ÁLGEBRA BÁSICA

Texto-Guía
Convocatoria IDU-99
Universidad de Murcia

Ángel del Río Mateos
Juan Jacobo Simón Pinero
Alberto del Valle Robles

Septiembre de 2001

A Ignacia, Ángel, Presentación, Rafael, Diotila, Julia, Maruchi y Álvaro

Contenidos

Introducción

Presentación

Este texto-guía corresponde con el curso de Álgebra Básica, una asignatura obligatoria dentro del plan de estudios vigente de la Licenciatura en Matemáticas en la Facultad de Matemáticas de la Universidad de Murcia. Se trata de una asignatura anual de primer curso con una carga docente de 12 créditos, 7'5 teóricos y 4'5 prácticos.

En este contexto, el Álgebra Básica tiene una característica que la hace muy particular. Con toda seguridad se trata de la asignatura del primer curso de la Licenciatura de Matemáticas que contiene conceptos más novedosos para los alumnos. Lo normal es que el estudiante de este curso ni siquiera haya oído hablar de un alto porcentaje de los conceptos que aquí se introducen. Además, la intuición geométrica no resulta tan útil como en otras asignaturas del primer curso.

En muchas universidades españolas, una buena parte de los contenidos de esta asignatura son impartidos en el segundo curso de la licenciatura. Por esta causa, los libros de texto en castellano que abarcan los temas de la asignatura suelen presuponer una destreza en el manejo de los conceptos abstractos que no podemos esperar en los alumnos recién llegados a la universidad. Esto es lo que nos ha hecho creer en la utilidad de este texto-guía, que hemos escrito pensando en alumnos de un primer curso de la Licenciatura en Matemáticas.

Objetivos

El objetivo genérico de la asignatura es la adquisición de capacidad de comprensión y manejo de conceptos abstractos, así como el desarrollo de la capacidad de análisis y el rigor en la comprensión de demostraciones y la resolución de problemas.

Más concretamente, en esta asignatura se pretende que el alumno adquiera destreza en la manipulación de los objetos algebraicos más básicos: anillos, grupos, polinomios, etc. Estos objetos serán una herramienta fundamental en muchas de las asignaturas de la licenciatura, especialmente de las del área de álgebra. Los métodos que se aprenderán en este curso dejarán al alumno a las puertas de la Teoría de Galois y la Teoría de Números, entre otras.

Temario

La organización en bloques temáticos es la siguiente:

- Primera parte: Anillos (48 horas)
  - Enteros (12 horas)
    - Capítulo 1: El anillo de los números enteros.
  - Anillos (24 horas)
    - Capítulo 2: Anillos.
    - Capítulo 3: Divisibilidad y factorización en dominios.
  - Polinomios (12 horas)
    - Capítulo 4: Anillos de polinomios.

- Segunda parte: Grupos (58 horas)
  - Grupos (22 horas)
    - Capítulo 5: Grupos.
    - Capítulo 6: Grupos de permutaciones.
  - Estructura de los grupos (36 horas)
    - Capítulo 7: Grupos abelianos finitamente generados.
    - Capítulo 8: Estructura de los grupos finitos.
    - Capítulo 9: Series normales.
- Tercera parte: Formas canónicas (14 horas)
  - Formas canónicas (14 horas)
    - Capítulo 10: Formas canónicas de endomorfismos.

Estructura y uso del texto guía

El texto-guía está dividido en tres partes. Las dos primeras, más extensas, se dedican al estudio de los anillos y los grupos, y en una tercera se estudian las formas canónicas de matrices. Suponemos que el alumno está familiarizado con el lenguaje y las propiedades elementales de Lógica y Teoría de Conjuntos intuitiva, aunque no necesariamente de Lógica Formal y Teoría de Conjuntos avanzada. Más concretamente, suponemos que el alumno conoce y maneja las operaciones conjuntistas elementales; el concepto de aplicación entre conjuntos; los conceptos de relación binaria, de equivalencia y de orden; los números naturales, enteros, racionales, reales y complejos; y el Principio de Inducción.

Excepto por los prerrequisitos que acabamos de comentar, el texto es autocontenido; es decir, los conceptos, métodos y resultados necesarios son presentados siguiendo una secuencia lógica completa. Por tanto, una lectura del principio al final proporciona métodos y resultados que pueden ser utilizados posteriormente en el texto. Por supuesto, el orden elegido no es el único posible. De hecho, es habitual en muchos textos de álgebra empezar por grupos y acabar con anillos. Una tal lectura del texto es posible aunque llevaría consigo problemas en la comprensión de algunas demostraciones aunque no necesariamente de los conceptos. El último capítulo (sobre formas canónicas de endomorfismos) podría ser leído después del capítulo cuarto (sobre polinomios), y posiblemente esto sería más lógico desde un punto de vista conceptual. Sin embargo, hemos preferido dejarlo para el final ya que los métodos utilizados en el capítulo siete (sobre grupos abelianos) son muy similares a los que se usan en el último y más fáciles de asimilar en el contexto de grupos abelianos.

Hay dos excepciones a la afirmación de que el texto es autocontenido. La primera se refiere a la demostración del Teorema Fundamental del Álgebra, en la que adelantamos resultados que el alumno verá, en este mismo curso, en las asignaturas de Análisis Matemático y Topología. La segunda se refiere a las propiedades elementales de las expresiones matriciales de aplicaciones lineales, que el alumno ya conocerá por la asignatura de Álgebra Lineal cuando estudie el último capítulo.

Es bien sabido que las matemáticas sólo se asimilan correctamente comprendiendo las demostraciones de los resultados y resolviendo ejercicios. Por tanto, recomendamos al lector que lea el texto provisto de papel y lápiz para ir realizando los cálculos y argumentos necesarios que le garanticen que está comprendiendo todo lo que se afirma. Para incentivar esta actitud crítica hemos incluido en lugares claves del texto preguntas o ejercicios. La mayoría de los ejercicios incluidos en el texto son utilizados posteriormente en demostraciones; es decir, estos ejercicios deberán ser considerados como lemas o proposiciones que se dejan al lector porque se consideran accesibles y ponen de manifiesto el grado de comprensión que en ese momento se tiene. Por tanto, recomendamos encarecidamente su resolución en el momento en que sean propuestos.

Cada capítulo termina con una amplia lista de problemas y ejercicios cuya resolución es la mejor garantía de éxito. Hemos procurado incluir problemas de "todos los niveles", con el fin de que el estudiante se ejercite gradualmente sin frustrarse y que finalmente se alcance el nivel de dificultad habitualmente requerido en los exámenes. Algunos problemas especialmente difíciles, o que desarrollan conceptos que no están entre los contenidos fundamentales de la asignatura, han sido marcados con el símbolo [*]. No hay separación entre problemas teóricos y prácticos, simplemente porque es difícil

marcar la frontera entre unos y otros, al menos en el Álgebra Básica y, además, a nuestro entender, esta separación resultaría inútil. Hemos procurado presentarlos en orden de dificultad ascendente, pero por supuesto, la dificultad es un concepto subjetivo, así que hay que tomarlo con reservas. En la sección dedicada a la evaluación haremos más comentarios.

Evaluación

En general, en un examen de matemáticas los estudiantes se encuentran con dos grandes tipos de preguntas: aquéllas donde se pide que el estudiante reproduzca o aplique directamente algún resultado visto en clase y aquéllas donde se refleja el conocimiento operativo de los resultados vistos en clase y sus interconexiones. Las primeras se suelen llamar preguntas teóricas y las segundas prácticas, aunque muchas de éstas tienen un componente teórico importante.

Las preguntas teóricas esconden poco misterio. En ellas, se pretende comprobar que se hayan asimilado ciertas técnicas y resultados que se consideran especialmente importantes. Una condición necesaria (pero de ninguna manera suficiente) para estar verdaderamente preparado para un examen es ser capaz de reproducir la demostración de cualquier resultado visto en clase.

Las preguntas prácticas son ejercicios y problemas cuya resolución requiere la manipulación de los resultados y técnicas vistos en clase. Hay diversos subtipos en función de la cantidad de resultados y técnicas que se ven involucradas. El abanico se abriría con aquellas preguntas que se pueden resolver aplicando directamente un resultado o una técnica vista en clase, y se cerraría con aquellas donde la respuesta requiere mezclar diversas técnicas vistas en clase teniendo incluso que modificar los argumentos originales o, más aún, fabricar algunos argumentos elementales.

Vamos a ver algunos ejemplos. Como muestra de preguntas teóricas tenemos:

Septiembre 1992: ¿Cuáles de las siguientes afirmaciones son verdaderas? Razonar la respuesta:

1. Todo ideal maximal es primo.
2. Todo ideal primo es maximal.
3. Todo ideal primo de un DFU es maximal.
4. Todo DIP es DFU.
5. Todo DFU es DIP.

Febrero 1999: Demuestra el Teorema de Cauchy.

Diciembre 1998: Dar un contraejemplo al recíproco del Teorema de Lagrange.

Como se ve, no hay misterio. Casi se puede decir en qué página de los apuntes está la respuesta.

Como ejemplos de preguntas prácticas tenemos las siguientes, en orden de dificultad:

Julio 1999 Sea f el endomorfismo de $\mathbb{R}^3$ cuya matriz en cierta base es

$$A = \begin{pmatrix} 2 & -2 & 1 \\ 0 & 1 & 0 \\ -1 & 2 & 0 \end{pmatrix}$$

(a) Determinar su polinomio mínimo, sus factores invariantes, su forma canónica racional y su forma canónica de Jordan.

(b) Hallar una matriz invertible P tal que $P^{-1}AP$ sea la forma canónica de Jordan.

Julio 1999 Sea G un grupo y sean H, K subgrupos de G.

(a) Demostrar que, para cualesquiera dos clases laterales Hx y Ky de G, la intersección $Hx \cap Ky$ verifica una de dos: o es vacía, o es una clase lateral de G módulo $H \cap K$.

(b) Deducir que si H y K tienen ambos índice finito en G entonces $H \cap K$ también tiene índice finito en G.

Julio 1997 Sea G un grupo finito de orden n que actúa sobre sí mismo mediante traslaciones por la izquierda. Sabemos que dicha acción da lugar a un homomorfismo $L : G \to S_n$. Se pide:

1. Probar que si $g \in G$ es un elemento de orden m, entonces la paridad de la permutación $L(g)$ coincide con la paridad del entero $(m-1)\dfrac{n}{m}$.
2. Probar que si existe un $g \in G$ tal que la permutación $L(g)$ es impar, entonces G posee un subgrupo normal de índice dos.
3. Probar que si P es un 2-subgrupo de Sylow del grupo alternado A_5, entonces P es isomorfo al 4-grupo de Klein (es decir, isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$).

Diciembre 1992 Sea K un cuerpo y sean $P, Q \in K[X,Y]$ polinomios no nulos. Probar que si P y Q son coprimos entonces el siguiente conjunto es finito

$$\{(a,b) : P(a,b) = Q(a,b) = 0\}.$$

Los argumentos para responder a este tipo de preguntas pueden variar de una persona a otra. No pretendemos decir como "hay" que responder, sino sólo ilustrar la clasificación anterior.

Para responder a la primera pregunta hay que hacer los cálculos. Es directa.

La segunda pregunta es casi monotemática. Hay que manipular y reproducir las técnicas empleadas en los resultados sobre el Teorema de Lagrange y propiedades de las clases laterales. Para obligar al estudiante a repetir técnicas y manipulaciones se elimina la hipótesis de que el grupo sea finito.

La tercera es del tipo que involucra diversos temas, de los que hay que usar propiedades y también reproducir técnicas. Los temas involucrados en este caso son: Teorema de Cayley, clases laterales y Teorema de Lagrange, permutaciones, grupos alternados y clasificación de grupos finitos.

Para resolver la última pregunta se utiliza el cuerpo de cocientes, $K(X)$, del anillo de polinomios $K[X]$ para construir un dominio de ideales principales $K(X)[Y]$ donde aplicar el Lema de Bezout. Luego, es necesario fabricar un argumento dentro de este dominio y aplicar que un polinomio en una indeterminada sobre un cuerpo tiene un número finito de raíces. A menudo, en este tipo de problemas se da una indicación. En este caso se dio la siguiente: Utilizar el Lema de Bezout en $K(X)[Y]$.

Como se ve, presentarse a un examen con solamente un "panorama" de los resultados vistos en clase es como jugar a la lotería (o peor, porque el precio de la matrícula es superior al de un billete de lotería de navidad). Para presentarse a un examen con opciones a un buen resultado, además de saber resolver los problemas más típicos y de conocer y saber manipular las técnicas de demostración involucradas en los resultados vistos en clase, es necesario tener una visión general que permita hacer interconexiones entre los temas. De hecho, este último es uno de los grandes objetivos de esta asignatura.

Agradecimientos

Durante la elaboración de este texto guía nos hemos beneficiado de muchas conversaciones con nuestros compañeros del área de Álgebra de la Universidad de Murcia (e incluso de sus notas de clase), cuya experiencia previa como profesores de la asignatura Álgebra Básica y de su predecesora, el Álgebra I del antiguo plan de estudios, está sin duda reflejada en el texto.

Capítulo 1

El anillo de los números enteros

Partiendo de nociones básicas sobre números naturales y números enteros, se demuestran los principales teoremas de la aritmética.

Introducción

Todos tenemos una noción intuitiva de los números enteros $(\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots)$, y manejamos con soltura algunas de sus propiedades básicas, que a menudo asumimos como verdades indiscutibles. Sin embargo, estas propiedades no son independientes; es decir, algunas de ellas se pueden deducir a partir de otras. En este capítulo vamos a introducir los números enteros de forma axiomática: Definiremos el conjunto de los números enteros enunciando una lista de propiedades elementales, llamadas *axiomas*, que entenderemos como verdades asumidas (y que por tanto no requieren demostración). A partir de ellas, y usando las reglas de la lógica, iremos deduciendo otras propiedades importantes.

Nos centraremos en los aspectos multiplicativos, hasta llegar al Teorema Fundamental de la Aritmética: todo número entero se factoriza, de modo esencialmente único, como producto de números primos. Entre las herramientas que usaremos, las más importantes serán: la posibilidad de cancelar enteros no nulos en productos, la posibilidad de dividir con resto por enteros no nulos, y la propiedad que tiene todo número primo de dividir a alguno de los factores cuando divide a un producto.

En la segunda mitad del capítulo estudiaremos la aritmética de congruencias, que se revelará como un concepto de la mayor importancia en diversos momentos del curso. Estableceremos sus propiedades básicas y las usaremos para esbozar una aplicación a la criptografía de clave pública. Además, el proceso de dotar a los "enteros módulo n" de una estructura algebraica a partir de la que ya conocemos en los números enteros ilustra la que será otra de las nociones fundamentales del curso: la formación de "estructuras cociente".

Objetivos del capítulo

- Deducir las propiedades básicas de los números enteros a partir de los axiomas.
- Conocer los conceptos de máximo común divisor y mínimo común múltiplo de un conjunto de enteros, y relacionarlos con el concepto de ideal.
- Usar el Algoritmo de Euclides para calcular el máximo común divisor de dos enteros y la correspondiente identidad de Bezout, y para resolver algunas ecuaciones diofánticas.
- Conocer las propiedades básicas de los números primos.
- Demostrar el Teorema Fundamental de la Aritmética, y utilizarlo para obtener otras propiedades de los números enteros.
- Manejar las operaciones con congruencias; en particular, el cálculo de inversos y de potencias y la resolución de ciertas ecuaciones.
- Usar el Teorema Chino de los Restos para resolver sistemas de ecuaciones de congruencias.

Desarrollo de los contenidos

1.1 Axiomas y propiedades básicas

Se llaman *números enteros* los elementos de un conjunto que denotamos por $\mathbb{Z}$ de forma que se verifican los siguientes axiomas[1]:

Axiomas de operaciones. Existen dos operaciones en $\mathbb{Z}$, o sea, dos aplicaciones

$$\begin{array}{ccc} \mathbb{Z}\times\mathbb{Z} & \xrightarrow{+} & \mathbb{Z} \\ (a,b) & \mapsto & a+b \end{array} \qquad \text{y} \qquad \begin{array}{ccc} \mathbb{Z}\times\mathbb{Z} & \xrightarrow{\cdot} & \mathbb{Z} \\ (a,b) & \mapsto & a\cdot b = ab \end{array}$$

llamadas, respectivamente, *suma* y *producto*, que verifican:

- *Asociativa*: Para todo $a,b,c\in\mathbb{Z}$, $a+(b+c)=(a+b)+c$ y $a(bc)=(ab)c$.
- *Conmutativa*: Para todo $a,b\in\mathbb{Z}$, $a+b=b+a$ y $ab=ba$.
- *Distributiva*: Para todo $a,b,c\in\mathbb{Z}$, $a(b+c)=ab+ac$.
- *Neutros*: Existen dos números enteros $0\neq 1$ tales que $a+0=a$ y $a1=a$, para todo $a\in\mathbb{Z}$.
- *Opuestos*: Para cada $a\in\mathbb{Z}$ existe $a'\in\mathbb{Z}$ tal que $a+a'=0$.
- *Regularidad*: Si a y b son dos números enteros tales que $ab=0$, entonces $a=0$ ó $b=0$.

Axiomas de orden. Existe una relación binaria $\leq$ en $\mathbb{Z}$ (si a está relacionado con b por la relación "$\leq$" escribimos $a\leq b$) para la que se verifican:

- *Reflexiva*: Para todo $a\in\mathbb{Z}$, $a\leq a$.
- *Antisimétrica*: Si $a,b\in\mathbb{Z}$ verifican $a\leq b$ y $b\leq a$, entonces $a=b$.
- *Transitiva*: Si $a,b,c\in\mathbb{Z}$ satisfacen $a\leq b$ y $b\leq c$, entonces $a\leq c$.
- *Dicotomía*: Dados $a,b\in\mathbb{Z}$ se tiene o bien $a\leq b$ o bien $b\leq a$.
- *Buena Ordenación*: Todo subconjunto S de $\mathbb{Z}$ no vacío y acotado inferiormente tiene un *mínimo* (o *primer elemento*). Es decir, si $S\neq\emptyset$ y existe $c\in\mathbb{Z}$ tal que $c\leq s$ para cada $s\in S$, entonces existe $m\in S$ tal que $m\leq s$ para todo $s\in S$.
- *Compatibilidad del orden con las operaciones* : Si a y b son dos números enteros tales que $a\leq b$ entonces $a+c\leq b+c$, para todo $c\in\mathbb{Z}$. Además, si $0\leq c$, entonces $ac\leq bc$.

A partir de estos axiomas podemos empezar a demostrar propiedades del conjunto de los números enteros. Empezamos con las que afectan a las operaciones suma y producto:

Proposición 1.1.1 *En $\mathbb{Z}$ se verifican las siguientes propiedades:*

1. (Unicidad de los neutros) *Sólo hay un entero 0 tal que $0+a=a$ para todo $a\in\mathbb{Z}$. Y sólo hay un entero 1 tal que $1a=a$ para todo $a\in\mathbb{Z}$.*
2. (Unicidad de los opuestos) *Para cada $a\in\mathbb{Z}$ existe un único $a'\in\mathbb{Z}$ tal que $a+a'=0$. Este único elemento se llama el* opuesto *de a y se denota por $-a$; la suma $b+(-a)$ se denota por $b-a$.*
3. (Cancelación en sumas) *Dados $a,b,c\in\mathbb{Z}$, la igualdad $a+b=a+c$ implica $b=c$.*
4. (Multiplicación por cero) *Para cada $a\in\mathbb{Z}$ se verifica $a0=0$.*
5. (Reglas de signos) *Dados $a,b\in\mathbb{Z}$ se verifican $-(-a)=a$, $a(-b)=(-a)b=-(ab)$ y $(-a)(-b)=ab$.*
6. (Cancelación en productos) *Dados $a,b,c\in\mathbb{Z}$ con $a\neq 0$, la igualdad $ab=ac$ implica $b=c$.*

[1] El origen de la notación $\mathbb{Z}$ es la palabra alemana *Zahl* que significa número.

Demostración. 1. Supongamos que 0 y $0'$ satisfacen la propiedad. Entonces $0' = 0 + 0' = 0' + 0 = 0$. La unicidad del neutro para el producto se demuestra de forma similar.

2. Sabemos que existe un entero a' con esa propiedad, y si otro entero a'' la verifica entonces $a'' = 0 + a'' = (a' + a) + a'' = a' + (a + a'') = a' + 0 = a'$.

3. No hay más que sumar $-a$ en ambos miembros.

4. Basta cancelar en la igualdad $0 + a0 = a0 = a(0 + 0) = a0 + a0$.

5. La primera igualdad es consecuencia de 2. Para la segunda, como $ab + a(-b) = a((b + (-b)) = a0 = 0$, deducimos que $a(-b)$ es el opuesto de ab. La igualdad $(-a)b = -(ab)$ se obtiene de modo similar, y usando esas dos igualdades y el hecho de que $-(-x) = x$ se deduce que $(-a)(-b) = ab$.

6. De $ab = ac$ se obtiene $a(b - c) = ab - ac = 0$ (usando 5), y como $a \neq 0$, deducimos por el Axioma de Regularidad que $b - c = 0$, de donde $b = c$ (sumando c en ambos miembros). □

Las siguientes propiedades que consideraremos tienen que ver con el orden; es conveniente introducir la terminología y la notación siguientes:

- Emplearemos del modo usual los símbolos $\geq$, $<$ y $>$ y la terminología "menor o igual", "mayor o igual", "estrictamente mayor", etc. Con esta notación, el axioma de dicotomía se puede reenunciar como una tricotomía: Dados $a, b \in \mathbb{Z}$, se verifica exactamente una de las siguientes condiciones:

$$a < b, \qquad a = b \qquad \text{ó} \qquad a > b.$$

- Los números enteros mayores o iguales que 0 se llaman *números naturales*, y el conjunto que forman se denota por $\mathbb{N}$. Los números enteros estrictamente mayores que 0 se llaman *enteros positivos*, y el conjunto que forman se denota por $\mathbb{Z}^+$. Los números enteros estrictamente menores que 0 se llaman *enteros negativos*, y el conjunto que forman se denota por $\mathbb{Z}^-$. En símbolos:

$$\mathbb{N} = \{a \in \mathbb{Z} : a \geq 0\} \qquad \mathbb{Z}^+ = \{a \in \mathbb{Z} : a > 0\} \qquad \mathbb{Z}^- = \{a \in \mathbb{Z} : a < 0\}$$

Las siguientes propiedades sobre el orden tienen demostraciones sencillas a partir de los axiomas (principalmente el de compatibilidad) y de las propiedades ya demostradas, y las dejamos como ejercicio para el lector. ¡Cuidado! no se puede utilizar nada que no sea una axioma o no haya sido previamente demostrado.

Ejercicio 1.1.2 *Demostrar que se verifican las siguientes propiedades para $a, b, c, d \in \mathbb{Z}$.*

1. *$a \leq b$ si y sólo si $a + c \leq b + c$.*
2. *$a < b$ si y sólo si $a + c < b + c$.*
3. *Si $c > 0$ entonces $a \leq b$ si y sólo si $ac \leq bc$.*
4. *Si $c > 0$ entonces $a < b$ si y sólo si $ac < bc$.*
5. *Si $a \leq b$ y $c \leq d$ entonces $a + c \leq b + d$, y esta desigualdad es estricta si lo es alguna de las iniciales.*
6. *Dados $a, b, c, d \in \mathbb{Z}^+$ con $a \leq b$ y $c \leq d$, se tiene $ac \leq bd$, y esta desigualdad es estricta si lo es alguna de las iniciales.*
7. *$a \in \mathbb{Z}^+$ si y sólo si $-a \in \mathbb{Z}^-$.*
8. *$a < b$ si y sólo si $b - a \in \mathbb{Z}^+$, si y sólo si $a - b \in \mathbb{Z}^-$*
9. *$a < b$ si y sólo si $-a > -b$.*

Proposición 1.1.3 *Se verifican las siguientes propiedades para $a, b, c \in \mathbb{Z}$.*

1. *Si $a \leq b$ y $c < 0$ entonces $ac \geq bc$.*
2. *Si $a \neq 0$ entonces $a^2 > 0$. En particular, $1 > 0$ y $-1 < 0$.*

3. *El 1 es el mínimo de $\mathbb{Z}^+$; es decir, $1 \leq n$ para cada $n \in \mathbb{Z}^+$.*

4. *No hay enteros entre a y $a+1$; es decir, no existe ningún $n \in \mathbb{Z}$ tal que $a < n < a+1$.*

5. *$a < b$ si y sólo si $a + 1 \leq b$.*

Demostración. 1. Si $c < 0$ entonces $-c > 0$ (Ejercicio 1.1.2), y el Axioma de Compatibilidad nos dice que $a(-c) \leq b(-c)$, o sea $-(ac) \leq -(bc)$. Finalmente, $ac \geq bc$, por el Ejercicio 1.1.2.

2. Por el Axioma de Dicotomía, se tiene o bien $a > 0$ o bien $a < 0$; el resultado se deduce entonces del Axioma de Compatibilidad (en el primer caso) o del apartado 1 (en el segundo). Como $1 = 1^2$, deducimos que $1 > 0$, y entonces $-1 < 0$, por el Ejercicio 1.1.2.

3. Por su definición, $\mathbb{Z}^+$ está acotado inferiormente por el 0, y no es vacío pues $1 \in \mathbb{Z}^+$; entonces $\mathbb{Z}^+$ tiene un elemento mínimo m por el Axioma de Buena Ordenación. Entonces $m \leq 1$, de donde $m^2 \leq m$ por compatibilidad; pero $m^2 \in \mathbb{Z}^+$ por el apartado anterior, y en consecuencia $m^2 = m$ por la minimalidad de m; cancelando m en esa igualdad obtenemos finalmente $m = 1$, como queríamos ver.

4. Una desigualdad $a < n < a + 1$ implicaría $0 < n - a < 1$, contra el apartado anterior.

5. Si $a < b$ entonces $b - a \in \mathbb{Z}^+$ y por lo tanto $1 \leq b - a$, de donde $a + 1 \leq b$. La implicación recíproca es fácil usando que $0 < 1$ y la transitividad. □

Ejercicio 1.1.4 *Demostrar que:*

1. *Ninguna sucesión estrictamente decreciente de enteros está acotada inferiormente. En particular, no existen sucesiones estrictamente decrecientes de enteros positivos.*

2. *Todo subconjunto S de $\mathbb{Z}$ no vacío y acotado superiormente tiene un máximo. Es decir, si $S \neq \emptyset$ y existe $c \in \mathbb{Z}$ tal que $c \geq s$ para cada $s \in S$, entonces existe $m \in S$ tal que $m \geq s$ para todo $s \in S$.*

3. *Ninguna sucesión estrictamente creciente de enteros está acotada superiormente.*

Teorema 1.1.5 (Principio de Inducción) *Sea S un subconjunto de $\mathbb{N}$ tal que $0 \in S$ y para todo $n \in S$ se verifica que $n + 1 \in S$. Entonces $S = \mathbb{N}$.*

Demostración. Procederemos por reducción al absurdo. Supongamos que $S \neq \mathbb{N}$. Entonces $X = \mathbb{N} \setminus S$ es un subconjunto de $\mathbb{Z}$ no vacío y acotado inferiormente por el 0, por lo que tiene un primer elemento a, y de hecho $a \in \mathbb{Z}^+$ puesto que $0 \in S$. Entonces $a \geq 1$, lo que implica que $a - 1 \in \mathbb{N}$; además, $a - 1 \in S$, pues de lo contrario se tendría $a - 1 \in X$, en contra de la elección de a. Pero ahora la hipótesis del teorema nos dice que $a = (a - 1) + 1 \in S$, una contradicción. □

Ejercicio 1.1.6 *Demostrar las siguientes variantes del Principio de Inducción (en ambas, b es un entero fijo y S es un subconjunto de $\mathbb{Z}$):*

1. *Si $b \in S$, y si $n \in S$ implica $n+1 \in S$ (o lo que es lo mismo, si $n-1 \in S$ implica $n \in S$), entonces S contiene a todos los enteros mayores o iguales que b.*

2. *Si $b \in S$, y si la condición "$a \in S$ cuando $b \leq a < n$" implica que $n \in S$, entonces S contiene a todos los enteros mayores o iguales que b.*

Concluimos esta sección con una última propiedad básica de los números enteros: la posibilidad de *dividir con resto*. Se define el *valor absoluto* de un entero a como

$$|a| = \begin{cases} a & \text{si } a \in \mathbb{N} \\ -a & \text{si } a \notin \mathbb{N} \end{cases}$$

Del apartado 7 del Ejercicio 1.1.2 se deduce que $|a| \in \mathbb{N}$, para todo $a \in \mathbb{Z}$.

Ejercicio 1.1.7 *Demostrar que para toda pareja de números enteros a y b se verifica la igualdad:*

$$|ab| = |a| \cdot |b|.$$

Teorema 1.1.8 (División con Resto) *Para toda pareja de números enteros a y b con $b \neq 0$ existen otros dos números enteros q y r tales que*

$$a = bq + r \qquad y \qquad 0 \leq r < |b|.$$

Estos enteros q y r son únicos y se les llama, respectivamente, el cociente *y el* resto *de la división de a entre b.*

Demostración. Como $b \neq 0$, el conjunto $S = \{a - bn : n \in \mathbb{Z}\}$ contiene una sucesión estrictamente creciente (¿por qué?). Por tanto no tiene una cota superior (¿por qué?) y en consecuencia $S \cap \mathbb{N} \neq \emptyset$ (¿por qué?). Sea r el mínimo de $S \cap \mathbb{N}$ y sea $q \in \mathbb{Z}$ tal que $a - bq = r$. Obsérvese que

$$r - |b| = a - bq - |b| = a - b(q \pm 1) \in S.$$

De la minimalidad de r se deduce que $r - |b| < 0$ y, por tanto $r < |b|$. Esto prueba la existencia de q y r satisfaciendo la propiedad requerida.

Veamos la unicidad. Supongamos que $a = bq + r = bq_1 + r_1$ con $0 \leq r, r_1 < |b|$. Entonces

$$|b| > |r_1 - r| = |b(q_1 - q)| = |b| \cdot |q_1 - q|$$

(¿por qué?). De donde se deduce que $q_1 = q$ (¿por qué?) y, por tanto, $r = r_1$. □

Ejercicio 1.1.9 *Dar demostraciones rigurosas de todas las afirmaciones que se han acompañado de un "¿por qué?" en la demostración anterior.*

1.2 Divisibilidad e ideales

Definición 1.2.1 *Sean a y b dos números enteros. Diremos que a* divide a *b, o que a* es un divisor de *b, o que b* es múltiplo de *a, si existe un entero n tal que $b = an$. En tal caso escribiremos $a \mid b$.*

De la propiedad de cancelación en productos se deduce que si $a \neq 0$ y $a \mid b$, entonces existe un único elemento $n \in \mathbb{Z}$ tal que $b = an$. Denotaremos este elemento n por $\frac{b}{a}$ o por b/a.

El lector puede demostrar algunas propiedades básicas de la relación de divisibilidad.

Ejercicio 1.2.2 *Dados $a, b, c, d \in \mathbb{Z}$ se verifica:*

1. *(Reflexiva) $a \mid a$.*
2. *(Transitiva) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*
3. *(Casi Antisimétrica) Si $a \mid b$ y $b \mid a$, entonces $b = \pm a$ (o sea, $|b| = |a|$).*
4. *El 0 es múltiplo de cualquier entero, y sólo es divisor de sí mismo.*
5. *El 1 es divisor de cualquier entero, y sólo es múltiplo de 1 y de -1 (para demostrar esto último, usa las propiedades del orden en $\mathbb{Z}$).*
6. *$a \mid b$ si y sólo si $a \mid -b$, si y sólo si $-a \mid b$, si y sólo si $-a \mid -b$.*
7. *Si $a \mid b$ y $a \mid c$, entonces $a \mid rb + sc$ para cualesquiera $r, s \in \mathbb{Z}$ (en particular, $a \mid b + c$, $a \mid b - c$ y $a \mid rb$ para cualquier $r \in \mathbb{Z}$).*
8. *Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$.*
9. *Si $0 \neq r \in \mathbb{Z}$ entonces: $a \mid b$ si y sólo si $ar \mid br$.*
10. *Si $a \mid b$, entonces $|a| \leq |b|$.*

El apartado 7 del Ejercicio 1.2.2 sugiere las siguientes definiciones, que serán muy útiles para trabajar con cuestiones de divisibilidad.

Definición 1.2.3 *Una* combinación lineal *con coeficientes enteros (o una* combinación $\mathbb{Z}$-lineal*) de los enteros $a_1, \ldots, a_n$ es un entero de la forma*

$$r_1 a_1 + \cdots + r_n a_n,$$

donde cada $r_i \in \mathbb{Z}$. Los enteros r_i son los coeficientes *de la combinación lineal.*

Un subconjunto I de $\mathbb{Z}$ es un ideal *si no es vacío y si, dados $a, b \in I$, cualquier combinación lineal suya $ra + sb$ sigue siendo un elemento de I.*

Por inducción, se ve fácilmente que cualquier combinación lineal de un numero finito de elementos de un ideal I sigue siendo un elemento de I. Por otra parte, en la definición de ideal, la condición $I \neq \emptyset$ se puede sustituir por la condición $0 \in I$, tomando combinaciones lineales con coeficientes nulos.

Proposición 1.2.4 *Para un subconjunto no vacío I de $\mathbb{Z}$, las condiciones siguientes son equivalentes:*

1. *I es un ideal.*
2. *Si $a, b \in I$, entonces $a+b \in I$ y $ra \in I$ para cada $r \in \mathbb{Z}$ (I es cerrado para sumas y para múltiplos).*
3. *Si $a, b \in I$ entonces $a - b \in I$ (I es cerrado para restas).*

Demostración. Es claro que las dos primeras condiciones son equivalentes e implican la tercera. Por último, si asumimos 3, es elemental ver, por este orden, que $0 \in I$, que si $a \in I$ entonces $-a \in I$, y que si $a, b \in I$ entonces $a + b \in I$. Ahora es fácil ver, por inducción, que si $a \in I$ entonces $ra \in I$ (y por lo tanto $-ra \in I$) para cada $r \in \mathbb{N}$, con lo que se tiene 2. □

Veamos algunos ejemplos de ideales. Dejamos al lector que demuestre las afirmaciones que siguen.

Ejemplos 1.2.5 *Ideales.*

1. $\mathbb{Z}$ y $\{0\}$ son dos ideales de $\mathbb{Z}$.
2. Si $a \in \mathbb{Z}$, el conjunto (a) formado por los múltiplos de a es un ideal de $\mathbb{Z}$. Este ideal se llama *ideal principal* generado por a.
3. Más generalmente, si $a_1, \ldots, a_n \in \mathbb{Z}$, entonces el conjunto

$$(a_1, \ldots, a_n) = \{k_1 a_1 + \cdots + k_n a_n : k_1, \ldots, k_n \in \mathbb{Z}\} \tag{1.2.1}$$

   es un ideal de $\mathbb{Z}$, llamado *ideal generado* por $a_1, \ldots, a_n$.
4. La intersección de una familia de ideales es un ideal.
5. Si I y J son dos ideales de $\mathbb{Z}$, entonces

$$I + J = \{a + b : a \in I, b \in J\}$$

   es un ideal de $\mathbb{Z}$. Más generalmente, si $I_1, \ldots, I_r$ son ideales de $\mathbb{Z}$, entonces

$$I_1 + \cdots + I_r = \{a_1 + \cdots + a_r : \text{cada } a_i \in I_i\}$$

   es un ideal de $\mathbb{Z}$. Obsérvese que, con esta notación, se tiene

$$(a_1, \ldots, a_n) = (a_1) + \cdots + (a_n).$$

Sea S un subconjunto de $\mathbb{Z}$. Como $\mathbb{Z}$ es un ideal de $\mathbb{Z}$, entonces existe al menos un ideal de $\mathbb{Z}$ que contiene a S. Acabamos de mencionar que la intersección de una familia de ideales de $\mathbb{Z}$ es otro ideal de $\mathbb{Z}$. En particular, la intersección I de todos los ideales que contienen a S es un ideal que está contenido en todos los ideales que contienen a S. Es decir, I es el menor ideal que contiene a S, donde el sentido de menor se refiere a la relación de inclusión. Por esta razón dicho ideal se llama *ideal generado* por S. Obsérvese que en los ejemplos anteriores también hemos llamado ideal generado por $a_1, \ldots, a_n$ al conjunto (1.2.1). Vamos a ver que la utilización del mismo nombre está justificada:

Proposición 1.2.6 *Sea S un conjunto de números naturales; entonces la intersección de los ideales de $\mathbb{Z}$ que contienen a S coincide con el conjunto*

$$(S) = \{\sum_{i=1}^{n} k_i a_i : k_i \in \mathbb{Z}, a_i \in S\}$$

de todas las combinaciones lineales de familias finitas de elementos de S.

Demostración. En los comentarios realizados antes de la proposición se ha visto que la intersección de los ideales de $\mathbb{Z}$ que contienen a S es el menor ideal de $\mathbb{Z}$ que contiene a S. Por tanto basta demostrar que el conjunto (S) del enunciado también es el menor ideal de $\mathbb{Z}$ que contiene a S; es decir, que se verifican las tres siguientes condiciones:

- $S \subseteq (S)$.
- (S) es un ideal de $\mathbb{Z}$.
- Si I es un ideal de $\mathbb{Z}$ que contiene a S, entonces $(S) \subseteq I$.

El lector puede demostrar que efectivamente estas condiciones se verifican. □

Ejercicio 1.2.7 *Demostrar que si I y J son conjuntos de números enteros, entonces $(I)+(J) = (I \cup J)$. En particular, si I y J son ideales, entonces $I + J$ es el menor ideal que contiene a I y a J.*

La relación de divisibilidad se puede expresar de forma sencilla en términos de ideales:

Proposición 1.2.8 *Las siguientes condiciones son equivalentes para dos números enteros a y b.*

1. $a \mid b$.
2. $b \in (a)$.
3. $(b) \subseteq (a)$.

Demostración. La equivalencia entre 1 y 2 viene de la definición de ideal principal. Como (b) es el menor ideal de $\mathbb{Z}$ que contiene a b, se tiene $(b) \subseteq (a)$ precisamente si $b \in (a)$. □

Usando este resultado y las propiedades del Ejercicio 1.2.2, los ejercicios siguientes son fáciles:

Ejercicio 1.2.9 *Las siguientes condiciones son equivalentes para un número entero a:*

1. $(a) = \mathbb{Z}$.
2. $a \mid 1$.
3. $a = 1$ *ó* $a = -1$ *(o sea, $|a| = 1$).*

Ejercicio 1.2.10 *Las siguientes condiciones son equivalentes para dos números enteros a y b:*

1. $(a) = (b)$.
2. $a \mid b$ *y* $b \mid a$.
3. $a = b$ *ó* $a = -b$ *(o sea, $|a| = |b|$).*

Nuestros primeros ejemplos de ideales de $\mathbb{Z}$ fueron los ideales principales; terminaremos esta sección viendo que no hay otros.

Teorema 1.2.11 *Todos los ideales de $\mathbb{Z}$ son principales. Es decir, si I es un ideal de $\mathbb{Z}$, entonces existe un entero a tal que $I = (a)$.*

Demostración. Sea I un ideal de $\mathbb{Z}$. Si $I = \{0\} = (0)$, entonces I es principal. Supongamos que $I \neq \{0\}$. Entonces I contiene un elemento x diferente de 0, y además $-x = (-1)x \in I$, por lo que I contiene algún entero positivo. Sea a el menor entero positivo que pertenece a I (el mínimo de $I \cap \mathbb{Z}^+$). Veamos que $I = (a)$. Como (a) es el menor ideal que contiene a a, se tiene que $(a) \subseteq I$. Recíprocamente, si $x \in I$, existen $q, r \in \mathbb{Z}$ tales que $x = aq + r$ y $0 \leq r < |a| = a$ (Teorema 1.1.8). Como $a \in I$ y $x \in I$, deducimos que $r = x - aq \in I$, y de la minimalidad de a se deduce que r no es positivo. Por tanto $r = 0$, y en consecuencia $x = aq \in (a)$, como queríamos ver. □

Corolario 1.2.12 *Si S es un conjunto no vacío de números enteros y d es un número entero, las condiciones siguientes son equivalentes:*

1. *$(d) = (S)$; es decir, el ideal generado por S coincide con el ideal principal generado por d.*
2. *$d \mid s$ para cada $s \in S$ y d es una combinación lineal de elementos de S.*

Demostración. $(d) \subseteq (S)$ si y sólo si $d \in (S)$, si y sólo si d es combinación lineal de elementos de S. Por otra parte, $(S) \subseteq (d)$ si y sólo si $s \in (d)$ para cada $s \in S$ (pues (S) es el menor ideal que contiene a cada $s \in S$), si y sólo si d divide a cada $s \in S$. Esto demuestra el resultado. □

1.3 Máximo común divisor y mínimo común múltiplo

Definición 1.3.1 *Sea S un conjunto de números enteros y sean d y m números enteros.*

- *Se dice que d es un* máximo común divisor *de S si se verifican las dos condiciones siguientes:*
  1. *d divide a todos los elementos de S.*
  2. *Si x es un entero que divide a todos los elementos de S, entonces x divide a d.*

  (Es fácil ver que estas dos condiciones equivalen a una sola: Un entero x divide a todos los elementos de S si y sólo si x divide a d).
- *Diremos que m es* mínimo común múltiplo *de S si se verifican las dos condiciones siguientes:*
  1. *m es múltiplo de todos los elementos de S.*
  2. *Si x es un entero que es múltiplo de todos los elementos de S, entonces x es múltiplo de m.*

  (Equivalentemente: Un entero x es múltiplo de cada $s \in S$ si y sólo si x es múltiplo de m).

Escribiremos $d = \text{mcd}(S)$ para indicar que d es un máximo común divisor de S, y $m = \text{mcm}(S)$ si m es un mínimo común múltiplo de S. Si $S = \{a_1, \ldots, a_n\}$, entonces utilizaremos la notación:

$$\text{mcd}(a_1, \ldots, a_n) = \text{mcd}(S) \quad y \quad \text{mcm}(a_1, \ldots, a_n) = \text{mcm}(S).$$

Hay que tener cuidado con esta notación, ya que es ambigua. Por ejemplo, $a = \text{mcd}(S)$ y $b = \text{mcd}(S)$, no implica que $a = b$. En efecto, si a es máximo común divisor de S, entonces $-a$ también es máximo común divisor de S. Una propiedad similar se verifica para el mínimo común múltiplo. Sin embargo, el siguiente ejercicio muestra los límites de esta ambigüedad.

Ejercicio 1.3.2 *Sean a y b dos números enteros y S un conjunto de números enteros. Demostrar que si a y b son ambos máximos comunes divisores de S, entonces $a = \pm b$. Demostrar que la misma propiedad se verifica para el mínimo común múltiplo.*

Obsérvese que todavía no hemos demostrado que cualquier subconjunto de $\mathbb{Z}$ tenga un máximo común divisor ni un mínimo común múltiplo. Usando el concepto de ideal podemos demostrar no sólo la existencia, sino también otras propiedades importantes del máximo común divisor y el mínimo común múltiplo.

Proposición 1.3.3 *Sea S un conjunto de números enteros y sean $d, m \in \mathbb{Z}$. Entonces:*

1. *Las siguientes condiciones son equivalentes:*
   (a) $d = \text{mcd}(S)$.
   (b) $(d) = (S)$.
   (c) $d \mid s$ *para cada* $s \in S$ *y existen* $s_1, \ldots, s_n \in S$ *y* $r_1, \ldots, r_n \in \mathbb{Z}$ *tales que* $d = r_1 s_1 + \cdots + r_n s_n$.
2. *Las siguientes condiciones son equivalentes:*
   (a) $m = \text{mcm}(S)$.
   (b) $(m) = \cap_{s \in S}(s)$.
3. *En particular, S tiene máximo común divisor y mínimo común múltiplo.*

Demostración. De la Proposición 1.2.8, se deduce que $d = \text{mcd}(S)$ precisamente si se verifican las dos siguientes condiciones:

- $S \subseteq (d)$.
- Si x es un entero tal que $S \subseteq (x)$, entonces $(d) \subseteq (x)$.

En otras palabras, $d = \text{mcd}(S)$ precisamente si (d) es el menor ideal que contiene a S; es decir, $(d) = (S)$. Esto demuestra la equivalencia de (a) y (b) en 1, y la equivalencia de (b) y (c) no es más que el Corolario 1.2.12. Dejamos que el lector demuestre 2. Finalmente, 3 es consecuencia del hecho de que todo ideal de $\mathbb{Z}$ es principal (Teorema 1.2.11). □

El siguiente corolario es inmediato.

Corolario 1.3.4 *Dados enteros $a_1, \ldots, a_n$ y d, se verifica: $d = \text{mcd}(a_1, \ldots, a_n)$ si y sólo si d divide a cada a_i y existen $r_1, \ldots, r_n \in \mathbb{Z}$ tales que*

$$r_1 a_1 + \cdots + r_n a_n = d.$$

Esta última expresión se conoce como una identidad de Bezout *para $a_1, \ldots, a_n$.*

Los conjuntos cuyo máximo común divisor es 1 son especialmente importantes, y por eso destacamos aquí el siguiente caso particular del corolario anterior:

Corolario 1.3.5 (Lema de Bezout) *Las siguientes condiciones son equivalentes para los números enteros $a_1, \ldots, a_n$:*

1. *Los únicos divisores comunes a todos los a_i son 1 y -1.*
2. $\text{mcd}(a_1, \ldots, a_n) = 1$.
3. $(a_1, \ldots, a_n) = \mathbb{Z}$.
4. *Existen $r_1, \ldots, r_n \in \mathbb{Z}$ tales que $r_1 a_1 + \cdots + r_n a_n = 1$.*

Diremos que los números enteros $a_1, \ldots, a_n$ son *coprimos* o *primos entre sí* cuando verifiquen las condiciones equivalentes del Corolario 1.3.5. Usando adecuadamente las identidades de Bezout se pueden demostrar fácilmente numerosas propiedades:

Proposición 1.3.6 *Se verifican las siguientes propiedades sobre números enteros:*

1. *Si* $\text{mcd}(a_1, \ldots, a_n) = d$ *entonces* $\text{mcd}(\frac{a_1}{d}, \ldots, \frac{a_n}{d}) = 1$.
2. $\text{mcd}(a, b) = 1$ *y* $\text{mcd}(a, c) = 1$ *si y sólo si* $\text{mcd}(a, bc) = 1$.
3. *Si* $\text{mcd}(a, b) = 1$ *y* $a \mid bc$, *entonces* $a \mid c$.
4. *Si* $\text{mcd}(a, b) = 1$, $a \mid c$ *y* $b \mid c$, *entonces* $ab \mid c$.

Demostración. 1. Si $\mathrm{mcd}(a_1,\ldots,a_n)=d$ entonces $d=r_1a_1+\cdots+r_na_n$ para ciertos enteros $r_1,\ldots,r_n$. Dividiendo por d en ambos miembros y aplicando el Lema de Bezout (1.3.5) se obtiene el resultado deseado.

2. Si $\mathrm{mcd}(a,bc)=1$, del Lema de Bezout se deduce que existen $u,v\in\mathbb{Z}$ tales que $au+bcv=1$. De nuevo aplicando el Lema de Bezout se obtiene que $\mathrm{mcd}(a,b)=1=\mathrm{mcd}(a,c)$.

Supongamos ahora que $\mathrm{mcd}(a,b)=1$ y $\mathrm{mcd}(a,c)=1$. Por el Lema de Bezout (1.3.5), existen enteros r,s,t,u tales que $ra+sb=1$ y $ta+uc=1$. Multiplicando ambas expresiones se obtiene

$$(rat+ruc+sbt)a+(su)(bc)=1,$$

y por lo tanto $\mathrm{mcd}(a,bc)=1$.

3. Por las hipótesis existen enteros r,s,t tales que $1=ra+sb$ y $bc=at$, y multiplicando por c la primera expresión se obtiene $c=rac+sbc=rac+sat=(rc+st)a$, por lo que $a\mid c$.

4. Como $b\mid c$, existe un entero t tal que $c=bt$, y ahora el apartado 3, aplicado a las otras dos hipótesis, nos dice que a divide a t, por lo que ab divide a $tb=c$. □

Ejercicio 1.3.7 *Dar ejemplos que muestren que los dos últimos apartados del resultado anterior son falsos si a y b no son coprimos.*

1.4 Algoritmo de Euclides y ecuaciones diofánticas

En esta sección resolvemos dos problemas prácticos: comenzamos mostrando un método para calcular el máximo común divisor de dos números enteros y la correspondiente identidad de Bezout, y aplicamos entonces esto a la resolución de cierto tipo de ecuaciones.

El primer método es conocido con el nombre de *Algoritmo de Euclides para el Cálculo del Máximo Común Divisor* y está basado en el siguiente ejercicio.

Ejercicio 1.4.1 *Sean a y b dos números enteros. Si $a=bq+r$, entonces* $\mathrm{mcd}(a,b)=\mathrm{mcd}(b,r)$.

Sean a y b dos números enteros cuyo máximo común divisor queremos calcular. Si $a=0$ entonces $\mathrm{mcd}(a,b)=b$. Por tanto podemos suponer que a y b son distintos de 0. Si a se cambia por su opuesto el máximo común divisor de a y b no varía. Por tanto, podemos suponer que a y b son positivos. Supongamos que $b\leq a$. Construimos una tabla como la siguiente:

$a=r_{-1}$	$b=r_0$	r_1	r_2	$\ldots$	$r_n=d$	$r_{n+1}=0$
	q_1	q_2	q_3	$\cdots$	q_{n+1}	

donde q_i y r_i son, respectivamente, el cociente y el resto de dividir r_{i-2} por r_{i-1}, y denotamos por d al último resto no nulo. Obsérvese que algún r_i tiene que ser 0 ya que la sucesión $r_{-1},r_0,r_1,r_2\ldots$ está formada por enteros no negativos y es estrictamente decreciente (Ejercicio 1.1.4). Entonces

$$\mathrm{mcd}(a,b)=\mathrm{mcd}(r_{-1},r_0)=\mathrm{mcd}(r_0,r_1)=\mathrm{mcd}(r_1,r_2)=\cdots=\mathrm{mcd}(r_{n-1},r_n)=\mathrm{mcd}(r_n,0)=r_n=d.$$

De hecho, el método anterior sirve para calcular dos enteros s y t tales que $d=sa+tb$, donde $d=r_n=\mathrm{mcd}(a,b)$. El método consiste en escribir $d=r_n$ en función de a y b utilizando las ecuaciones $r_i=r_{i-2}-q_ir_{i-1}$ "de derecha a izquierda", y lo ilustramos con el siguiente ejemplo:

Ejemplo 1.4.2 *Algoritmo de Euclides en $\mathbb{Z}$.*

Sean $a=18444$ y $b=1632$. Entonces construimos la tabla

$a=18444$	$b=1632$	492	156	24	12	0
	11	3	3	6	2	

Luego $\mathrm{mcd}(a,b)=12$ y

$$\begin{aligned}
12 &= 156-6\cdot 24 &&= 156-6\cdot(492-3\cdot 156)\\
&= -6\cdot 492+19\cdot 156 &&= -6\cdot 492+19\cdot(b-3\cdot 492)\\
&= 19\cdot b-63\cdot 492 &&= 19\cdot b-63\cdot(a-11\cdot b)\\
&= -63\cdot a+712\cdot b.
\end{aligned}$$

Una vez que sabemos cómo calcular el máximo común divisor, podemos calcular el mínimo común múltiplo utilizando la siguiente proposición.

Proposición 1.4.3 *Si a y b son dos números enteros, entonces*

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

O más rigurosamente, si d es un máximo común divisor de a y b, entonces ab/d es un mínimo común múltiplo de a y b.

Demostración. Sean $d = \mathrm{mcd}(a,b)$, $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$ y $m = da_1b_1$. Basta con demostrar que $m = \mathrm{mcm}(a,b)$. Claramente m es múltiplo de a y de b. Sea x un múltiplo de a y de b. Entonces $\frac{x}{d}$ es múltiplo de a_1 y de b_1. Por la Proposición 1.3.6, $\frac{x}{d}$ es múltiplo de a_1b_1 y, por tanto, x es múltiplo de $da_1b_1 = m$. □

A continuación damos una aplicación de los resultados vistos hasta ahora. Se trata de la resolución de las *ecuaciones diofánticas* del tipo

$$aX + bY = c \tag{1.4.2}$$

donde a, b, c son números enteros con a y b no nulos y X e Y son incógnitas. El adjetivo "diofántica" (en honor del matemático griego Diofanto de Alejandría) significa que sólo nos interesan las soluciones de dicha ecuación que sean números enteros. Por lo tanto, una *solución* de la ecuación diofántica (1.4.2) es un par ordenado de números enteros (x,y) tal que $ax+by = c$. Comenzaremos estudiando la existencia de soluciones, para pasar después a su cálculo. En lo que sigue hacemos $d = \mathrm{mcd}(a,b)$, $a' = \frac{a}{d}$ y $b' = \frac{b}{d}$, y tomamos enteros r, s tales que $ra + sb = d$.

Proposición 1.4.4 *Con la notación anterior, la ecuación (1.4.2) tiene soluciones enteras si y sólo si $d \mid c$. En este caso, si $c' = \frac{c}{d}$, las soluciones de (1.4.2) son las mismas que las de*

$$a'X + b'Y = c'. \tag{1.4.3}$$

(Nótese que la ecuación inicial siempre tiene solución en dos casos especiales: cuando a y b son coprimos y cuando $c = 0$.)

Demostración. Si (x,y) es una solución de (1.4.2) entonces $d \mid ax+by = c$. Recíprocamente, si existe $c' \in \mathbb{Z}$ tal que $c = c'd$, entonces (rc', sc') es una solución de (1.4.2). Esto prueba el "si y sólo si", y el resto es claro pues $d \neq 0$ y por lo tanto podemos cancelarlo. □

Supongamos ahora que (1.4.2) tiene solución, y veamos cómo calcular todas sus soluciones. De hecho calcularemos las de (1.4.3), que es más sencilla. La demostración anterior nos dice que una solución "particular" es $(x_0, y_0) = (rc', sc')$, pero puede haber otras. Si (x,y) es otra solución de (1.4.3) entonces, restando las igualdades $a'x + b'y = c'$ y $a'x_0 + b'y_0 = c'$, se obtiene

$$a'(x - x_0) + b'(y - y_0) = 0. \tag{1.4.4}$$

Esto implica que b' divide a $a'(x - x_0)$, y como $\mathrm{mcd}(a', b') = 1$ (Proposición 1.3.6) deducimos que b' divide a $x - x_0$, y por lo tanto existe $\lambda \in \mathbb{Z}$ tal que $x - x_0 = \lambda b'$. Sustituyendo en (1.4.4), cancelando b' y despejando deducimos que $y - y_0 = -\lambda a'$, de modo que

$$(x,y) = (x_0 + \lambda b', y_0 - \lambda a'). \tag{1.4.5}$$

Como es inmediato comprobar que todos los pares de esa forma (con $\lambda \in \mathbb{Z}$) son soluciones de (1.4.3), deducimos que estas son todas las soluciones de nuestra ecuación.

En resumen, para resolver la ecuación diofántica (1.4.2) procedemos de la siguiente forma (el lector puede estudiar cómo se simplifican los pasos en los dos casos especiales $\mathrm{mcd}(a,b) = 1$ ó $c = 0$):

1. Calculamos $d = \mathrm{mcd}(a,b)$, por ejemplo usando el Algoritmo de Euclides.

2. Si d no divide a c, deducimos que la ecuación no tiene solución y acabamos.

3. Si d divide a c, calculamos una solución particular como sigue: Ponemos $c' = \frac{c}{d}$ y buscamos, usando el Algoritmo de Euclides, enteros r, s tales que $ar + bs = d$; entonces $(x_0, y_0) = (rc', sc')$ es una solución de (1.4.2).

