-lineal en $\mathrm{Hom}_{\mathbb{F}}(V^{**},W^{**})$. Así se define un nuevo funtor (covariante) $\mathscr{D}^2\colon \mathsf{VectFin}\text{-}\mathbb{F} \to \mathsf{VectFin}\text{-}\mathbb{F}$ por $V \mapsto V^{**}$ y $S \mapsto S^{tt}$. ◊

Ejemplo 2.21. En el ejemplo anterior, la igualdad de dimensiones (finitas) $\dim_{\mathbb{F}} V = \dim_{\mathbb{F}} V^* = \dim_{\mathbb{F}} V^{**}$ muestra que siempre hay isomorfismos lineales[8] $V \simeq V^*$ y $V^* \simeq V^{**}$. Sin embargo, cada uno de estos isomorfismos *depende de una base* de V previamente elegida, que da lugar a una base dual para V^* y otra para V^{**}. No hay una manera "natural" de especificar estos isomorfismos sin elegir bases.

En cambio, hay un *isomorfismo natural* $V \simeq V^{**}$ que no depende de las bases. Se trata de la **evaluación** $\eta_V : V \to V^{**}$, definida por

$$\eta_V(x) : f \mapsto f(x), \quad \text{para} \quad x \in V,\ f \in V^*. \tag{2.4}$$

[8]Un **isomorfismo** $\mathbb{F}$**-lineal** es, por definición, una aplicación $\mathbb{F}$-lineal biyectiva. En el contexto más amplio de las categorías, un **isomorfismo** es sencillamente *un morfismo invertible* en la categoría de marras.

Fíjese que η_V es biyectiva ya que $\dim_{\mathbb{F}} V$ es finita.

Si $S: V \to W$ es una transformación lineal, de modo que $\eta_V(x) \in V^{**}$, entonces

$$\big(S^{tt} \circ \eta_V(x)\big)(g) = \eta_V(x)(S^t(g)) = \eta_V(x)(g \circ S) = g \circ S(x) = g(S(x)) = \eta_W(S(x))(g)$$

para todo $x \in V$, $g \in W^*$. Esto dice que

$$S^{tt} \circ \eta_V = \eta_W \circ S : V \to W^{**}. \tag{2.5}$$

En otras palabras, la *familia* de todas las evaluaciones η_V *entrelaza* los efectos del funtor bidual $\mathscr{D}^2$ sobre VectFin-$\mathbb{F}$. ◊

Definición 2.22. Si $\mathscr{F}, \mathscr{G}: \mathsf{C} \to \mathsf{D}$ son dos funtores, una **transformación natural** entre $\mathscr{F}$ y $\mathscr{G}$ es una familia de morfismos $\theta_A \in \mathrm{Hom}_{\mathsf{D}}(\mathscr{F}A, \mathscr{G}A)$, uno para cada objeto A en $\mathrm{Ob}(\mathsf{C})$, tal que

$$\mathscr{G}\varphi \circ \theta_A = \theta_B \circ \mathscr{F}\varphi, \quad \text{para cada} \quad \varphi \in \mathrm{Hom}_{\mathsf{C}}(A, B). \tag{2.6}$$

Dicho de otro modo: para cada $\varphi \in \mathrm{Mor}(\mathsf{C})$, *el siguiente diagrama es conmutativo*:

$$\begin{array}{ccc} \mathscr{F}A & \xrightarrow{\mathscr{F}\varphi} & \mathscr{F}B \\ \Big\downarrow{\scriptstyle \theta_A} & & \Big\downarrow{\scriptstyle \theta_B} \\ \mathscr{G}A & \xrightarrow{\mathscr{G}\varphi} & \mathscr{G}B \end{array}$$

de modo que la familia de los θ_A entrelaza los efectos de los funtores $\mathscr{F}$ y $\mathscr{G}$; se escribe $\theta: \mathscr{F} \to \mathscr{G}$, en forma abreviada. (Dícese que θ es un **isomorfismo natural** si cada θ_A es un isomorfismo en la categoría D.)

Una transformación natural también se llama **morfismo de funtores**: hay una categoría $\underline{\mathsf{Fun}(\mathsf{C}, \mathsf{D})}$ cuyos objetos son los funtores $\mathscr{F}: \mathsf{C} \to \mathsf{D}$ y cuyos morfismos son las transformaciones naturales $\theta: \mathscr{F} \to \mathscr{G}$. Cada funtor determina una transformación idéntica $\iota = 1_{\mathscr{F}} : \mathscr{F} \to \mathscr{F}$ dada por $\iota_A := 1_{\mathscr{F}A}$ y la ley de composición es obvia: $(\theta\eta)_A := \theta_A \circ \eta_A$ para cada objeto A en $\mathrm{Ob}(\mathsf{C})$. ◊

A la luz de esta definición, la relación (2.5) dice que las evaluaciones $\eta_V: V \to V^{**}$ definidas en el Ejemplo 2.21 forman una transformación natural $\eta: \mathbf{1}_{\mathsf{VectFin}\text{-}\mathbb{F}} \to \mathscr{D}^2$ entre el funtor idéntico y el funtor bidual. Cada η_V es biyectivo y por ende es invertible[9] así que η es un isomorfismo natural. Este es el contenido preciso del enunciado: *cada espacio vectorial finitodimensional es* ***naturalmente isomorfo*** *a su espacio bidual*.[10]

[9] Fíjese que η_V^{-1} lleva la evaluación en x de vuelta al vector original $x \in V$.

[10] Si V es un espacio $\mathbb{F}$-vectorial de dimensión infinita, la evaluación $\eta_V: V \to V^{**}$ de la fórmula (2.4) siempre es una aplicación lineal inyectiva, pero no necesariamente sobreyectiva.

3 Anillos

3.1 Definición y ejemplos de anillos

Definición 3.1. Un **anillo** es un conjunto R con dos operaciones binarias: una **suma** $(a,b) \mapsto a+b$ y un **producto** $(a,b) \mapsto a \cdot b = ab$, tales que:

(a) $(R,+)$ es un *grupo abeliano* con elemento neutro 0, el **cero** de R;

(b) $(R,\cdot)$ es un *monoide* con elemento neutro 1, la **identidad** de R;

(c) se cumplen las *leyes distributivas*: $a(b+c) = ab+ac$, $(a+b)c = ab+ac$, para todo $a,b,c \in R$. ◊

Si $ab = ba$ para todo $a,b \in R$, dícese que R es un **anillo conmutativo**. Esta propiedad es opcional: algunos anillos son conmutativos, otros no.

Proposición 3.2. *En un anillo R:*

(a) vale $0a = a0 = 0$ para todo $a \in R$;

(b) $a(-b) = (-a)b = -(ab)$ para todo $a,b \in R$;

(c) $(-1)a = -a$ para todo $a \in R$;

(d) $(na)b = a(nb) = n(ab)$ para todo $a,b \in R$ y todo $n \in \mathbb{Z}$.

Demostración. Ad(a): Si $a \in R$, entonces $0a = (0+0)a = 0a+0a$, así que $0a = 0$ por cancelación (de la Proposición 1.2(e), en notación aditiva). De igual manera, las igualdades $a0 = a(0+0) = a0+a0$ implican $a0 = 0$.

Ad(b): De $0 = 0b = (a+(-a))b = ab+(-a)b$ se deduce $-(ab) = (-a)b$. Se ve que $a(-b) = -(ab)$ de manera similar.

Ad(c): De $a+(-a) = 0 = 0a = (1+(-1))a = a+(-1)a$ se concluye $-a = (-1)a$.

Ad(d): La notación na denota una suma repetida de n copias de a, si $n \in \mathbb{P}$; es decir, $na := a+a+\cdots+a$, unas n veces. También se define $0a := 0$ y $(-n)a := -(na)$ en vista de las partes (a) y (c). En el caso $n = 2$, se obtiene

$$(2a)b = (a+a)b = ab+ab = 2ab = a(b+b) = a(2b)$$

de las leyes distributivas. El caso general sigue por inducción sobre $n \in \mathbb{P}$. □

Ejemplo 3.3. Los *números enteros* $\mathbb{Z}$, con la suma y producto usuales, forman un anillo conmutativo. ◊

Ejemplo 3.4. Cualquier *cuerpo* $\mathbb{F}$ —en particular $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{F}_p$ para p primo— es un anillo conmutativo. ◊

Ejemplo 3.5. Si $m \in \mathbb{P}$ con $m > 1$, el conjunto $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$ de residuos bajo división por m, introducido en el Ejemplo 1.8, es un anillo conmutativo. El producto es simplemente $\overline{r} \cdot \overline{s} := \overline{rs}$ (véase el Ejemplo 1.9). Este anillo es un cuerpo si y sólo si m es un número primo. ◊

Ejemplo 3.6. Si $\mathbb{F}$ es un cuerpo, los **polinomios** $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ con coeficientes $a_0, a_1, \ldots, a_n \in \mathbb{F}$ forman un anillo conmutativo $\mathbb{F}[x]$. Su producto con otro polinomio $q(x) = b_0 + b_1 x + \cdots + b_m x^m$ está dado por

$$p(x)\,q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + a_n b_m\, x^{n+m}. \quad (3.1)$$

El **grado** de un polinomio no nulo $p(x) \neq 0$ es $\underline{\operatorname{gr} p := n}$, el mayor exponente del *monomio* $a_n x^n$ con coeficiente no cero. El polinomio constante $c(x) = c_0$ tiene grado $\operatorname{gr} c = 0$ si $c_0 \neq 0$ en $\mathbb{F}$; no se define el grado del polinomio nulo.[1]

⟦ Dícese que el símbolo x es un **indeterminado**. En realidad, la presencia de x es superflua: se podría reemplazar $p(x)$ por la sucesión terminante $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ con entradas en $\mathbb{F}$. Sin embargo, la regla de multiplicación sería menos cómoda con esa notación. El anillo de polinomios también puede denotarse por $\mathbb{F}[X]$, o bien $\mathbb{F}[t]$, etc.: el nombre del indeterminado es irrelevante. ⟧ ◊

Ejemplo 3.7. Si $\mathbb{F}$ es un cuerpo y $n \in \mathbb{P}$, el **anillo de matrices** $M_n(\mathbb{F}) \equiv \mathbb{F}^{n\times n}$ es la totalidad de matrices $n \times n$ con entradas en $\mathbb{F}$, con las operaciones conocidas: la suma entrada por entrada y el producto matricial. Si $A = [a_{ij}]$, $B = [b_{ij}]$ y $C = [c_{ij}]$, entonces

$$C = AB \quad \text{si y ślo si todo} \quad c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}.$$

Es evidente que $M_1(\mathbb{F}) = \mathbb{F}$. Para $n \geqslant 2$, el anillo $M_n(\mathbb{F})$ no es conmutativo.

Más generalmente, las mismas fórmulas para la suma y el producto matriciales permiten definir $M_n(R)$, el anillo de matrices $n \times n$ con entradas en un anillo R cualquiera. ◊

Ejemplo 3.8. Si G es un grupo finito y si $\mathbb{F}$ es un cuerpo, el **anillo del grupo** $\mathbb{F}[G]$ es la totalidad de combinaciones lineales formales $a = \sum_{g\in G} a_g\, g$ con $g \in G$ y $a_g \in \mathbb{F}$, con la

[1] Algunos autores definen $\operatorname{gr} 0 := -\infty$ para hacer cálculos con grados de polinomios sin hacer excepciones para el caso del polinomio nulo.

suma "vectorial": si $b = \sum_{g\in G} b_g\, g$, entonces $a + b := \sum_{g\in G}(a_g + b_g)\, g$. El producto en $\mathbb{F}[G]$ aprovecha la multiplicación en el grupo G:

$$ab = \Big(\sum_{h\in G} a_h\, h\Big)\Big(\sum_{k\in G} b_k\, k\Big) := \sum_{h\in G}\sum_{k\in G} a_h b_k\, hk = \sum_{g\in G}\Big(\sum_{hk=g} a_h b_k\Big) g\,,$$

con lo cual $(ab)_g := \sum_{hk=g} a_h b_k$.

Fíjese que $G \subset \mathbb{F}[G]$, al considerar cada elemento $g \in G$ con una combinación lineal con un solo término. En particular, la identidad de $\mathbb{F}[G]$ es el elemento neutro $1 \in G$. ◊

Ejemplo 3.9. El **anillo trivial** es $R = \{0\}$, con suma y producto dado por $0 + 0 = 0$, $0 \cdot 0 = 0$, porque no hay otra opción. Nótese que $1 = 0$ en este anillo! ⟦ Tal posibilidad no fue excluida en la Definición 3.1. Sin embargo, en vista de la Proposición 3.2(a), el anillo trivial es el *único* anillo en el cual vale $1 = 0$. ⟧ ◊

Definición 3.10. Si R es un anillo, un elemento $u \in R$ es una **unidad a izquierda** si hay otro elemento $v \in R$ tal que $\underline{uv = 1}$; en cuyo caso, v es una **unidad a derecha**. Dícese que u es una **unidad** en R si tiene estas dos propiedades: hay elementos $v, w \in R$ tales que $uv = 1 = wu$. En este último caso, el cálculo

$$w = w\,1 = wuv = 1\,v = v$$

muestra que $v = w$ y por ende el inverso de una unidad es única. Se escribe $u^{-1} = v = w$, de modo que $\underline{u^{-1}u = uu^{-1} = 1}$.

Es evidente que la identidad 1 es una unidad. El conjunto $R^\times$ de todas las unidades en R es un **grupo** multiplicativo. ◊

Ejemplo 3.11. En un cuerpo $\mathbb{F}$, el grupo de las unidades es $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$. La notación es la misma que la del Ejemplo 1.7.

El grupo de unidades de $\mathbb{Z}$ es $\mathbb{Z}^\times = \{1, -1\} \simeq C_2$.

El grupo de unidades de $M_n(\mathbb{F})$ es $GL(n, \mathbb{F})$, el grupo de matrices invertibles $n \times n$.

El grupo de unidades de $\mathbb{F}[t]$ es $\mathbb{F}^\times$, los *polinomios constantes* no nulos. En un producto de polinomios, los grados se suman; para que $p(t)q(t) = 1$, tanto $p(t)$ como $q(t)$ deben tener grado 0, es decir, deben ser constantes no nulas.

El grupo de unidades de $\mathbb{Z}_m$ es $\mathbb{Z}_m^\times := \{\, \overline{r} \in \mathbb{Z}_m : r \perp m \,\}$. (Véase el Ejemplo 1.9 de nuevo.) ◊

Definición 3.12. Un **anillo de división** es un anillo no trivial R en donde cada elemento no cero es invertible; su grupo de unidades es $R^\times = R \setminus \{0\}$.

Un anillo de división conmutativo es un cuerpo. Un anillo de división no conmutativo a veces se llama *cuerpo sesgado*. ◊

Ejemplo 3.13. Sea $\mathbb{H}$ el espacio vectorial sobre $\mathbb{R}$ con la base $\{1, i, j, k\}$. Un elemento típico $q \in \mathbb{H}$ se escribe como

$$q = q_0 + q_1\, i + q_2\, j + q_3\, k \quad \text{con} \quad q_0, q_1, q_2, q_3 \in \mathbb{R}.$$

Desde luego, $(\mathbb{H}, +)$ es un grupo abeliano aditivo. Defínase el producto en $\mathbb{H}$ por

$$\begin{aligned}(p_0 + p_1 i + p_2 j + p_3 k)&(q_0 + q_1 i + q_2 j + q_3 k) \\ &:= (p_0 q_0 - p_1 q_1 - p_2 q_2 - p_3 q_3) + (p_0 q_1 + p_1 q_1 + p_2 q_3 - p_3 q_2)\, i \\ &\quad + (p_0 q_2 - p_1 q_3 + p_2 q_0 + p_3 q_1)\, j + (p_0 q_3 + p_1 q_2 - p_2 q_1 + p_3 q_0)\, k. \end{aligned} \tag{3.2}$$

Si además $\bar{q} := q_0 - q_1\, i - q_2\, j - q_3\, k$, se calcula que $q\bar{q} = N(q)\, 1$, donde la *norma*[2] $N(q) := q_0^2 + q_1^2 + q_2^2 + q_3^2$ es un número real no negativo. Si $q \neq 0$ en $\mathbb{H}$, entonces $N(q) > 0$ y $q^{-1} := \bar{q}/N(q)$ es un inverso multiplicativo para q. Entonces $\mathbb{H}$ es un anillo de división.

Los ocho elementos $\{\pm 1, \pm i, \pm j, \pm k\}$ forman un subgrupo de $\mathbb{H}^{\setminus}\{0\}$: este el es grupo Q de cuaterniones del Ejemplo 1.114. En efecto, las reglas $i^2 = j^2 = k^2 = -1$; $jk = i = -kj$; $ki = j = -ik$; $ij = k = -ji$ son casos particulares de (3.2). Los elementos $q \in \mathbb{H}$ se llaman **cuaterniones**. (Fíjese que la asociatividad del producto (3.2) es una consecuencia de la asociatividad en el grupo Q.) ◊

El último ejemplo introduce una estructura nueva: los cuaterniones $\mathbb{H}$ forman un anillo (no conmutativo) que es a la vez un espacio vectorial sobre un cuerpo. La multiplicación escalar es compatible con la suma (por linealidad: esta propiedad es parte de la definición de espacio vectorial) y también con el producto del anillo.

Definición 3.14. Sea $\mathbb{F}$ un cuerpo. Un **álgebra** sobre $\mathbb{F}$ es un espacio $\mathbb{F}$-vectorial A que además posee un producto tal que

(a) $(A, +, \cdot)$ es un anillo;

(b) la multiplicación escalar $\mathbb{F} \times A \to A : (\lambda, a) \mapsto \lambda a$ es compatible con el producto; es decir, $(\lambda a)b = \lambda(ab) = a(\lambda b)$ para todo $a, b \in A$ y $\lambda \in \mathbb{F}$. ◊

Por ejemplo, el *álgebra de matrices* $M_n(\mathbb{F})$ tiene dimensión $\dim_{\mathbb{F}} M_n(\mathbb{F}) = n^2$ como espacio vectorial. El **álgebra de cuaterniones** $\mathbb{H}$ es un álgebra sobre $\mathbb{R}$, con $\dim_{\mathbb{R}} \mathbb{H} = 4$, e incluye $\mathbb{C} = \{\, q_0 + q_1\, i : q_0, q_1 \in \mathbb{R} \,\}$ como $\mathbb{R}$-subálgebra. Sin embargo, $\mathbb{H}$ *no es* un álgebra sobre $\mathbb{C}$, porque la multiplicación escalar por i no es compatible con el producto de $\mathbb{H}$: vale $i(jk) = -1$ pero $j(ik) = +1$ en $\mathbb{H}$.

[2] La palabra **norma** para esta función cuadrática con valores no negativos no tiene la misma usanza que la "norma" en análisis, pues obviamente no cumple una desigualdad triangular.

► La Definición 3.1 de un anillo pide la presencia de una identidad multiplicativa 1. Esta es la usanza moderna; sin embargo, al reemplazar la propiedad (b) de esa definición por:

(b′) $(R,\cdot)$ es un *semigrupo*;

se obtiene un **anillo sin identidad**. Por ejemplo, si $m \in \mathbb{P}$ con $m \geqslant 2$, el conjunto $m\mathbb{Z} = \{\, mn : n \in \mathbb{Z} \,\}$ de los enteros divisibles por m es un anillo sin identidad.

Un anillo sin identidad R da lugar a un anillo R^+ por la siguiente construcción. Considérese el producto cartesiano de conjuntos $R^+ := \mathbb{Z} \times R$; es cuestión de definir una suma y producto en R^+, a partir de las operaciones análogas en $\mathbb{Z}$ y en R, para que R^+ sea un anillo (con identidad). Defínase:

$$\begin{aligned}(m,a)+(n,b) &:= (m+n, a+b),\\ (m,a)\cdot(n,b) &:= (mn,\ mb+na+ab), \quad \text{si} \quad m,n \in \mathbb{Z};\ a,b \in R.\end{aligned}$$

(Al lado derecho, $mb = b+\cdots+b$ unas m veces y $na = a+\cdots+a$ unas n veces, de modo que $mb+na+ab \in R$ aunque R no contenga una identidad.) Estas operaciones son asociativas y satisfacen las leyes distributivas. Además, se puede notar que

$$(1,0)\cdot(n,b) = (n, b+0+0) = (n,b), \qquad (m,a)\cdot(1,0) = (m, 0+a+0) = (m,a),$$

así que $(R^+,\cdot)$ es un monoide con identidad $(1,0)$. También, la parte $\{0\}\times R \subset R^+$ es una copia de R encajada en R^+. Es decir, la correspondencia $a \mapsto (0,a)$ es inyectiva y conserva sumas y productos: el anillo R^+ incluye una copia isomorfa de R.

3.2 Ideales y homomorfismos de anillos

Definición 3.15. Un **ideal** en un anillo R es una parte $I \subseteq R$ tal que:

(a) $(I,+)$ es un subgrupo de $(R,+)$;

(b) Si $a \in R$ y $c \in I$, entonces $ac \in I$ y $ca \in I$.

Más generalmente, un subgrupo aditivo J de R se llama un **ideal a izquierda** si $ac \in J$ para todo $a \in R$ y $c \in J$. De igual modo se define un **ideal a derecha** si $a \in R$, $c \in J$ implican $ca \in J$. Un ideal (a veces llamado *ideal bilateral*) cumple ambas condiciones a la vez. Nótese que generalmente un ideal es un anillo sin identidad.

Las coclases aditivas $\{\, a+I : a \in R \,\}$ forman un anillo, denotado por $\underline{R/I}$, con las siguientes operaciones:

$$\begin{aligned}(a+I)+(b+I) &:= a+b+I,\\ (a+I)(b+I) &:= ab+I.\end{aligned} \tag{3.3}$$

Obsérvese que $(R/I,+)$ es un grupo aditivo porque el subgrupo $(I,+)$ de $(R,+)$ es normal ya que $(R,+)$ es abeliano; y que el producto de coclases está bien definido, porque si $c,d \in I$, entonces

$$(a+c)(b+d) = ab + (ad + cb + cd) \in ab + I.$$

Con estas operaciones, R/I es el **anillo cociente** de R por el ideal I. El cero de R/I es la coclase I y la identidad es la coclase $1+I$. ◊

Definición 3.16. La intersección de una familia de ideales de un anillo R es también un ideal de R. Sea S una parte de R. Denótese por (S) el menor ideal que incluye S, esto es,

$$(S) := \bigcap \{ I \text{ un ideal de } R : S \subseteq I \}.$$

Dícese que (S) es el **ideal generado por** S.[3]

Si $S = \{ c_1, \ldots, c_m \}$ es finito, se escribe $(S) = (c_1, \ldots, c_m)$. Dícese que un ideal $I = (c)$ es un **ideal principal** si está generado por un solo elemento.

Si R es un anillo *conmutativo*, entonces $(c) = Rc = cR = \{ ac : a \in R \}$ y los elementos de un ideal finitamente generado se describen así:

$$(c_1, \ldots, c_m) = \{ a_1c_1 + a_2c_2 + \cdots + a_mc_m : a_1, \ldots, a_m \in R \}.$$

Un anillo R es un **simple** si sus únicos ideales son los ideales triviales $\{0\}$ y R. ◊

Lema 3.17. *Un anillo conmutativo es simple si y sólo si es un cuerpo.*

Demostración. Sea I un ideal no nulo de un cuerpo $\mathbb{F}$. Si $c \in I$ con $c \neq 0$, entonces $1 = c^{-1}c \in I$, así que $a = a\,1 \in I$ para todo $a \in \mathbb{F}$. Por tanto, el único ideal no nulo es $I = \mathbb{F}$, así que $\mathbb{F}$ es un anillo simple.

Inversamente, sea R un anillo conmutativo simple. Si $a \in R \setminus \{0\}$, entonces $(a) \neq \{0\}$ así que $(a) = R$. En particular, $1 \in (a) = Ra = aR$ así que hay $b \in R$ con $ba = ab = 1$; se concluye que R es un anillo de división conmutativo, esto es, un cuerpo. □

Ejemplo 3.18. Un subgrupo aditivo de $\mathbb{Z}$ es también cíclico, por la Proposición 1.22, por lo tanto es de la forma $k\mathbb{Z} = \{ kl : l \in \mathbb{Z} \}$ para algún $k \in \mathbb{N}$. Este subgrupo aditivo es evidentemente un ideal; de hecho, es un ideal principal, $(k) = k\mathbb{Z}$. Fíjese que $(0) = \{0\}$ y $(1) = \mathbb{Z}$, mientras (k) es un ideal propio si $k \geqslant 2$.

Si $m \in \mathbb{P}$ no es primo, un subgrupo aditivo propio de $\mathbb{Z}_m$ es cíclico, luego es de la forma $I = \{\overline{0}, \overline{k}, \overline{2k}, \ldots, \overline{k(r-1)}\}$ donde $kr = m$. (Por el teorema de Lagrange, el orden $|I| = r$ y el índice $[\mathbb{Z}_m : I] = k$ del subgrupo aditivo son divisores de m.) En este caso también, cada subgrupo aditivo es un anillo principal: $I = (\overline{k})$ para algún $\overline{k} \in \mathbb{Z}_m$. ◊

[3] Compárese esta noción con la Definición 1.19 de subgrupo generado por una parte de un grupo.

Ejemplo 3.19. En el anillo matricial $R = M_n(\mathbb{F})$, las *ideales a izquierda* están clasificados por una selección de columnas. En efecto, si $J = \{j_1, \ldots, j_r\} \subseteq \{1, \ldots, n\}$, sea $M_{(J)}$ la totalidad de matrices en R cuyas entradas no ceros ocurren solamente en las columnas indiciadas por J. En otras palabras, $C = [c_{ij}] \in M_{(J)}$ si y sólo si $c_{ij} = 0$ para $j \notin J$. Este es obviamente un subgrupo aditivo de R. Si $A \in R$, la entrada (i, j) de AC es $\sum_{k=1}^{n} a_{ik}c_{kj}$, también cero si $j \notin J$. Luego $M_{(J)}$ es un ideal a izquierda en R.

No es difícil comprobar que cualquier ideal a izquierda de $M_n(\mathbb{F})$ es de la forma $M_{(J)}$ para algún $J \subseteq \{1, \ldots, n\}$. (Nótese que $J = \emptyset$ corresponde al ideal trivial $\{0\}$.)

La transpuesta de AC es la matriz $(AC)^t = C^t A^t$. De ahí se ve que cualquier *ideal a derecha* de $M_n(\mathbb{F})$ es de la forma $M^{(J)}$, la totalidad de matrices cuyas entradas no ceros ocurren solamente en las *filas* indiciadas por J.

Fíjese también que el ideal a izquierda $M_{(J)}$ no es un ideal a derecha excepto en los dos casos extremos $J = \emptyset$ y $J = \{1, \ldots, n\}$. Por lo tanto, los únicos ideales (bilaterales) de $R = M_n(\mathbb{F})$ son los ideales triviales $\{0\}$ y R: el anillo de matrices $M_n(\mathbb{F})$ es *simple*. ◊

Ejemplo 3.20. Si $\mathbb{F}$ es un cuerpo, sea $\mathbb{F}[x, y]$ el anillo de *polinomios en dos incógnitas*; sus elementos tiene la forma[4]

$$p(x, y) = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \cdots + a_{mn}x^m y^n$$

con un número finito de sumandos. El ideal (x, y) consta de todos los polinomios con término constante nulo, $a_{00} = 0$. Este ideal no es principal. ◊

► Hay una cierta analogía entre los ideales de un anillo y los subgrupos normales de un grupo. En los dos casos, se trata de la estructura que forma el núcleo de un homomorfismo. Ya es hora de introducir los homomorfismos de anillos, que permitirá ampliar los teoremas de isomorfía al contexto de los anillos.

Definición 3.21. Si R y S son dos anillos, un **homomorfismo** de R en S es una función $\varphi : R \to S$ tal que:

(a) $\varphi(a + b) = \varphi(a) + \varphi(b)$ para todo $a, b \in R$;

(b) $\varphi(ab) = \varphi(a)\varphi(b)$ para todo $a, b \in R$;

(c) $\varphi(1) = 1$.

La **imagen** de φ es $\operatorname{im}\varphi := \varphi(R)$ y su **núcleo** es $\ker\varphi := \{\, a \in R : \varphi(a) = 0 \in S \,\}$. ◊

[4]Es implícita en la notación que las incógnitas conmutan, $yx = xy$.

Como en el caso de los grupos, dícese que un homomorfismo biyectivo es un **isomorfismo**. Dos anillos son **isomorfos** si hay un isomorfismo de anillos de uno al otro.

Un homomorfismo de anillos $\varphi : R \to S$ es en particular un homomorfismo de grupos desde $(R,+)$ a $(S,+)$. Como tal, φ es inyectivo si y sólo si $\ker\varphi = \{0\}$.

Proposición 3.22. *Si $\varphi : R \to S$ es un homomorfismo de anillos, entonces su imagen* $\operatorname{im}\varphi$ *es un* subanillo *de S; su núcleo* $\ker\varphi$ *es un* ideal *de R.*

Demostración. La imagen $\operatorname{im}\varphi = \varphi(R)$ es un subgrupo aditivo de S. Las igualdades $\varphi(a)\varphi(b) = \varphi(ab)$ y $\varphi(1) = 1$ muestran que $\varphi(R)$ es un submonoide multiplicativo de S también. Luego $\varphi(R) \subseteq S$ es un subanillo.

Es evidente que $\ker\varphi$ es un subgrupo aditivo de R. Si $c \in \ker\varphi$ y $a \in R$, entonces $\varphi(ac) = \varphi(a)\varphi(c) = \varphi(a)0 = 0$ y $\varphi(ca) = \varphi(c)\varphi(a) = 0\varphi(a) = 0$, así que $ac \in \ker\varphi$ y $ca \in \ker\varphi$. Luego $\ker\varphi$ es un ideal de R. □

Definición 3.23. En la **categoría de anillos** An, los objetos son anillos y los morfismos son los homomorfismos de anillos. La composición de homomorfismos es la composición usual de funciones: si $\varphi \in \operatorname{Hom}_{\mathsf{An}}(R,S)$ y $\psi \in \operatorname{Hom}_{\mathsf{An}}(S,T)$, entonces $\psi\varphi = \psi \circ \varphi \in \operatorname{Hom}_{\mathsf{An}}(R,T)$.

Los *anillos conmutativos* forman una subcategoría plena AnCom de An. ◊

En la categoría An, hay teoremas de isomorfía análogos a los de la Sección 1.4 para la categoría de grupos. Cada ideal I de un anillo R da lugar a una aplicación cociente $\eta : R \to R/I : a \mapsto a + I$ que es un homomorfismo sobreyectivo de anillos.

Proposición 3.24. *Sea $\varphi : R \to S$ un homomorfismo de anillos. Entonces hay un isomorfismo $\psi : R/\ker\varphi \to \varphi(R)$ tal que $\varphi = \iota \circ \psi \circ \eta$, donde $\eta : R \to R/\ker\varphi$ es sobreyectivo y $\iota : \varphi(R) \to S$ es inyectivo.*

Demostración. En esta *factorización canónica* de φ, el homomorfismo η es la aplicación cociente asociada con el ideal $\ker\varphi$ y ι es la inclusión del subanillo $\varphi(R)$ en S.

Defínase $\psi : R/\ker\varphi \to \varphi(R)$ por $\psi(a + I) := \varphi(a)$. Por la demostración del Teorema 1.50, este ψ está bien definido como homomorfismo biyectivo de grupos aditivos. Además, se puede notar que

$$\psi(a+I)\psi(b+I) = \varphi(a)\varphi(b) = \varphi(ab) = \psi(ab+I) \quad \text{y} \quad \psi(1+I) = \varphi(1) = 1,$$

así que ψ es un isomorfismo de anillos. □

Proposición 3.25. *Sea I un ideal de un anillo R y sea Q un subanillo de R. Entonces $Q + I$ es un subanillo de R que incluye I como ideal, la intersección $Q \cap I$ es un ideal de Q y hay un isomorfismo de anillos $(Q+I)/I \simeq Q/(Q \cap I)$.*

Demostración. Está claro que $Q+I=\{\,b+c\,:\,b\in Q, c\in I\,\}$ es un subanillo de R (fíjese que $1\in Q\subseteq Q+I$ porque Q es un subanillo). También se ve que I es un ideal en $Q+I$. La correspondencia $\varphi\colon b\mapsto b+I$ es un homomorfismo de anillos sobreyectivo de Q en $(Q+I)/I$, cuyo núcleo es $\ker\varphi=\{\,b\in Q\,:\,b\in I\,\}=Q\cap I$. La Proposición 3.24 entonces produce un isomorfismo de anillos $\psi\colon Q/(Q\cap I)\to(Q+I)/I$. □

► Dícese que un ideal I de R es un **ideal maximal** si $I\neq R$ y si no hay ideal J alguno con $I\subset J\subset R$.

Proposición 3.26. *Sea R un anillo conmutativo. Un ideal M de R es maximal si y sólo si el anillo cociente R/M es un cuerpo.*

Demostración. Si M es un ideal cualquiera de R, sea $\eta\colon R\to R/M$ el homomorfismo cociente. Entonces $R/M=\eta(R)$ es un anillo conmutativo porque R es conmutativo.

El ideal M es maximal si y sólo si R/M es simple. En efecto, si $\underline{K}$ es un ideal de R/M, entonces $K:=\eta^{-1}(\underline{K})=\{\,d\in R\,:\,d+M\in\underline{K}\,\}$ es un ideal de R con $M\subseteq K\subseteq R$; si M es maximal, $\underline{K}$ no puede ser un ideal propio de R/M. Inversamente, si J es un ideal de M con $M\subseteq J\subseteq R$, entonces $\eta(J)$ es un ideal de R/M; si R/M es simple, las únicas posibilidades son $J=M$ y $J=R$.