4. Si $a' = \frac{a}{d}$ y $b' = \frac{b}{d}$, las soluciones de (1.4.2) son entonces todos los pares $(x, y) = (x_0 + \lambda b', y_0 - \lambda a')$, donde λ es un entero arbitrario.

Ejemplos 1.4.5 *Ecuaciones Diofánticas.*

1. Considérese la ecuación diofántica $18X + 15Y = 14$. En este caso, como $\mathrm{mcd}(18, 15) = 3$ no divide a 14, concluimos que la ecuación no tiene solución.

2. Considérese la ecuación diofántica $1717X + 2121Y = 0$, que tiene al menos la solución trivial $(X_0, Y_0) = (0, 0)$. Para calcular el resto de soluciones, dividimos la ecuación inicial por $\mathrm{mcd}(1717, 2121) = 101$ y obtenemos la ecuación equivalente $17X + 21Y = 0$. Como sus coeficientes son coprimos, la solución general de la ecuación es

$$(X, Y) = (21\lambda,\ -17\lambda) \qquad (\lambda \in \mathbb{Z}).$$

3. Considérese ahora la ecuación diofántica $100X + 35Y = 20$. En este caso, como $\mathrm{mcd}(100, 35) = 5$ divide a 20, sabemos que hay soluciones, y que éstas son las mismas que las de la ecuación $20X + 7Y = 4$. Los coeficientes de ésta, 20 y 7, son coprimos, y una identidad de Bezout para ellos es $20 \cdot (-1) + 7 \cdot 3 = 1$. Así, $(X_0, Y_0) = (-4, 12)$ es una solución particular. Finalmente, la solución general es

$$(X, Y) = (-4 + 7\lambda,\ 12 - 20\lambda) \qquad (\lambda \in \mathbb{Z}).$$

1.5 El Teorema Fundamental de la Aritmética

En esta sección vamos a demostrar el Teorema Fundamental de la Aritmética que asegura que todo entero se puede escribir de forma esencialmente única como producto de números primos. Por supuesto tenemos que empezar definiendo qué significa ser primo. Si a es un entero, entonces 1, -1, a y $-a$ son divisores de a.

Proposición 1.5.1 *Las siguientes condiciones son equivalentes para un entero p distinto de 0, 1 y -1.*

1. *Los únicos divisores de p son 1, -1, p y $-p$.*

2. *Si a y b son enteros tales que $p = ab$, entonces $a = \pm 1$ ó $b = \pm 1$.*

3. *Si I es un ideal de $\mathbb{Z}$ tal que $(p) \subseteq I$, entonces $I = (p)$ ó $I = \mathbb{Z}$.*

4. *Si a y b son enteros tales que $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.*

5. *Si a y b son enteros que no son múltiplos de p, entonces ab tampoco es múltiplo de p.*

Demostración. La equivalencia entre 1 y 2 es evidente. También es evidente que las condiciones 4 y 5 son equivalentes. La equivalencia entre 1 y 3 es una consecuencia inmediata del Teorema 1.2.11, la Proposición 1.2.8 y el Ejercicio 1.2.9.

1 implica 4. Supongamos que p satisface 1 y sean a y b enteros tales que $p \mid ab$. Si p no divide a a entonces a y p no tienen más divisores comunes que ± 1 y por lo tanto son coprimos; entonces $p \mid b$ por la Proposición 1.3.6.

4 implica 1. Supongamos que p satisface 4 y sea a un divisor de p. Si $p = ab$ entonces $p \mid a$ ó $p \mid b$. En el primer caso $(p) = (a)$, y del Ejercicio 1.2.10 se deduce que $a = \pm p$. En el segundo caso $b = pt$ para cierto entero t; entonces $1 = ta$ y del Ejercicio 1.2.9 se deduce que $a = \pm 1$. □

Definición 1.5.2 *Un número entero p se dice* primo *si es distinto de 0, 1 y -1 y satisface las condiciones de la Proposición 1.5.1.*

Ejercicio 1.5.3 *Si p es un entero primo y $p \mid a_1 \cdots a_n$ (para ciertos enteros $a_1, \ldots, a_n$), demostrar que p divide a a_i para cierto índice i.*

Teorema 1.5.4 (Teorema Fundamental de la Aritmética) *Sea a un número entero diferente de 0 y ± 1. Entonces:*

1. *a es producto de números primos.*
2. *Si $a = p_1 \cdots p_n = q_1 \cdots q_m$, con $p_1, \ldots, p_n, q_1, \ldots, q_m$ primos, entonces $n = m$ y podemos reordenar los q_i de modo que se tenga $q_i = \pm p_i$ para cada índice i.*

Demostración. Para demostrar 1, podemos suponer que $a \geq 2$ (¿por qué?). Por reducción al absurdo suponemos que a es el menor número natural mayor que 1 que no es producto de primos. Entonces a no puede ser primo, y por tanto $a = bc$ para dos enteros b y c, ambos diferentes de 1 y -1. Cambiando el signo si hace falta podemos suponer que b y c son números positivos y por tanto son ambos estrictamente menores que a. Por la minimalidad de a, se tiene que tanto b como c son producto de números primos. Por tanto a es producto de números primos, lo que induce una contradicción. Esto prueba 1.

Supongamos que $a = p_1 \cdots p_n = q_1 \cdots q_m$, como en 2. Podemos suponer que $n \leq m$. Razonamos por inducción sobre n. Si $n = 1$, entonces a es primo y, por tanto, todos los q_i menos uno son iguales a 1 ó -1. Como ninguno de los q_i puede ser 1 ni -1, se deduce que $m = 1$ y $p_1 = q_1$. Supongamos que el resultado es cierto para menos de n primos p_i. Entonces p_n divide a $a = q_1 \cdots q_m$. Como p_n es primo, divide a algún q_i, y reordenando los q_i si es necesario podemos suponer que p_n divide a q_m. Como q_m es primo, se tiene que $q_m = \pm p_n$, y por tanto $\frac{a}{p_n} = p_1 \cdots p_{n-1} = q_1 \ldots (\pm q_{m-1})$. Por hipótesis de inducción se tiene $n - 1 = m - 1$ (luego $n = m$) y podemos reordenar los q_i de manera que se tenga $q_i = \pm p_i$ para todo $i = 1, 2, \ldots, n-1$, y por supuesto también para $i = n$. □

Ejercicio 1.5.5 *Dados enteros a y b, demostrar que:*

1. *Si $|b| > 1$ entonces existe un entero primo p que divide a b.*
2. *a y b son coprimos si y sólo si no tienen ningún divisor primo común (es decir, si no existe ningún entero primo p tal que $p \mid a$ y $p \mid b$.*

Sea a un número entero no nulo. Una *factorización prima* de a es una expresión del tipo

$$a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n} \tag{1.5.6}$$

donde $n \geq 0$, los p_i son primos positivos distintos, y los exponentes α_i son enteros no negativos (cuando $n = 0$ se obtiene un "producto vacío" que, por convenio, vale 1). Obsérvese que la definición permite la aparición de exponentes nulos; es decir, de "primos ficticios" en la descomposición de a; si esto no ocurre (si los α_i son positivos) decimos que (1.5.6) es una *factorización prima irredundante* de a. Con esta terminología, el Teorema Fundamental de la Aritmética puede reenunciarse como sigue:

Teorema 1.5.6 (Teorema Fundamental de la Aritmética) *Todo entero no nulo tiene una factorización prima irredundante que es única salvo el orden.*

El exponente α_i de la expresión (1.5.6) se llama *multiplicidad* de p_i (ó de $-p_i$) en a. Claramente, un primo p divide a a precisamente si la multiplicidad de p en a no es 0. Más generalmente tenemos el siguiente criterio de divisibilidad.

Ejercicio 1.5.7 *Sean a y b dos números enteros. Demostrar que a divide a b precisamente si para todo primo p la multiplicidad de p en a es menor o igual que la multiplicidad de p en b.*

De donde se deduce fácilmente:

Ejercicio 1.5.8 *Sean $a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ y $b = \pm p_1^{\beta_1} \cdots p_n^{\beta_n}$ factorizaciones primas de los números enteros a y b (siempre podemos encontrar dos factorizaciones en las que aparecen los mismos primos, añadiendo con exponente 0 los que sean necesarios). Demostrar que*

$$\mathrm{mcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_n^{\min(\alpha_n,\beta_n)} \quad y \quad \mathrm{mcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdots p_n^{\max(\alpha_n,\beta_n)}.$$

Una consecuencia elemental pero importante del Teorema Fundamental de la Aritmética es que cada entero diferente de 0 y de ± 1 tiene (al menos) un divisor primo. Esto nos permite demostrar el siguiente Teorema de Euclides:

Teorema 1.5.9 (Euclides) *El conjunto de enteros primos es infinito.*

Demostración. Supongamos por reducción al absurdo que el conjunto de enteros primos es finito y sean $p_1, \ldots, p_n$ todos los primos positivos. Sea $a = p_1 \cdots p_n + 1$. Por el Ejercicio 1.5.5, a es divisible por algún primo positivo, que debe ser uno de los p_i. Entonces p_i divide a $a - p_1 \cdots p_n = 1$, de lo que se deriva una contradicción. □

Terminamos esta sección con una consecuencia del Teorema Fundamental de la Aritmética de la que haremos uso más adelante. En ella usaremos el concepto de número racional, que el lector conocerá al menos de forma intuitiva. De forma natural, es posible construir los números racionales de forma rigurosa a partir de los números enteros. Veremos una construcción más general en la Sección 2.9.

Proposición 1.5.10 *Si a es un entero que no es un cuadrado de un número entero (es decir, la ecuación $a = x^2$ no tiene ninguna solución entera), entonces tampoco es el cuadrado de un número racional (es decir, la ecuación $a = x^2$ no tiene ninguna solución racional).*

Demostración. Vamos a probar que, si $0 \neq a \in \mathbb{Z}$ es el cuadrado de un número racional, entonces es el cuadrado de un número entero, lo que obviamente equivale al enunciado. Supongamos pues que existen enteros no nulos b y c tales que $a = (b/c)^2$, o sea, $ac^2 = b^2$. Sabemos que existen enteros primos $p_1, \ldots, p_r$ distintos dos a dos y enteros no negativos $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r, \gamma_1, \ldots, \gamma_r$ tales que

$$a = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \qquad b = \pm p_1^{\beta_1} \cdots p_r^{\beta_r} \qquad \text{y} \qquad c = \pm p_1^{\gamma_1} \cdots p_r^{\gamma_r}.$$

La unicidad del Teorema Fundamental de la Aritmética aplicada a la igualdad $ac^2 = b^2$ nos dice que, para cada $i = 1, \ldots, r$, se tiene $\alpha_i + 2\gamma_i = 2\beta_i$, de donde $2(\beta_i - \gamma_i) = \alpha_i \geq 0$ y por tanto $\beta_i \geq \gamma_i$. Esto implica que c divide a b y en consecuencia a es el cuadrado del número entero b/c. □

1.6 Congruencias

Dados tres números enteros a, b y n, la expresión $a \equiv b \bmod n$ se lee "a es *congruente* con b módulo n" y significa $n \mid b - a$. En otras palabras

$$a \equiv b \bmod n \text{ precisamente si } b - a \in (n).$$

Dejaremos que el lector demuestre las propiedades más elementales de la relación de congruencia.

Ejercicio 1.6.1 *Demostrar que se verifican la siguientes propiedades (todas las variables representan números enteros):*

1. $a \equiv a \bmod n$.
2. *Si* $a \equiv b \bmod n$, *entonces* $b \equiv a \bmod n$.
3. *Si* $a \equiv b \bmod n$ *y* $b \equiv c \bmod n$, *entonces* $a \equiv c \bmod n$.
4. $a \equiv b \bmod 0$ *precisamente si* $a = b$.
5. $a \equiv b \bmod 1$ *para cualquier par de enteros* a, b.
6. $a \equiv b \bmod n$ *precisamente si* $a \equiv b \bmod (-n)$.
7. $a \equiv 0 \bmod n$ *precisamente si* $n \mid a$.
8. *Si* r *es el resto de dividir* a *entre* n, *entonces* $a \equiv r \bmod n$.

9. *Sea $n \neq 0$. Entonces $a \equiv b \bmod n$ si y sólo si a y b dan el mismo resto al dividirlos entre n.*

10. *Si $a \equiv b \bmod n$ y $c \equiv d \bmod n$, entonces $a + c \equiv b + d \bmod n$ y $ac \equiv bd \bmod n$.*

11. *Si $a \equiv b \bmod n$ y $m \mid n$, entonces $a \equiv b \bmod m$.*

12. *Las dos congruencias $a \equiv b \bmod n$ y $a \equiv b \bmod m$ equivalen a la congruencia $a \equiv b \bmod t$, donde $t = \text{mcm}(n, m)$.*

Fijemos un entero n. Las tres primeras propiedades del Ejercicio 1.6.1 muestran que la relación binaria "ser congruente módulo n" es una relación de equivalencia. La propiedad 6 muestra que n y $-n$ definen la misma relación de equivalencia, y por lo tanto no perdemos generalidad si suponemos que n no es negativo. Esta relación induce una partición de $\mathbb{Z}$ en clases de equivalencia. Denotaremos con $[a]_n$ (ó con $[a]$, si n está claro por el contexto) la clase de equivalencia que contiene a a. O sea

$$\begin{aligned} [a]_n &= \{b \in \mathbb{Z} : a \equiv b \bmod n\} \\ &= \{b \in \mathbb{Z} : n \mid b - a\} \\ &= \{a + tn : t \in \mathbb{Z}\}; \end{aligned}$$

En vista de esta última expresión, a veces se escribe $a + (n)$ en vez de $[a]_n$. El conjunto de las clases de equivalencia se denota $\mathbb{Z}/(n)$ ó $\mathbb{Z}_n$, y en él definimos una suma y un producto mediante las reglas:

$$[a] + [b] = [a + b] \qquad \text{y} \qquad [a] \cdot [b] = [ab].$$

Observación 1.6.2 Es conveniente observar que para sumar (o multiplicar) dos elementos A y B de $\mathbb{Z}_n$ hacemos lo siguiente:

1. Elegimos $a \in A$ y $b \in B$.
2. Calculamos $a + b$ (ó ab).
3. Definimos $A + B$ (ó AB) como la clase de equivalencia de $a + b$ (ó de ab).

Hemos hecho la anterior observación para que quede claro que, en principio, el valor de la suma $A + B$ podría depender de los elementos $a \in A$ y $b \in B$ elegidos. Es decir, si $a, a' \in A$ y $b, b' \in B$, entonces, en principio, podría ocurrir que $a + b$ y $a' + b'$ no estuvieran en la misma clase y, por tanto, $[a + b]$ y $[a' + b']$ serían distintos. En tal caso la definición de $A + B$ que hemos dado sería ambigua. Las mismas observaciones podrían hacerse sobre la definición del producto. Sin embargo, la propiedad 10 del Ejercicio 1.6.1 nos muestra que esto no ocurre, con lo que podemos garantizar que la suma y el producto de $\mathbb{Z}_n$ *están bien definidas*.

Obsérvese que si $n = 0$, entonces cada clase de equivalencia tiene un único elemento. Por tanto, podemos identificar $\mathbb{Z}_0$ con $\mathbb{Z}$ y cada $a \in \mathbb{Z}$ con $[a]_0$.

Supongamos que $n > 0$. Por las propiedades 8 y 9 del Ejercicio 1.6.1, cada número entero está en una de las siguientes clases de equivalencia: $[0], [1], \ldots, [n-1]$; y cada dos de estas clases de equivalencia son diferentes (¿por qué?). Luego $\mathbb{Z}_n$ tiene n elementos y

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

Casi todas las propiedades de la suma y el producto de números enteros también se verifican en $\mathbb{Z}_n$:

Ejercicio 1.6.3 *Sea n un número entero. Demostrar:*

1. Asociativa*: Dados $r, s, t \in \mathbb{Z}_n$, se tiene $r + (s + t) = (r + s) + t$ y $r(st) = (rs)t$.*
2. Conmutativa*: Dados $r, s \in \mathbb{Z}_n$, se tiene $r + s = s + r$ y $rs = sr$.*
3. Distributiva*: Dados $r, s, t \in \mathbb{Z}_n$, se tiene $r(s + t) = rs + rt$.*
4. Neutro*: Para todo $r \in \mathbb{Z}_n$ se verifican $r + [0] = r$ y $r[1] = r$. Además $[0]$ y $[1]$ son los únicos elementos de $\mathbb{Z}_n$ que satisfacen esta propiedad.*
5. Opuesto*: Para todo $a \in \mathbb{Z}$, $[a] + [-a] = [0]$. Además, $[-a]$ es el único elemento de $\mathbb{Z}_n$ que verifica esta propiedad.*

Sin embargo, en general, la propiedad de regularidad no se verifica en $\mathbb{Z}_n$. Por ejemplo $[2]_4[2]_4 = [0]_4$.

Se dice que $x \in \mathbb{Z}_n$ es un *divisor de cero*, o que es *singular*, si existe un $y \neq [0]$, tal que $xy = [0]$. En caso contrario (es decir, si $xy = [0]$ implica $y = [0]$) decimos que x es *regular*. Se dice que x es *invertible* si existe $y \in \mathbb{Z}_n$ tal que $xy = [1]$.

Ejercicio 1.6.4 *Demostrar que si un elemento x de $\mathbb{Z}_n$ es invertible, entonces existe un único $y \in \mathbb{Z}_n$ tal que $xy = [1]_n$. Dicho elemento se llama* inverso *de x y se denota x^{-1}.*

Las definiciones anteriores pueden aplicarse a los elementos de $\mathbb{Z}$, y en este caso sabemos que 0 es el único divisor de cero y que los únicos elementos invertibles son 1 y -1. En particular, en $\mathbb{Z}$ hay elementos regulares que no son invertibles (cualquiera distinto de 0 y de ± 1). Esto no ocurre en $\mathbb{Z}_n$ (cuando $n \neq 0$), como muestra la siguiente proposición.

Proposición 1.6.5 *Sea $0 \neq n \in \mathbb{Z}$. Las siguientes condiciones son equivalentes para todo $a \in \mathbb{Z}$.*

1. *$[a]_n$ es invertible.*
2. *$[a]_n$ es* cancelable*; es decir, si $[a]_n y = [a]_n z$ con $y, z \in \mathbb{Z}_n$ entonces $y = z$.*
3. *$[a]_n$ es regular.*
4. *$\mathrm{mcd}(a, n) = 1$.*

Demostración. Pongamos $x = [a]_n$, y en general $[r] = [r]_n$.

1 implica 2. Si x es invertible y se verifica $xy = xz$ entonces, multiplicando ambos miembros por x^{-1}, deducimos que $y = z$.

2 implica 3. Si $xy = 0$ entonces $xy = x[0]$, y cancelando x deducimos que $y = [0]$.

3 implica 4. Veamos que si un entero d divide a a y a n entonces $d \mid 1$. Poniendo $a' = \frac{a}{d}$ y $n' = \frac{n}{d}$ tenemos

$$x[n'] = [an'] = [a'dn'] = [a'n] = [0],$$

y entonces por hipótesis $[n'] = [0]$; es decir, $n'd = n \mid n'$ y por lo tanto $d \mid 1$.

4 implica 1. Supongamos ahora que a y n son coprimos. Por el Lema de Bezout existen enteros r, s tales que $ra + sn = 1$, y entonces $ra \equiv 1 \bmod n$, o sea $[r][a] = 1$, por lo que $[a]$ es invertible en $\mathbb{Z}_n$. □

La demostración de la última implicación nos dice cómo se calcula en la práctica un inverso de $[a]$ en $\mathbb{Z}_n$ (cuando existe): basta con encontrar una identidad de Bezout $ra + sn = 1$, y entonces $[r] = [a]^{-1}$.

Ejemplo 1.6.6 *Inversos en $\mathbb{Z}_n$.*

Consideremos el elemento $[7]$ en $\mathbb{Z}_{26}$. Aplicando el Algoritmo de Euclides a 7 y 26 obtenemos la tabla:

26	7	5	2	1	0
	3	1	2	2	

que nos dice que $\mathrm{mcd}(7, 26) = 1$; por lo tanto $[7]$ es invertible, y como además

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 5 \cdot 1) \\ &= 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (26 - 3 \cdot 7) - 2 \cdot 7 \\ &= 3 \cdot 26 - 11 \cdot 7, \end{aligned}$$

deducimos que $[7]^{-1} = [-11] = [15]$ en $\mathbb{Z}_{26}$.

Cuando n es pequeño, hay una forma rudimentaria de calcular el inverso de $[a]$ en $\mathbb{Z}_n$ que suele ser más rápida que el Algoritmo de Euclides. Se trata simplemente de ir multiplicando $[a]$ por $[1], [2], \ldots$ hasta que el producto valga $[1]$. Por cierto, el inverso de $[n-1]$ es precisamente $[n-1]$ (¿por qué?).

1.7 Ecuaciones de congruencias; Teorema Chino de los Restos

Una *ecuación lineal de congruencias* es una ecuación del tipo

$$aX \equiv c \bmod n \tag{1.7.7}$$

con $n \neq 0$. Una *solución* de (1.7.7) es un número entero x tal que $ax \equiv c \bmod n$. La ecuación (1.7.7) es equivalente a la ecuación

$$[a]_n X = [c]_n. \tag{1.7.8}$$

Esto quiere decir que $x \in \mathbb{Z}$ es una solución de la ecuación (1.7.7) precisamente si $[x]_n$ es una solución de la ecuación (1.7.8).

Vamos a ver cómo resolver ecuaciones lineales de congruencias. Empezaremos considerando el caso más sencillo, que se da cuando $[a]_n$ es invertible. Entonces la única solución de la ecuación (1.7.8) es $[a]_n^{-1}[c]_n$ (es decir, se obtiene "dividiendo por $[a]_n$"). En otras palabras, si $[a]_n^{-1}[c]_n = [b]_n$, entonces las soluciones de la ecuación (1.7.7) son los números enteros de la forma

$$b + \lambda n \quad (\lambda \in \mathbb{Z}).$$

Por ejemplo, para resolver la ecuación

$$7X \equiv 3 \bmod 26$$

observamos que $[7] = [7]_{26}$ es invertible y su inverso es $[15] = [15]_{26}$. Como $[15][3] = [45] = [19]$, las soluciones de la ecuación son los números enteros de la forma

$$19 + 26\lambda \quad (\lambda \in \mathbb{Z}).$$

Obsérvese que, en este caso, todas las soluciones son congruentes (entre sí) módulo n. Este hecho se suele expresar diciendo que (1.7.7) *tiene solución única módulo* n.

El caso general ($[a]_n$ no es necesariamente invertible) se reduce al anterior gracias al siguiente resultado (compárese con la Proposición 1.4.4).

Proposición 1.7.1 *Sean a y n enteros con $n \neq 0$, y sean $d = \mathrm{mcd}(a, n)$, $a' = \frac{a}{d}$ y $n' = \frac{n}{d}$. Entonces la ecuación (1.7.7) tiene solución si y sólo si $d \mid c$. En este caso, si $c' = \frac{c}{d}$, las soluciones de (1.7.7) son las mismas que las de*

$$a'X \equiv c' \bmod n', \tag{1.7.9}$$

y por tanto (1.7.7) tiene solución única módulo n'.

Demostración. El "si y sólo si" se tiene porque ambas condiciones equivalen a la existencia de enteros x, y tales que $c = ax + ny$. El resto es claro pues podemos cancelar $d \neq 0$. □

En resumen, para resolver la ecuación (1.7.7) seguiremos los siguientes pasos, en los que mantenemos la notación anterior:

1. Calculamos $d = \mathrm{mcd}(a, n)$.

2. Si d no divide a c, concluimos que la ecuación no tiene solución y acabamos.

3. Si d divide a c entonces las soluciones de (1.7.7) son las de (1.7.9); es decir, las de la forma

$$b' + \lambda n' \qquad (\lambda \in \mathbb{Z})$$

con $[b']_{n'} = [a']_{n'}^{-1}[c']_{n'}$.

Ejemplo 1.7.2 *Ecuación lineal de congruencias.*
Vamos a resolver la ecuación lineal de congruencias

$$6x \equiv 9 \bmod 15$$

Como $\mathrm{mcd}(6,15) = 3$ divide a 9, la ecuación tiene solución y es equivalente a la ecuación

$$2x \equiv 3 \bmod 5.$$

Como $[2]_5^{-1} = [3]_5$ y $[3]_5[3]_5 = [4]_5$, las soluciones de esta ecuación son de la forma

$$4 + 5\lambda \qquad (\lambda \in \mathbb{Z}).$$

En la segunda parte de esta sección vamos a ver cómo se resuelve un sistema de ecuaciones lineales de congruencias del tipo

$$\begin{array}{rcll} X & \equiv & c_1 & \bmod n_1 \\ X & \equiv & c_2 & \bmod n_2 \\ & \vdots & & \\ X & \equiv & c_k & \bmod n_k \end{array} \tag{1.7.10}$$

donde los n_i son *coprimos dos a dos*; es decir, $\mathrm{mcd}(n_i, n_j) = 1$ para todo $i \neq j$. Comencemos con el siguiente lema:

Lema 1.7.3 *Si los enteros $n_1, \ldots, n_k$ son coprimos dos a dos, entonces su mínimo común múltiplo coincide con su producto $n = n_1 \cdots n_k$.*

Demostración. Cuando $k = 2$, el resultado es una consecuencia inmediata de la Proposición 1.4.3, y el caso general se demuestra fácilmente por inducción usando la "asociatividad del mínimo común múltiplo", que a su vez es consecuencia de la Proposición 1.3.3. □

Teorema 1.7.4 (Teorema Chino de los Restos) *Sean $n_1, \ldots, n_k$ enteros coprimos dos a dos, y sea $n = n_1 \cdots n_k$. Entonces la aplicación*

$$\begin{array}{ccc} \mathbb{Z}_n & \xrightarrow{f} & \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \\ [x]_n & \mapsto & ([x]_{n_1}, \ldots, [x]_{n_k}) \end{array} \tag{1.7.11}$$

es biyectiva. (De hecho, usando la terminología que introduciremos más tarde, esta aplicación es un isomorfismo de anillos*; ver el Teorema 2.7.10.)*

Demostración. Primero hay que asegurarse de que f está bien definida (su valor no depende del representante de $[x]_n$ que tomemos; ver la Observación 1.6.2), pero eso es muy fácil y lo dejamos como ejercicio para el lector. Para ver que f es biyectiva, como los conjuntos $\mathbb{Z}_n$ y $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ tienen el mismo cardinal (véase el Problema 7), basta con demostrar que f es inyectiva. Sean pues $[x]_n$ e $[y]_n$ con la misma imagen por f; esto significa que $x \equiv y \bmod n_i$ para cada $i = 1, 2, \ldots, k$, de modo que $x - y$ es un múltiplo común de los n_i y por lo tanto es múltiplo de su mínimo común múltiplo, que por el lema es n; en otras palabras, $x \equiv y \bmod n$, y esto prueba que f es inyectiva. □

Aunque el teorema, tal como lo hemos enunciado, no parece tener nada que ver con sistemas de ecuaciones, una lectura atenta del mismo nos permite deducir que el sistema (1.7.10) tiene solución única módulo n cuando los n_i son coprimos dos a dos. En efecto, la suprayectividad de f se traduce en que, dados enteros arbitrarios $c_1, \ldots, c_k$, existe un entero x con $f([x]_n) = ([c_1]_{n_1}, \ldots, [c_k]_{n_k})$, y esta igualdad significa exactamente que x es una solución del sistema. Por otra parte, es claro que la inyectividad de f se traduce en la unicidad módulo n de esta solución. Por lo tanto, se tiene:

Teorema 1.7.5 *Sean $n_1, \ldots, n_k$ enteros coprimos dos a dos y sean $c_1, \ldots, c_k$ enteros arbitrarios. Entonces el sistema (1.7.10) tiene solución única módulo $n = n_1 \cdots n_k$.*

La demostración que hemos dado del Teorema Chino presenta un problema: en ella se deduce que f es suprayectiva porque es una aplicación inyectiva entre conjuntos finitos del mismo cardinal, pero dados $c_1, \ldots, c_k$ no nos dice cómo es el elemento $[x]_n$ tal que $f([x]_n) = ([c_1]_{n_1}, \ldots, [c_k]_{n_k})$. Afortunadamente, hay un método para obtener ese x. En el párrafo siguiente vemos cómo se obtiene x cuando sólo hay 2 ecuaciones, y en el ejemplo que le sigue queda claro que para sistemas con más ecuaciones basta con repetir este método.

Supongamos pues que $k = 2$, y sean r_1, r_2 enteros tales que $r_1 n_1 + r_2 n_2 = 1$; entonces se tiene

$$r_1 n_1 \equiv 0 \bmod n_1, \quad r_2 n_2 \equiv 1 \bmod n_1, \quad r_1 n_1 \equiv 1 \bmod n_2 \quad \text{y} \quad r_2 n_2 \equiv 0 \bmod n_2,$$

de donde se deduce que el entero $x = c_2 r_1 n_1 + c_1 r_2 n_2$ verifica

$$x \equiv c_1 \bmod n_1, \quad x \equiv c_2 \bmod n_2,$$

y por tanto x es la solución buscada.

Ejemplo 1.7.6 *Sistemas de ecuaciones lineales de congruencias.*
Vamos a resolver el sistema de ecuaciones lineales de congruencias

$$\begin{array}{rcll} x & \equiv & 1 & \bmod 3 \\ 2x & \equiv & 3 & \bmod 7 \\ 3x & \equiv & 12 & \bmod 15 \end{array}$$

En primer lugar convertimos cada ecuación en otra ecuación equivalente, en la que el coeficiente de la incógnita sea 1 en todas las ecuaciones y en la que los módulos sean coprimos dos a dos (en el sistema dado, 3 y 15 no son coprimos). A la primera ecuación no hay que hacerle nada. Como $[2]_7$ es invertible y $[2]_7^{-1} = [4]$, la segunda ecuación es equivalente a $x \equiv 5 \bmod 7$. Esto no vale para la tercera ecuación, pues $[3]_{15}$ no es invertible. Sin embargo esta ecuación es equivalente a $x \equiv 4 \bmod 5$ por la Proposición 1.7.1. Por tanto el sistema original es equivalente a

$$\begin{array}{rcll} x & \equiv & 1 & \bmod 3 \\ x & \equiv & 5 & \bmod 7 \\ x & \equiv & 4 & \bmod 5 \end{array}$$

Como $(-2)3 + 1 \cdot 7 = 1$, el párrafo anterior nos dice que podemos sustituir las dos primeras ecuaciones por la ecuación $x \equiv 5(-2)3 + 1 \cdot 1 \cdot 7 = -23 \bmod 21$, o lo que es lo mismo por $x \equiv -2 \bmod 21$. Nos queda así el sistema

$$\begin{array}{rcll} x & \equiv & -2 & \bmod 21 \\ x & \equiv & 4 & \bmod 5 \end{array}$$

Finalmente como $1 \cdot 21 + (-4)5 = 1$, nos quedamos con la única ecuación

$$x \equiv 4 \cdot 1 \cdot 21 + (-2)(-4)5 = 124 \equiv 19 \bmod 105.$$

Luego las soluciones del sistema son las de la forma:

$$x = 19 + 105t \qquad (t \in \mathbb{Z})$$

(¡compruébalo!).

1.8 Teoremas de Euler y Fermat

Denotaremos por $\mathbb{Z}_n^*$ al conjunto de los elementos invertibles de $\mathbb{Z}_n$. El cardinal de $\mathbb{Z}_n^*$ se denota por $\phi(n)$, y la aplicación $\phi : \mathbb{N} \to \mathbb{N}$ se llama *función de Euler*. Para algunos valores bajos de n, el lector puede dar una descripción explícita de $\mathbb{Z}_n^*$ (usando la Proposición 1.6.5) y deducir el valor de $\phi(n)$. Por otra parte, es elemental ver que, si p es un entero primo positivo, entonces $\phi(p) = p - 1$.

La función de Euler es útil a la hora de hacer cálculos con congruencias en los que aparecen potencias, como veremos en los ejemplos que siguen. El resultado fundamental para esto es el siguiente:

Teorema 1.8.1 (Teorema de Euler) *Si* $\mcd(a,n)=1$, *entonces* $a^{\phi(n)}\equiv 1 \bmod n$.

Demostración. Sean $[x_1],[x_2],\dots,[x_k]$ todos los elementos invertibles de $\mathbb{Z}_n$, de modo que $k=\phi(n)$ y $\mathbb{Z}_n^*=\{[x_1],[x_2],\dots,[x_k]\}$. Como $[a]$ es invertible, los elementos $[a][x_1],[a][x_2],\dots,[a][x_k]$ están en $\mathbb{Z}_n^*$ (por las Proposiciones 1.6.5 y 1.3.6) y son distintos entre sí (porque $[a]$ es cancelable). Por lo tanto, $\mathbb{Z}_n^*=\{[a][x_1],[a][x_2],\dots,[a][x_k]\}$, y en consecuencia se tiene

$$[x_1][x_2]\cdots[x_k]=[a]\cdot[x_1]\cdot[a]\cdot[x_1]\cdots[a]\cdot[x_k].$$

Ahora basta con cancelar los $[x_i]$ para obtener el resultado deseado. □

Un caso particular del Teorema de Euler (1.8.1) es el siguiente:

Corolario 1.8.2 (Teorema Pequeño de Fermat) *Si* p *es un número primo y* $p\nmid a$, *entonces*

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

Por tanto, para todo número entero x *se verifica*

$$x^p\equiv x \bmod p.$$

Estos teoremas sirven para resolver situaciones como las del siguiente ejemplo:

Ejemplos 1.8.3 *Aplicaciones de los Teoremas de Euler y Fermat.*

1. Vamos a calcular el resto que se obtiene al dividir 347^{231} entre 5, lo que equivale a encontrar un entero x entre 0 y 4 tal que $x\equiv 347^{231} \bmod 5$. Por una parte tenemos $347\equiv 2 \bmod 5$, por otra el Teorema de Fermat nos dice que $2^4\equiv 1 \bmod 5$, y por último dividiendo entre 4 tenemos $231=4\cdot 57+3$. Juntando todo esto deducimos que

$$347^{231}\equiv 2^{4\cdot 57+3}\equiv (2^4)^{57}2^3\equiv 1^{57}2^3\equiv 8\equiv 3 \bmod 5,$$

   así que el resto buscado es 3.

2. Para calcular el resto de dividir 23^{70} por 18 procedemos de modo similar: como $\phi(18)=6$ (¡compruébalo!), el Teorema de Euler nos dice que $23^6\equiv 1 \bmod 18$, y como $70=6\cdot 11+4$ obtenemos

$$23^{70}\equiv 5^{6\cdot 11+4}\equiv (5^6)^{11}5^4\equiv 1^{11}5^4\equiv 625\equiv 13 \bmod 18,$$

   así que el resto buscado es 13.

En el apartado 2 del ejemplo anterior hemos necesitado el valor de $\phi(18)$, que se puede calcular de modo directo. Para valores grandes de n es interesante encontrar un modo rápido de calcular $\phi(n)$, y eso es lo que hacemos en el último resultado de este capítulo.

Proposición 1.8.4 *(Cálculo de la función de Euler)*

1. *Si* p *es un entero primo positivo y* α *es un entero positivo, entonces* $\phi(p^\alpha)=p^{\alpha-1}(p-1)$.
2. *Si* n *y* m *son enteros coprimos entonces* $\phi(nm)=\phi(n)\phi(m)$.
3. *Si* $n=\pm p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ *es una factorización prima irredundante del entero* n, *entonces*

$$\phi(n)=p_1^{\alpha_1-1}\cdots p_r^{\alpha_r-1}(p_1-1)\cdots(p_r-1)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

Demostración. 1. Podemos describir $\mathbb{Z}_{p^\alpha}^*$ eliminando en $\mathbb{Z}_{p^\alpha}=\{[1],[2],\dots,[p^\alpha]\}$ los elementos no invertibles, que son los $[a]$ en los que a no es coprimo con p^α; como esto ocurre si y sólo si a es múltiplo de p, estamos eliminando exactamente $p^{\alpha-1}$ elementos (uno de cada p), por lo que en $\mathbb{Z}_{p^\alpha}^*$ quedan exactamente $p^\alpha-p^{\alpha-1}=p^{\alpha-1}(p-1)$ elementos, y esto es lo que queríamos ver.

2. Si n y m son coprimos, el Teorema Chino nos dice que la aplicación $f:\mathbb{Z}_{nm}\to\mathbb{Z}_n\times\mathbb{Z}_m$ dada por $f([x]_{nm})=([x]_n,[x]_m)$ es una biyección. Usando la Proposición 1.3.6 es fácil ver que $[x]_{nm}$ está en $\mathbb{Z}_{nm}^*$ si y sólo si su imagen por f está en $\mathbb{Z}_n^*\times\mathbb{Z}_m^*$, por lo que f se restringe a una biyección entre esos conjuntos. Por lo tanto $\mathbb{Z}_{nm}^*$ y $\mathbb{Z}_n^*\times\mathbb{Z}_m^*$ tienen el mismo cardinal, y ahora el resultado es claro.

Ahora 3 se demuestra fácilmente por inducción a partir de los apartados anteriores. □

1.9 Apéndice: criptografía de clave pública

Algunas de las ideas que hemos desarrollado en este capítulo admiten una interesante aplicación a la criptografía que, obviando algunos detalles técnicos, desarrollaremos en este apéndice. El "sistema criptográfico de clave pública" que vamos a describir es el más utilizado en la actualidad, y recibe el nombre de RSA por las iniciales de sus autores: Rivest, Shamir y Adleman. El sistema funciona así:

Nosotros queremos que cualquier usuario del sistema pueda cifrar y enviarnos un mensaje, con un procedimiento que ha de ser público. Y queremos ser los únicos capaces de descifrarlo, incluso en el caso de que, en el proceso de envío del mensaje, éste sea interceptado por alguien. Obviamente, el procedimiento de descifrado debe tener alguna diferencia con el de cifrado. Hacemos lo siguiente:

Elegimos dos números primos distintos p y q que sean "grandes", y calculamos $n = pq$ y $\phi(n) = (p-1)(q-1)$. Elegimos entonces un entero k coprimo con $\phi(n)$ y obtenemos una identidad de Bezout $1 = kr + \phi(n)s$. Hacemos públicos los valores de n y de k y reservamos en secreto el resto (de hecho, basta con conservar el valor de r). En lo que sigue trabajaremos en $\mathbb{Z}_n$, y asumiremos que las igualdades son módulo n y que cada elemento viene dado por su representante en $\{0, 1, \ldots, n-1\}$.

Un mensaje puede descomponerse en bloques de un cierto número de caracteres, y cada bloque puede asociarse unívocamente a un elemento a de $\mathbb{Z}_n$. Este proceso de traducción de un mensaje a una sucesión de elementos de $\mathbb{Z}_n$ (los asociados a cada bloque), y el proceso inverso, son también públicos, de modo que podemos asumir que cada $a \in \mathbb{Z}_n$ es un mensaje claro. El problema estriba entonces en cifrar y descifrar elementos de $\mathbb{Z}_n$.

Para cifrar $a \in \mathbb{Z}_n$, simplemente se calcula $c = a^k$ (mejor dicho, el resto de la división entera de a^k por n). Por tanto, nosotros recibimos el mensaje cifrado c; vamos a ver que, para descifrarlo, basta con calcular c^r. En efecto, se trata de ver que $c^r \equiv a \bmod n$ y, por el Teorema Chino de los Restos, esto equivale a que la congruencia valga módulo p y módulo q. Comprobaremos sólo que $c^r \equiv a \bmod p$, pues el otro caso es análogo. Ahora hay dos opciones: Si $a \equiv 0 \bmod p$ entonces $c = a^k \equiv 0 \bmod p$ y el resultado es claro. En otro caso, el Teorema Pequeño de Fermat nos dice que

$$c^r = (a^k)^r = a^{kr} = a^{1-\phi(n)s} = a^{1-(p-1)(q-1)s} = a(a^{p-1})^{(1-q)s} = a1^{(1-q)s} = a,$$

como queríamos comprobar.

Los cálculos que se han indicado, especialmente las exponenciaciones, pueden ser tremendos si los enteros que intervienen son grandes. Además hay mensajes que viajan y pueden ser interceptados. Por tanto, hay que convencerse de dos cosas:

- Los cálculos son factibles. Es decir, un buen ordenador puede hacerlos en poco tiempo.
- El sistema es seguro. Es decir, si alguien intercepta $c = a^k$, no será capaz de calcular a en un tiempo razonable. El punto anterior exige que nosotros sí seamos capaces de hacer esto, y para eso usamos la clave secreta r.

En cuanto al primer punto, diremos que hay algoritmos rápidos[2] para tratar enteros grandes, que nos permiten hacer sumas, multiplicaciones y exponenciaciones en un tiempo razonable; y también es rápido el algoritmo de Euclides, que nos permite hallar identidades de Bezout.

En cuanto al segundo punto, observemos lo siguiente: Si alguien intercepta el mensaje $c = a^k$, puede tratar de descifrarlo encontrando nuestra clave secreta r, y en seguida veremos que esto es prácticamente imposible si elegimos adecuadamente los primos p y q del principio. Antes de eso comentaremos que podrían estudiarse otros métodos para obtener a conociendo $c = a^k$, pero hoy en día no se conoce ninguno. Es decir, no hay algoritmos rápidos para la extracción de raíces k-ésimas módulo n.

Volvamos pues al problema de encontrar r, el inverso de k módulo $\phi(n)$. Para ello sólo se necesita conocer $\phi(n)$, porque entonces, como k es público, el Algoritmo de Euclides proporciona r. Como el interceptor también conoce n, hemos de estar seguros de que no puede calcular $\phi(n)$ a partir de n, y por tanto no debe ser capaz de hallar la factorización prima de n. El problema es entonces este: ¿pueden encontrarse primos p y q tales que, en la práctica, sea imposible factorizar $n = pq$ sin conocer de antemano esos factores?

La respuesta es, hoy día, sí. Si se toman dos primos p y q suficientemente grandes, los mejores algoritmos de factorización tardarían siglos en hallar p y q a partir de n. Actualmente, no es difícil

[2] Ni la idea de algoritmo rápido ni la descripción de esos algoritmos son difíciles, pero se salen de los objetivos de este texto.

generar enteros primos de unas 200 cifras decimales, y los números de 400 cifras (como n) son demasiado grandes para los algoritmos de factorización actuales.

Tal vez un ejemplo sencillo ayude a comprender esto: Es fácil ver a mano que el número $p = 1.607$ es primo, pues ningún primo menor que $\sqrt{1.607} = 40'08...$ lo divide (sólo hay que probar con 12 primos). Del mismo modo, 16 divisiones sencillas son suficientes para asegurarse de que $q = 3.433$ es primo. Pero si nos dan directamente $n = 5.516.831$, tendríamos que hacer unas 400 divisiones de enteros medianamente grandes para encontrar el factor p, lo que llevaría mucho tiempo si trabajamos a mano. Esto ilustra la situación a la que nos referíamos en el párrafo anterior: si dos personas usan el mismo algoritmo y los mismos medios técnicos, una puede fabricar fácilmente un número compuesto de tal forma que a la otra le cueste mucho trabajo encontrar sus factores primos.

Terminaremos con algunos comentarios. Los dos primeros se refieren a la elección de las claves, y los restantes ponen de manifiesto otras ventajas del sistema.

- No es difícil, si se tiene un buen test de primalidad y un buen ordenador, obtener primos de unas 200 cifras: Se genera aleatoriamente un número impar m de 200 cifras y se le aplica el test sucesivamente a $m, m+2, m+4...$ (para enteros de este tamaño los mejores tests dan un resultado seguro). Por mucho que tarde en aparecer un primo, la cosa no llevará más de unos minutos.

- Los primos p y q no sólo han de ser grandes, sino que deben cumplir otras condiciones sin las cuales serían detectados por algunos tests de factorización. Por ejemplo: no deben estar muy próximos entre sí, no deben ser de ciertos tipos especiales (por ejemplo, de la forma $2^n - 1$), y el máximo común divisor de $p-1$ y $q-1$ no debe ser muy grande. Si se obtienen p y q aleatoriamente, como en el punto anterior, hay que tener muy mala suerte para que no se cumplan estos requisitos. En estos casos nos olvidamos de los primos obtenidos y repetimos el proceso.

- La clave secreta r no ha de ser compartida con el emisor, no ha de viajar, y esto hace al sistema muy seguro.

- Los mensajes cifrados pueden hacerse públicos, no hay que enviarlos a escondidas.

- Si cada usuario U del sistema hace pública su propia clave de cifrado (n_U, k_U) y conserva secreta su clave de descifrado r_U, se pueden enviar mensajes firmados. Sean V y W dos usuarios del sistema, y sea $a \in \mathbb{Z}_{n_W}$ un mensanje claro. Si V envía a W el mensaje cifrado $c = (a^{r_V})^{k_W}$, W puede descifrarlo calculando $(c^{r_W})^{k_V} = a$, y además puede estar seguro de que V es el emisor (¿por qué?).

1.10 Problemas

1. Sean $a, b, c, d \in \mathbb{Z}$. Demostrar
   (a) Si $a \leq b$ y $c \leq d$, entonces $a + c \leq b + d$.
   (b) Si $0 < a < b$ y $0 < c \leq d$, entonces $ac < bd$.
   (c) Si $a < b < 0$ y $c \leq d < 0$, entonces $bd < ac$.

2. Demostrar por inducción que se verifican las siguientes fórmulas:
   (a) (Binomio de Newton) $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.
   (b) $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.
   (c) $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

3. Demostrar que, en $\mathbb{N}$, la relación de divisibilidad verifica las propiedades reflexiva, antisimétrica y transitiva, pero no la dicotomía (en otras palabras, la relación es un *orden parcial* pero no es un *orden total*).

4. Demostrar que el Principio de Inducción y el Axioma de Buena Ordenación son equivalentes; es decir, demostrar el Axioma de Buena Ordenación a partir de los demás axiomas del conjunto de los enteros y del Principio de Inducción.

5. Decimos que un conjunto X con una relación de orden parcial está bien ordenado si todo subconjunto no vacío tiene un mínimo. Demostrar que el Axioma de Buena Ordenación es equivalente a que el conjunto $\mathbb{N}$, con la relación de orden inducida por $\mathbb{Z}$, esté bien ordenado.

6. Dado $n \in \mathbb{N}$, denotamos por $\mathbb{N}_n$ al conjunto de los enteros positivos menores o iguales que n; es decir, $\mathbb{N}_n = \{a \in \mathbb{Z} : 1 \leq a \leq n\}$ (en particular, $\mathbb{N}_0$ es el conjunto vacío). Demostrar que las siguientes condiciones son equivalentes para un conjunto A:

   (a) Para cierto $n \in \mathbb{N}$, existe una aplicación biyectiva $\mathbb{N}_n \to A$.

   (b) Para cierto $m \in \mathbb{N}$, existe una aplicación suprayectiva $\mathbb{N}_m \to A$.

   (c) Para cierto $k \in \mathbb{N}$, existe una aplicación inyectiva $A \to \mathbb{N}_k$.

   (d) Si $f : A \to A$ es una aplicación inyectiva, entonces f es suprayectiva.

   (e) Si $f : A \to A$ es una aplicación suprayectiva, entonces f es inyectiva.

   (f) Si S es un subconjunto propio de A, no existe ninguna aplicación inyectiva $A \to S$.

   (g) Si S es un subconjunto propio de A, no existe ninguna aplicación suprayectiva $S \to A$.

   (h) Si S es un subconjunto propio de A, no existe ninguna aplicación biyectiva $S \to A$.

   Un conjunto se dice que es *finito* si satisface las condiciones anteriores.

7. Demostrar que si A es un conjunto finito (ver el Problema 6), entonces el número $n \in \mathbb{N}$ para el que existe una biyección $A \to \mathbb{N}_n$ es único. Dicho número natural n se llama *cardinal* de A y lo denotaremos por $|A|$. En particular $|\emptyset| = 0$. Demostrar:

   (a) Dos conjuntos finitos tienen el mismo cardinal precisamente cuando existe una biyección entre ellos.

   (b) Dados $a, b \in \mathbb{Z}$ con $a < b$, el conjunto $A = \{x \in \mathbb{Z} : a \leq x \leq b\}$ es finito y $|A| = b - a + 1$.

   (c) Si A y B son dos conjuntos finitos, entonces $|A \times B| = |A| \cdot |B|$.

   (d) Si A es finito, entonces el conjunto $\mathcal{P}(A)$ formado por los subconjuntos de A es finito y $|\mathcal{P}(A)| = 2^{|A|}$.

8. Calcular el máximo común divisor y el mínimo común múltiplo de $a = 2689$ y $b = 4001$. Encontrar también enteros r y s tales que $\mathrm{mcd}(a, b) = ra + sb$. ¿Son únicos estos valores de r y s?

9. Demostrar que, para cualquier $n \in \mathbb{Z}$, los enteros $5n + 2$ y $12n + 5$ son coprimos.

10. Demostrar que cualesquiera dos miembros consecutivos de la *sucesión de Fibonacci*

$$1,\ 1,\ 2,\ 3,\ 5,\ 8, \ldots \qquad a_n = a_{n-1} + a_{n-2}$$

    son coprimos.

11. Sean $a, b, c \in \mathbb{Z}$ y sean $d = \mathrm{mcd}(a, b)$ y $m = \mathrm{mcm}(a, b)$. Demostrar que

$$cd = \mathrm{mcd}(ac, bc) \qquad \text{y} \qquad cm = \mathrm{mcm}(ac, bc).$$

12. Sean S y T dos conjuntos de números enteros. Demostrar que

$$\mathrm{mcd}(S \cup T) = \mathrm{mcd}(\mathrm{mcd}(S), \mathrm{mcd}(T)) \qquad \text{y} \qquad \mathrm{mcm}(S \cup T) = \mathrm{mcm}(\mathrm{mcm}(S), \mathrm{mcm}(T)).$$

13. Resolver las siguientes ecuaciones diofánticas:

   (a) $225X + 15Y = 100$.

   (b) $213X + 180Y = 300$.

   (c) $2040X - 3740Y = 1360$.

14. En una clase hay 30 alumnos que cursan dos asignaturas. Se llega al acuerdo siguiente: El que suspenda dos asignaturas pagará 3 euros; el que apruebe sólo una recibirá 2 euros y el que apruebe las dos recibirá 4 euros. ¿Cuántos alumnos han de aprobar dos, una y ninguna asignatura para que no sobre ni falte dinero? ¿Hay una única respuesta válida?

15. Un hombre compró una docena de piezas de fruta (naranjas y manzanas) por 99 pesetas. Si una manzana cuesta 3 pesetas más que una naranja y compró más manzanas que naranjas, ¿cuántas manzanas y cuántas naranjas compró?

16. Demostrar que, si S es un conjunto infinito de números enteros, entonces $\mathrm{mcm}(S) = 0$.

17. Para $a, b, c \in \mathbb{Z}$, demostrar las fórmulas

$$\mathrm{mcm}(a, \mathrm{mcd}(b,c)) = \mathrm{mcd}(\mathrm{mcm}(a,b), \mathrm{mcm}(a,c)), \qquad \mathrm{mcd}(a, \mathrm{mcm}(b,c)) = \mathrm{mcm}(\mathrm{mcd}(a,b), \mathrm{mcd}(a,c)).$$

18. Sean $a_1, \ldots, a_n$ números enteros y sean $c = a_1 \cdots a_n$, $A_i = c/a_i$, $d = \mathrm{mcd}(A_1, \ldots, A_n)$ y $m = \mathrm{mcm}(a_1, \ldots, a_n)$. Demostrar que $dm = \pm c$.

19. Demostrar que el número de divisores de un entero no nulo es finito y obtener una fórmula que proporcione el número de divisores de un número entero en función de su descomposición en producto de primos.

20. Se pide, dados los números enteros

$$a = 464200, \qquad b = 905760 \qquad \text{y} \qquad c = 336435 :$$

    (a) Hallar las factorizaciones primas irredundantes de a, b y c.

    (b) Usarlas para calcular $\mathrm{mcd}(a,b)$, $\mathrm{mcd}(a,c)$, $\mathrm{mcd}(b,c)$, $\mathrm{mcm}(a,b)$, $\mathrm{mcm}(a,c)$ y $\mathrm{mcm}(b,c)$.

    (c) Calcular el número de divisores positivos de a, b y c, y encontrar explícitamente los de c (usar el Problema 19).

21. Sean a y b dos enteros coprimos. Demostrar que ab y $a+b$ también son coprimos.

22. Sea b un número natural mayor que 1. Demostrar que para todo número natural n existe una única lista de enteros $r_0, r_1, \ldots, r_k$ tales que

$$0 \leq r_0, r_1, \ldots, r_k < b, \qquad r_k \neq 0 \qquad \text{y} \qquad n = r_0 + r_1 b + r_2 b^2 + \cdots + r_k b^k.$$

    La sucesión $r_k, \ldots, r_2, r_1, r_0$ se llama *representación de n en base b* (cuando $n = 2$ se habla de *representación binaria* y cuando $n = 10$ se habla de *representación decimal*, y si no se dice otra cosa usaremos las representaciones decimales). Como aplicación, calcular las representaciones de 69 en bases 2, 3 y 6.

23. Demostrar los criterios escolares de divisibilidad por 2, 3, 5 y 9:

    (a) Un número entero es múltiplo de 2 (respectivamente de 5) precisamente si lo es su última cifra en base decimal.

    (b) Un número entero es múltiplo de 3 (respectivamente de 9) precisamente si la suma de sus cifras en base decimal es múltiplo de 3 (respectivamente de 9).

24. Dar criterios de divisibilidad por 4, 6, 11, 13 y 101.

25. [*] Demostrar que si $a_1, \ldots, a_n$ son números enteros consecutivos, entonces n divide a exactamente uno de ellos y $n!$ divide a su producto.

26. Demostrar que un entero positivo p es primo si y sólo si p divide al coeficiente binomial $\binom{p}{i}$ para cada $i = 1, 2, \ldots, p-1$.

27. Demostrar que hay infinitos números primos positivos de la forma $4n-1$. (Indicación: Un entero positivo de esa forma ha de tener un divisor primo que también sea de esa forma.)

28. Se pide:

    (a) Si a es un número entero y p es un divisor primo impar de a^2+1, demostrar que $p \equiv 1 \bmod 4$. (Indicación: Poner $p = 2t+1$ y usar el Teorema de Fermat para ver que t es par.)

    (b) Deducir que hay infinitos números primos positivos de la forma $4n+1$. (Indicación: En caso contrario, considerar $a = q!$, donde q es el mayor de tales primos.)

    (c) ¿Por qué no sirve un argumento como el del Problema 27 para demostrar el apartado anterior?

29. Demostrar que un número primo mayor que 3 es congruente con 1 o con -1 módulo 6, y deducir que hay infinitos números primos de la forma $6n-1$.

30. Sean m y n números enteros y sea k un número natural. Demostrar que:

    (a) $n-1$ divide a n^k-1; más generalmente, $n-m$ divide a n^k-m^k.

    (b) Si k es impar, entonces $n+1$ divide a n^k+1; más generalmente, $n+m$ divide a n^k+m^k.

31. Demostrar los siguientes enunciados, donde $n \in \mathbb{N}$ (usar el Problema 30):

    (a) Si el entero[3] 2^n-1 es primo, entonces n es primo.

    (b) Si el entero[4] 2^n+1 es primo, entonces $n = 0$ ó n es una potencia de 2.

32. Para cada $n \in \mathbb{N}$, sea $F_n = 2^{2^n}+1$. Demostrar que se tiene

$$F_{n+1} = 2 + F_0 F_1 \cdots F_n,$$

    y deducir que los F_n son coprimos dos a dos y que por tanto existen infinitos enteros primos.

33. Dados $a, b \in \mathbb{Z}$ tales que $3 \mid a^2+b^2$, demostrar que $3 \mid a$ y $3 \mid b$.

34. Hallar todas las soluciones enteras de la ecuación $x^2 \equiv 1 \bmod 4$.

35. Demostrar que la ecuación $x^2+y^2 \equiv 3 \bmod 4$ no tiene soluciones enteras.

36. Demostrar que 13 divide a $4^{2n+1}+3^{n+2}$ para todo $n \in \mathbb{N}$.

37. Demostrar que 4 no divide a n^2+1 ni a n^2+2 para ningún número entero n.

38. Resolver cada una de las ecuaciones lineales de congruencias siguientes:

$3x \equiv 14 \bmod 17$	$2x-1 \equiv 1 \bmod 5$	$3x+6 \equiv 0 \bmod 12$	$33x \equiv 9 \bmod 1128$
$6x \equiv 3 \bmod 35$	$3x \equiv 13 \bmod 18$	$7x \equiv 4 \bmod 10$	$33x \equiv 9 \bmod 128$

39. Determinar los números enteros entre 400 y 500 que dan resto 5 al dividirlos por 6 y dan resto 2 al dividirlos por 11.

40. Resolver los siguientes sistemas de congruencias:

$$\left\{ \begin{array}{ll} x \equiv 3 & \bmod 4 \\ x \equiv 4 & \bmod 25 \\ x \equiv 5 & \bmod 9 \end{array} \right\} \qquad \left\{ \begin{array}{ll} 7x \equiv 28 & \bmod 35 \\ 6x \equiv 18 & \bmod 42 \\ 5x \equiv 3 & \bmod 12 \end{array} \right\}$$

41. Demostrar que si a, b y n son enteros tales que $a \equiv b \bmod n$ entonces $\mathrm{mcd}(a,n) = \mathrm{mcd}(b,n)$.

42. Sean $a, b \in \mathbb{Z}_n$. Demostrar que ab es invertible precisamente si lo son a y b.

[3] Los enteros de la forma $M_p = 2^p - 1$ con p primo se llaman *números de Mersenne*. No es cierto que todos ellos sean primos (¿cuál es el menor primo p tal que M_p no es primo?). Por otra parte, los mayores números primos que se conocen son de este tipo.

[4] Los enteros de la forma $F_m = 2^{2^m}+1$ se llaman *números de Fermat*. No es difícil comprobar que F_m es primo para $m = 1, 2, 3, 4$ y que F_5 es divisible por 641. De hecho, para $m \geq 5$, todos los F_m que se han analizado son compuestos, pero no existe una demostración de la conjetura que este hecho sugiere.

43. Si $n \neq 0$ y $d = \mathrm{mcd}(a, n)$ divide a c, demostrar que la ecuación $aX \equiv c \bmod n$ tiene exactamente d soluciones en $\mathbb{Z}_n$.

44. Si p es un entero positivo primo, demostrar que, para enteros arbitrarios a y b, se tiene

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

45. Sean a, b y c enteros tales que $a^2 + b^2 = c^2$. Demostrar que:

    (a) Al menos uno de los enteros a, b ó c es múltiplo de 3.

    (b) Al menos uno de los enteros a, b ó c es múltiplo de 5.

    (c) El producto abc es múltiplo de 60. (Indicación: Trabajar módulo 8 para ver que abc es múltiplo de 4.)

46. Sean $a, k, l, n \in \mathbb{Z}$. Demostrar que las condiciones

$$\mathrm{mcd}(a, n) = 1, \qquad \mathrm{mcd}(k, \phi(n)) = 1 \qquad \text{y} \qquad kl \equiv 1 \bmod \phi(n)$$

    implican que $a^{kl} \equiv a \bmod n$, y usar este resultado para resolver la ecuación $x^7 \equiv 5 \bmod 64$.

47. [*] Sea n un entero positivo. Demostrar que

$$n = \sum \phi(d),$$

    donde d recorre el conjunto de los divisores positivos de n. (Indicación: Para cada d, considerar el conjunto $X_d = \{[\frac{n}{d}x]_n : [x]_d \in \mathbb{Z}_d^*\}$.)

48. Demostrar que, si $a, m, n \in \mathbb{N}$ y $m \neq n$, entonces $\mathrm{mcd}(a^{2^m}+1, a^{2^n}+1)$ vale 1 si a es par y 2 si a es impar.

49. Calcular el último dígito decimal de 3^{400}.

50. Hallar el resto de las siguientes divisiones enteras:

    (a) 132^{231} entre 7.

    (b) 246^{218} entre 11.

    (c) 211^{3143} entre 12.

    (d) 347^{231} entre 35.

51. Para cada uno de los valores $n = 2, 3, \ldots, 30$, se pide:

    (a) Calcular $\phi(n)$ usando la fórmula de la Proposición 1.8.4.

    (b) Describir explícitamente $\mathbb{Z}_n^*$ y comprobar que tiene $\phi(n)$ elementos.

52. Determinar todos los enteros n tales que $\phi(n) = 4$, y todos los enteros n tales que $\phi(n) = 8$.

Bibliografía del capítulo

Allenby [1], Clark [9], Cohn [10], Delgado-Fuertes-Xambó [12], Dorronsoro-Hernández [13], Jacobson [23].

Capítulo 2

Anillos

Se estudia la estructura de anillo y se presentan sus ejemplos y propiedades básicas.

Introducción

Algunas de las propiedades que verifican la suma y el producto de números enteros son compartidas por otros "sistemas" formados por un conjunto con dos operaciones: clases de restos, polinomios, matrices, funciones... Estos sistemas, y otros muchos que veremos, se engloban en el concepto abstracto de anillo, a cuyo estudio dedicamos este capítulo.

Los primeros problemas que abordaremos son los que se plantean al estudiar la mayoría de las estructuras abstractas en Matemáticas. Para un anillo A, describiremos los subconjuntos de A que, con las operaciones de A, siguen siendo anillos (subanillos). También consideraremos las relaciones de equivalencia en A que son compatibles con sus operaciones, lo que dará lugar a los conceptos de ideal y de anillo cociente. Por último, estudiaremos las aplicaciones entre anillos que conservan la estructura (homomorfismos de anillos) y las entenderemos como el modo natural de establecer relaciones entre anillos, hasta interpretar los anillos isomorfos como anillos "esencialmente iguales".

En las últimas secciones estudiamos dos tipos de anillos con ciertas propiedades especiales: los dominios y los cuerpos. Sus prototipos son los anillos de números enteros y racionales, respectivamente, y veremos cómo, imitando la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$, a cada dominio se le puede asociar un cuerpo con el que se relaciona estrechamente.

Objetivos del capítulo

- Conocer los axiomas que definen un anillo, las propiedades básicas de las operaciones en un anillo arbitrario y los principales ejemplos de anillos.

- Conocer y manejar los conceptos de subanillo e ideal; saber identificar el ideal generado por un subconjunto y saber encontrar y manejar sistemas generadores de ideales.

- Conocer el concepto de anillo cociente y la relación entre los ideales de un anillo y los de sus cocientes (Teorema de la Correspondencia).

- Conocer las propiedades básicas de los homomorfismos de anillos, las nociones de núcleo e imagen y los Teoremas de Isomorfía.

- Manejar las nociones de elemento cancelable e invertible, las de dominio y cuerpo, y las relaciones de éstas con los ideales primos y maximales.

- Entender la construcción del cuerpo de fracciones de un dominio y la relación entre ambos.

Desarrollo de los contenidos

2.1 Operaciones

En las matemáticas elementales se consideran y estudian las "operaciones aritméticas"; primero con números naturales, luego con enteros y con racionales, más tarde con reales o complejos, o con vectores del plano o del espacio, por ejemplo. Entre estas operaciones, las más simples son la suma y el producto, cuyas definiciones dependen del conjunto que estemos considerando. Por ejemplo, el producto de dos números naturales n y m puede definirse como el resultado de sumar n consigo mismo m veces. El producto de dos números reales (positivos) x e y tiene un significado más geométrico: puede interpretarse como el valor del área de un rectángulo cuyos lados tienen longitud x e y. Análogamente, la suma de números naturales no tiene el mismo significado que la suma de vectores o la de números complejos.

Lo que resulta de la discusión anterior es que, si uno quiere abstraer una idea general de "operación entre los elementos de un conjunto", no es posible atender al significado de cada operación particular. Lo que hay de común entre todas las operaciones que hemos considerado antes es algo formal, que se refleja en la definición que sigue:

Definición 2.1.1 *Una* operación[1] *o* ley de composición interna *en un conjunto A es una aplicación del producto cartesiano $A \times A$ en A.*

Usualmente, una operación se denota por un símbolo como $*$, $+$, $\cdot$, $\times$, $\cap$, $\cup$, etcétera, y entonces la imagen del par $(a, b) \in A \times A$ se denota por $a * b$, $a + b$, $a \cdot b$, etcétera. De hecho, cuando se usa la notación $\cdot$ es costumbre omitir el punto y se suele escribir ab en lugar de $a \cdot b$.

La mayoría de los símbolos propuestos en el párrafo anterior sugerirán al lector ejemplos de operaciones que conoce. Algunas "operaciones" familiares pueden no serlo en el sentido de la definición precedente. Por ejemplo, la resta de números naturales puede no ser un número natural, de modo que la resta no es una ley de composición interna en $\mathbb{N}$ (sí podríamos verla como una "ley de composición externa" $\mathbb{N} \times \mathbb{N} \to \mathbb{Z}$). Por razones análogas, la división no es una operación en $\mathbb{Z}$ ni en $\mathbb{Q}$, aunque sí lo es en $\mathbb{Q} \setminus \{0\}$.

La definición de operación es demasiado general, y en la práctica nos interesarán sólo las operaciones que verifiquen ciertas propiedades que las hagan manejables. Pasamos pues a considerar ciertas propiedades que puede verificar una operación.

Definición 2.1.2 *Sea $*$ una operación en un conjunto A. Decimos que:*

- *La operación es* asociativa *si $a * (b * c) = (a * b) * c$ para cualesquiera $a, b, c \in A$.*
- *La operación es* conmutativa *si $a * b = b * a$ para cualesquiera $a, b \in A$.*
- *El elemento $e \in A$ es un* elemento neutro *si $a * e = a = e * a$ para cada $a \in A$.*
- *Si existe un elemento neutro e, el elemento $b \in A$ es* simétrico[2] *de $a \in A$ si $a * b = e = b * a$.*
- *El elemento $a \in A$ es* cancelable *si cualquiera de las relaciones $a * b = a * c$ ó $b * a = c * a$ (con $b, c \in A$) implica que $b = c$.*

Es claro que, cuando se cumple la propiedad conmutativa, las definiciones de elemento neutro, elemento simétrico y elemento cancelable se simplifican.

Ejemplos 2.1.3 *Operaciones.*

1. La suma usual es una operación en cada uno de los conjuntos $\mathbb{Z}$, $\mathbb{N}$ y $\mathbb{Z}^+$. En los tres casos es asociativa y conmutativa, sólo hay elemento neutro en los dos primeros y el 1 sólo tiene elemento simétrico en el primer caso. Otra operación que podemos considerar en esos conjuntos es el producto usual. ¿Qué propiedades tiene en cada uno de ellos?

   Este ejemplo y otros muchos que vendrán muestran que, en general, las propiedades de una operación dependen fuertemente del *conjunto ambiente* en el que la estemos considerando.

[1] Deberíamos decir *operación binaria* porque se aplica a pares de elementos, pero no necesitaremos hablar de otro tipo de operaciones y nos ahorraremos la repetición del adjetivo.

[2] En contextos más concretos usaremos *elemento opuesto* y *elemento inverso* en lugar de *elemento simétrico*.

2. Si A es el conjunto de todas las funciones reales de variable real, la composición de funciones es una operación en A que es asociativa y tiene un elemento neutro e dado por $e(x) = x$, pero en general no es conmutativa; por ejemplo, si f y g son las funciones definidas por $f(x) = x^2$ y $g(x) = x + 1$ entonces $(f \circ g)(x) = x^2 + 2x + 1$, mientras que $(g \circ f)(x) = x^2 + 1$.

3. En el conjunto $\mathbb{Z}^+$ la operación $*$ dada por $a * b = a^b$ no es asociativa ni conmutativa ni tiene elemento neutro (aunque sí tiene lo que podríamos llamar un *neutro por la derecha*: el 1 verifica $a * 1 = a$ para cualquier a, pero no $1 * a = a$).

Ejercicio 2.1.4 *Para un conjunto A con una operación asociativa $*$ con un elemento neutro e, demostrar que se verifican las siguientes propiedades (ver la demostración de la Proposición 1.1.1):*

1. (Unicidad del neutro) *El neutro es único; más aún, si e verifica $e * a = a$ para cada $a \in A$ y f verifica $a * f = a$ para cada $a \in A$ entonces $e = f$.*

2. (Unicidad de los simétricos) *Si $a \in A$ tiene elemento simétrico, éste es único; más aún, si $b \in A$ verifica $a * b = e$ y $c \in A$ verifica $c * a = a$ entonces $b = c$.*

3. *Todo elemento que tenga un simétrico es cancelable.*

En virtud de este resultado, cuando existan, hablaremos de *el* elemento neutro de la operación y de *el* elemento simétrico de a, y no sólo de *un* elemento neutro o *un* elemento simétrico de a. También es claro que, si b es el simétrico de a, entonces a es el simétrico de b.

En este párrafo suponemos que $*$ es una operación asociativa en el conjunto A. Dados tres elementos $a, b, c \in A$ podemos escribir $a * b * c$ sin ambigüedad, en el sentido de que es indiferente cuál de los dos $*$ actúe primero. Cuando tenemos cuatro elementos, la asociatividad nos dice que

$$a * ((b * c) * d) = a * (b * (c * d)) = (a * b) * (c * d) = ((a * b) * c) * d = (a * (b * c)) * d$$

y por lo tanto tampoco en este caso hay ambigüedad al escribir $a * b * c * d$ sin paréntesis (comprueba que no hay otras opciones para el orden en el que actúan los tres $*$). Esta propiedad de *asociatividad generalizada* es cierta para cualquier conjunto finito de elementos, y la asumiremos sin demostración. Así, dados elementos $a_1, \ldots, a_n$ en A, escribiremos $a_1 * \cdots * a_n$ sin ambigüedad y se verificarán relaciones como

$$a_1 * \cdots * a_n = (a_1 * \cdots * a_{n-1}) * a_n = a_1 * (a_2 * \cdots * a_n).$$

Cuando además la operación sea conmutativa, entonces se tiene una *conmutatividad generalizada* que nos permite, en una expresión como la anterior, reordenar los a_i de cualquier forma sin alterar el resultado de la operación.

2.2 Grupos abelianos y anillos

Definición 2.2.1 *Un* grupo abeliano *es un par*[3] $(A, +)$ *formado por un conjunto no vacío A y una operación $+$ en A que es asociativa, conmutativa, con elemento neutro y tal que cada elemento de A tiene un simétrico (y por lo tanto es cancelable).*

Al neutro le llamaremos cero *y lo denotaremos por* 0. *Al simétrico de a le llamaremos su* opuesto *y lo denotaremos por $-a$ (se tiene por lo tanto $-(-a) = a$). Escribiremos además $a - b$ en lugar de $a + (-b)$.*

Ejemplos 2.2.2 *Grupos abelianos.*

1. Los conjuntos $\mathbb{Z}$ de números enteros, $\mathbb{Q}$ de números racionales, $\mathbb{R}$ de números reales y $\mathbb{C}$ de números complejos son grupos abelianos con la suma usual. También lo es el conjunto $2\mathbb{Z}$ de los números enteros pares, y en general cualquier ideal de $\mathbb{Z}$.

2. La suma de números naturales no convierte a $\mathbb{N}$ en un grupo abeliano; ¿por qué?

[3] Cuando no haya riesgo de confusión con la operación diremos simplemente que A es un grupo abeliano.

3. Un conjunto con un único elemento es un grupo abeliano con la única operación posible, y se llama *grupo trivial*. Obsérvese que hay muchos grupos triviales (uno por cada conjunto unitario) pero todos son *esencialmente iguales*.

4. La operación de un grupo abeliano no siempre es una suma en el sentido usual. Por ejemplo, el conjunto $\mathbb{Q}^*$ de los números racionales no nulos con el producto usual es un grupo abeliano (con neutro 1), y lo mismo ocurre con los conjuntos $\mathbb{Z}_n^*$ definidos en la Sección 1.8. Nos referiremos a estos grupos como el *grupo multiplicativo* de los racionales no nulos o de $\mathbb{Z}_n^*$.

Definición 2.2.3 *Un* anillo (conmutativo y con identidad) *es una terna*[4] $(A, +, \cdot)$ *formada por un conjunto no vacío A y dos operaciones $+$ y $\cdot$ en A; la primera llamada usualmente* suma *y la segunda* producto *o* multiplicación, *que verifican:*

1. *A es un grupo abeliano con la suma (cuyo neutro denotamos por 0).*

2. *El producto es asociativo y conmutativo y tiene un elemento neutro al que llamaremos* uno *o* identidad, *y que denotaremos por 1.*

   Se pueden definir anillos "no conmutativos" o "sin identidad" excluyendo las correspondientes propiedades para el producto en la definición. En este curso asumiremos que los anillos son conmutativos y con identidad y avisaremos cuando esto no ocurra. Por ejemplo, en el Capítulo 10 trabajaremos con anillos no conmutativos.

3. *Se verifica la siguiente* propiedad distributiva *que relaciona las dos operaciones: Dados $a, b, c \in A$ se verifica*
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

En general, no se asume que cada elemento a de A tenga simétrico para el producto. Cuando lo tiene, lo denotamos por a^{-1} (de modo que $aa^{-1} = 1$ y $(a^{-1})^{-1} = a$), le llamamos el inverso *de a y decimos que a es* invertible *o una* unidad *en A (del Ejercicio 2.1.4 se deduce que si a es invertible entonces es cancelable en productos; es decir, $ab = ac$ implica $b = c$). Denotaremos por A^* al conjunto de todas las unidades de A.*

Usualmente escribiremos ab en vez de $a \cdot b$. Además asumiremos que, en ausencia de paréntesis, los productos se realizan antes que las sumas (y que las restas). Así, por ejemplo, la propiedad distributiva se reescribe como $a(b + c) = ab + ac$.

Si A es conmutativo y b es invertible, escribiremos a veces a/b ó $\frac{a}{b}$ en lugar de ab^{-1}. Esta notación no se debe utilizar con anillos no conmutativos pues en ese caso ab^{-1} y $b^{-1}a$ pueden ser diferentes.

De los axiomas de anillo se pueden deducir algunas propiedades elementales:

Ejercicio 2.2.4 *Sea A un anillo y sean $a, b, c \in A$. Demostrar que se verifican las siguientes propiedades:*

1. $0a = 0 = a0$.

2. $a(-b) = (-a)b = -(ab)$.

3. $a(b - c) = ab - ac$.

4. *ab es invertible precisamente si a y b son invertibles. En tal caso $(ab)^{-1} = a^{-1}b^{-1}$.*

5. *A^* es un grupo abeliano con el producto de A.*

Dados un anillo A, un elemento $a \in A$ y un entero positivo n, la notación na (respectivamente a^n) representa el resultado de sumar (respectivamente multiplicar) a consigo mismo n veces, y si $n = 0$ hacemos[5] $0a = 0$ y $a^0 = 1$. Más rigurosamente, a partir de estas últimas igualdades se definen na y a^n de forma recurrente poniendo $(n + 1)a = a + na$ y $a^{n+1} = aa^n$ para $n \geq 0$. Por último, si $n \geq 1$ se define $(-n)a = -(na)$, y si además a es invertible se define $a^{-n} = (a^{-1})^n$.

[4] Cuando no haya riesgo de confusión con las operaciones diremos simplemente que A es un anillo.

[5] En general, si una operación en un conjunto tiene neutro, se asume que "operar el conjunto vacío" da como resultado el neutro. Así, con las notaciones usuales, la "suma de ningún elemento" se interpreta como el cero y el "producto de ningún elemento" se interpreta como el uno. Esta convención tiene importantes ventajas para la notación que se pueden observar ya en el ejercicio que sigue.

Ejercicio 2.2.5 *Dados un anillo A, elementos $a, b \in A$ y enteros $m, n \in \mathbb{Z}$, se verifican las siguientes propiedades:*

1. $n(a+b) = na + nb$.
2. $(n+m)a = na + ma$.
3. *Si $n \geq 0$ entonces* $(ab)^n = a^n b^n$.
4. *Si $n, m \geq 0$ entonces* $a^{n+m} = a^n a^m$.
5. *Si a y b son invertibles, las dos propiedades anteriores valen también para exponentes negativos.*

Ejemplos 2.2.6 *Anillos.*

1. Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos con la suma y el producto usuales. Nótese que todo elemento no nulo es invertible en $\mathbb{Q}$, pero en $\mathbb{Z}$ sólo hay dos elementos invertibles; en general, las propiedades de un elemento dependerán del anillo en el que lo estemos considerando.

2. El conjunto $2\mathbb{Z}$ de los números enteros pares es un "anillo sin identidad".

3. Las operaciones definidas en la Sección 1.6 dotan a $\mathbb{Z}_n$ de una estructura de anillo. Obsérvese que $\mathbb{Z}_0$ es el propio $\mathbb{Z}$ y que la notación $\mathbb{Z}_n^*$ para el conjunto de las unidades de $\mathbb{Z}_n$ es consistente con la que se empleó anteriormente .

4. Sean A y B dos anillos. Entonces el producto cartesiano $A \times B$ tiene una estructura de anillo con las operaciones

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \quad \text{y} \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

   (se dice que las operaciones en $A \times B$ se definen *componente a componente*). Obsérvese que $A \times B$ es conmutativo precisamente si lo son A y B, y que esta construcción se puede generalizar a productos cartesianos de cualquier familia (finita o no) de anillos.

5. Dados un anillo A y un conjunto X, el conjunto A^X de las aplicaciones de X en A es un anillo con las siguientes operaciones:

$$(f+g)(x) = f(x) + g(x) \qquad (f \cdot g)(x) = f(x) \cdot g(x).$$

   ¿Cuál es la relación entre este ejemplo y el anterior?

6. Dado un anillo A, un *polinomio* en la *indeterminada* X con coeficientes en A es[6] una expresión del tipo

$$P = P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

   donde n es un número entero no negativo y $a_i \in A$ para todo i. Para cada i, a_i se llama *coeficiente* de *grado* i de P, a_0 se llama *coeficiente independiente* de P y, si $a_n \neq 0$, entonces n es el *grado* de P y a_n es su *coeficiente principal*. Dos polinomios son iguales si y sólo si lo son coeficiente a coeficiente. Denotaremos por $A[X]$ al conjunto de los polinomios en la indeterminada X con coeficientes en A.

   Utilizando la estructura de anillo de A se puede dotar a $A[X]$ de una estructura de anillo definiendo la suma y el producto de la forma usual:

$$(a_0 + a_1 X + a_2 X^2 + \cdots) + (b_0 + b_1 X + b_2 X^2 + \cdots) = c_0 + c_1 X + c_2 X^2 + \cdots,$$

   donde cada $c_n = a_n + b_n$, y

$$(a_0 + a_1 X + a_2 X^2 + \cdots) \cdot (b_0 + b_1 X + b_2 X^2 + \cdots) = d_0 + d_1 X + d_2 X^2 + \cdots,$$

   donde cada $d_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0 = \sum_{i=0}^{n} a_i b_{n-i}$ (si un coeficiente no aparece en la expresión de un polinomio se considera que vale 0).

[6] Por ahora no daremos definiciones rigurosas sobre polinomios; éstas vendrán en el Capítulo 4.

7. Dado un anillo A, denotamos por $A[[X]]$ el conjunto de las sucesiones $(a_0, a_1, a_2, \ldots)$ de elementos de A. En $A[[X]]$ consideramos la suma y el producto dados por

$$\begin{aligned}(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)\\ (a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) &= (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots).\end{aligned}$$

Obsérvese la similitud con la definición de las operaciones en el anillo de polinomios; de hecho, el elemento $(a_0, a_1, a_2, \ldots)$ se suele denotar por $\sum_{i=0}^{\infty} a_i X^i$. Con estas operaciones, $A[[X]]$ es un anillo llamado el *anillo de series de potencias* con coeficientes en A.

8. Sean A un anillo y n un número natural. Denotaremos por $M_n(A)$ el conjunto de las matrices cuadradas de dimensión n con coeficientes en A. Es decir un elemento de $M_n(A)$ tiene la forma

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

con $a_{ij} \in A$, para todo $1 \leq i, j \leq n$. Con el fin escribir menos, una matriz como la anterior la representaremos como $(a_{ij})_{1 \leq i,j \leq n}$ o simplemente como (a_{ij}). Definimos la suma y el producto de matrices como

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \qquad (a_{ij}) \cdot (b_{ij}) = (a_{i1}b_{1j} + \cdots + a_{in}b_{nj}).$$

El lector reconocerá la suma y producto de matrices del álgebra lineal y no debe tener problemas para demostrar que $M_n(A)$ es un anillo cuando A lo es. Obsérvese que $M_n(A)$ sólo es conmutativo si $n = 1$ y A es conmutativo.

9. Sea V un espacio vectorial no trivial sobre un cuerpo K. El lector que no esté familiarizado con el concepto de cuerpo puede pensar que $K = \mathbb{R}$. Sea A el conjunto de los endomorfismos de V. Entonces A tiene una estructura de anillo dada por las operaciones

$$(f + g)(x) = f(x) + g(x) \qquad (fg)(x) = f(g(x)).$$

Es decir, el producto en A es la composición de endomorfismos. Este anillo sólo es conmutativo si la dimensión de V es 1.

2.3 Subanillos

Si A es un conjunto con una operación $*$ y B es un subconjunto de A, decimos que B es *cerrado para la operación* $*$ si se tiene $x * y \in B$ cuando $x, y \in B$. Esto implica que $* : A \times A \to A$ se restringe a una aplicación $* : B \times B \to B$, y por lo tanto podemos considerar a $*$ como una operación en B que se dice *inducida* por la operación en A.

Definición 2.3.1 *Si $(A, +, \cdot)$ es un anillo, un* subanillo *de A es un subconjunto B de A cerrado para ambas operaciones, que contiene al 1 y tal que $(B, +, \cdot)$ es un anillo.*

La siguiente proposición nos dice cómo comprobar si un subconjunto es un un subanillo.

Proposición 2.3.2 *Las condiciones siguientes son equivalentes para un subconjunto B de un anillo A:*

1. *B es un subanillo de A.*
2. *B contiene al 1 y es cerrado para sumas, productos y opuestos.*
3. *B contiene al 1 y es cerrado para restas y productos.*

Demostración. 1 implica 2. Si B es un subanillo de A es evidente que B contiene al 1 y es cerrado para sumas y productos. Por otro lado, como B es un anillo, cada elemento $b \in B$ tiene un opuesto. Por la unicidad del elemento simétrico (Ejercicio 2.1.4), este opuesto ha de ser el de A, con lo que B es cerrado para opuestos.

2 implica 3 es evidente.

3 implica 1. Sea B un subconjunto de A que contiene al uno y es cerrado para restas y productos. Entonces $0 = 1 - 1 \in B$, con lo que si $b \in B$, entonces $-b = 0 - b \in B$; es decir, B es cerrado para opuestos. Si $a, b \in B$, entonces $-b \in B$ y, por tanto, $a + b = a - (-b) \in B$; es decir, B es cerrado para sumas. Ahora es evidente que B es un subanillo de A. □

Ejemplos 2.3.3 *Subanillos.*

1. Cada uno de los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es un subanillo de los posteriores.

2. Todo anillo A es un subanillo de sí mismo, al que llamamos *impropio* por oposición al resto de subanillos, que se dicen *propios*.

3. Si A es un anillo, el subconjunto $\{0\}$ es cerrado para sumas, productos y opuestos. Sin embargo, no contiene al 1 (si $A \neq 0$), con lo que no es un subanillo de A.

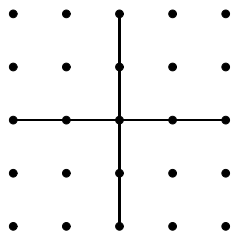
4. Si A es un anillo, el conjunto
$$\mathbb{Z}1 = \{n1 : n \in \mathbb{Z}\}$$
de los múltiplos enteros de 1 es un subanillo de A contenido en cualquier otro subanillo de A; es decir, $\mathbb{Z}1$ es el menor subanillo de A, y se conoce como el *subanillo primo* de A.

   Es claro que $\mathbb{Z}$ y los $\mathbb{Z}_n$ son sus propios subanillos primos, y por lo tanto no tienen subanillos propios.

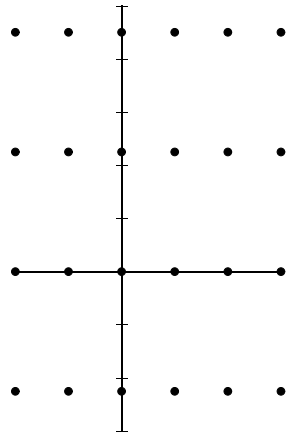
5. Si A y B son anillos y $B \neq 0$ entonces $A \times 0 = \{(a, 0) \mid a \in A\}$ es cerrado para sumas y productos pero no es un subanillo de $A \times B$ (¿por qué?).

6. Dado un número entero m, los conjuntos
$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \qquad \text{y} \qquad \mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$$
son subanillos de $\mathbb{C}$. Si además m es positivo, entonces ambos son subanillos de $\mathbb{R}$. Si m es el cuadrado de un número entero entonces esos conjuntos coinciden con $\mathbb{Z}$ y con $\mathbb{Q}$, respectivamente, por lo que el ejemplo carece de interés. Cuando m no es el cuadrado de un entero (por ejemplo $m = 2$ ó $m = -1$) entonces, por la Proposición 1.5.10, tampoco es el cuadrado de un número racional, de manera que, en cualquiera de los dos anillos descritos, la igualdad $a + b\sqrt{m} = 0$ implica que $a = 0$ y $b = 0$, y por lo tanto la igualdad $a + b\sqrt{m} = c + d\sqrt{m}$ implica que $a = c$ y $b = d$.

   Un caso particular es el anillo $\mathbb{Z}[i]$, donde $i = \sqrt{-1}$, llamado el *anillo de los enteros de Gauss*. Podemos visualizar $\mathbb{Z}[i]$ dentro del plano complejo como el conjunto de los vértices de un enlosado del plano complejo por losas cuadradas de lado 1, como muestra el siguiente esquema:



   Más generalmente, si $m < 0$, entonces podemos visualizar $\mathbb{Z}[\sqrt{m}]$ como el conjunto de vértices de un enlosado del plano complejo por losas rectangulares con una base de longitud 1 y una altura de longitud $\sqrt{-m}$. Por ejemplo, una porción de $\mathbb{Z}[\sqrt{-5}]$ está representada por los siguientes puntos del plano complejo:



7. Todo anillo A puede verse como un subanillo del anillo de polinomios $A[X]$ si identificamos los elementos de A con los *polinomios constantes* (del tipo $P = a_0$).

8. Sea A un anillo y X un conjunto. Entonces la *diagonal*

$$B = \{f \in A^X : f(x) = f(y) \text{ para todo } x, y \in X\}$$

(es decir, el conjunto de las *aplicaciones constantes* de X en A) es un subanillo de A^X.

2.4 Ideales y anillos cociente

La noción de ideal que vimos en el Capítulo 1 para números enteros se puede generalizar a un anillo arbitrario.

Definición 2.4.1 *Sea A un anillo. Una* combinación lineal *con coeficientes en A (o una* combinación A-lineal*) de los elementos $a_1, \ldots, a_n$ de A es un elemento de A de la forma*

$$r_1 a_1 + \cdots + r_n a_n,$$

donde cada $r_i \in A$. Los enteros r_i son los coeficientes *de la combinación lineal.*

Un subconjunto I de A es un ideal *si no es vacío y si, dados $a, b \in I$, cualquier combinación A-lineal suya $ra + sb$ está en I.*

Como ocurre con los ideales de $\mathbb{Z}$, en la definición podemos sustituir la condición $I \neq \emptyset$ por la condición $0 \in I$, y cualquier combinación lineal de un numero finito de elementos de un ideal I sigue siendo un elemento de I.

Ejemplos 2.4.2 *Ideales.*

1. Si A es un anillo, el conjunto

$$bA = (b) = \{ba : a \in A\}$$

es un ideal de A llamado *ideal principal generado por b*. Ya vimos en el Capítulo 1 que todos los ideales de $\mathbb{Z}$ son de esta forma. Esto no es cierto en general, como pronto veremos. Obsérvese que bA es el menor ideal de A que contiene a b. Obsérvese también que $1A = A$ y que $0A = \{0\}$, con lo que estos dos son ideales principales de A llamados respectivamente *ideal impropio* (en oposición a *ideales propios*, para los demás) e *ideal cero* o *trivial*. El ideal trivial $\{0\}$ lo representaremos a partir de ahora por 0.

2. Más generalmente, si T es un subconjunto de un anillo, entonces el conjunto

$$(T) = \{\sum_{i=1}^{n} a_i t_i : n \in \mathbb{Z}^+, a_i \in A, t_i \in X\}$$

es un ideal, llamado *ideal generado* por T.

3. Si A y B son dos anillos entonces $A \times 0 = \{(a,0) : a \in A\}$ es un ideal de $A \times B$.

4. Sea $\mathbb{Z}[X]$ el anillo de los polinomios con coeficientes enteros. Es fácil ver que el ideal generado por el elemento X puede describirse como el de los polinomios sin coeficiente independiente; es decir,

$$I = (X) = \{a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X] : a_0 = 0\}.$$

También es sencillo ver que el conjunto

$$J = \{a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X] : a_0 \in 2\mathbb{Z}\}$$

de los polinomios con coeficiente independiente par es un ideal de $\mathbb{Z}[X]$. En el Ejemplo 2.5.9 veremos que este ideal no es principal.

Definición 2.4.3 *Sea I un ideal de un anillo A. Decimos que dos elementos $a, b \in A$ son* congruentes módulo I, *y escribimos $a \equiv b \mod I$, si su diferencia está en I; o sea:*

$$a \equiv b \mod I \Leftrightarrow b - a \in I.$$

¿A qué te recuerda esto?

Ejercicio 2.4.4 *Dados un anillo A, un ideal I de A y elementos $a, b, c, d \in A$, demostrar que:*

1. $a \equiv a \mod I$
2. *Si* $a \equiv b \mod I$, *entonces* $b \equiv a \mod I$.
3. *Si* $a \equiv b \mod I$ *y* $b \equiv c \mod I$, *entonces* $a \equiv c \mod I$.
4. $a \equiv b \mod (0)$ *precisamente si* $a = b$.

Del Ejercicio 2.4.4 se deduce que la relación "ser congruente módulo I" es una relación de equivalencia en A y, por tanto, las clases de equivalencia por esta relación definen una partición de A. La clase de equivalencia que contiene a un elemento $a \in A$ es

$$a + I = \{a + x : x \in I\}$$

(en particular $0 + I = I$), de modo que

$$a + I = b + I \Leftrightarrow a \equiv b \mod I$$

(en particular $a + I = 0 + I \Leftrightarrow a \in I$). El conjunto de las clases de equivalencia se denota

$$A/I = \frac{A}{I} = \{a + I : a \in A\}.$$

Ejercicio 2.4.5 *Sea A un anillo con un ideal I. Las operaciones suma y producto en A/I dadas por*

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I) \cdot (b + I) = (ab) + I$$

están bien definidas (ver la Observación 1.6.2) y dotan a A/I de una estructura de anillo con neutro $0 + I$ y unidad $1 + I$. Este anillo se llama anillo cociente *de A módulo I.*

Al hacer el cociente de un anillo A por un ideal I, elementos que eran distintos en A "pasan a ser iguales" en el cociente (estrictamente hablando, son sus clases de equivalencia las que se hacen iguales); en particular, los elementos de I "se hacen cero". En muchas de las ocasiones en las que se construyen estructuras cociente eso es precisamente lo que se busca, identificar entre sí o anular ciertos elementos.

Ejemplos 2.4.6 *Anillos cociente.*

1. El anillo cociente del anillo $\mathbb{Z}$ por el ideal (n) es el anillo $\mathbb{Z}_n$ de las clases de restos módulo n.

2. Para analizar las soluciones enteras de la ecuación $x^2 - 15y^2 = \pm 2$ podemos considerarla en $\mathbb{Z}_5$, donde toma la forma más sencilla $x^2 = \pm 2$ (¡anulamos ese -15 que complicaba la ecuación!); ahora es elemental ver que esta ecuación no tiene soluciones en $\mathbb{Z}_5$ y deducir que la ecuación inicial no tiene soluciones enteras.

3. $A/0$ es el propio anillo A, mientras que $A/A = 0$.

4. Consideremos el ideal (X) del anillo de polinomios $\mathbb{Z}[X]$ (ver los Ejemplos 2.4.2). Como todo polinomio es congruente módulo (X) con su coeficiente independiente (visto como polinomio), no es difícil convencerse de que $\mathbb{Z}[X]/(X)$ y $\mathbb{Z}$ son, en esencia, el mismo anillo (más tarde precisaremos este comentario viendo que son *isomorfos*).

5. Sean A y B anillos e $I = A \times 0$. Como $(a, b) \equiv (0, b) \bmod I$, los anillos $(A \times B)/I$ y B son esencialemente iguales (isomorfos).

Ejercicio 2.4.7 *Demostrar que un elemento b de un anillo A es invertible si y sólo si $(b) = A$, y deducir que las siguientes condiciones son equivalentes para un ideal I de A.*

1. *I es impropio; es decir, $I = A$.*

2. *I contiene a la identidad de A; es decir, $1 \in I$.*

3. *I contiene una unidad de A; es decir, $I \cap A^* \neq \emptyset$.*

El siguiente resultado describe los ideales de un anillo cociente. Emplearemos la siguiente notación: si A es un anillo e I es un ideal suyo, $\pi : A \to A/I$ denotará la aplicación que lleva cada elemento de A a su clase de equivalencia; es decir, $\pi(a) = a + I$. La imagen por π de un subconjunto J de A es

$$\pi(J) = \{a + I : a \in J\}.$$

Si J contiene a I, denotaremos este conjunto por J/I. La preimagen por π de un subconjunto X de A/I es

$$\pi^{-1}(X) = \{a \in A : a + I \in X\}.$$

Teorema 2.4.8 (Teorema de la Correspondencia) *Si I es un ideal de un anillo A, las asignaciones $J \mapsto J/I$ y $X \mapsto \pi^{-1}(X)$ son biyecciones (una inversa de la otra) que conservan la inclusión entre el conjunto de los ideales de A que contienen a I y el conjunto de todos los ideales de A/I.*

Demostración. Hay que comprobar los siguientes puntos, cosa que el lector podrá hacer como ejercicio:

- Si J es un ideal de A que contiene a I entonces J/I es un ideal de A/I y $\pi^{-1}(J/I) = J$.
- Si X es un ideal de A/I entonces $\pi^{-1}(X)$ es un ideal de A que contiene a I y $\pi^{-1}(X)/I = X$.
- Si $J \subseteq K$ son ideales de A que contienen a I entonces $J/I \subseteq K/I$.
- Si $X \subseteq Y$ son ideales de A/I entonces $\pi^{-1}(X) \subseteq \pi^{-1}(Y)$.

□

Ejercicio 2.4.9 *Si n es un entero positivo, demostrar que los ideales de $\mathbb{Z}/n\mathbb{Z}$ son precisamente los de la forma $m\mathbb{Z}/n\mathbb{Z}$, donde m es un divisor positivo de n, y además $m\mathbb{Z}/n\mathbb{Z}$ está contenido en $m'\mathbb{Z}/n\mathbb{Z}$ si y sólo si m' divide a m.*

2.5 Operaciones con subanillos e ideales

Ejercicio 2.5.1 *Si A es un anillo, demostrar que la intersección de cualquier familia de subanillos (respectivamente de ideales) de A es un subanillo (respectivamente un ideal) de A. En general, no ocurre lo mismo con las uniones.*

El Ejercicio 2.5.1 nos va a permitir repetir lo que hicimos al definir el ideal de $\mathbb{Z}$ generado por un subconjunto.

Definición 2.5.2 *Sea A un anillo y sea X un subconjunto de A. Llamamos* subanillo *de A* generado *por X a la intersección B de todos los subanillos de A que contienen a X (¿podemos asegurar que al menos existe uno?). Es claro que B es el menor subanillo de A que contiene a X; es decir, B es un subanillo de A y todos los subanillos de A que contienen a X también contienen a B.*

De modo análogo, se define el ideal *de A* generado *por X que, siguiendo la notación del Capítulo 1, se denota (X).*

Ejercicio 2.5.3 *Demostrar que las dos definiciones de ideal generado (ver los Ejemplos 2.4.2 y la Definición 2.5.2) coinciden.*

Ejemplos 2.5.4 *Subanillos e ideales generados por conjuntos.*

1. Si A es un anillo, el ideal generado por $\emptyset$ es el ideal trivial, y el subanillo generado por $\emptyset$ es el subanillo primo (ver los Ejemplos 2.3.3).

2. Si b es un elemento de un anillo A, el ideal generado por $\{b\}$ es $bA = (b)$ (ver los Ejemplos 2.4.2).

3. Si m es un entero que no es un cuadrado, el subanillo de $\mathbb{C}$ generado por $\sqrt{m}$ es el anillo $\mathbb{Z}[\sqrt{m}]$.

4. Si X es un subanillo (respectivamente, un ideal) de A entonces el subanillo (respectivamente, el ideal) que genera es el propio X.

Ejercicio 2.5.5 *Demostrar que el conjunto*

$$I = \{a + bi : a \equiv b \bmod 2\}$$

es el ideal principal de $\mathbb{Z}[i]$ generado por el elemento $1+i$. (Indicación: Usar la igualdad $2 = (1+i)(1-i)$.)

Ya hemos observado que, en general, la unión de ideales no es un ideal, así que es razonable considerar los ideales generados por esas uniones. Comenzamos con un ejercicio que resuelve el caso finito, y pasaremos luego al caso general.

Ejercicio 2.5.6 *Sean I y J ideales de un anillo A. Demostrar que el ideal de A generado por la unión $I \cup J$ es*

$$I + J = \{x + y : x \in I, y \in J\}.$$

Generalizar este resultado considerando un número finito de ideales $B_1, \ldots, B_n$.

Un primer intento de generalizar la primera parte del ejercicio anterior al caso de familias infinitas de ideales puede llevarnos a la consideración de sumas infinitas, que no están definidas. Esto se resuelve fácilmente como sigue: Diremos que una propiedad se cumple *para casi todos* los elementos de un conjunto X si se cumple para todos los elementos de X, salvo para una cantidad finita. Por ejemplo, si $\{a_x : x \in X\}$ es una familia de elementos de un grupo abeliano, diremos que $a_x = 0$ para casi todo $x \in X$ (o que casi todos los a_x son nulos) si el conjunto $\{x \in X : a_x \neq 0\}$ es finito. En este caso tiene sentido considerar la suma infinita $\sum_{x \in X} a_x$ interpretada como la suma de los elementos a_x distintos de cero.

Proposición 2.5.7 *Sea $\{I_t : t \in T\}$ una familia de ideales de un anillo A. Entonces el subconjunto definido por*

$$\sum_{t\in T} I_t = \{\sum_{t\in T} x_t : x_t \in I_t \text{ para cada } t \in T \text{ y } x_t = 0 \text{ para casi todo } t \in T\}$$

(llamado la suma de los ideales $\{I_t : t \in T\}$*) coincide con el ideal generado por la unión $\cup_{t\in T} I_t$; es decir, es el menor ideal de A que contiene a cada uno de los I_t. Con la notación anterior*

$$\sum_{t\in T} I_t = (\cup_{t\in T} I_t).$$

Demostración. Se trata de ver que el conjunto definido es el menor ideal de A que contiene a $\cup_{t\in T} I_t$; es decir, hay que comprobar tres cosas:

1. $\sum_{t\in T} I_t$ es un ideal de A.
2. $\sum_{t\in T} I_t$ contiene a $\cup_{t\in T} I_t$.
3. Cualquier ideal de A que contenga a $\cup_{t\in T} I_t$ debe contener a $\sum_{t\in T} I_t$.

Las tres demostraciones son elementales y se dejan a cargo del lector. □

Ejercicio 2.5.8 *Si A es un anillo y X es un subconjunto, demostrar que el ideal generado por X es $\sum_{x\in X} xA$; es decir, el ideal formado por todas las combinaciones A-lineales de elementos de X.*

Ejemplo 2.5.9 *Un ideal que no es principal.*

El ideal J de $\mathbb{Z}[X]$ descrito en los Ejemplos 2.4.2, consistente en los polinomios con coeficiente independiente par, está generado por el conjunto $\{2, X\}$; es decir, $J = (2, X)$. Vamos a ver que, de hecho, J no es un ideal principal. Para ello, llegaremos a una contradicción suponiendo que existe un polinomio $p \in \mathbb{Z}[X]$ tal que $J = (p)$. En efecto, en ese caso se tendría $p \in J$ y por tanto $p = 2a_0 + a_1X + a_2X^2 + \cdots$ para ciertos enteros a_i. Pero también se tendría $2 \in (p)$ y $X \in (p)$, lo que significa que existen enteros b_i y c_i tales que

$$\begin{array}{rcll} 2 & = & p(b_0 + b_1X + \cdots) & = 2a_0b_0 + (2a_0b_1 + a_1b_0)X + \cdots \\ X & = & p(c_0 + c_1X + \cdots) & = 2a_0c_0 + (2a_0c_1 + a_1c_0)X + \cdots \end{array}$$

Comparando términos independientes en las igualdad obtenemos $a_0b_0 = 1$, de donde $a = \pm 1$, y $a_0c_0 = 0$, de donde $c_0 = 0$. Comparando ahora los coeficientes de X en la segunda igualdad obtenemos $1 = 2a_0c_1 + a_1c_0 = 2a_0c_1$, lo que nos da la contradicción buscada.

Terminamos la sección considerando los productos de ideales. Dados dos ideales I y J de un anillo A, parece natural definir su producto como el conjunto T de todos los elementos de la forma ab con $a \in I$ y $b \in J$. Sin embargo este conjunto no es, en general, cerrado para sumas. Por ejemplo, si $A = \mathbb{Z}[X]$ e $I = J$ consiste en los polinomios con término independiente par, entonces los polinomios $2(2 + X) = 4 + 2X$ y X^2 están en T, pero su suma $4 + 2X + X^2$ no está en T, pues una igualdad

$$\begin{array}{rcl} 4 + 2X + X^2 & = & (2a_0 + a_1X + a_2X^2 + \cdots)(2b_0 + b_1X + b_2X^2 + \cdots) \\ & = & 4(a_0b_0) + 2(a_0b_1 + a_1b_0)X + (2a_0b_2 + a_1b_1 + 2a_2b_0)X^2 + \cdots \end{array}$$

implicaría $a_0 = b_0 = \pm 1$ y por tanto $a_1 + b_1 = \pm 1$, por lo que a_1b_1 sería par, y en consecuencia lo sería $1 = 2a_0b_2 + a_1b_1 + 2a_2b_0$, lo que supone una contradicción.

Por tanto hay que ser algo más sutil en la definición del producto de ideales.

Definición 2.5.10 *Sea A un anillo con ideales I y J. El producto de ambos, denotado IJ, es el ideal de A generado por los elementos de la forma ab con $a \in I$ y $b \in J$.*

Ejercicio 2.5.11 *Sean $I, J, K, I_1, \ldots, I_r$ ideales de un anillo A. Demostrar:*

1. *El ideal producto IJ consiste en las sumas finitas de elementos de la forma ab con $a \in I$ y $b \in J$. Es decir,*
$$IJ = \{\sum_{i=1}^{n} a_i b_j : n \in \mathbb{Z}^+, a_i \in I, b_i \in J\}.$$
2. *Si $I = (a)$ es un ideal principal, entonces $IJ = \{ab : b \in J\}$. En particular, si $I = (a)$ y $J = (b)$ son principales, entonces $IJ = (ab)$ es principal.*
3. *Se verifica $IJ \subseteq I \cap J$, y la igualdad se da si $I + J = A$.*
4. *El producto de ideales es asociativo; es decir, $I(JK) = (IJ)K$. Esto permite definir sin ambigüedad el producto de un número finito de ideales, $I_1 \cdots I_r$, y se verifica*
$$I_1 \cdots I_r = \{\sum_{i=1}^{n} a_{i,1} \cdots a_{i,r} : n \in \mathbb{Z}^+, a_{i,j} \in I_j\}.$$

2.6 Homomorfismos

En Matemáticas se suele llamar *homomorfismo* entre dos objetos A y B con una estructura a una aplicación $f : A \to B$ que conserva la estructura. Por supuesto, la frase es bastante ambigua porque no hemos dicho qué significa la palabra "estructura" ni la expresión "conservar la estructura", y en cada caso hemos de dar una definición explícita.

Definición 2.6.1 *Sean A y B dos anillos. Un* homomorfismo de anillos *entre A y B es una aplicación $f : A \to B$ que conserva las operaciones y la unidad; es decir, que satisface*
$$f(x + y) = f(x) + f(y), \qquad f(x \cdot y) = f(x) \cdot f(y)$$
para cada par de elementos $x, y \in A$ y
$$f(1) = 1.$$
Un endomorfismo *de A es un homomorfismo de un anillo de A en sí mismo.*

En la definición anterior hemos usado el mismo símbolo para las operaciones y los neutros en los dos anillos que intervienen. Por ejemplo, para calcular $f(x+y)$ primero hay que sumar x con y en A y luego aplicarle f al resultado, mientras que en $f(x) + f(y)$ primero hay que calcular las imágenes de x e y por f y luego hay que sumar éstas en B. Usualmente el contexto hace evidente a qué operación o a qué neutro nos referimos en cada caso, así que mantendremos estos abusos de notación y dejaremos que el lector analice cada caso. Análogamente, las unidades de la ecuación $f(1) = 1$ están en dos anillos probablemente diferentes y por tanto son objetos distintos, que sin embargo denotamos igual.

La condición $f(x + y) = f(x) + f(y)$ suele leerse como *la imagen de la suma es la suma de las imágenes*, o también como *f conserva sumas*. Del mismo modo se habla de aplicaciones que *conservan productos* o que *conservan identidades*.

A continuación establecemos ciertas propiedades elementales de los homomorfismos de anillos. Demostramos algunas y dejamos el resto como ejercicio para el lector.

Proposición 2.6.2 *Sea $f : A \to B$ un homomorfismo de anillos. Entonces se verifican las siguientes propiedades para $a, b, a_1, \ldots, a_n \in A$:*

1. (f conserva ceros) $f(0) = 0$.
2. (f conserva opuestos) $f(-a) = -f(a)$.
3. (f conserva restas) $f(a - b) = f(a) - f(b)$.
4. (f conserva sumas finitas) $f(a_1 + \cdots + a_n) = f(a_1) + \cdots + f(a_n)$.
5. (f conserva múltiplos enteros) *Si $n \in \mathbb{Z}$ entonces* $f(na) = nf(a)$.

6. (f conserva inversos) *Si a es invertible, entonces $f(a)$ es invertible y $f(a)^{-1} = f(a^{-1})$.*
7. (f conserva productos finitos) $f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$.
8. *Si A_1 es un subanillo de A, entonces $f(A_1)$ es un subanillo de B.*
9. *Si B_1 es un subanillo de B, entonces $f^{-1}(B_1)$ es un subanillo de A.*
10. *Si X es un ideal de B, entonces $f^{-1}(X)$ es un ideal de A.*
11. *Si I es un ideal de A y f es suprayectiva, entonces $f(I)$ es un ideal de B.*

Demostración. Para ver 1 basta con aplicar la propiedad de cancelación a la igualdad $0 + f(0) = f(0+0) = f(0) + f(0)$. 2 se tiene porque $f(a) + f(-a) = f(a + (-a)) = f(0) = 0$, y entonces 3 es claro. 4 se demuestra por inducción; el caso $n = 2$ no es más que la definición de homomorfismo y el caso general se reduce a éste notando que $a_1 + \cdots + a_n = (a_1 + \cdots + a_{n-1}) + a_n$. □

Ejercicio 2.6.3 *Comprobar que la hipótesis de suprayectividad en el apartado 11 de la Proposición 2.6.2 no es superflua; es decir, dar un ejemplo de un homomorfismo de anillos $f : A \to B$ y un ideal I de A, tal que $f(I)$ no es un ideal de B.*

Observación 2.6.4 En la Proposición 2.6.2 hemos visto que la conservación de sumas implica la conservación del neutro para la suma, pero no hemos podido adaptar la demostración al caso de productos (¿por qué?); de hecho, en seguida veremos ejemplos de aplicaciones entre anillos que conservan sumas y productos pero no identidades.

Ejemplos 2.6.5 *Homomorfismos de anillos.*

1. Si A y B son anillos, la aplicación $f : A \to B$ dada por $f(a) = 0$ para cada $a \in A$ *no* es un homomorfismo de anillos salvo que $B = 0$. Este homomorfismo se llama *homomorfismo cero* u *homomorfismo trivial*. Obsérvese que no hay ningún homomorfismo $0 \to B$, salvo que B sea 0.

   He aquí otro ejemplo menos trivial de anillos entre los que no hay homomorfismos: la existencia de un homomorfismo de anillos $f : \mathbb{Z}_2 \to \mathbb{Z}_3$ nos llevaría al absurdo

   $$[0]_3 = f([0]_2) = f([1]_2 + [1]_2) = f([1]_2) + f([1]_2) = [1]_3 + [1]_3 = [2]_3.$$

2. Sea A un un anillo con un subanillo B. Entonces la aplicación de inclusión $u : B \hookrightarrow A$, dada por $u(b) = b$, es un homomorfismo. En particular, la aplicación identidad $1_A : A \to A$ es un homomorfismo.

3. Sea A un anillo con un ideal I. Entonces la *proyección* (o *proyección canónica*) $\pi : A \to A/I$, dada por $\pi(a) = a + I$, es un homomorfismo. Obsérvese que parte de la demostración del Teorema de la Correspondencia puede verse como un caso particular de la Proposición 2.6.2 aplicada a la proyección π.

4. Si A es un anillo, la aplicación $\mu : \mathbb{Z} \to A$ dada por $\mu(n) = n1$ (es decir, la aplicación consistente en multiplicar por 1) es un homomorfismo de anillos. De hecho, es el único homomorfismo de anillos $f : \mathbb{Z} \to A$ (¿por qué es el único?).

5. Si A y B son anillos, la aplicación $p_A : A \times B \to A$ dada por $p_A(a, b) = a$ es un homomorfismo llamado *proyección en la primera coordenada*, y de modo análogo se tiene una proyección en la segunda coordenada.

   Dado un producto arbitrario de anillos, debe estar claro cómo se generaliza este ejemplo para definir la proyección en cada coordenada.

6. Dados $a, b \in \mathbb{R}$, el *conjugado* del número complejo $z = a + bi$ es $\bar{z} = a - bi$, y la aplicación *conjugación* $\mathbb{C} \to \mathbb{C}$ dada por $z \mapsto \bar{z}$ es un homomorfismo de anillos.