El Lema 3.17 dice que R/M (¡conmutativo!) es simple si y sólo si es un cuerpo. □

3.3 Anillos enteros y sus cuerpos de fracciones

Una diferencia entre los anillos $\mathbb{Z}$ y $\mathbb{Z}_6$ es el fenómeno $\overline{2}\cdot\overline{3}=\overline{0}$ en $\mathbb{Z}_6$, ya observado en el Ejemplo 1.9. En cambio, en $\mathbb{Z}$ el producto de dos enteros no ceros nunca es igual a cero. En un estudio de la divisibilidad de números enteros, esta ausencia de "divisores de cero" juega un papel importante.

Definición 3.27. Sea R un anillo no trivial. Dos elementos $a,b\in R$ se llaman **divisores de cero**[5] si $a\neq 0$, $b\neq 0$, pero $ab=0$.

Un **anillo entero** (también llamado *dominio entero*, o simplemente *dominio*)[6] es un anillo conmutativo no trivial sin divisores de cero:

$$ab=0\implies a=0\ \text{ o bien }\ b=0. \qquad \lozenge$$

[5] Más precisamente, a es un divisor de cero *a izquierda* y b es un divisor de cero *a derecha*. Sin embargo, esta es una distinción de poco monta cuando el anillo es conmutativo.

[6] El término *dominio entero* nada tiene que ver con el dominio de una función; en estos apuntes se sigue el libro de Lang, que prefiere el término **anillo entero**. Un término análogo, *dominio racional*, fue introducido por Kronecker en 1881 para referirse a un anillo de números en donde también es posible dividir (salvo por cero): ha caído en desuso, porque un dominio racional no es otra cosa que un *cuerpo*.

Lema 3.28. *Un anillo conmutativo no trivial R es un anillo entero si y sólo si la* ley de cancelación *es válida en R:*

$$\text{si } a \neq 0, \ \text{entonces } \ ab = ac \implies b = c.$$

Demostración. Si $ab = ac$ en R, entonces $a(b-c) = 0$. El anillo R es entero si y sólo si uno de estos dos factores es cero. Luego, si $a \neq 0$, entonces $b - c = 0$. □

Obsérvese que el anillo $\mathbb{Z}_m$ es entero si y sólo si m es primo, en cuyo caso $\mathbb{Z}_m$ es un cuerpo: $\mathbb{Z}_p = \mathbb{F}_p$ para p primo.

Ejemplo 3.29. El juego de números complejos $\mathbb{Z}[i] := \{ m + n\,i : m, n \in \mathbb{Z} \}$ es el anillo de los **enteros gaussianos**. Es un anillo entero, porque $\mathbb{Z}[i] \subset \mathbb{C}$ y por tanto no contiene divisores de cero. ◊

Definición 3.30. Sea R un anillo entero. Defínase una relación de equivalencia en el conjunto $R \times (R \setminus \{0\})$ por $(a, b) \sim (c, d)$ si y sólo si $ad = bc$; denótese por $\overline{a/b}$ la clase de equivalencia de (a, b). La totalidad de estas clases $\mathrm{Frac}(R) := \{ a/b : a, b \in R, \ b \neq 0 \}$ es el **cuerpo de fracciones** (o *cuerpo de cocientes*) de R. ◊

El término *cuerpo* en el nombre de $\mathrm{Frac}(R)$ se justifica por la observación siguiente.

Proposición 3.31. *Sea R un anillo entero y sea $F = \mathrm{Frac}(R)$ el juego de fracciones formados por elementos de R. Es posible definir una suma y un producto en F tal que F sea un cuerpo. Además, la correspondencia $R \to F : a \mapsto a/1$ incluye R como un subanillo de F.*

Demostración. La suma y el producto en F se definen por analogía con la aritmética de los números racionales en $\mathbb{Q}$, esto es,

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}. \tag{3.4}$$

Para comprobar que estas operaciones están *bien definidas*, nótese en primera instancia que si $b \neq 0$ y $d \neq 0$, entonces $bd \neq 0$ porque R es un anillo entero. Si $a'/b' = a/b$ y $c'/d' = c/d$, entonces $a'b = ab'$ y $c'd = cd'$; luego, como R es conmutativo,

$$\begin{aligned} (a'd' + b'c')bd &= a'bdd' + bb'c'd = ab'dd' + bb'cd' = (ad + bc)b'd', \\ a'c'bd &= a'bc'd = ab'cd' = acb'd', \end{aligned}$$

así que $(a'd' + b'c')/b'd' = (ad + bc)/bd$ y también $a'c'/b'd' = ac/bd$.

Con estas operaciones, F es un anillo conmutativo: se comprueba la asociatividad y conmutatividad de las dos operaciones y también su ley distributiva con cálculos idénticos

al caso del cuerpo $\mathbb{Q}$. Fíjese que $0/b = 0/1$ para $b \in R \setminus \{0\}$, porque $0 \cdot b = 0 \cdot 1 = 0$ en R; el cero de F es esta fracción $0/1$. También, $b/b = 1/1$ para todo $b \in R \setminus \{0\}$; la fracción $1/1$ es la identidad de F.

Nótese también que $a/b = 0/1$ en F si y sólo si $a = 0$. Si $a, b \in R \setminus \{0\}$, entonces $(a/b) \cdot (b/a) = ab/ab = 1/1$; esto dice que cualquier elemento no cero a/b en F posee un recíproco b/a. Por lo tanto, el anillo F es un cuerpo.

Defínase $\varphi : R \to F$ por $\varphi(a) := a/1$. De las fórmulas (3.4) es inmediato que φ es un homomorfismo de anillos, cuyo núcleo es $\ker \varphi = \{0\}$. Entonces φ es inyectivo y $R \simeq \varphi(R)$. En otras palabras, R es isomorfo al subanillo $\varphi(R)$ de F. □

De ahora en adelante, conviene escribir $a/1 = a$, identificando R con su copia isomorfa dentro de F. Nótese que $R = F$ si y sólo si F es un cuerpo, en cuyo caso $a/b = ab^{-1}/1$ para todo $b \neq 0$.

Ejemplo 3.32. En el caso del anillo entero $\mathbb{Z}$, su cuerpo de fracciones es $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, el cuerpo conocido de los números racionales. En efecto, la construcción del cuerpo $\mathrm{Frac}(R)$ para cualquier anillo entero R sigue el proceso clásico que construye $\mathbb{Q}$ a partir de $\mathbb{Z}$. ◊

Ejemplo 3.33. Si $\mathbb{F}$ es un cuerpo, el anillo de polinomios $\mathbb{F}[x]$ es un anillo entero. En efecto, el producto de los polinomios $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ y $q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$ es otro polinomio

$$p(x)\,q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + a_n b_m\, x^{n+m}.$$

Si los dos polinomios no son nulos, entonces $a_n \neq 0$ y $b_m \neq 0$, así que $a_n b_m \neq 0$ en $\mathbb{F}$, así que $\mathbb{F}[x]$ no posee divisores de cero. (Además, $\mathrm{gr}(pq) = n + m = \mathrm{gr}\, p + \mathrm{gr}\, q$; en un producto de polinomios, los grados se suman.)

El cuerpo de cocientes de $\mathbb{F}[x]$ es la totalidad de **funciones racionales** de una variable x, es decir, expresiones de la forma[7]

$$f(x) = \frac{p(x)}{q(x)} = \frac{a_0 + a_1 x + \cdots + a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m} \quad \text{con} \quad q(x) \neq 0.$$

Este cuerpo de funciones racionales se denota por $\underline{\mathbb{F}(x)}$, con paréntesis redondas. ◊

Definición 3.34. Si R es un anillo entero cualquiera, se puede formar el anillo $\underline{R[x]}$, de **polinomios con coeficientes en** R, generalizando así el Ejemplo 3.6. El argumento del Ejemplo 3.33 es aplicable y demuestra que $R[x]$ es también un anillo entero: si $a_n \neq 0$ y $b_m \neq 0$ en R, entonces $a_n b_m \neq 0$ en $R[x]$, lo cual comprueba $p(x)\,q(x) \neq 0$ en $R[x]$.

[7] En este cociente de polinomios, el símbolo 'x' sigue siendo un *indeterminado*: no se trata, a esta altura, de evaluar la función al sustituir un elemento particular de $\mathbb{F}$ en lugar de x.

En particular, si $R = \mathbb{F}[x]$ es el anillo de polinomios en un indeterminado x, se puede formar el anillo de polinomios $R[y]$ en otro indeterminado y:

$$\mathbb{F}[x,y] := R[y] = \mathbb{F}[x][y].$$

Este anillo entero es el anillo de *polinomios en dos variables* con coeficientes en $\mathbb{F}$. Al repetir este proceso varias veces, se obtiene así un anillo de polinomios en k variables, $\mathbb{F}[x_1, x_2, \ldots, x_k]$ para cualquier $k \in \mathbb{P}$. Todos estos anillos son enteros. ◊

3.4 Módulos sobre un anillo

Definición 3.35. Sea R un anillo. Un ***R*-módulo a izquierda** es un *grupo abeliano* M junto con una aplicación $R \times M \to M : (a,x) \mapsto ax$ que satisface:

(a) $a(x+y) = ax + ay$ para todo $a \in R$, $x, y \in M$;

(b) $(a+b)x = ax + bx$ para todo $a, b \in R$, $x \in M$;

(c) $a(bx) = (ab)x$ para todo $a, b \in R$, $x \in M$;

(d) $1x = x$ para todo $x \in M$. ◊

Las propiedades (a) y (b) de esta definición de módulo generalizan la ley distributiva de un anillo; las propiedades (c) y (d) son análogas a las propiedades de una acción de grupo. Se trata, entonces, de *la acción de un anillo sobre un grupo abeliano*. En el caso de que R sea un *cuerpo* $\mathbb{F}$, la Definición 3.35 dice simplemente que M es un espacio vectorial sobre $\mathbb{F}$, en donde la operación $(a,x) \mapsto ax$ es la *multiplicación escalar* de un vector x por un escalar a. En síntesis: *el concepto de R-módulo a izquierda generaliza la multiplicación escalar de un espacio vectorial*, pero los "escalares" en R tal vez no conmutan.

Los grupos pueden actuar sobre conjuntos a la izquierda o bien a la derecha. De forma totalmente análoga, se puede definir una estructura de R-módulo en donde el anillo actúa a la derecha.

Definición 3.36. Sea R un anillo. Un ***R*-módulo a derecha** es un grupo abeliano N junto con una aplicación $N \times R \to N : (x,a) \mapsto xa$ que satisface:

(a) $(x+y)a = xa + ya$ para todo $a \in R$, $x, y \in N$;

(b) $x(a+b) = xa + xb$ para todo $a, b \in R$, $x \in N$;

(c) $(xb)a = x(ba)$ para todo $a, b \in R$, $x \in N$;

(d) $x1 = x$ para todo $x \in N$. ◊

Dado un R-módulo a izquierda M, cada aplicación $\sigma_a : M \to M : x \mapsto ax$ es un homomorfismo de grupos abelianos, por la Definición 3.35(a). Dícese que $\sigma_a \in \mathrm{Hom}_{\mathsf{Ab}}(M, M)$ es un **endomorfismo**[8] del grupo abeliano M. Denótese por

$$\mathrm{End}\, M \equiv \mathrm{End}_{\mathsf{Ab}}(M) := \mathrm{Hom}_{\mathsf{Ab}}(M, M)$$

la totalidad de endomorfismos de M como grupo abeliano. Obsérvese que $\mathrm{End}(M)$ *es un anillo* bajo la suma de endomorfismos (2.2) y la composición $\varphi\psi : x \mapsto \varphi(\psi(x))$; la identidad es el endomorfismo 1_M. Las demás propiedades de la Definición 3.35 son:

$$\text{(b) } \sigma_{a+b} = \sigma_a + \sigma_b, \qquad \text{(c) } \sigma_a\sigma_b = \sigma_{ab}, \qquad \text{(d) } \sigma_1 = 1_M\,.$$

Por lo tanto, la correspondencia $a \mapsto \sigma_a$ *es un homomorfismo de anillos* $\sigma : R \to \mathrm{End}\, M$.

También es evidente que cualquier homomorfismo $\sigma : R \to \mathrm{End}\, M$ determina una estructura de R-módulo sobre el grupo abeliano M al definir $ax := \sigma(a)(x)$.

La misma lógica identifica la estructura de un R-módulo a derecha con un homomorfismo de R en un anillo de endomorfismos. En efecto, dado un R-módulo a derecha N, cada aplicación $\tau_a : N \to N : x \mapsto xa$ es un endomorfismo de N como grupo abeliano. Además $\tau_{a+b} = \tau_a + \tau_b$ y $\tau_1 = 1_N$, como antes. Pero ahora la Definición 3.36(c) dice que $\tau_a\tau_b = \tau_{ba}$. Esto dice que $a \mapsto \tau_a$ es un homomorfismo de anillos $\tau : R \to (\mathrm{End}\, N)^\circ$ cuyo codominio es el **anillo opuesto** de $\mathrm{End}\, N$. En dicho anillo, la misma suma de endomorfismo se combina con la composición al revés, $\varphi^\circ\psi^\circ = (\psi\varphi)^\circ$. ⟦ Compárese con la Definición 2.18 de categoría opuesta. También es posible considerar τ como homomorfismo $R^\circ \to \mathrm{End}\, N$. ⟧

Cualquier *ideal a izquierda* J en un anillo R es un R-módulo a izquierda, cuya acción $R \times J \to J$ es el producto del anillo, porque $ac \in J$ toda vez que $a \in R$ y $c \in J$.

Ejemplo 3.37. El anillo de polinomios $R[x]$ es un R-módulo bajo la "multiplicación por constantes" $a(b_0 + b_1x + \cdots + b_nx^n) := ab_0 + ab_1x + \cdots + ab_nx^n$. ◊

Ejemplo 3.38. *Un grupo abeliano es un $\mathbb{Z}$-módulo*. En efecto, en un grupo abeliano $(A, +)$, la suma repetida $na := a+a+\cdots+a$ (unas n veces) para $n \in \mathbb{P}$, junto con las reglas $0a := 0$ y $(-n)a := n(-a) = -na$, define una acción de $\mathbb{Z}$ sobre A que satisface las propiedades de la Definición 3.35. Como $1a = a$ necesariamente, se ve que esta es la *única* manera que A resulta ser un $\mathbb{Z}$-módulo a izquierda.

El grupo abeliano A es también un $\mathbb{Z}$-módulo a derecha de una sola manera: para que $(a, n) \mapsto a \cdot n$ cumpla la Definición 3.36, como $a \cdot 1 = a$ necesariamente, es obligatorio que $a \cdot n = na$ para todo $a \in A$, $n \in \mathbb{Z}$. ◊

[8] El prefijo *endo-* significa que el codominio coincide con el dominio.

El último ejemplo señala una propiedad importante de anillos conmutativos. Si M es un R-módulo a izquierda donde R es un *anillo conmutativo*, la identificación $\underline{xa \equiv ax}$, para $a \in R$, $x \in M$, hace de M un R-módulo a derecha. En tal caso, se puede hablar de un **R-módulo** simplemente.

Ejemplo 3.39. Sea $\mathbb{F}^n$ el espacio vectorial de *vectores columna* con n entradas en un cuerpo $\mathbb{F}$. El anillo de matrices $R = M_n(\mathbb{F})$ actúa sobre $\mathbb{F}^n$ por $(A, x) \mapsto Ax$, al multiplicar una matriz en R por un vector columna. De este modo, $\mathbb{F}^n$ es un R-módulo a izquierda.

Denótese por $\mathbb{F}_n := \{ x^t : x \in \mathbb{F}^n \}$ el espacio vectorial de *vectores fila* con n entradas en $\mathbb{F}$. El mismo anillo de matrices $R = M_n(\mathbb{F})$ actúa a la derecha sobre vectores de fila por $(x^t, A) \mapsto x^t A$, de manera que $\mathbb{F}_n$ es un R-módulo a derecha. ◊

Ejemplo 3.40. Sea V Las transformaciones $\mathbb{F}$-lineales de V en sí mismo —es decir, los **endomorfismos lineales** de V, forman un anillo $R = \mathrm{End}_{\mathbb{F}}(V) := \mathrm{Hom}_{\mathbb{F}}(V, V)$. La evaluación $(T, x) \mapsto T(x)$ indica que V es un R-módulo a izquierda. ◊

Definición 3.41. Si V es un espacio vectorial sobre un cuerpo $\mathbb{F}$, sea $GL(V)$ el grupo de transformaciones lineales biyectivas $S : V \to V$; entonces $GL(V)$ es el grupo de unidades del anillo $\mathrm{End}_{\mathbb{F}}(V)$. Una **representación de un grupo** G sobre V es un homomorfismo $\pi : G \to GL(V)$.

El espacio vectorial V es *un módulo a izquierda para el anillo de grupo* $\mathbb{F}[G]$, al extender la acción de G sobre V a una acción de $\mathbb{F}[G]$, por linealidad:

$$a = \sum_{g \in G} a_g g \quad \text{actúa por} \quad a \cdot x := \sum_{g \in G} a_g \, \pi(g)\, x. \tag{3.5}$$

En tal caso, dícese que V es un **G-módulo**, como abreviatura de "$\mathbb{F}[G]$-módulo".

Cualquier operador lineal $T : V \to V$ que *conmuta* con π, en el sentido de que

$$T\, \pi(g)\, x = \pi(g)\, T(x) \quad \text{para todo} \quad g \in G,\ x \in V, \tag{3.6}$$

también respeta la acción de $\mathbb{F}[G]$, por su linealidad:

$$T(a \cdot x) = a \cdot T(x) \quad \text{para todo} \quad a \in \mathbb{F}[G],\ x \in V. \qquad ◊$$

Definición 3.42. Un **submódulo**[9] de un R-módulo (a izquierda) M es un subgrupo aditivo $N \leqslant M$ tal que $ay \in N$ para todo $a \in R$, $y \in N$.

La intersección de varios submódulos de M es otro submódulo de M. Si $S \subseteq M$, el menor submódulo de M que incluye S es la intersección $\langle S \rangle$ de todos los submódulos

[9] Se sobreentiende que el mismo anillo R actúa sobre el módulo y el submódulo. En caso de duda, se puede decir que N es un **R-submódulo** de M.

de M que incluyen S. Aquí se emplea el mismo vocabulario de la Definición 1.19: $\langle S\rangle$ es el submódulo *generado* por S; y un R-módulo es **cíclico** si está generado por un solo elemento. Si $M = \langle x_1, \ldots, x_n\rangle$ donde $S = \{x_1, \ldots, x_n\}$ es finito, dícese que M es un R-módulo **finitamente generado**.

Si N es el submódulo de M, el grupo abeliano cociente M/N es un R-módulo cociente bajo la acción $a(x+N) := ax + N$. Este es el ***R*-módulo cociente** de M por N. ◊

Definición 3.43. Un ***R*-homomorfismo** $\varphi : M \to P$ entre dos R-módulos (a izquierda) M y P es un homomorfismo de grupos abelianos tal que $\underline{\varphi(ax) = a\varphi(x)}$, para todo $a \in R$, $x \in M$. Un ***R*-isomorfismo** es un R-homomorfismo biyectivo.

Es evidente que la aplicación $\eta : M \to M/N : x \mapsto x + N$ es un R-homomorfismo.

Si $\psi : P \to Q$ es otro R-homomorfismo, la composición $\psi\varphi \equiv \psi\circ\varphi : M \to Q$ es también un R-homomorfismo. Está claro que dicha composición es asociativa.

Los R-módulos a izquierda, para un anillo fijo R, forman los objetos de una *categoría* $\underline{R\text{-Mod}}$ cuyos morfismos son estos R-homomorfismos. El conjunto $\mathrm{Hom}_R(M,P) \equiv \mathrm{Hom}_{R\text{-Mod}}(M,P)$ es un grupo abeliano, con suma $\varphi + \psi : x \mapsto \varphi(x) + \psi(x)$.

El grupo abeliano $\underline{\mathrm{End}_R(M)} \equiv \mathrm{Hom}_R(M,M)$ es el *anillo* de los ***R*-endomorfismos** de M; su producto es la composición de R-homomorfismos. ◊

Del mismo modo se puede definir R-homomorfismos entre R-módulos a derecha: son las aplicaciones aditivas que cumplen $\underline{\varphi(xa) = \varphi(x)a}$, para $a \in R$, $x \in M$. Así se forma la categoría $\underline{\text{Mod-}R}$ de R-módulos a derecha, cuyos conjuntos de morfismos también se denotan por $\mathrm{Hom}_R(M,P)$, confiando en el contexto para distinguir los dos casos.

► El **núcleo** de un R-homomorfismo $\psi : M \to P$ es $\ker\psi := \{x \in M : \psi(x) = 0\}$. El "primer teorema de isomorfía" para R-módulos es análogo al caso de los grupos.

Proposición 3.44. *Sea $\varphi : M \to P$ un R-homomorfismo de R-módulos a izquierda. Entonces $M/\ker\varphi \simeq \varphi(M)$ en la categoría R-*Mod.

Demostración. La aplicación $\psi : M/\ker\varphi \to \varphi(M) : x + \ker\varphi \mapsto \varphi(x)$ es un isomorfismo de grupos abelianos, por el Teorema 1.50. Además, si $a \in R$, entonces

$$a(x + \ker\varphi) = ax + \ker\varphi \overset{\psi}{\longmapsto} \varphi(ax) = a\varphi(x),$$

así que esta aplicación conmuta con la acción de R y por ende es un R-isomorfismo. □

Definición 3.45. Dados dos R-módulos a izquierda, M y N, su **suma directa** $\underline{M \oplus N}$ es el grupo abeliano $M \times N$ con suma y acción de R dadas por

$$(x,y) + (x',y') := (x + x', y + y'); \qquad a(x,y) := (ax, ay)$$

para $x, x' \in M$; $y, y' \in N$; $a \in R$.

Más generalmente, si $M_1, \ldots, M_n$ son R-módulos, su suma directa $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ es el producto cartesiano de los M_j con suma y R-acción definidas entrada por entrada. $\Diamond$

Proposición 3.46. *En la categoría R-*Mod*, hay un isomorfismo $L \simeq M \oplus N$ si y sólo si hay cuatro homomorfismos*

$$M \underset{\pi_1}{\overset{\iota_1}{\rightleftarrows}} L \underset{\pi_2}{\overset{\iota_2}{\rightleftarrows}} N$$

que cumplen las siguientes igualdades:

$$\pi_1 \iota_1 = 1_M, \quad \pi_1 \iota_2 = 0, \quad \pi_2 \iota_1 = 0, \quad \pi_2 \iota_2 = 1_N, \quad \iota_1 \pi_1 + \iota_2 \pi_2 = 1_L\,. \tag{3.7}$$

Demostración. Defínase cuatro R-homomorfismos $i_1 \colon M \to M \oplus N$, $i_2 \colon M \to M \oplus N$, $p_1 \colon M \oplus N \to M$, $p_2 \colon M \oplus N \to N$ por:

$$i_1(x) := (x,0), \quad i_2(y) := (0,y), \quad p_1(x,y) := x, \quad p_2(x,y) := y.$$

Las primeras cuatro de las relaciones (3.7) son evidentes. Además, nótese que tanto $i_1 p_1$ como $i_2 p_2$ pertenecen al anillo $\mathrm{End}_R(M \oplus N)$ y por ende poseen una suma puntual:

$$(i_1 p_1 + i_2 p_2)(x,y) \equiv i_1 p_1(x,y) + i_2 p_2(x,y) = i_1(x) + i_2(y) = (x,0) + (0,y) = (x,y)$$

así que $i_1 p_1 + i_2 p_2 = 1_M$ en el anillo $\mathrm{End}_R(M \oplus N)$.

Más generalmente, si hay un R-isomorfismo $\theta : M \oplus N \to L$, entonces los R-homomorfismos $\iota_1 := \theta\, i_1$, $\iota_2 := \theta\, i_2$, $\pi_1 := p_1 \theta^{-1}$, $\pi_2 := p_2 \theta^{-1}$ cumplen las relaciones (3.7).

Por otro lado, dados R-homomorfismos ι_1, ι_2, π_1, π_2 que satisfacen (3.7), defínase

$$\theta := i_1 \pi_1 + i_2 \pi_2 : L \to M \oplus N, \qquad \lambda := \iota_1 p_1 + \iota_2 p_2 : M \oplus N \to L.$$

Sus composiciones son R-endomorfismos: $\lambda\theta \in \mathrm{End}_R(L)$ mientras $\theta\lambda \in \mathrm{End}_R(M \oplus N)$. De las relaciones (3.7), se obtiene

$$\begin{aligned} \lambda\theta &= \iota_1 p_1 i_1 \pi_1 + \iota_1 p_1 i_2 \pi_2 + \iota_2 p_2 i_1 \pi_1 + \iota_2 p_2 i_2 \pi_2 = \iota_1 \pi_1 + \iota_2 \pi_2 = 1_L, \\ \theta\lambda &= i_1 \pi_1 \iota_1 p_1 + i_2 \pi_2 \iota_1 p_1 + i_1 \pi_1 \iota_2 p_2 + i_2 \pi_2 \iota_2 p_2 = i_1 p_1 + i_2 p_2 = 1_{M \oplus N}, \end{aligned}$$

lo cual dice que θ es un R-isomorfismo con inverso $\theta^{-1} = \lambda$; así que $L \simeq M \oplus N$. $\square$

Corolario 3.47. *Si M y N son R-submódulos de un R-módulo K tales que $M \cap N = 0$, la suma (ordinaria) $\underline{M+N} := \{\, x+y \in K : x \in M,\ y \in N \,\}$ es isomorfo a $M \oplus N$.*

Demostración. Sean $\iota_1 : M \to M+N$, $\iota_2 : N \to M+N$ las inclusiones de R-módulos.

Para definir R-homomorfismos π_1 y π_2 que cumplen (3.7) en el caso $L = M+N$, fíjese que cada elemento de $M+N$ se escribe como $x+y$ con $x \in M$, $y \in N$ *de manera única*. En efecto, si $x' \in M$, $y' \in N$ con $x'+y' = x+y$, entonces $x'-x = y-y'$ en K; esta diferencia queda en $M \cap N$, así que $x'-x = y-y' = 0$; por tanto, $x' = x$, $y' = y$.

Las proyecciones $\pi_1(x+y) := x$, $\pi_2(x+y) := y$ ahora están bien definidas y se verifican las primeras cuatro relaciones de (3.7). Además,

$$(\iota_1 \pi_1 + \iota_2 \pi_2)(x+y) = \iota_1(x) + \iota_2(y) = x+y,$$

de modo que $\iota_1 \pi_1 + \iota_2 \pi_2 = 1_{M+N}$ y por ende $M+N \simeq M \oplus N$. □

Definición 3.48. Sea M un R-módulo a izquierda. Dícese que M es **irreducible** si los únicos submódulos de M son los submódulos triviales $\{0\}$ y M.

Una representación de grupo $\pi : G \to GL(V)$ sobre un espacio $\mathbb{F}$-vectorial V se llama irreducible si V es irreducible como $\mathbb{F}[G]$-módulo a izquierda. ◊

Proposición 3.49 (Lema de Schur)**.** *Si un R-módulo a izquierda M es irreducible, entonces* $\mathrm{End}_R(M)$ *es un anillo de división.*

Demostración. Sea $\psi : M \to M$ un R-homomorfismo *no cero*; entonces $\ker\psi$ resulta ser un R-submódulo de M que no es todo M, así que $\ker\psi = \{0\}$. Además, la imagen $\mathrm{im}\,\psi = \psi(M)$ es un R-submódulo de M que no es nulo, así que $\psi(M) = M$. Se concluye que ψ es inyectivo y sobreyectivo; en otras palabras, ψ es un *R-isomorfismo* y por ende posee un inverso ψ^{-1} en el anillo $\mathrm{End}_R(M)$. □

Corolario 3.50. *Si $\pi : G \to GL(V)$ es una representación* irreducible *de un grupo sobre un espacio vectorial* complejo *V, cualquier operador lineal $T : V \to V$ que conmuta con la representación es necesariamente un operador* escalar: *$T = \lambda\, 1_V$ para algún $\lambda \in \mathbb{C}$.*

Demostración. Sea R el subanillo de $\mathrm{End}_{\mathbb{C}}(V)$ que consta de los operadores T que conmutan con π, es decir, cumplen (3.6). Cada $T \in R$ satisface, por linealidad:

$$T(a \cdot x) = a \cdot T(x) \quad \text{para todo} \quad a \in \mathbb{C}[G],\ x \in V,$$

En otras palabras, T es un $\mathbb{F}[G]$-*homomorfismo*. Esto muestra que $R = \mathrm{End}_{\mathbb{C}[G]}(V)$.

Si π es irreducible —es decir, si V es irreducible como $\mathbb{C}[G]$-módulo, entonces R es un anillo de división. Cualquier $T \in R$ posee[10] un autovalor $\lambda \in \mathbb{C}$. El operador lineal $T - \lambda\, 1_V$ pertenece a R y no es inyectivo: $\ker(T - \lambda\, 1_V)$ es el subespacio de autovectores para λ. Se concluye que $T - \lambda\, 1_V = 0$, es decir, $T = \lambda\, 1_V$. □

[10] Un autovalor de T es una raíz del polinomio característico $p_T(x)$. Con el uso de escalares *complejos*, se garantiza la existencia de al menos un autovalor, a partir del teorema fundamental del álgebra.

► Un $\mathbb{Z}$-módulo es simplemente un grupo abeliano (Ejemplo 3.38). Es hora de examinar en más detalle la estructura de grupos abelianos con un número finito de generadores.

Proposición 3.51. *Un grupo abeliano finitamente generado es una suma directa de un número finito de subgrupos cíclicos.*

Demostración. Sea $n \in \mathbb{P}$ el menor entero positivo tal que haya un juego de n elementos que genera A como grupo abeliano, es decir, $A = \langle u_1, u_2, \ldots, u_n \rangle$. Cada elemento de A es una suma $\sum_{j=1}^{n} m_j u_j$ con $m_1, \ldots, m_n \in \mathbb{Z}$. Se demuestra el resultado por inducción sobre n.

Si $\sum_{j=1}^{n} m_j u_j = 0$ implica $m_k u_k = 0$ para cada k, entonces $A \simeq \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \cdots \oplus \langle u_n \rangle$ es una suma directa de grupos cíclicos.

En cualquier otro caso, debe haber algunos $m_1, \ldots, m_n \in \mathbb{Z}$ tales que $\sum_{j=1}^{n} m_j u_j = 0$ pero $m_k u_k \neq 0$ para algún k. Al reordenar $\{u_1, \ldots, u_n\}$ si fuera necesario, se puede suponer que $\sum_{j=1}^{n} m_j u_j = 0$, $m_1 u_1 \neq 0$, $m_1 > 0$; y que $m_1 \in \mathbb{P}$ es el menor entero positivo con estas propiedades.

Si $\sum_{j=1}^{n} l_j u_j = 0$ en A, hay enteros q, s tales que $l_1 = q m_1 + s$ con $s \in \{0, 1, \ldots, m_1 - 1\}$; luego $s u_1 + (l_2 - q m_2) u_2 + \cdots + (l_2 - q m_2) u_2 = 0$. Entonces $s = 0$ por la minimalidad de m_1; se concluye que m_1 divide l_1.

Resulta que m_1 divide $m_2, \ldots, m_n$ también: pues si $m_2 = q_2 m_1 + t$ con $0 \leqslant t < m_1 - 1$, entonces $t u_2 + m_1(u_1 + q_2 u_2) + m_3 u_3 + \cdots + m_n u_n = 0$. Como $A = \langle u_2, u_1 + q_2 u_2, u_3, \ldots, u_n \rangle$, la minimalidad de m_1 conlleva $t = 0$; por lo tanto, m_1 divide m_2. Se obtiene $m_k = q_k m_1$ para $k = 3, \ldots, n$ de modo similar.

Tómese $v_1 := u_1 + \sum_{j=2}^{n} q_j u_j$ y considérese el subgrupo $B := \langle u_2, \ldots, u_n \rangle$. Está claro que $\langle v_1, u_2, \ldots, u_n \rangle = A$, así que $A = \langle v_1 \rangle + B$. Los cálculos anteriores implican que $m_1 v_1 = \sum_{j=1}^{n} m_j u_j = 0$.

Un elemento de $\langle v_1 \rangle \cap B$ tiene la forma $l_1 v_1 = l_2 u_2 + \cdots + l_n u_n$ para algunos enteros l_j, así que $l_1 u_1 + \sum_{j=2}^{n} (l_1 q_j - l_j) u_j = 0$. Por lo tanto, l_1 es divisible por m_1, lo cual implica $l_1 v_1 = 0$. Se ha comprobado que $A = \langle v_1 \rangle \oplus B$. Como B está generado por $(n-1)$ elementos, la hipótesis inductiva dice que $B = \langle v_2 \rangle \oplus \cdots \oplus \langle v_n \rangle$ para algunos $v_2, \ldots, v_n \in B$. Se concluye que $A = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_n \rangle$. □

En la demostración anterior, la condición $m_1 v_1 = 0$ implica que $\langle v_1 \rangle \simeq \mathbb{Z}_{m_1}$. En consecuencia, cualquier grupo abeliano finitamente generado es la suma directa de grupos cíclicos finitos $T = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ (con $k \in \{0, 1, \ldots, n\}$) y otros $(n - k)$ grupos cíclicos infinitos $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \simeq \mathbb{Z}^{n-k}$. En la descomposición $A = T \oplus \mathbb{Z}^{n-k}$, el **subgrupo de torsión** T está compuesto de todos los elementos de período finito en A.

El subgrupo T es finito. Si $|T| = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$, entonces (por los teoremas de Lagrange y Sylow) se obtiene $T \simeq T_1 \oplus \cdots \oplus T_k$ donde cada P_j es el p_j-subgrupo de Sylow de T.

Si P es un p-grupo abeliano finito de orden p^r, la Proposición 3.51 muestra que que $P = P_1 \oplus \cdots \oplus P_q$ donde cada P_i es un grupo cíclico de orden p^{r_i}, con $r_1 \geqslant r_2 \geqslant \cdots \geqslant r_q$. En la notación de la demostración anterior, resulta que $m_1 = p^{r-r_1}$.