   Análogamente, si d es un entero que no sea un cuadrado entonces el conjugado $a - b\sqrt{d}$ de $a + b\sqrt{d}$ (elementos de $\mathbb{Q}[\sqrt{d}]$ o de $\mathbb{Z}[\sqrt{d}]$) está bien definido y la conjugación $\mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[\sqrt{d}]$ ó $\mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ es un homomorfismo de anillos.

7. Sea A un anillo y sea $b \in A$. Entonces la aplicación

$$\begin{array}{ccc} A[X] & \xrightarrow{S_b} & A \\ P = a_0 + a_1X + \cdots + a_nX^n & \mapsto & P(b) = a_0 + a_1b + \cdots + a_nb^n \end{array}$$

es un homomorfismo de anillos llamado *homomorfismo de sustitución* en b. En particular, el homomorfismo de sustitución en 0 lleva cada polinomio a su coeficiente independiente.

Hemos visto que, si $f : A \to B$ es un homomorfismo de anillos, entonces $f(A)$ es un subanillo de B, y es evidente que f es suprayectivo precisamente cuando $f(A) = B$. Más generalmente, podemos decir que cuanto mayor es $f(A)$ más cerca está f de ser suprayectivo. En el otro extremo, $f^{-1}(0)$ es un ideal de A que nos va a servir para determinar si f es o no inyectivo.

Definición 2.6.6 *Sea $f : A \to B$ un homomorfismo de anillos; llamamos* imagen *y* núcleo *de f, respectivamente, a los conjuntos*

$$\text{Im } f = f(A) = \{f(a) : a \in A\} \qquad \text{Ker } f = f^{-1}(0) = \{a \in A : f(a) = 0\}$$

(la notación para el núcleo procede de la voz germánica Kernel*). En general* Im f *es un subanillo de B y* Ker f *es un ideal de A.*

Proposición 2.6.7 *Un homomorfismo de anillos $f : A \to B$ es inyectivo precisamente si* Ker $f = 0$.

Demostración. Si f es inyectivo, entonces $f^{-1}(a)$ tiene a lo sumo un elemento, para todo $a \in A$. En particular Ker $f = f^{-1}(0)$ tiene exactamente un elemento, a saber 0.

Recíprocamente, supongamos que Ker $f = 0$ y sean $a, b \in A$ tales que $a \neq b$. Entonces $f(a) - f(b) = f(a - b) \neq 0$; es decir, $f(a) \neq f(b)$, y por tanto f es inyectiva. □

2.7 Isomorfismos y Teoremas de Isomorfía

Ejercicio 2.7.1 *Demostrar que, si $f : A \to B$ y $g : B \to C$ son homomorfismos de anillos, entonces su composición $g \circ f : A \to C$ es también un homomorfismo. Además se verifican los siguientes enunciados (que de hecho son ciertos para aplicaciones entre conjuntos, no sólo para homomorfismos de anillos):*

1. *Si f y g son ambas inyectivas entonces $g \circ f$ es inyectiva.*
2. *Si f y g son ambas suprayectivas entonces $g \circ f$ es suprayectiva.*
3. *Si f y g son ambas biyectivas entonces $g \circ f$ es biyectiva.*
4. *Si $g \circ f$ es inyectiva entonces f es inyectiva.*
5. *Si $g \circ f$ es suprayectiva entonces g es suprayectiva.*

Definición 2.7.2 *Un homomorfismo de anillos $f : A \to B$ que sea biyectivo se llama un* isomorfismo *de anillos. Un* automorfismo *es un endomorfismo biyectivo. Si existe un isomorfismo $f : A \to B$, se dice que los anillos A y B son* isomorfos*, situación que se denota por $A \cong B$.*

Conforme vayamos estudiando propiedades de los anillos y de sus elementos, veremos que los isomorfismos *conservan esas propiedades* en un sentido que estará claro en cada caso. Como consecuencia, dos anillos isomorfos tendrán las mismas propiedades y deberán ser considerados como *esencialmente iguales.*

Proposición 2.7.3 *Si $f : A \to B$ es un isomorfismo de anillos, entonces la aplicación inversa $f^{-1} : B \to A$ también lo es. En consecuencia, la relación* ser isomorfos *es una relación de equivalencia en la clase de todos los anillos.*

Demostración. Sean $x, y \in B$; entonces

$$f(f^{-1}(x+y)) = x + y = f(f^{-1}(x)) + f(f^{-1}(y)) = f(f^{-1}(x) + f^{-1}(y)),$$

y como f es inyectiva esto implica que $f^{-1}(x+y) = f^{-1}(x) + f^{-1}(y)$. De igual modo se ve que f^{-1} conserva productos e identidades. Como además f^{-1} es biyectiva, deducimos que es un isomorfismo.

Como las identidades son isomorfismos, la relación de isomorfía es reflexiva, mientras que es simétrica por la primera parte de esta proposición y es transitiva por el Ejercicio 2.7.1. □

En el Capítulo 1 hemos introducido los números enteros de forma axiomática. Es decir, por definición, los números enteros forman un objeto que satisface una lista de axiomas. ¿Cuántos conjuntos de números enteros hay? Es decir, ¿cuántos objetos hay que satisfagan los axiomas de la Sección 1.1? En realidad hay muchos. En efecto, si $f : A \to \mathbb{Z}$ es una aplicación biyectiva y definimos en A las operaciones

$$a + b = f^{-1}(f(a) + f(b)), \qquad ab = f^{-1}(f(a) \cdot f(b))$$

y el orden

$$a \leq b \Leftrightarrow f(a) \leq f(b),$$

entonces es fácil ver que A satisface los axiomas de la Sección 1.1 y por tanto es *un* conjunto de números enteros. En tal caso, ¿qué nos permite hablar de *el* conjunto de los números enteros utilizando el artículo determinado? En este momento debe estar claro que la respuesta a esta pregunta es que todos los conjuntos que satisfacen los axiomas de la Sección 1.1 son isomorfos. Esto es consecuencia del apartado 4 del Ejemplo 2.6.5. Éste es un modo típico de trabajo con el método axiomático: se define un objeto matemático en función de sus propiedades básicas y eventualmente se prueba que dicho objeto es "esencialmente único"; es decir, que todos los objetos que satisfacen dichas propiedades son isomorfos. Veremos otro ejemplo de este modo de actuar al final de la Sección 2.8.

Los siguientes resultados establecen la existencia de ciertos isomorfismos de anillos que usaremos con frecuencia.

Teorema 2.7.4 (Primer Teorema de Isomorfía) *Sea $f : A \to B$ un homomorfismo de anillos. Entonces existe un único isomorfismo de anillos $\bar{f} : A/\mathrm{Ker}\ f \to \mathrm{Im}\ f$ que hace conmutativo el diagrama*

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ A/\mathrm{Ker}\ f & \xrightarrow{\quad \bar{f} \quad} & \mathrm{Im}\ f \end{array}$$

es decir, $i \circ \bar{f} \circ p = f$, donde i es la inclusión y p es la proyección. En particular

$$\frac{A}{\mathrm{Ker}\ f} \cong \mathrm{Im}\ f.$$

Demostración. Sean $K = \mathrm{Ker}\ f$ e $I = \mathrm{Im}\ f$. La aplicación $\bar{f} : A/K \to I$ dada por $\bar{f}(x + K) = f(x)$ está bien definida (no depende de representantes) pues si $x+K = y+K$ entonces $x-y \in K$ y por lo tanto $f(x) - f(y) = f(x-y) = 0$; es decir, $f(x) = f(y)$. Además es elemental ver que es un homomorfismo de anillos y que es suprayectiva. Para ver que es inyectiva usamos la Proposición 2.6.7: si $x + K$ está en el núcleo de $\bar{f}$ entonces $0 = \bar{f}(x + K) = f(x)$, de modo que $x \in K$ y así $x + K = 0 + K$. Es decir $\mathrm{Ker}\ \bar{f} = 0$ y por lo tanto $\bar{f}$ es inyectiva. En conclusión, $\bar{f}$ es un isomorfismo, y hace conmutativo el diagrama porque, para cada $x \in K$, se tiene

$$i(\bar{f}(p(x))) = \bar{f}(x + K) = f(x).$$

En cuanto a la unicidad, supongamos que otro homomorfismo $\widehat{f} : A/K \to I$ verifica $i \circ \widehat{f} \circ p = f$; entonces para cada $x \in K$ se tiene $\widehat{f}(x + K) = i(\widehat{f}(p(x))) = f(x) = \bar{f}(x + K)$, y por lo tanto $\widehat{f} = \bar{f}$. □

Teorema 2.7.5 (Segundo Teorema de Isomorfía) *Sea A un anillo y sean I y J dos ideales tales que $I \subseteq J$. Entonces J/I es un ideal de A/I y existe un isomorfismo de anillos*

$$\frac{A/I}{J/I} \cong \frac{A}{J}.$$

Demostración. Por el Teorema de la Correspondencia 2.4.8, J/I es un ideal de A/I. Sea $f : A/I \to A/J$ la aplicación definida por $f(a+I) = a+J$. Es elemental ver que f está bien definida, que es un homomorfismo suprayectivo de anillos y que Ker $f = J/I$. Entonces el isomorfismo buscado se obtiene aplicando el Primer Teorema de Isomorfía a f. □

Teorema 2.7.6 (Tercer Teorema de Isomorfía) *Sea A un anillo con un subanillo B y un ideal I. Entonces:*

1. *$B \cap I$ es un ideal de B.*
2. *$B + I$ es un subanillo de A que contiene a I como ideal.*
3. *Se tiene un isomorfismo de anillos $\dfrac{B}{B \cap I} \cong \dfrac{B+I}{I}$.*

Demostración. Los dos primeros apartados se dejan como ejercicio. En cuanto al último, sea $f : B \to A/I$ la composición de la inclusión $j : B \to A$ con la proyección $p : A \to A/I$. Es claro que Ker $f = B \cap I$ y que Im $f = (B+I)/I$, por lo que el resultado se sigue del Primer Teorema de Isomorfía. □

Ejemplos 2.7.7 *Aplicaciones del Primer Teorema de Isomorfía.*

1. Si A y B son anillos, el homomorfismo $A \times B \to A$ de proyección en la primera componente es suprayectivo y tiene núcleo $I = 0 \times B$, por lo que $\frac{A \times B}{0 \times B} \cong A$.
2. Si A es un anillo, el homomorfismo $f : A[X] \to A$ de sustitución en 0 (dado por $a_0 + a_1X + \cdots \mapsto a_0$) es suprayectivo y tiene por núcleo el ideal (X) generado por X (consistente en los polinomios con coeficiente independiente nulo), de modo que $A[X]/(X) \cong A$, como ya habíamos observado en los Ejemplos 2.4.6.
3. Sean A un anillo e I un ideal de A. Para cada $a \in A$, sea $\overline{a} = a + I$. La aplicación $f : A[X] \to (A/I)[X]$ dada por $f(a_0 + a_1X + \cdots + a_nX^n) = \overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n$ es un homomorfismo suprayectivo de anillos cuyo núcleo es $I[X] = \{a_0 + a_1X + \cdots + a_nX^n : a_i \in I\}$. Del Primer Teorema de Isomorfía se deduce que $(A/I)[X] \cong A[X]/I[X]$.

Definición 2.7.8 *Sea A un anillo, y recordemos que si $n \in \mathbb{Z}^+$ escribimos $n1 = 1 + \cdots + 1$ (n veces). Si existe $n \in \mathbb{Z}^+$ tal que $n1 = 0$, definimos la* característica *de A como el menor $n \in \mathbb{Z}^+$ que verifica tal igualdad. Si no existe un tal n, decimos que la característica de A es 0.*

Proposición 2.7.9 *Sea A un anillo A y sea $f : \mathbb{Z} \to A$ el único homomorfismo de anillos (dado por $f(n) = n1$). Para un número natural n las condiciones siguientes son equivalentes:*

1. *n es la característica de A.*
2. *$n\mathbb{Z}$ es el núcleo de f.*
3. *El subanillo primo de A es isomorfo a $\mathbb{Z}_n$ (recuérdese que $\mathbb{Z}_0 = \mathbb{Z}$ y $\mathbb{Z}_1 = 0$).*
4. *A contiene un subanillo isomorfo a $\mathbb{Z}_n$.*

Demostración. La equivalencia entre 1 y 2 se deja como ejercicio para el lector, y es obvio que 3 implica 4.

2 implica 3. Se obtiene aplicando el Primer Teorema de Isomorfía y observando que Im f es el subanillo primo de A.

4 implica 2. Si B es un subanillo de A y $g : \mathbb{Z}_n \to B$ es un isomorfismo, considerando la proyección $\pi : \mathbb{Z} \to \mathbb{Z}_n$ y la inclusión $u : B \hookrightarrow A$ se obtiene un homomorfismo de anillos $u \circ g \circ \pi : \mathbb{Z} \to A$ que debe coincidir con f por su unicidad (Ejemplos 2.6.5). Como $u \circ g$ es inyectiva, es elemental ver que Ker $f = n\mathbb{Z}$. □

Terminamos esta sección generalizando el Teorema Chino de los Restos (1.7.4) a anillos arbitrarios.

Teorema 2.7.10 (Teorema Chino de los Restos) *Sea A un anillo y sean $I_1, \ldots, I_n$ ideales de A tales que $I_i + I_j = A$ para todo $i \neq j$. Entonces $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. Además*

$$\frac{A}{I_1 \cap \cdots \cap I_n} \cong \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}.$$

Demostración. Razonamos por inducción sobre n, empezando con el caso $n = 2$. La hipótesis $I_1 + I_2 = A$ nos dice que existen $x_1 \in I_1$ y $x_2 \in I_2$ tales que $x_1 + x_2 = 1$, y entonces para cada $a \in I_1 \cap I_2$ se tiene $a = ax_1 + ax_2 \in I_1 I_2$, de modo que $I_1 \cap I_2 \subseteq I_1 I_2$, y la otra inclusión es clara. Claramente la aplicación $f : A \to A/I_1 \times A/I_2$ dada por $f(a) = (a + I_1, a + I_2)$ es un homomorfismo de anillos con núcleo $I_1 \cap I_2$, y es suprayectiva pues, dado un elemento arbitrario $(a_1 + I_1, a_2 + I_2)$ de $A/I_1 \times A/I_2$, el elemento $a = a_1 x_2 + a_2 x_1$ verifica $f(a) = (a_1 + I_1, a_2 + I_2)$. Ahora el resultado se obtiene aplicando el Primer Teorema de Isomorfía.

En el caso general ($n > 2$) basta ver que las hipótesis implican que $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$, pues entonces la hipótesis de inducción nos da

$$I_1 \cap \cdots \cap I_{n-1} \cap I_n = (I_1 \cap \cdots \cap I_{n-1}) I_n = I_1 \cdots I_{n-1} I_n$$

y

$$\frac{A}{I_1 \cap \cdots \cap I_n} = \frac{A}{(\cap_{i=1}^{n-1} I_i) \cap I_n} \cong \frac{A}{\cap_{i=1}^{n-1} I_i} \times \frac{A}{I_n} \cong \frac{A}{I_1} \times \cdots \times \frac{A}{I_{n-1}} \times \frac{A}{I_n}.$$

Para ver que $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$ notemos que, para cada $i \leq n-1$, existen $a_i \in I_i$ y $b_i \in I_n$ tales que $1 = a_i + b_i$, y multiplicando todas esas expresiones se obtiene

$$1 = \Pi_{i=1}^{n-1}(a_i + b_i) = a_1 \cdots a_{n-1} + b,$$

donde b engloba a todos los sumandos que se obtendrían desarrollando los productos (excepto $a_1 \cdots a_{n-1}$) y está en I_n porque en cada sumando hay al menos un factor del ideal I_n. Como además $a_1 \cdots a_{n-1} \in I_1 \cap \cdots \cap I_{n-1}$, deducimos que $1 \in (I_1 \cap \cdots \cap I_{n-1}) + I_n$ y así $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$, como queríamos ver. □

2.8 Cuerpos y dominios; ideales maximales y primos

En esta sección suponemos que, en todos los anillos que aparecen, el 1 es distinto del 0.

Definición 2.8.1 *Un elemento a de un anillo A se dice* regular *si la relación $ab = ac$ con $b, c \in A$ implica que $b = c$; es decir, si a es* cancelable *para el producto en el sentido de la Definición 2.1.2.*

Claramente, el 0 nunca es cancelable[7]*. Un* cuerpo *es un anillo en el que todos los elementos no nulos son invertibles, y un* dominio *(o* dominio de integridad*) es un anillo en el que todos los elementos no nulos son regulares.*

Como todo elemento invertible es regular (Ejercicio 2.1.4), tenemos:

Proposición 2.8.2 *Todo cuerpo es un dominio.*

[7] Obsérvese la importancia de la hipótesis $1 \neq 0$ en este caso.

Otras propiedades que se demuestran fácilmente quedan recogidas en el siguiente ejercicio:

Ejercicio 2.8.3 *Si A es un anillo, demostrar que:*

1. *Las condiciones siguientes son equivalentes (usar el Ejercicio 2.4.7, la Proposición 2.6.7 y las proyecciones $A \to A/I$):*
   (a) *A es un cuerpo.*
   (b) *Los únicos ideales de A son 0 y A.*
   (c) *Todo homomorfismo de anillos $A \to B$ es inyectivo.*
2. *Un elemento $a \in A$ es regular si y sólo si la relación $ab = 0$ con $b \in A$ implica $b = 0$ (por este motivo, los elementos no regulares se suelen llamar* divisores de cero*).*
3. *A es un dominio si y sólo si, para cualesquiera $a, b \in A$ no nulos, se tiene $ab \neq 0$.*
4. *Todo subanillo de un dominio es un dominio.*
5. *La característica de un dominio es cero o un número primo.*

Ejemplos 2.8.4 *Dominios y cuerpos.*

1. Los anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos y $\mathbb{Z}$ es un dominio que no es un cuerpo (aunque es subanillo de un cuerpo).
2. Para $n \geq 2$, el anillo $\mathbb{Z}_n$ es un dominio si y sólo si es un cuerpo, si y sólo si n es primo (¿por qué?).
3. Si $m \in \mathbb{Z}$ no es un cuadrado entonces $\mathbb{Z}[\sqrt{m}]$ es un dominio (subanillo de $\mathbb{C}$) que no es un cuerpo (el 2 no tiene inverso). Sin embargo, $\mathbb{Q}[\sqrt{m}]$ sí que es un cuerpo; de hecho, si $a + b\sqrt{m} \neq 0$, entonces $q = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - b^2 m$ es un número racional no nulo (¿por qué?) y $aq^{-1} - bq^{-1}\sqrt{m}$ es el inverso de $a + b\sqrt{m}$.
4. Un producto de anillos $A \times B$ nunca es un dominio, pues $(1,0)(0,1) = (0,0)$.
5. Los anillos de polinomios no son cuerpos, pues la indeterminada genera un ideal propio y no nulo.

   Por otra parte, $A[X]$ es un dominio si y sólo si lo es A. Una implicación es clara, pues A es un subanillo de $A[X]$. La otra se sigue del siguiente resultado, interesante en sí mismo, que el lector puede intentar demostrar (véase el Ejercicio 4.1.2): Si A es un dominio y P, Q son polinomios de $A[X]$ de grados n y m, entonces el grado del producto PQ es $n + m$.

Definición 2.8.5 *Sean A un anillo e I un ideal propio de A.*
Se dice que I es maximal *si no está contenido en ningún ideal propio (excepto en sí mismo).*
Se dice que I es primo *si, para todo $a, b \in A$, la relación $ab \in I$ implica $a \in I$ ó $b \in I$.*

De la Proposición 1.5.1 se deduce que los ideales maximales de $\mathbb{Z}$ son los ideales principales generados por números primos, y sus ideales primos son los anteriores junto con el ideal trivial 0.

Proposición 2.8.6 *Sean A un anillo e I un ideal propio de A. Entonces:*

1. *I es maximal precisamente si A/I es un cuerpo.*
2. *I es primo precisamente si A/I es un dominio.*
3. *Si I es maximal entonces es primo.*
4. *A es un cuerpo precisamente si el ideal 0 es maximal.*
5. *A es un dominio precisamente si el ideal 0 es primo.*

Demostración. El apartado 1 es consecuencia inmediata del primer apartado del Ejercicio 2.8.3 y del Teorema de la Correspondencia 2.4.8. Para ver 2, supongamos que I es primo y sean $a+I, b+I$ dos elementos no nulos de A/I; entonces $a, b \notin I$ y por lo tanto $ab \notin I$, luego $(a+I)(b+I) = ab + I \neq 0$ y en consecuencia A/I es un dominio. El recíproco se demuestra usando la misma idea, y el resto de apartados se deducen de estos dos y de la Proposición 2.8.2. □

A continuación estudiamos algunas propiedades de los ideales primos y maximales.

Ejercicio 2.8.7 *Si I es un ideal propio del anillo A, las biyecciones del Teorema de la Correspondencia llevan ideales maximales (respectivamente primos) de A que contienen a I a ideales maximales (respectivamente primos) de A/I, y viceversa. (Indicación: Usar la Proposición 2.8.6 y el Segundo Teorema de Isomorfía.)*

Ejercicio 2.8.8 *Sea $f : A \to B$ un homomorfismo de anillos. Demostrar que:*

1. *Si p es un ideal primo de B, entonces $f^{-1}(p)$ es un ideal primo de A.*
2. *En general, no se verifica el resultado análogo para ideales maximales. (Indicación: Considerar la inclusión de $\mathbb{Z}$ en $\mathbb{Q}$.)*

La siguiente proposición proporciona nueva una caracterización de los ideales primos.

Proposición 2.8.9 *Un ideal P de un anillo A es primo precisamente si para cada dos ideales I y J de A, si $IJ \subseteq P$ entonces $I \subseteq P$ ó $J \subseteq P$.*

Demostración. Supongamos que P no es primo. Entonces existen $a, b \in A \setminus P$ tales que $ab \in P$, de modo que el ideal $(a)(b) = (ab)$ está incluido en P mientras que (a) y (b) no lo están.

Recíprocamente, supongamos que P es un ideal primo y que I y J son ideales de A no contenidos en P. Entonces existen $a \in I \setminus P$ y $b \in J \setminus P$, por lo que $ab \in IJ \setminus P$ y así $IJ \not\subseteq P$. □

De la Proposición 2.8.9 y de la inclusión $IJ \subseteq I \cap J$ se deduce:

Corolario 2.8.10 *Sea P un ideal primo de un anillo A y sean I y J ideales de A tales que $I \cap J \subseteq P$. Entonces $I \subseteq P$ ó $J \subseteq P$.*

El recíproco del Corolario 2.8.10 no se verifica. Por ejemplo, el ideal (4) de $\mathbb{Z}$ no es primo. Sin embargo para cada dos ideales I y J de $\mathbb{Z}$ tales que $I \cap J \subseteq (4)$ se verifica que $I \subseteq (4)$ ó $J \subseteq (4)$.

Terminamos la sección con un resultado que se sale de los objetivos de este curso, pero que incluimos aquí por su importancia en Teoría de Anillos. Se trata del hecho, nada evidente, de que todo anillo posee ideales maximales. Para demostrar este tipo de resultados "de existencia" suele ser útil el siguiente Lema de Zorn, que es un resultado fundamental de Teoría de Conjuntos. Por desgracia, su demostración requiere herramientas de las que carecemos en este momento. Necesitamos además una definición previa.

Un conjunto ordenado $(A, \leq)$ se dice que es *inductivo* si toda *cadena* (o subconjunto linealmente ordenado) B de A posee una cota superior en A.

Teorema 2.8.11 (Lema de Zorn) *Todo conjunto ordenado no vacío e inductivo tiene un elemento maximal.*

Teorema 2.8.12 *Todo ideal propio J de un anillo A está contenido en un ideal maximal de A. En particular, tomando $J = 0$, todo anillo tiene al menos un ideal maximal.*

Demostración. Sea X el conjunto de los ideales propios de A que contienen a J, ordenado por inclusión. Como X no es vacío (J es un elemento suyo), si vemos que es inductivo el Lema de Zorn nos dirá que X posee un elemento maximal, que claramente será el ideal postulado en el enunciado.

Sea pues $\{I_t\}_{t \in T}$ una cadena de X, y sea $I = \cup_{t \in T} I_t$. Vamos a demostrar que I está en X, lo que acabará demostración ya que I es claramente una cota superior del conjunto $\{I_t\}_{t \in T}$. Se trata pues de ver que I es un ideal propio de A que contiene a J. Es obvio que I contiene a J, y también es claro que $1 \notin I$ pues los I_t son ideales propios. Sólo queda pues ver que I es un ideal.

Claramente $I \neq \emptyset$, y si $a, a' \in I$ entonces existen $t, t' \in T$ tales que $a \in I_t$ y $a' \in I_{t'}$. Como $\{I_t\}_{t \in T}$ está linealmente ordenado, podemos suponer que $I_{t'} \subseteq I_t$, y entonces cualquier combinación lineal de a y a' está en I_t y por tanto en I. Esto prueba que I es un ideal y termina la demostración. □

2.9 El cuerpo de fracciones de un dominio

En esta sección vamos a ver que todo dominio D es un subanillo de un cuerpo. De hecho existe un cuerpo que, en cierto sentido, es el menor cuerpo que contiene a D. Dicho cuerpo es único salvo isomorfismos y se llama el *cuerpo de fracciones* de D. Comenzaremos con la construcción de ese cuerpo, que es una traducción literal de la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$, y analizaremos entonces sus propiedades. En realidad, la construcción del cuerpo de fracciones es parte de una construcción más general, que presentaremos al final de la sección en una serie de ejercicios.

En esta sección, D representará un dominio. Un subanillo de un anillo A que sea un cuerpo se llama un *subcuerpo* de A, y un homomorfismo de anillos entre dos cuerpos (que ha de ser inyectivo por el Ejercicio 2.8.3) se llama *homomorfismo de cuerpos*, y también *extensión de cuerpos*.

La idea de la construcción es la de formar un cuerpo $Q(D)$ cuyos elementos sean "fracciones" del tipo a/b con $a, b \in D$ y $b \neq 0$. De este modo, D estará contenido en $Q(D)$ (identificando cada elemento a de D con la fracción $a/1$), y los elementos no nulos de $Q(D)$ serán invertibles, pues b/a será el inverso de a/b. Por supuesto, hay que definir con más rigor las fracciones y hay que dotar a $Q(D)$ de una estructura de cuerpo. El primer problema que se presenta, si pensamos en el caso $D = \mathbb{Z}$ y $Q(D) = \mathbb{Q}$, es el hecho de que dos fracciones aparentemente distintas pueden representar el mismo elemento, como en el caso $10/15 = 2/3$. Esto se resuelve identificando ciertas fracciones mediante una relación de equivalencia, y este será el primer paso en nuestra construcción.

Sean $S = D \setminus \{0\}$ y $X = D \times S$. Definimos en X la relación binaria

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow a_1 s_2 = a_2 s_1$$

que, como el lector comprobará fácilmente, es una relación de equivalencia. La clase de equivalencia de (a, s) se denota por a/s o por $\frac{a}{s}$, y el conjunto cociente $X/\sim$ (es decir, el conjunto de las clases de equivalencia para esa relación) por $Q(D)$. Dotamos a $Q(D)$ de una estructura de anillo con las siguientes operaciones:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2} \qquad \frac{a_1}{s_1}\frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}. \tag{2.9.1}$$

Hay que asegurarse de que esas definiciones no dependen de los representantes elegidos para cada fracción. Es decir, si $a_1/s_1 = b_1/t_1$ y $a_2/s_2 = b_2/t_2$, hay que comprobar que se obtiene la misma suma y el mismo producto si aplicamos las fórmulas a a_1/s_1 y a_2/s_2 que si se las aplicamos a b_1/t_1 y b_2/t_2. Las igualdades anteriores significan que $a_1 t_1 = b_1 s_1$ y $a_2 t_2 = b_2 s_2$, de donde

$$(a_1 s_2 + a_2 s_1)(t_1 t_2) = a_1 s_2 t_1 t_2 + a_2 s_1 t_1 t_2 = b_1 s_2 s_1 t_2 + b_2 s_1 t_1 s_2 = (b_1 t_2 + b_2 t_1)(s_1 s_2)$$

y por tanto $\frac{a_1 s_2 + a_2 s_1}{s_1 s_2} = \frac{b_1 t_2 + b_2 t_1}{t_1 t_2}$. Esto demuestra que la suma está bien definida, y con el producto se procede de modo análogo.

Ejercicio 2.9.1 *Dados $a, b, s, t \in D$ con $s, t \neq 0$, demostrar que:*

1. *El neutro para la suma es $0/1$. Además, la igualdad $a/s = 0/1$ se verifica si y sólo si $a = 0$.*
2. *El neutro para el producto es $1/1$. Además, la igualdad $a/s = 1/1$ se verifica si y sólo si $a = s$.*
3. *Se tiene $at/st = a/s$.*
4. *La igualdad $a/s = b/s$ se verifica si y sólo si $a = b$.*
5. *La definición de suma se simplifica cuando hay "denominador común": $a/s + b/s = (a + b)/s$.*

Usando adecuadamente el Ejercicio 2.9.1, la comprobación de que $Q(D)$ es un cuerpo es rutinaria. Demostramos como ejemplo la propiedad distributiva, y dejamos el resto para el lector:

$$\frac{a}{s}\left(\frac{b_1}{t_1} + \frac{b_2}{t_2}\right) = \frac{a}{s}\left(\frac{b_1 t_2 + b_2 t_1}{t_1 t_2}\right) = \frac{a b_1 t_2 + a b_2 t_1}{s t_1 t_2} = \frac{a b_1 t_2}{s t_1 t_2} + \frac{a b_2 t_1}{s t_1 t_2} = \frac{a b_1}{s t_1} + \frac{a b_2}{s t_2} = \frac{a}{s}\frac{b_1}{t_1} + \frac{a}{s}\frac{b_2}{t_2}.$$

Definición 2.9.2 *El cuerpo $Q(D)$ se llama* cuerpo de fracciones *o* cuerpo de cocientes *del dominio D.*

Ejemplos 2.9.3 *Cuerpos de fracciones.*

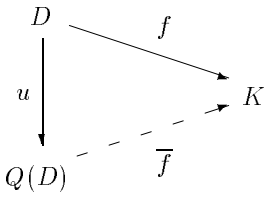
1. Obviamente, $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$.

2. Supongamos que un anillo de polinomios $A[X]$ es un dominio (lo que ocurre precisamente si A es un dominio por los Ejemplos 2.8.4). Su cuerpo de fracciones se suele denotar por $A(X)$ y se llama el *cuerpo de las funciones racionales* sobre A. Sus elementos son fracciones del tipo P/Q con $P, Q \in A[X]$, que se suman y se multiplican de forma natural.

Usando el Ejercicio 2.9.1, es sencillo ver que la aplicación $u : D \to Q(D)$ dada por $u(a) = a/1$ es un homomorfismo inyectivo de anillos, lo que nos permite ver a D como un subanillo de $Q(D)$ si identificamos cada elemento a de D con la fracción $a/1$ de $Q(D)$. El par $(Q(D), u)$ verifica una interesante propiedad:

Proposición 2.9.4 *Sean D un dominio, $Q(D)$ su cuerpo de fracciones y $u : D \to Q(D)$ la aplicación dada por $u(a) = a/1$. Entonces:*

1. **(Propiedad Universal del Cuerpo de Fracciones)** *Para toda pareja (K, f) formada por un cuerpo K y un homomorfismo inyectivo de anillos $f : D \to K$, existe una única extensión de cuerpos $\bar{f} : Q(D) \to K$ tal que $\bar{f} \circ u = f$. Se dice que $\bar{f}$* completa de modo único *el diagrama*



2. *Si dos extensiones de cuerpos $g, h : Q(D) \to K$ coinciden sobre D entonces son iguales. Es decir, si $g \circ u = h \circ u$ entonces $g = h$.*

3. *$Q(D)$ está determinado salvo isomorfismos por la Propiedad Universal. Explícitamente: supongamos que existen un cuerpo F y un homomorfismo inyectivo de anillos $v : D \to F$ tales que, para todo cuerpo K y todo homomorfismo inyectivo de anillos $f : D \to K$, existe una única extensión de cuerpos $\bar{f} : F \to K$ tal que $\bar{f} \circ v = f$. Entonces existe un isomorfismo $\phi : F \to Q(D)$ tal que $\phi \circ v = u$.*

Demostración. 1. Sea $f : D \to K$ como en el enunciado. Si $\bar{f} : Q(D) \to K$ es una extensión de cuerpos tal que $\bar{f} \circ u = f$ entonces, para todo $a/s \in Q(D)$, se verifica

$$\bar{f}(a/s) = \bar{f}(u(a)u(s)^{-1}) = (\bar{f} \circ u)(a)(\bar{f} \circ u)(s)^{-1} = f(a)f(s)^{-1}.$$

Esto prueba que la única extensión de cuerpos $\bar{f} : Q(D) \to K$ que puede satisfacer $\bar{f} \circ u = f$ tiene que venir dada por $\bar{f}(a/s) = f(a)f(s)^{-1}$. Sólo falta comprobar que $\bar{f}$ está bien definido y es un homomorfismo. Si $a_1/s_1 = a_2/s_2$ entonces $a_1 s_2 = a_2 s_1$, luego $f(a_1)f(s_2) = f(a_2)f(s_1)$ y, por tanto, $f(a_1)f(s_1)^{-1} = f(a_2)f(s_2)^{-1}$. Esto prueba que $\bar{f}$ está bien definido. Dejaremos que el lector compruebe que es efectivamente un homomorfismo.

2. Si ponemos $f = g \circ u = h \circ u : D \to K$, los homomorfismos g y h completan el diagrama del apartado 1. Por la unicidad se tiene $g = h$.

3. Sea $v : D \to F$ como en el enunciado. Aplicando 1 encontramos una extensión $\bar{v} : Q(D) \to F$ tal que $\bar{v} \circ u = v$, y aplicando la hipótesis de 3 encontramos una extensión $\bar{u} : F \to Q(D)$ tal que $\bar{u} \circ v = u$. Entonces la composición $\bar{u} \circ \bar{v} : Q(D) \to Q(D)$ verifica $(\bar{u} \circ \bar{v}) \circ u = \bar{u} \circ v = u$, y por 2 se obtiene $\bar{u} \circ \bar{v} = 1_{Q(D)}$. En particular $\bar{u}$ es suprayectiva, y como es inyectiva por ser una extensión de cuerpos, $\phi = \bar{u}$ es el isomorfismo que buscamos. □

La Propiedad Universal permite afirmar que $Q(D)$ es "el menor cuerpo que contiene a D" en un sentido que se hace explícito en el siguiente resultado:

Proposición 2.9.5 *Sea D un dominio. Si K es un cuerpo y $f : D \to K$ es un homomorfismo inyectivo de anillos, entonces K contiene un subcuerpo isomorfo a $Q(D)$.*

Demostración. Por la propiedad universal del cuerpo de fracciones existe una extensión de cuerpos $\bar{f} : Q(D) \to K$, y como $\bar{f}$ es inyectiva, Im $\bar{f}$ es un subcuerpo de K isomorfo a $Q(D)$. □

Ejemplo 2.9.6 *El cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$.*
Sea m un número entero que no es un cuadrado, y sea $f : \mathbb{Z}[\sqrt{m}] \to \mathbb{C}$ la inclusión. Si $\bar{f}$ es como en la demostración de la Proposición 2.9.5, entonces Im $\bar{f}$ es el cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$. Un elemento genérico de Im $\bar{f}$ es de la forma $x = \frac{a+b\sqrt{m}}{c+d\sqrt{m}}$, con $a, b, c, d \in \mathbb{Z}$ y $c + d\sqrt{m} \neq 0$. Si ponemos $t = (c + d\sqrt{m})(c - d\sqrt{m}) \neq 0$ entonces $t = c^2 - d^2 m \in \mathbb{Z}$, y así

$$x = \frac{a + b\sqrt{m}}{c + d\sqrt{m}} = \frac{(a + b\sqrt{m})(c - d\sqrt{m})}{t} = \frac{r + s\sqrt{m}}{t} = \frac{r}{t} + \frac{s}{t}\sqrt{m},$$

donde $r, s \in \mathbb{Z}$, y por tanto $x \in \mathbb{Q}[\sqrt{m}]$. Esto demuestra que Im $\bar{f} \subseteq \mathbb{Q}[\sqrt{m}]$, y el otro contenido es claro, pues un elemento genérico $\frac{a}{s} + \frac{b}{t}\sqrt{m}$ de $\mathbb{Q}[\sqrt{m}]$ se reescribe como $\frac{at+bs\sqrt{m}}{st}$.
En conclusión, el cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$ es $\mathbb{Q}[\sqrt{m}]$.

Un interesante corolario de la Proposición 2.9.5 es el siguiente:

Corolario 2.9.7 *Todo cuerpo K posee un subcuerpo K', llamado el* subcuerpo primo *de K, que está contenido en cualquier otro subcuerpo de K (es decir, K' es "el menor subcuerpo de K"). Si la característica de K es un entero primo p, entonces K' es isomorfo a $\mathbb{Z}_p$; en caso contrario K' es isomorfo a $\mathbb{Q}$.*

Demostración. Si la característica es un primo p entonces el subanillo primo de K (isomorfo a $\mathbb{Z}_p$) es ya un cuerpo, y contiene a cualquier subcuerpo (de hecho, a cualquier subanillo) de K.

En otro caso, al ser K un cuerpo, la característica es cero; es decir, el homomorfismo de anillos $f : \mathbb{Z} \to K$ es inyectivo. El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$, y la extensión de cuerpos $\bar{f} : \mathbb{Q} \to K$ que nos da la Propiedad Universal viene dada por $\bar{f}(n/m) = f(n)f(m)^{-1}$. Como $\bar{f}$ es inyectivo, $K' = $ Im $\bar{f}$ es un subcuerpo de K isomorfo a $\mathbb{Q}$, y ahora basta ver que K' está contenido en cualquier subcuerpo F de K. Dado un tal F, se tiene $f(m) \in F$ para cada $m \in \mathbb{Z}$, y si $m \neq 0$ entonces $f(m) \neq 0$ y $f(m)^{-1} \in F$. Por tanto, para cada $n/m \in \mathbb{Q}$ se tiene $\bar{f}(n/m) = f(n)f(m)^{-1} \in F$, lo que demuestra que $K' \subseteq F$. □

Como ya hemos dicho, la construcción del cuerpo de fracciones es parte de una construcción más general: la del anillo de fracciones por un subconjunto multiplicativo. Presentaremos a continuación este concepto, dejando los detalles a cargo del lector. Para mostrar otro enfoque (que puede adoptarse también para definir el cuerpo de fracciones), en lugar de construir primero el anillo de fracciones y demostrar después que verifica cierta propiedad universal, lo que hacemos es definir el anillo de fracciones como el que verifica cierta propiedad, y después lo construimos.

Definición 2.9.8 *Un* subconjunto multiplicativo *de un anillo A es un subconjunto S cerrado para el producto y que contiene al 1 pero no al 0; es decir, $1 \in S$, $0 \notin S$ y si $a, b \in S$ entonces $ab \in S$.*

Ejercicio 2.9.9 *Comprobar que los siguientes son subconjuntos multiplicativos de A.*

1. *El conjunto A^* de las unidades de A.*
2. *El conjunto de los elementos regulares de A.*
3. *El conjunto $A \setminus P$, donde P es un ideal primo de A.*
4. *El conjunto de los elementos no nulos de un dominio.*
5. *El conjunto $\{a^n : n \in \mathbb{N}\}$ de las potencias de un elemento regular a de A.*

Definición 2.9.10 *Sea S un subconjunto multiplicativo de un anillo A. Un* anillo de fracciones *de A por S es una pareja (B, j) formada por un anillo B y un homomorfismo de anillos $j : A \to B$ tal que $j(S) \subseteq B^*$ (es decir, $j(s)$ es invertible en B para todo $s \in S$) y tal que se verifica la siguiente propiedad:*

Si (C, f) es una pareja formada por un anillo C y un homomorfismo de anillos $f : A \to C$ tal que $f(S) \subseteq C^*$, entonces existe un único homomorfismo de anillos $\bar{f} : B \to C$ tal que $\bar{f} \circ j = f$.

Por ejemplo, si $S = A^*$ entonces el par (A, i), donde $i : A \to A$ es la identidad, es un anillo de fracciones de A por S. Y si D es un dominio entonces un anillo de fracciones de D por $S = D \setminus \{0\}$ es lo mismo que un cuerpo de fracciones de D.

Ejercicio 2.9.11 *Demostrar que si (B, j) y (B', j') son dos anillos de fracciones de A por S, entonces existe un único isomorfismo de anillos $f : B \to B'$ tal que $f \circ j = j'$.*

Ejercicio 2.9.12 *Sea A un anillo y sea S un subconjunto multiplicativo de A.*

1. *Demostrar que la siguiente es una relación de equivalencia en $X = A \times S$:*

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow \text{ existe } t \in S \text{ tal que } ta_1s_2 = ta_2s_1.$$

   Denotamos por a/s la clase de equivalencia de $(a, s) \in X$ y por AS^{-1} el conjunto de las clases de equivalencia.

2. *Demostrar que las fórmulas (2.9.1) proporcionan operaciones bien definidas en AS^{-1} que lo dotan de una estructura de anillo.*

3. *Demostrar que la aplicación $j : A \to AS^{-1}$ dada por $j(a) = a/1$ es un homomorfismo de anillos y que $j(s)$ es invertible en AS^{-1} para todo $s \in S$.*

4. *Demostrar que (AS^{-1}, j) es un anillo de fracciones de A por S.*

2.10 Problemas

1. Decir cuáles de los siguientes conjuntos son anillos con las operaciones que se describen:

   (a) El conjunto $\mathbb{Z}$ de los números enteros con las siguientes operaciones:

$$a \oplus b = a + b + 1, \qquad a \otimes b = ab + a + b.$$

   (b) El conjunto 2^X de los subconjuntos de un conjunto X con las operaciones de unión e intersección. ¿Y si se cambian los papeles de forma que la intersección represente la suma y la unión el producto?

   (c) El mismo conjunto 2^X, tomando como suma la *diferencia simétrica*, $A+B = (A\setminus B)\cup(B\setminus A)$, y como producto la intersección.

   (d) El conjunto $\mathbb{R}^{\mathbb{R}}$ de las funciones reales de variable real con las operaciones:

$$(f + g)(x) = f(x) + g(x) \qquad \text{y} \qquad (fg)(x) = f(x)g(x) \qquad (\forall x \in \mathbb{R}).$$

   (e) El conjunto $\mathbb{R}^{\mathbb{R}}$ anterior con la misma suma y el producto dado por la composición de funciones. ¿Y si limitamos el conjunto a las funciones que conserven la suma?

2. Indicar si son ciertas, en general, las siguientes relaciones en un anillo A (no necesariamente conmutativo):

   (a) $a^2 - b^2 = (a + b)(a - b)$.

   (b) $(a + b)^3 = a^3 + aba + ba^2 + b^2a + a^2b + ab^2 + bab + b^3$.

   (c) $a^m a^n = a^{m+n}$.

   (d) $(ab)^m = a^m b^m$.

3. Sea $f : A \to B$ un isomorfismo de anillos. Demostrar que:
   (a) Un elemento $a \in A$ es cancelable en A si y sólo si $f(a)$ es cancelable en B.
   (b) Un elemento $a \in A$ es invertible en A si y sólo si $f(a)$ es invertible en B.
   (c) Un subconjunto I de A es un subanillo de A si y sólo si $f(I)$ es un subanillo de B.
   (d) Un subconjunto I de A es un ideal de A si y sólo si $f(I)$ es un ideal de B.
   (e) Un ideal I de A es principal si y sólo si el ideal $f(I)$ de B es principal.
   (f) Un ideal I de A es maximal si y sólo si el ideal $f(I)$ de B es maximal.
   (g) Un ideal I de A es primo si y sólo si el ideal $f(I)$ de B es primo.
   (h) Un subconjunto X de A genera el ideal I si y sólo si el subconjunto $f(X)$ de B genera el ideal $f(I)$.
   (i) A y B tienen la misma característica.
   (j) A es un cuerpo si y sólo si B es un cuerpo.
   (k) A es un dominio si y sólo si B es un dominio.
4. Calcular las unidades del anillo $\mathbb{Z}[i]$.
5. Sean a y b dos elementos de un anillo. Demostrar que ab es un divisor de cero precisamente si a ó b es un divisor de cero.
6. Sea A un anillo finito. Demostrar que todo elemento de A es o divisor de cero o unidad. Deducir que todo dominio finito es un cuerpo. (Indicación: Considerar la aplicación $x \mapsto ax$.)
7. Demostrar que todo anillo con tres elementos es un cuerpo.
8. Calcular los divisores de cero y las unidades del anillo $\mathbb{R}^{\mathbb{R}}$ del apartado 1d del Problema 1.
9. Encontrar todos los divisores de cero en los anillos: $\mathbb{Z}_4$, $\mathbb{Z}_{10}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{R} \times \mathbb{R}$.
10. Un elemento e de un anillo A es *idempotente* si verifica $e^2 = e$. Demostrar que la suma y el producto de A convierten al subconjunto $eA = \{ea : a \in A\}$ en un anillo. ¿Cuál es su elemento identidad? ¿Es eA un subanillo de A?
11. Decimos que $d \in \mathbb{Z}$ es *libre de cuadrados* si p^2 no divide a d para ningún número primo p (en particular 1 es libre de cuadrados). Demostrar que para todo $m \in \mathbb{Z}$ existe un $d \in \mathbb{Z}$ libre de cuadrados tal que $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{d}]$. ¿Ocurre lo mismo si cambiamos $\mathbb{Q}$ por $\mathbb{Z}$?
12. Sea $d \in \mathbb{Z}$ libre de cuadrados y sea $\alpha = \frac{1+\sqrt{d}}{2}$. Demostrar que $\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}$ es un subanillo de $\mathbb{Q}[\sqrt{d}]$ precisamente si $d \equiv 1 \bmod 4$.
13. En cada apartado se describen un anillo A y un subconjunto B. Decir cuáles de los subconjuntos son subanillos:
   (a) A es el cuerpo $\mathbb{C}$ y $B = \mathbb{R}i$ consiste en los números de la forma ri con $r \in \mathbb{R}$.
   (b) A es el anillo $\mathbb{R}^{\mathbb{R}}$ del Problema 1d y B es el subconjunto de las funciones continuas.
   (c) A es el cuerpo racional $\mathbb{Q}$, q es un entero libre de cuadrados y B es el subconjunto $\mathbb{Z}_{(q)}$ de los números a/b con $\mathrm{mcd}(q, b) = 1$. ¿Qué ocurre si q no es libre de cuadrados?
   (d) A es el anillo $R[X]$ de polinomios con coeficientes en un anillo R, y B es el conjunto de los polinomios de grado menor o igual que n, donde $n \in \mathbb{Z}^+$.
   (e) En el cuerpo $A = \mathbb{C}$ consideramos, dado un entero primo p, una *raíz p-ésima primitiva* de la unidad ξ (es decir, $\xi^p = 1$ y $\xi^n \neq 1$ para $n = 1, \ldots, p-1$; por ejemplo, $\xi = e^{2\pi i/p} = \cos(2\pi/p) + \mathrm{sen}\ (2\pi/p)i$). B se define como el subconjunto

$$B = \mathbb{Z}[\xi] = \{a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{p-1}\xi^{p-1} \ : \ a_0, a_1, \ldots, a_{p-1} \in \mathbb{Z}\}.$$

(f) A es el anillo (no conmutativo) $M_n(R)$ de matrices sobre un anillo R y B consiste en las *matrices diagonales* de A, o sea las matrices en las que todos los elementos que no estén en la diagonal son nulos.

(g) $A = M_n(R)$ es como en el apartado anterior y B es el conjunto de las *matrices triangulares superiores*; es decir, las matrices de la forma

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}.$$

(h) A es el anillo de los endomorfismos de un espacio vectorial V y B es el conjunto

$$\{f \in A : f(W) \subseteq W\}$$

de los endomorfismos que dejan invariante W, donde W es un subespacio de V.

14. Sean A un anillo y $a \in A$. Demostrar que el subanillo de A generado por a está formado por los elementos de la forma $n_0 1 + n_1 a + n_2 a^2 + \cdots + n_k a^k$ donde k es un entero no negativo y $n_0, \dots, n_k$ son enteros. ¿Cómo son los elementos del subanillo generado por un conjunto arbitrario?

15. Sea A un anillo y sea $\sim$ una relación de equivalencia en A tal que, para cualesquiera $a, a', b, b' \in A$, se verifica

$$a \sim a',\ b \sim b' \ \Rightarrow\ a + b \sim a' + b',\ ab \sim a'b'$$

(se dice entonces que la relación es "compatible con las operaciones"). Si I es la clase de equivalencia que contiene al 0, demostrar que I es un ideal de A y que la relación $\sim$ es la que induce I; es decir, que $a \sim b$ si y sólo si $a - b \in I$.

En otras palabras, dar una relación de equivalencia en A compatible con sus operaciones equivale a dar un ideal de A.

16. Demostrar que el subconjunto de $\mathbb{Z}[i]$ formado por los elementos $a + bi$ con $2a \equiv b \bmod 5$ es un ideal principal.

17. Sean A y B dos anillos. Describir los ideales de $A \times B$ en función de los ideales de A y de B. Determinar todos los ideales de $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$.

18. Si I, J y K son ideales de un anillo A, demostrar que:

(a) $I(J \cap K) \subseteq IJ \cap IK$.

(b) $IJ = JI$.

(c) $I(JK) = (IJ)K$.

(d) $I(J + K) = IJ + IK$.

(e) $IA = I$.

19. Sea A un anillo. Para cada subconjunto X de A se define su *anulador* como $\mathrm{Anu}X = \{a \in A : ax = 0 \text{ para cada } x \in X\}$. Demostrar las siguientes propiedades para subconjuntos X e Y de A:

(a) $\mathrm{Anu}X$ es un ideal de A.

(b) $\mathrm{Anu}X = \mathrm{Anu}(X)$. Es decir, el anulador de un conjunto coincide con el anulador del ideal que genera dicho conjunto.

(c) Si $X \subseteq Y$, entonces $\mathrm{Anu}Y \subseteq \mathrm{Anu}X$.

(d) $X \subseteq \mathrm{AnuAnu}X$.

(e) $\mathrm{AnuAnuAnu}X = \mathrm{Anu}X$.

20. [*] Demostrar que las siguientes condiciones son equivalentes para un anillo A.

    (a) Todo ideal de A es finitamente generado; es decir, para todo ideal I existen $a_1, \ldots, a_n$ tales que $I = (a_1, \ldots, a_n)$.

    (b) Toda cadena creciente de ideales de A se estaciona; es decir, dado ideales $I_1 \subseteq I_2 \subseteq \cdots$ de A, existe $n \in \mathbb{N}$ tal que $I_n = I_{n+h}$ para todo $h \in \mathbb{N}$.

    (c) Todo conjunto no vacío de ideales de A tiene un elemento maximal con respecto a la inclusión.

    Un anillo que verifique estas condiciones se llama *anillo noetheriano* (Indicación: Aplicar el Lema de Zorn, observando que la unión de una cadena creciente de ideales es un ideal.)

21. Demostrar que si $f : A \to B$ es un homomorfismo suprayectivo de anillos y todos los ideales del anillo A son principales entonces todos los ideales de B son principales.

22. Sea $a \in \mathbb{R}$. ¿Qué se deduce al aplicar el Primer Teorema de Isomorfía al homomorfismo $\mathbb{R}[X] \to \mathbb{R}$, dado por $P(X) \mapsto P(a)$? ¿Y qué se deduce al aplicarlo al homomorfismo $\mathbb{R}[X] \to \mathbb{C}$, dado por $P(X) \mapsto P(i)$?

23. Sea $f : A \to B$ un homomorfismo suprayectivo de anillos. Demostrar que existe una correspondencia biunívoca, que conserva la inclusión, entre el conjunto de los ideales de B y los ideales de A que contienen a Ker f.

24. Demostrar el recíproco del Teorema Chino de los Restos para anillos; es decir, probar que si $I_1, \ldots, I_n$ son ideales de un anillo A tales que la aplicación $f : A \to \prod_{i=1}^{n} A/I_i$, dada por $f(a) = (a + I_1, \ldots, a + I_n)$ es suprayectiva, entonces $I_i + I_j = (1)$, para todo $i \neq j$.

25. Sean $A_1, \ldots, A_n$ anillos. Demostrar que la característica del anillo producto $A_1 \times \cdots \times A_n$ es el mínimo común múltiplo de las características de los A_i.

26. Sea A un anillo cuya característica es un número primo p. Demostrar que la aplicación $x \mapsto x^{p^n}$ es un endomorfismo de A para todo $n \in \mathbb{N}$.

27. Demostrar que, si K es un cuerpo finito con un subcuerpo F, entonces el cardinal de K es una potencia del cardinal de F. (Indicación: Considerar K como espacio vectorial sobre F). Deducir que:

    (a) El cardinal de cualquier cuerpo finito es una potencia de un número primo. (Indicación: Considerar el subanillo primo de K.)

    (b) Si K es un cuerpo finito con un subcuerpo F, entonces existen un número primo p y enteros positivos n y m tales que $n \mid m$, $|F| = p^n$ y $|K| = p^m$.

28. Determinar los automorfismos de $\mathbb{C}$ que cumplen $f(x) = x$, para todo $x \in \mathbb{R}$.

29. [*] Demostrar que el único automorfismo de $\mathbb{R}$ es la identidad. (Indicación: Un automorfismo de $\mathbb{R}$ debe fijar los números racionales y conservar el orden.)

30. Sea A un anillo de característica n y sea m un número entero. ¿Cuántos homomorfismos de anillos $\mathbb{Z}_m \to A$ existen? ¿Cuántos homomorfismos de anillos $\mathbb{Z}_n \to \mathbb{Z}_m$ existen?

31. Determinar los ideales de $\mathbb{Z}_n$. ¿Cuáles de ellos son primos o maximales? Dar una fórmula, en función de la descomposición de n en producto de primos para el número de ideales de $\mathbb{Z}_n$.

32. ¿Es $\mathbb{Z}_3[X]/(X^2 + 1)$ un cuerpo?

33. [*] Se considera el anillo $A[[X]]$ de series de potencias con coeficientes en un anillo A. Se pide:

    (a) Demostrar que $\sum_{i=1}^{\infty} a_i X^i$ es una unidad de $A[[X]]$ precisamente si a_0 es una unidad de A.

    (b) Si A es un cuerpo, demostrar que todo ideal de $A[[X]]$ es de la forma (X^n) para algún $n \in \mathbb{N}$.

    (c) Demostrar que $A[[X]]$ es un dominio precisamente si A es un dominio.

    (d) Identificar los ideales maximales de $A[[X]]$ en función de los ideales maximales de A.

34. [*] Sea A un anillo. Un elemento $a \in A$ es *nilpotente* si existe un entero $n \geq 1$ tal que $a^n = 0$. Demostrar que:

    (a) Si $x \in A$ es nilpotente y $u \in A$ es una unidad, entonces $u + x$ es una unidad.

    (b) El conjunto de los elementos nilpotentes de A es un ideal de A que coincide con la intersección de todos los ideales primos de A.

    (c) Si I es un ideal, entonces Rad $I = \{a \in A : a^n \in I, \text{ para algún } n \in \mathbb{N}\}$ es un ideal de A que se llama *radical* de I, y que coincide con la intersección de todos los ideales primos de A que contienen a I. ¿Cómo se relaciona esto con el apartado anterior?

    (d) Calcular Rad (n) para $n \in \mathbb{Z}$. (Indicación: Considerar la factorización prima de n.)

35. Demostrar que si p es un ideal primo de A, entonces $p[X]$ es un ideal primo de $A[X]$. ¿Puede ser $p[X]$ maximal?

36. Sea A un anillo. Demostrar que el conjunto S de los divisores de cero de A contiene un ideal primo de A. (Indicación: Aplicar el Lema de Zorn al conjunto de los ideales contenidos en S.)

37. Demostrar que si p es un ideal maximal (respectivamente primo) de A, entonces

$$p + (X) = \{a_0 + a_1 X + \cdots \in A[X] \ : \ a_0 \in p\}$$

    es un ideal maximal (respectivamente primo) de $A[X]$.

38. [*] Sea I un ideal de A y sean $p_1, \ldots, p_n$ ideales primos de A. Demostrar que si $I \subseteq \cup_{i=1}^n p_i$, entonces $I \subseteq p_i$, para algún $i = 1, \ldots, n$. (Indicación: Razonar por inducción sobre n.)

39. Demostrar que las siguientes condiciones son equivalentes para un anillo A.

    (a) A tiene un único ideal maximal.

    (b) A tiene un ideal propio I que contiene todos los elementos no invertibles de A.

    (c) El conjunto de los elementos no invertibles de A es un ideal.

    (d) Para todo $a, b \in A$, si $a + b$ es invertible, entonces a ó b es invertible.

    Un anillo que satisface las condiciones anteriores se dice que es *local*.

40. Demostrar que los siguientes anillos son locales:

    (a) $\mathbb{Z}_{p^n}$, donde p es primo y $n \geq 0$.

    (b) A/m^n, donde A es cualquier anillo, m es un ideal maximal y $n \in \mathbb{Z}^+$.

    (c) $\mathbb{Z}_{(p)}$, donde p es primo (ver el Problema 13).

    (d) [*] $K[[X]]$, donde K es un cuerpo.

41. Demostrar que si $f : A \to B$ es un homomorfismo suprayectivo de anillos y A es local, entonces B también es local.

42. [*] Un ideal I de un anillo A se dice que es *primario* si $I \neq A$ y para todo $x, y \in A$ tales que $xy \in I$, se verifica que $x \in I$ o existe $n \in \mathbb{Z}^+$ tal que $y^n \in I$. Demostrar:

    (a) Si I es un ideal primario, entonces Rad (I) es un ideal primo.

    (b) Si $I \neq A$, entonces I es primario precisamente si todo divisor de cero de A/I es nilpotente.

    (c) Encontrar los ideales primarios de $\mathbb{Z}$.

43. Sea D un dominio y sea Q su cuerpo de fracciones. Demostrar que:

    (a) Si D' es un subanillo de D con cuerpo de fracciones Q', entonces Q contiene un subcuerpo isomorfo a Q'.

    (b) Si A es un subanillo de Q que contiene a D, entonces Q es un cuerpo de cocientes de A.

44. [*] Sean A un anillo, S un subconjunto multiplicativo de A, y (AS^{-1}, j) el anillo de cocientes de A por S. Demostrar:

    (a) $\frac{a}{s} = \frac{0}{1}$ precisamente si existe un $t \in S$ tal que $ta = 0$.

    (b) AS^{-1} es un dominio si lo es A.

    (c) La aplicación j es inyectiva precisamente si S no contiene divisores de cero.

    (d) Si todo elemento de S es invertible, entonces j es un isomorfismo.

    (e) Si I es un ideal de A, entonces $IS^{-1} = \{\frac{a}{s} : a \in I, s \in S\}$ es un ideal de AS^{-1}. Si I es principal, entonces lo es IS^{-1}.

    (f) Si I es un ideal de A, entonces $IS^{-1} = AS^{-1}$ precisamente si $I \cap S \neq \emptyset$.

    (g) Si J es un ideal de AS^{-1}, entonces existe un ideal I de A tal que $J = AS^{-1}$.

    (h) Si p es un ideal primo de A tal que $S \cap p = \emptyset$, entonces pS^{-1} es un ideal primo de AS^{-1}.

    (i) La aplicación $p \mapsto pS^{-1}$ define una correspondencia biunívoca entre los ideales primos de A que no intersecan a S y los ideales primos de AS^{-1} cuya inversa es la aplicación dada por $q \mapsto j^{-1}(q)$.

    (j) Sea T un subconjunto multiplicativo de AS^{-1}. Probar que $\bar{T} = \{a \in A : \frac{a}{s} \in T \text{ para algún } s \in S\}$ es un subconjunto multiplicativo de A y que $A\bar{T}^{-1} \cong (AS^{-1})T^{-1}$.

    (k) Sea I un ideal de A tal que $S \cap I = \emptyset = S \cap (1 + I)$. Sea $\pi : A \to A/I$ el homomorfismo proyección. Demostrar que $\pi(S)$ es un subconjunto multiplicativo de A/I y que $(A/I)\pi(S)^{-1}$ es isomorfo a $(AS^{-1})/(IS^{-1})$.

45. Sea $q = p_1 \dots p_n$ un entero libre de cuadrados (los p_i son primos distintos), y sea S el conjunto de los enteros de la forma $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ con cada $\alpha_i \in \mathbb{N}$.

    (a) Demostrar que S es un subconjunto multiplicativo de $\mathbb{Z}$ y que $\mathbb{Z}S^{-1}$ es el anillo $\mathbb{Z}_{(q)}$ del Problema 13c.

    (b) [*] Deducir del Problema 44 que $\mathbb{Z}_{(q)}$ es un dominio cuyos ideales son todos principales.

46. [*] Sean A un anillo y p un ideal primo de A. Sea $S = A \setminus p$. El anillo $S^{-1}A$ se denota A_p y se llama el *anillo localizado* de A en p. Análogamente, si I es un ideal de A, entonces $S^{-1}I$ se denota I_p. Demostrar que todos los ideales propios de A_p están contenidos en p_p. Concluir que A_p es un anillo local cuyo único ideal maximal es p_p.

47. [*] Demostrar que si $S = \{X^n : n \in \mathbb{Z}\}$, donde X es la indeterminada de un anillo de polinomios $A = B[X]$, entonces AS^{-1} es isomorfo al anillo

$$B[X, X^{-1}] = \{b_n X^n + b_{n+1} X^{n+1} + \cdots + b_m X^m : n \leq m \in \mathbb{Z} \text{ y } b_i \in B \ \forall i\}$$

    con la suma y el producto naturales.

Bibliografía del capítulo

Allenby [1], Atiyah-Macdonald [5], Delgado-Fuertes-Xambó [12], Dorronsoro-Hernández [13], Hartley-Hawks [19].

Capítulo 3

Divisibilidad y factorización en dominios

Se estudian diversas condiciones de divisibilidad y factorización que pueden verificarse en un dominio, se establecen las relaciones entre ellas y se presentan algunas aplicaciones a la Teoría de Números.

Introducción

En el Capítulo 1 vimos algunas propiedades básicas relativas a la divisibilidad en el anillo de los números enteros. Entre ellas la división entera (y con ella el algoritmo de Euclides), el hecho de que todos los ideales de $\mathbb{Z}$ son principales, y el Teorema Fundamental de la Aritmética, que asegura que todo número entero se puede escribir, de modo esencialmente único, como producto de números primos. Estas tres propiedades se pueden estudiar en abstracto, como veremos en este capítulo, y son fundamentales para entender la divisibilidad en los anillos que las satisfagan. Por ejemplo, si un anillo satisface una propiedad análoga al Teorema Fundamental de la Aritmética, entonces podremos usar las descomposiciones en productos de primos para determinar si un elemento divide a otro, o para calcular el máximo común divisor y el mínimo común múltiplo de cualquier conjunto de elementos. Por otra parte, como veremos, las tres propiedades no son independientes.

Comenzaremos definiendo las nociones generales relativas a la divisibilidad entre los elementos de un dominio y estableciendo sus primeras propiedades, en particular la relación con los ideales principales; esto nos llevará al estudio de la divisibilidad en los dominios de ideales principales. Más tarde, consideraremos anillos en los que hay una función euclídea (un modo razonable de "dividir con resto") y observaremos que éstos son dominios de ideales principales en los que se puede aplicar el algoritmo de Euclides. En tercer lugar consideraremos los dominios en los que todo elemento es producto de primos, llamados dominios de factorización única, y demostraremos que todo dominio de ideales principales es de este tipo.

Además de $\mathbb{Z}$ y de los anillos de polinomios sobre cuerpos, los principales ejemplos del capítulo serán ciertos subanillos del cuerpo complejo $\mathbb{C}$, que en muchos casos son necesarios para demostrar resultados clásicos sobre números enteros. El capítulo terminará con varios ejemplos de esta situación, en los que usaremos las propiedades del anillo $\mathbb{Z}[i]$ de los enteros de Gauss.

Objetivos del capítulo

- Conocer las nociones básicas sobre divisibilidad en dominios (la relación 'ser asociado", elementos primos e irreducibles, máximo común divisor y mínimo común múltiplo), y su traducción en términos de ideales principales.
- Conocer algunos ejemplos de dominios euclídeos, y saber usar el algoritmo de Euclides.
- Conocer las distintas caracterizaciones de los dominios de factorización única, y saber usar las factorizaciones en irreducibles para deducir cuestiones sobre divisibilidad.

- Conocer la relación entre los tres tipos de dominios estudiados: los dominios euclídeos son dominios de ideales principales, y éstos son dominios de factorización única.
- Manejar cuestiones de divisibilidad y factorización en subanillos de $\mathbb{C}$ del tipo $\mathbb{Z}[\sqrt{m}]$, con $m \in \mathbb{Z}$, y ser capaz de aplicarlas para resolver ciertos problemas clásicos sobre números enteros.

Desarrollo de los contenidos

3.1 Divisibilidad

Definición 3.1.1 *Sea A un anillo y sean $a, b \in A$. Se dice que a* divide *a b en A, o que a es* un divisor *de b en A, o que b es* un múltiplo *de a en A, si existe $c \in A$ tal que $b = ac$.*

Para indicar que a divide a b en A escribiremos $a \mid b$ en A. Si el anillo A está claro por el contexto escribiremos simplemente $a \mid b$.

Obsérvese que la noción de divisibilidad depende del anillo. Por ejemplo, si a es un entero diferente de 0, entonces a divide a todos los números enteros en $\mathbb{Q}$, pero no necesariamente en $\mathbb{Z}$.

Ejercicio 3.1.2 *Sea A un anillo y sean $a, b, c \in A$. Demostrar que se verifican las siguientes propiedades:*

1. *(Reflexiva) $a \mid a$.*
2. *(Transitiva) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*
3. *$a \mid 0$ y $1 \mid a$.*
4. *$0 \mid a$ si y sólo si $a = 0$.*
5. *$a \mid 1$ si y sólo si a es una unidad; en este caso $a \mid x$ para todo $x \in A$ (es decir, las unidades dividen a cualquier elemento).*
6. *Si $a \mid b$ y $a \mid c$ entonces $a \mid rb + sc$ para cualesquiera $r, s \in A$ (y en particular $a \mid b + c$, $a \mid b - c$ y $a \mid rb$ para cualquier $r \in A$). Más generalmente, si a divide a ciertos elementos, entonces divide a cualquier combinación lineal suya con coeficientes en A.*
7. *Si A es un dominio, $c \neq 0$ y $ac \mid bc$, entonces $a \mid b$.*

Definición 3.1.3 *Dos elementos a y b de un anillo A se dice que son* asociados *si se dividen mutuamente; es decir, si $a \mid b$ y $b \mid a$. Cuando no esté claro por el contexto en qué anillo estamos trabajando, hablaremos de elementos* asociados en A.

Por ejemplo, una unidad es lo mismo que un elemento asociado a 1.

Es elemental ver que "ser asociados" es una relación de equivalencia en A, y que dos elementos son asociados si y sólo si tienen los mismos divisores, si y sólo si tienen los mismos múltiplos. Por lo tanto, al estudiar cuestiones de divisibilidad, un elemento tendrá las mismas propiedades que sus asociados.

La siguiente caracterización de la relación "ser asociado" en un dominio será importante (y por motivos como éste pronto empezaremos a suponer sistemáticamente que los anillos que aparecen son dominios):

Ejercicio 3.1.4 Si D es un dominio, demostrar que dos elementos $a, b \in D$ son asociados si y sólo si existe una unidad $u \in D^*$ tal que $b = au$ (si D no es un dominio, se verifica el "si").

Ejercicio 3.1.5 *Consideremos el anillo $\mathbb{Z}[\sqrt{m}]$, donde $m \in \mathbb{Z}$ no es un cuadrado, y recordemos que el conjugado de $x = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ es $\bar{x} = a - b\sqrt{m}$. Definimos la* norma *de x como el entero*

$$N(x) = x \cdot \bar{x} = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2.$$

Esta noción es útil porque permite traducir problemas de divisibilidad en $\mathbb{Z}[\sqrt{m}]$ a problemas de divisibilidad entre enteros, como se aprecia en las siguientes propiedades elementales. Demostrar que:

1. *$N(x) = 0$ si y sólo si $x = 0$.*
2. *La norma es multiplicativa; es decir, $N(xy) = N(x)N(y)$ para cualesquiera $x, y \in \mathbb{Z}[\sqrt{m}]$ (recuérdese que la conjugación es un homomorfismo de anillos $\mathbb{Z}[\sqrt{m}] \to \mathbb{Z}[\sqrt{m}]$).*
3. *$x \in \mathbb{Z}[\sqrt{m}]^*$ si y sólo si $N(x) = \pm 1$, y en este caso $x^{-1} = N(x)\bar{x}$ (es decir, $x^{-1} = \pm\bar{x}$, donde el signo es el de $N(x)$).*
4. *Si $x \mid y$ en $\mathbb{Z}[\sqrt{m}]$ entonces $N(x) \mid N(y)$ en $\mathbb{Z}$.*
5. *Si x e y son asociados en $\mathbb{Z}[\sqrt{m}]$ entonces $N(x) = \pm N(y)$.*
6. *Si $x \mid y$ en $\mathbb{Z}[\sqrt{m}]$ y $N(x) = \pm N(y)$ entonces x e y son asociados en $\mathbb{Z}[\sqrt{m}]$.*
7. *$\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.*
8. *Si $m \leq -2$ entonces $\mathbb{Z}[\sqrt{m}]^* = \{1, -1\}$.*

Observaciones 3.1.6

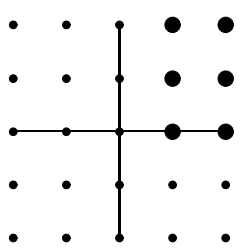
1. *Si $m < 0$, entonces el conjugado $\bar{z} = a - b\sqrt{m}$ de $z = a + b\sqrt{m}$ es su conjugado complejo en el sentido usual. Por tanto, $N(z) = z\bar{z} = |z|^2$, lo que implica que los elementos invertibles de $\mathbb{Z}[\sqrt{m}]$ son los que pertenecen a la circunferencia de centro 0 y radio 1. Esto ilustra los dos últimos apartados del ejercicio anterior.*
2. *Si $m \geq 2$ entonces $\mathbb{Z}[\sqrt{m}]$ tiene una infinidad de elementos invertibles, pero no es fácil demostrarlo. O sea, la* Ecuación de Pell *$x^2 - my^2 = 1$ tiene infinitas soluciones enteras. Éste es un profundo resultado que se verá en el curso de* Introducción a la Teoría de Números *y que implica que las ecuaciones diofánticas del tipo $x^2 - my^2 = n$ (con $m \geq 2$ y $n \in \mathbb{Z}$) tienen infinitas soluciones o ninguna. Sí es fácil ver, por ejemplo, que en $\mathbb{Z}[\sqrt{2}]$ el elemento $1+\sqrt{2}$ es invertible, y por lo tanto lo son todas sus potencias, que son distintas entre sí (¿por qué?).*
3. *En general un elemento de $\mathbb{Z}[\sqrt{m}]$ no es asociado de su conjugado, aunque el hecho de que la conjugación sea un isomorfismo nos permitirá relacionar algunas de sus propiedades (por ejemplo, usando nociones que vamos a definir en seguida, x es irreducible o primo si y sólo si lo es $\bar{x}$).*

Del Ejercicio 3.1.4 se deduce que, si en un dominio D se conocen todas las unidades, se conocen automáticamente todos los asociados de un elemento. Por ejemplo, como $\mathbb{Z}^* = \{1, -1\}$, los asociados de a en $\mathbb{Z}$ son el propio a y $-a$.

El conocimiento de D^* también es útil para encontrar un conjunto de representantes de los elementos no nulos de D para la relación "ser asociados"; es decir, un subconjunto D_0 de D tal que cada elemento no nulo de D es asociado a un único elemento de D_0. Por ejemplo:

Ejercicio 3.1.7 *Con la notación anterior, demostrar que:*

1. *Si $D = \mathbb{Z}$, podemos tomar $D_0 = \mathbb{Z}^+$.*
2. *Si $D = \mathbb{Z}[i]$ entonces podemos tomar como D_0 el conjunto de los enteros de Gauss de la forma $a + bi$, con $a > 0$ y $b \geq 0$ (es decir, los del primer cuadrante, incluido el semieje real positivo pero no el eje imaginario).*



3. *Encontrar un conjunto de representantes salvo asociados para $\mathbb{Z}[\sqrt{m}]$ con $m \leq -2$.*

4. *Si K es un cuerpo y $D = K[X]$, entonces D^* consiste en los polinomios constantes no nulos (es decir, $D^* = K^* = K \setminus \{0\}$), y podemos tomar como D_0 el conjunto de los polinomios con coeficiente principal 1.*

Sabemos que cualquier elemento a de un anillo A es divisible por sus asociados y por las unidades de A, y que si a divide a uno de los elementos b ó c entonces divide a su producto bc. A continuación estudiamos los elementos que verifican "los recíprocos" de estas propiedades. A menudo consideraremos elementos a de un anillo A que no son cero ni unidades, lo que sintetizaremos en la forma $0 \neq a \in A \setminus A^*$.

Definición 3.1.8 *Diremos que un elemento a del anillo A es* irreducible *si $0 \neq a \in A \setminus A^*$ y la relación $a = bc$ en A implica que $b \in A^*$ ó $c \in A^*$ (y por lo tanto que uno de los dos es asociado de a).*

Diremos que a es primo *si $0 \neq a \in A \setminus A^*$ y la relación $a \mid bc$ en A implica que $a \mid b$ ó $a \mid c$.*

Ambas nociones dependen del anillo ambiente, y si éste no está claro por el contexto hablaremos de irreducibles y primos "en A".

Ejercicio 3.1.9 *Si D es un dominio, demostrar que:*

1. *Un elemento $0 \neq a \in D \setminus D^*$ es irreducible si y sólo si sus únicos divisores son sus asociados y las unidades*[1].
2. *Si dos elementos son asociados, entonces uno es irreducible (respectivamente primo) si y sólo si lo es el otro.*
3. *En $\mathbb{Z}[\sqrt{m}]$, un elemento es irreducible (respectivamente primo) si y sólo si lo es su conjugado.*

Ejemplos 3.1.10 *Irreducibles y primos.*

1. En $\mathbb{Z}$ ambos conceptos coinciden con la noción usual de entero primo (Proposición 1.5.1).
2. Supongamos que $m \in \mathbb{Z}$ no es un cuadrado. Entonces, en $\mathbb{Z}[\sqrt{m}]$, los elementos de norma prima son irreducibles; es decir, si $x \in \mathbb{Z}[\sqrt{m}]$ y $N(x)$ es un entero primo, entonces x es irreducible en $\mathbb{Z}[\sqrt{m}]$. En efecto, es claro que x no es cero ni invertible, y si $x = yz$, entonces $N(x) = N(y)N(z)$, con lo que $N(y) = \pm 1$ ó $N(z) = \pm 1$, y por tanto y ó z es una unidad de $\mathbb{Z}[\sqrt{m}]$.

   El recíproco no es cierto. Por ejemplo, 3 es irreducible en $\mathbb{Z}[i]$ (¿por qué?), aunque su norma no es un entero primo.
3. El polinomio X^2+1 es irreducible en $\mathbb{R}[X]$ pero no en $\mathbb{C}[X]$, donde se tiene $X^2+1 = (X+i)(X-i)$.
4. El polinomio $2X + 2$ es irreducible en $\mathbb{Q}[X]$ pero no en $\mathbb{Z}[X]$, donde se tiene $2X + 2 = 2(X + 1)$.

Acabamos de ver que un elemento de $\mathbb{Z}$ es irreducible si y sólo si es primo. Sólo una parte es cierta en general (la demostración se deja como ejercicio).

Proposición 3.1.11 *En un dominio A todo elemento primo es irreducible.*

El recíproco no se verifica en general, como muestra el siguiente ejemplo.

Ejemplo 3.1.12 *Irreducible no implica primo.*

En el anillo $\mathbb{Z}[\sqrt{-5}]$ hay elementos irreducibles que no son primos. Comencemos observando que los cuadrados en $\mathbb{Z}_5$ son $[0]_5$ y $[\pm 1]_5$, y que por lo tanto la congruencia $a^2 \equiv \pm 2 \bmod 5$ no tiene solución. Esto implica que en $\mathbb{Z}[\sqrt{-5}]$ no hay elementos cuya norma valga 2, 3 ó 12 (¿por qué?; obsérvese que en $\mathbb{Z}[\sqrt{-5}]$ todas las normas son positivas). Sea ahora $x \in \mathbb{Z}[\sqrt{-5}]$ con $N(x) = 4$; si $y \mid x$ entonces $N(y) \mid N(x) = 4$ y por lo tanto $N(y)$ vale 1, 2 ó 4; en el primer caso y es una unidad, el segundo es imposible y en el tercero y es asociado de x (¿por qué?), y en consecuencia x es irreducible. De igual modo se ve que los elementos con norma 6 ó 9 son irreducibles, y en particular lo son todos los factores de la igualdad

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Pero ninguno de ellos es primo: por ejemplo de la igualdad se deduce que $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, y es claro que $2 \nmid (1 + \sqrt{-5})$ y $2 \nmid (1 - \sqrt{-5})$.

[1] Si D no es un dominio se verifica el "sólo si". En $A = \mathbb{Z}_6$ el "si" falla para $a = [4]_6$.

Las definiciones de máximo común divisor y mínimo común múltiplo, así como sus propiedades elementales, son análogas a las de $\mathbb{Z}$ y las resumimos en el siguiente ejercicio/definición:

Ejercicio 3.1.13 *Sean A un anillo, S un subconjunto de A y $a, b, d, m \in A$. Demostrar que:*

1. *Las condiciones siguientes son equivalentes:*
   (a) *m es múltiplo de cada elemento de S, y si un elemento $x \in A$ es múltiplo de cada elemento de S entonces x es múltiplo de m.*
   (b) *Un elemento $x \in A$ es múltiplo de cada elemento de S si y sólo si es múltiplo de m.*

   En este caso se dice que m es un mínimo común múltiplo *de S, y otro elemento es un mínimo común múltiplo de S si y sólo si es asociado de m. Escribiremos $m = \operatorname{mcm}(S)$, entendiendo que tal elemento (si existe) es único salvo asociados. Asimismo, hablaremos de* el *mínimo común múltiplo de S, con el mismo significado de unicidad salvo asociados.*

2. *Las condiciones siguientes son equivalentes:*
   (a) *d divide a cada elemento de S, y si un elemento $x \in A$ divide a cada elemento de S entonces x divide a d.*
   (b) *Un elemento $x \in A$ divide a cada elemento de S si y sólo si divide a d.*

   En este caso se dice que d es un máximo común divisor *de S, y otro elemento es un máximo común divisor de S si y sólo si es asociado de d. Escribiremos $d = \operatorname{mcd}(S)$, entendiendo que tal elemento (si existe) es único salvo asociados.*

3. *Si d es un divisor común de los elementos de S y además es combinación lineal de elementos de S; es decir, existen elementos $s_1, \ldots, s_n \in S$ y $a_1, \ldots, a_n \in A$ tales que*
$$d = a_1 s_1 + \cdots + a_n s_n, \tag{3.1.1}$$
   entonces $d = \operatorname{mcd}(S)$, y se dice que esta expresión es una identidad de Bezout *para S.*
   Si existe una identidad de Bezout (3.1.1) con $d = 1$ entonces $\operatorname{mcd}(S) = 1$.

4. *Se verifica $1 = \operatorname{mcd}(S)$ si y sólo si los únicos divisores comunes de los elementos de S son las unidades de A. En este caso decimos que los elementos de S son* coprimos. *Si para cada par de elementos distintos $a, b \in S$ se verifica $\operatorname{mcd}(a, b) = 1$, decimos que los elementos de S son* coprimos dos a dos.

5. *$a \mid b$ si y sólo si $a = \operatorname{mcd}(a, b)$, si y sólo si $b = \operatorname{mcm}(a, b)$.*

6. *En particular, $1 = \operatorname{mcd}(a, 1)$, $\operatorname{mcd}(a, 0) = a = \operatorname{mcm}(a, 1)$ y $0 = \operatorname{mcm}(a, 0)$.*

7. *Si a es irreducible entonces $\operatorname{mcd}(a, b) = 1$ si y sólo si $a \not\mid b$.*

Ejercicio 3.1.14 *Demostrar que, para cualquier entero m, dos enteros a y b son coprimos en $\mathbb{Z}[\sqrt{m}]$ si y sólo si son coprimos en $\mathbb{Z}$.*

El siguiente ejemplo muestra ciertos fenómenos que no ocurrían en $\mathbb{Z}$; en particular, la existencia de un máximo común divisor o un mínimo común múltiplo no está garantizada en un dominio arbitrario.

Ejemplo 3.1.15 *Patologías en $\mathbb{Z}[\sqrt{-5}]$.*
En este ejemplo trabajamos en el anillo $\mathbb{Z}[\sqrt{-5}]$ y hacemos uso de las afirmaciones del Ejemplo 3.1.12. Se verifican:

1. Los elementos 2 y $1 + \sqrt{-5}$ son coprimos, pues si x es un divisor común entonces su norma divide a 4 y a 6, luego divide a 2 y por lo tanto vale 1, de manera que x es una unidad. Sin embargo no hay una identidad de Bezout para $\{2, 1 + \sqrt{-5}\}$, pues la igualdad en $\mathbb{Z}[\sqrt{-5}]$
$$1 = 2(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5})$$
   equivale al par de igualdades en $\mathbb{Z}$
$$2a + c - 5d = 1 \qquad 2b + c + d = 0,$$
   que reducidas módulo 2 nos llevan al absurdo $c + d \equiv 1 \bmod 2$ y $c + d \equiv 0 \bmod 2$.

2. Aunque acabamos de ver que 2 y $1+\sqrt{-5}$ tienen máximo común divisor, no tienen mínimo común múltiplo. Supongamos que existe $x = \text{mcm}(2, 1+\sqrt{-5})$; entonces $N(x)$ sería un múltiplo común de 4 y 6, y por lo tanto sería un múltiplo de 12. Por otra parte los elementos 6 y $2(1+\sqrt{-5})$ son múltiplos comunes de 2 y de $1+\sqrt{-5}$, luego x los divide y por lo tanto $N(x)$ divide a 36 y a 24, por lo que divide a 12. En conclusión, si existe $\text{mcm}(2, 1+\sqrt{-5})$ su norma es 12, pero ya vimos que esto es imposible.

3. Veamos por último que no existe $x = \text{mcd}(6, 2(1+\sqrt{-5}))$. Si existiera, $N(x)$ dividiría a 36 y a 24 y por lo tanto dividiría a 12; pero además, como 2 y $1+\sqrt{-5}$ dividen a 6 y a $2(1+\sqrt{-5})$, deberían dividir a x y así $N(x)$ sería un múltiplo común de 4 y 6 y por lo tanto sería un múltiplo de 12, lo que nos llevaría a la situación imposible $N(x) = 12$.

3.2 Dominios de ideales principales

Comenzamos esta sección observando que, sobre un dominio, todas las nociones de divisibilidad que hemos presentado pueden reenunciarse en términos de los ideales principales generados por los elementos involucrados.

Ejercicio 3.2.1 *Sea D un dominio con elementos a, b, d, m y un subconjunto S. Demostrar que se verifican las siguientes propiedades:*

1. *$a = 0$ precisamente si $(a) = 0$.*
2. *$a \in D^*$ precisamente si $(a) = D$.*
3. *$a \mid b$ precisamente si $(b) \subseteq (a)$ (o si $b \in (a)$).*
4. *a y b son asociados precisamente si $(a) = (b)$.*
5. *a es primo precisamente si (a) es un ideal primo no nulo de D.*
6. *a es irreducible precisamente si (a) es maximal entre los ideales principales propios no nulos de D; es decir, $a \neq 0$ y $(a) \subseteq (b) \subset D$ implica $(a) = (b)$.*
7. *$d = \text{mcd}(S)$ precisamente si (d) es mínimo entre los ideales principales que contienen a S (o al ideal generado por S).*

   En particular, si (S) es un ideal principal entonces cualquier generador suyo es un máximo común divisor de S, y además existe una identidad de Bezout para S.
8. *$m = \text{mcm}(S)$ si y sólo si $(m) = \cap_{s \in S}(s)$.*

   En consecuencia, $\text{mcm}(S)$ existe si y sólo si el ideal $\cap_{s \in S}(s)$ es principal, y entonces cualquier generador de $\cap_{s \in S}(s)$ es un mínimo común múltiplo de S.

En vista de estos resultados, las nociones sobre divisibilidad se manejarán fácilmente en dominios en los que todos los ideales son principales.

Definición 3.2.2 *Un* dominio de ideales principales, *o* DIP *(PID, en la literatura en inglés), es un dominio en el que todos los ideales son principales.*

Proposición 3.2.3 *Si D es un DIP y $0 \neq a \in D \setminus D^*$, las siguientes condiciones son equivalentes:*

1. *a es irreducible.*
2. *(a) es un ideal maximal.*
3. *$A/(a)$ es un cuerpo.*
4. *a es primo.*
5. *(a) es un ideal primo.*
6. *$A/(a)$ es un dominio.*

Demostración. La equivalencia entre 1, 2 y 3 es consecuencia del Ejercicio 3.2.1 y de la Proposición 2.8.6, y lo mismo puede decirse de la equivalencia entre 4, 5 y 6. También de la Proposición 2.8.6 se deduce que 2 implica 5. Finalmente, 4 implica 1 por la Proposición 3.1.11. □

Ejemplos 3.2.4 *Dominios de ideales principales.*

1. $\mathbb{Z}$ es un DIP por el Teorema 1.2.11.
2. El anillo de polinomios $\mathbb{Z}[X]$ no es un DIP por el Ejemplo 2.5.9.
3. $\mathbb{Z}[\sqrt{-5}]$ no es un DIP, pues contiene elementos irreducibles que no son primos. También podemos observar que el ideal $(6, 2(1+\sqrt{-5})$ no es principal, pues no existe $\mathrm{mcd}(6, 2(1+\sqrt{-5}))$. Véase el Ejemplo 3.1.15.

Veamos otra consecuencia inmediata del Ejercicio 3.2.1.

Proposición 3.2.5 *Sea D un DIP y sea S un subconjunto de D. Entonces*

1. *S tiene un mínimo común múltiplo (cualquier generador de $\cap_{s\in S}(s)$).*
2. *S tiene un máximo común divisor d (cualquier generador del ideal que genera S) y además existe una identidad de Bezout para S.*
3. *El elemento d es un máximo común divisor de $a_1, \ldots, a_n$ si y sólo si $d \mid a_i$ para cada $i = 1, \ldots, n$ y existen $r_1, \ldots, r_n \in D$ tales que*

$$r_1a_1 + \cdots + r_na_n = d.$$

4. *Los elementos $a_1, \ldots, a_n$ son coprimos si y sólo si existen $r_1, \ldots, r_n \in D$ tales que*

$$r_1a_1 + \cdots + r_na_n = 1.$$

Ejercicio 3.2.6 *Si D es un DIP, demostrar que para cualesquiera $a, b, c \in D$ se verifican las siguientes propiedades (ver las Proposiciones 1.3.6 y 1.4.3):*

1. *Si $d = \mathrm{mcd}(a, b)$, entonces $\mathrm{mcd}(\frac{a}{d}, \frac{b}{d}) = 1$.*
2. *Si $\mathrm{mcd}(a, b) = \mathrm{mcd}(a, c) = 1$, entonces $\mathrm{mcd}(a, bc) = 1$.*
3. *Si $\mathrm{mcd}(a, b) = 1$ y $a \mid bc$, entonces $a \mid c$.*
4. *Si $\mathrm{mcd}(a, b) = 1$, $a \mid c$ y $b \mid c$, entonces $ab \mid c$.*
5. *ab y $\mathrm{mcd}(a, b)\mathrm{mcm}[a, b]$ son asociados.*

3.3 Dominios euclídeos

En esta sección nos ocuparemos del concepto de división con resto. En realidad existen varias posibles generalizaciones de dicho concepto. Todas ellas tienen consecuencias similares, y nosotros elegiremos la más general.

Definición 3.3.1 *Sea D un dominio. Una* función euclídea *en D es una aplicación $\delta : D \setminus \{0\} \to \mathbb{N}$ que cumple las siguientes condiciones:*

(DE1) Si $a, b \in D \setminus \{0\}$ verifican $a \mid b$ entonces $\delta(a) \leq \delta(b)$.

(DE2) Dados $a, b \in D$ con $b \neq 0$, existen $q, r \in D$ tales que $a = bq + r$ y o bien $r = 0$ o bien $\delta(r) < \delta(b)$.

Un dominio euclídeo *es un dominio que admite una función euclídea.*

La posibilidad de "dividir con resto" en un dominio euclídeo nos permite demostrar propiedades como las que siguen:

Proposición 3.3.2 *Sea δ una función euclídea en un dominio D. Entonces las siguientes condiciones son equivalentes para $a \in D$:*

1. *a es una unidad de D.*
2. *$\delta(a) = \delta(1)$.*
3. *$\delta(a) \leq \delta(x)$, para todo $x \in D \setminus \{0\}$.*

Demostración. 1 implica 2. Por hipótesis, a es asociado de 1, y por (DE1) se tiene $\delta(1) = \delta(a)$.

2 implica 3. Si $x \in D \setminus \{0\}$ entonces $1 \mid x$, y por (DE1) se tiene $\delta(a) = \delta(1) \leq \delta(x)$.

3 implica 1. Por (DE2) existen $q, r \in D$ tales que $1 = aq + r$ y o bien $r = 0$ o bien $\delta(r) < \delta(a)$; como la hipótesis excluye la segunda posibilidad, debe ser $r = 0$ y así $1 = aq$, por lo que a es invertible. □

Teorema 3.3.3 *Todo dominio euclídeo D es un dominio de ideales principales.*

Demostración. La demostración es esencialmente igual a la del Teorema 1.2.11. Por tanto, mencionaremos sus líneas maestras y dejaremos los detalles para el lector. Sea δ una función euclídea en D y sea I un ideal no nulo de D. Sea a un elemento no nulo de I tal que $\delta(a)$ es mínimo entre los elementos no nulos de I. Entonces $I = (a)$. □

El recíproco de este teorema es falso, pero no es fácil encontrar un DIP que no sea un dominio euclídeo. Un tal ejemplo[2] es el subanillo $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ de $\mathbb{C}$ formado por los elementos de la forma $a + b\frac{1+\sqrt{-19}}{2}$ con $a, b \in \mathbb{Z}$.

Como consecuencia del Teorema 3.3.3 y la Proposición 3.2.5, todo subconjunto de un dominio euclídeo tiene máximo común divisor y mínimo común múltiplo. De hecho, el Algoritmo de Euclides sirve en cualquier dominio euclídeo D para calcular el máximo común divisor de dos elementos de D y la correspondiente identidad de Bezout, lo que a su vez permite resolver ecuaciones del tipo

$$ax + by = c$$

en D. Las demostraciones de estos hechos son meras adaptaciones de las que hicimos en el Capítulo 1 para el anillo de los números enteros y se dejan a cargo del lector.

En el resto de esta sección vemos algunos ejemplos de dominios euclídeos y de cómo se usa en ellos el Algoritmo de Euclides.

Ejercicio 3.3.4 *Demostrar las afirmaciones siguientes.*

1. *Si D es un dominio y $\delta : D \to \mathbb{N}$ es una aplicación que conserva productos y verifica $\delta(x) = 0$ si y sólo si $x = 0$, entonces δ verifica (DE1) (estrictamente hablando, es su restricción a $D \setminus \{0\}$ la que lo verifica).*
2. *En particular, si $D = \mathbb{Z}[\sqrt{m}]$ y δ se define como el valor absoluto de la norma (o como la propia norma, cuando m es negativo), entonces δ satisface la condición (DE1).*
3. *Si además, dados $a, b \in D$ con $b \neq 0$, existen $q, r \in D$ con $a = bq + r$ y $\delta(r) < \delta(b)$ entonces δ es una función euclídea en D.*

Ejemplos 3.3.5 *Funciones euclídeas y dominios euclídeos.*

1. La aplicación valor absoluto $\mathbb{Z}^* \to \mathbb{N}$ es una función euclídea en $\mathbb{Z}$ (Teorema 1.1.8). En realidad, hay una sutil diferencia entre la división entera y este hecho: Dados $a, b \in \mathbb{Z}$, los elementos q y r postulados en (DE2) no son únicos; por ejemplo $42 = 5 \cdot 8 + 2 = 5 \cdot 9 + (-3)$.

[2] Una demostración de este hecho que sólo usa técnicas elementales puede consultarse en [Oscar A. Cámpoli, "A Principal Ideal Domain That Is Not Euclidean Domain", *The Teaching of Mathematics* (Noviembre 1988), 868-871].

2. Un ejemplo trivial de anillo euclídeo es un cuerpo K, pues entonces la aplicación que asocia 1 a todo elemento de K^* es una función euclídea.

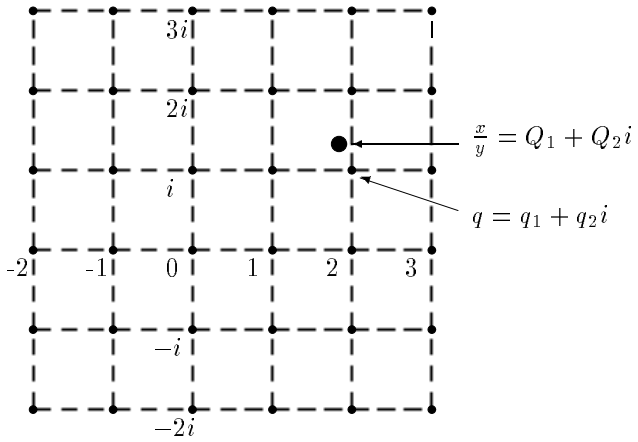
3. En el anillo $\mathbb{Z}[i]$ de los enteros de Gauss la norma $N : \mathbb{Z}[i] \to \mathbb{N}$ (dada por $N(a+bi) = a^2+b^2$) es una función euclídea. Por el Ejercicio 3.3.4 basta ver que, dados $a, b \in \mathbb{Z}[i]$ con $b \neq 0$, existen $q, r \in \mathbb{Z}[i]$ con $a = bq + r$ y $N(r) < N(b)$. Para ello, observemos primero que la norma puede extenderse a una función $N : \mathbb{Q}[i] \to \mathbb{Q}$ definida también por $N(a+bi) = a^2+b^2$ y que conserva productos. Como $\mathbb{Q}[i]$ es el cuerpo de cocientes de $\mathbb{Z}[i]$ (Ejemplo 2.9.6), existen $Q_1, Q_2 \in \mathbb{Q}$ tales que $\frac{a}{b} = Q_1 + Q_2 i$. Aproximando los Q_i por el entero más próximo encontramos $q_1, q_2 \in \mathbb{Z}$ y $R_1, R_2 \in \mathbb{Q}$ con $Q_i = q_i + R_i$ y $|R_i| \leq \frac{1}{2}$ para cada $i = 1, 2$. Entonces se tiene

$$a = b(Q_1 + Q_2 i) = b(q_1 + q_2 i) + b(R_1 + R_2 i),$$

de modo que podemos tomar a $q = q_1 + q_2 i$ como cociente y a $r = b(R_1 + R_2 i)$ como resto, pues está en $\mathbb{Z}[i]$ (vale $a - bq$) y verifica

$$N(r) = N(b(R_1 + R_2 i)) = N(b)N(R_1 + R_2 i) = N(b)(R_1^2 + R_2^2) \leq N(b)(\frac{1}{4} + \frac{1}{4}) < N(b).$$

El siguiente diagrama ilustra el proceso:



4. Una sencilla adaptación del argumento anterior permite ver que la norma es una función euclídea en $\mathbb{Z}[\sqrt{-2}]$ (el $\frac{1}{4} + \frac{1}{4}$ anterior se transforma en $\frac{1}{4} + 2\frac{1}{4}$, que sigue siendo menor que 1), pero esa adaptación ya no funciona con $\mathbb{Z}[\sqrt{-3}]$; de hecho, éste no es un dominio euclídeo (ni con la norma ni con ninguna otra posible función euclídea) porque ni siquiera es un DIP: contiene elementos irreducibles que no son primos (considérese la igualdad $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$).

Ejemplo 3.3.6 *Algoritmo de Euclides en* $\mathbb{Z}[i]$.

Vamos a calcular el máximo común divisor de $a = 2+2i$ y $b = -1+7i$ en $\mathbb{Z}[i]$ utilizando el Algoritmo de Euclides. Como $N(a) = 8$ y $N(b) = 50$, dividimos b entre a siguiendo el proceso explicado en el Ejemplo 3.3.5. Como

$$\frac{b}{a} = \frac{-1+7i}{2+2i} = \frac{(-1+7i)(2-2i)}{8} = \frac{12+16i}{8} = \frac{3}{2} + 2i,$$

tomamos $q = 1+2i$ y $r = b - aq = 1-i$. Es decir, empezamos construyendo la tabla

$b = -1+7i$	$a = 2+2i$	$1-i$
	$1+2i$	

Dividimos ahora a entre $r = 1-i$.

$$\frac{a}{r} = \frac{2+2i}{1-i} = \frac{(2+2i)(1+i)}{2} = \frac{4i}{2} = 2i.$$

Por tanto, completamos la tabla anterior:

$b=-1+7i$	$a=2+2i$	$1-i$	0
	$1+2i$	$2i$	

y deducimos que $\mathrm{mcd}(2+2i,-1+7i)=1-i$. El lector puede ahora encontrar la correspondiente identidad de Bezout, así como las soluciones en $\mathbb{Z}[i]$ de la ecuación $ax+by=5+3i$.

Obsérvese que no hay unicidad en la división euclídea en $\mathbb{Z}[i]$. Por ejemplo, tras obtener $b/a=(3/2)+2i$, podíamos haber elegido como primer cociente $q'=2+2i$, lo que nos habría dado un resto $r'=b-aq'=-1-i$, y como r' divide a a obtendríamos $\mathrm{mcd}(2+2i,-1+7i)=-1-i$. ¿Atenta esto contra la unicidad del máximo común divisor?

Otro ejemplo de dominios euclídeos lo constituyen los anillos de polinomios en una indeterminada con coeficientes en un cuerpo, como se demuestra a continuación. En la Proposición 4.1.4 y el Lema 4.3.1 se añadirán algunos matices al resultado que sigue.

Proposición 3.3.7 *Si K es un cuerpo, entonces el anillo de polinomios $K[X]$ es un dominio euclídeo. De hecho, la aplicación* $\mathrm{gr}: K[X]\setminus\{0\}\to\mathbb{N}$ *que asocia a cada polinomio f su grado* $\mathrm{gr}(f)$ *es una función euclídea.*

Demostración. Sabemos (Ejemplos 2.8.4) que $\mathrm{gr}(fg)=\mathrm{gr}(f)+\mathrm{gr}(g)$, de donde se deduce (DE1).

En cuanto a (DE2), fijemos $0\neq g\in K[X]$ con grado $m=\mathrm{gr}(g)$ y coeficiente principal $b\neq 0$ (invertible en K). Dado $f\in K[X]$ vamos a ver, por inducción en $n=\mathrm{gr}(f)$, que existen $q,r\in K[X]$ con $f=gq+r$ y $r=0$ ó $\mathrm{gr}(r)<m$. Si $n<m$ podemos tomar $q=0$ y $r=f$. Supongamos pues que $n\geq m$ y que la propiedad se verifica si f se sustituye por un polinomio de grado menor. Si a es el término principal de f, es claro que el polinomio $f_1=f-ab^{-1}X^{n-m}g\in K[X]$ tiene grado menor que el de f. Por hipótesis de inducción existen $q_1,r\in K[X]$ tales que $f_1=gq_1+r$ y $r=0$ o $\mathrm{gr}(r)<m$. Entonces $f=g(q_1+ab^{-1}X^{n-m})+r$, lo que termina la demostración. □

Ejemplo 3.3.8 *Algoritmo de Euclides en $\mathbb{Q}[X]$.*

Vamos a resolver la siguiente ecuación con incógnitas U y V en el anillo de polinomios $\mathbb{Q}[X]$:

$$(X^4-1)U+(X^2-2X+1)V=X^2-1.$$

Para ello calculamos el máximo común divisor de X^4+1 y X^2-2X+1:

X^4-1	X^2-2X+1	$4X-4$	0
	X^2+2X+3	$\frac{1}{4}(X-1)$	

Por tanto $\mathrm{mcd}(X^4-1,X^2-2X+1)=X-1$ (el "asociado cómodo" de $4X-4$), y como $X-1$ divide a X^2-1 deducimos que la ecuación tiene solución. Para encontrar una de ellas, utilizamos los cálculos del Algoritmo de Euclides para expresar el máximo común divisor en función de los coeficientes:

$$X-1=\frac{1}{4}(4X-4)=\frac{1}{4}(X^4-1)-\frac{X^2+2X+3}{4}(X^2-2X+1).$$

Multiplicando por $\frac{X^2-1}{X-1}=X+1$ se obtiene

$$X^2-1=(X+1)\left(\frac{X^4-1}{4}-\frac{X^2+2X+3}{4}(X^2-2X+1)\right)$$

de donde se deduce que $(U,V)=\left(\frac{X+1}{4},\frac{-(X+1)(X^2+2X+3)}{4}\right)$ es una solución particular de nuestra ecuación. Como $\frac{X^4-1}{X-1}=X^3+X^2+X+1$ y $\frac{X^2-2X+1}{X-1}=X-1$, la solución general es:

$$\begin{aligned} U &= \tfrac{X+1}{4}+(X-1)P \\ V &= -\tfrac{(X+1)(X^2+2X+3)}{4}-(X^3+X^2+X+1)P \end{aligned} \qquad (P\in\mathbb{Q}[X]).$$

3.4 Dominios de factorización única

Definición 3.4.1 *Sea D un dominio. Una* factorización en producto de irreducibles *de un elemento a de D es una expresión del tipo*

$$a = up_1 \cdots p_n$$

donde $n \in \mathbb{N}$, u es una unidad de D y $p_1, \ldots, p_n$ son irreducibles de D (se admite la posibilidad de que sea $n = 0$, en cuyo caso la factorización se reduce a $a = u$). Diremos que D es un dominio de factorización *si todo elemento no nulo de D admite una factorización en producto de irreducibles.*

Dos factorizaciones de $a \in D$ en producto de irreducibles se dice que son equivalentes si sólo se diferencian en el orden y en asociados. Dicho con más rigor, las factorizaciones

$$a = up_1 \cdots p_n = vq_1 \cdots q_m$$

(con $u, v \in D^*$ y el resto de factores irreducibles) son equivalentes *si $n = m$ y existe una* permutación *σ de $\mathbb{N}_n$ (una biyección de $\mathbb{N}_n = \{1, 2, \ldots, n\}$ en sí mismo) tal que p_i y $q_{\sigma(i)}$ son asociados para cada $i = 1, \ldots, n$. Diremos que D es un* dominio de factorización única *ó* DFU *(UFD, en inglés) si es un dominio de factorización en el que, para cada $0 \neq a \in D$, todas las factorizaciones de a son equivalentes.*

Comenzamos observando que, sobre un DFU, los elementos irreducibles coinciden con los primos, por lo que podemos hablar indistintamente de factorizaciones en irreducibles o factorizaciones en primos.

Lema 3.4.2 *Si D es un DFU, entonces todo elemento irreducible de D es primo.*

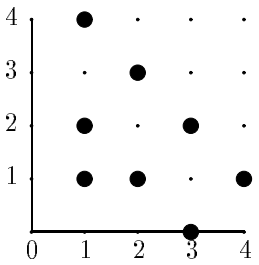
Demostración. Sea $p \in D$ irreducible, y sean $a, b, t \in D$ tales que $pt = ab$. Se trata de ver que $p \mid a$ ó $p \mid b$. Si $t = up_1 \cdots p_n$, $a = vq_1 \cdots q_m$ y $b = wr_1 \cdots r_k$ son factorizaciones en irreducibles (con $u, v, w \in D^*$), entonces se tiene

$$upp_1 \cdots p_n = (vw)q_1 \cdots q_m r_1 \cdots r_k,$$

y por la unicidad de la factorización p es asociado de algún q_i (y entonces $p \mid a$) o de algún r_i (y entonces $p \mid b$). □

Sea D un dominio y sea D_0 un conjunto de representantes de los elementos no nulos de D para la relación "ser asociados" (ver el Ejercicio 3.1.7). El conjunto P de los elementos de D_0 que son irreducibles es entonces un conjunto de representantes de los elementos irreducibles de D para la relación "ser asociados"; es decir, todo irreducible de D es asociado a un único elemento de P (¿por qué?). Por ejemplo, usando el Ejercicio 3.1.7, sabemos que:

- Si $D = \mathbb{Z}$ entonces podemos tomar como P el conjunto de los enteros primos positivos.
- Si $D = \mathbb{Z}[i]$ entonces podemos tomar como P el conjunto de los enteros de Gauss irreducibles del primer cuadrante (incluyendo el eje real positivo pero no el imaginario). De los puntos de $\mathbb{Z}[i]$ que aparecen en el siguiente gráfico, se han señalado los que están en P.



- Si K es un cuerpo y $D = K[X]$, podemos tomar como P el conjunto de los polinomios irreducibles con coeficiente principal 1.

Si D es un DFU y P es como en el párrafo anterior, entonces todo elemento no nulo a de D tiene una única factorización de la forma

$$a = u \prod_{p \in P} p^{\alpha_p}$$

donde u es una unidad de D, $\alpha_p \in \mathbb{N}$ para todo $p \in P$ y $\alpha_p = 0$ para casi todo $p \in P$. Llamaremos a ésta la *factorización prima* de a o la *factorización de a en irreducibles de P*. En muchos casos nos interesará escribir sólo los factores distintos de 1 (es decir, con exponente no nulo), y en ese caso tendremos una *factorización prima irredundante*. En otras ocasiones, como veremos en seguida, es conveniente dejar que aparezcan "factores ficticios" con exponente 0.

La gran ventaja de que un dominio sea un DFU es que la noción de divisibilidad, y por tanto todas las que dependen de ella, se pueden expresar en términos de las factorizaciones primas. En particular se pueden calcular el máximo común divisor y el mínimo común múltiplo de un conjunto a partir de esas factorizaciones. Dejaremos que el lector demuestre estos hechos, que se encuentran resumidos en el siguiente ejercicio.

Ejercicio 3.4.3 *Sean D un DFU y P un conjunto de representantes de los irreducibles de D por la relación de equivalencia "ser asociados". Sean*

$$a = u \prod_{p \in P} p^{\alpha_p} \qquad y \qquad b = v \prod_{p \in P} p^{\beta_p}$$

las factorizaciones de a y b en irreducibles de P. Demostrar:

1. *$a \mid b$ precisamente si $\alpha_p \leq \beta_p$, para todo $p \in P$.*
2. *El número de divisores de a es finito, salvo asociados. Es decir, existe un conjunto finito F tal que todos los divisores de a son asociados de un elemento de F.*
3. *Obtener una fórmula para calcular el número de divisores de a, salvo asociados, en términos de los exponentes α_p.*
4. $\mathrm{mcm}(a,b) = \prod_{p \in P} p^{\max(\alpha_p, \beta_p)}$.
5. $\mathrm{mcd}(a,b) = \prod_{p \in P} p^{\min(\alpha_p, \beta_p)}$.
6. *a y b son coprimos si y sólo si no tienen ningún divisor primo común.*

Las fórmulas de los apartados 4 y 5 del Ejercicio 3.4.3 se generalizan del modo obvio al caso de familias arbitrarias de elementos, con un precaución en el caso del cálculo del mínimo común múltiplo de familias infinitas: Si no existe alguno de los máximos que intervienen, ese mínimo común múltiplo vale 0. En particular, todo subconjunto de un DFU tiene un máximo común divisor y un mínimo común múltiplo.

Sin embargo, no es cierto en general que existan identidades de Bezout. Por ejemplo, en Capítulo 4 demostraremos que $D = \mathbb{Z}[X]$ es un DFU, y como 2 y X son irreducibles no asociados en D, deducimos que son coprimos; es decir, $\mathrm{mcd}(2, X) = 1$. Sin embargo $1 \notin (2, X)$ (ver el Ejemplo 2.5.9).

La unicidad en las factorizaciones permite demostrar resultados como este:

Proposición 3.4.4 *Sea D un DFU y sean $a, b, c \in D$, con a y b coprimos. Demostrar que:*

1. *$a + b$ y ab son coprimos.*
2. $\mathrm{mcd}(a, c) = \mathrm{mcd}(a, bc)$.
3. *Si $a \mid bc$ entonces $a \mid c$.*
4. *Si $a \mid c$ y $b \mid c$ entonces $ab \mid c$.*
5. *Si $ab = c^n$ (con $n \geq 2$) entonces existe $x \in D$ tal que a es asociado de x^n.*

Demostración. Usaremos repetidamente el Ejercicio 3.4.3, y fijaremos las siguientes factorizaciones en elementos de un conjunto de representantes de irreducibles P:

$$a = u\prod_{p\in P} p^{\alpha_p}, \qquad b = v\prod_{p\in P} p^{\beta_p} \qquad \text{y} \qquad c = w\prod_{p\in P} p^{\gamma_p}.$$

Como a y b son coprimos, para cada $p \in P$ se tiene $\alpha_p = 0$ ó $\beta_p = 0$ (tal vez ambos).

1. Si existiera un divisor primo común $p \in P$ de $a+b$ y de ab, entonces p dividiría a las combinaciones lineales $a(a+b) - ab = a^2$ y $b(a+b) - ab = b^2$, y por tanto p sería un divisor común de a y de b, lo cual es imposible.

2. Como $bc = vw\prod_{p\in P} p^{\beta_p+\gamma_p}$, basta ver que $\min(\alpha_p, \gamma_p) = \min(\alpha_p, \beta_p + \gamma_p)$ para cada $p \in P$, lo cual es obvio pues $\alpha_p = 0$ ó $\beta_p = 0$.

3. Es consecuencia de 2, pues $a \mid bc$ implica $a = \mathrm{mcd}(a, bc) = \mathrm{mcd}(a, c)$ y por tanto $a \mid c$.

4. Para cada $p \in P$ se tiene $\alpha_p \leq \gamma_p$ y $\beta_p \leq \gamma_p$ por hipótesis, y como $\alpha_p = 0$ ó $\beta_p = 0$ se tiene $\alpha_p + \beta_p \leq \gamma_p$. En consecuencia $ab \mid c$.