Las potencias de primos p^{r_i} que son ordenes de un componente cíclico de un grupo abeliano finito A se llaman **invariantes** del grupo abeliano. Un grupo abeliano finitamente generado está determinado, hasta isomorfismo, por el rango $(n-k)$ de su componente libre abeliano $\mathbb{Z}^{n-k}$ y por los invariantes de su subgrupo de torsión. En general, el número n de componentes en la suma directa se llama el **rango** del grupo abeliano.

Ejemplo 3.52. Los grupos abelianos de rango 2 son los siguientes: $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$; $\mathbb{Z}_{p^i} \oplus \mathbb{Z}$; $\mathbb{Z}_{p^i} \oplus \mathbb{Z}_{q^k}$; $\mathbb{Z}_{p^i} \oplus \mathbb{Z}_{p^j}$; donde p, q son números primos distintos y i, j, k son enteros positivos con $i \geqslant j$.

Hay exactamente cinco grupos abelianos no isomorfos de orden 16. Ellos son $\mathbb{Z}_{16}$; $\mathbb{Z}_8 \oplus \mathbb{Z}_2$; $\mathbb{Z}_4 \oplus \mathbb{Z}_4$; $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$; y $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. En notación multiplicativa, estos serían C_{16}; $C_8 \times C_2$; $C_4 \times C_4$; $C_4 \times C_2 \times C_2$; y $C_2 \times C_2 \times C_2 \times C_2$. ◊

3.5 Polinomios y su factorización

En esta sección, todos anillo R será *conmutativo*.

Si R es un anillo conmutativo cualquiera, la notación $R[x]$ denota el anillo de polinomios (en un indeterminado x) con coeficientes en R. Más generalmente, con los mismos coeficientes se puede formar un anillo $R[x_1, \ldots, x_m]$ en m indeterminados x_j, cuyos elementos son sumas finitos de *monomios* de la forma $a\, x_1^{r_1} x_2^{r_2} \ldots x_m^{r_m}$ con $a \in R$. La notación presupone la regla $x_j x_k = x_k x_j$ para $j, k = 1, \ldots, m$, y por lo tanto este anillo de polinomios es también conmutativo.

Proposición 3.53. *Sea $\varphi : R \to S$ un homomorfismo entre dos anillos conmutativos y sean $b_1, \ldots, b_m \in S$. Entonces existe un único homomorfismo $\Phi : R[x_1, \ldots, x_m] \to S$ tal que $\Phi|_R = \varphi$ y $\Phi(x_j) = b_j$ para $j = 1, \ldots, m$.*

Demostración. Si $m > 1$, entonces $R[x_1, \ldots, x_m] = \widetilde{R}[x_m]$, donde $\widetilde{R} := R[x_1, \ldots, x_{m-1}]$. Luego, por inducción sobre m, basta demostrar el caso $m = 1$.

Dado un elemento $b \in S$, las condiciones $\Phi(a) = \varphi(a)$ para $a \in R$ y $\Phi(x) = b$ determinan un homomorfismo $\Phi : R[x] \to S$ por la siguiente receta:

$$\Phi(a_0 + a_1 x + \cdots + a_n x^n) = \varphi(a_0) + \varphi(a_1)\, b + \cdots + \varphi(a_n) b^n,$$

lo cual comprueba la unicidad de Φ. Por otro lado, al aplicar esta receta al producto (3.1) de dos polinomios, se obtiene $\Phi\big(p(x)q(x)\big) = \Phi(p(x))\Phi(q(x))$. Como Φ es obviamente aditivo y $\Phi(1) = \varphi(1) = 1$, se concluye que Φ es un homomorfismo de anillos. □

En particular, si R es un subanillo de otro anillo conmutativo S y si $b \in S$, la inclusión $\iota : R \hookrightarrow S$ es un homomorfismo con una extensión $E : R[x] \to S$ determinada por $x \mapsto b$. Denótese por $R[b]$ el subanillo de S generado por el conjunto $R \cup \{b\}$. Resulta que $R[b] = E(R[x]) \simeq R[x]/\ker E$ por la Proposición 3.24. En el caso $S = R$, donde $b \in R$, el homomorfismo $E : R[x] \to R$ lleva un polinomio $p(x)$ en un elemento $\underline{p(b)} \in R$: este es el **homomorfismo de evaluación** en b de polinomios.[11]

Definición 3.54. Un polinomio no nulo $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ es **mónico** si su coeficiente delantero[12] es 1, es decir, si $a_n = 1$. ◊

Proposición 3.55. *Sean $p(x)$ y $d(x)$ son dos polinomios en $R[x]$. Supóngase que $d(x)$ mónico; entonces hay un único par de polinomios $q(x), r(x) \in R[x]$ tales que*

$$p(x) = d(x)\,q(x) + r(x), \quad \textit{con} \quad \begin{cases} \operatorname{gr} r(x) < \operatorname{gr} d(x) \\ \textit{o bien} \;\; r(x) = 0. \end{cases} \tag{3.8}$$

Demostración. Sean $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ y $d(x) = b_0 + b_1 x + \cdots + b_{m-1} x^{m-1} + x^m$. Si $m = 0$, entonces $d(x) = 1$ y la solución es trivial y única: $d(x) = p(x)$, $r(x) = 0$. Supóngase que $m > 0$.

Si $p(x) = a_0$ es un polinomio constante, la única solución es $d(x) = 0$, $r(x) = a_0$. Si $m > n$, la única solución es $q(x) = 0$, $r(x) = p(x)$. Supóngase que $m \leqslant n$.

Se procede ahora por inducción sobre n. Nótese que

$$p(x) - a_n\, x^{n-m}\, d(x) =: p_1(x)$$

es un polinomio con $\operatorname{gr} p_1(x) < n$. Luego se puede asumir que $p_1(x) = q_1(x)d(x) + r_1(x)$, con $\operatorname{gr} r_1(x) < m$ o bien $r_1(x) = 0$. Entonces

$$p(x) = \big(a_n\, x^{n-m} + q_1(x)\big)d(x) + r_1(x),$$

y el resultado (3.8) sigue por la inducción sobre n.

Para comprobar la unicidad de $q(x)$ y $r(x)$, obsérvese que si $q(x)d(x) + r(x) = \tilde{q}(x)d(x) + \tilde{r}(x)$, entonces $\big(q(x) - \tilde{q}(x)\big)d(x) = \tilde{r}(x) - r(x)$. Si los dos lados de esta ecuación no se anulan, el lado izquierdo tendría grado $\geqslant m$, mientras al lado derecho el grado sería $< m$, lo cual es imposible. Por lo tanto, $\tilde{r}(x) = r(x)$ y $\big(q(x) - \tilde{q}(x)\big)d(x) = 0$. Al lado izquierdo, si fuera $q(x) \neq \tilde{q}(x)$ el grado total sería $\operatorname{gr}(q - \tilde{q}) + m \geqslant m$, imposible para el polinomio nulo; se concluye que $\tilde{q}(x) = q(x)$ también. □

[11] En virtud de la existencia de este homomorfismo, es legítimo considerar $p \equiv p(x)$ como una *función* que toma valores en el anillo R: el valor de esta función en $b \in R$ es el elemento $p(b)$ obtenido por sustitución de b en lugar del indeterminado x. Sin embargo, fíjese bien que $p(x)$ no es un valor de dicha función, porque $x \notin R$.

[12] Otros autores lo llaman el "primer coeficiente" o el "coeficiente principal".

Fíjese que si en la última proposición el anillo R es *entero*, entonces $R[x]$ también lo es (véase la Definición 3.34) y no hace falta contar grados para mostrar que $(q-\tilde{q})d = 0$, con d mónico, implica $q - \tilde{q} = 0$.

► Si el *polinomio divisor* $d(x)$ tiene grado $m = 1$, de modo que $d(x) = x - a$ con $a \in R$, el resultado (3.8) toma la forma

$$p(x) = (x-a)\,q(x) + r \quad \text{con} \quad r = p(a) \in R.$$

La fórmula $p(x) = (x-a)\,q(x)+p(a)$ se conoce popularmente como el *teorema del residuo*. Un corolario evidente es que $(x-a)$ divide el polinomio $p(x)$ sin residuo si y sólo si $p(a) = 0$ en R. Este corolario se conoce como el *teorema del factor*.

Definición 3.56. Una **raíz** de un polinomio $p(x) \in R[x]$ es un elemento $a \in R$ tal que $p(a) = 0$. Por lo que se ha dicho, a cada raíz a de $p(x)$ le corresponde un factor de primer grado $(x-a)$ de ese polinomio. Fíjese que si $p(x) = (x-a)\,q(x)$, cabe la posibilidad de que a también fuera una raíz de $q(x)$, en cuyo caso $p(x) = (x-a)^2\,q_2(x)$ para algún polinomio $q_2(x) \in R[x]$. Dícese que la **multiplicidad** de una raíz a de $p(x)$ es el mayor entero positivo $m \in \mathbb{P}$ tal que $(x-a)^k$ sea un factor de $p(x)$. Dado un polinomio $p(x)$, es costumbre *contar sus raíces con multiplicidad*, es decir, una raíz de multiplicidad m puede ser considerada como un juego de m raíces "que coinciden". ◊

Proposición 3.57. *Si $p(x) \in R[x]$ es un polinomio de grado n, entonces tiene a lo sumo n raíces en R, contados con multiplicidad.*

Demostración. Nótese que $p(x)$ no es el polinomio nulo, el cual no posee grado alguno. Si $a_1, \ldots, a_k \in R$ son raíces *distintas* en R, con multiplicidades respectivas $m_1, \ldots, m_k \in \mathbb{P}$, entonces al aplicar la Proposición 3.55 unas k veces, se obtiene

$$p(x) = (x-a_1)^{m_1}(x-a_2)^{m_2}\cdots(x-a_k)^{m_k}q_k(x)$$

para algún polinomio no nulo $q_k(x) \in R[x]$. Como los grados de un producto de polinomios se suman, se obtiene

$$m_1 + m_2 + \cdots + m_k = \operatorname{gr} p(x) - \operatorname{gr} q_k(x) \leqslant n - \operatorname{gr} q_k(x) \leqslant n.$$

En consecuencia, $k \leqslant m_1 + m_2 + \cdots + m_k \leqslant n$: el número de raíces distintas es finito y no excede n. Si $\{a_1, \ldots, a_k\}$ resulta ser el conjunto de *todas* las raíces distintas de $p(x)$, entonces $m_1 + m_2 + \cdots + m_k$ es el número total de raíces *contados con multiplicidad*, el cual es menor o igual que n. □

Corolario 3.58. *Si $\mathbb{F}$ es un cuerpo finito, el grupo multiplicativo $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ es cíclico.*

Demostración. Sea $q := |\mathbb{F}|$; entonces $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ es un grupo finito de orden $q-1$. Sea m el *exponente* de este grupo abeliano finito: el menor entero positivo tal que $a^m = 1$ para todo $a \in \mathbb{F}^\times$. Obviamente $m \leqslant q-1$; de hecho, m divide $q-1$, por el teorema de Lagrange.

Por otro lado, el polinomio $x^m - 1 \in \mathbb{F}[x]$ posee $q-1$ raíces no nulos y distintos: en efecto, todos los elementos de $\mathbb{F}^\times$ son raíces de este polinomio. De la Proposición 3.57 se obtiene $q-1 \leqslant m$. Se deduce que el exponente de $\mathbb{F}^\times$ es $q-1$.

Si la factorización prima de este exponente es $q-1 = p_1^{m_1} \dots p_k^{m_k}$, la Proposición 3.51 muestra que $\mathbb{F}^{m_1} \simeq P_1 \times \cdots \times P_k$ es un producto directo de sus subgrupos de Sylow; y que cada P_j es un p_j-grupo abeliano de exponente $p_j^{m_j}$, así que $P_j \simeq C_{p_j^{m_j}}$. Si $a_j \in \mathbb{F}^\times$ es un generador de P_j, entonces $a := a_1 \dots a_k$ es un elemento de período $q-1$, y por ende $\mathbb{F}^\times = \langle a \rangle$ es un grupo cíclico multiplicativo. □

► De la fórmula (3.8) se obtiene un proceso algorítmico conocido como la "división larga" de polinomios, análogo a la división de números enteros con cociente y residuo.

Definición 3.59. Si cada ideal en un anillo conmutativo R es un ideal principal, dícese que R es un **anillo principal**. ◊

Proposición 3.60. *Si $\mathbb{F}$ es un cuerpo, entonces el anillo de polinomios $\mathbb{F}[x]$ es un anillo entero principal.*

Demostración. Sea I un ideal no nulo de $\mathbb{F}[x]$ y sea $d(x)$ un polinomio no nulo de grado mínimo en I. Sin perder generalidad, se puede suponer que $d(x)$ es mónico; porque si su coeficiente delantero es $b_m \neq 1$, se puede reemplazar $d(x)$ por $b_m^{-1} d(x)$.

Si $p(x) \in I \setminus \{0\}$, la fórmula $p(x) = d(x)q(x) + r(x)$ muestra que $r(x) = p(x) - d(x)q(x) \in I$; como $\operatorname{gr} r < \operatorname{gr} d$ no es posible, entonces $r(x) = 0$ necesariamente. Se deduce que $p(x) = d(x)q(x)$. En consecuencia, $I = (d(x))$ es un ideal principal: cualquier polinomio en I es un múltiplo de $d(x)$. □

Para continuar con la analogía entre $\mathbb{F}[x]$ y $\mathbb{Z}$, conviene repasar las propiedades de divisibilidad de los números enteros. Si $m, n \in \mathbb{Z}$, dícese que m *divide* n, escrito $m \mid n$, si hay $q \in \mathbb{Z}$ tal que $n = qm$. Las propiedades esenciales para que $k \in \mathbb{Z}$ sea un **máximo común divisor** de m y n son:

$$k \mid m,\ k \mid n; \qquad \text{y si } t \mid m,\ t \mid n, \text{ entonces } t \mid k. \tag{3.9}$$

Si además se exige $k > 0$, entonces k es único: este es *el* máximo común divisor de m y n; se escribe $k = \underline{\mathrm{mcd}(m,n)}$.

Para *calcular* $\mathrm{mcd}(m,n)$ para dos enteros dados, se usa el **algoritmo euclidiano**.[13]

Lema 3.61. *Si $n, d \in \mathbb{P}$, entonces hay enteros únicos $q, r \in \mathbb{N}$ tales que*

$$n = qm + r, \quad con \quad 0 \leqslant r < d. \tag{3.10}$$

Demostración. Si $d > n$, tómese $q := 0$, $r := n$. En cambio, si $d \leqslant n$, la sucesión de enteros positivos $n, n-d, n-2d, \ldots$ debe terminar, en vista de la propiedad arquimediana de los enteros: debe haber $q \in \mathbb{P}$ (necesariamente único) tal que $n - qd \geqslant 0$ mientras $n-(q+1)d < 0$; tómese $r := n - qd$. □

Proposición 3.62 (Algoritmo euclidiano)**.** *Si $m, n \in \mathbb{P}$, su máximo común divisor se calcula como sigue. Defínase dos sucesiones de enteros (q_j), (r_j) así:*

$$\begin{aligned}
n &= q_1 m + r_1 && con \quad 0 < r_1 < m,\\
m &= q_2 r_1 + r_2 && con \quad 0 < r_2 < r_1,\\
r_1 &= q_3 r_2 + r_3 && con \quad 0 < r_3 < r_2,\\
\vdots &= \quad \vdots &&\\
r_{k-2} &= q_k r_{k-1} + r_k && con \quad 0 < r_k < r_{k-1},\\
r_{k-1} &= q_{k+1} r_k + 0\,. &&
\end{aligned}$$

Entonces $\mathrm{mcd}(m,n) = r_k$*, el último residuo no cero en estas divisiones. En consecuencia, se verifica la siguiente relación:*

$$\mathrm{mcd}(m,n) = am + bn \quad para\ algunos \quad a, b \in \mathbb{Z}. \tag{3.11}$$

Demostración. Para ver que $r_k \mid n$, obsérvese que

$$n = q_1 m + r_1 = q_1(q_2 r_1 + r_2) + r_1 = (q_1 q_2 + 1) r_1 + q_1 r_2.$$

Sustituyendo $m, r_1, r_2, \ldots, r_{k-2}$ uno por uno por los lados derechos que aparecen en el enunciado de la Proposición, se llega a $n = c r_{k-1} + d r_k$ para algunos $c, d \in \mathbb{Z}$, así que $n = (cq_{k+1} + d) r_k$ y por tanto $r_k \mid n$. El mismo proceso muestra que $r_k \mid m$.

Ahora, si $t \in \mathbb{N}$ satisface $t \mid m$ y $t \mid n$, entonces t divide $n - q_1 m = r_1$. En seguida, $t \mid (m - q_2 r_1) = r_2$ y así sucesivamente hasta llegar a $t \mid (r_{k-2} - q_k r_{k-1}) = r_k$. Se concluye que $r_k = \mathrm{mcd}(m,n)$.

[13] Este procedimiento está expuesto en las Proposiciones VII.1 y VII.2 de los *Elementos* de Euclides, bajo el nombre de *anthyphairesis*, la "sustracción continuada" de un número menor desde un número mayor.

Para comprobar (3.11), fíjese que $r_1 = n - q_1 m$, y que

$$r_2 = m - q_2 r_1 = m - q_2(n - q_1 m) = (q_1 q_2 + 1)m - q_2 n.$$

Al repetir el proceso, se encuentran $a_j, b_j \in \mathbb{Z}$ con $r_j = a_j m + b_j n$, para $j = 1, \ldots, k$. □

En particular, m y n son relativamente primos en $\mathbb{P}$ [escrito $m \perp n$, como antes, como sinónimo de $\mathrm{mcd}(m,n) = 1$] si y sólo si hay $a, b \in \mathbb{Z}$ tales que $am + bn = 1$.

Para extender el concepto de máximo común divisor a números enteros negativos, nótese que se pierde su unicidad; porque si k cumple las propiedades (3.9), entonces $-k$ también los cumple. Esto sucede porque -1 es una *unidad* en el anillo $\mathbb{Z}$. La divisibilidad en anillos enteros debe tomar en cuenta sus unidades.

Definición 3.63. Un **anillo euclidiano** es un anillo entero dotado con alguna función $\delta : R \setminus \{0\} \to \mathbb{N}$ con la siguiente propiedad: si $a, b \in R$ con $b \neq 0$, existen $q, r \in R$ tales que $a = qb + r$, con $r = 0$ o bien $\delta(r) < \delta(b)$. ◊

Está claro que $\mathbb{Z}$ es un anillo euclidiano, al tomar $\delta(n) := |n|$. Si $\mathbb{F}$ es un cuerpo, la Proposición 3.55 dice que $\mathbb{F}[x]$ es un anillo euclidiano, con $\delta(p(x)) := \mathrm{gr}\, p(x)$. Otro ejemplo es el anillo $\mathbb{Z}[i]$ de enteros gaussianos (Ejemplo 3.29), con $\delta(m + ni) := m^2 + n^2$.

Proposición 3.64. *Cada anillo euclidiano es un anillo entero principal.*

Demostración. Sea I un ideal no nulo en un anillo euclidiano R. La función δ, restringido a $I \setminus \{0\}$, toma valores en $\mathbb{N}$ y alcanza su mínimo en algún $b \in I$, con $b \neq 0$. Si $c \in I$, hay $q, r \in R$ con $c = qb + r$. La opción $\delta(r) < \delta(b)$ está excluida por la minimalidad de $\delta(b)$, puesto que $r = c - qb \in I$; esto implica que $r = 0$. En resumen, todo $c \in I$ cumple $c = qb$ para algún $q \in R$, lo cual dice que $I = (b)$. Por lo tanto, todo ideal en R es un ideal principal. □

En particular, el anillo $\mathbb{F}[x]$ de polinomios sobre un *cuerpo* $\mathbb{F}$ es un anillo entero principal.

Los conceptos siguientes tienen especial importancia en anillos de polinomios en un solo indeterminado.

Definición 3.65. Sea R un anillo entero. Dados dos elementos $a, b \in R$, dícese que a **divide** b [y que b es un *múltiplo* de a] si $b = ac$ para algún $c \in R$; se escribe $a \mid b$ en ese caso. Es trivial que $a \mid 0$ para todo $a \in R$; y $u \mid 1$ si y sólo si u es una *unidad* en R.

Dícese que dos elementos no nulos $a, b \in R$ son **asociados** si $a \mid b$ y $b \mid a$. Fíjese que $au = b$, $bv = a$ implica $auv = a$ y por consiguiente $uv = 1$, por cancelación en el anillo entero R. Luego a y b son asociados si y sólo si $au = b$ para alguna unidad $u \in R^\times$.

Un elemento $b \in R \setminus \{0\}$ se llama **irreducible** si no es una unidad y si $b = ac$ sólo si uno de a y c es una unidad; es decir, *b no posee una factorización propia* como producto de dos elementos que no son unidades de R.

Un **máximo común divisor** para dos elementos $a, b \in R \setminus \{0\}$ es un elemento no nulo $d \in R$ que satisface la generalización de (3.9):

$$d \mid a,\ d \mid b; \quad \text{y si} \quad c \mid a \text{ y } c \mid b, \text{ entonces } c \mid d. \tag{3.12}$$

Un máximo común divisor, *si existe*, generalmente no es único: porque si $d \in R \setminus \{0\}$ cumple (3.12) y si u es una unidad en R, entonces ud también lo cumple. Por otro lado, es obvio que si d_1 y d_2 tienen esta propiedad, entonces $d_1 \mid d_2$ y $d_2 \mid d_1$, de modo que d_1 y d_2 son asociados. ◊

En el anillo de polinomios $\mathbb{F}[x]$, las unidades son los polinomios constantes no nulos: $\mathbb{F}[x]^\times = \mathbb{F}^\times$. En ese caso es posible eliminar la ambigüedad en la definición del máximo común divisor $d(x)$ de dos polinomios $p(x)$ y $q(x)$ al agregar el requisito de que $d(x)$ sea un polinomio *mónico*.

Proposición 3.66. *Si R es un anillo entero principal, cada par de elementos $a, b \in R \setminus \{0\}$ posee un máximo común divisor, de la forma*

$$d = as + bt, \quad \textit{para algunos} \quad s, t \in R.$$

Demostración. El conjunto $J := \{ ap + bq : p, q \in R \}$ no es otra cosa que el ideal generado por los elementos a y b; es decir, $J = (a, b)$. Como R es un anillo principal, este ideal es también principal, así que hay un elemento $d = as + bt \in R$ tal que $J = (d)$. Cada elemento de J, en particular a y b, es un múltiplo de d.

Por otro lado, si $c \mid a$ y $c \mid b$, existen $h, k \in R$ tales que $a = ch$ y $b = ck$. Entonces $d = as + bt = chs + ckt = c(hs + kt)$, y por ende $d \mid c$. Luego, d es un máximo común divisor de a y b. □

Nótese que esta proposición, aplicada al anillo $\mathbb{Z}$, expresa el máximo común divisor en la forma conocida: $\mathrm{mcd}(a, b) = am + bn$ para algunos $m, n \in \mathbb{Z}$. Como dos máximos comunes divisores son asociados, lo cual dice que $d_1 = \pm d_2$ en el caso de $\mathbb{Z}$, se logra unicidad al pedir que $\mathrm{mcd}(a, b)$ sea *positiva*.

Definición 3.67. En un anillo entero R, un elemento $a \notin R^\times$ admite una **factorización** si hay irreducibles $p_1, \ldots, p_n$ cuyo producto es a, de modo que $a = p_1 p_2 \cdots p_n$. Dado un juego de unidades $u_1, \ldots, u_n \in R^\times$, los elementos $p'_j := u_j p_j$ también son irreducibles; y $a = p'_1 p'_2 \cdots p'_n$ toda vez que $u_1 u_2 \cdots u_n = 1$. Además, como R es conmutativo, siempre

resulta posible permutar el orden de los factores p_j. Por estas razones, la factorización de a no puede ser estrictamente única.

Dícese que la factorización de a es *esencialmente única* si no hay más posibilidades: dadas dos factorizaciones en irreducibles $a = p_1 p_2 \cdots p_n = p'_1 p'_2 \cdots p'_n$, hay una permutación $\sigma \in S_n$ y un juego de unidades $u_1, \ldots, u_n$ tales que $p'_j = u_j p_{\sigma(j)}$ y $u_1 u_2 \cdots u_n = 1$.

Un anillo entero R se llama **factorial** si cada elemento $a \in R \setminus R^\times$ admite una factorización esencialmente única. También se dice, un poco incorrectamente, que R es un *anillo con factorización única*. ◊

Ejemplo 3.68. El anillo entero $R = \mathbb{Z}[\sqrt{-5}]$ *no es* factorial. El elemento 6 no es una unidad y admite dos factorizaciones esencialmente distintos,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Para ver que estos factores son irreducibles, considérese la *norma* $N(z) := z\bar{z}$ de un número complejo (compárese el Ejemplo 3.13). Nótese que $N(ab) = N(a)N(b)$ y que $N(m + n\sqrt{-5}) = m^2 + 5n^2 \in \mathbb{P}$ si $m + n\sqrt{-5} \neq 0$. Entonces $m + n\sqrt{-5}$ es una unidad en R si sólo si su norma es 1; por lo tanto, $R^\times = \{1, -1\}$ en este caso. Ahora $N(2) = 4$, $N(3) = 9$, $N(1 \pm \sqrt{-5}) = 26$. Una factor no trivial de 2, 3 o $1 \pm \sqrt{-5}$ debe tener norma 2, 3 o 13, pero estos enteros positivos no son de la forma $m^2 + 5n^2$. Por lo tanto, 2, 3 y $1 \pm \sqrt{-5}$ son irreducibles en $\mathbb{Z}[\sqrt{-5}]$. ◊

Definición 3.69. En un anillo entero R, un elemento $p \in R \setminus R^\times$ es **primo** si

$$p \mid ab \implies p \mid a \quad \text{o bien} \quad p \mid b. \qquad \text{◊}$$

Está claro que *un elemento primo es irreducible*. En efecto, si p es primo y si $p = ac$, entonces $p \mid a$ o $p \mid c$; sin perder generalidad, se puede asumir que $p \mid a$, así que $a = pb$ para algún $b \in R$. Ahora $p = pbc$; y por cancelación, $bc = 1$, así que c es una unidad y por tanto la factorización $p = ac$ no es propia.

Proposición 3.70. *(a) En un anillo entero principal, cada elemento irreducible es primo.*

(b) Un anillo entero principal es factorial.

Demostración. Sea R un anillo entero principal.

Ad (a): Sea $p \in R$ irreducible y supóngase que $p = ab$ en R. Si $p \nmid a$, entonces 1 es un máximo divisor de a y p; por la Proposición 3.66, hay $s, t \in R$ con $as + pt = 1$. Entonces $b = abs + bpt = p(s + bt)$ así que $p \mid b$.

Ad (b): Sea R un anillo entero principal. Si $a \in R$ no es una unidad, entonces a es irreducible, o bien $a = a_1 b_1$ es una factorización propia de a. En el segundo caso, a_1 es

irreducible o bien $a_1 = a_2 b_2$ es una factorización propia. Continuando así, en el k-ésimo paso se obtiene $a = a_k b_1 b_2 \dots b_k$, donde $a_1 \mid a$, $a_2 \mid a_1$, …, $a_k \mid a_{k-1}$; etcétera. Esto da lugar a una *cadena ascendente de ideales*,

$$(a) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_k) \subseteq \cdots$$

cuya unión es también un ideal de R, que debe ser un ideal principal: $\uparrow\bigcup_k (a_k) = (e)$ para algún $e \in R$. El elemento e pertenece a uno de los ideales de la cadena: hay $m \in \mathbb{P}$ con $e \in (a_m)$. Se ve que entonces $(a_k) = (e)$ para todo $k \geqslant m$: la cadena ascendente debe terminar.[14]

Entonces $a = p_1 c_1$ donde $p_1 := a_m$ es irreducible y $c_1 = b_1 b_2 \dots b_m$. Si c_1 no es irreducible, de igual modo se obtiene un irreducible p_2 tal que $c_1 = p_2 c_2$. Continuando así, se obtiene otra cadena ascendente de ideales,

$$(c_1) \subseteq (c_2) \subseteq \cdots \subseteq (c_k) \subseteq \cdots$$

que también debe terminar. Se ha mostrado que existe una cantidad finita de irreducibles $p_1, \dots, p_n$ tales que $a = p_1 p_2 \cdots p_n$.

Para ver que esta factorización es esencialmente única, considérese otra manera de expresar a como producto de irreducibles, $a = p'_1 p'_2 \cdots p'_m$. Como p'_1 es primo, por la parte (a) de la demostración, p'_1 divide alguno de los p_j. Reordenando el producto si fuera necesario, se puede suponer que $p'_1 \mid p_1$. Luego $p_1 = u_1 p'_1$ donde u_1 es una unidad.

Si $n > 1$, sea $b := p_2 \cdots p_n \notin R^\times$. Entonces $a = u_1 p'_1 b = p'_1 p'_2 \cdots p'_m$, y por cancelación, $b = p_2 \cdots p_n = u_1^{-1} p'_2 \cdots p'_m$. El argumento anterior muestra que (al reordenar $p'_2, \dots, p'_m$) hay una unidad u_2 tal que $p_2 = u_2 p'_2$; etcétera. Si fuera $m < n$, en m pasos se descubriría que $p_{m+1} \cdots p_n \in R^\times$, contrario a hipótesis; igual sucede si $n < m$. Luego $m = n$ y hay unidades u_j tales que $p_j = u_j p'_j$ para $j = 1, \dots, n$, hasta una posible permutación del orden de los p'_j. □

Un ejemplo de un anillo factorial pero no principal es el anillo $\mathbb{Z}[x]$. Su ideal $(2, x)$ es un ideal propio que no admite un solo generador. Se verá luego, sin embargo, que $\mathbb{Z}[x]$ sí es un anillo factorial: cada polinomio en $\mathbb{Z}[x]$ es un producto de factores irreducibles con coeficientes enteros.

► En vista de la última demostración, se puede reescribir las propiedades de divisibilidad en términos de ideales. Conviene hacer un pequeño diccionario que traduce relaciones multiplicativos entre elementos en comparación de ideales en un anillo entero.

[14] Se ha mostrado que un anillo entero principal satisface la siguiente condición: *cada cadena ascendente de ideales termina en un número finito de pasos*.

Definición 3.71. Sea R un anillo conmutativo y sea P un ideal de R. Dícese que P es un **ideal primo** si R/P es un anillo entero.

Dicho de otra manera, un ideal P es primo si y sólo si $ab \in P \implies a \in P$ o $b \in P$. ◊

En $\mathbb{Z}[\sqrt{-5}]$, el ideal principal $(2) = \{\, 2m + 2n\sqrt{-5} : m, n \in \mathbb{Z} \,\}$ no es primo, porque $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 \in (2)$ pero $1 \pm \sqrt{-5} \notin (2)$.

Ahora sea R un anillo entero. Lo que sigue es un mini-diccionario de conceptos.

Relaciones entre elementos	*Comparación de ideales*
u es una unidad	$(u) = R$
a divide b	$(b) \subseteq (a)$
a divide b propiamente	$(b) \subset (a) \subset R$
a y b son asociados	$(b) = (a)$
b es irreducible	(b) es un ideal maximal
p es primo	(p) es un ideal primo

► El problema clásico de factorización de polinomios consiste en la determinación de los elementos irreducibles del anillo $\mathbb{Z}[x]$ y la descomposición de un polinomio dado en un producto de irreducibles. Este anillo resulta ser factorial pero no principal. En la discusión que sigue, muchos conceptos admiten generalizaciones al caso del anillo $R[x]$ donde R es un anillo factorial.

En un anillo factorial R, un *máximo común divisor* d de un juego finito de elementos $a_1, \ldots, a_m \in R$ se define por extensión de (3.12): $d \mid a_j$ para $j = 1, \ldots, n$; y si $c \mid a_j$ para cada j, entonces $c \mid d$. La existencia de d es consecuencia de la factorización (esencialmente) única de elementos de R. En general, no hay unicidad, pero tales d son asociados entre sí. Para $R = \mathbb{Z}$, se obtiene unicidad al requerir $d > 0$; y para $R = \mathbb{F}[x]$, al requerir que d sea un polinomio mónico.

Definición 3.72. Un polinomio $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ en $\mathbb{Z}[x]$ es **primitivo** si $n > 0$, $a_n > 0$ y $\mathrm{mcd}(a_0, a_1, \ldots, a_n) = 1$. ◊

Proposición 3.73 (Lema de Gauss)**.** *El producto de dos polinomios primitivos es primitivo.*

Demostración. Sean $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ dos polinomios primitivos; su producto $f(x)\,g(x)$ es un polinomio de grado $n + m > 0$, con coeficiente delantero $a_n b_m > 0$. Falta comprobar que el máximo común divisor de los coeficientes de $f(x)\,g(x)$ es 1. Si así no fuera, habría un número primo $p \in \mathbb{P}$ que divide

cada coeficiente $c_k := \sum_{i+j=k} a_i b_j$ de $f(x)\,g(x)$. Sean a_r, b_s los primeros coeficientes de $f(x)$, $g(x)$ respectivamente que *no* son divisibles por p. Entonces

$$c_{r+s} = (a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1}) + a_r b_s + (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0),$$

en donde $p \mid a_i$ para $i = 0, \ldots, r-1$; $p \mid b_j$ para $j = 0, \ldots, s-1$ y $p \mid c_{r+s}$. Esto implica que $p \mid a_r b_s$ y en consecuencia $p \mid a_r$ o bien $p \mid b_s$, contrario a hipótesis. Por lo tanto, $c_0, c_1, \ldots, c_{n+m}$ no pueden tener un factor primo común. □

Corolario 3.74. *Sea $f(x) \in \mathbb{Z}[x]$ un polinomio con coeficientes enteros. Entonces $f(x)$ se factoriza en $\mathbb{Q}[x]$ si y sólo si se factoriza en $\mathbb{Z}[x]$.*[15]

Demostración. Después de dividir los coeficientes de $f(x)$ por factores primos comunes y multiplicarlo por (-1) si fuera necesario, se puede suponer que $f(x)$ es primitivo. Sea $f(x) = p(x)\,q(x)$ una factorización, en $\mathbb{Q}[x]$, en dos factores no constantes.

Después de calcular denominadores comunes de los coeficientes de $p(x)$ y $q(x)$ y sacar factores comunes de sus numeradores, se obtiene números enteros $a, b, c, d \in \mathbb{Z}\setminus\{0\}$ tales que $p(x) = (a/b)\,\tilde{p}(x)$ y $q(x) = (c/d)\,\tilde{q}(x)$ para dos polinomios primitivos $\tilde{p}(x)$ y $\tilde{q}(x)$ en $\mathbb{Z}[x]$. Ahora se verifica:

$$bd\,f(x) = ac\,\tilde{p}(x)\,\tilde{q}(x) \quad \text{en } \mathbb{Z}[x].$$

Al lado izquierdo, el máximo común divisor de los coeficientes es bd. Como $\tilde{p}(x)\tilde{q}(x)$ es primitivo, por la Proposición 3.73, el máximo común divisor al lado derecho es ac. Luego $bd = ac$, así que $f(x) = \tilde{p}(x)\,\tilde{q}(x)$ es una factorización de $f(x)$ en $\mathbb{Z}[x]$. □

El Lema de Gauss y su corolario admiten una generalización en donde $\mathbb{Z}$ queda reemplazado por un *anillo factorial* R cualquiera. Dícese que un polinomio en $R[x]$ es *primitivo* si su grado es positivo y cualquier máximo común divisor de sus coeficientes es una unidad en R. En la demostración de la Proposición 3.73, se ignora la condición $a_n b_m > 0$ y se reemplaza el número primo $p \in \mathbb{P}$ por un irreducible $p \in R$ que sea factor común de cada c_{r+s} (al expresar estos coeficientes como productos de irreducibles en R). Como R es un anillo entero, la condición $p \mid a_r b_s$ implica $p \mid a_r$ o bien $p \mid b_s$. El enunciado del Corolario 3.74 se generaliza como sigue, con una demostración similar.

Corolario 3.75. *Sea R un anillo factorial y sea $\mathbb{F} = \mathrm{Frac}(R)$ su cuerpo de fracciones. Un polinomio $f(x) \in R[x]$ se factoriza en $\mathbb{F}[x]$ si y sólo si se factoriza en $R[x]$.* ⊟

[15] Este corolario es el resultado demostrado originalmente por Gauss; constituye el inciso 42 en el libro: Carl Friedrich Gauß, *Disquisitiones Arithmeticæ*, Leipzig, 1801. Hay una traducción al español disponible, editado por Hugo Barrantes, Michael Josephy y Ángel Ruiz (Academia Colombiana de Ciencias, Santafé de Bogotá, 1995).

Proposición 3.76. *Si R es un anillo factorial, entonces el anillo $R[x]$ es también factorial.*

Demostración. Sea $f(x) \in R[x]$ un polinomio no nulo y sea $c \in R$ un máximo común divisor de sus coeficientes. Si $\mathbb{F} = \mathrm{Frac}(R)$, entonces $\mathbb{F}[x]$ es un anillo entero principal; por la Proposición 3.70, $f(x)$ posee una factorización esencialmente única en $\mathbb{F}[x]$. Al aplicar el corolario anterior, se puede expresar $f(x)$ como un producto

$$f(x) = p_1 p_2 \cdots p_s \, q_1(x) q_2(x) \cdots q_r(x)$$

en donde $c = p_1 p_2 \ldots p_s$ es una factorización de c en irreducibles p_i de R y los $q_j(x)$ son irreducibles y primitivos en $R[x]$.

Falta mostrar que la factorización es esencialmente única. Si $c\, q_1(x) q_2(x) \cdots q_r(x) = c' q_1'(x) q_2'(x) \cdots q_t'(x)$ son dos factorizaciones de $f(x)$ en $R[x]$ (e *ipso facto* en $\mathbb{F}[x]$), entonces tanto los $q_j(x)$ como los $q_k'(x)$ son irreducibles en $\mathbb{F}[x]$. Por factorización única en $\mathbb{F}[x]$, se obtiene $t = r$, y después de una permutación de los factores, $q_j'(x) = (a_j/b_j) q_j(x)$ para algunos $a_j/b_j \in \mathbb{F}$. Con un ajuste en el coeficiente c', se puede tomar los $q_j'(x)$ también primitivos en $R[x]$; resulta entonces que $a_j/b_j = u_j/1$ con $u_j \in R^\times$. Por lo tanto, $c' = c u_1 \cdots u_r$ y c son asociados en R: las dos factorizaciones coinciden hasta multiplicación por una unidad de R. □

Corolario 3.77. *Si $\mathbb{F}$ es un cuerpo, el anillo $\mathbb{F}[x_1, x_2, \ldots, x_n]$ es factorial.* ⊟

Ejemplo 3.78. El polinomio $p(x) = x^2 + 1$ es irreducible en $\mathbb{Z}[x]$. Tiene una factorización

$$x^2 + 1 = (x + i)(x - i)$$

en el anillo $\mathbb{Z}[i][x]$, el cual es una anillo factorial porque $\mathbb{Z}[i]$ es euclidiano. Entonces esta factorización es esencialmente única. Nótese que el grupo de unidades de $\mathbb{Z}[i]$ es $\{1, i, -1, -i\} \simeq C_4$. La factorización $1 + x^2 = (1 + ix)(1 - ix)$ no difiere esencialmente de la anterior, pues $1 + ix = i(x - i)$ y $1 - ix = -i(x + i)$. ◊

Ejemplo 3.79. El *teorema fundamental del álgebra* (no demostrada aquí) dice que cada polinomio irreducible en $\mathbb{C}[x]$ es de primer grado. La factorización única de un polinomio en $\mathbb{C}[x]$ entonces toma la forma

$$a_0 + a_1 x + \cdots + a_n x^n = a_n (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

en donde $\alpha_1, \alpha_2, \ldots, \alpha_n$ son las *raíces* del polinomio, no necesariamente distintas.

Un polinomio $f(x) \in \mathbb{R}[x]$ se factoriza de igual manera en $\mathbb{C}[x]$; y tanto los coeficientes a_i como el producto de los factores $x - \alpha_j$ son invariantes bajo conjugación compleja. Si $\alpha_j \in \mathbb{R}$, entonces $x - \alpha_j$ es un factor de $f(x)$ en $\mathbb{R}[x]$. Si $\alpha_j = b_j + i c_j$ con

$b_j, c_j \in \mathbb{R}$ pero $c_j \neq 0$, debe haber otro factor $x - \alpha_k$ en el producto con $\alpha_k = b_j - ic_j$. Entonces

$$(x-\alpha_1)(x-\alpha_2) = (x-b_j-ic_j)(x-b_j+ic_j) = x^2 - 2b_j x + (b_j^2 + c_j^2)$$

es un factor irreducible de $f(x)$, de grado 2. En consecuencia, todos los polinomios irreducibles en $\mathbb{R}[x]$ son de grado 1 o 2; cualquier polinomio de grado 3 o superior es factorizable. Por ejemplo:

$$x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2 + \sqrt{2}\,x + 1)(x^2 - \sqrt{2}\,x + 1). \qquad \Diamond$$

La factorización en $\mathbb{Z}[x]$ es más intrincada. Una variante del último ejemplo da

$$x^4 + 4 = x^4 + 4x^2 + 4 - 4x^2 = (x^2 + 2x + 2)(x^2 - 2x + 2).$$

Es fácil ver que los dos factores a la derecha son irreducibles: por el Lema de Gauss, basta buscar factores en $\mathbb{Q}[x]$; en seguida se puede hallar factores en $\mathbb{C}[x]$, mediante la fórmula cuadrática o por simple inspección:

$$x^4 + 4 = (x+1+i)(x+1-i)(x-1+i)(x-1-i).$$

Luego los factores $x^2 + 2x + 2$ son irreducibles tanto en $\mathbb{R}[x]$ como en $\mathbb{Q}[x]$.

► La dificultad esencial de la factorización en $\mathbb{Z}[x]$ es decidir si un polinomio (primitivo) dado es irreducible o no.

Si un polinomio $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ tiene un factor de primer grado en $\mathbb{Z}[x]$, entonces tiene un factor mónico $(x - r/s) \in \mathbb{Q}[x]$, con raíz $r/s \in \mathbb{Q}$ expresable como una fracción: $r, s \in \mathbb{Z}$; $s \neq 0$; y $r \perp s$ si $r \neq 0$. Luego $(sx - r)$ es un factor de $f(x)$ en $\mathbb{Z}[x]$, lo cual implica que $r \mid a_0$ y $s \mid a_n$. La descomposición prima de a_0 y a_n limita la búsqueda de r y s a sus factores (no necesariamente factores primos). Si se descubre un factor de primer grado de esta manera, entonces $f(x) = (sx - r)\, g(x)$ y luego se puede buscar un factor de primer grado de $g(x)$ de modo similar.

Para buscar factores de grado 2 o superior, hay que usar métodos más sofisticados. Uno de ellos es la *reducción módulo primos*.

Lema 3.80. *Sea* $\Psi_p \colon \mathbb{Z}[x] \to \mathbb{F}_p[x]$ *el homomorfismo dado por*[16]

$$\Psi_p\big(a_0 + a_1 x + \cdots + a_n x^n\big) := \overline{a_0} + \overline{a_1} x + \cdots + \overline{a_n} x^n.$$

Escríbase $\overline{f}(x) := \Psi_p(f(x))$*, la* ***reducción módulo p*** *de* $f(x)$*. Si un polinomio* $f(x)$ *es primitivo y* reducible *en* $\mathbb{F}_p[x]$ *y si* $\operatorname{gr}\overline{f}(x) = \operatorname{gr} f(x)$*, entonces* $\overline{f}(x)$ *es también reducible en* $\mathbb{F}_p[x]$.

[16] Si $\psi_p \colon \mathbb{Z} \to \mathbb{F}_p : a \mapsto (a \bmod p)$ y si $\iota \colon \mathbb{F}_p \hookrightarrow \mathbb{F}_p[x]$ es la inclusión, este homomorfismo Ψ_p se obtiene de la Proposición 3.53 aplicada a $\varphi := \iota \circ \psi_p$.

Demostración. Si $f(x) = g(x)h(x)$ es una factorización propia en $\mathbb{Z}[x]$, es evidente que $\operatorname{gr}\overline{g}(x) \leqslant \operatorname{gr} g(x)$ y $\operatorname{gr}\overline{h}(x) \leqslant \operatorname{gr} h(x)$. La hipótesis $\operatorname{gr}\overline{f}(x) = \operatorname{gr} f(x)$ muestra que hay igualdad en los dos casos, así que la relación $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ en $\mathbb{F}_p[x]$ es una factorización propia. □

Nótese que $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \ker \Psi_p$ si $p \mid \operatorname{mcd}(a_0, \ldots, a_n)$. Entonces se debe descartar primos p tales que $p \mid a_n$, en la búsqueda de reducciones irreducibles.

Este lema es muy útil en su forma contrapositiva: dado un polinomio primitivo $f(x) = a_0 + a_1x + \cdots + a_nx^n$, si es posible hallar un número primo p tal que $\operatorname{gr}\overline{f}(x) = \operatorname{gr} f(x)$ y $\overline{f}(x)$ sea *irreducible* en $\mathbb{F}_p[x]$, entonces el polinomio original $f(x)$ es irreducible en $\mathbb{Z}[x]$.

Ejemplo 3.81. Considérese el polinomio $p(x) = x^2 + x + 2$ en $\mathbb{Z}[x]$. Su reducción módulo 2 es $x^2 + x \in \mathbb{F}_2[x]$, obviamente reducible: $x^2 + x = x(x+1)$. Fíjese que las dos *evaluaciones* de este polinomio en $\mathbb{F}_2$ son nulas: $0(0+1) = 0 \cdot 1 = 0$ y $1(1+1) = 1 \cdot 0 = 0$.

Al tomar $p = 3$, se considera $\overline{p}(x) = x^2 + x + \overline{2}$ en $\mathbb{F}_3[x]$. Al considerar todos los polinomios mónicos de la forma $(x + \overline{a})(x + \overline{b})$ con $\overline{a}, \overline{b} \in \mathbb{F}_3$, solo hay seis posibilidades:

$$x^2, \quad x^2 + x, \quad x^2 + \overline{2}x, \quad x^2 + \overline{2}x + \overline{1}, \quad x^2 + \overline{2}, \quad x^2 + x + \overline{1}.$$

Por ejemplo, $(x + \overline{1})(x + \overline{2}) = x^2 + \overline{3}x + \overline{2} = x^2 + \overline{2}$. No hay otros polinomios reducibles de grado 2; luego, $x^2 + x + \overline{2}$ es irreducible.

Del Lema 3.80, se concluye que $x^2 + x + 2$ es irreducible en $\mathbb{Z}[x]$. ◊

Se debe advertir que el resultado del Lema 3.80 es unidireccional: hay polinomios irreducibles en $\mathbb{Z}[x]$ cuyas reducciones módulo primos son todos reducibles. Un ejemplo es $x^4 + 1$, irreducible en $\mathbb{Z}[x]$ o $\mathbb{Q}[x]$ porque su factorización en $\mathbb{R}[x]$ es irracional. Sin embargo, $x^4 + \overline{1} = (x + \overline{1})^4$ en $\mathbb{F}_2[x]$; mientras que en $\mathbb{F}_3[x]$,

$$x^4 + \overline{1} = x^4 + \overline{4} = (x^2 + \overline{2}x + \overline{2})(x^2 + x + \overline{2}).$$

Resulta que $x^4 + \overline{1}$ también es reducible en $\mathbb{F}_p[x]$ si $p \geqslant 5$ es primo.[17]

En el sentido contrario, el siguiente resultado establece una circunstancia en la cual se puede establecer irreducibilidad de modo directo.

Proposición 3.82 (Criterio de Eisenstein)**.** *Si $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ y si existe un número primo p que cumple:*

$$p \nmid a_n; \quad p \mid a_j \text{ para } j = 0, 1, \ldots, n-1; \quad p^2 \nmid a_0,$$

entonces $f(x)$ es irreducible en $\mathbb{Z}[x]$.

[17] Para una demostración que emplea la teoría de cuerpos, véase el Ejemplo VII.5.3 del libro de Aluffi.

Demostración. Supóngase que $f(x) = g(x)h(x)$ es una factorización propia en $\mathbb{Z}[x]$, con $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ y $h(x) = c_0 + c_1 x + \cdots + c_{n-m} x^{n-m}$, para algún $m \in \{1, \ldots, n-1\}$. Nótese que $a_0 = b_0 c_0$. Como $p \mid a_0$ pero $p^2 \nmid a_0$, resulta entonces que p divide solo uno de b_0 y c_0: sin perder generalidad, se puede suponer que $p \mid b_0$ pero $p \nmid c_0$.

Está claro que p no divide *todo* b_j, porque entonces dividiría $b_m c_{n-m} = a_n$. Sea $r \in \{1, \ldots, m\}$ el menor índice tal que $p \nmid b_r$. Entonces

$$a_r = (b_0 c_r + \cdots + b_{r-1} c_1) + b_r c_0,$$

en donde $p \mid b_j$ para $j = 0, \ldots, r-1$; y $p \mid a_r$ porque $r \leqslant m < n$. Luego $p \mid b_r c_0$, lo cual contradice las hipótesis $p \nmid b_r$ y $p \nmid c_0$. Se concluye que no puede haber una factorización propia de $f(x)$. □

Si $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ tiene factorización prima $a = \pm p_1 p_2 \cdots p_r$ como producto de primos *distintos*, entonces el criterio de Eisenstein muestra que $x^n - a$ es irreducible en $\mathbb{Z}[x]$ para todo $n \in \mathbb{P}$.

Ejemplo 3.83. Si p es un número primo, considérese este polinomio en $\mathbb{Z}[x]$:

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

El criterio de Eisenstein no se directamente aplicable a $h(x)$. Sin embargo, la sustitución $x \mapsto x + 1$ lo convierte en otro polinomio $g(x) := h(x+1)$; y una factorización propia de $h(x)$ conllevaría otra de $g(x)$.

Fíjese que $(x-1)h(x) = x^p - 1$ telescópicamente. Luego

$$g(x) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{p-2} x + \binom{p}{p-1}.$$

Para $k = 1, \ldots, p-1$, el coeficiente binomial

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$

es divisible por p, porque p divide el numerador pero no el denominador, y el resultado es un número entero. Además, $\binom{p}{1} = \binom{p}{p-1} = p$. Ahora el criterio de Eisenstein permite concluir que $g(x)$ es irreducible; y por ende $h(x)$ es también irreducible.[18] ◊

[18] Este $h(x) =: \Phi_{p-1}(x)$ es el **polinomio ciclotómico** de grado $p-1$. Si $m \in \mathbb{P}$, el polinomio ciclotómico $\Phi_m(x) \in \mathbb{C}[x]$ es el producto $\prod_k (x - \omega_k)$ donde las ω_k son las raíces m-ésimas primitivas de 1; esto es, $\omega_k^m = 1$ pero $\omega_k^r \neq 1$ si $r \mid m$ propiamente. Cada ω_j es un número complejo de valor absoluto 1; en efecto, se puede tomar $\omega_k := e^{2\pi i k/m}$ con $k \perp m$. Obsérvese que $\operatorname{gr} \Phi_m(x) = \varphi(m)$. Por ejemplo, $\Phi_6(x) = (x - e^{\pi i/3})(x - e^{5\pi i/3}) = x^2 - x + 1$. Resulta que cada $\Phi_m(x)$ queda en $\mathbb{Z}[x]$ y es irreducible.

4 Representaciones de grupos

Una de los mayores logros en la matemática del siglo XX fue la teoría de representaciones de grupos. Para grupos finitos o grupos de Lie compactos,[1] la teoría ya es extensa y completa en algunos aspectos. Los grupos de Lie no compactos y los grupos infinitos discretos aun guardan muchos misterios por revelar.

Ya entrado al siglo XXI, está de moda hablar de la *teoría de representaciones* sin especificar la categoría de objetos representados. Dichas categorías comprenden las álgebras asociativas, las llamadas álgebras de Lie no asociativas, o bien entes combinatorios como los carcajes,[2] amén de los grupos. En esa teoría se combinan las técnicas de grupos y anillos en una síntesis muy agradable.

4.1 Representaciones irreducibles y reducibles

De manera informal, se puede afirmar que una representación de un grupo es una *acción lineal* del grupo *sobre un espacio vectorial*. Es oportuno recapitular la Definición 3.41 del capítulo anterior.

Definición 4.1. Sea V un espacio vectorial sobre un cuerpo $\mathbb{F}$. Denótese por $\mathrm{End}_{\mathbb{F}}(V)$ el *álgebra* de aplicaciones $\mathbb{F}$-lineales $S\colon V \to V$; este es un anillo bajo suma y composición de aplicaciones lineales, pero a la vez es un espacio vectorial sobre $\mathbb{F}$ – en breve, $\mathrm{End}_{\mathbb{F}}(V)$ es una $\mathbb{F}$-*álgebra* (asociativa).

El grupo de unidades de esta $\mathbb{F}$-álgebra es $\mathrm{GL}(V) \equiv \mathrm{GL}_{\mathbb{F}}(V)$, la totalidad de aplicaciones $\mathbb{F}$-lineales *biyectivas* de V en V.

Si G es un grupo cualquiera, una **representación de G sobre V** es simplemente un homomorfismo $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$.

El **álgebra de grupo** $\mathbb{F}[G]$ [también llamado *anillo de grupo*] es la totalidad de combinaciones lineales $a = \sum_{g\in G} a_g\, g$ de elementos de G con coeficientes en $\mathbb{F}$: con la suma obvia, la multiplicación escalar obvia, y el producto dado por $ab := \sum_{g,h\in G} a_g b_h\, gh$. Los elementos de G forman una *base* de $\mathbb{F}[G]$ como espacio $\mathbb{F}$-vectorial.[3]

[1] Un **grupo de Lie** es un grupo parametrizado por un número finito de parámetros reales, el cual a su vez es una variedad diferenciable en donde el producto y la inversión son funciones suaves (o analíticas). En este curso no se discute la estructura diferenciable, pero aun así tales grupos proporcionan ejemplos muy importantes. Un grupo de Lie es *compacto* si la totalidad de sus parámetros forman una parte acotada y cerrada de algún $\mathbb{R}^N$; de lo contrario, el grupo solo sería localmente compacto.

[2] Un **carcaj**, como su nombre indica, es un manojo de flechas. Más correctamente, es un grafo dirigido con diversos *nodos*, cuyas aristas son las "flechas".

[3] Una combinación lineal es, por definición, una *suma finita* de términos. Si G es infinito, hay diversas maneras de completar $\mathbb{F}[G]$ en una $\mathbb{F}$-álgebra más apropiada. Por ejemplo, si G es un grupo compacto, se puede considerar $\underline{C(G)}$, la totalidad de funciones continuas de G en $\mathbb{F}$.

La representación $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$ *se extiende por* $\mathbb{F}$*-linealidad* a todo $\mathbb{F}[G]$, así:

$$a = \sum_{g\in G} a_g\, g \quad \text{actúa por} \quad a\cdot x := \sum_{g\in G} a_g\, \pi(g)\, x. \tag{4.1}$$

De esta manera, V resulta ser un $\mathbb{F}[G]$-módulo (a izquierda). Es costumbre decir que V es un ***G*-módulo**, como abreviatura. Bajo este punto de vista, la acción (a izquierda) de G sobre V está dada por $g\cdot x \equiv \pi(g)\,x$.

Nótese que la acción $x \mapsto a\cdot x$, que puede denotarse por $\tilde{\pi}(a)$, define un *homomorfismo de* $\mathbb{F}$*-álgebras* $\tilde{\pi}\colon \mathbb{F}[G] \to \mathrm{End}_{\mathbb{F}}(V)$, cuya imagen incluye algunas aplicaciones $\mathbb{F}$-lineales no invertibles. ◊

El proceso de pasar de π a $\tilde{\pi}$ es un *funtor*. La representación $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$ es un morfismo en la categoría Gr de grupos. En cambio, $\tilde{\pi}\colon \mathbb{F}[G] \to \mathrm{End}_{\mathbb{F}}(V)$ es un morfismo en la categoría $\mathbb{F}$-Alg de $\mathbb{F}$-álgebras. En efecto, *cualquier* homomorfismo de grupos $\varphi\colon G \to K$ da lugar a un homomorfismo de $\mathbb{F}$-álgebras $\tilde{\varphi}\colon \mathbb{F}[G] \to \mathbb{F}[K]$ al definir

$$\tilde{\varphi}\Big(\sum_{g\in G} a_g\, g\Big) := \sum_{g\in G} a_g\, \varphi(g).$$

Basta notar que $\mathbb{F}[\mathrm{GL}_{\mathbb{F}}(V)] = \mathrm{End}_{\mathbb{F}}(V)$; cualquier endomorfismo $\mathbb{F}$-lineal de V es una combinación lineal de endomorfismos invertibles. Entonces la receta $\mathscr{F}G := \mathbb{F}[G]$, $\mathscr{F}\varphi := \tilde{\varphi}$ es un funtor $\mathscr{F}\colon \mathsf{Gr} \to \mathbb{F}$-$\mathsf{Alg}$.

Entonces, si A es un $\mathbb{F}$-álgebra cualquiera y V un espacio $\mathbb{F}$-vectorial, un $\mathbb{F}$-homomorfismo $\tilde{\pi}\colon A \to \mathrm{End}_{\mathbb{F}}(V)$ se llama una **representación de *A* sobre *V***.

Definición 4.2. Sea $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$ una representación de un grupo G sobre V. Si U es un subespacio $\mathbb{F}$-vectorial de V tal que $\pi(g)(U) \subseteq U$ para todo $g \in G$, la restricción $g \mapsto \pi(g)|_U$ lleva G en $\mathrm{GL}_{\mathbb{F}}(U)$: esta es una **subrepresentación** de π. Dicho de otro modo, el subespacio U es un $\mathbb{F}[G]$-*submódulo de* V.

La representación π se llama **irreducible** si no posee subrepresentaciones no triviales; es decir, si los únicos $\mathbb{F}[G]$-submódulos de V son $\{0\}$ y V mismo. Si R es un anillo, un R-módulo M es **simple** si no posee R-submódulos propios. Para $R = \mathbb{F}[G]$, un G-módulo V es simple si la representación de G (o bien de $\mathbb{F}[G]$) sobre V es irreducible. ◊

Definición 4.3. Sea $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$ y $\sigma\colon G \to \mathrm{GL}_{\mathbb{F}}(W)$ dos representaciones de un mismo grupo G sobre los espacios $\mathbb{F}$-vectoriales respectivos V y W. Dícese que una aplicación $\mathbb{F}$-lineal $T\colon V \to W$ **entrelaza** π y σ si

$$T\,\pi(g)\,x = \sigma(g)\,T(x) \quad \text{para todo} \quad g \in G,\ x \in V, \tag{4.2}$$

o más brevemente, si $T \circ \pi(g) = \sigma(g) \circ T$ en $\mathrm{Hom}_{\mathbb{F}}(V, W)$ para todo $g \in G$. Esto sucede si y sólo si T es un $\mathbb{F}[G]$-homomorfismo de módulos, es decir, $T \in \mathrm{Hom}_{\mathbb{F}[G]}(V, W)$.

En el caso $V = W$ y $\sigma = \pi$, dícese que $T \in \mathrm{End}_{\mathbb{F}}(V)$ **conmuta con** π si T entrelaza π consigo mismo, como en (3.6):

$$T \circ \pi(g) = \pi(g) \circ T \quad \text{para todo} \quad g \in G. \tag{4.3}$$

Obsérvese que en este caso, T también conmuta con la extensión de π por linealidad: $T \circ \tilde{\pi}(a) = \tilde{\pi}(a) \circ T$ para todo $a \in \mathbb{F}[G]$; o bien, $T \in \mathrm{End}_{\mathbb{F}[G]}(V)$. ◊

En este contexto, la (Proposición 3.49) admite la siguiente reformulación.

Proposición 4.4 (Lema de Schur, bis)**.** *Sea $T : V \to W$ una aplicación $\mathbb{F}$-lineal* no nula *que entrelaza dos representaciones π y σ de un grupo G, sobre V y W respectivamente. Si π es irreducible, entonces T es inyectivo; si σ es irreducible, entonces T es sobreyectivo; y si las dos representaciones son irreducibles, entonces T es un $\mathbb{F}[G]$-isomorfismo de V en W.*

En particular, si $T : V \to V$ conmuta *con una representación* irreducible *π de G sobre V y si $T \neq 0$, entonces T es un $\mathbb{F}[G]$-isomorfismo.*

Demostración. La condición $T \neq 0$ dice que $\ker T \neq V$ y $\mathrm{im}\, T \neq 0$. Como T es un $\mathbb{F}[G]$-homomorfismo, $\ker T$ es un G-submódulo de V y $\mathrm{im}\, T$ es un G-submódulo de W.

Luego $\ker T = \{0\}$ si V es irreducible; $\mathrm{im}\, T = W$ si W es irreducible. Lo demás es inmediato. □

Definición 4.5. Dos representaciones $\pi : G \to \mathrm{GL}_{\mathbb{F}}(V)$ y $\sigma : G \to \mathrm{GL}_{\mathbb{F}}(W)$ son **equivalentes** si poseen un operador entrelazante *biyectivo* $T : V \to W$; es decir, si V y W son isomorfos como $\mathbb{F}[G]$-módulos (esto es, son isomorfos como G-módulos).

Si π y σ son equivalentes y si $T \in \mathrm{Hom}_{\mathbb{F}[G]}(V, W)$ es biyectivo, entonces (4.2) puede ser escrito así:

$$\sigma(g) = T \circ \pi(g) \circ T^{-1} \quad \text{para todo} \quad g \in G, \tag{4.4}$$

de modo que los endomorfismos $\mathbb{F}$-lineales $\pi(g)$ y $\sigma(g)$ son *semejantes* mediante un operador que no depende de g.

Si π y σ *no son* equivalentes, el lema de Schur implica que $\mathrm{Hom}_{\mathbb{F}[G]}(V, W) = \{0\}$.

Es necesario que $\dim_{\mathbb{F}} W = \dim_{\mathbb{F}} V$ para que π y σ sean equivalentes. La dimensión de V se llama el **grado** de la representación π. ◊

En el caso de que $\mathbb{F} = \mathbb{C}$, el cuerpo de los números complejos, y si $\pi : G \to \mathrm{GL}_{\mathbb{F}}(V)$ es una representación irreducible de grado finito (es decir, $\dim_{\mathbb{F}}(V) < \infty$), entonces cualquier operador T que conmuta con π posee un autovalor $\lambda \in \mathbb{C}$; y la diferencia $T - \lambda\, 1_V$ no es inyectivo, por lo cual $T - \lambda\, 1_V = 0$. Este es el Corolario 3.50 ya visto: el espacio vectorial complejo $\mathrm{End}_{\mathbb{C}[G]}(V) \simeq \mathbb{C}\, 1_V$ es unidimensional si π es irreducible.

Lema 4.6. *Si G es un grupo* abeliano *y $\mathbb{F} = \mathbb{C}$, cualquier representación irreducible de G tiene dimensión* 1.

Demostración. Si $\pi\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ es una representación irreducible de G, entonces

$$\pi(h) \circ \pi(g) = \pi(hg) = \pi(gh) = \pi(g) \circ \pi(h) \quad \text{para todo} \quad g, h \in G.$$

Luego cada $\pi(h)\colon V \to V$ es un operador que conmuta con π. Por el lema de Schur, $\pi(h) = \lambda(h)\, 1_V$ para algún $\lambda(h) \in \mathbb{C}$, es decir, cada $\pi(h)$ es un operador escalar sobre V. Cualquier subespacio $U \leqslant V$ entonces determina una subrepresentación de π; lo cual implica que $\dim_{\mathbb{C}} V = 1$ pues π es irreducible. □

Ejemplo 4.7. El grupo aditivo $(\mathbb{R}, +)$ tiene muchas representaciones inequivalentes sobre $\mathbb{C}$. Por ejemplo, si $t \in \mathbb{R}$, sea

$$\pi_t(x) := e^{itx} = \cos tx + i \operatorname{sen} tx \in \mathbb{C} \quad \text{para} \quad x \in \mathbb{R}.$$

Está claro que $\pi_t(x + y) = e^{it(x+y)} = e^{itx}\, e^{ity}$, así que $\pi_t\colon \mathbb{R} \to \mathbb{C}^\times = \mathrm{GL}(1, \mathbb{C})$ es un homomorfismo. Cualquier operador entrelazante $T\colon \mathbb{C} \to \mathbb{C}$ es escalar, $z \mapsto \lambda z$, y por ende $\pi_s(x) \equiv T \circ \pi_t(x) \circ T^{-1}$ si y sólo si $\pi_s(x) \equiv \pi_t(x)$, es decir, $e^{isx} = e^{itx}$ para todo $x \in \mathbb{R}$, así que $s = t$. Todas estas representaciones son inequivalentes entre sí. ◊

Ejemplo 4.8. El grupo no abeliano S_3 tiene una representación obvia sobre $\mathbb{F}^3$, cualquiera que sea el cuerpo $\mathbb{F}$, por matrices 3×3. De hecho, $\mathrm{GL}_{\mathbb{F}}(\mathbb{F}^3) = \mathrm{GL}(3, \mathbb{F})$ es el grupo de matrices invertibles 3×3 con entradas en $\mathbb{F}$. Defínase $\pi\colon S_3 \to \mathrm{GL}(3, \mathbb{F})$ por

$$\underline{1} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (123) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad (132) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$(12) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (13) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad (23) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

La recta diagonal $U = \{\, (x, y, z) \in \mathbb{F}^3 : x = y = z \,\}$ es un S_3-submódulo de $\mathbb{F}^3$. Luego, esta representación π de $\mathbb{S}_3$ no es irreducible.

El plano $W = \{\, (x, y, z) \in \mathbb{F}^3 : x + y + z = 0 \,\}$ es otro S_3-submódulo de $\mathbb{F}^3$, el cual es simple: la restricción de π a W sí es irreducible. Fíjese que $\mathbb{F}^3 = U \oplus W$ como espacios $\mathbb{F}$-vectoriales pero también como S_3-módulos.

Los primeros tres de estas seis matrices determinan una representación del subgrupo cíclico $C_3 \leqslant S_3$. Entonces $\mathbb{F}^3 = U \oplus W$ como C_3-módulos. En el caso $\mathbb{F} = \mathbb{C}$, este W es reducible como C_3-módulo.

En efecto, tómese $\omega = e^{2\pi i/3} = \frac{1}{2}(-1+i\sqrt{3})$, así que que $\omega^2 = e^{-2\pi i/3} = \frac{1}{2}(-1-i\sqrt{3})$ y $\omega^3 = 1$. Entonces $W = W_1 \oplus W_2$, donde

$$W_1 = \{(x,y,z) \in W : x + \omega y + \omega^2 z = 0\}; \quad W_2 = \{(x,y,z) \in W : x + \omega^2 y + \omega z = 0\}.$$

Luego $\mathbb{C}^3 = U \oplus W_1 \oplus W_2$ es una suma directa de C_3-submódulos unidimensionales. ◊

Ejemplo 4.9. Sea G un grupo finito. Si se toma $V = \mathbb{F}[G]$, la **representación regular** (a izquierda) de G se define por $\lambda(g)\colon \sum_{h\in G} b_h h \mapsto \sum_{h\in G} b_h gh$. La representación correspondiente de $\mathbb{F}[G]$ está dada por el producto en esta $\mathbb{F}$-álgebra; en otras palabras, $\tilde{\lambda}(a)\colon b \mapsto ab$ para $a, b \in \mathbb{F}[G]$.