5. La igualdad $ab = c^n$ nos da la igualdad entre factorizaciones primas

$$uv\prod_{p\in P} p^{\alpha_p+\beta_p} = w\prod_{p\in P} p^{n\gamma_p},$$

por lo que $\alpha_p + \beta_p = n\gamma_p$ para cada $p \in P$. Si $\alpha_p \neq 0$ entonces $\beta_p = 0$ y por tanto $\alpha_p = n\gamma_p$. En consecuencia se tiene

$$\alpha = u\prod_{p\in P,\alpha_p\neq 0} p^{\alpha_p} = u\left(\prod_{p\in P,\alpha_p\neq 0} p^{\gamma_p}\right)^n,$$

y el resultado se obtiene tomando $x = \prod_{p\in P,\alpha_p\neq 0} p^{\gamma_p}$. □

Proposición 3.4.5 *Para un dominio D, las condiciones siguientes son equivalentes:*

1. *D es un dominio de factorización única.*

2. *D es un dominio de factorización en el que todo elemento irreducible es primo.*

Demostración. 1 implica 2. Por la definición de DFU y por el Lema 3.4.2.

2 implica 1. Por hipótesis, todo elemento no nulo de D se factoriza como un producto de primos, y podemos demostrar la unicidad de tales factorizaciones adaptando la demostración del Teorema Fundamental de la Aritmética (1.5.4). En efecto, sean $up_1\cdots p_n = vq_1\cdots q_m$, con p_i y q_i irreducibles para todo i, y $u, v \in D^*$. Suponemos que $n \leq m$ y razonamos por inducción sobre n. Si $n = 0$ entonces $m = 0$, ya que los divisores de unidades son unidades, y no hay nada que demostrar. Supongamos que $n > 0$ y, la hipótesis de inducción. Por hipótesis, p_n es primo, luego divide a algún q_i y de hecho son asociados (¿por qué?); además, reordenando si es necesario, podemos suponer que $i = m$. Es decir, existe una unidad w tal que $q_m = wp_n$. Entonces

$$up_1\cdots p_{n-1} = (vw)q_1\cdots q_{m-1}.$$

Por hipótesis de inducción se tiene $n-1 = m-1$ (luego $n = m$) y existe una biyección $\tau : \{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ tal que p_i y $q_{\tau(i)}$ son asociados para cada $i = 1, \ldots, n-1$. Ahora es evidente que τ se extiende a una permutación σ de $\mathbb{N}_n$ tal que p_i y $q_{\sigma(i)}$ son asociados para cada $i = 1, \ldots, n$, y por lo tanto las factorizaciones iniciales son equivalentes. □

Pero no hemos dado todavía ningún ejemplo de DFU, que no sea $\mathbb{Z}$. Vamos a terminar esta sección demostrando que todo DIP es un DFU. Esto, junto con los ejemplos de la sección anterior, nos proporciona ejemplos de dominios de factorización única. El recíproco del teorema que sigue es falso: en el siguiente capítulo veremos que $\mathbb{Z}[X]$ es un DFU que no es un DIP.

Teorema 3.4.6 *Todo dominio de ideales principales D es un dominio de factorización única.*

Demostración. Por las Proposiciones 3.4.5 y 3.2.3, basta con demostrar que D es un dominio de factorización. Por reducción al absurdo suponemos que D no lo es, y vamos a construir, por recurrencia, una sucesión $a_1, a_2, \ldots$ de elementos de D que no admiten factorización y tales que $(a_1) \subset (a_2) \subset \cdots$ es una cadena estrictamente creciente de ideales de D. Para el primer paso simplemente elegimos un elemento arbitrario a_1 de D que no admita factorización en irreducibles. Supongamos ahora que hemos elegido $a_1, \ldots, a_n$ satisfaciendo las condiciones requeridas. Entonces a_n no es irreducible, luego existen $x, y \in D \setminus D^*$ tales que $a_n = xy$. Como a_n no es producto de irreducibles, al menos uno de los factores x ó y (digamos que x) no es producto de irreducibles. Entonces, poniendo $a_{n+1} = x$, tenemos $(a_n) \subset (a_{n+1})$ con la inclusión estricta porque y no es una unidad.

Una vez construida la sucesión (a_i), tomamos $I = (a_1, a_2, \ldots) = \cup_{i \in \mathbb{Z}^+}(a_i)$ (dejamos que el lector compruebe la igualdad anterior). Como D es un DIP, existe $x \in D$ tal que $I = (x)$; en particular $x \in I = \cup_{i \in \mathbb{Z}^+}(a_i)$ y por tanto existe un índice i tal que $x \in (a_i)$; como es claro que $a_i \in (x)$, se tiene $(a_i) = (x) = I$ y por lo tanto $(a_i) = (a_{i+1})$, en contra de la construcción realizada. Este absurdo concluye la demostración. □

3.5 Aplicaciones de la factorización única

El hecho de que un dominio sea un DFU suele tener muchas aplicaciones en Teoría de Números. En esta sección vamos a ver tres de ellas: La determinación de todos los números naturales que son suma de dos cuadrados, la descripción de los triángulos rectángulos con lados enteros, y la solución del Último Teorema de Fermat para el exponente 4. Consideraremos el dominio $\mathbb{Z}$ de los números enteros y el dominio $\mathbb{Z}[i]$ de los enteros de Gauss, y en el camino daremos una descripción precisa de los elementos irreducibles del segundo.

Sumas de cuadrados en $\mathbb{Z}$ e irreducibles en $\mathbb{Z}[i]$

Comencemos preguntándonos qué numeros naturales son suma de dos cuadrados. El lector puede analizar los casos pequeños y tratar de sacar conclusiones. Quizás no se haga evidente una regla general, pero si nos fijamos en los números primos parece que sólo el 2 y los que son congruentes con 1 módulo 4 son suma de dos cuadrados. De modo que puede ser interesante atacar primero el "caso primo", pero esto sólo nos servirá para el caso general si probamos que la condición es multiplicativa. Esto es lo que hacemos en el primer lema, que además nos indica el papel que va a representar $\mathbb{Z}[i]$ en este problema.

Lema 3.5.1 *1. Un entero es la suma de dos cuadrados en $\mathbb{Z}$ si y sólo si es la norma de un elemento de $\mathbb{Z}[i]$; es decir, si es de la forma $N(x) = x\bar{x}$ con $x \in \mathbb{Z}[i]$.*

2. Si los enteros $n_1, \ldots, n_r$ se expresan como suma de dos cuadrados en $\mathbb{Z}$, lo mismo le ocurre a su producto $n_1 \cdots n_r$.

Demostración. El apartado 1 es claro. En 2, para cada $i = 1, \ldots, r$ existe $x_i \in \mathbb{Z}[i]$ tal que $n_i = N(x_i)$, y entonces, poniendo $x = x_1 \cdots x_r$, se tiene

$$n_1 \cdots n_r = N(x_1) \cdots N(x_r) = N(x_1 \cdots x_r) = N(x),$$

lo que demuestra la afirmación. □

Para abordar el caso primo comenzamos con un resultado clásico sobre congruencias que usaremos como herramienta en la siguiente demostración y que deducimos aquí de un resultado más general:

Lema 3.5.2 (Teorema de Wilson) *Si K es un cuerpo finito entonces el producto de todos sus elementos no nulos vale -1. En particular, si p es un entero positivo primo, se verifica la congruencia*

$$(p-1)! \equiv -1 \bmod p$$

.

Demostración. En $K^* = K \setminus \{0\}$ definimos la relación dada por $a \sim b$ si $a = b$ ó $a = b^{-1}$, que es claramente de equivalencia. En K^* hay dos clases de equivalencia (sólo una si la característica de K es 2) que constan de un solo elemento: $\{1\}$ y $\{-1\}$, y el resto de clases consta exactamente de dos elementos a y a^{-1} (no puede haber más de dos elementos en cada clase por la unicidad del inverso, y hay dos porque $a = a^{-1}$ implicaría $a^2 = 1$, o sea $(a+1)(a-1) = a^2 - 1 = 0$, y por lo tanto sería $a = -1$ ó $a = 1$). Como estas clases forman una partición de K^*, al hacer el producto los pares equivalentes se van simplificando y sólo sobrevive el -1. (Si la característica de K es 2 entonces $1 = -1$ y la demostración sigue valiendo). El caso particular se obtiene considerando el cuerpo finito $\mathbb{Z}_p$. □

Proposición 3.5.3 (Fermat) *Para un entero positivo primo p, son equivalentes las condiciones:*

1. *p es suma de dos cuadrados en $\mathbb{Z}$.*
2. *$p \not\equiv 3 \bmod 4$*
3. *$p = 2$ ó $p \equiv 1 \bmod 4$.*
4. *La ecuación $X^2 \equiv -1 \bmod p$ tiene soluciones enteras (o la ecuación $X^2 = -1$ las tiene en $\mathbb{Z}_p$).*
5. *p no es irreducible (ni primo) en $\mathbb{Z}[i]$.*

En este caso, la expresión de p como suma de dos cuadrados, $p = a^2 + b^2$, es única salvo el orden y el signo de a y b.

Demostración. 1 implica 2. Como $0^2 \equiv 2^2 \equiv 0 \bmod 4$ y $1^2 \equiv 3^2 \equiv 1 \bmod 4$, una suma de dos cuadrados no puede ser congruente con 3 módulo 4.

2 implica 3. Un primo positivo o es 2 o es impar, y en este caso sólo puede vale 1 ó 3 módulo 4, pero la última posibilidad está excluida por la hipótesis.

3 implica 4. Si $p = 2$, el 1 es solución. Si $p = 4t+1$, usando el Teorema de Wilson (3.5.2) y operando módulo p, se tiene

$$\begin{aligned} -1 &\equiv (p-1)! \equiv (4t)! \\ &= 1 \cdot 2 \cdots (2t-1)(2t)(2t+1)(2t+2) \cdots (4t-1)(4t) \\ &\equiv 1 \cdot 2 \cdots (2t-1)(2t)(-(2t))(-(2t-1)) \cdots (-2)(-1) \\ &= (-1)^{2t}((2t)!)^2 = ((2t)!)^2, \end{aligned}$$

de modo que $(2t)!$ es solución.

4 implica 5. Si existe $n \in \mathbb{Z}$ con $n^2 \equiv -1 \bmod p$ entonces $p \mid n^2+1$ en $\mathbb{Z}$ y por lo tanto $p \mid (n+i)(n-i)$ en $\mathbb{Z}[i]$. Como es claro que p no divide a $n+i$ ni a $n-i$ en $\mathbb{Z}[i]$, deducimos que p no es primo en $\mathbb{Z}[i]$.

5 implica 1. Por hipótesis existen $x, y \in \mathbb{Z}[i]$, no unidades, con $p = xy$; por lo tanto se tiene, en $\mathbb{Z}$, $p^2 = N(p) = N(xy) = N(x)N(y)$, y como $N(x), N(y) > 1$ por no ser unidades, deducimos que $N(x) = N(y) = p$. En particular, si $x = a + bi$ con $a, b \in \mathbb{Z}$, se tiene $p = a^2 + b^2$.

En cuanto a la unicidad, si $p = a^2 + b^2 = c^2 + d^2$, con $a, b, c, d \in \mathbb{Z}$, entonces los elementos $a \pm bi$ y $c \pm di$ son irreducibles en $\mathbb{Z}[i]$ por tener norma prima, de modo que $p = (a+bi)(a-bi) = (c+di)(c-di)$ son factorizaciones en irreducibles de p. Por la unicidad de la factorización se deduce que $c + di$ es asociado de $a + bi$ o de $a - bi$, y en consecuencia $c + di$ es igual a uno de estos:

$$a + bi, \quad -a - bi, \quad b - ai, \quad -b + ai, \quad a - bi, \quad -a + bi, \quad b + ai, \quad -b - ai,$$

lo que prueba la afirmación del enunciado. □

La demostración del caso general requiere el siguiente resultado, bien interesante por sí mismo.

Proposición 3.5.4 *Un entero de Gauss es irreducible si y sólo si es de una de estas dos formas:*

Tipo A: *$\pm p$ ó $\pm pi$, donde p es un entero positivo primo y $p \equiv 3 \bmod 4$.*

Tipo B: *$a + bi$ con $a^2 + b^2$ primo en $\mathbb{Z}$. En este caso $a^2 + b^2 \not\equiv 3 \bmod 4$.*

En consecuencia, un conjunto de representantes salvo asociados de los irreducibles de $\mathbb{Z}[i]$ está formado por los enteros primos positivos congruentes con 3 módulo 4 y por los elementos de norma prima del primer cuadrante.

Demostración. Los elementos del tipo A son irreducibles en $\mathbb{Z}[i]$ por la Proposición 3.5.3, y los del tipo B lo son por tener norma prima (Ejemplos 3.1.10) y ésta no es congruente con 3 módulo 4 por la Proposición 3.5.3. Se trata de ver que no hay más irreducibles en $\mathbb{Z}[i]$; sea pues $x = a + bi$ uno de ellos. Si $a = 0$ ó $b = 0$ entonces x es asociado de un entero positivo, que obviamente debe ser primo y entonces debe ser congruente con 3 módulo 4 por la Proposición 3.5.3; por consiguiente, x es del tipo A en este caso. En el otro caso, como $\bar{x}$ también es irreducible en $\mathbb{Z}[i]$ (¿por qué?), $a^2 + b^2 = x\bar{x}$ es una factorización en irreducibles en $\mathbb{Z}[i]$. Si el entero $a^2 + b^2$ se factorizase en $\mathbb{Z}$ tendríamos dos factorizaciones en irreducibles no equivalentes (¿por qué?) en $\mathbb{Z}[i]$, que es un DFU. Deducimos que $a^2 + b^2$ es un entero primo y por lo tanto x es del tipo B. □

Ejemplo 3.5.5 *Factorizaciones en $\mathbb{Z}[i]$.*

Factorizar en $\mathbb{Z}[i]$ un elemento α que esté en $\mathbb{Z}$ no es mucho más difícil que factorizarlo en $\mathbb{Z}$: Primero se factoriza α en $\mathbb{Z}$; los factores primos que no sean congruentes con 3 módulo 4 siguen siendo primos en $\mathbb{Z}[i]$ y los otros son el producto de dos primos de $\mathbb{Z}[i]$. Por ejemplo,

$$252 = 2^2 \cdot 3^2 \cdot 7 = [(1+i)(1-i)]^2 \cdot 3^2 \cdot 7 = (1+i)^2 \cdot (1-i)^2 \cdot 3^2 \cdot 7$$

es la factorización prima de 252, y

$$46631 = 211 \cdot 13 \cdot 17 = 211 \cdot (2^2 + 3^2) \cdot (1^2 + 4^2) = 211(2+3i)(2-3i)(1+4i)(1-4i)$$

es la factorización de 46631.

Las factorizaciones de elementos de $\mathbb{Z}$ también son útiles para factorizar en $\mathbb{Z}[i]$ elementos que no están en $\mathbb{Z}$. En efecto, dado $\alpha \in \mathbb{Z}[i]$ podemos factorizar $N(\alpha) = \alpha \cdot \bar{\alpha}$ en $\mathbb{Z}[i]$, y en esa factorización estarán todos los divisores primos de α. Por ejemplo, si $\alpha = 5 + i$ entonces

$$\alpha \cdot \bar{\alpha} = 5^2 + 1^2 = 26 = 2 \cdot 13 = (1+i)(1-i)(3+2i)(3-2i),$$

y dividiendo α entre $1 + i$ se obtiene la factorización prima $\alpha = (1+i)(3-2i)$.

Veamos un caso más complicado, por ejemplo $\alpha = 33 + 4i$. Entonces

$$\alpha \cdot \bar{\alpha} = 33^2 + 4^2 = 1105 = 5 \cdot 13 \cdot 17 = (2+i)(2-i)(3+2i)(3-2i)(4+i)(4-i).$$

De cada par de factores conjugados, uno divide a α y el otro a $\bar{\alpha}$. Dividiendo con resto se obtiene $\frac{\alpha}{2+i} = 14 - 5i$, que no es divisible por $3 + 2i$ pero sí por su conjugado, de hecho $\frac{14-5i}{3-2i} = 4 - i$, lo que nos da la factorización

$$\alpha = (2+i)(3-2i)(4-i).$$

La Proposición 3.5.4 nos permite, por fin, caracterizar los enteros que son suma de dos cuadrados. Obsérvese que no podemos decir nada (sencillo) sobre la unicidad, pues se tienen situaciones como $25 = 0^2 + 5^2 = 3^2 + 4^2$, $169 = 0^2 + 13^2 = 5^2 + 12^2$ ó $1125 = 6^2 + 33^2 = 15^2 + 30^2$.

Teorema 3.5.6 *Un entero positivo n es suma de dos cuadrados si y sólo cada entero primo positivo congruente con 3 módulo 4 tiene multiplicidad par en n. Es decir, si en su descomposición prima irredundante (con primos positivos), los primos congruentes con 3 módulo 4 tienen exponente par.*

Demostración. Si, al factorizar n como producto de enteros primos positivos, los que son congruentes con 3 módulo 4 aparecen con exponente par, podemos agruparlos y escribir $n = m^2 p_1 \cdots p_r$ con cada p_i en las condiciones de la Proposición 3.5.3. Entonces n es suma de dos cuadrados por el Lema 3.5.1 (¡porque $m^2 = m^2 + 0^2$!).

Recíprocamente, si n es suma de dos cuadrados, entonces $n = N(x)$ con $x \in \mathbb{Z}[i]$ (Lema 3.5.1). Por la Proposición 3.5.4, la factorización en irreducibles de x en $\mathbb{Z}[i]$ podemos ponerla como $x = p_1 \cdots p_r z_1 \cdots z_s$ con cada p_i del tipo A, que podemos suponer en $\mathbb{Z}$, y cada z_i del tipo B. Entonces

$$n = N(x) = p_1^2 \cdots p_r^2 N(z_1) \cdots N(z_s),$$

y los $N(z_i)$ son enteros primos no congruentes con 3 módulo 4. □

Ternas pitagóricas

Definición 3.5.7 *Una terna (a,b,c) de enteros positivos tales que $a^2+b^2=c^2$ se llama* terna pitagórica. *Los enteros a y b son los* catetos *de la terna, y c es su* hipotenusa. *La terna es* primitiva *si sus catetos son coprimos (es decir,* $\mathrm{mcd}(a,b)=1$*) y b es par.*

Las siguientes ternas son pitagóricas, y sólo las 3 primeras son primitivas:

$$(3,4,5)\quad (5,12,13)\quad (55,48,73)\quad (24,7,25)\quad (45,24,51)\quad (80,18,82).$$

Por el Teorema de Pitágoras, cada terna pitagórica se corresponde con un triángulo rectángulo tal que la longitud de sus tres lados (con respecto a cierta unidad de medida) es un entero. El objetivo en este apartado es la descripción de todas las ternas pitagóricas, y en consecuencia la de todos esos triángulos[3].

Lema 3.5.8 *Toda terna pitagórica se obtiene a partir de una primitiva, multiplicando cada componente de ésta por el mismo entero positivo y, si es necesario, cambiando el orden de sus catetos.*

Es decir, dada cualquier terna pitagórica (a,b,c), existen una terna pitagórica primitiva (a',b',c') y un entero positivo t tales que

$$a=ta', b=tb', c=tc' \qquad \text{ó} \qquad a=tb', b=ta', c=tc'.$$

Demostración. Comencemos observando que, si (a,b,c) es una terna pitagórica arbitraria, entonces a y b no pueden ser simultáneamente impares, pues en ese caso la igualdad $a^2+b^2=c^2$ implicaría $c^2\equiv 2 \bmod 4$, lo cual es imposible.

Si t es el máximo común divisor positivo de a y b, entonces es obvio que $(a/t, b/t, c/t)$ es una terna pitagórica con catetos coprimos, y por el párrafo anterior uno (y sólo uno) de ellos ha de ser par. Cambiando el orden de los catetos si es necesario, obtenemos la terna primitiva del enunciado. □

Las ternas primitivas asociadas a las que hemos mostrado anteriormente son:

$$(3,4,5)\quad (5,12,13)\quad (55,48,73)\quad (7,24,25)\quad (15,8,17)\quad (9,40,41).$$

En el siguiente teorema describimos todas las ternas pitagóricas primitivas. Combinándolo con el Lema 3.5.8, tendremos descritas todas las ternas pitagóricas.

Teorema 3.5.9 *Si $r>s>0$ son enteros coprimos y $r \not\equiv s \bmod 2$, entonces*

$$(r^2-s^2,\ 2rs,\ r^2+s^2)$$

es una terna pitagórica primitiva, y toda terna pitagórica primitiva es de esa forma.

Demostración. Dados r y s en esas condiciones, se comprueba operando que la terna dada es pitagórica, y es obvio que su segundo cateto es par. Supongamos que un primo p divide a r^2-s^2 y a $2rs$. La condición $r\not\equiv s \bmod 2$ implica que r^2-s^2 es impar, y por tanto p es un primo impar. De la condición $p \mid 2rs$ se deduce entonces que $p \mid r$ ó $p \mid s$. La primera opción implica $p \mid r^2$, por lo que $p \mid s^2$ (pues $p \mid r^2-s^2$) y en consecuencia $p \mid s$, lo cual es imposible porque r y s son coprimos. De igual modo se descarta la segunda opción, y en consecuencia r^2-s^2 y $2rs$ son coprimos, por lo que la terna pitagórica $(r^2-s^2, 2rs, r^2+s^2)$ es primitiva.

Veamos ahora que toda terna pitagórica primitiva (a,b,c) tiene la forma requerida.

Comenzamos demostrando que los elementos $a+bi$ y $a-bi$ son coprimos en $\mathbb{Z}[i]$. Supongamos que $\gamma\in\mathbb{Z}[i]$ es un divisor primo común de $a+bi$ y $a-bi$. Entonces γ divide a la suma y a la diferencia, de donde $\gamma \mid 2a$ y $\gamma \mid 2b$. Como $\mathrm{mcd}(a,b)=1$ en $\mathbb{Z}[i]$ (¿por qué?), debe ser $\gamma \mid 2$ y por tanto γ es asociado de $1+i$ (¿por qué?). Pero esto implica que $a\equiv b \bmod 2$ (Ejercicio 2.5.5), lo que contradice el hecho de que la terna (a,b,c) sea primitiva.

Como en $\mathbb{Z}[i]$ se tiene $(a+bi)(a-bi)=a^2+b^2=c^2$, el párrafo anterior y la Proposición 3.4.4 implican que $a+bi$ es asociado de $(r+si)^2$ para cierto elemento $r+si$ de $\mathbb{Z}[i]$. Sustituyendo $r+si$ por

[3] Se han encontrado listas de ternas pitagóricas en tablas babilónicas datadas entre los años 1900 y 1600 antes de Cristo. Parece ser que Pitágoras visitó Babilonia antes de establecerse en el sur de lo que hoy es Italia, donde nació el "grupo de los Pitagóricos".

su opuesto, si hace falta, podemos asumir que $r \geq 0$, y de hecho $r > 0$ pues de lo contrario a ó b sería 0. Las opciones son

$$a + bi = \pm(r + si)^2 = \pm[(r^2 - s^2) + 2rsi] \qquad \text{ó} \qquad a + bi = \pm i(r + si)^2 = \pm[2rs - (r^2 - s^2)i],$$

y como b es par y a no lo es, se tiene una de las primeras. La opción $a + bi = (r + si)^2$ equivale a

$$a = r^2 - s^2, \qquad b = 2rs$$

con $s > 0$ (pues $b > 0$) y $r > s$ (pues $a > 0$). La opción $a + bi = -(r + si)^2$ equivale a

$$a = (-s)^2 - r^2, \qquad b = 2(-s)r$$

con $-s > 0$ (pues $b > 0$) y $-s > r$ (pues $a > 0$). Además r y s son coprimos en $\mathbb{Z}$, pues un divisor primo común dividiría claramente a los dos catetos. Finalmente, se tiene $r \not\equiv s \bmod 2$, pues de lo contrario a sería par. En consecuencia (a, b, c) tiene la forma requerida. □

Es muy fácil ver que la asignación $(r, s) \mapsto (r^2 - s^2, 2rs, r^2 + s^2)$ es inyectiva si r y s son positivos. Por tanto, esa asignación define una biyección entre el conjunto de los pares (r, s) que satisfacen las condiciones del Teorema 3.5.9, y el conjunto de todas las ternas pitagóricas primitivas. También es elemental ver que la biyección inversa viene dada por

$$(a, b, c) \mapsto \left(\sqrt{\frac{a + c}{2}}, \frac{b}{\sqrt{2(a + c)}} \right).$$

Así, las ternas pitagóricas primitivas mostradas más arriba se corresponden, en el mismo orden, con

$$(2, 1) \quad (3, 2) \quad (8, 3) \quad (4, 3) \quad (4, 1) \quad (5, 4).$$

El Último Teorema de Fermat (exponente 4)

La historia de este teorema es bien conocida. Las ternas pitagóricas son las soluciones enteras positivas de la ecuación $X^2 + Y^2 = Z^2$. Fermat, hacia 1637, afirmó sin demostrarlo que, para cualquier exponente $n \geq 3$, la ecuación

$$X^n + Y^n = Z^n$$

no tiene soluciones enteras no triviales (es decir, con $XYZ \neq 0$; es elemental ver que esto equivale a que no tenga soluciones positivas; es decir, con $X, Y, Z \in \mathbb{Z}^+$). Los esfuerzos realizados durante siglos por demostrar este resultado contribuyeron enormemente al desarrollo de la Teoría de Números. Por citar un ejemplo, en algunas supuestas demostraciones se cometió el error de asumir que en cualquier subanillo de $\mathbb{C}$ hay factorización única, lo que dio origen al concepto abstracto de DFU. Finalmente, en la última década del siglo XX, Andrew Wiles (con la ayuda de R. Taylor) demostró el teorema combinando diversas técnicas que los citados esfuerzos habían "generado", y que han tenido aplicaciones en muchos otros contextos.

En este apartado demostraremos el Último Teorema de Fermat para el exponente $n = 4$. De hecho, veremos algo un poco más fuerte: la ecuación

$$X^4 + Y^4 = Z^2 \tag{3.5.2}$$

no posee soluciones positivas. La estrategia que emplearemos se debe al propio Fermat y se conoce como el "Método del Descenso Infinito". Vamos a demostrar, usando los resultados sobre ternas pitagóricas, que a partir de una supuesta solución positiva (a, b, c) de la ecuación, se obtiene otra solución positiva (A, B, C) con $C < c$. Repitiendo el proceso encontraríamos una sucesión estrictamente decreciente infinita de enteros positivos, lo cual es absurdo.

Supongamos pues que (a, b, c) es una solución positiva de (3.5.2); es decir, que $a^4 + b^4 = c^2$. Si $d = \text{mcd}(a, b) > 1$ entonces $d^2 \mid c$ y $(A, B, C) = (\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2})$ es una solución positiva de (3.5.2) con $C < c$, que es lo que buscamos. Podemos pues suponer que a y b son coprimos, e intercambiando a con b si es

necesario podemos suponer que a es impar. Por tanto, (a^2, b^2, c) es una terna pitagórica primitiva, y por el Teorema 3.5.9 existen enteros $r > s > 0$, coprimos y de distinta paridad, tales que

$$a^2 = r^2 - s^2, \qquad b^2 = 2rs, \qquad c = r^2 + s^2.$$

Considerando la primera de esas igualdades módulo 4 se deduce que r es impar y s es par. Además, todo divisor primo de s divide a $b^2 = 2rs$ y por tanto a b, por lo que a y s son coprimos. Así, (a, s, r) es una terna pitagórica primitiva, y por consiguiente existen enteros coprimos $u > v > 0$ tales que

$$a = u^2 - v^2, \qquad s = 2uv, \qquad r = u^2 + v^2.$$

Se tiene pues $b^2 = 4ruv$, y la Proposición 3.4.4 nos dice que r, u y v son asociados de cuadrados en $\mathbb{Z}$, y de hecho son cuadrados por ser positivos. Poniendo $r = C^2$, $u = A^2$ y $v = B^2$ con $A, B, C > 0$ se obtiene una solución positiva (A, B, C) de (3.5.2) con $C = \sqrt{r} \leq r^2 < c$, que es lo que buscamos.

3.6 Problemas

1. Sea $f : A \to B$ un isomorfismo de anillos, y sean $a, a' \in A$. Demostrar (hasta estar seguro de que se va a saber demostrar el resto) los siguientes apartados:

   (a) $a \mid a'$ en A si y sólo si $f(a) \mid f(a')$ en B.

   (b) a y a' son asociados en A si y sólo si $f(a)$ y $f(a')$ son asociados en B.

   (c) d es el máximo común divisor en A del subconjunto S si y sólo si $f(d)$ es el máximo común divisor en B del subconjunto $f(S)$.

   (d) d es el mínimo común múltiplo en A del subconjunto S si y sólo si $f(d)$ es el mínimo común múltiplo en B del subconjunto $f(S)$.

   (e) Un elemento $a \in A$ es irreducible en A si y sólo si $f(a)$ es irreducible en B.

   (f) Un elemento $a \in A$ es primo en A si y sólo si $f(a)$ es primo en B.

   (g) Los elementos a y a' de A son coprimos si y sólo si los elementos $f(a)$ y $f(a')$ de B son coprimos.

   (h) A es un DIP si y sólo si B es un DIP.

   (i) A es un dominio euclídeo si y sólo si B es un dominio euclídeo.

   (j) A es un dominio de factorización si y sólo si B es un dominio de factorización.

   (k) A es un DFU si y sólo si B es un DFU.

2. Calcular el cociente y el resto de las siguientes divisiones:

   (a) $X^5 - 1$ entre $X^2 + 3X$, en $\mathbb{Z}_5[X]$.

   (b) $X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ entre $X^3 + X^2 + X + 1$ en $\mathbb{Z}_2$.

3. Calcular el máximo común divisor y el mínimo común múltiplo de:

   (a) $X^4 + 3X^3 + 4X^2 + 2X$ y $X^5 + X^2$ en $\mathbb{R}[X]$.

   (b) $16 + 17i$ y $3 + 2i$ en $\mathbb{Z}[i]$.

   (c) $20 + 17i$ y $4 + 5i$ en $\mathbb{Z}[i]$.

4. Hallar el inverso de $X^2 + X + 1 + (X^5 - 2)$ en $\mathbb{Q}[X]/(X^5 - 2)$. Como aplicación, racionalizar la siguiente expresión (es decir, transformarla en otra equivalente sin raíces en el denominador):

$$\frac{\sqrt[5]{2} - 3}{\sqrt[5]{4} + \sqrt[5]{2} + 1}.$$

5. Si D es un dominio y $a, b, c \in D$, demostrar que:

   (a) Si existe $d = \mathrm{mcd}(a, b)$ entonces existe $\mathrm{mcd}(a + bc, b)$ y vale d.

   (b) Si existe $\mathrm{mcm}(a, b)$ entonces existe $\mathrm{mcd}(a, b)$. ¿Es cierto el recíproco?

   (c) Si existen $d = \mathrm{mcd}(a, b)$ y $t = \mathrm{mcd}(ca, cb)$ entonces t es asociado de cd.

   (d) Si existe el máximo común divisor de cualquier par de elementos de D entonces existe el mínimo común múltiplo de cualquier par de elementos de D. ¿Es cierto el recíproco?

6. Sea D un dominio y supongamos que existe una aplicación $\mu : D \to \mathbb{N}$ que verifica las tres propiedades siguientes:

   - $\mu(ab) = \mu(a)\mu(b)$ para cualesquiera $a, b \in D$.
   - $\mu(a) = 0$ si y sólo si $a = 0$.
   - $\mu(a) = 1$ si y sólo si a es invertible.

   Demostrar que D es un dominio de factorización (no necesariamente única), y deducir que $\mathbb{Z}[\sqrt{m}]$ lo es para cualquier $m \in \mathbb{Z}$.

7. Factorizar el elemento $5 + \sqrt{3}$ como producto de irreducibles en $\mathbb{Z}[\sqrt{3}]$.

8. Mostrar mediante ejemplos que las propiedades de la Proposición 3.4.4 (excepto la primera) no son ciertas en general sobre un dominio de factorización.

9. Demostrar que si $f : A \to B$ es un homomorfismo suprayectivo entre dominios de ideales principales, entonces f es un isomorfismo o B es un cuerpo.

10. Sea δ una función euclídea en D tal que $\delta(xy) = \delta(x)\delta(y)$ para todo $x, y \in D \setminus \{0\}$. Demostrar, para $a \in D$, que si $\delta(a)$ es un número primo diferente de $\delta(1)$, entonces a es irreducible en D. ¿Es cierto el recíproco?

11. Sea $\omega = \frac{-1+\sqrt{-3}}{2}$ una raíz cúbica de 1 y sea $D = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$. Demostrar que D es un subanillo del anillo de números complejos y que $\delta(a + b\omega) = a^2 - ab + b^2$ es una función euclídea en D. Calcular las unidades de D. (Indicación: Representar los elementos de D en el plano.)

12. [*] Demostrar las afirmaciones siguientes:

    (a) Sean D un dominio, K su cuerpo de cocientes y $\delta : K^* \to \mathbb{Q}^*$ una aplicación que conserva productos y tal que $\delta(D \setminus \{0\}) \subseteq \mathbb{N}$. Entonces la restricción de δ a $D \setminus \{0\}$ es una función euclídea en D precisamente si para todo $x \in K \setminus D$ existe $y \in D$ tal que $\delta(x - y) < 1$.

    (b) Sea m un entero negativo libre de cuadrados y sea $\delta : \mathbb{Q}[\sqrt{m}]^* \to \mathbb{Q}$ la aplicación dada por $\delta(a + b\sqrt{m}) = a^2 - mb^2$. Entonces la restricción de δ a $\mathbb{Z}[\sqrt{m}] \setminus \{0\}$ es una función euclídea precisamente si $m = -1$ ó $m = -2$.

    (c) Si además $m \equiv 1 \bmod 4$, entonces la restricción de δ a $\mathbb{Z}[\frac{1+\sqrt{m}}{2}] \setminus \{0\}$ es una función euclídea precisamente si $m = -3$, -7 ó -11. ¿Prueba esto que $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ no es un dominio euclídeo? ¿Por qué hemos hecho esta pregunta?

    (d) Las restricciones de δ a $\mathbb{Z}[\sqrt{2}]$ y a $\mathbb{Z}[\sqrt{3}]$ son normas euclídeas.

13. ¿Para qué valores de $a, b \in \mathbb{Z}$ son asociados en $\mathbb{Z}[i]$ los elementos $a + bi$ y $a - bi$?

14. Determinar todos los irreducibles de $\mathbb{Z}[i]$ con norma ≤ 5.

15. Encontrar todos los divisores de $X^4 + 3X^3 + 4X^2 + X + 4$ en $\mathbb{Z}_5[X]$.

16. En $\mathbb{Z}[i]$, encontrar todos los pares de elementos que pueden aparecer como cociente y resto para la división de $1 + 2i$ entre $1 + i$. Repetir para la división de $11 + 7i$ entre $2 + 5i$.

17. Encontrar todas las soluciones (X, Y) en $\mathbb{Z}[i]$ de cada una de las ecuaciones siguientes:

    (a) $(2+2i)X + (1-7i)Y = 4-6i$.

    (b) $(4+5i)X + (20+17i)Y = 0$.

    (c) $(11-7i)X + (14-3i)Y = 3-4i$.

18. Calcular en $\mathbb{Z}[\sqrt{-2}]$ el máximo común divisor de los elementos $\alpha = 5 - 2\sqrt{-2}$ y $\beta = 1 + 5\sqrt{-2}$, así como la correspondiente identidad de Bezout.

19. Sea D un DIP, sea $0 \neq a \in D \setminus D^*$ y sea $a = p_1^{n_1} \cdots p_r^{n_r}$ la factorización prima irredundante de a en D. Demostrar que existe un isomorfismo de anillos

$$\frac{D}{(a)} \cong \frac{D}{(p_1^{n_1})} \times \cdots \times \frac{D}{(p_r^{n_r})}.$$

20. Se pide, para los siguientes elementos de $\mathbb{Z}[i]$:

$$\alpha_1 = 3+i, \quad \alpha_2 = 4430, \quad \alpha_3 = 4437, \quad \alpha_4 = 4+3i, \quad \alpha_5 = 75+28i.$$

    (a) Expresar cada α_i como producto de irreducibles de $\mathbb{Z}[i]$.

    (b) Calcular el máximo común divisor y el mínimo común múltiplo de cada dos de ellos.

    (c) Describir todos los ideales primos de cada uno de los anillos $\frac{\mathbb{Z}[i]}{\alpha_i}$. ¿Cuáles de ellos son maximales?

    (d) Calcular la característica de cada uno de los anillos $\frac{\mathbb{Z}[i]}{\alpha_i}$. (Indicación: Usar el Problema 19 de este capítulo, y el Problema 25 del Capítulo 2.)

21. Dados $a, b \in \mathbb{Z}$, demostrar que:

    (a) $a + bi$ es múltiplo de $1 + i$ si y sólo si $a \equiv b \bmod 2$.

    (b) $a + bi$ es coprimo con 2 en $\mathbb{Z}[i]$ si y sólo si $a \not\equiv b \bmod 2$.

    (c) Si $a \not\equiv b \bmod 2$ entonces en $\mathbb{Z}[i]$ se tiene $\mathrm{mcd}(a, b) = \mathrm{mcd}(a + bi, a - bi)$.

    (d) Si a y b son coprimos en $\mathbb{Z}$ y b es par entonces $a + bi$ y $a - bi$ son coprimos en $\mathbb{Z}[i]$.

22. Demostrar que si A es un DIP y $0 \neq b \in A$, entonces el número de ideales de A que contienen a b es finito.

23. Sea A un DIP.

    (a) Probar que todo ideal propio de A se puede poner de forma única, salvo el orden, como producto de ideales maximales.

    (b) Demostrar que un ideal q de A es primario precisamente si es de la forma (p^n) para algún irreducible p de A y algún número natural n.

    (c) Demostrar que todo ideal propio I de A se puede poner de forma única, salvo el orden, como un producto $I = Q_1 \cdots Q_r$ en el que cada Q_i es un ideal primario y, para cada $i \neq j$, se tiene $Q_i + Q_j = A$.

24. [*] Un anillo en el que todos los ideales tienen un sistema generador finito se dice que es *noetheriano*. Demostrar que todo dominio noetheriano es un dominio de factorización. (Indicación: Adaptar la demostración del Teorema 3.4.6.)

25. Sea $m \neq 1$ un entero libre de cuadrados y sea $R = \mathbb{Z}[\sqrt{m}]$; se pide:

    (a) Usando la igualdad $(m + \sqrt{m})(m - \sqrt{m}) = m(m-1)$, demostrar que 2 no es primo en R.

    (b) Si $m \leq -3$, demostrar que 2 es irreducible en R y deducir que R no es un DFU.

    (c) Si m es un múltiplo de 5, demostrar que 2 es irreducible en R y deducir que R no es DFU.

    (d) Si $m \equiv 1 \bmod 4$, demostrar que 2 es irreducible en R y deducir que R no es DFU.

(e) Encontrar dos factorizaciones de 4 esencialmente distintas en $\mathbb{Z}[\sqrt{-3}]$.

(f) Encontrar dos factorizaciones de 6 esencialmente distintas en $\mathbb{Z}\sqrt{-6}]$.

(g) Encontrar dos factorizaciones de 4 esencialmente distintas en $\mathbb{Z}[\sqrt{5}]$.

(h) Encontrar dos factorizaciones de 6 esencialmente distintas en $\mathbb{Z}[\sqrt{10}]$.

26. En el problema 12 se ha visto que $\delta(a+b\sqrt{2}) = |a^2-2b^2|$ es una norma euclídea en $\mathbb{Z}[\sqrt{2}]$, y por tanto $\mathbb{Z}[\sqrt{2}]$ es un DFU. ¿Contradice a esta afirmación el hecho de que se tenga la igualdad $(5+\sqrt{2})(2-\sqrt{2}) = (11-7\sqrt{2})(2+\sqrt{2})$ con los cuatro factores irreducibles?

27. Sea $q = p_1 \cdots p_r$ un entero libre de cuadrados (los p_i son primos distintos). Por el Problema 45 del Capítulo 2 sabemos que el subanillo de $\mathbb{Q}$

$$\mathbb{Z}_{(q)} = \{a/b : \mathrm{mcd}(q,b) = 1\}$$

es un DIP, y por tanto es un DFU. Aquí vamos a describir la factorización de sus elementos. Demostrar que:

(a) Un elemento a/b de $\mathbb{Z}_{(q)}$ es invertible si y sólo si $\mathrm{mcd}(q,a) = 1$.

(b) Cada elemento no nulo de $\mathbb{Z}_{(q)}$ se expresa de modo único en la forma $up_1^{\alpha_1}\cdots p_r^{\alpha_r}$, donde u es invertible y cada $\alpha_i \in \mathbb{N}$.

(c) Salvo asociados, $p_1, \ldots, p_n$ son los únicos elementos irreducibles de $\mathbb{Z}_{(q)}$, y son todos ellos primos. Por tanto $\mathbb{Z}_{(q)}$ es un DFU.

(d) Como en $\mathbb{Z}_{(q)}$ sólo hay un número finito de primos salvo asociados, un intento de adaptar la demostración del Teorema de Euclides (1.5.9) a este caso debe fallar en algún paso. ¿En cuál lo hace?

(e) Si q es primo (es decir, si $r = 1$) entonces $\mathbb{Z}_{(q)}$ es un dominio euclídeo y todo ideal no nulo de $\mathbb{Z}_{(q)}$ es el ideal principal generado por q^α para cierto $\alpha \in \mathbb{N}$. (Indicación: Usa la factorización del apartado (b) para definir una función euclídea.)

28. Encontrar todas las formas posibles de expresar 169 como suma de dos cuadrados de enteros positivos. Lo mismo para 1125 y para 2197.

29. Fermat escribió: "¿Puede encontrarse un número entero cuyo cuadrado, distinto de 25, cuando se aumente en 2 sea un cubo?". Vamos a trabajar en el DFU $\mathbb{Z}[\sqrt{-2}]$ para responder a esta pregunta.

(a) Demuestra que, para cualquier entero impar y, los elementos $y+\sqrt{-2}$ e $y-\sqrt{-2}$ son coprimos en $\mathbb{Z}[\sqrt{-2}]$.

(b) Demuestra que si los enteros x, y verifican $x^3 = y^2+2$ entonces el elemento $y+\sqrt{-2}$ es un cubo (no sólo el asociado de un cubo) en $\mathbb{Z}[\sqrt{-2}]$.

(c) Demuestra que las únicas soluciones enteras de la ecuación $3a^2b-2b^3 = 1$ son $b = 1$ y $a = \pm 1$.

(d) Responde a la pregunta de Fermat.

30. [*] Sea D un dominio. Demostrar que el ideal (X^2, XY, Y^2) del anillo de polinomios en dos indeterminadas $D[X,Y]$ no es principal. ¿Tiene un conjunto de generadores con dos elementos? Determinar los ideales de $A = K[X,Y]/(X^2,XY,Y^2)$, siendo K un cuerpo y demostrar que A tiene ideales que no son principales.

31. Demostrar el recíproco del Teorema de Wilson: Si un entero $p \geq 2$ verifica $(p-1)! \equiv -1 \bmod p$ entonces p es primo.

Bibliografía del capítulo

Allenby [1], Clark [9], Delgado-Fuertes-Xambó [12], Dorronsoro-Hernández [13], Jacobson [23], Sharpe [32].

Capítulo 4

Anillos de polinomios

Se estudian con detenimiento los anillos de polinomios, con especial dedicación a los anillos de polinomios en una indeterminada con coeficientes en un dominio de factorización única o en un cuerpo.

Introducción

En los capítulos anteriores hemos usado los anillos de polinomios de modo informal para manejar algunos ejemplos. En éste comenzamos con una definición rigurosa del anillo de polinomios en una indeterminada sobre un anillo arbitrario, y observamos cómo el concepto de grado y la Propiedad Universal nos permiten obtener numerosas propiedades elementales de estos anillos. A continuación estudiamos las raíces de un polinomio con coeficientes en un dominio D, viendo que son importantes a la hora de factorizar el polinomio, que siempre existen (en cierto cuerpo que contiene a D) y que su número está acotado por el grado del polinomio.

Entre los resultados elementales habremos visto que el anillo de polinomios $A[X]$ es un dominio euclídeo, o un dominio de ideales principales, si y sólo si A es un cuerpo. Es natural preguntarse cuándo es $A[X]$ un dominio de factorización única, y buena parte del capítulo la dedicamos a demostrar que esto ocurre precisamente cuando lo es A. Abordamos a continuación el problema práctico de factorizar polinomios con coeficientes en un dominio de factorización única (o en su cuerpo de fracciones, pues ambas factorizaciones se relacionan estrechamente), para lo que es necesario establecer criterios que permitan confirmar la irreducibilidad de un polinomio.

El capítulo termina con la definición de los anillos de polinomios en un número finito de indeterminadas y con el análisis de sus propiedades elementales, algunas de las cuales generalizan las correspondientes propiedades en el caso de una indeterminada.

Objetivos del capítulo

- Conocer la definición formal de los anillos de polinomios en una indeterminada y alcanzar fluidez en el manejo de sus operaciones, especialmente del producto y de la división con resto.
- Conocer y manejar las propiedades del grado y la Propiedad Universal. En particular, manejar los homomorfismos de sustitución y comprender la diferencia entre polinomio y función polinómica.
- Interpretar las raíces de un polinomio f en términos de los factores lineales de f, y saber calcular su multiplicidad.
- Dado un dominio de factorización única D con cuerpo de fracciones K, conocer la relación entre las factorizaciones de un polinomio en $D[X]$ y en $K[X]$.
- Manejar métodos de factorización y criterios de irreducibilidad para polinomios sobre cuerpos y sobre dominios de factorización única.
- Conocer la definición formal y las propiedades básicas de los anillos de polinomios en un número finito de indeterminadas.

Desarrollo de los contenidos

4.1 Definiciones y propiedades básicas

Existen diversas formas equivalentes de definir los anillos de polinomios. Ya vimos una, poco rigurosa, en los Ejemplos 2.2.6. Una alternativa más formal es la siguiente:

Sea A un anillo. Un *polinomio en una indeterminada* con coeficientes en A es una sucesión

$$p = (p_n)_{n\in\mathbb{N}} = (p_0, p_1, p_2, \ldots)$$

con cada p_n en A y tal que $p_n = 0$ para casi todo $n \in \mathbb{N}$, lo que equivale a que exista $n_0 \in \mathbb{N}$ tal que $p_n = 0$ para cada $n \geq n_0$. Estas sucesiones se conocen como *sucesiones casi nulas*. El elemento $p_i \in A$ se conoce como el *coeficiente de grado i* del polinomio p, y p_0 es el *coeficiente independiente* de p. De la definición se deduce la siguiente propiedad, obvia pero fundamental: Dos polinomios $p = (p_n)_{n\in\mathbb{N}}$ y $q = (q_n)_{n\in\mathbb{N}}$ son iguales precisamente si lo son coeficiente a coeficiente; es decir, si $p_n = q_n$ para cada $n \in \mathbb{N}$.

Por ahora, llamaremos $P(A)$ al conjunto de todos los polinomios en una indeterminada con coeficientes en A. Vamos a definir en $P(A)$ dos operaciones que lo convertirán en un anillo. Dados dos polinomios $p = (p_n)_{n\in\mathbb{N}}$ y $q = (q_n)_{n\in\mathbb{N}}$, la suma $p + q$ se define componente a componente; es decir

$$p + q = (p_n + q_n)_{n\in\mathbb{N}}.$$

La definición del producto es más compleja: el producto de p y q es un nuevo polinomio

$$pq = r = (r_n)_{n\in\mathbb{N}}$$

cuyo coeficiente de grado n (para cada $n \in \mathbb{N}$) viene dado por

$$r_n = \sum_{i+j=n} p_i q_j = \sum_{i=0}^{n} p_i q_{n-i} = p_0 q_n + p_1 q_{n-1} + \cdots + p_{n-1} q_1 + p_n q_0.$$

Antes de comprobar que estas operaciones hacen de $P(A)$ un anillo, vamos a introducir una notación que nos devolverá al concepto habitual de polinomio que hemos usado en los capítulos previos. De esta forma habremos resuelto los problemas del rigor en la definición de los anillos de polinomios sin perder la facilidad de manejo que aporta una notación adecuada y típica.

Dado $a \in A$, también denotaremos por a al polinomio

$$a = (a, 0, 0, \ldots),$$

y le llamaremos *polinomio constante*. La aplicación $u : A \to P(A)$ dada por $a \mapsto a = (a, 0, 0, \ldots)$ es claramente inyectiva y nos permite identificar al anillo A con el subconjunto de $P(A)$ formado por los polinomios constantes. Es decir, podemos interpretar u como una inclusión.

Llamaremos *indeterminada* de $P(A)$ al elemento

$$X = (0, 1, 0, 0, \ldots).$$

Usando la definición del producto y la notación usual de exponentes, es fácil ver que se tiene

$$X^2 = (0, 0, 1, 0, \ldots), \qquad X^3 = (0, 0, 0, 1, 0, \ldots)$$

y así sucesivamente. Por tanto, si $a \in A$ y $n \in \mathbb{N}$, tenemos

$$aX^n = (0, 0, \ldots, 0, a, 0, \ldots),$$

donde a aparece en el lugar correspondiente al subíndice n (recuérdese que el primer subíndice es el 0). A los elementos de la forma aX^n se les llama *monomios* (de grado n). Para un polinomio arbitrario $p = (p_n)_{n\in\mathbb{N}} \in P(A)$ se tiene

$$\begin{aligned} p &= (p_0, p_1, p_2, \ldots) \\ &= (p_0, 0, 0, \ldots) + (0, p_1, 0, \ldots) + (0, 0, p_2, \ldots) + \cdots \\ &= p_0 + p_1 X + p_2 X^2 + \cdots \\ &= \textstyle\sum_{n\in\mathbb{N}} p_n X^n, \end{aligned}$$

donde las sumas tienen sentido porque casi todos los sumandos son nulos. Como p está determinado por sus coeficientes, tenemos:

Lema 4.1.1 *Todo polinomio en una indeterminada con coeficientes en A se escribe de modo único como suma de monomios.*

A partir de ahora olvidaremos la notación $P(A)$ y denotaremos por $A[X]$ el conjunto de los polinomios en una indeterminada con coeficientes en A. Con frecuencia usaremos la notación $p(X)$ para un polinomio, para destacar qué nombre le estamos dando a la indeterminada (por supuesto, la elección del símbolo X es meramente convencional).

Dado un polinomio $p = \sum_{i\in\mathbb{N}} p_i X^i$ en $A[X]$, existe $m \in \mathbb{N}$ tal que $p_{m+1} = p_{m+2} = \cdots = 0$, luego p puede escribirse como un suma finita de monomios

$$p = \sum_{i=0}^{m} p_i X^i = p_0 + p_1 X + p_2 X^2 + \cdots + p_{m-1} X^{m-1} + p_m X^m.$$

Podemos pues escribir un polinomio de $A[X]$ como suma infinita o finita de monomios, y usaremos en cada caso la notación que más nos convenga. En las sumas infinitas entenderemos que casi todos los coeficientes son nulos; y en las finitas podremos omitir los sumandos con coeficiente 0.

Con la notación de sumas de monomios, las operaciones en $A[X]$ pueden reenunciarse como

$$\sum_{n\in\mathbb{N}} p_n X^n + \sum_{n\in\mathbb{N}} q_n X^n = \sum_{n\in\mathbb{N}} (p_n + q_n) X^n \qquad \text{y} \qquad (\sum_{n\in\mathbb{N}} p_n X^n) \cdot (\sum_{n\in\mathbb{N}} q_n X^n) = \sum_{n\in\mathbb{N}} (\sum_{i+j=n} p_i q_j) X^n.$$

El lector podrá ahora comprobar que estas operaciones dotan a $A[X]$ de una estructura de anillo conmutativo (el *anillo de polinomios en una indeterminada con coeficientes en A*) cuyos elementos nulo e identidad son los de A, vistos como polinomios constantes. Como ejemplo, desarrollamos a continuación la comprobación de la asociatividad del producto. Dados tres polinomios $p = \sum_{i\in\mathbb{N}} p_i X^i$, $q = \sum_{j\in\mathbb{N}} q_j X^j$ y $r = \sum_{k\in\mathbb{N}} r_k X^k$, se tiene

$$\begin{aligned} p(qr) &= \left(\sum_{i\in\mathbb{N}} p_i X^i\right) \left(\sum_{n\in\mathbb{N}} (\sum_{j+k=n} q_j r_k) X^n\right) \\ &= \sum_{m\in\mathbb{N}} \left(\sum_{i+n=m} p_i (\sum_{j+k=n} q_j r_k)\right) X^m \\ &= \sum_{m\in\mathbb{N}} \left(\sum_{i+j+k=m} p_i q_j r_k\right) X^m, \end{aligned}$$

y de modo análogo se obtiene la misma expresión para $(pq)r$, lo que prueba la asociatividad.

Hablaremos en consecuencia de $A[X]$ como del *anillo de polinomios en una indeterminada* con coeficientes en A. Es fácil ver que A es un subanillo de $A[X]$.

Sea A un anillo y sea $p = \sum_{i\in\mathbb{N}} p_i X^i \in A[X]$ un polinomio no nulo de $A[X]$. Entonces, por definición de polinomio, el conjunto $\{i \in \mathbb{N} : p_i \neq 0\}$ no es vacío y está acotado superiormente. Por tanto ese conjunto tiene un máximo, al que llamamos *grado* del polinomio p y denotamos por $\mathrm{gr}(p)$. Es decir,

$$\mathrm{gr}(p) = \max\{i \in \mathbb{N} : p_i \neq 0\}.$$

El coeficiente de mayor grado, $p_{\mathrm{gr}(p)}$, se conoce como el *coeficiente principal* de p, y diremos que p es *mónico* si su coeficiente principal es 1. Por convenio, consideramos que el polinomio 0 tiene grado $-\infty$ y coeficiente principal 0. Es claro que los polinomios de grado 0 son precisamente los polinomios constantes no nulos. A veces llamaremos *lineales* a los polinomios de grado 1, *cuadráticos* a los de grado 2, *cúbicos* a los de grado 3, etcétera.

Ejercicio 4.1.2 *Sean $p = a_0 + a_1 X + \cdots + a_n X^n$ y $q = b_0 + b_1 X + \cdots + b_m X^m$ polinomios de $A[X]$, con $a_n \neq 0 \neq b_m$. Demostrar que:*

1. $\mathrm{gr}(p+q) \leq \max(\mathrm{gr}(p), \mathrm{gr}(q))$, *con la desigualdad estricta si y sólo si $n = m$ y $a_n + b_m = 0$.*

2. $\mathrm{gr}(pq) \leq \mathrm{gr}(p) + \mathrm{gr}(q)$, *con igualdad si y sólo si $a_n b_m \neq 0$.*

3. *Si a_n es regular (por ejemplo, si p es mónico, o si A es un dominio), entonces se tiene*

$$\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q).$$

4. *Las desigualdades de los apartados 1 y 2 pueden ser estrictas (buscar un ejemplo cuando $A = \mathbb{Z}_6$).*

Una consecuencia inmediata del Ejercicio 4.1.2 es:

Corolario 4.1.3 *Un anillo de polinomios $A[X]$ es un dominio si y sólo si lo es el anillo de coeficientes A. En este caso se tiene $A[X]^* = A^*$; es decir, los polinomios invertibles de $A[X]$ son los polinomios constantes invertibles en A. En particular, los polinomios invertibles sobre un cuerpo son exactamente los de grado 0, y $A[X]$ nunca es un cuerpo.*

En vista de este resultado, es natural preguntarse qué condiciones deberá cumplir un anillo A para que el anillo de polinomios $A[X]$ sea un dominio euclídeo, un dominio de ideales principales o un dominio de factorización única. Las dos primeras cuestiones las podemos resolver ya, y la última la estudiaremos en la Sección 4.5.

Proposición 4.1.4 *Para un anillo A, las condiciones siguientes son equivalentes:*

1. *$A[X]$ es un dominio euclídeo.*
2. *$A[X]$ es un dominio de ideales principales.*
3. *A es un cuerpo.*

En este caso, un polinomio no constante $f \in A[X]$ es irreducible (o primo) si y sólo si no es producto de dos polinomios de grado menor; es decir, si una igualdad $f = gh$ en $A[X]$ implica que $\mathrm{gr}(g) = \mathrm{gr}(f)$ (y $\mathrm{gr}(h) = 0$) ó $\mathrm{gr}(h) = \mathrm{gr}(f)$ (y $\mathrm{gr}(g) = 0$).

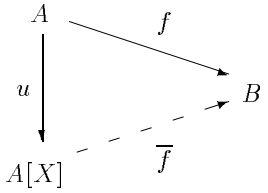
Demostración. De la Proposición 3.3.7 se deduce que 3 implica 1, y del Teorema 3.3.3 que 1 implica 2. Es fácil ver que, si A es un dominio, el polinomio X es un elemento irreducible de $A[X]$. Por tanto, del isomorfismo $A \cong A[X]/(X)$ (Ejemplos 2.7.7) y de la Proposición 3.2.3 se deduce que 2 implica 3. Dejamos que el lector demuestre la afirmación sobre los polinomios irreducibles. □

4.2 Propiedad Universal

Hemos observado que un anillo A es un subanillo del anillo de polinomios $A[X]$, y por tanto la inclusión $u : A \to A[X]$ es un homomorfismo de anillos. También es claro que el subanillo de $A[X]$ generado por A y X es todo $A[X]$. Es decir, la indeterminada X y las constantes de A (las imágenes de u) generan todos los elementos de $A[X]$. El siguiente resultado nos dice que $A[X]$ puede caracterizarse por una propiedad en la que sólo intervienen X y u.

Proposición 4.2.1 *Sea A un anillo y sean $A[X]$ y $u : A \to A[X]$ los que se acaban de describir.*

1. **(Propiedad Universal del Anillo de Polinomios, PUAP)** *Para todo homomorfismo de anillos $f : A \to B$ y todo elemento b de B existe un único homomorfismo de anillos $\bar{f} : A[X] \to B$ tal que $\bar{f} \circ u = f$ y $\bar{f}(X) = b$. Se dice que $\bar{f}$* completa de modo único *el diagrama*



2. *Si dos homomorfismos de anillos $g, h : A[X] \to B$ coinciden sobre A y en X entonces son iguales. Es decir, si $g \circ u = h \circ u$ y $g(X) = h(X)$ entonces $g = h$.*

3. *$A[X]$ y u están determinados salvo isomorfismos por la PUAP. Explícitamente: supongamos que existen un homomorfismo de anillos $v : A \to P$ y un elemento $T \in P$ tales que, para todo homomorfismo de anillos $f : A \to B$ y todo elemento $b \in B$, existe un único homomorfismo de anillos $\bar{f} : P \to B$ tal que $\bar{f} \circ v = f$ y $\bar{f}(T) = b$. Entonces existe un isomorfismo $\phi : A[X] \to P$ tal que $\phi \circ u = v$ y $\phi(X) = T$.*

Demostración. 1. Sean $f : A \to B$ y $b \in B$ como en el enunciado. Si existe un homomorfismo $\bar{f} : A[X] \to B$ tal que $\bar{f} \circ u = f$ y $\bar{f}(X) = b$, entonces para un polinomio $p = \sum_{n\in\mathbb{N}} p_n X^n$, se tendrá

$$\bar{f}(p) = \bar{f}(\sum_{n\in\mathbb{N}} u(p_n)X^n) = \sum_{n\in\mathbb{N}} f(p_n)b^n.$$

Por tanto, la aplicación dada por $\bar{f}(p) = \sum_{n\in\mathbb{N}} f(p_n)b^n$ es la única que puede cumplir tales condiciones. El lector puede ahora comprobar que esta aplicación $\bar{f}$ es un homomorfismo de anillos, y es elemental ver que satisface $\bar{f} \circ u = f$ y $\bar{f}(X) = b$.

2. Si ponemos $f = g \circ u = h \circ u : A \to B$, los homomorfismos g y h completan el diagrama del apartado 1. Por la unicidad se tiene $g = h$.

3. Sean $v : A \to P$ y $T \in P$ como en 3. Aplicando 1 y la hipótesis de 3 encontramos homomorfismos $\bar{v} : A[X] \to P$ y $\bar{u} : P \to A[X]$ tales que

$$\bar{v} \circ u = v \quad \text{y} \quad \bar{v}(X) = T \qquad \bar{u} \circ v = u \quad \text{y} \quad \bar{u}(T) = X.$$

Entonces la composición $\bar{u} \circ \bar{v} : A[X] \to A[X]$ verifica

$$(\bar{u} \circ \bar{v}) \circ u = \bar{u} \circ v = u \qquad \text{y} \qquad (\bar{u} \circ \bar{v})(X) = \bar{u}(T) = X,$$

y por 2 se obtiene $\bar{u} \circ \bar{v} = 1_{A[X]}$. De modo análogo, y observando que v y T verifican una condición similar a 2, se demuestra que $\bar{v} \circ \bar{u} = 1_P$, con lo que $\bar{v}$ es el isomorfismo que buscamos. □

Observación 4.2.2 *La PUAP admite una "versión no conmutativa" que necesitaremos en el Capítulo 10, y que es la siguiente (la demostración es análoga a la anterior y se deja a cargo del lector):*

Sea $u : A \to A[X]$ como antes (A conmutativo), y sea B un anillo no necesariamente conmutativo. Sea $f : A \to B$ un homomorfismo de anillos y sea $b \in B$ un elemento tal que $f(a)b = bf(a)$ para cualquier $a \in A$. Entonces existe un único homomorfismo de anillos $\bar{f} : A[X] \to B$ tal que $\bar{f} \circ u = f$ y $f(X) = b$.

La utilidad de la PUAP estriba en que, dado un homomorfismo $f : A \to B$, nos permite crear un homomorfismo $A[X] \to B$ que "respeta" a f y que "se comporta bien" sobre un elemento $b \in B$ que nos interese. Los siguientes ejemplos son aplicaciones de la PUAP a ciertos homomorfismos que aparecen con frecuencia y son importantes tanto en este capítulo como en algunos de los siguientes (y en otras muchas situaciones que no estudiaremos aquí).

Ejemplos 4.2.3 *Aplicaciones de la PUAP.*

1. Sean A un subanillo de B y $b \in B$. Aplicando la PUAP a la inclusión $A \hookrightarrow B$ obtenemos un homomorfismo $S_b : A[X] \to B$ que es la identidad sobre A (decimos a veces que *fija* los elementos de A) y tal que $S_b(X) = b$. Se le llama el *homomorfismo de sustitución* (o de *evaluación*) en b. Dado $p = p(X) \in A[X]$, escribiremos a menudo $p(b)$ en vez de $S_b(X)$. Podemos describir explícitamente la acción de S_b en un polinomio:

$$S_b : A[X] \to B \qquad p(X) = \sum_{n\in\mathbb{N}} p_n X^n \qquad \rightsquigarrow \qquad S_b(p) = p(b) = \sum_{n\in\mathbb{N}} p_n b^n.$$

2. Sean A un anillo y $a \in A$. Si en el ejemplo anterior tomamos $B = A[X]$ y $b = X + a$, obtenemos un homomorfismo $A[X] \to A[X]$ dado por

$$p(X) \mapsto p(X + a).$$

Este homomorfismo es un automorfismo cuyo inverso viene dado por $p(X) \mapsto p(X - a)$ (¿por qué?).

3. Todo homomorfismo de anillos $f : A \to B$ induce un homomorfismo entre los correspondientes anillos de polinomios: Aplicándole la PUAP a la composición de f con la inclusión $B \hookrightarrow B[X]$ obtenemos $\bar{f} : A[X] \to B[X]$ tal que $\bar{f}\,|_A = f$ y $\bar{f}(X) = X$. Explícitamente, dado $p = \sum_{n\in\mathbb{N}} p_n X^n$ en $A[X]$, se tiene

$$\bar{f}(p) = \sum_{n\in\mathbb{N}} f(p_n)\,X^n\,.$$

Es fácil ver que, si f es inyectivo o suprayectivo, entonces lo es $\bar{f}$; como casos particulares de esta afirmación se obtienen los dos ejemplos siguientes:

4. Si A es un subanillo de B entonces $A[X]$ es un subanillo de $B[X]$.

5. Si I es un ideal del anillo A, la proyección $\pi : A \to A/I$ induce un homomorfismo suprayectivo $\bar{\pi} : A[X] \to (A/I)[X]$. Si ponemos $\bar{a} = a + I$, el homomorfismo $\bar{\pi}$ viene dado explícitamente por

$$\bar{\pi}(\sum_{n\in\mathbb{N}} p_n X^n) = \sum_{n\in\mathbb{N}} \overline{p_n} X^n.$$

A $\bar{\pi}$ se le llama el homomorfismo de *reducción de coeficientes módulo I*. Su núcleo, que es un ideal de $A[X]$, consiste en los polinomios con coeficientes en I, y lo denotaremos por $I[X]$. Obsérvese que $(A/I)[X] \cong \dfrac{A[X]}{I[X]}$.

Ejercicio 4.2.4 *Sea A un subanillo de B y sea $S_b : A[X] \to B$ el homomorfismo de sustitución en cierto elemento b de B. Demostrar que:*

1. *Im S_b es el subanillo de B generado por $A \cup \{b\}$, y consiste en las "expresiones polinómicas en b con coeficientes en A"; es decir, en los elementos de la forma*

$$\sum_{i=0}^{n} a_i b^i,$$

donde $n \in \mathbb{N}$ y $a_i \in A$ para cada i. Este subanillo se suele denotar por $A[b]$.

2. *Si $A = \mathbb{Z}$, $B = \mathbb{C}$ y $b = \sqrt{m}$ (ó $b = \frac{1+\sqrt{m}}{2}$ con $m \equiv 1 \bmod 4$) para cierto $m \in \mathbb{Z}$, la notación anterior es compatible con la que se usó anteriormente (es decir, $\mathbb{Z}[\sqrt{m}]$ representa el mismo subanillo atendiendo a cualquiera de las dos definiciones). Lo mismo ocurre si se toma $A = \mathbb{Q}$.*

Es importante observar que, mientras que dos polinomios coinciden sólo si lo hacen coeficiente a coeficiente, en general no ocurre lo mismo con las expresiones polinómicas. Por ejemplo, en $Z[\sqrt{-7}]$ se tiene, poniendo $b = \sqrt{-7}$,

$$2 + 3b - b^2 + 4b^3 + b^4 = 58 - 25b.$$

Es conveniente en este punto hacer una precisión sobre los polinomios. Hemos definido un polinomio $p = p(X) \in A[X]$ como una sucesión de elementos de A (los coeficientes). Sin embargo, el lector puede estar familiarizado con la interpretación de un polinomio, digamos que con coeficientes reales, como una función real de variable real. En ese caso, si es un lector inquieto, se habrá preguntado ya si es posible hacer una interpretación de este tipo en general; es decir, para cualquier anillo de coeficientes A. La respuesta es sí, pero con un matiz importante. En efecto, fijado un polinomio $p \in A[X]$, podemos considerar la *función polinómica* determinada por p, que se define como la aplicación $A \to A$ dada por $a \mapsto p(a)$ (con la notación usada para el homomorfismo de sustitución). El matiz es el siguiente: en contra de lo que ocurre cuando $A = \mathbb{R}$, en general dos polinomios distintos pueden dar lugar a la misma función polinómica. Esto es claro si A es finito, pues entonces sólo hay una cantidad finita de aplicaciones $A \to A$, mientras que hay una cantidad infinita de polinomios en $A[X]$. Como ejemplos concretos, el lector puede analizar lo que ocurre con los polinomios 0 y $X + X^2$ en $\mathbb{Z}_2[X]$; o con los polinomios X^2 y X^4 en $\mathbb{Z}_4[X]$; o con los polinomios X y X^p en $\mathbb{Z}_p[X]$, cuando p es un primo positivo. Volveremos sobre esta discusión en el Corolario 4.3.5.

4.3 Raíces de polinomios

Empezaremos esta sección con el siguiente lema, que generaliza la Proposición 3.3.7 y le añade una condición de unicidad; recuérdese que consideramos el polinomio cero como un polinomio de grado $-\infty$.

Lema 4.3.1 *Sea A un anillo y sean $f, g \in A[X]$. Si el coeficiente principal de g es invertible en A, entonces existen dos únicos polinomios $q, r \in A[X]$ tales que $f = gq + r$ y $\mathrm{gr}(r) < \mathrm{gr}(g)$.*

En esta situación, q y r se llaman cociente *y* resto *de la división de f entre g.*

Demostración. La existencia se demuestra como en la Proposición 3.3.7. En cuanto a la unicidad, supongamos que $f = gq_1 + r_1 = gq_2 + r_2$ con $\mathrm{gr}(r_i) < \mathrm{gr}(g)$ para cada $i = 1, 2$. Como el término principal de g es regular, del Ejercicio 4.1.2 se deduce que

$$\mathrm{gr}(g) + \mathrm{gr}(q_1 - q_2) = \mathrm{gr}(g(q_1 - q_2)) = \mathrm{gr}(r_2 - r_1) \leq \max\{\mathrm{gr}(r_2), \mathrm{gr}(r_1)\} < \mathrm{gr}(g).$$

Luego $\mathrm{gr}(q_1 - q_2) < 0$ y en consecuencia $q_1 = q_2$, de donde $r_1 = r_2$. □

Especialmente sencillo es el caso en el que se divide por un polinomio lineal y mónico.

Proposición 4.3.2 *Sean A un anillo, $a \in A$ y $f \in A[X]$. Entonces:*

1. **(Teorema del Resto)** *El resto de la división de f entre $X - a$ es $f(a)$.*
2. **(Teorema de Ruffini)** *f es divisible por $X - a$ precisamente si $f(a) = 0$.*

Demostración. Dividiendo f entre $X - a$ tenemos $f = q(X - a) + r$ con $\mathrm{gr}(r) < 1$, por lo que r es constante y así $r = r(a) = f(a) - q(a)(a - a) = f(a)$. Esto demuestra 1, y 2 es entonces inmediato. □

Diremos que $a \in A$ es una *raíz* de $f \in A[X]$ si $f(a) = 0$ (es decir, si $X - a$ divide a f). Por ejemplo, 0 es raíz de f si y sólo si f tiene coeficiente independiente 0, y cualquier elemento de A es raíz del polinomio 0.

Fijemos $a \in A$. Como, para cada $k \in \mathbb{N}$, el polinomio $(X - a)^k$ es mónico de grado k, se tiene $\mathrm{gr}((X-a)^k q) = k + \mathrm{gr}(q)$ para cada $q \in A[X]$. Por tanto, para cada $f \in A[X]$ no nulo, existe un mayor $m \in \mathbb{N}$ tal que $(X-a)^m$ divide a f. Este entero m, que verifica $0 \leq m \leq \mathrm{gr}(f)$, se llama la *multiplicidad de a en f*. Por el Teorema de Ruffini, a es raíz de f precisamente si $m \geq 1$. Cuando $m = 1$ se dice que a es una *raíz simple* de f, y cuando $m > 1$ se dice que a es una *raíz múltiple* de f.

Ejercicio 4.3.3 *Sean A un anillo y $a \in A$. Demostrar que el polinomio $X - a$ es cancelable en $A[X]$, y deducir que $m \in \mathbb{N}$ es la multiplicidad de a en $f \in A[X]$ si y sólo si existe un polinomio $q \in A[X]$ con $f = (X - a)^m q$ y $q(a) \neq 0$.*

Cuando D es un dominio, del Teorema de Ruffini se deduce que $X - a$ es primo para cualquier $a \in D$. Esto es esencial en la demostración del siguiente resultado.

Proposición 4.3.4 (Acotación de raíces) *Sean D un dominio y $0 \neq f \in D[X]$. Entonces:*

1. *Si $a_1, \ldots, a_n \in D$ son distintos dos a dos y $\alpha_1, \ldots \alpha_n \geq 1$ son enteros con cada $(X - a_i)^{\alpha_i} \mid f$, entonces $(X - a_1)^{\alpha_1} \cdots (X - a_n)^{\alpha_n} \mid f$. Por tanto $\sum_{i=1}^n \alpha_i \leq \mathrm{gr}(f)$.*
2. *La suma de las multiplicidades de todas las raíces de f es menor o igual que $\mathrm{gr}(f)$. En particular, el número de raíces distintas de f es menor o igual que $\mathrm{gr}(f)$.*

Demostración. Es claro que basta con demostrar la primera afirmación de 1, cosa que hacemos por inducción en $s = \sum_{i=1}^n \alpha_i$ con el caso $s = 1$ evidente. Cuando $s > 1$, usando la hipótesis $(X - a_1)^{\alpha_1} \mid f$ y la hipótesis de inducción, sabemos que existen polinomios g y h tales que

$$g(X - a_1)^{\alpha_1} = f = h(X - a_1)^{\alpha_1 - 1}(X - a_2)^{\alpha_2} \cdots (X - a_n)^{\alpha_n}.$$

Cancelando $(X - a_1)^{\alpha_1 - 1}$ y usando el hecho de que $X - a_1$ es primo y no divide a ningún otro $X - a_i$ (¿por qué?), deducimos que $X - a_1$ divide a h, y esto nos da el resultado. □

Si D no es un dominio, siempre podemos encontrar un polinomio en $D[X]$ para el que falle la acotación de raíces (es decir, "con más raíces que grado"). En efecto, si $0 \neq a, b \in D$ y $ab = 0$, entonces aX es un polinomio de grado 1 con al menos 2 raíces, 0 y b. Otro ejemplo se obtiene considerando el polinomio $X^2 - 1$, que tiene 4 raíces en $\mathbb{Z}_8$.

El siguiente corolario evidente de la Proposición 4.3.4 se conoce como el *principio de las identidades polinómicas*. Ya hemos comentado que su segundo apartado falla sobre cualquier anillo finito.

Corolario 4.3.5 *Sea D un dominio, y sean $f, g \in D[X]$. Entonces:*

1. *Si las funciones polinómicas $f, g : D \to D$ coinciden en m puntos, con $m > \mathrm{gr}(f)$ y $m > \mathrm{gr}(g)$, entonces $f = g$ (como polinomios).*
2. *Si D es infinito entonces dos polinomios distintos definen funciones polinómicas distintas en D.*

El siguiente concepto es útil para calcular multiplicidades: Si A es un anillo, la *derivada* de $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ se define como

$$D(P) = P' = a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1}.$$

Obsérvese que la derivada no se ha definido a partir de ningún concepto topológico, y por ejemplo no es cierto en general que un polinomio con derivada nula sea constante (considérese por ejemplo $X^n \in \mathbb{Z}_n[X]$). Sin embargo, esta *derivada formal* satisface las mismas propiedades algebraicas que la derivada del Análisis.

Ejercicio 4.3.6 *Dados $a, b \in A$ y $P, Q \in A[X]$, demostrar que:*

1. $(aP + bQ)' = aP' + bQ'$.
2. $(PQ)' = P'Q + PQ'$.
3. $(P^n)' = nP^{n-1}P'$.

Proposición 4.3.7 *Una raíz $a \in A$ de $P \in A[X]$ es múltiple precisamente si $P'(a) = 0$.*

Demostración. Si a es raíz simple se tiene $P = (X - a)Q$ para cierto $Q \in A[X]$ con $Q(a) \neq 0$, por lo que $P' = Q + (X - a)Q'$ y así $P'(a) = Q(a) \neq 0$. Si a es raíz múltiple se tiene $P = (X - a)^2Q$ para cierto $Q \in A[X]$, por lo que $P' = 2(X - a)Q + (X - a)^2Q'$ y así $P'(a) = 0$. □

En dominios de característica cero, la idea de la demostración anterior puede usarse para determinar la multiplicidad de a en P (no sólo para decidir si a es simple o múltiple). Para ello, necesitamos considerar las *derivadas sucesivas* de un polinomio: Para cada $n \in \mathbb{N}$ se define la derivada n-ésima $P^{(n)}$ de $P \in A[X]$, de forma recurrente, por las fórmulas:

$$P^{(0)} = P \quad \text{y} \quad P^{(n+1)} = (P^{(n)})'.$$

Proposición 4.3.8 *Sea D un dominio de característica 0, y sean $P \in D[X]$ y $a \in D$. Entonces la multiplicidad de a en P es el menor número natural $m \in \mathbb{N}$ tal que $P^{(m)}(a) \neq 0$.*

Demostración. Haremos inducción en la multiplicidad m de a en P, con el caso $m = 0$ claro. Si $m \geq 1$ entonces a es raíz de P y por tanto $P = (X - a)Q$ para cierto $Q \in D[X]$. Entonces la multiplicidad de a en Q es $m - 1$, y por hipótesis de inducción $Q^{(i)}(a) = 0 \neq Q^{(m-1)}(a)$ para todo $i < m - 1$. Además, para cada $t \geq 1$ se tiene

$$P^{(t)} = tQ^{(t-1)} + (X - a)Q^{(t)}.$$

Ahora el lector podrá completar fácilmente la demostración. □

La hipótesis sobre la característica de D en la Proposición 4.3.8 es necesaria. Por ejemplo, si p es un número primo, $K = \mathbb{Z}_p$ y $P = X^p$, entonces $P' = 0$ y así $P^{(n)}(0) = 0$ para todo n.

4.4 Existencia de raíces; Teorema Fundamental del Álgebra

No todos los polinomios con coeficientes en un anillo A tienen raíces en A. Por ejemplo, los polinomios de grado 0 no tienen ninguna raíz, y un polinomio lineal $aX + b$ (con $a \neq 0$) tiene una raíz en A si y sólo si a divide a b. En particular, todo polinomio lineal sobre un cuerpo tiene una raíz, pero puede haber polinomios de grado positivo sin raíces: por ejemplo, $X^2 + 1$ no tiene raíces en $\mathbb{R}$, y $X^3 - 2$ no las tiene en $\mathbb{Q}$.

Ejercicio 4.4.1 *Sea K un cuerpo. Demostrar que las siguientes condiciones son equivalentes:*

1. *Todo polinomio no constante de $K[X]$ tiene una raíz en K.*
2. *Los polinomios irreducibles de $K[X]$ son precisamente los de grado 1.*
3. *Todo polinomio no constante de $K[X]$ se factoriza como producto de polinomios lineales de $K[X]$.*

Se dice que un cuerpo K es *algebraicamente cerrado* cuando verifica las condiciones equivalentes del Ejercicio 4.4.1.

Es fácil encontrar ejemplos de cuerpos que *no* son algebraicamente cerrados. Por ejemplo, considerando el polinomio $X^2 + 1$ vemos que no lo son $\mathbb{Q}$ ni $\mathbb{R}$, y el polinomio $X^2 + X + 1$ nos dice que $\mathbb{Z}_2$ tampoco lo es. Si $p \geq 3$ es un entero primo entonces $\mathbb{Z}_p$ no es algebraicamente cerrado, pues $X^{p-1} + 1$ no tiene raíces en $\mathbb{Z}_p$ por el Teorema Pequeño de Fermat (1.8.2). Más generalmente, ningún cuerpo finito es algebraicamente cerrado (Problema 17). Sin embargo, se tiene:

Teorema 4.4.2 (Teorema Fundamental del Álgebra) *El cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.*

El Teorema Fundamental del Álgebra puede demostrarse usando algunos resultados que no se explicarán hasta el final del primer curso, en la asignatura de Topología. En este sentido, esa demostración se sale de los límites de la asignatura de Álgebra Básica, pero la incluiremos (al final de la sección, para no interrumpir el discurso principal) anticipando esos resultados de Topología.

Del Teorema Fundamental del Álgebra se deduce que todo polinomio no constante con coeficientes en $\mathbb{Z}$, $\mathbb{Q}$ ó $\mathbb{R}$ tiene raíces en $\mathbb{C}$. De modo más general, es posible demostrar que todo polinomio sobre un cuerpo tiene raíces "en algún sitio". Recuérdese que una extensión de cuerpos no es más que un homomorfismo de anillos $f : K \to Q$, donde K y Q son cuerpos. Un tal f es necesariamente inyectivo, y esto permite ver a K, identificado con la imagen de f, como un subcuerpo de Q.

Teorema 4.4.3 (Kronecker) *Sea K un cuerpo y sea $P \in K[X]$ un polinomio no constante. Entonces existe una extensión de cuerpos $K \to K_1$ tal que K_1 contiene una raíz de P.*

Demostración. Como $K[X]$ es un DIP (Proposición 4.1.4) y P no es una unidad, P es divisible por un polinomio irreducible Q. Entonces el anillo cociente $K_1 = K[X]/(Q)$ es un cuerpo en el que $P + (Q) = 0$. Entonces $f : K \to K_1$, la composición de la inclusión $K \hookrightarrow K[X]$ con la proyección $K[X] \to K[X]/(Q)$, es una extensión de cuerpos. Por último, $\alpha = X + (Q) \in K_1$ es una raíz de P, pues si $P = a_0 + a_1X + \cdots + a_nX^n$ entonces

$$\begin{aligned} P(\alpha) &= a_0 + a_1(X + (Q)) + a_2(X + (Q))^2 + \cdots + a_n(X + (Q))^n \\ &= a_0 + a_1(X + (Q)) + a_2(X^2 + (Q)) + \cdots + a_n(X^n + (Q)) \\ &= (a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) + (Q) \\ &= P + (Q) = 0. \end{aligned}$$

□

Para un cuerpo arbitrario K, diremos que un polinomio no constante $P \in K[X]$ *se descompone completamente* en K, o que es *completamente descomponible* en K, si se factoriza como producto de polinomios lineales de $K[X]$; es decir, si existen $a_1, \ldots, a_n \in K$ (no necesariamente distintos) tales que $P = u(X - a_1) \cdots (X - a_n)$, donde u es el coeficiente principal de P y n es el grado de P.

El Teorema de Kronecker nos permite demostrar que todo polinomio con coeficientes en un cuerpo K se descompone completamente en algún cuerpo que contiene a K como subcuerpo.

Corolario 4.4.4 *Sean K un cuerpo y $P \in K[X]$ un polinomio no constante. Entonces existe una extensión de cuerpos $K \to K'$ tal que P se descompone completamente en K'.*

Demostración. Razonamos por inducción sobre $n = \mathrm{gr}(P)$, con el caso $n = 1$ trivial. Si $n > 1$, por el Teorema de Kronecker (4.4.3), existe una extensión $K \to K_1$ tal que P tiene una raíz a_1 en K_1, de modo que $P = (X - a_1)Q$ para cierto polinomio $Q \in K_1[X]$. Por hipótesis de inducción, hay una extensión $K_1 \to K'$ tal que $Q = u(X - a_2)\cdots(X - a_n)$ para ciertos $a_2, \ldots, a_n \in K'$, y por tanto $P = u(X - a_1)\cdots(X - a_n)$. Componiendo ambas extensiones obtenemos la del enunciado. □

Observaciones 4.4.5

1. *Como todo dominio es subanillo de su cuerpo de fracciones, los enunciados del Teorema de Kronecker (4.4.3) y del Corolario 4.4.4 pueden generalizarse asumiendo que K es un dominio, y sustituyendo las extensiones de cuerpos por homomorfismos de anillos desde K hacia un cuerpo.*

2. *Por el Teorema Fundamental del Álgebra, $\mathbb{C}$ es un cuerpo que contiene las raíces de* todos *los polinomios no constantes de $\mathbb{R}[X]$. En vista de esto y del Corolario 4.4.4, es natural preguntarse si, dado un cuerpo arbitrario K, existirá una extensión $K \to \bar{K}$ tal que todo polinomio no constante de K se descomponga totalmente en $\bar{K}[X]$. La respuesta es afirmativa, como se verá en el curso de Ecuaciones Algebraicas, y ese resultado será fundamental para un estudio en profundidad de los cuerpos.*

Demostración del Teorema Fundamental del Álgebra

Como hemos comentado, el Teorema Fundamental del Álgebra (también conocido como Teorema de d'Alembert-Gauss[1]) afirma que el cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado, y en este apartado usaremos algunos resultados básicos de Topología para dar una demostración de este hecho basada en una incompleta de Argand, en 1814.

Recordando la definición de cuerpo algebraicamente cerrado, se trata de ver que, dado un polinomio

$$p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

de grado $n \geq 1$ ($a_n \neq 0$) con coeficientes complejos ($a_i \in \mathbb{C}$ para cada $i = 0, 1, \ldots, n$), existe un número complejo z tal que $p(z) = 0$.

Usaremos propiedades elementales de los números complejos, como las desigualdades entre módulos

$$|z_1| - |z_2| \leq |z_1 + z_2| \leq |z_1| + |z_2|$$

[1] Aunque a menudo se suele afirmar que la primera demostración completa del Teorema Fundamental del Álgebra es debida a Gauss, esto no es completamente cierto. En 1746 d'Alembert dio una demostración que utilizaba la siguiente afirmación de Newton: Sean $p \in \mathbb{C}[X]$ y $a \in \mathbb{C}$ tales que $p(a) \neq 0$. Entonces en todo círculo cerrado centrado en a hay un $z \in \mathbb{C}$ tal que $|p(z)| < |p(a)|$. En dicho momento no existía ninguna ninguna demostración de la afirmación de Newton, por lo que la demostración de d'Alembert no era completa.

En 1799, Gauss presentó una demostración del teorema a la que le faltaba un detalle: Gauss considera las curvas Re $(P(x)) = 0$ e Im $(P(x)) = 0$, que representan las partes real e imaginaria de $p(z) \in \mathbb{C}$. Utilizando que $P(z)$ crece en módulo como z^n, donde n es el grado de P, Gauss prueba que dichas curvas intersecan a una circunferencia y que las intersecciones de dichas curvas con los puntos de la circunferencia aparecen de forma alterna; es decir, moviéndonos a lo largo de la circunferencia encontramos un punto de una de las curvas entre cada dos de la otra. Entonces Gauss afirma que "sin duda" eso implica que dichas curvas se intersecan dentro del circulo limitado por la circunferencia. Gauss escribe: "Nadie, por lo que yo sé, lo ha dudado nunca. Pero si alguien lo desea en otra ocasión intentaré dar una demostración que no dejará dudas". Realmente es difícil negar la afirmación de Gauss; sin embargo, parece ser que el propio Gauss no estaba completamente satisfecho porque continuó proporcionando otras demostraciones del Teorema Fundamental del Álgebra.

En 1850, Puiseux demostró la afirmación de Newton que completaba la prueba de D'Alembert. Por otro lado, la afirmación "indudable" de Gauss es fácilmente demostrable a partir de las propiedades básicas del concepto de continuidad, que no fueron establecidas hasta 1874 por Weierstrass.

Sin embargo, existía una demostración de la afirmación de Newton anterior incluso a la demostración de Gauss. Ésta es debida a Wessel en el año 1797. Por tanto, antes incluso de que Gauss diera su demostración casi completa del Teorema Fundamental del Álgebra, existía una demostración completa uniendo los resultados de d'Alembert y Wessel. La razón de que se asigne a Gauss la primera demostración completa de dicho teorema es que la demostración de Wessel permaneció oculta durante muchos años.

o el hecho de que todos ellos tienen raíces m-ésimas para cualquier entero $m \geq 1$ (esto se demuestra considerando la forma polar, o forma módulo-argumento, de un complejo, y aplicando el Teorema de Bolzano al polinomio $X^m - r$ en el intervalo $[0, r+1]$ para demostrar que todo número real positivo r tiene una raíz m-ésima).

También emplearemos los conceptos de límite y continuidad. En particular, el hecho de que toda función continua $\mathbb{C} \to \mathbb{R}$, por ejemplo, $z \mapsto |p(z)| = +\sqrt{p(z)\overline{p(z)}}$, alcanza su mínimo en cualquier subconjunto cerrado y acotado de $\mathbb{C}$, y por tanto en cualquier "bola" $\{z \in \mathbb{C} \ : \ |z| \leq r\}$, donde r es un número real positivo (Teorema de Weierstrass).

El esquema de la demostración, que desarrollaremos de inmediato, es el siguiente: Comenzamos viendo que la función $z \mapsto |p(z)|$ alcanza su mínimo absoluto en $\mathbb{C}$; para ello, se demuestra que $|p(z)|$ "se hace grande" fuera de cierta bola $\{z \in \mathbb{C} \ : \ |z| \leq r\}$, y entonces el mínimo que alcanza $|p(z)|$ en esa bola es de hecho un mínimo absoluto en $\mathbb{C}$. Bastará entonces ver que ese mínimo vale 0, y esto lo hacemos por reducción al absurdo: si el mínimo no es 0, construimos una función $\mathbb{C} \to \mathbb{R}$ cuyo mínimo absoluto vale 1, y sin embargo encontramos un punto en el que la misma función vale menos de 1. Vamos con los detalles:

Veamos, por inducción en el grado n, que $|p(z)|$ se hace más grande que cualquier número real positivo fuera de cierta bola; es decir, veamos que:

Para cada real $k \geq 0$, existe un real $r \geq 0$ tal que $|p(z)| > k$ para cada complejo $|z| > r$.

En efecto, la expresión de $p(X)$ se reesecribe como

$$p(X) = a_0 + Xq(X), \qquad \text{donde} \quad q(X) = a_1 + a_2 X + \cdots + a_n X^{n-1},$$

y entonces

$$|p(z)| = |zq(z) + a_0| \geq |z| \cdot |q(z)| - |a_0| \qquad \text{para cada } z \in \mathbb{C}.$$

Si $n = 1$ entonces $q = a_1$ es constante y podemos tomar $r = \dfrac{k + |a_0|}{|a_1|}$. En el caso general, la hipótesis de inducción aplicada al polinomio q y a $k' = k + |a_0|$ asegura que existe un real $s \geq 0$ tal que $|q(z)| > k + |a_0|$ cuando $|z| > s$, y entonces es claro que $|p(z)| > a_0$ cuando $|z| > r = \max\{s, 1\}$.

En particular, tomando $k = |a_0|$, encontramos $r \geq 0$ con $|p(z)| > |a_0|$ cuando $|z| > r$. Como la función $|p(z)|$ es continua, alcanza un mínimo en la bola $B = \{z \in \mathbb{C} \ : \ |z| \leq r\}$; es decir, existe $z_0 \in B$ tal que $|p(z_0)| \leq |p(z)|$ para cada $z \in B$. La misma desigualdad se tiene cuando $z \notin B$, pues entonces $|z| > r$ y así $p(z) > |a_0| = p(0) \geq |p(z_0)|$. En consecuencia, $|p(z)|$ alcanza un mínimo absoluto en z_0; es decir, $|p(z_0)| \leq |p(z)|$ para cada $z \in \mathbb{C}$.

Es claro que $p(X)$ tiene una raíz si y sólo si la tiene $p(X + z_0)$, y éste tiene la ventaja de que su módulo alcanza un mínimo absoluto en el 0. Por tanto, sustituyendo $p(X)$ por $p(X + z_0)$, podemos suponer que $z_0 = 0$, y por tanto que $|p(z)| \geq |p(0)| = |a_0|$ para cada $z \in \mathbb{C}$. Si $a_0 = 0$ hemos terminado, claramente, así que se trata de ver que la condición $a_0 \neq 0$ nos lleva a una contradicción.

En este caso, dividir por a_0 no va a cambiar el punto en el que se alcanza el mínimo, por lo que podemos suponer que $a_0 = 1$. Excluyendo monomios con coeficiente nulo, podemos escribir

$$p(X) = 1 + a_m X^m + a_{m+1} X^{m+1} + \cdots + a_n X^n \qquad (\text{con } a_m \neq 0)$$

para cierto entero m con $1 \leq m \leq n$. Sea ahora ω una raíz m-ésima de $-a_m^{-1}$ (es decir, $\omega \in \mathbb{C}$ verifica $\omega^m = -a_m^{-1}$). Entonces $p(\omega X) = 1 - X^m +$ (términos de grado mayor que m); es decir,

$$p(\omega X) = 1 - X^m + X^m h(X),$$

donde $h(X)$ es cierto polinomio con $h(0) = 0$.

Finalmente, vamos a encontrar un número real t tal que $|p(\omega t)| < 1$, lo que nos dará la contradicción buscada puesto que 1 es el mínimo absoluto de $|p(z)|$. Consideremos la función $\mathbb{R} \to \mathbb{R}$ dada por $t \mapsto |h(t)|$. Considerando su límite en $x = 0$ (que vale 0 por continuidad) encontramos un número t en el intervalo $(0, 1)$ tal que $|h(t)| < 1$ (haciendo $\epsilon = 1$ en la formulación usual del límite). Entonces también t^m y $1 - t^m$ están en el intervalo $(0, 1)$, por lo que

$$|p(\omega t)| \leq |1 - t^m| + |t^m h(t)| < 1 - t^m + t^m \cdot 1 = 1,$$

como queríamos ver.

4.5 Factorización única en anillos de polinomios

En toda esta sección, excepto mención expresa de lo contrario, D será un DFU y K será su cuerpo de fracciones. Estudiaremos la divisibilidad en el anillo de polinomios $D[X]$, hasta demostrar que $D[X]$ es también un DFU. Comenzamos con un resultado elemental:

Ejercicio 4.5.1 *Sea D un dominio (no necesariamente un DFU) y sea $p \in D$. Demostrar que:*

1. *p es irreducible en D si y sólo si lo es en $D[X]$.*
2. *Si p es primo en $D[X]$ entonces lo es en D.*

Este ejercicio se usará para demostrar el recíproco del resultado principal, y a su vez motiva el siguiente resultado, conocido como Lema de Gauss. Por otra parte, el paso clave en lo que sigue será la demostración de que todo irreducible es primo en $D[X]$, y podemos interpretar el Lema de Gauss como la solución del problema para polinomios constantes:

Lema 4.5.2 (Lema de Gauss) *Para un elemento $p \in D$, las condiciones siguientes son equivalentes:*

1. *p es irreducible (y primo) en D.*
2. *p es irreducible en $D[X]$.*
3. *p es primo en $D[X]$.*

Demostración. Como D es un DFU, las dos versiones de 1 son equivalentes. 3 implica 2 es cierto en general (Proposición 3.1.11), y 2 implica 1 se sigue del Ejercicio 4.5.1. Supongamos por tanto que p es primo en D, y veamos que lo es en $D[X]$. Para ello, sean

$$f = a_0 + \cdots + a_n X^n \qquad \text{y} \qquad g = b_0 + \cdots + b_m X^m$$

polinomios de $D[X]$ tales que $p \nmid f$ y $p \nmid g$, y veamos que $p \nmid fg$. Por hipótesis, existen un menor índice i tal que $p \nmid a_i$, y un menor índice j tal que $p \nmid b_j$. El coeficiente de grado $i+j$ de fg es

$$c_{i+j} = a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0,$$

y las condiciones dadas implican que p divide a todos los sumandos excepto a $a_i b_j$, por lo que $p \nmid c_{i+j}$ y en consecuencia $p \nmid fg$. □

En lo que sigue vamos a explotar sistemáticamente el hecho de que todo polinomio sobre D puede verse como un polinomio sobre su cuerpo de fracciones K. Para ello necesitamos un lema técnico en el que usaremos la función

$$\varphi : D \setminus \{0\} \to \mathbb{N}$$

que a cada $0 \neq a \in D$ le asocia el número $\varphi(a)$ de factores irreducibles en la expresión de a como producto de irreducibles de D, contando repeticiones. Por ejemplo, si $D = \mathbb{Z}$ entonces $\varphi(12) = 3$ y $\varphi(-80) = 5$. Es claro que, si $a, b \in D \setminus \{0\}$, entonces

$$\varphi(ab) = \varphi(a) + \varphi(b) \qquad \text{y} \qquad \varphi(a) = 0 \Leftrightarrow a \in D^*.$$

Lema 4.5.3 *Si $a \in D$ y $f, g, h \in D[X]$ verifican $af = gh \neq 0$, entonces existen $g_1, h_1 \in D[X]$ tales que*

$$f = g_1 h_1, \qquad \operatorname{gr}(g_1) = \operatorname{gr}(g), \qquad \operatorname{gr}(h_1) = \operatorname{gr}(h).$$

Demostración. Razonamos por inducción en $\varphi(a)$. Si $\varphi(a) = 0$ podemos tomar $g_1 = a^{-1} g$ y $h_1 = h$. Si $\varphi(a) > 0$, existen $p, b \in D$ tales que $a = pb$ y p es primo. Entonces $p \mid af = gh$ en $D[X]$ y, por el Lema de Gauss (4.5.2), podemos asumir que $p \mid g$ en $D[X]$. Es decir, existe $\bar{g} \in D[X]$ tal que $g = p\bar{g}$, de donde $\operatorname{gr}(g) = \operatorname{gr}(\bar{g})$. Cancelando p en la igualdad $af = gh$ obtenemos $bf = \bar{g}h$. Como $\varphi(b) = \varphi(a) - 1 < \varphi(a)$, la hipótesis de inducción nos dice que existen $g_1, h_1 \in D[X]$ tales que $f = g_1 h_1$, $\operatorname{gr}(g_1) = \operatorname{gr}(\bar{g})$, y $\operatorname{gr}(h_1) = \operatorname{gr}(h)$, lo que nos da el resultado. □

El siguiente resultado relaciona la irreducibilidad de un polinomio sobre D con su irreducibilidad sobre K. Aunque su recíproco es falso en general (piénsese en $2X$ como polinomio sobre $\mathbb{Z}$), pronto veremos que es válido con una condición extra sobre el polinomio (Proposición 4.6.1).

Lema 4.5.4 *Si $f \in D[X]$ es irreducible en $D[X]$, entonces es irreducible (o primo) en $K[X]$.*

Demostración. Supongamos que f no es irreducible en $K[X]$. Por la Proposición 4.1.4, existen $G, H \in K[X]$ tales que

$$f = GH, \qquad \mathrm{gr}(G) > 0, \qquad \mathrm{gr}(H) > 0.$$

Si $0 \neq b \in D$ es un múltiplo común de los denominadores de los coeficientes de G, se tiene $g = bG \in D[X]$, y análogamente existe $0 \neq c \in D$ tal que $h = cH \in D[X]$. Aplicando el Lema 4.5.3 a la igualdad $(bc)f = gh$ obtenemos $g_1, h_1 \in D[X]$ tales que $f = g_1 h_1$, $\mathrm{gr}(g_1) = \mathrm{gr}(g) = \mathrm{gr}(G) > 0$, y $\mathrm{gr}(h_1) = \mathrm{gr}(h) = \mathrm{gr}(H) > 0$, lo que nos da una factorización no trivial de f en $D[X]$. □

Podemos ya demostrar el resultado principal de esta sección:

Teorema 4.5.5 *D es un DFU si y sólo si lo es $D[X]$.*

Demostración. Supongamos primero que $D[X]$ es un DFU. Entonces D es un dominio (Corolario 4.1.3), y cada $0 \neq a \in D \setminus D^*$ es producto de irreducibles de $D[X]$, que tendrán grado 0 pues lo tiene a. Por el Ejercicio 4.5.1, ésa será una factorización de a en irreducibles de D. Del mismo ejercicio se deduce que todo irreducible de D es primo en D, por lo que D es un DFU.

Supongamos ahora que D es un DFU y veamos que lo es $D[X]$. Empezaremos demostrando que cada $f = a_0 + \cdots + aX^n \in D[X]$ (con $a \neq 0$) no invertible es producto de irreducibles, y lo haremos por inducción en $n + \varphi(a)$. Obsérvese que f es invertible si y sólo si $n + \varphi(a) = 0$. El caso $n + \varphi(a) = 1$ se resuelve fácilmente. Supongamos pues que $n + \varphi(a) > 1$ y que f no es irreducible. Entonces existen

$$g = b_0 + \cdots + b_m X^m \quad (b = b_m \neq 0) \qquad \text{y} \qquad h = c_0 + \cdots + c_k X^k \quad (c = c_k \neq 0)$$

en $D[X]$, no invertibles, con $f = gh$. Entonces se tiene

$$0 < m + \varphi(b), \quad 0 < k + \varphi(c) \quad \text{y} \quad n + \varphi(a) = m + k + \varphi(b) + \varphi(c).$$

En consecuencia, podemos aplicar la hipótesis de inducción a g y h, y pegando las factorizaciones así obtenidas conseguimos una factorización en irreducibles de f.

Por la Proposición 3.4.5, sólo falta demostrar que todo irreducible f de $D[X]$ es primo, y por el Lema de Gauss podemos suponer que $\mathrm{gr}(f) \geq 1$. Sean pues $g, h \in D[X]$ tales que $f \mid gh$ en $D[X]$, y veamos que $f \mid g$ ó $f \mid h$ en $D[X]$. Obviamente, $f \mid gh$ en $K[X]$, y como f es primo en $K[X]$ por el Lema 4.5.4, podemos asumir que $f \mid g$ en $K[X]$. Es decir, existe $G \in K[X]$ tal que $g = fG$, y si vemos que $G \in D[X]$ habremos terminado. Para ello, tomando $a \in D$ con $aG \in D[X]$ y $\varphi(a)$ mínimo, basta ver que $\varphi(a) = 0$. Supongamos que $\varphi(a) > 0$ y sean $p, b \in D$ con $a = pb$ y p primo. Entonces, en $D[X]$, se tiene $p \mid ag = f(aG)$. Como p es primo en $D[X]$ (Lema de Gauss) y $p \nmid f$ (pues f es irreducible y $\mathrm{gr}(f) \geq 1$), deducimos que $p \mid aG$ en $D[X]$. Si $g_1 \in D[X]$ verifica $aG = pg_1$ entonces $bG = g_1 \in D[X]$, contra la minimalidad de $\varphi(a)$, y esta contradicción termina la demostración. □

Del Teorema 4.5.5 se deduce que $\mathbb{Z}[X]$ es un DFU pero no un DIP, lo que muestra que el recíproco del Teorema 3.4.6 no es cierto.

4.6 Factorización e irreducibilidad de polinomios

En esta sección, como en la anterior, D denota un DFU y K su cuerpo de fracciones. El objetivo genérico es factorizar polinomios en $D[X]$ y en $K[X]$, y para ello es necesario disponer de métodos que nos digan cuándo un polinomio es irreducible. Como se verá, pocos de los resultados prácticos que obtendremos nos dan condiciones necesarias y suficientes para que un polinomio sea irreducible[2].

Comenzamos con un resultado que relaciona la irreducibilidad de polinomios en $D[X]$ y en $K[X]$, y que completa el Lema 4.5.4. Para ello introducimos una noción que será muy práctica: Diremos que un polinomio $f = a_0 + \cdots + a_n X^n \in D[X]$ es *primitivo* si $\mathrm{mcd}(a_0, \ldots, a_n) = 1$; es decir, si sus únicos divisores de grado 0 son las unidades de $D[X]$.

[2] En el Problema 31 esbozaremos el llamado *algoritmo de Kronecker*, que sí establece una condición necesaria y suficiente cuando $D = \mathbb{Z}$.

Proposición 4.6.1 *Para un polinomio primitivo $f \in D[X]$, las condiciones siguientes son equivalentes:*

1. *f es irreducible en $D[X]$.*
2. *f es irreducible en $K[X]$.*
3. *Si $f = GH$ con $G, H \in K[X]$ entonces $\mathrm{gr}(G) = 0$ ó $\mathrm{gr}(H) = 0$.*
4. *Si $f = gh$ con $g, h \in D[X]$ entonces $\mathrm{gr}(g) = 0$ ó $\mathrm{gr}(h) = 0$.*

Demostración. El Lema 4.5.4 y la Proposición 4.1.4 aseguran que 1 implica 2 y que 2 implica 3, respectivamente, y es claro que 3 implica 4. Finalmente, como f es primitivo, sus únicos divisores de grado 0 son unidades, por lo que 4 implica 1. □

Asumiremos que disponemos de un método para factorizar los coeficientes de D, y en particular para decidir si son irreducibles o no. Esto es teóricamente posible si $D = \mathbb{Z}$ ó $D = \mathbb{Z}[i]$ (y también lo es en la práctica en los casos que se nos presentarán), y nos permite además decidir si un polinomio de $D[X]$ es o no primitivo.

En general, dado un polinomio $0 \neq f \in D[X]$, calcularemos el máximo común divisor $d \neq 0$ de sus coeficientes y obtendremos $f = df_1$, con $f_1 \in D[X]$ primitivo. El polinomio constante d es una unidad en $K[X]$, mientras que en $D[X]$ tiene la misma factorización en irreducibles que tenga como elemento de D. En cuanto a f_1, para decidir su irreducibilidad, la Proposición 4.6.1 nos permite considerarlo como polinomio sobre D o sobre K según nos convenga. Por tanto, es importante tener criterios de irreducibilidad como los que siguen para polinomios sobre cuerpos.

Ejercicio 4.6.2 *Sea K un cuerpo y sea $f \in K[X]$. Demostrar que:*

1. *Si $\mathrm{gr}(f) = 1$ entonces f es irreducible en $K[X]$.*
2. *Si $\mathrm{gr}(f) > 1$ y f tiene una raíz en K, entonces f no es irreducible en $K[X]$.*
3. *Si $\mathrm{gr}(f) = 2$ ó 3 entonces f es irreducible en $K[X]$ si y sólo si f no tiene raíces en K.*
4. *Si K es algebraicamente cerrado (por ejemplo, si $K = \mathbb{C}$), entonces f es irreducible si y sólo si $\mathrm{gr}(f) = 1$.*

La no existencia de raíces no garantiza la irreducibilidad de polinomios de grado mayor que 3. Por ejemplo, $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ es reducible en $\mathbb{R}[X]$ pero no tiene raíces reales.

La estrecha relación entre $\mathbb{R}$ y $\mathbb{C}$ nos permite obtener el siguiente criterio de irreducibilidad para polinomios con coeficientes reales. Nótese que, en la práctica, considerar sólo polinomios mónicos no supone ninguna restricción.

Proposición 4.6.3 *Sea $f \in \mathbb{R}[X]$ un polinomio mónico con coeficientes reales. Entonces:*

1. *Si α es una raíz de f en $\mathbb{C}$, el conjugado $\bar{\alpha}$ también es una raíz de f en $\mathbb{C}$, y las multiplicidades de α y $\bar{\alpha}$ en f son iguales.*
2. *f es irreducible en $\mathbb{R}[X]$ precisamente si tiene grado 1 o es de la forma $X^2 + bX + c$ con $b^2 < 4c$.*

Demostración. El automorfismo de conjugación en $\mathbb{C}$ induce un automorfismo $\mathbb{C}[X] \to \mathbb{C}[X]$ que es la identidad sobre $\mathbb{R}[X]$, por lo que f coincide con su imagen por este automorfismo. Por tanto, si $f = \prod_{i=1}^{n}(X - \alpha_i)^{k_i}$ es la factorización irredundante de f en $\mathbb{C}[X]$, entonces $f = \prod_{i=1}^{n}(X - \overline{\alpha_i})^{k_i}$, de donde se deduce 1.

La condición de 2 es claramente suficiente para la irreducibilidad de f en $\mathbb{R}[X]$, y necesaria si $\mathrm{gr} f \leq 2$. De 1 y de la igualdad

$$(X - \alpha)(X - \bar{\alpha}) = (X - r - si)(X - r + si) = (X - r)^2 - (si)^2 = X^2 - 2rX + (r^2 + s^2)$$

(donde $\alpha = r + si$) se deduce que los polinomios irreducibles de $\mathbb{R}[X]$ tienen grado menor o igual que 2, lo que termina la demostración. □

El Ejercicio 4.6.2 pone de manifiesto la importancia de encontrar raíces de un polinomio para decidir si es irreducible. Cuando los coeficientes están en un DFU podemos seleccionar los "candidatos a raíces":

Proposición 4.6.4 *Sea D un DFU con cuerpo de fracciones K, y sea $f = a_0+a_1X+\cdots+a_nX^n \in D[X]$ con $a_n \neq 0$. Entonces todas las raíces de f en K son de la forma r/s, donde $r \mid a_0$ y $s \mid a_n$.*

Demostración. Sea $t = \frac{r}{s}$ una raíz de f con $r, s \in D$ primos entre sí. Multiplicando la igualdad $f(t) = 0$ por s^n obtenemos

$$a_0 s^n + a_1 r s^{n-1} + a_2 r^2 s^{n-2} + \cdots + a_{n-1} r^{n-1} s + a_n r^n = 0,$$

luego $r \mid a_0 s^n$ y $s \mid a_n r^n$. Como r y s son coprimos, deducimos de la Proposición 3.4.4 que $r \mid a_0$ y $s \mid a_n$. □

Ejemplos 4.6.5 *Factorizaciones de polinomios.*

1. Las posibles raíces en $\mathbb{Q}$ del polinomio $f = 3X^3 + X^2 + X - 2$ son ± 2, ± 1, $\pm 2/3$ y $\pm 1/3$, y de hecho $f(2/3) = 0$. Por tanto $(X - 2/3) \mid f$, y así $(3X - 2) \mid f$. Dividiendo se obtiene $f = (3X - 2)(X^2 + X + 1)$. Como ambos factores son primitivos sobre $\mathbb{Z}$ e irreducibles sobre $\mathbb{Q}$ y sobre $\mathbb{R}$, deducimos que la anterior es una factorización en irreducibles de f en cualquiera de los anillos $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ ó $\mathbb{R}[X]$. La factorización en $\mathbb{C}[X]$ es $f = (3X - 2)(X - \omega)(X - \bar{\omega})$, donde $\omega = \frac{-1+\sqrt{-3}}{2}$.

2. El polinomio $f = 6X^4 + 6X^2 + 18X - 30 = 3 \cdot 2 \cdot (X^4 + X^2 + 3X - 5)$ tiene al 1 por raíz, y dividiendo se tiene $X^4 + X^2 + 3X - 5 = (X - 1)(X^3 + X^2 + 2X + 5)$. El factor cúbico es primitivo y no tiene raíces en $\mathbb{Q}$ (al sustituir ± 1 ó ± 5 se obtiene un entero impar), por lo que

   $$f = 3 \cdot 2 \cdot (X - 1)(X^3 + X^2 + 2X + 5) \qquad \text{y} \qquad f = 6(X - 1)(X^3 + X^2 + 2X + 5)$$

   son las factorizaciones de f en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$, respectivamente (en la segunda el 6 no es un factor irreducible, sino una unidad). El polinomio cúbico no es irreducible en $\mathbb{R}[X]$ ni en $\mathbb{C}[X]$. De hecho, un análisis del crecimiento de la función polinómica $f : \mathbb{R} \to \mathbb{R}$ nos lleva a la conclusión de que f tiene una raíz real y dos complejas conjugadas. Para la determinación explícita de estas raíces, véase el Problema 39.

3. El polinomio $f = X^4 + X^3 + 2X^2 + X + 1$ no tiene raíces racionales, pero esto no implica que sea irreducible sobre $\mathbb{Q}$. De hecho, se tiene $f(i) = 0$, y por tanto $(X - i)(X + i) = X^2 + 1$ divide a f; el otro factor es $X^2 + X + 1$, por lo que $f = (X^2 + 1)(X^2 + X + 1)$ es una factorización en irreducibles en $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ ó $\mathbb{R}[X]$, y $f = (X - i)(X + i)(X - \omega)(X - \bar{\omega})$ (con $\omega = \frac{-1+\sqrt{-3}}{2}$) es una factorización en $\mathbb{C}[X]$.