Conviene distinguir el papel de $\mathbb{F}[G]$ como G-módulo al denotar su base natural por $\{x_g : g \in G\}$ (una copia biyectiva del conjunto G); un elemento típico de este espacio vectorial es una combinación lineal $\sum_{g\in G} a_g x_g$, olvidando la estructura de producto.[4] La representación regular entonces se escribe como $\lambda(g)\colon \sum_{h\in G} b_h x_h \mapsto \sum_{h\in G} b_h x_{gh}$. El grado de λ es $|G|$, obviamente. ◊

En un cuerpo cualquiera $\mathbb{F}$, el elemento identidad 1 en $\mathbb{F}$ puede tener período aditivo finito o infinito. Si es infinito, dícese que $\mathbb{F}$ tiene **característica 0**, pues $n \cdot 1 = 0$ para $n \in \mathbb{Z}$ sólo si $n = 0$. Si posee período finito $p \in \mathbb{P}$, dícese que $\mathbb{F}$ tiene **característica p**, en cuyo caso p es primo [porque $m \cdot 1 = n \cdot 1 = 0$ implica $d \cdot 1 = 0$ para $d = \mathrm{mcd}(m,n)$] y el subanillo $\{0, 1, 2, \ldots, p-1\} \subseteq \mathbb{F}$ es isomorfo a $\mathbb{F}_p$. (Si $\mathbb{F}$ tiene característica 0, el subanillo generado por 1 es una copia isomorfa de $\mathbb{Z}$, por lo cual $\mathbb{F}$ es necesariamente infinito.)

Proposición 4.10. *Sean G un grupo finito, $\mathbb{F}$ un cuerpo cuya característica no divide $|G|$ y $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$ una representación de G. Si U es un G-submódulo propio de V, hay un subespacio $W \leqslant V$ tal que $V = U \oplus W$ y $\pi(g)W \subseteq W$ para todo $g \in G$.*

Demostración. Elíjase cualquier subespacio $W_1 \leqslant V$ tal que $V = U \oplus W_1$ como espacios $\mathbb{F}$-vectoriales (por ejemplo, al completar una base de U en una base de V). Si $x \in V$, entonces $x = y + z$ de manera única, con $y \in U$, $z \in W_1$. El operador lineal $P_1\colon V \to V$ dado por $P_1(y+z) := y$ es "la proyección de V sobre U a lo largo de W_1". Defínase

$$P := \frac{1}{|G|} \sum_{h\in G} \pi(h) \circ P_1 \circ \pi(h)^{-1}. \tag{4.5}$$

Fíjese que el multiplicador escalar $1/|G| \in \mathbb{F}$ está bien definido porque la característica de $\mathbb{F}$ no divide $|G|$.

[4] En otras palabras: se aplica un *funtor olvidadizo* que lleva la categoría $\mathbb{F}$-Alg de $\mathbb{F}$-álgebras en la categoría $\mathbb{F}$-Vect de espacios $\mathbb{F}$-vectoriales.

El subespacio U es estable bajo cada $\pi(h)$: esto muestra que $Py = y$ para $y \in U$. Además, para todo $g \in G$ vale

$$\pi(g) \circ P = \frac{1}{|G|} \sum_{h \in G} \pi(gh) \circ P_1 \circ \pi(h^{-1}) = \frac{1}{|G|} \sum_{k \in G} \pi(k) \circ P_1 \circ \pi(k^{-1}g) = P \circ \pi(g),$$

así que P conmuta con π. Sea $W := \ker P$; entonces $\pi(g)W \subseteq W$ para todo $g \in G$. [De hecho, resulta que $\pi(g)W = W$, porque $W \subseteq \pi(g^{-1})W$ también.]

Obsérvese que $Px \in U$ para $x \in V$ y además $Py = y$ para $y \in U$, así que $P^2 = P$ en $\mathrm{End}_{\mathbb{F}}(V)$; entonces $V = \operatorname{im} P \oplus \ker P = U \oplus W$ como espacios $\mathbb{F}$-vectoriales. □

El resultado de la última proposición dice que la descomposición $\underline{V = U \oplus W}$ es una *suma directa de G-módulos*. Si se denota $\rho(g) := \pi(g)|_U$ y $\sigma(g) := \pi(g)|_W$, también se escribe $\underline{\pi = \rho \oplus \sigma}$ y se dice que π es *la suma directa de sus subrepresentaciones* ρ y σ.

Corolario 4.11 (Teorema de Maschke)**.** *Si G es un grupo finito, si $\mathbb{F}$ es un cuerpo cuya característica no divide $|G|$, y si $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$ es una representación de grado finito, entonces π es* ***completamente reducible****: se puede descomponer $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$ en una suma directa de G-módulos que forman subrepresentaciones irreducibles de π.*

Demostración. Si π es irreducible, la reducción es válida con $m = 1$. Si no, la Proposición 4.10 muestra que existe un G-submódulo propio V_1 con $\{0\} < V_1 < V$. Hay un submódulo complementario W_1 con $V = V_1 \oplus W_1$. Inductivamente, se puede suponer que $W_1 = V_2 \oplus \cdots \oplus V_r$. □

Definición 4.12. Un R-módulo M es **semisimple** si es una suma directa $M = M_1 \oplus \cdots \oplus M_r$ de una cantidad finita de R-submódulos simples. El anillo R mismo es semisimple si resulta ser semisimple como R-módulo.

Nótese que una representación π sobre V es completamente reducible si y sólo si el G-módulo V es semisimple. ◊

Corolario 4.13. *Si G es un grupo finito y si $\mathbb{F}$ es un cuerpo cuya característica no divide $|G|$, entonces el anillo $\mathbb{F}[G]$ es semisimple.* ⊟

4.2 El carácter de una representación

Si $T\colon V \to V$ es un endomorfismo $\mathbb{F}$-lineal de un espacio $\mathbb{F}$-vectorial V de dimensión finita, se sabe que la *matriz* de T con respecto a una base $\{x_1, \ldots, x_n\}$ de V es el elemento $A = [a_{ij}] \in M_n(\mathbb{F})$ obtenido por la fórmula

$$Tx_j =: \sum_{i=1}^{n} a_{ij} x_i \quad \text{para} \quad j = 1, \ldots, n.$$

La **traza** de T es la traza de esta matriz,

$$\operatorname{Tr} T := \operatorname{tr} A = \sum_{i=1}^{n} a_{ii}\,.$$

Un resultado fundamental del álgebra lineal asegura que $\operatorname{Tr} T$ no depende de la elección de una base, porque $\operatorname{tr}(PAP^{-1}) = \operatorname{tr}(AP^{-1}P) = \operatorname{tr} A$, para todo $P \in \mathrm{GL}(n,\mathbb{F})$.

Si $\mathbb{F} = \mathbb{C}$, la traza $\operatorname{Tr} T$ es la suma de los autovalores de T, repetidos con multiplicidad.

Definición 4.14. Sea $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$ una representación de un grupo G sobre un espacio $\mathbb{F}$-vectorial finitodimensional V. El **carácter** de π es la función $\chi_\pi\colon G \to \mathbb{F}$ dada por

$$\chi_\pi(g) := \operatorname{Tr} \pi(g), \quad \text{para todo} \quad g \in G. \tag{4.6}$$

Fíjese bien que si $\dim_{\mathbb{F}} V > 1$, el carácter χ_π *no es un homomorfismo* de G en $\mathbb{F}^\times$. ◊

Definición 4.15. Si G es un grupo y $\mathbb{F}$ es un cuerpo, una función $f : G \to \mathbb{F}$ se llama **función de clase** si

$$f(ghg^{-1}) = f(h) \quad \text{para todo} \quad g,h \in G.$$

En otras palabras, una función de clase es constante sobre cada una de las clases conjugadas de G. Al sustituir $h \mapsto hg$, la condición anterior es equivalente a $f(gh) = f(hg)$ para todo $g,h \in G$: las funciones de clase también se llaman *funciones centrales*.

El carácter de una representación es una función de clase, porque

$$\chi_\pi(ghg^{-1}) = \operatorname{Tr} \pi(ghg^{-1}) = \operatorname{Tr}\big(\pi(g)\,\pi(h)\,\pi(g)^{-1}\big) = \operatorname{Tr} \pi(h) = \chi_\pi(h). \qquad \text{◊}$$

Lema 4.16. *El grado de una representación π es $\chi_\pi(1)$. Dos representaciones equivalentes tienen el mismo carácter.*

Demostración. Como $\pi(1) = 1_V$ (π es un homomorfismo), sigue $\dim_{\mathbb{F}} V = \operatorname{Tr} 1_V = \chi_\pi(1)$.

Además, si dos representaciones π y σ son equivalentes mediante un operador entrelazante T, de (4.4) se obtiene

$$\chi_\sigma(g) = \operatorname{Tr} \sigma(g) = \operatorname{Tr}\big(T\,\pi(g)\,T^{-1}\big) = \operatorname{Tr} \pi(g) = \chi_\pi(g), \quad \text{para todo} \quad g \in G. \qquad \square$$

Lema 4.17. *El carácter de la representación regular $\lambda\colon G \to \mathrm{GL}_{\mathbb{F}}(\mathbb{F}[G])$ está dado por*

$$\chi_\lambda(1) = |G|; \qquad \chi_\lambda(g) = 0 \quad \textit{para} \quad g \neq 1.$$

Demostración. Es inmediato que $\chi_\lambda(1) = \dim_{\mathbb{F}} \mathbb{F}[G] = |G|$. En cambio, si $g \neq 1$, entonces $\lambda(g)\,x_h = x_{gh}$; la matriz de $\lambda(g)$ con respecto a la base $\{\,x_g : g \in G\,\}$ tiene todas sus entradas diagonales iguales a 0, y por ende si traza es 0. $\square$

► Hay dos maneras de combinar espacios vectoriales que llevan representaciones de un grupo. Si V y W son dos espacios vectoriales finitodimensionales sobre un cuerpo $\mathbb{F}$, se puede formar su *suma directa* $V \oplus W$; dadas dos bases $\{x_1, \ldots, x_n\}$ de V y $\{y_1, \ldots, y_m\}$ de W, los vectores $(x_j, 0)$ y los vectores $(0, y_k)$ juntos forman una base de $V \oplus W$, así que $\dim_{\mathbb{F}}(V \oplus W) = n + m = \dim_{\mathbb{F}} V + \dim_{\mathbb{F}} W$.

El **producto tensorial** $V \otimes W$ (a veces escrito $V \otimes_{\mathbb{F}} W$) es un espacio $\mathbb{F}$-vectorial dotado con una aplicación $\mathbb{F}$-bilineal $V \times W \to V \otimes W : (x, y) \mapsto x \otimes y$ tal que el conjunto $\{x_i \otimes y_j : i = 1, \ldots, n;\ j = 1, \ldots, m\}$ sea una base de $V \otimes W$. La existencia y unicidad hasta isomorfismo de $V \otimes W$ es un resultado conocido del álgebra lineal.[5] Por su definición, es evidente que $\dim_{\mathbb{F}}(V \otimes W) = nm = (\dim_{\mathbb{F}} V)(\dim_{\mathbb{F}} W)$.

Definición 4.18. Dadas dos representaciones $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$ y $\sigma\colon G \to \mathrm{GL}_{\mathbb{F}}(W)$ de un grupo G, su **suma directa** $\underline{\pi \oplus \sigma} : G \to \mathrm{GL}_{\mathbb{F}}(V \oplus W)$ se define por $\pi \oplus \sigma(g) = \pi(g) \oplus \sigma(g)$ para cada $g \in G$. En notación matricial, se escribe

$$\pi \oplus \sigma(g) := \begin{pmatrix} \pi(g) & 0 \\ 0 & \sigma(g) \end{pmatrix} \in \mathrm{GL}_{\mathbb{F}}(U \oplus W).$$

Su **producto tensorial** $\underline{\pi \otimes \sigma} : G \to \mathrm{GL}_{\mathbb{F}}(V \otimes W)$ se define por

$$\pi \otimes \sigma(g)[x \otimes y] := \pi(g)\, x \otimes \sigma(g)\, y, \quad \text{para} \quad x \in V,\ y \in W;\ g \in G,$$

extendido por $\mathbb{F}$-linealidad a todo $V \otimes W$. ◊

Proposición 4.19. *Sean $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$ y $\sigma\colon G \to \mathrm{GL}_{\mathbb{F}}(W)$ dos representaciones de un grupo G.*

(a) *El carácter de la suma directa $\pi \oplus \sigma$ es la suma de sus caracteres: $\chi_{\pi\oplus\sigma} = \chi_\pi + \chi_\sigma$.*

(b) *El carácter del producto tensorial $\pi \otimes \sigma$ es el producto de caracteres: $\chi_{\pi\otimes\sigma} = \chi_\pi \cdot \chi_\sigma$.*

Demostración. Ad (a): En una suma directa de matrices las trazas individuales se suman:

$$\chi_{\pi\oplus\sigma}(g) = \mathrm{Tr}\begin{pmatrix} \pi(g) & 0 \\ 0 & \sigma(g) \end{pmatrix} = \mathrm{Tr}\,\pi(g) + \mathrm{Tr}\,\sigma(g) = \chi_\pi(g) + \chi_\sigma(g).$$

Luego, $\chi_{\pi\oplus\sigma} = \chi_\pi + \chi_\sigma$ como suma de funciones (de clase).

[5] Para mostrar existencia, se *define* $V \otimes W$ como el espacio de aplicaciones bilineales $V^* \times W^* \to \mathbb{F}$, donde V^* y W^* son los respectivos espacios duales de V y W. Se define $x \otimes y$ como la aplicación bilineal $(f, g) \mapsto f(x)\, g(y)$; dadas las dos bases, no es difícil comprobar que los $x_i \otimes y_j$ son linealmente independientes y generan $V \otimes W$.

Ad (b): Con respecto a dos bases dadas de V y W, sean $A(g) \in M_n(\mathbb{F})$, $B(g) \in M_m(\mathbb{F})$ las matrices respectivas de $\pi(g)$ y $\sigma(g)$:

$$\pi(g)x_j =: \sum_{i=1}^{n} a_{ij}(g)\, x_i, \qquad \sigma(g)y_l =: \sum_{k=1}^{m} b_{kl}(g)\, y_k. \tag{4.7}$$

Entonces la matriz de $\pi \otimes \sigma(g)$ es la matriz $A \otimes B(g) \in M_{nm}(\mathbb{F})$, cuya entrada (ik, jl) es $a_{ij}(g)\, b_{kl}(g)$. Por lo tanto,

$$\begin{aligned}\chi_{\pi\otimes\sigma}(g) = \operatorname{tr}\big(A \otimes B(g)\big) &= \sum_{i=1}^{n}\sum_{k=1}^{m} a_{ii}(g)\, b_{kk}(g) \\ &= \operatorname{tr}A(g)\, \operatorname{tr}B(g) = \operatorname{Tr}\pi(g)\, \operatorname{Tr}\sigma(g) = \chi_\pi(g)\, \chi_\sigma(g),\end{aligned}$$

así que $\chi_{\pi\otimes\sigma} = \chi_\pi \cdot \chi_\sigma$ como producto de funciones (de clase). □

Definición 4.20. Si $\pi : G \to \mathrm{GL}_{\mathbb{F}}(V)$ una representación sobre V, hay una **representación dual** $\underline{\pi^*}$: $G \to \mathrm{GL}_{\mathbb{F}}(V^*)$ sobre el espacio dual V^* de formas $\mathbb{F}$-lineales $f : V \to \mathbb{F}$, dado por

$$\pi^*(g) : f \mapsto f \circ \pi(g^{-1}).$$

Fíjese que este π^* es un homomorfismo, porque

$$\pi^*(g)\pi^*(h)[f] = \pi^*(h)[f] \circ \pi(g^{-1}) = f \circ \pi(h^{-1}) \circ \pi(g^{-1}) = f \circ \pi(h^{-1}g^{-1}) = \pi^*(gh)[f].$$

Si A es la matriz de $\pi(g)$ con respecto a una determinada base de V, la matriz de $\pi^*(g)$ con respecto a la base dual de V^* es la transpuesta de A^{-1}, denotable[6] por A^{-t}, la *matriz contragrediente* de A; y resulta que $(AB)^{-t} = A^{-t}B^{-t}$. ◊

Si $\chi : G \to \mathbb{F}$ es una función, se denota por $\chi^\vee$ la función $g \mapsto \chi(g^{-1})$.

Lema 4.21. *El carácter de la representación dual π^* es $\chi_{\pi^*} = \chi_\pi^\vee$.*

Demostración. Si A es una matriz de $\pi(g)$, entonces $\operatorname{tr}A^{-t} = \operatorname{tr}A^{-1}$ porque la traza no cambia bajo transposición. Además, A^{-1} es la matriz de $\pi(g)^{-1} = \pi(g^{-1})$. □

Las funciones de clase $f : G \to \mathbb{F}$ forman una $\mathbb{F}$-álgebra conmutativa $F_c(G, \mathbb{F})$. Si G es un grupo finito y la característica de $\mathbb{F}$ no divide $|G|$, el teorema de Maschke y la última Proposición muestran que cualquier carácter χ_π es una suma finita de los caracteres que corresponden a las representaciones irreducibles. Entonces es de gran importancia averiguar cuáles son estos caracteres básicos.

[6] Nótese que $(A^{-1})^t = (A^t)^{-1}$ para todo $A \in \mathrm{GL}(n, \mathbb{C})$.

► Para simplificar la tarea, conviene ahora tomar $\mathbb{F} = \mathbb{C}$ como cuerpo de escalares. El cuerpo de los números complejos tiene dos ventajas: primero, tiene característica 0, así que en el teorema de Maschke sólo hay que asumir que el grupo G es finito; y segundo, $\mathbb{C}$ es *algebraicamente cerrado*, es decir, cualquier polinomio en $\mathbb{C}[x]$ se factoriza en un producto de polinomios de primer grado (este es el "teorema fundamental del álgebra"). Además, tiene una tercera propiedad de interés: el cuerpo $\mathbb{C}$ posee un automorfismo no trivial, la *conjugación compleja* $z \mapsto \bar{z}$.

Si V es un espacio $\mathbb{C}$-vectorial finitodimensional, un **producto escalar** (o *producto interno*) sobre V es una aplicación $V \times V \to \mathbb{C} : (x, y) \mapsto \langle y \mid x \rangle$, tal que:

- $\langle y \mid x \rangle$ es $\mathbb{C}$-lineal en la *segunda* variable;[7]
- $\langle x \mid y \rangle = \overline{\langle y \mid x \rangle}$ para todo $x, y \in V$;
- $\langle x \mid x \rangle \geqslant 0$, con igualdad sólo si $x = 0$ en V.

Dado un producto escalar, el espacio dual V^* de formas $\mathbb{C}$-lineales $f : V \to \mathbb{C}$ puede ser identificado con V mismo, porque cada forma lineal está dada por $x \mapsto \langle y \mid x \rangle$ para algún vector $y \in V$ (este es el "lema de Riesz"). Sin embargo, como $\langle \alpha y \mid x \rangle = \bar{\alpha} \langle y \mid x \rangle$, hay que modificar la multiplicación escalar por la conjugación compleja, $\alpha \cdot y := \bar{\alpha}\, y$. Se escribe $y \in \overline{V}$ en tal caso; luego, hay un isomorfismo $\mathbb{C}$-lineal $V^* \simeq \overline{V}$.

Si $\chi : G \to \mathbb{C}$ es una función, se denota por $\overline{\chi}$ la función $g \mapsto \overline{\chi(g)}$.

Definición 4.22. Dada una representación $\pi \colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ de un grupo *finito* G, un producto escalar sobre V es *G-invariante* y π es una **representación unitaria** si

$$\langle \pi(g)y \mid \pi(g)x \rangle = \langle y \mid x \rangle \quad \text{para todo} \quad x, y \in V,\ g \in G.$$

De hecho, si $(\cdot|\cdot)$ es un producto escalar arbitrario sobre V, se obtiene un producto escalar G-invariante al calcular el siguiente promedio:

$$\langle y \mid x \rangle := \frac{1}{|G|} \sum_{g \in G} (\pi(g)y \mid \pi(g)x).$$

En adelante, sin perder generalidad, se asumirá que cada π es unitaria. ◊

[7] Algunos autores toman el producto escalar lineal en la *primera* variable, y semilineal o antilineal en la segunda. Eso es un error: el buen convenio, el de la linealidad en la segunda variable, fue introducido por Dirac hace más de 80 años.

Si $g \in G$, la matriz A de $\pi(g)$ con respecto a una base ortonormal de V es una *matriz unitaria*, es decir, satisface $A^*A = 1_n$; en consecuencia, sus autovalores $\lambda_1, \ldots, \lambda_n$ (contados con multiplicidad) tienen valores absolutos iguales a 1. Por lo tanto, vale

$$\overline{\chi}_\pi(g) = \overline{\operatorname{Tr}\pi(g)} = \sum_{i=1}^{n} \bar{\lambda}_i = \sum_{i=1}^{n} \frac{1}{\lambda_i} = \operatorname{Tr}\pi(g)^{-1} = \operatorname{Tr}\pi(g^{-1}) = \chi_\pi(g^{-1}).$$

En otras palabras, vale $\overline{\chi}_\pi = \chi_\pi^\vee = \chi_{\pi^*}$ cuando π es unitaria.

En el espacio $\mathbb{C}$-vectorial finitodimensional $F_c(G, \mathbb{C})$ de las funciones de clase complejas, la siguiente receta define un producto escalar:

$$\langle \psi \mid \varphi \rangle := \frac{1}{|G|} \sum_{h \in G} \overline{\psi(h)}\, \varphi(h). \tag{4.8a}$$

Si $\psi = \chi_\pi$ es el carácter de una representación unitaria, entonces también vale:

$$\langle \psi \mid \varphi \rangle = \frac{1}{|G|} \sum_{h \in G} \psi(h^{-1})\, \varphi(h). \tag{4.8b}$$

Proposición 4.23. *Sean $\pi : G \to \mathrm{GL}_{\mathbb{C}}(V)$ y $\sigma : G \to \mathrm{GL}_{\mathbb{C}}(W)$ dos representaciones unitarias* irreducibles *de un grupo finito G. Entonces:*

(a) *Si π y σ no son equivalentes, entonces $\langle \chi_\sigma \mid \chi_\pi \rangle = 0$.*

(b) *En el caso $V = W$ y $\pi = \sigma$, vale $\langle \chi_\pi \mid \chi_\pi \rangle = 1$.* □

Demostración. Si $T : V \to W$ es una aplicación $\mathbb{C}$-lineal cualquiera, defínase

$$\widetilde{T} := \frac{1}{|G|} \sum_{h \in G} \sigma(h^{-1}) T \pi(h).$$

Entonces $\sigma(g)\widetilde{T} = \widetilde{T}\pi(g)$ para $g \in G$, es decir, $\widetilde{T}$ entrelaza π y σ.

En términos de las matrices (4.7) y las matrices $[t_{kj}]$ y $[\tilde{t}_{kj}]$ de T y $\widetilde{T}$, respectivamente, se escribe

$$\tilde{t}_{kj} = \frac{1}{|G|} \sum_{h \in G} \sum_{i,l} b_{kl}(h^{-1})\, t_{li}\, a_{ij}(h).$$

Ad (a): Si π y σ no son equivalentes, el lema de Schur muestra que $\widetilde{T} = 0$. Al tomar para T la aplicación lineal con matriz elemental E_{li}, se concluye que

$$\frac{1}{|G|} \sum_{h \in G} b_{kl}(h^{-1})\, a_{ij}(h) = 0 \quad \text{para todo} \quad i, j, k, l.$$

Como $\chi_\pi(h) = \sum_{i=1}^{n} a_{ii}(h)$ y $\chi_\sigma(h) = \sum_{k=1}^{m} b_{kk}(h)$, se deduce que $\langle \chi_\sigma \mid \chi_\pi \rangle = 0$.

Ad (b): En el caso de que $V = W$ y $\pi = \sigma$, el lema de Schur implica que $\widetilde{T} = \lambda\, 1_V$ con $\lambda = (\operatorname{Tr} T)/n$.

Nuevamente, al tomar para T la matriz elemental E_{li}, cuya traza es δ_{li}, se obtiene

$$\frac{1}{|G|} \sum_{h \in G} a_{kl}(h^{-1})\, a_{ij}(h) = \frac{1}{n}\, \delta_{li}\, \delta_{kj}.$$

Entonces es inmediato que

$$\langle \chi_\pi \mid \chi_\pi \rangle = \frac{1}{|G|} \sum_{h \in G} \sum_{i,k=1}^{n} a_{kk}(h^{-1})\, a_{ii}(h) = \frac{1}{n} \sum_{i,k=1}^{n} \delta_{ki} = \frac{n}{n} = 1. \qquad \square$$

Teorema 4.24. *Dos representaciones (unitarias, de grados finitos) de un grupo finito son equivalentes si y sólo si sus caracteres son iguales.*

Demostración. Sea $\pi\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ una representación (unitaria, sin perder generalidad) sobre un espacio $\mathbb{C}$-vectorial finitodimensional. Por el teorema de Maschke (Corolario 4.11), π es completamente reducible, así que $\pi = \pi_1 \oplus \pi_2 \oplus \cdots \oplus \pi_r$ donde cada π_i es una subrepresentación irreducible de π.

Por la Proposición 4.19, el carácter de π es $\chi_\pi = \chi_1 + \cdots + \chi_r$, donde cada χ_j es el carácter de la subrepresentación π_j.

Si ρ es una representación irreducible cualquiera de G, las Proposición 4.23 muestra que $\langle \chi_\rho \mid \chi_\pi \rangle \in \mathbb{N}$ es el número de sumandos π_j que son equivalentes a ρ. [Este número se llama la **multiplicidad** de ρ en la descomposición de π.]

Dos representaciones π y σ son equivalentes si y sólo si las multiplicidades de cada irreducible ρ en sus descomposiciones coinciden, si y sólo si $\langle \chi_\rho \mid \chi_\pi \rangle = \langle \chi_\rho \mid \chi_\sigma \rangle$ para cada irreducible ρ. Tanto χ_π como χ_σ son sumas finitas $\sum_\rho n_\rho\, \chi_\rho$ con coeficientes $n_\rho \in \mathbb{N}$, así que estos productos escalares son iguales si y sólo si $\chi_\pi = \chi_\sigma$. $\square$

Proposición 4.25. *Si G es un grupo finito, cada representación unitaria irreducible de G de grado n aparece, con multiplicidad n, en la descomposición de la representación regular.*

Demostración. Del Lema 4.17 y la fórmula (4.8b), la multiplicidad de la representación irreducible ρ en la representación regular λ es

$$n_\rho = \langle \chi_\rho \mid \chi_\lambda \rangle = \frac{1}{|G|} \sum_{h \in G} \chi_\rho(h^{-1})\, \chi_\lambda(h) = \frac{1}{|G|}\, \chi_\rho(1)\, \chi_\lambda(1) = \chi_\rho(1).$$

En efecto, $\chi_\lambda(h) = 0$ para $h \neq 1$ y $\chi_\lambda(1) = |G|$. Por otro lado, $\chi_\rho(1) = \dim_{\mathbb{F}} V_\rho$ es el grado de ρ.

En particular, esta multiplicidad $n_\rho = \dim_{\mathbb{F}} V_\rho$ no es nula: cada irreducible ρ ocurre en la descomposición de λ. □

Corolario 4.26. *Un grupo finito G posee un número finito de representaciones unitarias irreducibles inequivalentes $\pi_1, \dots, \pi_k$ con caracteres $\chi_1, \dots, \chi_k$. Los grados respectivos $n_1, \dots, n_k$ cumplen la relación:*

$$n_1^2 + n_2^2 + \cdots + n_k^2 = |G|. \tag{4.9}$$

Además, si $g \neq 1$ en G, entonces $\sum_{j=1}^{k} n_j\, \chi_j(g) = 0$.

Demostración. Como λ es equivalente a $n_1\pi_1 \oplus \cdots \oplus n_k\pi_k$, la Proposición 4.19 muestra que $\chi_\lambda(g) = \sum_{j=1}^{k} n_j\, \chi_j(g)$ para todo $g \in G$. El caso $g = 1$ comprueba la relación (4.9). □

Ejemplo 4.27. En el Ejemplo 4.8 se han visto dos representaciones irreducible del grupo S_3 (ahora con $\mathbb{F} = \mathbb{C}$). La recta diagonal $x = y = z$ de $\mathbb{C}^3$ lleva la *representación trivial* π_1, de grado uno. [Se define la representación trivial sobre $\mathbb{C}$ por $\pi_1(g) := 1$ para todo g.] Otra representación unidimensional de S_3, no mencionada en el Ejemplo 4.8, viene del *signo de las permutaciones*, esto es, $\pi_2(\sigma) := (-1)^\sigma$ para $\sigma \in S_3$.

El plano $x + y + z = 0$ en $\mathbb{C}^3$ lleva otra representación π_3 de S_3. Una base de este plano está formada por los dos vectores $x_1 := (1, \omega, \omega^2)$ y $x_2 := (1, \omega^2, \omega)$. Con respecto a esta base, las matrices de los $\pi_3(g)$ están dadas por:

$$\underline{1} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad (123) \mapsto \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix}, \quad (132) \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix},$$
$$(12) \mapsto \begin{pmatrix} 0 & \omega^2 \\ \omega & 0 \end{pmatrix}, \quad (13) \mapsto \begin{pmatrix} 0 & \omega \\ \omega^2 & 0 \end{pmatrix}, \quad (23) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{4.10}$$

Entonces $\chi_3 \colon S_3 \to \mathbb{C}$ toma los seis valores $2, -1, -1, 0, 0, 0$; al notar que $1 + \omega + \omega^2 = 0$. Por lo tanto, vale

$$\langle \chi_3 \mid \chi_3 \rangle = \frac{1}{6}(4 + 1 + 1 + 0 + 0 + 0) = 1,$$

lo cual comprueba que π_3 es irreducible (¡como si ya no fuera obvio!).

Ahora bien, $n_1^2 + n_2^2 + n_3^2 = 1 + 1 + 4 = 6 = |S_3|$. Esto demuestra que *no hay otras* representaciones irreducibles de S_3 que faltan por descubrir. ◊

► Si $\psi \in F_c(G, \mathbb{C})$ y si $\pi \colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ es una representación unitaria de G de grado finito, considérese el operador siguiente en $\mathrm{End}_{\mathbb{C}}(V)$:

$$\Pi_\psi := \sum_{h \in G} \psi(h)\, \pi(h). \tag{4.11}$$

Para todo $g \in G$, vale

$$\begin{aligned}\pi(g)\,\Pi_\psi\,\pi(g)^{-1} &= \sum_{h\in G}\psi(h)\,\pi(g)\pi(h)\pi(g^{-1}) = \sum_{h\in G}\psi(h)\,\pi(ghg^{-1})\\ &= \sum_{k\in G}\psi(g^{-1}kg)\,\pi(k) = \sum_{k\in G}\psi(k)\,\pi(k) = \Pi_\psi\end{aligned}$$

así que Π_ψ conmuta con la representación π. Si π es irreducible, el lema de Schur muestra que $\Pi_\psi = c_\psi\,1_V$. Al tomar trazas, se obtiene

$$c_\psi \dim_{\mathbb{C}} V = \sum_{h\in G}\psi(h)\,\chi_\pi(h) = |G|\langle\overline{\psi}\mid\chi_\pi\rangle. \tag{4.12}$$

Proposición 4.28. *Si G es un grupo finito, los caracteres $\chi_1,\dots,\chi_k$ de representaciones unitarias irreducibles forman una* base ortonormal *para el espacio $\mathbb{C}$-vectorial $F_c(G,\mathbb{C})$ de las funciones de clase complejas.*

Demostración. La Proposición 4.23 muestra que los caracteres $\chi_1,\dots,\chi_k$ forman una familia ortonormal en $F_c(G,\mathbb{C})$, con respecto al producto escalar (4.8). En particular, estos "caracteres irreducibles" son linealmente independientes.

Falta mostrar que ellos generan $F_c(G,\mathbb{C})$ como espacio vectorial. Para ese efecto, basta comprobar que esta familia ortonormal es *total*: es decir, que la única función de clase ortogonal a todo χ_j es la función nula.

Tómese $\varphi \in F_c(G,\mathbb{C})$ tal que $\langle\chi_j\mid\varphi\rangle = 0$ [o bien, lo que es lo mismo, $\langle\varphi\mid\chi_j\rangle = 0$] para $j = 1,\dots,k$. Escríbase $\psi := \overline{\varphi} \in F_c(G,\mathbb{C})$. Si π es una representación unitaria de G de grado finito, sea Π_ψ el operador correspondiente dado por (4.11). En el caso de que π sea irreducible, con $\pi = \pi_i$, la fórmula (4.12) muestra que $c_\psi \dim_{\mathbb{C}} V_i = |G|\langle\varphi\mid\chi_i\rangle = 0$, así que $\Pi_\psi = 0$. En el caso general, el teorema de Maschke muestra que Π_ψ es una suma directa de operadores nulos, de manera que $\Pi_\psi = 0$ en general.

En particular, para la representación regular λ de G, la fórmula (4.11) define un operador L_ψ sobre $V_\lambda \equiv \mathbb{C}[G]$ que cumple $L_\psi = 0$. Entonces

$$\sum_{h\in g}\psi(h)\,x_h = \sum_{h\in g}\psi(h)\,\lambda(h)\,x_1 = L_\psi x_1 = 0 \quad \text{en } V_\lambda.$$

Como los x_h son linealmente independientes, se concluye que $\psi = 0$ y también $\varphi = 0$ en $F_c(G,\mathbb{C})$, como se quería. □

Corolario 4.29. *El número de representaciones unitarias irreducibles inequivalentes de un grupo finito G coincide con el número de sus clases conjugadas.*

Demostración. Las funciones que valen 1 en alguna clase conjugada y 0 en las demás forman una base para $F_c(G,\mathbb{C})$. Luego $\dim_{\mathbb{C}} F_c(G,\mathbb{C})$ es el número de clases conjugadas.

Por otro lado, como $F_c(G,\mathbb{C})$ admite el producto escalar (4.8), su dimensión es la cardinalidad k de la base ortonormal $\{\chi_1,\ldots,\chi_k\}$. □

El grupo S_3 posee exactamente tres representaciones unitarias irreducibles porque posee tres clases conjugadas (el elemento neutro, las transposiciones, los 3-ciclos).

En un grupo finito *abeliano*, las clases conjugadas son todos los singuletes $\{g\} \subset G$. Las funciones $\chi_g : G \to \mathbb{C}^\times : h \mapsto \delta_{g,h}$ son caracteres y a la vez son representaciones unitarias unidimensionales, obviamente irreducibles. En este caso, las dos bases mencionadas de $F_c(G,\mathbb{C})$ coinciden.

► La coincidencia numérica de la enumeración de clases conjugadas con la cantidad de representaciones unitarias irreducibles hace factible ilustrar todas estas representaciones mediante una **tabla de caracteres**. Se trata de un arreglo cuadrado, cuyas filas corresponden con los caracteres irreducibles $\chi_1,\ldots,\chi_k$ y cuyas columnas corresponden con las clases conjugadas; se coloca el valor $\chi_j(g)$ en la fila j y en la columna de la clase de g. Por convenio, se reserva la primera fila para la representación trivial y la primera columna para las evaluaciones en 1, notando que $\chi_j(1) = \dim_{\mathbb{C}} V_j$.

Ejemplo 4.30. Con $b = (12)$, $c = (123)$, la tabla de caracteres del *grupo de permutaciones* S_3 es la siguiente:

S_3	1	b	c
χ_1	1	1	1
χ_2	1	−1	1
χ_3	2	0	−1

La tercera fila está formada por las trazas de las matrices (4.10). Nótese que las filas son ortonormales para el producto escalar (4.8):

$$\langle\chi_1 \mid \chi_1\rangle = \langle\chi_2 \mid \chi_2\rangle = \frac{1+3+2}{6} = 1, \qquad \langle\chi_3 \mid \chi_3\rangle = \frac{4+0+2}{6} = 1,$$
$$\langle\chi_1 \mid \chi_3\rangle = \langle\chi_2 \mid \chi_3\rangle = \frac{2+0-2}{6} = 0, \qquad \langle\chi_1 \mid \chi_2\rangle = \frac{1-3+2}{6} = 0. \qquad \Diamond$$

Resulta que las *columnas* de una tabla de caracteres también son ortogonales, con respecto a otro producto escalar. Denótese por $h_1,\ldots,h_k$ unos representantes de cada una de las clases conjugadas de un grupo finito G, con $h_1 = 1$. Sea m_r la cardinalidad de la clase de h_r. Entonces las columnas de la tabla de caracteres, cuyas entradas son los valores $\chi_j(h_r)$, son ortogonales como vectores de columna en $\mathbb{C}^k$, de acuerdo con el lema siguiente.

Lema 4.31. *Si $\chi_1, \ldots, \chi_k$ son los caracteres de las representaciones unitarias irreducibles de G, entonces se cumplen las siguientes relaciones de ortogonalidad:*

$$\sum_{j=1}^{k} \chi_j(h_r)\,\overline{\chi_j(h_s)} = \frac{|G|}{m_r}\,\delta_{rs}\,. \tag{4.13}$$

Demostración. Sea M la *matriz diagonal* $k \times k$ con entradas diagonales $m_1, \ldots, m_k$. La ortonormalidad de las *filas* de la tabla se escribe así, en vista de (4.8):

$$\begin{aligned}\delta_{ij} = \langle \chi_i \mid \chi_j \rangle &= \frac{1}{|G|}\sum_{h\in G} \chi_i(h^{-1})\,\chi_j(h) = \frac{1}{|G|}\sum_{h\in G} \overline{\chi_i(h)}\,\chi_j(h) \\ &= \frac{1}{|G|}\sum_{r=1}^{k} m_r\,\overline{\chi_i(h_r)}\,\chi_j(h_r).\end{aligned}$$

Sea $C = [c_{rj}]$ la *transpuesta* de la matriz de entradas de la tabla de caracteres; es decir, $c_{rj} := \chi_j(h_r)$. Las relaciones de ortogonalidad anteriores pueden resumirse en la siguiente igualdad matricial:

$$C^* M C = |G|\,1_k\,.$$

Aquí C^* denota el *conjugado hermítico* de la matriz C: su entrada (i,r) es $\bar{c}_{ri} = \overline{\chi_i(h_r)}$. Si B es la matriz diagonal con entradas diagonales $b_r := \sqrt{m_r/|G|}$, entonces la matriz $U := BC \in M_k(\mathbb{C})$ cumple $U^*U = 1_k$, es decir, U es una *matriz unitaria*.

Ahora bien, una matriz unitaria es invertible, porque $|\det U|^2 = \det(U^*U) = 1$; y se ve que $U^{-1} = U^*$. Entonces la ecuación $U^*U = 1_k$ conlleva $UU^* = 1_k$. Esto a su vez implica $BCC^*B = 1_k$ (fíjese que $B^* = B$ por ser B diagonal y real), y en consecuencia $CC^* = B^{-2}$. Esta última igualdad de matrices se expande en las ecuaciones (4.13). □

En términos del producto escalar usual de $\mathbb{C}^k$, las columnas de la tabla de caracteres son ortogonales entre sí y la "longitud al cuadrado" de la clase de h_r es $|G|/m_r$.

Fíjese que $|G|/m_r \in \mathbb{P}$ por el teorema de Lagrange, porque $m_r = [G\colon Z_G(h_r)]$ y por ende $|G|/m_r = |Z_G(h_r)|$.

Ejemplo 4.32. Las clases conjugadas del *grupo diedral* D_4 son cinco, con representantes $1 = \rho_0$, $m = \rho_\pi$, $r = \rho_{\pi/2}$, $s = \mu_0$, $t = \mu_{\pi/2}$. Debe de haber, entonces, cinco representaciones unitarias irreducibles (inequivalentes). El centro no es trivial: $Z(D_4) = \{1, m\} \simeq C_2$, ejemplificando la Proposición 1.79, y es fácil comprobar que $D_4/Z(D_4) \simeq V$. Al componer el homomorfismo cociente $\eta\colon D_4 \to V$ con cada uno de las cuatro representaciones irreducibles $\sigma_j\colon V \to \mathbb{C}^\times$, resultan cuatro representaciones unitarias irreducibles $\pi_j := \sigma_j \circ \eta$ del grupo D_4, para $j = 1, 2, 3, 4$, todos de grado 1.

Falta una representación más, π_5, que debe ser de grado 2 a partir de (4.9), puesto que $1+1+1+1+4=8$.

Los $\sigma_j\colon V \to \mathbb{C}^\times$ solo puede tomar valores en $\{1,-1\}$, ya que V tiene exponente 2. Esto da las primeras cuatro filas de la tabla de caracteres de D_4:

D_4	1	m	r	s	t
χ_1	1	1	1	1	1
χ_2	1	1	1	−1	−1
χ_3	1	1	−1	1	−1
χ_4	1	1	−1	−1	1
χ_5	2	−2	0	0	0

La última fila empieza con $2=\chi_5(1)=\dim_{\mathbb{C}} V_5$. Si esta fila es $(2,q,j,k,l)\in\mathbb{N}^5$, entonces $2+q+2(\pm j\pm k\pm l)=0$ para cuatro patrones de signo diferentes. Luego $j=k=l=0$ y además $q=-2$.

No hay que ir muy lejos para encontrar una representación de D_4 en matrices 2×2 con estas trazas: la definición original de D_4 en el Ejemplo 1.13, como subgrupo finito de O(2), ¡es precisamente la representación π_5! ◊

Ejemplo 4.33. El *grupo alternante* A_4 tiene cuatro clases conjugadas, representadas por los elementos típicos $1=\underline{1}$, $a=(12)(34)$, $b=(123)$, $c=(132)$.

⟦ Fíjese que los 3-ciclos (123) y (132) son conjugados en S_3 o en S_4, pero no son conjugados en A_4. ⟧

Los pares de transposiciones, juntos son el elemento neutro, forman un subgrupo normal $N=\{1,a,bab^{-1},cac^{-1}\}$, porque este es el único 2-subgrupo de Sylow de A_4; los demás elementos de A_4 son 3-ciclos. Está claro que $A_4/N=\{N,bN,cN\}\simeq C_3$. Entonces las tres representaciones irreducibles del grupo abeliano C_3, compuestas con el homomorfismo cociente $\eta\colon A_4\to C_3$, dan tres representaciones irreducibles π_1, π_2, π_3 de A_4, todos de rango 1.

La cuarta representación irreducible debe tener rango 3 pues $|A_4|=12=1+1+1+9$. La tabla de caracteres de A_4 es la siguiente:

A_4	1	a	b	c
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	−1	0	0

La última fila empieza con $3 = \chi_4(1) = \dim_{\mathbb{C}} V_4$. Si esta fila es $(3, q, j, k) \in \mathbb{N}^4$, la ortogonalidad de las filas implica que

$$3 + 3q + 4(j + k) = 3 + 3q + 4(j\omega + k\omega^2) = 3 + 3q + 4(j\omega^2 + k\omega) = 0,$$

así que $j = k = 0$ y además $q = -1$.

Se sabe que A_4 actúa en $\mathbb{R}^3$, y de igual manera en $\mathbb{C}^3$, por rotaciones de un tetraedro regular centrado en el origen. Por ejemplo, se puede tomar cuatro de las ocho esquinas de un cubo como vértices del tetraedro: $(1,-1,-1)$, $(-1,1,-1)$, $(-1,-1,1)$ y $(1,1,1)$. La acción de los 3-ciclos b y c deja fijo el cuarto vértice y permuta los primeros tres; ellos actúan por rotaciones de ángulos $\pm 2\pi/3$ alrededor de la recta que pasa por el origen y $(1,1,1)$. El elemento a y sus conjugados actúan por rotaciones de π alrededor de los ejes coordenados. Concretamente:

$$a \mapsto A := \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad b \mapsto B := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad c \mapsto C := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

La acción de b y c deja fijo únicamente la recta $x = y = z$ y el plano $x + y + z = 0$, pero la acción de a no los preserva; luego esta acción de A_4 es irreducible en $\mathbb{R}^3$ o $\mathbb{C}^3$. Al calcular las trazas de las matrices exhibidas, se ve que esta acción de A_4 por rotaciones del tetraedro regular es precisamente la representación π_4. En efecto, se ve que $\chi_4(a) = \operatorname{tr} A = -1$, $\chi_4(b) = \operatorname{tr} B = 0$, y $\chi_4(c) = \operatorname{tr} C = 0$. ◊

En el Ejemplo 1.31, se identificó las cinco clases conjugadas de S_4 por sus patrones de productos de ciclos disjuntos. El Corolario 4.29 muestra que S_4 posee cinco representaciones unitarias irreducibles inequivalentes. Ellos son la representación trivial π_1, la representación de signo $\pi_2(\sigma) := (-1)^\sigma$ de rango 1, y tres más. Al expresar $|S_4| = 24$ como una suma de cuadrados, la única posibilidad es

$$|S_4| = 24 = 1 + 1 + 4 + 9 + 9.$$

Luego debe haber una representación π_3 de rango 2; y otros dos, π_4 y π_5, de rango 3.

4.3 Representaciones inducidas

Si $\pi\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ es una representación unitaria de un grupo G, su **restricción** *a un subgrupo* $H \leqslant G$ define una representación de H sobre el mismo espacio $\mathbb{C}$-vectorial V. Esta restricción se puede denotar por $\pi_H\colon H \to \mathrm{GL}_{\mathbb{C}}(V)$; por definición, $\pi_H(h) := \pi(h)$ para todo $h \in H$.

Si π es irreducible, la restricción π_H generalmente no es irreducible como representación de H. Por ejemplo, si H es un subgrupo abeliano, entonces π_H es una suma directa de subrepresentaciones de rango 1. En el Ejemplo 4.27 se exhibe la representación irreducible π_3 de grupo S_3, cuyo rango es 2, pero su restricción al subgrupo abeliano C_3 es reducible, como evidencian las primeras tres matrices diagonales en el despliegue (4.10).

Otro ejemplo de restricción de representaciones ocurre con la *representación regular* $\lambda\colon G \to \mathbb{C}[G]$ de un grupo finito, dado por $\lambda(g)\,x_k := x_{gk}$ para $k \in G$, según el Ejemplo 4.9. Entonces $\lambda_H(h)\,x_k = x_{hk}$ para $h \in H$ y $k \in G$. Sea $W = \operatorname{lin}\langle x_h : h \in H\rangle$ el subespacio de $V = \mathbb{C}[G]$ generado por la porción de la base que corresponde al subgrupo H. Entonces W es un subespacio invariante bajo λ_H y la subrepresentación correspondiente no es otra cosa que la representación regular de H. Además, si $\{1, g_2, \dots, g_m\}$, con $m = [G{:}H]$, es una familia de representantes de las coclases gH en G/H, entonces hay una suma directa de subespacios

$$V = W \oplus \lambda(g_2)W \oplus \cdots \oplus \lambda(g_m)W, \tag{4.14}$$

donde W es invariante bajo λ_H y cada sumando $\lambda(g_i)W$ solo depende de la coclase g_iH, pues $\lambda(g_ih)W = \lambda(g_i)\lambda(h)W = \lambda(g_i)W$ si $h \in H$.

► En la dirección opuesta, se quiere fabricar una representación del grupo G a partir de una representación dada de un subgrupo H. Esto resulta posible si se conserva la estructura genérica de la representación, en el sentido de la definición siguiente.

Definición 4.34. Sea G un grupo finito y H un subgrupo de G con $[G{:}H] = m$; escríbase $G/H = \{H, g_2H, \dots, g_mH\}$. Una representación unitaria $\sigma\colon H \to \mathrm{GL}_{\mathbb{C}}(W)$ **induce** una representación $\pi\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ con $W \leqslant V$ si

$$V = W \oplus W_2 \oplus \cdots \oplus W_m, \quad \text{donde} \quad \begin{cases} \pi(h)|_W = \sigma(h) & \text{si } h \in H, \\ \pi(g)W_i = W_{g\cdot i} & \text{si } g \in G, \end{cases} \tag{4.15}$$

donde $g \cdot i = j$ cuando $gg_iH = g_jH$. Nótese que $\dim_{\mathbb{C}} V = [G{:}H]\dim_{\mathbb{C}} W$ porque la suma de subespacios es directa. ◊

Proposición 4.35. *Sea $\pi\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ una representación unitaria de un grupo finito inducida por una representación $\sigma\colon H \to \mathrm{GL}_{\mathbb{C}}(W)$ de un subgrupo $H \leqslant G$. Si $\tau\colon G \to \mathrm{GL}_{\mathbb{C}}(U)$ es otra representación unitaria de G, sea $S\colon W \to U$ una aplicación $\mathbb{C}$-lineal tal que $S \circ \sigma(h) = \tau(h) \circ S : W \to U$ para todo $h \in H$; entonces existe una única aplicación $\mathbb{C}$-lineal $T\colon V \to U$ tal que $T|_W = S$ y $T \circ \pi(g) = \tau(g) \circ T : V \to U$ para todo $g \in G$.*

Demostración. Para la *unicidad* de T, fíjese que si $y \in W_i$, entonces $\pi(g_i^{-1})y \in W$, así que

$$Ty = T\pi(g_i)\big[\pi(g_i^{-1})y\big] = \tau(g_i)\,T\big[\pi(g_i^{-1})y\big] = \tau(g_i)\,S\big[\pi(g_i^{-1})y\big].$$

Entonces T queda determinada sobre cada W_i y por ende sobre su suma directa V.

Para la *existencia* de T, el resultado del cálculo anterior sirve como una definición:

$$Ty := \tau(g_i)\,S\big[\pi(g_i^{-1})y\big] \quad \text{para} \quad y \in W_i.$$

Falta comprobar que T está bien definida por esta fórmula, es decir, que no depende del elemento $g_i \in G$ que representa la coclase g_iH. Es cuestión de notar que, para todo $h \in H$, vale

$$\begin{aligned}\tau(g_ih)\,S\big[\pi((g_ih)^{-1})y\big] &= \tau(g_i)\,\tau(h)\,S\big[\sigma(h^{-1})\pi(g_i^{-1})y\big] \\ &= \tau(g_i)\,S\,\sigma(h)\big[\sigma(h^{-1})\pi(g_i^{-1})y\big] = \tau(g_i)\,S\big[\pi(g_i^{-1})y\big].\end{aligned}$$

Entonces T está bien definida sobre cada W_i y $Ty = Sy$ para $y \in W$ (al tomar $g_1 = 1$). Como la suma de subespacios en (4.15) es directa, cada $x \in V$ se puede escribir de manera única como $x = y_1 + y_2 + \cdots + y_m$ con $y_i \in W_i$ para $i = 1, \ldots, m$ (donde $W_1 = W$); y se define $Tx := Ty_1 + \cdots + Ty_m$.

Si $g \in G$, $y \in W_i$, se puede tomar $g_j := gg_i$. Entonces $\pi(g)y \in W_j$, así que

$$T\pi(g)y = \tau(g_j)\,S\big[\pi(g_j^{-1})\,\pi(g)y\big] = \tau(g)\,\tau(g_i)\,S\big[\pi(g_i^{-1})y\big] = \tau(g)\,Ty.$$

Esto verifica que $T \circ \pi(g) = \tau(g) \circ T$ para todo $g \in G$. □

Corolario 4.36. *Sea H un subgrupo de un grupo finito G y sea $\sigma\colon H \to \mathrm{GL}_{\mathbb{C}}(W)$ una representación unitaria de H. Entonces existe una representación unitaria $\pi\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ inducida por σ y esta representación inducida es única hasta equivalencia.*

Demostración. Si dos representaciones σ_1 y σ_2 de H inducen representaciones π_1 y π_2 de G, es fácil chequear que la representación $\sigma_1 \oplus \sigma_2$ de H induce la representación $\pi_1 \oplus \pi_2$ de G. Luego, para la existencia de π, se puede suponer que σ es irreducible. En tal caso σ es una subrepresentación de la representación regular de H y con la suma directa (4.14) se puede fabricar una representación inducida π de G.

Si $\tau\colon G \to \mathrm{GL}_{\mathbb{C}}(U)$ es otra representación unitaria de G inducida por la misma σ, la *inclusión* $S\colon W \hookrightarrow U$ cumple $S \circ \sigma(h) = \tau(h) \circ S$ para todo $h \in H$; en efecto, esto es otra manera de decir que $\tau(h)|W = \sigma(h)$ para $h \in H$. La Proposición anterior entonces proporciona una aplicación $\mathbb{C}$-lineal $T\colon V \to U$ que entrelaza las representaciones π y τ y coincide con 1_W sobre el subespacio W.

La relación $T\circ\pi(g)=\tau(g)\circ T$ implica que la imagen de T incluye cada $\tau(g)W$, así que T es sobreyectiva. Como $\dim_{\mathbb{C}} U=[G{:}H]\dim_{\mathbb{C}} W=\dim_{\mathbb{C}} V$ (estas dimensiones son finitas porque σ es irreducible), entonces T es también inyectiva. El operador entrelazante invertible T establece la equivalencia $\pi\sim\tau$. □

Notación. Si $H\leqslant G$ y σ es una representación unitaria de H, se denota por σ^G la representación de G inducida por σ. Con esta notación, la Proposición 4.35 puede reformularse como sigue.

Proposición 4.37. *Sea H un subgrupo de un grupo finito G; si $\sigma\colon H\to \mathrm{GL}_{\mathbb{C}}(W)$ es una representación unitaria de H que induce una representación unitaria $\pi\colon G\to\mathrm{GL}_{\mathbb{C}}(V)$; y si $\tau\colon G\to\mathrm{GL}_{\mathbb{C}}(U)$ es una representación unitaria de G, entonces hay un isomorfismo $\mathbb{C}$-lineal*

$$\mathrm{Hom}_{\mathbb{C}[H]}(W,U)\simeq\mathrm{Hom}_{\mathbb{C}[G]}(V,U) \tag{4.16}$$

que lleva cada operador $S\colon W\to U$ que entrelaza σ y τ en un operador $T\colon V\to U$ que entrelaza σ^G y τ. El isomorfismo inverso lleva cada T en su restricción $S:=T|_W$. ⊟

► Es posible calcular el carácter de una representación inducida σ^G en términos del carácter de la representación original σ, por una famosa fórmula de Frobenius.

Proposición 4.38 (Frobenius)**.** *Sea G un grupo finito y H un subgrupo de G con $[G{:}H]=m$; escríbase $G/H=\{H,g_2H,\dots,g_mH\}$. Si $\sigma\colon H\to\mathrm{GL}_{\mathbb{C}}(W)$ es una representación unitaria de H, el carácter de la representación inducida $\pi=\sigma^G$ de G está dado por*

$$\chi_\pi(k)=\sum_{i\,:\,g_i^{-1}kg_i\in H}\chi_\sigma(g_i^{-1}kg_i)=\frac{1}{|H|}\sum_{g\,:\,g^{-1}kg\in H}\chi_\sigma(g^{-1}kg) \tag{4.17}$$

para todo $k\in G$.

Demostración. Por la definición de representación inducida, cada operador $\pi(k)$ sobre V permuta los subespacios $W_j=\pi(g_j)W$ entre sí. Cada elemento kg_j queda en alguna coclase de H, así que $kg_j=g_ih$ para algún i y algún $h\in H$. Luego, $\pi(k)$ lleva W_j en $\pi(g_i)W=W_i$.

Para calcular la traza $\chi_\pi(k)=\mathrm{Tr}\,\pi(k)$, elíjase una base de V formado por una unión de bases de los W_i. Con respecto a esta base, $\pi(k)$ posee una matriz de bloques; los índices j para los cuales $g_j\neq g_i$ marcan columnas con *un bloque de ceros en la diagonal*: estas contribuyen cero a la traza de $\pi(k)$. En cambio, para $g_j=g_i$ la matriz tiene un bloque diagonal que contribuye a la traza. Ahora bien, la relación $kg_i=g_ih$ dice que $g_i^{-1}kg_i\in H$: este es el requisito para tener una contribución no nula a la traza.

Si $g_i^{-1}kg_i = h \in H$, entonces $\rho(g_i)$ es un isomorfismo entre los subespacios W y W_i, que entrelaza $\pi(k)|_{W_i}$ con $\pi(h)|_W = \sigma(h)$: la traza de este bloque es $\operatorname{Tr}\sigma(h) = \chi_\sigma(h) = \chi_\sigma(g_i^{-1}kg_i)$. Al sumar estas trazas parciales, se obtiene la primera igualdad en (4.17).

La segunda igualdad es inmediata, al tomar en cuenta que si $g^{-1}kg \in H$ con $g = g_i h$, entonces $\chi_\sigma(g^{-1}kg) = \chi_\sigma(h^{-1}g_i^{-1}kg_ih) = \chi_\sigma(g_i^{-1}kg_i)$ por ser χ_σ una función de clase sobre H; aunque de esta manera los términos $\chi_\sigma(g_i^{-1}kg_i)$ estarían sobrecontados $|H|$ veces cada uno. □

Dados dos representaciones unitarias $\pi\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ y $\sigma\colon H \to \mathrm{GL}_{\mathbb{C}}(W)$ sin relación alguna *a priori*, ahora se puede comparar π_H con σ, o bien π con σ^G. Ya se ha observado que π_H generalmente es reducible aunque π sea irreducible. También es cierto que σ^G generalmente es reducible aun cuando σ sea una representación irreducible de H.

El producto escalar de caracteres proporciona una manera de contar estas multiplicidades. Si $\pi \sim m_1\pi_1 \oplus \cdots \oplus m_k\pi_k$ es la descomposición en irreducibles de una representación unitaria de G, entonces

$$\langle \chi_\pi \mid \chi_\pi \rangle_G = m_1^2 + m_2^2 + \cdots + m_k^2$$

en vista de la Proposición 4.23. El lado derecho vale 1 si y sólo si $m_j = 1$ para algún j y $m_i = 0$ para $i \neq j$; si *y sólo si* π es irreducible. En la ecuación anterior, el subíndice al producto escalar hace notar que se trata del producto escalar de caracteres (o más generalmente, de funciones de clase) del grupo G. El coeficiente $m_i = \langle \chi_i \mid \chi_\pi \rangle_G$ es la multiplicidad de π_i en (la descomposición de) la representación π.

El siguiente resultado se llama el **teorema de reciprocidad de Frobenius**.

Proposición 4.39. *Sean $\pi\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ y $\sigma\colon H \to \mathrm{GL}_{\mathbb{C}}(W)$ dos representaciones unitarias de un grupo finito G y de un subgrupo $H \leqslant G$, respectivamente. Entonces*

$$\langle \chi_{\sigma^G} \mid \chi_\pi \rangle_G = \langle \chi_\sigma \mid \chi_{\pi_H} \rangle_H . \tag{4.18}$$

Demostración. Este es un cálculo directo, empleando la definición (4.8) del producto escalar y la fórmula (4.17) para χ_{σ^G}:

$$\begin{aligned}
\langle \chi_{\sigma^G} \mid \chi_\pi \rangle_G &= \frac{1}{|G|} \sum_{k\in G} \overline{\chi_{\sigma^G}(k)}\, \chi_\pi(k) = \frac{1}{|G|}\frac{1}{|H|} \sum_{k\in G} \sum_{g\,:\, g^{-1}kg\in H} \overline{\chi_\sigma(g^{-1}kg)}\, \chi_\pi(k) \\
&= \frac{1}{|G|}\frac{1}{|H|} \sum_{g\in G}\sum_{h\in H} \overline{\chi_\sigma(h)}\, \chi_\pi(ghg^{-1}) = \frac{1}{|G|}\frac{1}{|H|} \sum_{g\in G}\sum_{h\in H} \overline{\chi_\sigma(h)}\, \chi_\pi(h) \\
&= \frac{1}{|H|} \sum_{h\in H} \overline{\chi_\sigma(h)}\, \chi_\pi(h) = \langle \chi_\sigma \mid \chi_{\pi_H} \rangle_H .
\end{aligned}$$

La cuarta igualdad es válida porque χ_π es una función de clase sobre H. □

Una demostración alternativa, más conceptual, es la siguiente. Si $\sigma \sim s_1\sigma_1 \oplus \cdots \oplus s_k\sigma_l$ y $\pi_H \sim t_1\sigma_1 \oplus \cdots \oplus t_k\sigma_l$ son descomposiciones de σ y π_H en representaciones unitarias irreducibles de H, entonces $\langle \chi_\sigma \,|\, \chi_{\pi_H} \rangle_H = s_1t_1 + \cdots + s_lt_l$. En vista del Lema de Schur, este es la dimensión del espacio $\mathbb{C}$-vectorial $\mathrm{Hom}_{\mathbb{C}[H]}(W, \mathrm{Res}\, V)$, donde se considera W como un H-módulo – es decir, un módulo a izquierda para el anillo $\mathbb{C}[H]$ – y $\mathrm{Res}\, V$ denota el espacio vectorial V considerado como H-módulo (por restricción de la acción de $\mathbb{C}[G]$ al subanillo $\mathbb{C}[H]$), en vez de G-módulo.

Por otro lado, el H-módulo W da lugar a un G-módulo, denotado por $W \oplus W_2 \oplus \cdots \oplus W_m$ en (4.15), que ahora puede denotarse por $\mathrm{Ind}\, W$. El producto escalar $\langle \chi_{\sigma^G} \,|\, \chi_\pi \rangle_G$ es la dimensión del espacio $\mathbb{C}$-vectorial $\mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}\, W, V)$. Para mostrar que estas dimensiones son iguales, sólo es necesario comprobar que hay un isomorfismo $\mathbb{C}$-lineal

$$\mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}\, W, V) \simeq \mathrm{Hom}_{\mathbb{C}[H]}(W, \mathrm{Res}\, V). \tag{4.19}$$

Pero esto es una consecuencia inmediata de la Proposición 4.37, al reemplazar π por σ^G y V por $\mathrm{Ind}\, W$; y al reemplazar τ y U por π y V, respectivamente.

El isomorfismo (4.19) tiene una interpretación categórica. Al lado izquierdo hay un conjunto (que resulta ser un espacio $\mathbb{C}$-vectorial) de morfismos en la categoría $\mathbb{C}[G]$-Mod de G-módulos, mientras al lado derecho aparece un conjunto de morfismos en la categoría $\mathbb{C}[H]$-Mod de H-módulos. Luego, se puede considerar la restricción como un *funtor* $\mathrm{Res}\colon \mathbb{C}[G]\text{-Mod} \to \mathbb{C}[H]\text{-Mod}$, dado por $V \mapsto \mathrm{Res}\, V$ (el mismo espacio vectorial, con una acción de H por restricción) y por $S \mapsto S$ (el mismo operador, restringido a entrelazar acciones del subgrupo H).

Otro funtor en juego es la *inducción* $\mathrm{Ind}\colon \mathbb{C}[H]\text{-Mod} \to \mathbb{C}[G]\text{-Mod}$, cuya existencia viene de la Proposición 4.35 y del Corolario 4.36, dado por $\mathrm{Ind}\, W := W \oplus W_2 \oplus \cdots \oplus W_m$ sobre objetos y $\mathrm{Ind}\, S := T$ sobre morfismos. Si hay un subgrupo intermedio K tal que $H \leqslant K \leqslant G$, no es difícil comprobar la propiedad de *inducción por etapas* $(\sigma^K)^G \sim \sigma^G$, necesaria para verificar que Ind es efectivamente un funtor.

Ahora bien, el isomorfismo (4.19) ejemplifica un concepto importante: Res e Ind son *funtores adjuntos*. En general, dos funtores $\mathscr{F}\colon \mathsf{C} \to \mathsf{D}$ y $\mathscr{G}\colon \mathsf{D} \to \mathsf{C}$ se llaman adjuntos si para cada par de objetos A en $\mathrm{Ob}(\mathsf{C})$ y B en $\mathrm{Ob}(\mathsf{D})$, hay una biyección $\mathrm{Hom}_{\mathsf{D}}(\mathscr{F}A, B) \leftrightarrow \mathrm{Hom}_{\mathsf{D}}(A, \mathscr{G}B)$, que es "natural" en A y en B.[8] (Con más precisión, se dice que $\mathscr{G}$ es un *adjunto a derecha* de $\mathscr{F}$ y que $\mathscr{F}$ es un *adjunto a izquierda* de $\mathscr{G}$.) Hay una analogía visual entre esta situación y la del adjunto de un operador lineal con respecto a un par de productos escalares; de ahí la terminología.

[8] Para el alcance preciso del adjetivo "natural" en este contexto, véase, por ejemplo, el segundo tomo del libro de Jacobson.

► En los ejemplos que siguen, $\pi_1, \ldots, \pi_k$ denotan las representaciones unitarias irreducibles de un grupo finito G, con caracteres $\chi_1, \ldots, \chi_k$; mientras $\sigma_1, \ldots, \sigma_l$ denotan las representaciones unitarias irreducibles de un subgrupo $H \leqslant G$, con caracteres $\psi_1, \ldots, \psi_l$.

Ejemplo 4.40. Si $G = S_3$ y $H = C_2$, entonces σ_1 tiene grado 1 y σ_1^G es una representación de S_3 de grado 3, porque $[S_3{:}C_2] = 3$. Luego σ_1^G es reducible. Al restringir los caracteres de S_3 a $C_2 = \{1, b\}$ con $b = (12)$, se obtiene

$$\langle \psi_1 \mid \chi_{j,H} \rangle_H = \frac{1}{2}\big(\psi_1(1)\,\chi_j(1) + \psi_1(b^{-1})\,\chi_j(b)\big) = \frac{1}{2}\big(\chi_j(1) + \chi_j(b)\big).$$

De la tabla de caracteres de S_3 en el Ejemplo 4.30, se obtiene los valores $1, 0, 1$ para los casos $j = 1, 2, 3$. La reciprocidad de Frobenius dice que estos también son los valores de $\langle \psi_1^G \mid \chi_j \rangle_G$, donde $\psi_1^G := \operatorname{Tr} \sigma_1^G$. Se concluye que $\sigma_1^G \sim \pi_1 \oplus \pi_3$.

De modo similar, $\langle \psi_2 | \chi_{j,H} \rangle_H = \frac{1}{2}\big(\chi_j(1) - \chi_j(b)\big)$ toma los valores $0, 1, 1$ para $j = 1, 2, 3$. La reciprocidad de Frobenius ahora muestra que $\sigma_2^G \sim \pi_2 \oplus \pi_3$. ◊

Ejemplo 4.41. Si $G = S_3$ y $H = C_3$, entonces σ_1 tiene grado 1 y σ_1^G es una representación de S_3 de grado 2, porque $[S_3{:}C_3] = 2$. Los caracteres irreducibles de C_3 son visibles en las primeras tres filas de la tabla de caracteres de A_4, al omitir la segunda columna: si $C_3 = \{1, b, b^2\}$ con $b = (123)$, entonces $\psi_1(b) = 1$, $\psi_2(b) = \omega$, $\psi_3(b) = \omega^2$.

Ahora el lado derecho de (4.18) toma la forma

$$\langle \psi_i \mid \chi_{j,H} \rangle_H = \frac{1}{3}\big(\psi_i(1)\,\chi_j(1) + \psi_i(b^2)\,\chi_j(b) + \psi_i(b)\,\chi_j(b^2)\big),$$

De las fórmulas (4.10) se obtiene $\chi_3(1) = 2$ y $\chi_3(b) = \chi_3(b^2) = -1$, mientras χ_1 y χ_2 toman el valor constante 1 sobre el subgrupo C_3. Como $1 + \omega + \omega^2 = 0$, los productos escalares dan los siguientes valores: $1, 1, 0$ para ψ_1; $0, 0, 1$ para ψ_2; y $0, 0, 1$ para ψ_3.

Entonces la reciprocidad de Frobenius muestra que $\sigma_1^G \sim \pi_1 \oplus \pi_2$, reducible de grado 2; mientras $\sigma_2^G \sim \sigma_3^G \sim \pi_3$, irreducible de grado 2. ◊

Ejemplo 4.42. Si $G = S_4$ y $H = S_3$, se puede comparar las cinco representaciones irreducibles de S_4 con las tres representaciones inducidas σ_1^G, σ_2^G, σ_3^G a partir de las de S_3. Como σ_1 y σ_2 tienen grado 1, las representaciones σ_1^G y σ_2^G de S_4 tienen grado 4, porque $[S_4{:}S_3] = 4$. Como σ_3 tiene grado 2, σ_3^G tiene grado 8. Ninguna de estas representaciones inducidas es irreducible.

Hace falta exhibir la tabla de caracteres de S_4 para llevar a cabo el cálculo detallado, siguiendo el patrón de los dos ejemplos anteriores. El resultado del cálculo es el siguiente:

$$\sigma_1^G \sim \pi_1 \oplus \pi_5, \qquad \sigma_2^G \sim \pi_2 \oplus \pi_4, \qquad \sigma_3^G \sim \pi_3 \oplus \pi_4 \oplus \pi_5. \qquad \text{◊}$$

Ejercicios

1.1 Ejercicios básicos sobre grupos

Ejercicio 1.1. Si G es un grupo finito con un número par de elementos, $|G| = 2m$, demostrar que al menos hay un elemento $g \in G$ con $g \neq 1$ tal que $g^{-1} = g$.

Ejercicio 1.2. Si G es un grupo que cumple uno de estos hipótesis:

(a) $(gh)^2 = g^2h^2$ para todo $g, h \in G$; o bien

(b) $g^2 = 1$ para todo $g \in G$;

demostrar que el grupo G es abeliano.

Ejercicio 1.3. Es posible definir el producto en un grupo finito de n elementos al exhibir su **tabla de multiplicación**. Esta es una matriz $n \times n$, bordeada por una fila y una columna de los elementos del grupo, comenzando por 1; la entrada en la fila g y la columna h de la matriz es el producto gh:

$\bullet$	1	$\dots$	h	$\dots$
1	1	$\dots$	h	$\dots$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$
g	g	$\dots$	gh	$\dots$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$

Por ejemplo, si $\sigma = \rho_{2\pi/3}$, esta es la tabla de multiplicación del grupo de rotaciones C_3:

$\bullet$	1	σ	σ^2
1	1	σ	σ^2
σ	σ	σ^2	1
σ^2	σ^2	1	σ

Esta matriz depende del orden de los elementos en la fila y la columna del borde; no se distinguen dos tablas que coinciden hasta permutaciones de sus filas y columnas.

En el caso $n = 4$, comprobar que hay solamente dos tablas de multiplicación distinguibles, dando un ejemplo de cada una.

Ejercicio 1.4. El **producto directo** de dos grupos G y K es el producto cartesiano $G \times K$, dotado de la operación binaria $(g_1, k_1) \cdot (g_2, k_2) := (g_1g_2, k_1k_2)$. Demostrar que esta operación es asociativa. Encontrar un elemento neutro y un inverso para un elemento típico $(g, k) \in G \times K$, mostrando así que $G \times K$ es un grupo.

Ejercicio 1.5. Obtener todos los subgrupos de D_3 y de C_{12}.

Ejercicio 1.6. Si G es un grupo finito sin subgrupos no triviales, demostrar que G es un grupo cíclico de orden p para algún número primo p.

Ejercicio 1.7. Si $g \in G$ es un elemento de período rs, donde $r \perp s$ [es decir, r y s son *relativamente primos*], demostrar que hay elementos $h, k \in G$ donde h tiene período r y k tiene período s tales que $g = hk = kh$. ⟦ Indicación: Recordar que $r \perp s$ si y sólo si hay enteros $a, b \in \mathbb{Z}$ con $ar + bs = 1$. ⟧

Ejercicio 1.8. En el grupo $\mathrm{GL}(2,\mathbb{R})$, sean $g := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $h := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$; demostrar que g tiene período 4 y h tiene período 3 pero gh no tiene período finito.

Ejercicio 1.9. Sea $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$ el cuerpo finito con dos elementos. Escribir la lista de los elementos del grupo $G = \mathrm{GL}(2, \mathbb{F}_2)$ para obtener así su orden $|G|$. ¿Es G un grupo abeliano o no abeliano?

Ejercicio 1.10. Una matriz $A \in \mathrm{GL}(n,\mathbb{R})$ es una **matriz ortogonal** si $A^t A = AA^t = 1_n$, es decir, su *transpuesta* A^t coincide con su matriz inversa. Comprobar que una matriz A es ortogonal si y sólo si sus columnas forman una *base ortonormal* de $\mathbb{R}^n$ (con respecto al producto escalar usual en $\mathbb{R}^n$). Demostrar que $\det A = \pm 1$ para toda matriz ortogonal.

Denótese por $\mathrm{O}(n)$ el **grupo ortogonal** de las matrices ortogonales reales $n \times n$. El subgrupo

$$\mathrm{SO}(n) := \{ A \in \mathrm{O}(n) : \det A = 1 \}$$

se llama el **grupo ortogonal especial** $n \times n$. Demostrar que $\mathrm{SO}(n)$ es abeliano si y sólo si $n = 1$ ó $n = 2$.

Ejercicio 1.11. Una matriz $U \in \mathrm{GL}(n,\mathbb{C})$ es una **matriz unitaria** si $U^* U = UU^* = 1_n$, es decir, su *transpuesta conjugada* U^* coincide con su matriz inversa.[1] Comprobar que una matriz U es unitaria si y sólo si sus columnas forman una *base ortonormal* de $\mathbb{C}^n$ con respecto al producto escalar usual de $\mathbb{C}^n$, dado por $\langle z \mid w \rangle := \bar{z}_1 w_1 + \bar{z}_2 w_2 + \cdots + \bar{z}_n w_n$. Demostrar que $|\det A| = 1$ para toda matriz unitaria.

Denótese por $\mathrm{U}(n)$ el **grupo unitario** de las matrices unitarias complejas $n \times n$. El subgrupo

$$\mathrm{SU}(n) := \{ U \in \mathrm{U}(n) : \det U = 1 \}$$

[1] Si $A = [a_{ij}]$, entonces $A^* = [\bar{a}_{ji}]$. Dícese que A^* es la **transpuesta conjugada**, o bien la **matriz adjunta** de A. El segundo término no debe confundirse con la *matriz adjugada* $\mathrm{adj}\, A$ que aparece el la regla de Cramer para inversión, $A^{-1} = (1/\det A)\, \mathrm{adj}\, A$.

se llama el **grupo unitario especial** $n \times n$. Demostrar que $\mathrm{SU}(n)$ es abeliano si y sólo si $n = 1$. ¿Cuáles números complejos pertenecen a $\mathrm{U}(1)$?

1.2 Ejercicios sobre subgrupos normales

Ejercicio 1.12. Si G es un grupo y si $K \leqslant H \leqslant G$, demostrar que $[G : K] = [G : H][H : K]$.

Ejercicio 1.13. Sea $H \leqslant G$ tal que $|H| = m$ y supóngase que H es el *único* subgrupo de G de orden m. Demostrar que $H \trianglelefteq G$.

Ejercicio 1.14. Si $H \trianglelefteq G$ y $K \trianglelefteq G$, demostrar que $H \cap K \trianglelefteq G$ y que $HK \trianglelefteq G$.

Ejercicio 1.15. Si H, K son dos subgrupos normales de G tales que $H \cap K = \{1\}$, comprobar que $hk = kh$ para todo $h \in H$, $k \in K$.

Ejercicio 1.16. Si $H \leqslant G$ y $K \leqslant G$, el conjunto $HgK := \{ hgk \in G : h \in H, k \in K \}$ se llama una *coclase doble* de g respecto de H y K. Si el grupo G es finito, demostrar que $|HgK| = |K|[H : gKg^{-1} \cap H] = |H|[K : g^{-1}Hg \cap K]$.

Ejercicio 1.17. Si p es primo, demostrar que el único subgrupo normal no trivial de D_p es el subgrupo de rotaciones C_p. ¿Cuáles son los subgrupos normales de D_4 y de D_6?

Ejercicio 1.18. Demostrar que el grupo D_4 tiene dos subgrupos H, K tales que $H \trianglelefteq K$ y $K \trianglelefteq D_4$, pero H no es un subgrupo normal de D_4. (Luego la relación $\trianglelefteq$ no es transitiva).

Ejercicio 1.19. El **grupo afín** de la recta $\mathbb{R}$ es el juego de matrices

$$\mathrm{Af}(1, \mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R},\ a \neq 0 \right\}$$

cuyo producto está dado por la multiplicación de matrices. Demostrar que este es un subgrupo de $\mathrm{GL}(2, \mathbb{R})$. Sea

$$N := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\};$$

comprobar que N es un subgrupo normal de $\mathrm{Af}(1, \mathbb{R})$.

Ejercicio 1.20. Sea $D \in \mathrm{GL}(n, \mathbb{F})$ una matriz invertible *diagonal*. ¿Cómo se describe su centralizador $Z_G(D)$ en el grupo $\mathrm{GL}(n, \mathbb{F})$?

Ejercicio 1.21. El **grupo de cuaterniones** es un grupo multiplicativo de ocho elementos $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ con elemento neutro 1 en donde[2]

$$(-1)^2 = 1, \quad i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.$$

(En palabras: i, j, k son tres raíces cuadradas de -1 que anticonmutan entre sí.) Aunque Q es un grupo no abeliano, cada uno de sus subgrupos es normal: demostrar esta última afirmación.

1.3 Ejercicios sobre grupos e isomorfismos

Ejercicio 1.22. Ejecutar los siguientes cálculos en el grupo de permutaciones S_9:

(a) Expresar $(123)(45)(16789)(15)$ como producto de ciclos disjuntos.

(b) Calcular gxg^{-1} si $g = (135)(12)$, $x = (1579)$.

(c) Obtener g tal que $g(12)(34)g^{-1} = (13)(56)$.

Ejercicio 1.23. Demostrar que $Z(S_4) = \{\underline{1}\}$.

Ejercicio 1.24. Si $k, m \in \mathbb{N}$ con $k, m \geqslant 2$, sea $k\mathbb{Z} := \{kn : n \in \mathbb{Z}\}$. Demostrar que el grupo $k\mathbb{Z}/km\mathbb{Z}$ es isomorfo al grupo aditivo $\mathbb{Z}_m$.

Ejercicio 1.25. Si H es un subgrupo normal de G tal que $H \simeq C_2$ y $G/H \simeq C_5$, demostrar que el grupo G es abeliano.

Ejercicio 1.26. Si G es un grupo tal que $G/Z(G)$ es cíclico, demostrar que G es abeliano.

Ejercicio 1.27. Sea G el grupo de rotaciones de $\mathbb{R}^3$ que dejan invariante al cubo de vértices $(\pm 1, \pm 1, \pm 1)$. Demostrar que $G \simeq S_4$. ⟦ Indicación: Un cubo posee cuatro pares de vértices opuestos. ⟧ Concluir que S_4 posee 9 elementos de período 2, 8 elementos de período 3, 6 elementos de período 4 y el elemento neutro, repartidos en cinco clases conjugadas.

Ejercicio 1.28. (a) Demostrar que la aplicación $g \mapsto g^{-1}$ es un automorfismo de un grupo G si y sólo si G es abeliano.

(b) Mostrar que $g \mapsto g^m$ es un endomorfismo[3] de un grupo abeliano, para todo $m \in \mathbb{Z}$.

[2] Con esta notación, se puede asumir que $(-a)(-b) = ab$ y que $(-a)b = a(-b) = -ab$.

[3] Un **endomorfismo** de un grupo G es un homomorfismo $\varphi : G \to G$, no necesariamente inyectivo ni sobreyectivo.

(c) Sea G un grupo abeliano finito; sea m un entero tal que $m \perp |G|$ (enteros relativamente primos). Demostrar que cada $g \in G$ es de la forma $g = h^m$ para algún $h \in G$. ⟦ Indicación: Comprobar que $h \mapsto h^m$ es un automorfismo de G cuando $m \perp |G|$. ⟧

Ejercicio 1.29. Identificar el grupo $\mathrm{Aut}(D_4)$. (En otras palabras: encontrar un grupo "conocido" G tal que $\mathrm{Aut}(D_4) \simeq G$ y exhibir el isomorfismo.)

Ejercicio 1.30. Si $H \leqslant G$ y si A es un subgrupo de $\mathrm{Aut}(G)$ tal que $\alpha(H) \subseteq H$ para todo $\alpha \in A$, demostrar que $\alpha(Z_G(H)) \subseteq Z_G(H)$ y también $\alpha(N_G(H)) \subseteq N_G(H)$, para todo $\alpha \in A$.

Ejercicio 1.31. Sea G un grupo finito; para $\alpha \in \mathrm{Aut}(G)$, sea $I_\alpha := \{\, g \in G : \alpha(g) = g^{-1} \,\}$.

(a) Si $|I_\alpha| > \frac{3}{4}|G|$, demostrar que $I_\alpha = G$ y que G es abeliano.

(b) Dar un ejemplo de un grupo G y un $\alpha \in \mathrm{Aut}(G)$ tales que $|I_\alpha| = \frac{3}{4}|G|$.

(c) Si $|I_\alpha| = \frac{3}{4}|G|$, demostrar que G posee un subgrupo abeliano de índice 2.

Ejercicio 1.32. Sea $\mathbb{Z}^2 := \mathbb{Z} \times \mathbb{Z}$ (producto cartesiano) el grupo aditivo con la suma usual. Denótese por $\mathrm{SL}(2,\mathbb{Z})$ el grupo de matrices invertibles 2×2 con entradas en $\mathbb{Z}$ y determinante 1. Su centro es el subgrupo $\{1_2, -1_2\} \simeq C_2$; sea $\mathrm{PSL}(2,\mathbb{Z}) := \mathrm{SL}(2,\mathbb{Z})/C_2$ el cociente de $\mathrm{SL}(2,\mathbb{Z})$ por su centro. Demostrar que $\mathrm{Aut}(\mathbb{Z}^2) \simeq \mathrm{PSL}(2,\mathbb{Z})$.

Ejercicio 1.33. Un **subgrupo característico** del grupo G es un subgrupo $H \leqslant G$ tal que $\alpha(H) \subseteq H$ para todo $\alpha \in \mathrm{Aut}(G)$. Sean H y K dos subgrupos de G tales que $H \leqslant K \leqslant G$.

(a) Demostrar que cada subgrupo característico es un subgrupo normal de G.

(b) Demostrar que el centro $Z(G)$ es un subgrupo característico de G.

(c) Si H es un subgrupo característico de K y K es un subgrupo característico de G, mostrar H es un subgrupo característico de G.

(d) Si H es un subgrupo característico de K y si $K \trianglelefteq G$, mostrar que $H \trianglelefteq G$.

Ejercicio 1.34. El **conmutador** de $g, h \in G$ es un elemento $\underline{ghg^{-1}h^{-1}} \in G$. Sea G' el subgrupo de G generado por todos los conmutadores de elementos de G. (Obsérvese que $G' = \{1\}$ si y sólo si G es abeliano.)

(a) Demostrar que G' es un subgrupo normal (de hecho, característico) de G; y que G/G' es abeliano.

(b) Si $H \leqslant G$ es un subgrupo tal que $G' \subseteq H$, demostrar que $H \trianglelefteq G$.

Ejercicio 1.35. Sea $\mathbb{A}$ el grupo $\{(k,l,m) : k,l,m \in \mathbb{Z}\}$ con producto definido por

$$(k_1,l_1,m_1)(k_2,l_2,m_2) := (k_1+k_2, l_1+l_2, m_1+m_2+k_1l_2).$$

Verificar que $\mathbb{A}$ es un grupo no abeliano con elemento neutro $(0,0,0)$. Mostrar que su centro es $Z(\mathbb{A}) = \{(0,0,m) : m \in \mathbb{Z}\}$ y que $\mathbb{A}/Z(\mathbb{A}) \simeq \mathbb{Z}^2$.

Demostrar también que $\mathbb{A}' = Z(\mathbb{A})$.

1.4 Ejercicios sobre acciones de grupos

Ejercicio 1.36. Si un grupo G actúa sobre un conjunto X y si $g \cdot x = y$ en X, comprobar que los grupos de isotropía de estos puntos son conjugados, al mostrar que $G_y = gG_xg^{-1}$.

Ejercicio 1.37. Denótese por $\mathbb{Z}[x_1,x_2,\ldots,x_n]$ la totalidad[4] de polinomios en n variables con coeficientes enteros. Si $p = p(x_1,x_2,\ldots,x_n)$ es un polinomio y $\sigma \in S_n$ es una permutación, defínase otro polinomio $\sigma \cdot p$ por

$$(\sigma \cdot p)(x_1,x_2,\ldots,x_n) := p(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(n)}).$$

Comprobar que $p \mapsto \sigma \cdot p$ es una acción del grupo S_n sobre $\mathbb{Z}[x_1,x_2,\ldots,x_n]$. Considérese el **determinante de Vandermonde**,

$$v(x_1,x_2,\ldots,x_n) := \begin{vmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i).$$

Mostrar que $\tau \cdot v = -v$ si τ es una transposición. Concluir que $\underline{\pi \cdot v = (-1)^\pi v}$ en general: el polinomio v es *totalmente antisimétrico* en sus n variables.

Ejercicio 1.38. Cada permutación $\sigma \in S_n$ es un producto de ciclos disjuntos:

$$\sigma = (i_1 i_2 \ldots i_r)(j_1 j_2 \ldots i_s)\cdots(l_1 l_2 \ldots l_u),$$

El grupo S_n actúa, por su mera definición, sobre el conjunto $X = \{1,2,\ldots,n\}$. Considérese la acción sobre X (por restricción) del subgrupo cíclico $G = \langle\sigma\rangle$. ¿Cuáles son las órbitas $G \cdot x$ en este caso? Cuáles son los subgrupos de isotropía G_x, para $x \in \{1,2,\ldots,n\}$?

[4]Por ahora, es suficiente considerar el *conjunto* de todos estos polinomios. Más adelante, se verá que este es un *anillo conmutativo*.

Ejercicio 1.39. El grupo S_4 actúa por rotaciones sobre el cubo con vértices $(\pm 1, \pm 1, \pm 1)$ —véase el Ejercicio 1.27. Determinar los subgrupos de isotropía de:

(a) un vértice, p. ej. $(1,1,1)$;

(b) un centro de faceta, p. ej. $(1,0,0)$;

(c) un punto medio de arista, p. ej. $(1,1,0)$.

Ejercicio 1.40. Si $X \in M_n(\mathbb{C})$ es una matriz compleja y si $t \in \mathbb{R}$, se define la *matriz exponencial* $\underline{\exp tX} \in \mathrm{GL}(n,\mathbb{C})$ por la serie de potencias convergente:

$$\exp tX := \sum_{k=0}^{\infty} \frac{t^k}{k!} X^k.$$

Está claro que $(\exp sX)(\exp tX) = \exp((s+t)X)$ y que $(\exp tX)^{-1} = \exp(-tX)$, así que $\{\exp tX : t \in \mathbb{R}\}$ es un **subgrupo uniparamétrico** de $\mathrm{GL}(n,\mathbb{C})$ y $t \mapsto \exp(tX)$ es un homomorfismo de $\mathbb{R}$ en $\mathrm{GL}(n,\mathbb{C})$.⟦ Si $X \in M_n(\mathbb{R})$ es una matriz real, entonces $\exp tX \in \mathrm{GL}(n,\mathbb{R})$ para todo $t \in \mathbb{R}$. ⟧

(a) Si $X, Y \in M_n(\mathbb{C})$ son *dos matrices que conmutan*, es decir, $XY = YX$, demostrar que $\exp(X+Y) = (\exp X)(\exp Y)$.

(b) Concluir que $g(\exp tX)g^{-1} = \exp(tgXg^{-1})$ para todo $t \in \mathbb{R}$.⟦ Indicación: calcular la derivada de ambos lados en $t = 0$. ⟧

(c) Comprobar que $\Phi(g,X) := gXg^{-1}$ es una *acción a izqauierda* de $\mathrm{GL}(n,\mathbb{C})$ sobre $M_n(\mathbb{C})$. Esta es la **acción adjunta** del grupo $\mathrm{GL}(n,\mathbb{C})$.

(d) Si $t \in \mathbb{R}$, calcular $\exp tX_j$ para las siguientes matrices:[5]

$$X_1 = \frac{i}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad X_2 = \frac{1}{2}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad X_3 = \frac{i}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

y verificar que $\exp tX_j \in \mathrm{SU}(2)$ en cada caso, para $t \in \mathbb{R}$.

[5] La acción adjunta de un subgrupo $H \leqslant \mathrm{GL}(n,\mathbb{C})$ involucra el subespacio de matrices X tales que $\exp tX \in H$ para todo t. En el caso $H = \mathrm{SU}(2)$, estas son las matrices antihermíticas sin traza: $X^* = -X$, $\mathrm{tr}\, X = 0$, el cual forma un subespacio real 3-dimensional de $M_2(\mathbb{C})$.

1.5 Ejercicios sobre la estructura de grupos finitos

Ejercicio 1.41. Demostrar que el grupo A_4 (permutaciones pares de 4 objetos) tiene subgrupos de órdenes 2, 3 y 4, pero no tiene subgrupo alguno de orden 6.

Ejercicio 1.42. Encontrar un 2-subgrupo de Sylow y un 3-subgrupo de Sylow del grupo de permutaciones S_4. Comprobar que el 2-subgrupo de Sylow es isomorfo a D_4.

Ejercicio 1.43. Demostrar que un grupo de orden 455 es cíclico.

Ejercicio 1.44. Si G es un grupo con $|G| = 108$, demostrar que G posee un subgrupo normal de orden 27 o bien de orden 9.

Ejercicio 1.45. Sea p el menor número primo que divide $|G|$. Si H es un subgrupo de G tal que $[G : H] = p$, demostrar que $H \trianglelefteq G$. Concluir que un grupo de orden pq, donde p y q son primos distintos, no puede ser simple.

Ejercicio 1.46. Si G es un grupo simple de orden 168, ¿cuántos elementos de período 7 pertenecen a G?

Ejercicio 1.47. Demostrar que no hay grupos simples de ordenes 28, 56 ó 148.

Ejercicio 1.48. Si $n \in \mathbb{P}$ es impar, demostrar que todos los subgrupos de Sylow del grupo diédrico D_n son cíclicos.

Ejercicio 1.49 (Lema de Frattini)**.** Si G es un grupo finito y p es un primo que divide $|G|$, y si además $K \trianglelefteq G$ y P es un p-subgrupo de Sylow de K, demostrar que $G = K N_G(P)$. ⟦ Indicación: si $g \in G$, mostar que algún $k \in K$ tal que $gPg^{-1} = kPk^{-1}$. ⟧

Ejercicio 1.50. Comprobar que el grupo diédrico D_n es un producto semidirecto de la forma $C_n \rtimes_\alpha C_2$.

Ejercicio 1.51. Demostrar que S_4 es un producto semidirecto de V por S_3. ⟦ Indicación: usar el Ejemplo 1.59. ⟧

Ejercicio 1.52. Demostrar que el grupo afín $\mathrm{Af}(1, \mathbb{R})$ del Ejercicio 1.19 es un producto semidirecto de $\mathbb{R}$ por $\mathbb{R}^\times$.

Ejercicio 1.53. Sea $\mathrm{SO}(n)$ el grupo de matrices ortogonales $n \times n$ sobre $\mathbb{R}$ de determinante 1. El **grupo euclidiano** $\mathrm{E}(n)$ es el subgrupo de $\mathrm{SL}(n+1, \mathbb{R})$ formado por matrices de la forma $\begin{pmatrix} A & \mathbf{b} \\ 0 & 1 \end{pmatrix}$, con $A \in \mathrm{SO}(n)$, $\mathbf{b} \in \mathbb{R}^n$. Demostrar que $\mathrm{E}(n) \simeq \mathbb{R}^n \rtimes \mathrm{SO}(n)$, con respecto a la acción usual (como matrices) de $\mathrm{SO}(n)$ sobre $\mathbb{R}^n$.

1.6 Ejercicios sobre grupos resolubles y nilpotentes

Ejercicio 1.54. Demostrar que cualquier grupo *abeliano* finito es un producto directo de grupos cíclicos cuyos órdenes son potencias de primos.

Ejercicio 1.55. Si el grupo G es resoluble y si $\varphi: G \to K$ es un homomorfismo sobreyectivo, demostrar que K también es resoluble.

Ejercicio 1.56. Si $N \trianglelefteq G$ y si N y G/N son grupos resolubles, demostrar que G también es resoluble.

Ejercicio 1.57. Defínase una sucesión de subgrupos $\Gamma_j(G) \leqslant G$, para $j \in \mathbb{N}$, como sigue. Sea $\Gamma_0(G) := G$. Por inducción, sea $\Gamma_{j+1}(G)$ el subgrupo generado por los conmutadores $ghg^{-1}h^{-1}$ con $g \in G$, $h \in \Gamma_j(G)$; fíjese que $\Gamma_1(G) = G'$.

Dícese que un grupo finito G es **nilpotente** si $\Gamma_m(G) = \mathbf{1}$ para algún $m \in \mathbb{N}$. Demostrar que $\Gamma_{j+1}(G) \trianglelefteq \Gamma_j(G)$ para cada j y que $\Gamma_j(G)/\Gamma_{j-1}(G) \leqslant Z(G/\Gamma_{j-1}(G))$. Concluir que cada grupo nilpotente es resoluble.

Ejercicio 1.58. Demostrar que el grupo S_3 es resoluble pero no es nilpotente.

Ejercicio 1.59. Demostrar que cada p-grupo finito es nilpotente. ⟦ Indicación: usar la Proposición 1.79 y una inducción sobre $|G|$. ⟧

Ejercicio 1.60. Sea $G = \mathrm{UT}(n,p) \equiv \mathrm{UT}(n,\mathbb{F}_p)$ el grupo de *matrices unitriangulares* $n \times n$ con entradas en $\mathbb{F}_p$ (véase el Ejemplo 1.88). Verificar que $\Gamma_1(G)$ y $\Gamma_2(G)$ constan de matrices con ceros en uno o dos subdiagonales superiores, respectivamente. Demostrar además que este grupo $\mathrm{UT}(n,p)$ es nilpotente.

Ejercicio 1.61. Sea $G = \mathrm{T}(n,p) \equiv \mathrm{T}(n,\mathbb{F}_p)$ el grupo de *matrices triangulares* invertibles $n \times n$ con entradas en $\mathbb{F}_p$. Comprobar que el $G' = \mathrm{UT}(n,p)$ y concluir que $\mathrm{T}(n,p)$ es un grupo resoluble.

1.7 Ejercicios sobre grupos finitos

Ejercicio 1.62. Determinar todos los grupos no isomorfos de orden 21.

Ejercicio 1.63. Sea $T = C_3 \rtimes_\alpha C_4$ el producto semidirecto de los dos grupos cíclicos $C_3 = \{1, s, s^2\}$ y $C_4 = \{1, t, t^2, t^3\}$ determinado por $\alpha: C_4 \to \mathrm{Aut}(C_3)$ donde $\alpha_t(s) = s^2$. Demostrar que

$$T \simeq \langle a, b : a^6 = 1,\ b^2 = a^3,\ bab^{-1} = a^{-1} \rangle.$$

⟦ Indicación: léase el último renglón de la demostración del Teorema 1.115. ⟧

Ejercicio 1.64. Sea G un grupo finito generado por dos elementos distintos a, b, ambos de período 2. Comprobar que $G \simeq D_n$ para algún $n \geqslant 2$.

Ejercicio 1.65. Demostrar que $\mathrm{Aut}(C_8) \simeq V$.

Ejercicio 1.66. Con la notación $\zeta = e^{\pi i/4} = (1+i)\sqrt{2}/2$, sea G el grupo finito generado por las dos matrices

$$A = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

(a) Demostrar que G es un grupo no abeliano de orden 16.

(b) Dar una presentación de G por generadores y relaciones, $G \simeq \langle a, b : \cdots \rangle$.

(c) Determinar si $G \simeq C_4 \rtimes_\alpha C_4$ o no, para algún homomorfismo $\alpha\colon C_4 \to \mathrm{Aut}(C_4)$.

2.1 Ejercicios sobre categorías y funtores

Ejercicio 2.1. (a) Comprobar en detalle que la abelianización de grupos $\mathscr{A}G := G/G'$ define un funtor $\mathscr{A}$ entre las categorías Gr y Ab.

(b) La abelianización también puede considerarse como un funtor $\mathscr{A}\colon \mathsf{Gr} \to \mathsf{Gr}$ (en vez de $\mathscr{A}\colon \mathsf{Gr} \to \mathsf{Ab}$). Para cada grupo G, sea $\eta_G\colon G \to G/G'$ la aplicación cociente. Mostrar que la familia $\{\, \eta_G : G \text{ en } \mathrm{Ob}(\mathsf{Gr}) \,\}$ define una transformación natural entre las funtores 1_{Gr} y $\mathscr{A}$.

Ejercicio 2.2. Hay una categoría $\mathsf{SEC\text{-}Gr}$ cuyos objetos son sucesiones exactas cortas de grupos. ¿Cuál sería la definición correcta de morfismos en esta categoría para que dos extensiones de un grupo H por un grupo K sean equivalentes si y sólo si las sucesiones exactos cortas correspondientes son isomorfas?

3.1 Ejercicios básicos sobre anillos

Ejercicio 3.1. Si $(1-ab)$ es una unidad de un anillo no conmutativo R, demostrar que $(1-ba)$ es también una unidad.

Ejercicio 3.2. Sea R un *anillo sin identidad*. Un elemento $a \in R$ es **cuasiregular** a la izquierda [respectivamente, a la derecha] si existe $b \in R$ tal que $a + b - ba = 0$ [resp., $a + b - ab = 0$]. Demostrar que esto ocurre si y sólo si el elemento $(1, -a) \in R^+$ posee un inverso a la izquierda [resp., a la derecha] en el anillo $R^+ = \mathbb{Z} \times R$.

Ejercicio 3.3. Un elemento z de un anillo R se llama **nilpotente** si $z^n = 0$ para algún $n \in \mathbb{P}$. Si z es nilpotente, demostrar que el elemento $(1-z)$ es una unidad en R y encontrar una fórmula que expresa su inverso.

Ejercicio 3.4. Un anillo R se llama **booleano** si $a^2 = a$ para todo $a \in R$. Demostrar que un anillo booleano es conmutativo.

Ejercicio 3.5. Un elemento e de un anillo R se llama **idempotente** si $\underline{e^2 = e}$.

(a) Demostrar que los únicos idempotentes de un *anillo entero* son los elementos 0 y 1.

(b) ¿Cuáles son los idempotentes en el anillo $M_2(\mathbb{C})$? ⟦ Indicación: como primer paso, identificar los idempotentes que son matrices triangulares. ⟧

Ejercicio 3.6. Demostrar que el "teorema binomial rústico" $(a \pm b)^p = a^p \pm b^p$ es válido en el cuerpo finito $\mathbb{F}_p$.

Ejercicio 3.7. Sea R un anillo conmutativo. Si $M_n(R)$ es el anillo de matrices $n \times n$ con entradas en R, determinar el *centro* $Z(M_n(R)) := \{A \in M_n(R) : AB = BA \text{ para todo } B \in R\}$. ⟦ Indicación: sea E_{ij} la matriz cuya entrada (i,j) es 1 y cuyas demás entradas son 0. Examinar la ecuación $AE_{ij} = E_{ij}A$ para una matriz A dada. ⟧

Ejercicio 3.8. Demostrar que el anillo de cuaterniones $\mathbb{H}$ es isomorfo al subanillo de $M_2(\mathbb{C})$ de matrices de la forma $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ con $\alpha, \beta \in \mathbb{C}$. ?Cuáles son las imágenes de los cuaterniones $\{i, j, k\}$ bajo este isomorfismo?

Ejercicio 3.9. Si R es un anillo conmutativo, sea N el conjunto de elementos nilpotentes de R. Demostrar que N es un ideal en R; y que no hay elementos nilpotentes no nulos en el anillo cociente R/N.

Ejercicio 3.10. Sea $C[0,1]$ el anillo de funciones continuas $f : [0,1] \to \mathbb{R}$. Demostrar que $f \in C[0,1]$ es un divisor de cero si y sólo si f se anula en algún subintervalo abierto de $[0,1]$. ¿Cuáles son las unidades de este anillo?

Ejercicio 3.11. En el anillo $C[0,1]$ del ejercicio anterior, demostrar que un ideal M es un maximal si y sólo si existe $t \in [0,1]$ tal que $M = \{f \in C[0,1] : f(t) = 0\}$.

Ejercicio 3.12. Sea R un anillo conmutativo (no necesariamente entero) y sea $S \subseteq R \setminus \{0\}$ una *parte multiplicativa*: $1 \in S$; y $s, t \in S \implies st \in S$. Defínase una relación de equivalencia en $R \times S$ por $(a,s) \sim (c,t)$ si hay $r \in S$ tal que $\underline{r(at - bs) = 0}$; denótese la clase de equivalencia de (a,s) por a/s.

Comprobar que estas clases forman un anillo (denotado por RS^{-1}) bajo las operaciones usuales de fracciones. Demostrar que $a \mapsto a/1$ es un homomorfismo de R en RS^{-1}, el cual es inyectivo si y sólo si S no contiene divisores de cero. Demostrar que $s/1$ es una unidad de RS^{-1} para cada $s \in S$.

3.2 Ejercicios sobre ideales y módulos

Ejercicio 3.13. Si I es un ideal de R, sea $M_n(I) := \{A \in M_n(R) : \text{ cada } a_{ij} \in I\}$. Demostrar que $M_n(I)$ es un ideal de $M_n(R)$ y hallar un isomorfismo $M_n(R)/M_n(I) \simeq M_n(R/I)$.

Ejercicio 3.14. Sea S un anillo que contiene elementos $\{e_{ij} : i, j = 1, 2, \ldots, n\}$ tales que[6] $e_{ij}e_{rs} = \delta_{jr}e_{is}$ y $e_{11} + e_{22} + \cdots + e_{nn} = 1$. Para cada $a \in S$, escríbase $a_{ij} := \sum_{k=1}^{n} e_{ki}ae_{jk}$. Defínase $R := \{b \in S : be_{ij} = e_{ij}b \text{ para todo } i, j\}$, un subanillo de S.

Demostrar que $a_{ij} \in R$ y que $a = \sum_{i,j=1}^{n} a_{ij}e_{ij}$. Mostrar que la ecuación $\sum_{i,j=1}^{n} c_{ij}e_{ij} = 0$, donde cada $c_{ij} \in R$, sólo posee la solución trivial: todo $c_{ij} = 0$. Concluir que existe un isomorfismo $S \simeq M_n(R)$.

Ejercicio 3.15. Sea M un R-módulo a izquierda y sea $A := \{r \in R : rx = 0 \text{ para } x \in M\}$. Comprobar que A es un ideal de R y que M es un R/A-módulo a izquierda bajo la acción $(r + A)x := rx$.

Ejercicio 3.16. Si A y B son submódulos de un R-módulo a izquierda M, demostrar que $A \cap B$ y $A + B$ son submódulos de M y que $(A + B)/B \simeq B/(A \cap B)$ en la categoría R-Mod.

Ejercicio 3.17. Dado un anillo R, sean M un R-módulo a derecha y N un R-módulo a izquierda. Si $(A, +)$ es un grupo abeliano, una aplicación $f : M \times N \to A$ es ***R*-bilineal** si

$$\begin{aligned} f(x_1 + x_2, y) &= f(x_1, y) + f(x_2, y) && \text{para todo} \quad x_1, x_2 \in M,\ y \in N, \\ f(x, y_1 + y_2) &= f(x, y_1) + f(x, y_2) && \text{para todo} \quad x \in M,\ y_1, y_2 \in N, \\ f(xa, y) &= f(x, ay) && \text{para todo} \quad x \in M,\ y \in N,\ a \in R. \end{aligned}$$

Sea $\mathbb{Z}(M \times N)$ el grupo abeliano libre generado por el producto cartesiano $M \times N$; y sea U el subgrupo generado por todos sus elementos de estos tipos:

$$(x_1 + x_2, y) - (x_1, y) - (x_2, y), \quad (x, y_1 + y_2) - (x, y_1) - (x, y_2), \quad (xa, y) - (x, ay).$$

Escribase $M \otimes_R N := \mathbb{Z}(M \times N)/U$, el grupo abeliano cociente (el **producto tensorial** sobre R de los módulos M y N). Denótese por $x \otimes y$ la coclase $(x, y) + U$; cada elemento de $M \otimes_R N$ es una suma finita $\sum_j x_j \otimes y_j$.

[6] Aquí se usa la **delta de Kronecker**: $\delta_{jr} = 1$ si $j = r$, $\delta_{jr} = 0$ si $j \neq r$.

Comprobar que la aplicación $t: M \times N \to M \otimes_R N : (x,y) \mapsto x \otimes y$ es R-bilineal. Demostrar, además, que para cualquier aplicación R-bilineal $f: M \times N \to A$, existe un único homomorfismo de grupos $\varphi: M \otimes_R N \to A$ tal que $\varphi \circ t = f$.

Ejercicio 3.18. Sea R un anillo conmutativo y sean M, N dos R-módulos. Demostrar que $\mathrm{Hom}_R(M,N)$ es un R-módulo si se define $a\psi$ por $a\psi(x) := a(\psi(x))$, para $a \in R$, $\psi \in \mathrm{Hom}_R(M,N)$.

Ejercicio 3.19. Sean R un anillo conmutativo, M un R-módulo y $\mathrm{Hom}_R(R,M)$ la colección de R-homomorfismos $\psi: R \to M$. Demostrar que $\psi \mapsto \psi(1)$ es un R-isomorfismo de $\mathrm{Hom}_R(R,M)$ sobre M.

Ejercicio 3.20 (Teorema chino del residuo)**.** Sea R un anillo conmutativo.

(a) Sean I, J dos ideales de R tales que $I + J = R$. Hallar un isomorfismo de anillos $\psi: R/(I \cap J) \xrightarrow{\simeq} R/I \oplus R/J$. Dados dos elementos $b, c \in R$, concluir que existe $a \in R$ tal que $a - b \in I$ y $a - c \in J$.

(b) Si $I_1, I_2, \ldots, I_n$ son ideales de R tales que $I_j + I_k = R$ para todo $j \neq k$, demostrar (por inducción sobre n) que

$$\frac{R}{I_1 \cap \cdots \cap I_n} \simeq \frac{R}{I_1} \oplus \cdots \oplus \frac{R}{I_n}.$$

Dados $b_1, \ldots, b_n \in R$, concluir que existe $a \in R$ tal que $a - b_j \in I_j$ para $j = 1, \ldots, n$.

(c) Sean $m_1, \ldots, m_n \in \mathbb{P}$ enteros positivos tales que $m_j \perp m_k$ para $j \neq k$. Dados un juego de enteros $r_1, \ldots, r_n \in \mathbb{Z}$, comprobar que existe $s \in \mathbb{Z}$ tal que $s \equiv r_j \bmod m_j$ para cada $j = 1, \ldots, n$.

Ejercicio 3.21. Determinar todos los grupos *abelianos* no isomorfos de orden 360.

Ejercicio 3.22. Si $m, n \in \mathbb{P}$, describir el grupo abeliano $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n)$.

3.3 Ejercicios sobre polinomios y su factorización

Ejercicio 3.23. Si $\alpha \in \mathbb{C}$, denótese por $\mathbb{Q}[\alpha]$ la imagen de $\mathbb{Q}[x]$ bajo el homomorfismo de evaluación $E: \mathbb{Q}[x] \to \mathbb{C}$ definido por $E(q) := q$ si $q \in \mathbb{Q}$ y $E(x) := \alpha$.

(a) Si $m \in \mathbb{P}$ no es un cuadrado en $\mathbb{P}$, demostrar que $\mathbb{Q}[\sqrt{m}] \simeq \mathbb{Q}[x]/(x^2 - m)$.

(b) Comprobar que $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

(c) Demostrar que los anillos $\mathbb{Q}[\sqrt{2}]$ y $\mathbb{Q}[\sqrt{3}]$ no son isomorfos.

(d) Encontrar un polinomio $p(x) \in \mathbb{Q}[x]$ tal que $p(\sqrt{2}+\sqrt{3}) = 0$. Hallar un ideal I en $\mathbb{Q}[x]$ tal que $\mathbb{Q}[x]/I \simeq \mathbb{Q}[\sqrt{2}+\sqrt{3}]$.

Ejercicio 3.24. Si $\mathbb{F}_q$ es un cuerpo finito con q elementos, sea $\mathbb{F}_q^\times =: \{a_1, a_2, \ldots, a_{q-1}\}$ la lista de sus elementos no nulos.

(a) Sea $p \in \mathbb{P}$ el menor entero positivo tal que $p \cdot 1 = 0$ en $\mathbb{F}_q$. Mostrar que p es un número primo[7] y que $q = p^r$ para algún $r \in \mathbb{P}$. ⟦ Indicación: observar que $\mathbb{F}_q$ es un espacio vectorial sobre $\mathbb{F}_p$. ⟧

(b) Comprobar que $a_1 a_2 \cdots a_{q-1} = -1$ en $\mathbb{F}_q$. ⟦ Indicación: q puede ser par o impar. ⟧

(c) Demostrar el *teorema de Wilson*: si $p \in \mathbb{P}$ es primo, entonces $(p-1)! \equiv -1 \bmod p$.

Ejercicio 3.25. Demostrar que el anillo de división $\mathbb{H}$ (los cuaterniones) contiene infinitas elementos u que cumplen la ecuación $u^2 = -1$.

Ejercicio 3.26. (a) Comprobar que el anillo $\mathbb{Z}[i]$, los enteros gaussianos, es euclidiano para la función $\delta(m+ni) := m^2+n^2$.

(b) Demostrar que $\mathbb{Z}[\sqrt{2}]$ es euclidiano para la función $\delta(m+n\sqrt{2}) := |m^2-2n^2|$.

Ejercicio 3.27. Hallar el máximo común divisor $d(x)$ de los polinomios

$$p(x) = x^4+3x^3-x^2-4x-3, \qquad q(x) = 3x^3+10x^2+2x-3.$$

En seguida, encontrar $a(x)$, $b(x)$ en $\mathbb{Q}[x]$ tales que $a(x)p(x)+b(x)q(x) = d(x)$.

Ejercicio 3.28. Se sabe que el polinomio $x^4+x^3+x^2+x+1$ es irreducible en $\mathbb{Q}[x]$, pero reducible en $\mathbb{R}[x]$. Encontrar su factorización en $\mathbb{R}[x]$.

⟦ Indicación: recordar la fórmula de de Moivre: $(\cos\theta + i\,\mathrm{sen}\,\theta)^n = \cos n\theta + i\,\mathrm{sen}\,n\theta$. ⟧

Ejercicio 3.29. Calcular, con el algoritmo euclidiano, el máximo común divisor de estos pares de polinomios en $\mathbb{Q}[x]$:

(a) $f(x) := x^3+x^2+x-3$ y $g(x) := x^4-x^3+3x^2+x-4$.
(b) $f(x) := x^2+1$ y $g(x) := x^6+x^3+x+1$.
(c) $f(x) := x^{18}-1$ y $g(x) := x^{33}-1$.

[7] Este número primo se llama la **característica** del cuerpo $\mathbb{F}_q$.

Ejercicio 3.30. Calcular el máximo común divisor de este par de polinomios en $\mathbb{F}_7[x]$:

$$f(x) := \overline{3}x^6 + x^5 + \overline{4}x^4 + \overline{4}x^3 + \overline{3}x^2 + \overline{4}x + \overline{2},$$
$$g(x) := \overline{2}x^6 + \overline{4}x^5 + \overline{3}x^4 + \overline{4}x^3 + \overline{4}x^2 + x + \overline{3}.$$

Ejercicio 3.31. Encontrar máximos comunes divisores en $\mathbb{Z}[i]$ para:

$$\text{(a)} \quad 3+4i \quad \text{y} \quad 4-3i; \qquad \text{(b)} \quad 11+7i \quad \text{y} \quad 18-i.$$

Ejercicio 3.32. (a) Demostrar la siguiente variante del algoritmo euclidiano: si R es un anillo conmutativo, si $p(x), d(x) \in R[x]$ donde $d(x) = b_0 + b_1 x + \cdots + b_m x^m$ con $b_m \neq 0$, existen $k \in \mathbb{N}$ y un único par de polinomios $q(x), r(x) \in R[x]$ tales que

$$b_m^k\, p(x) = d(x)q(x) + r(x), \quad \text{con} \quad \begin{cases} \operatorname{gr} r(x) < \operatorname{gr} d(x) \\ \text{o bien} \;\; r(x) = 0. \end{cases}$$

(b) Con este algoritmo modificado, hallar el máximo común divisor mónico de

$$f(x) := x^4 + 3x^3 - x^2 - 4x - 3, \quad \text{y} \quad g(x) := 3x^3 + 10x^2 + 2x - 3,$$

en el anillo $\mathbb{Z}[x]$.

Ejercicio 3.33. Hallar el máximo común divisor mónico $h(x)$ en el anillo $\mathbb{Z}[x]$ de los polinomios

$$f(x) := x^{12} - 1, \quad \text{y} \quad g(x) := (x^2 - x + 1)^4.$$

⟦ Indicación: Se podría usar *Mathematica*™ para los cálculos intermedios. ⟧

Ejercicio 3.34. Si $g(x) \in \mathbb{F}_p[x]$ es un polinomio irreducible de grado m, demostrar que $\mathbb{F}_p[x]/(g(x))$ es un cuerpo finito con p^m elementos.

Ejercicio 3.35. Demostrar que el polinomio $x^3 + x^2 + 1$ es irreducible en $\mathbb{F}_2[x]$ y que $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ es un cuerpo con 8 elementos.

Ejercicio 3.36. Sea $p \in \mathbb{P}$ un número entero primo.

(a) Demostrar el *teorema pequeño de Fermat*: vale $a^p \equiv a \bmod p$ para todo $a \in \mathbb{Z}$.

(b) Sea $\Psi_p \colon \mathbb{Z}[x] \to \mathbb{F}_p[x]$ el homomorfismo de reducción módulo p. Mostrar que el polinomio $x^p - x \in \mathbb{Z}[x]$ no pertenece a $\ker \Psi_p$, pero que todas las evaluaciones de $\Psi_p(x^p - x) \in \mathbb{F}_p[x]$ son nulas.

Ejercicio 3.37. Si $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ tiene una raíz racional $\alpha = r/s \in \mathbb{Q}$, donde $r, s \in \mathbb{Z}$ con $s \neq 0$ y $\mathrm{mcd}(r,s) = 1$, comprobar que $r \mid a_0$ y $s \mid a_n$.

Usar este criterio para factorizar $2x^3 - 8x^2 - 9x + 5$ en $\mathbb{Z}[x]$.

Ejercicio 3.38. El Lema de Gauss muestra que los factores de un polinomio primitivo en $\mathbb{Z}[x]$ quedan también en $\mathbb{Z}[x]$.

(a) Mostrar que las posibles factorizaciones

$$x^4 + x + 1 = (x \pm 1)(x^3 + ax^2 + bx \pm 1) = (x^2 + cx \pm 1)(x^2 + dx \pm 1)$$

no pueden realizarse con $a, b, c, d \in \mathbb{Z}$, así que $x^4 + x + 1$ es irreducible en $\mathbb{Z}[x]$.

(b) Del mismo modo, comprobar que $x^5 + 5x^2 + 4x + 7$ es irreducible en $\mathbb{Z}[x]$.

Ejercicio 3.39. Verificar que el polinomio

$$f(x) := 2x^4 + 21x^3 - 6x^2 + 9x - 3$$

es irreducible en $\mathbb{Z}[x]$, con el criterio de Eisenstein, después de aplicar un cambio de tipo $x \mapsto x + a$.

Ejercicio 3.40. Factorizar los siguientes polinomios en $\mathbb{Z}[x]$:

$$x^3 - 1, \quad x^4 - 1, \quad x^5 - 1, \quad x^6 - 1, \quad x^7 - 1, \quad x^8 - 1, \quad x^9 - 1, \quad x^{10} - 1.$$

Ejercicio 3.41. Determinar si los siguientes polinomios son irreducibles o no en los respectivos anillos de polinomios; y factorizar los que son reducibles:

(a) $x^2 + x + 1$ en $\mathbb{F}_2[x]$;

(b) $x^3 + x + 2$ en $\mathbb{F}_3[x]$;

(c) $x^2 + 1$ en $\mathbb{F}_7[x]$;

(d) $x^3 - 9$ en $\mathbb{F}_{11}[x]$;

(e) $x^3 - 9$ en $\mathbb{F}_{31}[x]$;

(f) $x^4 + 2x + 2$ en $\mathbb{Q}[x]$.

4.1 Ejercicios sobre representaciones de grupos finitos

En estos ejercicios, G denota un grupo finito y $\mathbb{F}$ un cuerpo; U, V, W son espacios vectoriales finitodimensionales sobre $\mathbb{F}$. Se escribe $\pi \sim \sigma$ cuando dos representaciones π y σ son equivalentes.

Ejercicio 4.1. Si $\pi\colon G \to \mathrm{GL}_{\mathbb{F}}(V)$ y $\sigma\colon G \to \mathrm{GL}_{\mathbb{F}}(W)$ son dos representaciones de G, sea $U := \mathrm{Hom}_{\mathbb{F}}(V,W)$ el espacio vectorial de todas las aplicaciones $\mathbb{F}$-lineales $T\colon V \to W$.

(a) Defínase $\rho(g)\,T := \sigma(g) \circ T \circ \pi(g^{-1})$ para $g \in G$ y $T \in U$. Comprobar que ρ es una representación de G sobre U.

(b) Verificar que $\mathrm{Hom}_{\mathbb{F}}(V,W) \simeq V^* \otimes_{\mathbb{F}} W$ como espacios $\mathbb{F}$-vectoriales. ⟦ Indicación: usar bases. ⟧

(c) Demostrar que hay una equivalencia de representaciones, $\rho \sim \pi^* \otimes \sigma$.

Ejercicio 4.2. Si π y σ son dos representaciones de G sobre V y W, respectivamente, comprobar que $\pi \otimes \sigma \sim \sigma \otimes \pi$.

Ejercicio 4.3. Si $\eta\colon G \to K$ es un homomorfismo sobreyectivo de grupos, y si σ es una representación irreducible de K, comprobar que $\pi := \sigma \circ \eta$ es una representación irreducible de G.

Ejercicio 4.4. Si $\pi\colon G \to \mathbb{C}^\times$ es una representación compleja unidimensional de un grupo finito G, demostrar que $\pi(g) \in \mathrm{U}(1)$ para todo $g \in G$.

Ejercicio 4.5. Un **elemento de clase** en el álgebra de grupo $\mathbb{F}[G]$ es una suma $c := g_1 + g_2 + \cdots + g_m$ de todos los elementos en una clase conjugada $\{g_1, g_2, \ldots, g_m\}$ de G. Demostrar que $ah = ha$ en $\mathbb{F}[G]$ para todo $h \in G$ si y sólo si a es una combinación $\mathbb{F}$-lineal de elementos de clase. Concluir que los elementos de clase forman una base vectorial para el *centro* $Z(\mathbb{F}[G])$ del álgebra de grupo.

Ejercicio 4.6. Mostrar que existe una representación $\pi\colon S_3 \to \mathrm{GL}(2,\mathbb{R}) = \mathrm{GL}_{\mathbb{R}}(\mathbb{R}^2)$ dado por

$$(12) \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad (123) \mapsto \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}.$$

⟦ Indicación: como $S_3 \simeq \langle a, b : a^3 = b^2 = 1,\ ba = a^2 b\rangle$, solo es necesario comprobar que $\pi(a)$ y $\pi(b)$ cumplen las mismas relaciones que a y b. ⟧

Comprobar que esta representación es equivalente a la representación irreducible π_2 de S_3 sobre el plano $x + y + z = 0$ en $\mathbb{R}^3$.

Ejercicio 4.7. Si $\mathbb{K}$ es un cuerpo que incluye el cuerpo $\mathbb{F}$ como subanillo, y si V es un espacio vectorial sobre $\mathbb{F}$, se define $V_{\mathbb{K}} := \mathbb{K} \otimes_{\mathbb{F}} V$ (el lado derecho es un producto tensorial de dos espacios $\mathbb{F}$-vectoriales). Este $V_{\mathbb{K}}$ es un espacio vectorial sobre $\mathbb{K}$; al identificar $x \in V$ con $1 \otimes x \in V_{\mathbb{K}}$, se puede considerar[8] que $V \subset V_{\mathbb{K}}$ de tal manera que $V_{\mathbb{K}} = \mathbb{K}\, V$. Una base de V sobre $\mathbb{F}$ es también una base de $V_{\mathbb{K}}$ sobre $\mathbb{K}$; y por lo tanto cada $T : V \to V$ que es $\mathbb{F}$-lineal se identifica con una aplicación $\mathbb{K}$-lineal con las mismas valores sobre una base (denotado también por T), de modo que $\mathrm{End}_{\mathbb{K}}(V_{\mathbb{K}}) = \mathbb{K}\ \mathrm{End}_{\mathbb{F}}(V)$ como anillos.

(a) Si $\pi : G \to \mathrm{GL}_{\mathbb{F}}(V)$ es una representación de G sobre V, entonces $g \mapsto \pi(g)$ define una *representación ampliada* $\pi_{\mathbb{K}} : G \to \mathrm{GL}_{\mathbb{K}}(V_{\mathbb{K}})$.[9] Si $U \leqslant V$ es un subespacio invariante bajo $\pi(G)$, comprobar que $U_{\mathbb{K}}$ es un subespacio invariante de $V_{\mathbb{K}}$ bajo $\pi_{\mathbb{K}}(G)$. Concluir que si $\pi_{\mathbb{K}}$ es irreducible, entonces π es también irreducible.

(b) Con $\mathbb{F} = \mathbb{R}$ y $\mathbb{K} = \mathbb{C}$, dar un ejemplo de una representación real irreducible de C_4, de grado 2, cuya ampliación a una representación compleja es reducible.

Ejercicio 4.8. Si $C_n = \{1, g, g^2, \ldots, g^{n-1}\}$ es el grupo cíclico de n elementos, considérese las dos representaciones complejas λ y ρ de C_n sobre $\mathbb{C}^n$ determinadas por

$$\lambda(g) := E_{21} + E_{32} + \ldots + E_{n,n-1} + E_{1n} \in M_n(\mathbb{C}),$$
$$\rho(g) := \mathrm{diag}[1, e^{2\pi i/n}, e^{4\pi i/n}, \ldots, e^{2(n-1)\pi i/n}].$$

Por ejemplo, si $n = 4$,

$$\lambda(g) := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \rho(g) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}.$$

Estas representaciones son equivalentes.[10] Encontrar una matriz invertible $P \in \mathrm{GL}_n(\mathbb{C})$ tal que $P\,\lambda(g^k)\,P^{-1} = \rho(g^k)$ para $k = 0, 1, \ldots, n-1$.

Ejercicio 4.9. Si G es un grupo finito *abeliano*, los caracteres $\chi : G \to \mathbb{C}^\times$ de las representaciones complejas irreducibles de G forman un grupo abeliano $G^\vee$, bajo multiplicación ordinaria de funciones. Comprobar que, en efecto, el producto de dos caracteres

[8] Los elementos de $\mathbb{K}V$ son sumas finitas $\sum_i \alpha_i x_i$ donde $\alpha_i \in \mathbb{K}$ y $x_i \in V$. Sin perder generalidad, se puede asumir que los α_i pertenecen a una base fija de $\mathbb{K}$ como espacio vectorial sobre $\mathbb{F}$.

[9] Así, por ejemplo, cualquier representación real de G puede ampliarse en una representación compleja, usando las mismas matrices $\pi(g)$.

[10] La equivalencia $\lambda \sim \rho$ exhibe la descomposición de la representación regular de C_n en una suma directa de representaciones unitarias irreducibles.

y el recíproco de un carácter quedan en $G^\vee$. Si $G = C_n$, demostrar que el grupo $C_n^\vee$ es también cíclico de orden n. Concluir que $G^\vee \simeq G$ para todo grupo finito abeliano.

Ejercicio 4.10. Una *acción* de un grupo finito G sobre un conjunto finito X define una representación de G sobre el espacio $\mathbb{F}$-vectorial $\mathbb{F}[X]$ cuya base es X.

(a) Si χ es el carácter de esta representación, comprobar que $\chi(g)$ es el número de puntos fijos del elemento $g \in G$.

(b) Si χ_1 es el carácter de la representación trivial de G, demostrar que $\langle \chi_1 \mid \chi \rangle$ es el número de órbitas de la acción de G sobre X.

Ejercicio 4.11. Demostrar que g y g^{-1} son conjugados en G si y sólo si $\chi_j(g) \in \mathbb{R}$ para todo carácter χ_j de una representación unitaria irreducible de G.

Ejercicio 4.12. Hallar la tabla de caracteres para el grupo abeliano $V \simeq C_2 \times C_2$.

Ejercicio 4.13. Si Q es el grupo de cuaterniones, hallar todas las clases conjugadas de Q y verificar que $Q/Z(Q) \simeq V$. Demostrar que Q tiene la misma tabla de caracteres que el grupo diedral D_4. (Por lo tanto, los caracteres no determinan el grupo hasta isomorfismo, en general.) Hallar la representación unitaria irreducible de grado 2 del grupo Q, en términos de las **matrices de Pauli**:

$$\sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_2 := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ejercicio 4.14. Defínase una representación de grado 4 del grupo D_4 por

$$\pi(\rho_{\pi/2}) := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \pi(\mu_0) := \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Encontrar las matrices $\pi(g)$ para los demás elementos $g \in D_4$ y calcular el carácter χ_π de esta representación. Comprobar que π no es irreducible y hallar la descomposición de π como suma directa de representaciones irreducibles. ⟦ Indicación: Para el último paso, no es necesario transformar los $\pi(g)$ en sumas directas de matrices en bloques. ⟧

Ejercicio 4.15. Hallar la tabla de caracteres de S_4, mediante los pasos que siguen:

(a) Enumerar las clases conjugadas de S_4, a partir del Ejemplo 1.31. Concluir que S_4 posee cinco representaciones unitarias irreducibles inequivalentes.

(b) Verificar que $S_4 \simeq V \rtimes_\alpha S_3$, un producto semidirecto. ⟦ Indicación: Sea S_3 el subgrupo que deja fijo el 4 en $\{1,2,3,4\}$. ⟧ Deducir que hay un epimorfismo $\eta : S_4 \to S_3$ y con el Ejercicio 4.3 concluir que la tabla de S_3 aparece como un bloque 3×3 dentro de la table de S_4.

(c) Identificar las dos representaciones de S_4 de grado 1 y usar la ortogonalidad de filas para rellenar las primeras tres filas de la tabla de S_4.

(d) Verificar que las dos representaciones tienen grado 3. Concluir que $\pi_5 \sim \pi_2 \otimes \pi_4$, donde π_2 es la representación no trivial de grado 1.

(e) Usar la ortogonalidad de filas para rellenar las últimas dos filas de la tabla de S_4.

Ejercicio 4.16. Considérese las siguientes dos representaciones reales irreducibles de S_4 sobre $\mathbb{R}^3$ (sus ampliaciones complejas son unitarias sobre $\mathbb{C}^3$):

(a) S_4 actúa *por rotaciones* del cubo con vértices $(\pm 1, \pm 1, \pm 1)$.

(b) S_4 actúa *por rotaciones y reflexiones* del tetraedro regular con vértices $(1,-1,-1)$, $(-1,1,-1)$, $(-1,-1,1)$ y $(1,1,1)$; el subgrupo A_4 actúa por rotaciones solamente. Por ejemplo, la reflexión $x \leftrightarrow y$ en el plano vertical $x = y$ transpone los primeros dos vértices.

Demostrar que estas dos representaciones son inequivalentes. ⟦ Indicación: Basta calcular $\chi(g)$ para una transposición $g \in S_4$ en los dos casos. ⟧

Ejercicio 4.17. Sea $D_n \simeq \langle a, b : a^n = b^2 = 1,\ ba = a^{-1}b \rangle$ el grupo diedral de orden $2n$.

(a) Si $n = 2m+1$ es impar, mostrar que D_n posee $m+2$ clases conjugadas (dar un elemento de cada clase). Verificar que D_n tiene dos representaciones unitarias irreducibles de grado 1 y m representaciones unitarias irreducibles de grado 2. Encontrar estas representaciones de grado 2, donde el subgrupo C_n esté representada por matrices diagonales de determinante 1.

(b) Si $n = 2m$ es impar, mostrar que D_n posee $m+3$ clases conjugadas (dar un elemento de cada clase). Verificar que D_n tiene cuatro representaciones unitarias irreducibles de grado 1 y $(m-1)$ representaciones unitarias irreducibles de grado 2. Encontrar estas representaciones de grado 2, como en el caso anterior.

Ejercicio 4.18. Si π y σ son representaciones irreducibles de G, su producto tensorial $\pi\otimes\sigma$ generalmente es reducible. Si π_3 es la representación unitaria irreducible de grado 2 de S_3, demostrar que $\pi_3 \otimes \pi_3 \sim \pi_1 \oplus \pi_2 \oplus \pi_3$. ⟦ Indicación: examinar sus caracteres. ⟧

4.2 Ejercicios sobre representaciones inducidas

En estos ejercicios, G denota un grupo finito y $H \leqslant G$ un subgrupo de índice $[G{:}H] = m$; $\pi\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ y $\sigma\colon H \to \mathrm{GL}_{\mathbb{C}}(W)$ son representaciones unitarias de G y H, respectivamente, de grado finito. Se denota por π_H la representación de H obtenida de π por restricción a H; y por σ^G la representación de G obtenida de σ por inducción.

Ejercicio 4.19. Si $\dim_{\mathbb{C}} W = n$, sea $b(h) \in M_n(\mathbb{C})$ la matriz de $\sigma(h)$, para cada $h \in H$, con respecto a una determinada base de W. Escríbase $G/H = \{g_1H, g_2H, \ldots, g_mH\}$ con $g_1 = 1$. Defínase $\tilde{b}(k) \in M_n(\mathbb{C})$, para todo $k \in G$, por

$$\tilde{b}(k) := \begin{cases} b(h) & \text{si } k = h \in H, \\ 0 & \text{si } k \notin H. \end{cases}$$

Sea $a(k) \in M_{mn}(\mathbb{C})$ la *matriz de bloques* $n \times n$, cuyo bloque (i,j) es $\tilde{b}(g_i^{-1}kg_j)$. Demostrar que $k \mapsto a(k) : G \to \mathrm{GL}(mn, \mathbb{C})$ es un homomorfismo de grupos; y que la representación de G sobre $\mathbb{C}^{mn}$ así obtenida es equivalente a la representación inducida σ^G.

Usar esta descripción matricial de σ^G para verificar la fórmula de Frobenius para el carácter de una representación inducida.

Ejercicio 4.20. El grupo G actúa por permutaciones $g \cdot g_iH := gg_iH$ sobre el conjunto G/H, definiendo así un homomorfismo $\pi\colon G \to \mathrm{Perm}(m) \leqslant \mathrm{GL}(m, \mathbb{C})$ que es efectivamente una representación de G sobre $\mathbb{C}^m$. Si σ_1 es la representación trivial de H, comprobar que $\sigma_1^G \sim \pi$.

Ejercicio 4.21. Esta es la **construcción de Mackey**[11] de la representación inducida σ^G a partir de una representación dada $\sigma\colon H \to \mathrm{GL}_{\mathbb{C}}(W)$ de un subgrupo $H \leqslant G$. Defínase el espacio $\mathbb{C}$-vectorial $\mathscr{V}$ de funciones con valores vectoriales $\xi\colon G \to W$ tales que

$$\xi(hk) = \sigma(h)\,\xi(k) \quad \text{para todo} \quad h \in H,\ k \in G.$$

Defínase una representación ρ de G sobre $\mathscr{V}$ por

$$\rho(g) : \xi \mapsto \rho(g)\xi, \quad \text{donde} \quad \rho(g)\xi : k \mapsto \xi(kg) \quad \text{para} \quad g, k \in G.$$

Si $y \in W$, sea $\xi_y \in \mathscr{V}$ la función dada por $\xi_y(h) := \sigma(h)y$ si $h \in H$, $\xi_y(k) := 0$ si $k \notin H$. La aplicación $\mathbb{C}$-lineal $W \to \mathscr{V} : y \mapsto \xi_y$ es inyectiva. Demostrar que $\sigma^G \sim \rho$.

[11] Esta versión de σ^G funciona se adapta directamente a grupos infinitos y grupos de Lie. Véase, por ejemplo, el libro: George Mackey, *Unitary Group Representations in Physics, Probability, and Number Theory*, Benjamin-Cummings, Reading, MA, 1978.

Ejercicio 4.22. Si G posee una subgrupo *abeliano* de índice m y si π es una representación unitaria *irreducible* de G, demostrar que el grado de π no puede ser mayor que m.

⟦ Indicación: usar la fórmula de reciprocidad de Frobenius. ⟧

Ejercicio 4.23. Demostrar que todas las representaciones irreducibles del grupo D_7 tienen grado 1 o 2. Calcular los caracteres de las representaciones de grado 2 inducidas por representaciones del subgrupo C_7 y determinar así la tabla de caracteres de D_7. ⟦ Indicación: usar el ejercicio anterior. Si $\zeta = e^{2\pi i/7}$, notar que $1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6 = 0$. ⟧

Ejercicio 4.24. En el caso $G = S_4$ y $H = S_3$, se sabe que las tres representaciones inducidas σ_1^G, σ_2^G, σ_3^G tienen grados 4, 4 y 8 respectivamente y por tanto no son irreducibles de S_4. En términos de las representaciones unitarias irreducibles π_j de S_4 ya identificadas en el Ejercicio 4.15, usar la reciprocidad de Frobenius para comprobar estas equivalencias:

$$\sigma_1^G \sim \pi_1 \oplus \pi_5, \qquad \sigma_2^G \sim \pi_2 \oplus \pi_4, \qquad \sigma_3^G \sim \pi_3 \oplus \pi_4 \oplus \pi_5.$$

Ejercicio 4.25. Demostrar que la representación π del grupo A_5 sobre $\mathbb{C}^5$ por permutaciones pares de las coordenadas (x, y, z, u, v) es reducible: $\pi \sim \pi_1 \oplus \pi_4$, donde π_1 es la subrepresentación trivial sobre la recta diagonal $x = y = z = u = v$ y π_4 es la subrepresentación sobre el hiperplano $x+y+z+u+v = 0$. Demostrar que π_4 es una representación *irreducible* de A_4, de grado 4. ⟦ Indicación: calcular $\langle \chi_4 \mid \chi_4 \rangle$. ⟧

Ejercicio 4.26. Demostrar que los 5-ciclos (12345) y (13524) = $(12345)^2$ no son conjugados en el grupo A_5. Concluir que A_5 tiene cinco clases conjugadas y por ende cinco representaciones unitarias irreducibles inequivalentes. ¿Cuáles son los sus grados? ⟦ Indicación: usar el ejercicio anterior. ⟧

Ejercicio 4.27. En el caso $G = A_5$ y $H = A_4$, usar la tabla de caracteres de A_4, la fórmula de caracteres de Frobenius y la relación $\langle \chi_\pi \mid \chi_\pi \rangle = 1$ para caracteres irreducibles para determinar la descomposición de las representaciones inducidas σ_1^G, σ_2^G, σ_3^G y σ_4^G en términos de las representaciones unitarias irreducibles π_j de A_5.

Indíce General