4. Supongamos que el polinomio sin raíces racionales $f = X^4 - 2X^3 + 6X - 3$ no es irreducible en $\mathbb{Z}[X]$. Por la Proposición 4.6.1, existen $g, h \in \mathbb{Z}[X]$, ambos de grado ≥ 1, tales que $f = gh$. Podemos asumir que g y h son mónicos (¿por qué?), y por tanto no pueden tener grado 1 (¿por qué?). En consecuencia, ambos tienen grado 2 y por tanto existen $a, b, c, d \in \mathbb{Z}$ tales que $f = (X^2 + aX + b)(X^2 + cX + d)$. Igualando coeficientes, se obtienen las ecuaciones

   $$bd = -3, \quad ad + bc = 6, \quad b + ac + d = 0, \quad a + c = -2.$$

   La primera ecuación nos da 4 opciones para los valores de b y d. Una de ellas es $b = 1$ y $d = -3$, que sustituida en la segunda ecuación y combinada con la cuarta nos dice que $a = -2$ y $c = 0$; pero estos valores no satisfacen la tercera ecuación. De modo similar se ve que las otras opciones tampoco funcionan, lo que significa que no existen tales $a, b, c, d \in \mathbb{Z}$ y en consecuencia f es irreducible en $\mathbb{Z}[X]$, y por tanto también en $\mathbb{Q}[X]$.

El último ejemplo muestra lo penoso que puede resultar estudiar la irreducibilidad de un polinomio, incluso de grado bajo, con los métodos que hemos desarrollado hasta ahora. El resto de esta sección lo dedicamos a presentar otros dos criterios de irreducibilidad para polinomios sobre un DFU que son a menudo útiles.

En el primero de ellos usaremos los Ejemplos 4.2.3: Un homomorfismo de anillos $\phi : A \to B$ induce otro $A[X] \to B[X]$ dado por

$$f = \sum a_i X^i \mapsto f^\phi = \sum \phi(a_i) X^i.$$

En general se tiene $\operatorname{gr}(f^\phi) \leq \operatorname{gr}(f)$, con igualdad si el coeficiente principal de f no está en $\operatorname{Ker} \phi$.

Proposición 4.6.6 (Criterio de Reducción) *Sea $\phi : D \to K$ un homomorfismo de anillos, donde D es un DFU y K es un cuerpo, y sea f un polinomio primitivo de $D[X]$. Si f^ϕ es irreducible en $K[X]$ y $\mathrm{gr}(f^\phi) = \mathrm{gr}(f)$, entonces f es irreducible en $D[X]$.*

Demostración. Por la Proposición 4.6.1 basta ver que, si $f = gh$ con $g, h \in D[X]$, entonces $\mathrm{gr}(g) = 0$ ó $\mathrm{gr}(h) = 0$. Sean a, b y c los coeficientes principales de f, g y h, respectivamente. Entonces $a = bc \notin \mathrm{Ker}\ \phi$ y por tanto $b, c \notin \mathrm{Ker}\ \phi$, por lo que $\mathrm{gr}(g^\phi) = \mathrm{gr}(g)$ y $\mathrm{gr}(h^\phi) = \mathrm{gr}(h)$. Como K es un cuerpo y f^ϕ es irreducible en $K[X]$, la igualdad $f^\phi = g^\phi h^\phi$ implica que $\mathrm{gr}(g^\phi) = 0$ ó $\mathrm{gr}(h^\phi) = 0$, de donde se sigue el resultado. □

Cuando consideramos la proyección $\mathbb{Z} \to \mathbb{Z}_p$, el homomorfismo $\mathbb{Z}[X] \to \mathbb{Z}_p[X]$ viene dado por

$$f = \sum a_i X^i \mapsto \bar{f} = \sum \bar{a}_i X^i,$$

donde $\bar{a}$ es la clase de a en $\mathbb{Z}_p$. Aplicando el Criterio de Reducción se obtiene:

Corolario 4.6.7 *Sea p un entero primo y sea $f = a_0 + \cdots + a_n X^n$ un polinomio primitivo de $\mathbb{Z}[X]$. Si $p \nmid a_n$ y $\bar{f}$ es irreducible en $\mathbb{Z}_p[X]$, entonces f es irreducible en $\mathbb{Z}[X]$.*

Ejemplos 4.6.8 *Aplicaciones del Criterio de Reducción.*

1. Reduciendo módulo 2 el polinomio $f = 7X^3 + 218X^2 + 121X + 625$ obtenemos el polinomio $\bar{f} = X^3 + X + 1$ de $\mathbb{Z}_2[X]$, que es irreducible porque no tiene raíces. Por tanto f es irreducible en $\mathbb{Z}[X]$ (y en $\mathbb{Q}[X]$).

2. Reduciendo $f = X^4 + 5X + 1 \in \mathbb{Z}[X]$ módulo 2 obtenemos $\bar{f} = X^4 + X + 1 \in \mathbb{Z}_2[X]$. Como $\bar{f}$ no tiene raíces en $\mathbb{Z}_2$, si no fuera irreducible se factorizaría como producto de dos polinomios irreducibles de grado 2 en $\mathbb{Z}_2[X]$. Pero en $\mathbb{Z}_2[X]$ sólo hay 4 polinomios de grado 2, y de ellos sólo $X^2 + X + 1$ es irreducible (¿por qué?). Como $\bar{f}$ no es el cuadrado de éste, deducimos que $\bar{f}$ es irreducible en $\mathbb{Z}_2[X]$ y por tanto f es irreducible en $\mathbb{Z}[X]$.

3. Consideremos el polinomio $f = X^5 - X - 1$ de $\mathbb{Z}[X]$. Reduciendo módulo 2 obtenemos un polinomio que es divisible por $X^2 + X + 1$, por lo que no podemos aplicar el Criterio de Reducción. Reduciendo módulo 3 obtenemos $\bar{f} = X^5 + 2X + 2 \in \mathbb{Z}_3[X]$, que no tiene raíces. Si no fuera irreducible tendría un factor irreducible de grado 2; es fácil ver que los únicos irreducibles mónicos de grado 2 de $\mathbb{Z}_3[X]$ son
$$X^2 + 1, \qquad X^2 + X - 1, \qquad X^2 - X - 1.$$
Comprobando que ninguno de ellos divide a $\bar{f}$ deducimos que $\bar{f}$ es irreducible en $\mathbb{Z}_3[X]$, y por tanto f es irreducible en $\mathbb{Z}[X]$.

4. Dado el polinomio $f = X^4 + 4X + 1$ en $\mathbb{Z}[X]$, se tiene $\bar{f} = (X + 1)^4$ en $\mathbb{Z}_2[X]$ y $\bar{f} = (X + 2)(X^3 + X^2 + X + 2)$ en $\mathbb{Z}_3[X]$, con el factor cúbico irreducible porque no tiene raíces. Por tanto, no podemos aplicar el Criterio de Reducción. Sin embargo, la factorización en $\mathbb{Z}_3[X]$ nos va a permitir demostrar que f es irreducible en $\mathbb{Z}[X]$. En efecto, como f no tiene raíces en $\mathbb{Q}$, si no fuera irreducible en $\mathbb{Z}[X]$ se tendría $f = gh$ con $\mathrm{gr}(g) = \mathrm{gr}(h) = 2$. Esto nos daría, en $\mathbb{Z}_3$, la factorización $\bar{f} = \bar{g}\bar{h}$ con $\mathrm{gr}(\bar{g}) = \mathrm{gr}(\bar{h}) = 2$, incompatible con la factorización en irreducibles (única salvo asociados) que acabamos de obtener.

Veamos nuestro último criterio de irreducibilidad:

Proposición 4.6.9 (Criterio de Eisenstein) *Sea D un DFU y sea $f = a_0 + a_1 X + \cdots + a_n X^n$ (con $a_n \neq 0$) un polinomio primitivo de $D[X]$. Si existe un irreducible $p \in D$ tal que*

$$p \mid a_i \text{ para todo } i < n, \qquad y \qquad p^2 \nmid a_0,$$

entonces f es irreducible en $D[X]$.

Demostración. Veamos que, si $f = gh$ en $D[X]$, entonces $\mathrm{gr}(g) = n$ ó $\mathrm{gr}(h) = n$. Pongamos $g = b_0 + \cdots + b_m X^m$ y $h = c_0 + \cdots + c_k X^k$, con $b_m c_k \neq 0$. Como $p^2 \not| a_0 = b_0 c_0$, entonces $p \not| b_0$ ó $p \not| c_0$. Supongamos que se da la segunda opción. Como f es primitivo se tiene $p \not| g$, y por tanto existe

$$i = \min\{j : p \not| b_j\}.$$

Entonces p no divide a $a_i = (\sum_{j=0}^{i-1} b_j c_{i-j}) + b_i c_0$, y por tanto $i = n$, de modo que $\mathrm{gr}(g) = n$. La opción $p \not| b_0$ nos llevaría a $\mathrm{gr}(h) = n$, lo que demuestra el resultado. □

Ejemplos 4.6.10 *Aplicaciones del Criterio de Eisenstein.*

1. Sean a un entero y p un primo cuya multiplicidad en a es 1. Entonces $X^n - a$ es irreducible.

2. Un argumento similar al del apartado 4 de los Ejemplos 4.6.5 nos permitiría ver que el polinomio $f = X^4 - 3X^3 + 6X - 3$ es irreducible en $\mathbb{Z}[X]$. Ahora podemos asegurar lo mismo con menos trabajo aplicando el Criterio de Eisenstein con $p = 3$.

3. A menudo, el Criterio de Eisenstein se combina con un automorfismo de $\mathbb{Z}[X]$ de sustitución en $X+a$ (Ejemplos 4.2.3). Por ejemplo, el criterio no es aplicable a $f(X) = X^4+4X^3+10X^2+12X+7$, pero sí se puede aplicar (con $p = 2$) a $f(X-1) = X^4+4X^2+2$. Por tanto $f(X-1)$ es irreducible, y en consecuencia lo es $f(X)$.

4. Dado un entero $n \geq 3$, las raíces en $\mathbb{C}$ del polinomio $X^n - 1$ se llaman *raíces n-ésimas* de la unidad (o de 1). Considerando la interpretación geométrica de la multiplicación en $\mathbb{C}$, es fácil ver que estas raíces son exactamente los n vértices del n-ágono regular inscrito en el círculo unidad de $\mathbb{C}$ que tiene un vértice en la posición del 1. Estos números complejos son útiles en muy diversas circunstancias. El polinomio $X^n - 1$ se factoriza como

$$X^n - 1 = (X-1)\Phi_n(X), \qquad \text{donde } \Phi_n(X) = X^{n-1} + X^{n-2} + \cdots + X^2 + X + 1.$$

   El polinomio $\Phi_n(X)$ se conoce como el n-ésimo *polinomio ciclotómico*, y sus raíces son las raíces n-ésimas de 1 distintas de 1. $\Phi_n(X)$ no es en general irreducible sobre $\mathbb{Q}$ (por ejemplo, $\Phi_4(X)$ es divisible por $X + 1$), pero sí lo es cuando $n = p$ es primo. Como en el apartado anterior, esto quedará demostrado si podemos aplicar el Criterio de Eisenstein a $\Phi_p(X + 1)$. Ahora bien, $\Phi_p(X) = (X^n - 1)/(X - 1)$, y por tanto

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{p-1} X^{p-2} + \binom{p}{p-2} X^{p-3} + \cdots + \binom{p}{2} X + p.$$

   Cuando $1 \leq i < p$, el primo p no divide a $i!$ ni a $(p-i)!$, y por tanto sí divide a $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$, por lo que podemos aplicar el Criterio de Eisenstein, como queríamos.

Cerramos la sección con un ejemplo en el que se combinan casi todos los métodos empleados anteriormente.

Ejemplo 4.6.11 *Factorizaciones de $5X^4 + 5$ en distintos anillos.*

Vamos a factorizar en irreducibles el polinomio $g = 5X^4 + 5$ considerando cada uno de los siguientes anillos de coeficientes: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$ y $\mathbb{Z}_3$. Como $g = 5f$, donde $f = X^4 + 1$, podemos factorizar $f = X^4 + 1$ y añadir un 5 a cada una de las factorizaciones que siguen. En todas ellas ese 5 será una unidad, excepto en la de $\mathbb{Z}[X]$, donde será un factor irreducible más.

En $\mathbb{Z}_2[X]$ se tiene $X^4 + 1 = (X + 1)^4$, luego f es producto de cuatro irreducibles iguales.

Como f no tiene raíces en $\mathbb{Z}_3$, si no es irreducible en $\mathbb{Z}_3[X]$ será producto de dos irreducibles de grado 2. Como tenemos la lista de estos irreducibles (Ejemplos 4.6.8), podemos dividir f por cada uno de ellos hasta obtener la factorización $f = (X^2 + X + 2)(X^2 + 2X + 2)$.

La sencillez del polinomio $X^4 + 1$ nos permite calcular "a mano" sus raíces complejas. En efecto, la ecuación $X^4 + 1 = 0$ se reescribe como $(X^2)^2 = -1$, de donde $X^2 = \pm i$ y así $X = \dfrac{\pm 1 \pm i}{\sqrt{2}}$. Por tanto

$$f = (X - \frac{1+i}{\sqrt{2}})(X - \frac{1-i}{\sqrt{2}})(X - \frac{-1+i}{\sqrt{2}})(X - \frac{-1-i}{\sqrt{2}})$$

es la factorización de f como producto de irreducibles en $\mathbb{C}[X]$. Agrupando las raíces complejas como en la demostración de la Proposición 4.6.3, obtenemos la factorización en irreducibles de $\mathbb{R}[X]$:

$$f = \left[(X - \frac{1}{\sqrt{2}})^2 - (\frac{i}{\sqrt{2}})^2\right] \cdot \left[(X + \frac{1}{\sqrt{2}})^2 - (\frac{i}{\sqrt{2}})^2\right] = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$$

Esta factorización también puede obtenerse directamente, "completando cuadrados" como sigue:

$$f = X^4 + 2X^2 + 1 - 2X^2 = (X^2 + 1)^2 - (\sqrt{2}X)^2 = (X^2 + 1 + \sqrt{2}X)(X^2 + 1 - \sqrt{2}X).$$

Si f tuviera una factorización no trivial en $\mathbb{Q}[X]$, ésta sería también una factorización no trivial en $\mathbb{R}[X]$. Como es claro que cualquier asociado de $X^2 \pm \sqrt{2}X + 1$ en $\mathbb{R}[X]$ tiene coeficientes irracionales, no existe tal factorización y, en consecuencia, f es irreducible en $\mathbb{Q}[X]$, y también en $\mathbb{Z}[X]$ por ser primitivo. También podemos asegurar la irreducibilidad de f aplicando el Criterio de Eisenstein a $f(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 2$. En conclusión, g es irreducible en $\mathbb{Q}[X]$, mientras que en $\mathbb{Z}[X]$ se factoriza como producto de dos irreducibles, $g = 5f$.

4.7 Polinomios en varias indeterminadas

Dados un anillo A y un entero $n \geq 2$, definimos el *anillo de polinomios en n indeterminadas con coeficientes en A*, denotado por $A[X_1, \ldots, X_n]$, mediante la fórmula recurrente

$$A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n].$$

Los elementos $X_1, \ldots, X_n$ de $A[X_1, \ldots, X_n]$ se llaman *indeterminadas* y los elementos de $A[X_1, \ldots, X_n]$ se llaman *polinomios en n indeterminadas*.

Por inducción a partir del Corolario 4.1.3, de la Proposición 4.1.4 y del Teorema 4.5.5, se obtiene:

Proposición 4.7.1 *Para un anillo A y un entero positivo n se verifican:*

1. *$A[X_1, \ldots, X_n]$ nunca es un cuerpo.*
2. *$A[X_1, \ldots, X_n]$ es un dominio si y sólo si lo es A.*
3. *Si $n \geq 2$ entonces $A[X_1, \ldots, X_n]$ no es un DIP.*
4. *$A[X_1, \ldots, X_n]$ es un DFU si y sólo si lo es A.*

Si $a \in A$ e $i = (i_1, \ldots, i_n) \in \mathbb{N}^n$, el elemento $aX_1^{i_1} \cdots X_n^{i_n}$ de $A[X_1, \ldots, X_n]$ se llama *monomio* de *tipo i* y coeficiente a.

Lema 4.7.2 *Sean A un anillo y n un entero positivo. Entonces todo elemento p de $A[X_1, \ldots, X_n]$ se escribe de forma única como suma de monomios de distinto tipo, casi todos con coeficiente nulo. Es decir, se tiene una única expresión*

$$p = \sum_{i \in \mathbb{N}^n} p_i X_1^{i_1} \cdots X_n^{i_n} \tag{4.7.1}$$

con $p_i = 0$ para casi todo $i = (i_1, \ldots, i_n) \in \mathbb{N}^n$.

Demostración. Aplicamos inducción en n, con el caso $n = 1$ resuelto por el Lema 4.1.1. Cuando $n > 1$, un elemento de $A[X_1, \ldots, X_n]$ es, por definición, de la forma $\sum_{t \in \mathbb{N}} p_t X_n^t$ con cada $p_t \in A[X_1, \ldots, X_{n-1}]$ y casi todos los p_t nulos. Por hipótesis de inducción, cada p_t se expresa como

$$p_t = \sum_{(i_1, \ldots, i_{n-1}) \in \mathbb{N}^{n-1}} (p_t)_{(i_1, \ldots, i_{n-1})} X_1^{i_1} \cdots X_{n-1}^{i_{n-1}},$$

donde cada $(p_t)_{(i_1, \ldots, i_{n-1})}$ está en A y casi todos son nulos. Definiendo $p_i = (p_{i_n})_{(i_1, \ldots, i_{n-1})}$ (para $i = (i_1, \ldots, i_n)$) tenemos la expresión deseada.

Recíprocamente, una expresión como (4.7.1) puede reescribirse como un polinomio en X_n con coeficientes en $A[X_1,\dots,X_{n-1}]$ sin más que definir cada coeficiente como $p_t = \sum p_i X_1^{i_1}\cdots X_{n-1}^{i_{n-1}}$, con la suma extendida a todos los $i=(i_1,\dots,i_n)\in\mathbb{N}^n$ con $i_n = t$. Usando esto es sencillo demostrar que estas expresiones son únicas, asumiendo que lo son en $A[X_1,\dots,X_{n-1}]$. □

Usando el Lema 4.7.2 se demuestra:

Proposición 4.7.3 *Sean A un anillo, $n\geq 1$ un entero y $u: A\to A[X_1,\dots,X_n]$ la inclusión.*

1. **(PUAP en n indeterminadas)** *Dados un homomorfismo de anillos $f: A\to B$ y n elementos $b_1,\dots,b_n\in B$ (no necesariamente distintos) existe un único homomorfismo de anillos $\bar{f}: A[X_1,\dots,X_n]\to B$ tal que $\bar{f}\circ u = f$ y $\bar{f}(X_j) = b_j$ para cada $j=1,\dots,n$.*
2. *Si dos homomorfismos de anillos $g,h: A[X_1,\dots,X_n]\to B$ coinciden sobre A y en X_j para cada $j=1,\dots,n$ entonces son iguales.*
3. *La PUAP en n indeterminadas determina $A[X_1,\dots,X_n]$ salvo isomorfismos. Explícitamente: supongamos que existen un anillo P con elementos $T_1,\dots,T_n$ y un homomorfismo de anillos $v: A\to P$ tales que, dados un homomorfismo de anillos $f: A\to B$ y elementos $b_1,\dots,b_n\in B$, existe un único homomorfismo de anillos $\bar{f}: P\to B$ tal que $\bar{f}\circ v = f$ y $\bar{f}(T_j) = b_j$ para cada $j=1,\dots,n$. Entonces existe un isomorfismo $\phi: A[X_1,\dots,X_n]\to P$ tal que $\phi\circ u = v$ y $\phi(X_j) = T_j$ para cada $j=1,\dots,n$.*

Como en el caso de una indeterminada, se tiene:

Ejemplos 4.7.4 *Aplicaciones de la PUAP en n indeterminadas.*

1. Dados anillos $A\subseteq B$ y elementos $b_1,\dots,b_n\in B$, existe un homomorfismo $S: A[X_1,\dots,X_n]\to B$ que es la identidad sobre A y tal que $S(X_j) = b_j$ para cada $j=1,\dots,n$. Dado $p\in A[X_1,\dots,X_n]$, escribiremos a menudo $p(b_1,\dots,b_n)$ en lugar de $S(p)$. Si $p = \sum_{i\in\mathbb{N}^n} p_i X_1^{i_1}\cdots X_n^{i_n}$ es la expresión de p como suma de monomios, entonces
$$S(p) = p(b_1,\dots,b_n) = \sum_{i\in\mathbb{N}^n} p_i b_1^{i_1}\cdots b_n^{i_n}.$$
La imagen de este homomorfismo es el subanillo de B generado por $A\cup\{b_1,\dots,b_n\}$.
2. Sea A un anillo y sea σ una biyección del conjunto $\mathbb{N}_n = \{1,\dots,n\}$ en sí mismo con inversa $\tau = \sigma^{-1}$. Si en el ejemplo anterior tomamos $B = A[X_1,\dots,X_n]$ y $b_j = X_{\sigma(j)}$, obtenemos un homomorfismo $\bar{\sigma}: A[X_1,\dots,X_n]\to A[X_1,\dots,X_n]$ que "permuta las indeterminadas". Es claro que $\bar{\sigma}$ es de hecho un automorfismo con inverso $\bar{\tau}$. Usando estos isomorfismos y la definición de los anillos de polinomios en varias indeterminadas, es fácil establecer isomorfismos
$$A[X_1,\dots,X_n,Y_1,\dots,Y_m]\cong A[X_1,\dots,X_n][Y_1,\dots,Y_m]\cong A[Y_1,\dots,Y_m][X_1,\dots,X_n],$$
por lo que, en la práctica, no hay que distinguir entre estos anillos.
3. Todo homomorfismo de anillos $f: A\to B$ induce un homomorfismo $\bar{f}: A[X_1,\dots,X_n]\to B[X_1,\dots,X_n]$ que coincide con f sobre A y verifica $\bar{f}(X_j) = X_j$ para cada $j=1,\dots,n$. Si $p = \sum_{i\in\mathbb{N}^n} p_i X_1^{i_1}\cdots X_n^{i_n}$ es la expresión de p como suma de monomios, entonces
$$\bar{f}(p) = \sum_{i\in\mathbb{N}^n} f(p_i) X_1^{i_1}\cdots X_n^{i_n}.$$

Veamos cómo pueden usarse las identificaciones del apartado 2 de los Ejemplos 4.7.4.

Ejemplo 4.7.5 *El Criterio de Eisenstein aplicado a polinomios en dos indeterminadas*

El polinomio $f = X^3Y + X^2Y^2 - X^2 + Y^3 + Y^2\in\mathbb{Q}[X,Y]$ puede considerarse como un polinomio en $\mathbb{Q}[X][Y]$, poniendo $f = Y^3 + (X^2+1)Y^2 + X^3Y - X^2$, o como un polinomio en $\mathbb{Q}[Y][X]$, poniendo $f = YX^3 + (Y^2-1)X^2 + (Y^3+Y^2)$. A esta última expresión le podemos aplicar el Criterio de Eisenstein con el polinomio irreducible $p = Y+1\in\mathbb{Q}[Y]$ para deducir que f es irreducible en $\mathbb{Q}[X,Y]$.

Por definición, el *grado de un monomio* $aX_1^{i_1}\cdots X_n^{i_n}$ de $A[X_1,\dots,X_n]$ es $i_1+\cdots+i_n$. El grado $\mathrm{gr}(p)$ de un polinomio $p\neq 0$ de $A[X_1,\dots,X_n]$ se define como el mayor de los grados de los monomios que aparecen con coeficiente no nulo en la expresión de p como suma de monomios de distinto tipo. Es claro que, dados dos polinomios p y q, se tiene

$$\mathrm{gr}(p+q)\leq \max\{\mathrm{gr}(p),\mathrm{gr}(q)\} \qquad \text{y} \qquad \mathrm{gr}(pq)\leq \mathrm{gr}(p)+\mathrm{gr}(q).$$

Sin embargo, no es tan fácil como en el caso de una indeterminada ver que, cuando A es un dominio, la segunda desigualdad es de hecho una igualdad. Para esto, y para otras cosas, es interesante considerar el siguiente concepto:

Un polinomio $p\neq 0$ de $A[X_1,\dots,X_n]$ se dice *homogéneo de grado* $n\geq 0$ si es suma de monomios de grado n. Por ejemplo, de los polinomios de $\mathbb{Z}[X,Y,Z]$

$$X^2Y+Y^3-3XYZ+6YZ^2, \quad X^6+Y^6+Z^6+X^3Y^3+X^3Z^3+Y^3Z^3, \quad XYZ+X+Y+Z,$$

los dos primeros son homogéneos (de grados 3 y 6, respectivamente) y el último no lo es.

Proposición 4.7.6 *Dados un anillo A y un entero $n\geq 1$, todo polinomio de $A[X_1,\dots,X_n]$ se escribe de modo único como suma de polinomios homogéneos de distintos grados.*

Demostración. Si $p=\sum_{i\in\mathbb{N}^n} p_iX_1^{i_1}\cdots X_n^{i_n}$ es la expresión de p como suma de monomios y ponemos $h_j=\sum_{i_1+\cdots+i_n=j} p_iX_1^{i_1}\cdots X_n^{i_n}$, es claro que $p=h_0+h_1+\cdots+h_k$ (donde $k=\mathrm{gr}(p)$) es la expresión buscada. □

Corolario 4.7.7 *Si D es un dominio y $n\geq 1$, se tiene $\mathrm{gr}(pq)=\mathrm{gr}(p)+\mathrm{gr}(q)$ para cualesquiera $p,q\in D[X_1,\dots,X_n]$. Además, los grupos de unidades de $D[X_1,\dots,X_n]$ y de D coinciden; es decir, $D[X_1,\dots,X_n]^*=D^*$.*

Demostración. Dados polinomios p y q de grados n y m, sean $p=h_0+h_1+\cdots+h_n$ y $q=l_0+l_1+\cdots+l_m$ sus expresiones como suma de polinomios homogéneos. Entonces

$$pq=h_0l_0+(h_0l_1+h_1l_0)+\cdots+(h_{n-1}l_m+h_nl_{m-1})+h_nl_m$$

es la expresión de pq como suma de polinomios homogéneos. Como $D[X_1,\dots,X_n]$ es un dominio y $h_n\neq 0\neq l_m$, deducimos que $h_nl_m\neq 0$, lo que nos da la igualdad deseada. La última afirmación se demuestra ahora como en el caso de una indeterminada. □

Terminaremos haciendo algunos comentarios sobre las "raíces" de polinomios en varias indeterminadas, que no se suelen llamar raíces sino ceros. Para simplificar, consideraremos sólo polinomios de grado 2 con coeficientes en $\mathbb{R}$, y el lector podrá imaginar las generalizaciones pertinentes.

Un elemento $(a,b)\in\mathbb{R}^2$ es un *cero* del polinomio $f\in\mathbb{R}[X,Y]$ si $f(a,b)=0$. Denotaremos por $V(f)$ el conjunto de todos los ceros de f. Por ejemplo, $V(XY)$ consiste en los ejes de $\mathbb{R}^2$, y $V(X^2+Y^2-\rho^2)$ es la circunferencia de radio ρ centrada en el origen.

Estos ejemplos muestran que el grado de un polinomio en varias indeterminadas no acota en modo alguno el número de ceros del polinomio, lo que da a éstos una gran riqueza geométrica. En efecto, el "dibujo" de las raíces de un polinomio de $\mathbb{R}[X]$ es muy simple: son unos puntos aislados en la recta real. En $\mathbb{R}[X,Y]$ (y, por supuesto, en tres o más indeterminadas), los ejemplos anteriores son sólo una muestra de las curvas que pueden obtenerse como conjuntos de ceros de un polinomio. De hecho, es claro que $V(fg)=V(f)\cup V(g)$, y así $V(XY(X^2+Y^2-1))$ es la unión de los ejes con la circunferencia de radio 1 centrada en el origen. Por otra parte, se suele denotar por $V(f,g)$ la intersección de $V(f)$ con $V(g)$, de modo que

$$V(X-a,Y-b)=\{(a,b)\} \qquad \text{y} \qquad V(XY,X^2+Y^2-1)=\{(1,0),(-1,0),(0,1),(0,-1)\}.$$

Sobre $\mathbb{R}$ se tiene $V(f,g)=V(f^2+g^2)$, lo que permite construir polinomios con conjuntos finitos de ceros, como $(X-a)^2+(Y-b)^2$.

En general, la complejidad de $V(f)$ aumenta con el grado de f. El estudio de los conjuntos $V(f)$ con $\mathrm{gr}(f)=1$ (y de sus intersecciones) corresponde a la llamada *Geometría Afín*, y el caso de grados arbitrarios corresponde a la *Geometría Algebraica*.

4.8 Problemas

1. Sea A un anillo y sean $a, u \in A$. Demostrar que el homomorfismo $A[X] \to A[X]$ de sustitución en $uX + a$ es un automorfismo si y sólo si u es invertible en A.

2. Sea $P \in \mathbb{Z}_2[X]$. Demostrar que $X - 1$ divide a P precisamente si P tiene un número par de coeficientes no nulos.

3. Justificar la *regla de Ruffini* para el cálculo del cociente y el resto en la división de $p = p_0 + p_1X + \ldots + p_nX^n$ entre $X - a$. La regla está representada por la tabla

$$\begin{array}{c|cccccc} & p_n & p_{n-1} & p_{n-2} & \cdots & p_1 & p_0 \\ a & 0 & aq_{n-1} & aq_{n-2} & \ldots & aq_1 & aq_0 \\ \hline & q_{n-1} & q_{n-2} & q_{n-3} & \cdots & q_0 & r \end{array}$$

   en la que los q_i se obtienen, de izquierda a derecha, sumando los dos elementos que están encima. Entonces $q = q_0 + q_1X + \cdots + q_{n-1}X^{n-1}$ es el cociente de la división de p entre $X - a$, y r es su resto.

4. ¿Para qué cuerpos es válida la fórmula usual $(\frac{-b \pm \sqrt{b^2-4ac}}{2a})$ para el cálculo de las raíces de un polinomio $aX^2 + bX + c$ de grado 2?

5. Sea p un entero primo. Demostrar que los polinomios $X^p - X$ y $\prod_{i=1}^{p}(X - i)$ de $\mathbb{Z}_p[X]$ son iguales y deducir una nueva demostración del Teorema de Wilson: $(p-1)! \equiv -1 \bmod p$. (Indicación: Para la primera parte, considerar las raíces de ambos polinomios.)

6. Hemos observado que la Proposición 4.3.4 no se verifica para polinomios sobre un anillo que no sea un dominio. Comprobar que en este caso ni siquiera se verifica la afirmación sobre la finitud del número de raíces; es decir, dar un ejemplo de un polinomio no nulo en una indeterminada con infinitas raíces.

7. [*] Sea A un anillo. Demostrar que si $P \in A[X]$ es un divisor de cero en $A[X]$, entonces existe $0 \neq a \in A$ tal que $aP = 0$. (Indicación: Elegir un polinomio $Q \neq 0$ de grado mínimo entre los que satisfacen $PQ = 0$ y demostrar por inducción que $p_iQ = 0$, donde $p_0, p_1, \ldots, p_n$ son los coeficientes de P.)

8. Si K es un cuerpo de característica 0, ¿qué polinomios $P \in K[X]$ verifican $P' = 0$? ¿Y si la característica es un primo p?

9. Sea D un dominio y sea $P \in D[X]$ el polinomio

$$P = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$$

   ($n \in \mathbb{Z}^+$). Demostrar que la multiplicidad de 1 como raíz de P es al menos 3, y que es exactamente 3 si la característica de D es 0. (Advertencia: El caso de característica 2 ha de ser considerado aparte.)

10. Demostrar que si $0 \neq a \in K$, siendo K un cuerpo de característica 0, entonces $X^n - a$ no tiene raíces múltiples en ningún cuerpo que contenga a K como subcuerpo. ¿Qué se puede afirmar si K es un cuerpo de característica p, con p primo.

11. Dados dos polinomios $P, Q \in A[X]$, se define su *composición* $P(Q)$ de forma natural utilizando la PUAP. Demostrar que se satisface la *regla de la cadena* para la derivada de la composición: $(P(Q))' = P'(Q) \cdot Q'$.

12. Demostrar la fórmula de Leibnitz para el cálculo de las derivadas sucesivas de un producto de polinomios:

$$(PQ)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} P^{(n-i)}Q^{(i)}.$$

13. Sea K un cuerpo de característica 0 y sea $P = a_0 + a_1X + \cdots + a_nX^n \in K[X]$.

    (a) Demostrar que, para cada $i \geq 0$, se tiene $a_i = \frac{1}{i!}P^{(i)}(0)$.

    (b) Demostrar que, para todo $b \in K$, se verifica la *fórmula de Taylor*[3]

    $$P(X-b) = \sum_{i=0}^{n} \frac{P^{(i)}(b)}{i!}(X-b)^i.$$

    (c) Deducir del apartado anterior una demostración alternativa de la Proposición 4.3.8.

14. Sea K un cuerpo y sean $P_1, \ldots, P_r$ polinomios de $K[X]$. Demostrar que existe una extensión de cuerpos $K \to K'$ tal que cada P_i se descompone totalmente en $K'[X]$.

15. Sean K un cuerpo, $P \in K[X]$ un polinomio no constante y $K_1 = K[X]/(P)$. ¿Cuál es la dimensión de K_1 como espacio vectorial sobre K? Deducir que el cuerpo K' construido en el Corolario 4.4.4 tiene dimensión finita como espacio vectorial sobre K.

16. Sea K un cuerpo y sean $a_0, a_1, \ldots, a_n \in K$ distintos y $b_0, b_1, \ldots, b_n \in K$. Demostrar que

    $$P(X) = \sum_{r=0}^{n} b_r \prod_{i \neq r} \frac{(X-a_i)}{a_r - a_i}$$

    es el único polinomio de $K[X]$ de grado $\leq n$ que verifica $P(a_i) = b_i$ para todo i. La fórmula para P se conoce con el nombre de *fórmula de interpolación de Lagrange*.

17. Demostrar que, si K es un cuerpo, entonces $K[X]$ tiene infinitos elementos irreducibles. Deducir que:

    (a) Todo cuerpo algebraicamente cerrado es infinito.

    (b) Si K es finito, entonces en $K[X]$ existen polinomios irreducibles de grado arbitrariamente grande (es decir, para cada $n \in \mathbb{Z}^+$, existe un polinomio irreducible de grado mayor o igual que n).

18. [*] Sea K un subcuerpo de K', y sean $f, g \in K[X]$. Demostrar:

    (a) El máximo común divisor de f y g en $K[X]$ también es su máximo común divisor en $K'[X]$.

    (b) Si f es irreducible en $K[X]$ y en K' hay una raíz común de f y g, entonces $f \mid g$ en $K[X]$.

19. [*] Sea K un cuerpo, sea $f \in K[X]$. Demostrar que f tiene una raíz doble en alguna extensión de K si y sólo si f y su derivada f' no son coprimos en $K[X]$. (Indicación: Usar los Problemas 14 y 18.)

20. [*] Sea F un cuerpo y K un subcuerpo de F. Se dice que F es *algebraico* sobre K (o que F es una *extensión algebraica* de K) si todo elemento de F es la raíz de un polinomio no nulo de $K[X]$.

    (a) Demostrar que F es algebraico sobre K precisamente si F no contiene un subanillo isomorfo a $K[X]$.

    (b) Demostrar que si F no es algebraico sobre K, entonces F contiene un subcuerpo isomorfo al cuerpo de cocientes $K(X)$ de $K[X]$.

    (c) Demostrar que si F tiene dimensión finita como espacio vectorial sobre K, entonces F es algebraico sobre K.

21. ¿Es cierto que, si D es un DFU y b es un elemento de D, entonces sólo hay una cantidad finita de ideales de D que contienen a b?

[3] En el estudio de funciones reales de variable real, la fórmula de Taylor se usa para aproximar una función f por un polinomio en un entorno de un punto b. Este problema nos dice que, como es de esperar, si f es un polinomio entonces se obtiene una igualdad, y no sólo una aproximación de f.

22. Dar un ejemplo de un ideal primo no nulo de un DFU que no sea maximal.

23. Demostrar que toda raíz racional de un polinomio mónico con coeficientes enteros es entera.

24. Sea D un DFU y sea $f = a_o + a_1X + \cdots + a_nX^n$ un polinomio primitivo en $D[X]$. Demostrar que, si existe un irreducible $p \in D$ tal que

$$p \mid a_i \text{ para todo } i > 0, \qquad \text{y} \qquad p^2 \not\mid a_n,$$

entonces f es irreducible en $D[X]$ (es decir, el Criterio de Eisenstein se puede aplicar "al revés").

25. Descomponer en factores irreducibles el polinomio $X^4 - 4$ en cada uno de los siguientes anillos: $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{Z}_2[X]$ y $\mathbb{Z}_3[X]$.

26. Descomponer los siguientes anillos cociente como producto de anillos "conocidos":

    (a) $\mathbb{R}[X]$ módulo el ideal principal generado por el polinomio $X^3 - X^2 + X - 1$.

    (b) $\mathbb{Q}[X]$ módulo el ideal principal generado por el polinomio $X^3 - X^2 + X - 1$.

    (c) $\mathbb{Q}[X]$ módulo el ideal principal generado por el polinomio $3X^2 - 6$.

27. Calcular el máximo común divisor y el mínimo común múltiplo en $\mathbb{Z}[X]$ de las siguientes parejas de polinomios:

    (a) $X^3 - 6X^2 + X + 4$ y $X^5 - 6X + 1$.

    (b) $X^2 + 1$ y $X^6 + X^3 + X + 1$.

    (c) $26X^2 - 104X + 104$ y $195X^2 + 65X - 910$.

28. Demostrar que los siguientes polinomios son irreducibles en los anillos que se indican:

    (a) $X^4 + X + 1$, $4X^3 - 3X - \frac{1}{2}$, $X^4 + 1$, $X^6 + X^3 + 1$, $X^3 + 6X + 3X + 3$, $X^5 - 5X + 15$ y $X^4 + 5X + 12$ en $\mathbb{Q}[X]$.

    (b) $X^2 + X + 1$ en $\mathbb{Z}_2[X]$.

    (c) $X^2 + Y^2 - 1$ y $X^5Y^3 - X^3 + XY^2 - Y^2 + 1$ en $\mathbb{Q}[X, Y]$.

    (d) $X^4 + X + a$ con a impar, en $\mathbb{Q}[X]$.

    (e) $X^5 + 3aX^4 - 4X + 4$ con $a \in \mathbb{Z}$, en $\mathbb{Q}[X]$.

    (f) $Y^3 + X^2Y^2 + X^3Y + X$, en $D[X, Y]$ donde D es un DFU arbitrario.

29. Factorizar los siguientes polinomios en los anillos que se indican:

    (a) $3X^4 - 3X^2 + 6$, en $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

    (b) $X^3 + 3X^2 + 3X + 4$ en $\mathbb{Z}_5[X]$.

30. Decidir cuáles de los siguientes polinomios son irreducibles en los anillos que se indican:

    (a) $2X^2 + 2X + 2$ en $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_5[X]$.

    (b) $X^4 + 2$ en $\mathbb{Z}_7[X]$ y $\mathbb{Q}[X]$.

    (c) $X^3 - 18X^2 + 106X - 203$ en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$.

    (d) $X^5 + X + 2$ en $\mathbb{R}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_3[X]$.

    (e) $X^5 + X - 2$ en $\mathbb{R}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_3[X]$.

    (f) $2X^5 - 6X^3 + 9X^2 - 15$ en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$.

    (g) $X^4 + 15X^3 + 7$ en $\mathbb{Z}[X]$.

    (h) $X^n - p$, donde $n > 0$ y p es un entero primo con $p \equiv 1 \bmod 3$, en $\mathbb{R}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_3[X]$.

31. [*] El *método de Kronecker* para factorizar en $\mathbb{Z}[X]$ funciona como sigue: Dado $0 \neq f \in \mathbb{Z}[X]$, podemos limitarnos a buscar divisores g de f con $\mathrm{gr}(g) \leq m$, donde m es la parte entera de $\mathrm{gr}(f)/2$. Dado un tal g, para cada $a \in \mathbb{Z}$ se tiene $g(a) \mid f(a)$ en $\mathbb{Z}$. Si fijamos enteros $a_0, \ldots, a_m$ con $f(a_i) \neq 0$, los posibles valores de cada $g(a_i)$ quedan limitados por la condición $g(a_i) \mid f(a_i)$. Combinando esto con la fórmula de interpolación de Lagrange (Problema 16) obtenemos un número finito de candidatos a divisores de f. Si alguno está en $\mathbb{Z}[X]$ y divide a f, tenemos un primer paso en la factorización y repetimos el método. En caso contrario, f es ya irreducible.

    Un ejemplo: Si $f = X^4 + X + 1$, entonces $m = 2$ y podemos considerar los enteros $a_0 = -1$, $a_1 = 0$ y $a_2 = 1$. Entonces $g(-1) \mid 1$, $g(0) \mid 1$ y $g(1) \mid 3$, por lo que hay 8 posibilidades para g. Se pide: Calcular estos 8 polinomios, comprobar que ninguno divide a f en $\mathbb{Z}[X]$, y deducir que f es irreducible.

    Esto da idea de lo ineficaz que es el método si se emplea "a mano". Sin embargo, el método es fácil de programar, y es eficaz para polinomios "de grado no muy grande y con coeficientes no muy grandes". De hecho, el método funciona si sustituimos $\mathbb{Z}$ por un DFU infinito D (para poder elegir los a_i cuando m es grande) con D^* finito (para que cada $f(a_i)$ tenga un número finito de divisores) en el que haya un método para factorizar elementos.

32. [*] En el Problema 27 del Capítulo 2 se ha visto que el cardinal de un cuerpo finito K es una potencia de un número primo (de hecho, una potencia de la característica de K). En este problema, fijado un entero primo positivo p, vamos a ver que existen cuerpos[4] de cardinal p^n para cada $n \in \mathbb{Z}^+$.

    (a) Sea K un cuerpo de característica p (entero positivo primo), y sea $n \in \mathbb{Z}^+$. Demostrar que el conjunto de las raíces en K del polinomio $X^{p^n} - X$ es un subcuerpo finito de K. (Indicación: Usar el Problema 26 del Capítulo 2.)

    (b) Deducir que, para cada $n \in \mathbb{Z}^+$, existe un cuerpo de cardinal p^n.

33. [*] Construir cuerpos de 4, 8, 16, 9, 27 y 121 elementos.

34. Calcular todos los polinomios mónicos irreducibles de grado ≤ 4 en $K[X]$, cuando K es cada uno de los cuerpos $\mathbb{Z}_p$ con p primo menor o igual que 11. ¿Te atreves con los cuerpos K construidos en el Problema 33?

35. Sea A un anillo. Demostrar que si $P \in A[X_1, \ldots, X_n]$ tiene grado 1 y uno de los coeficiente es una unidad de A, entonces $A[X_1, \ldots, X_n]/(P) \cong A[X_1, \ldots, X_{n-1}]$.

36. [*] Sean K un cuerpo y $P = p_0 + p_1 X + \cdots + p_n X^n$ (con $p_n \neq 0$) un polinomio de $K[X]$. Se llama *homogeneizado* de P al polinomio de $K[X, Y]$

$$\widehat{P} = p_0 Y^n + p_1 X Y^{n-1} + \cdots + p_{n-1} X^{n-1} Y + p_n X^n.$$

    Demostrar:

    (a) Si $P \in K[X]$ entonces $\widehat{P}(X, 1) = P$.

    (b) Si $P, Q \in K[X]$ entonces $\widehat{PQ} = \widehat{P}\widehat{Q}$.

    (c) Si $R \in K[X, Y]$ es homogéneo de grado n y el coeficiente de X^n en R es diferente de 0, entonces $\widehat{R(X, 1)} = R$.

    (d) Si $R_1, R_2 \in K[X, Y]$ y $R_1 R_2$ es homogéneo, entonces R_1 y R_2 son homogéneos.

    (e) Si K es algebraicamente cerrado entonces todo polinomio homogéneo en $K[X, Y]$ es producto de polinomios homogéneos de grado 1.

    (f) Escribir $Y^3 - 3Y^2 X + 2X^3 \in \mathbb{Q}[X]$ como producto de polinomios homogéneos de grado 1.

[4] De hecho, salvo isomorfismos, existe un único cuerpo de cardinal q para cada entero positivo $q > 1$ que sea potencia de primo. La demostración de este hecho se verá en la asignatura de tercer curso *Ecuaciones Algebraicas*. Este único cuerpo de cardinal q se suele denotar por $\mathbb{F}_q$; en particular, para p primo, se tiene $\mathbb{F}_p = \mathbb{Z}_p$.

37. [*] Sea K un cuerpo y sea $P \in K[X,Y]$. Supongamos que el coeficiente principal de P, considerado como polinomio en $K[X][Y]$, no es divisible por $X-1$. Demostrar que, si $P(X,1)$ es irreducible en $K[X]$, entonces $P(X,Y)$ es irreducible en $K[X,Y]$.

38. [*] Demostrar que si K es un cuerpo y $P, Q \in K[X,Y]$ son coprimos, entonces el conjunto

$$V(P) \cap V(Q) = \{(a,b) \in K^2 : P(a,b) = Q(a,b) = 0\}$$

es finito. (Indicación: Aplicar el Lema de Bezout en el dominio euclídeo $K(X)[Y]$, donde $K(X)$ es el cuerpo de cocientes de $K[X]$.)

39. [*] En este problema se van a dar las claves para resolver las ecuaciones de tercer grado sobre un cuerpo K algebraicamente cerrado y de característica distinta de 2 y de 3 (en particular, sobre el cuerpo complejo $\mathbb{C}$). El lector deberá comprobar las afirmaciones que se hacen.

(a) Si $\alpha, \beta \in K$ son las raíces del polinomio $X^2 + aX + b \in K[X]$, entonces $\alpha + \beta = -a$ y $\alpha\beta = b$.

(b) Sea $\omega = \frac{-1+\sqrt{-3}}{2}$ una raíz en K del polinomio $X^2 + X + 1$. Entonces 1, ω y $\omega^2 = \frac{-1-\sqrt{-3}}{2}$ son las tres raíces del polinomio $X^3 - 1$; es decir, son las tres raíces cúbicas de la unidad. Si u es una raíz cúbica de $0 \neq a \in K$ (es decir, una raíz del polinomio $X^3 - a$), entonces $u\omega$ y $u\omega^2$ son las otras dos raíces cúbicas de a.

(c) Para resolver una ecuación polinómica podemos suponer, si perder generalidad, que el polinomio es mónico. Sustituyendo X por $X - a$, para un $a \in K$ apropiado, una ecuación de tercer grado se convierte en una de la forma

$$X^3 - qX - r = 0, \tag{4.8.2}$$

y si β es una solución de (4.8.2) entonces $\alpha = \beta - a$ es una solución de la ecuación original. Por tanto podemos limitarnos a resolver (4.8.2), y como esto es trivial cuando $r = 0$ o cuando $q = 0$, supondremos que $r, q \neq 0$.

(d) Sustituyendo X por $u + v$ e imponiendo la condición $3uv + q = 0$, se obtiene la ecuación *bicúbica* (es decir, cuadrática en u^3)

$$u^6 - ru^3 - \frac{q^3}{27} = 0, \tag{4.8.3}$$

llamada *resolvente* de la ecuación (4.8.2).

(e) Una solución de (4.8.3) viene dada por una raíz cúbica u de $(r/2) + \sqrt{(r^2/4) + (q^3/27)}$. Entonces $v = -q/(3u)$ es una raíz cúbica de $(r/2) - \sqrt{(r^2/4) + (q^3/27)}$, y por tanto u, $u\omega$, $u\omega^2$, v, $v\omega$ y $v\omega^2$ son las seis soluciones de la resolvente.

(f) Las tres soluciones de (4.8.2) son entonces $u + v$, $u\omega + v\omega^2$ y $u\omega^2 + v\omega$.

(g) Se obtiene así la *fórmula de Cardano* para las soluciones de (4.8.2):

$$\sqrt[3]{\frac{r}{2} + \sqrt{\frac{r^2}{4} + \frac{q^3}{27}}} + \sqrt[3]{\frac{r}{2} - \sqrt{\frac{r^2}{4} + \frac{q^3}{27}}},$$

donde las dos raíces cúbicas han de ser tales que su producto sea $-q/3$.

(h) Como aplicación, pueden calcularse las raíces complejas de los polinomios

$$X^3 - X^2 - X + 2, \qquad X^3 + X^2 + 2X + 5, \qquad X^6 + X^2 + 3.$$

Bibliografía del capítulo

Allenby [1], Clark [9], Delgado-Fuertes-Xambó [11] y [12], Hungerford [22], Jacobson [23].

Capítulo 5

Grupos

Se estudia la estructura de grupo y se presentan sus ejemplos y propiedades básicas.

Introducción

Un grupo es un conjunto con una operación asociativa y con elemento neutro para la que todo elemento tiene un simétrico (inverso). Esta estructura es, en principio, más sencilla que la de anillo. Sin embargo, no se asume la conmutatividad de la operación, y esto la convierte en una estructura de naturaleza muy distinta cuando se opera formalmente y cuando se manejan ejemplos. Comenzamos el capítulo presentando las propiedades elementales de la operación en un grupo y mostrando diversos ejemplos que ponen de manifiesto que la noción de grupo aparece de modo natural en muy diversas situaciones. Particularmente importantes serán los grupos simétricos y los grupos diédricos.

A continuación recorremos un camino similar al que seguimos al estudiar la estructura de anillo: Para un grupo G, describiremos los subconjuntos que, con la misma operación, siguen siendo grupos (subgrupos), y consideraremos las relaciones de equivalencia en G que son compatibles con su operación, lo que dará lugar a los conceptos de subgrupo normal y de grupo cociente. También estudiaremos los homomorfismos de grupos, hasta interpretar los grupos isomorfos como grupos "esencialmente iguales".

En el camino aparecerán otras nociones específicas del estudio de los grupos, acompañadas de resultados que serán fundamentales: las clases laterales (y el Teorema de Lagrange), el orden de un elemento (y la caracterización de los grupos cíclicos) y la conjugación (y la Ecuación de Clases). Todas ellas son especialmente útiles cuando el grupo considerado es finito, pues permiten obtener información usando sólo el cardinal del grupo y de algunos de sus subgrupos. De hecho, con la información básica de este capítulo, describiremos los grupos finitos con un número primo de elementos, y plantearemos cuestiones sobre la descripción de otros grupos finitos de cardinal pequeño que iremos resolviendo en los próximos capítulos.

Objetivos del capítulo

- Conocer la definición de grupo y sus principales ejemplos, y dominar su aritmética.
- Conocer el concepto de subgrupo y los criterios para determinar cuándo un subconjunto es subgrupo.
- Saber identificar el subgrupo generado por un subconjunto, y saber encontrar y manejar sistemas generadores de subgrupos.
- Conocer los conceptos de clase lateral e índice, y el Teorema de Lagrange.
- Conocer el concepto de subgrupo normal N de un grupo G, y los criterios para decidir si un subgrupo es normal. Manejar la operación del grupo cociente G/N y la relación entre los subgrupos de G y los de G/N (Teorema de la Correspondencia).

- Conocer las propiedades básicas de los homomorfismos de grupos, las nociones de núcleo e imagen y los Teoremas de Isomorfía.
- Conocer la definición de orden de un elemento, sus distintas interpretaciones y sus propiedades elementales. Saber determinar el orden de un elemento en ejemplos concretos.
- Conocer la clasificación de los grupos cíclicos y el hecho de que verifican el "recíproco del Teorema de Lagrange".
- Conocer el concepto de elementos conjugados, la relación entre la clase de conjugación de un elemento a y el centralizador de a, y la Ecuación de Clases.

Desarrollo de los contenidos

5.1 Grupos

En el Capítulo 2 hemos visto la noción de grupo abeliano. En muchas ocasiones hay que considerar estructuras que cumplen todas las propiedades de un grupo abeliano excepto la conmutatividad de la operación; son los grupos:

Definición 5.1.1 *Un* grupo *es un par*[1] $(G, *)$ *formado por un conjunto* G *con una operación* $*$ *que:*

- *Es asociativa: para cualesquiera* $x, y, z \in G$*, se verifica* $(x * y) * z = x * (y * z)$*.*
- *Tiene elemento neutro: existe* $e \in G$ *tal que, para todo* $x \in G$*, se verifica* $x * e = x = e * x$*.*
- *Todo elemento* x *de* G *tiene un elemento simétrico: existe* $y \in G$ *tal que* $x * y = e = y * x$*.*

Si la operación es además conmutativa tenemos la definición de grupo abeliano. En los capítulos precedentes hemos visto numerosos grupos abelianos; por ejemplo, si $(A, +, \cdot)$ es un anillo entonces $(A, +)$ es un grupo abeliano y $(A^*, \cdot)$ también lo es. Si el anillo no es conmutativo entonces $(A^*, \cdot)$ es un grupo que en general no es abeliano: por ejemplo, no lo es si $A = M_n(\mathbb{R})$ y $n > 1$ (en cuyo caso A^* está formado por las matrices con determinante no nulo). Vamos a posponer la presentación de los principales ejemplos de grupos hasta la sección siguiente, y dedicaremos ésta a establecer algunas generalidades sobre el concepto.

Como vimos en la Sección 2.2, las condiciones de la definición de grupo tienen algunas consecuencias inmediatas:

- La asociatividad garantiza una asociatividad generalizada que permite considerar la acción de la operación $*$ en un conjunto finito $x_1, \ldots, x_n$ de elementos de G y escribir sin ambigüedad $x_1 * \cdots * x_n$.
- El elemento neutro es único.
- El elemento simétrico de cada elemento es único.
- Todo elemento es cancelable por la derecha y por la izquierda: si $x * y = x * z$ ó $y * x = z * x$ entonces $y = z$.

En la mayoría de las ocasiones usaremos la *notación multiplicativa* para un grupo G. Denotaremos la operación por $\cdot$ (y escribiremos ab en vez de $a \cdot b$), el neutro por 1 y el simétrico de x por x^{-1} (y le llamaremos el *inverso* de x). La notación x^n (con $x \in G$ y $n \in \mathbb{Z}$) tendrá el significado habitual: $x^0 = 1$, si $n > 0$ entonces x^n representa el resultado de operar x consigo mismo n veces, y si $n < 0$ entonces $x^n = (x^{-1})^{|n|}$. Así, cuando digamos "G es un grupo" asumiremos que su operación es $\cdot$ y que su neutro es 1.

Por lo general, reservaremos la *notación aditiva* para grupos abelianos: en este contexto denotaremos la operación (conmutativa) por $+$, el neutro por 0 y el simétrico de x por $-x$ (y le llamaremos el *opuesto* de x). En este caso, la notación x^n se sustituye por nx.

Algunas propiedades elementales de la operación en un grupo están vistas en la Sección 2.2, pero no está de más reenunciarlas aquí.

[1] Cuando no existe riesgo de confusión con la operación diremos simplemente que G es un grupo.

Ejercicio 5.1.2 *Si G es un grupo y $e, x, y, x_1, \ldots, x_r \in G$, demostrar:*

1. *Si $e \in G$ verifica $ex = x$ para cada $x \in G$ entonces $e = 1$. Es decir, un* neutro por la izquierda *es ya el neutro de G.*
2. *Si $x, y \in G$ verifican $xy = 1$ entonces se tiene también $yx = 1$ y por tanto $y = x^{-1}$. Es decir, un* inverso por la izquierda *de x es ya el inverso de x.*
3. *$(x^{-1})^{-1} = x$.*
4. *$(xy)^{-1} = y^{-1}x^{-1}$; más generalmente $(x_1 \cdots x_r)^{-1} = x_r^{-1} \cdots x_1^{-1}$ (en general no se tiene necesariamente $(xy)^{-1} = x^{-1}y^{-1}$).*
5. *Si $n, m \in \mathbb{Z}$ entonces $x^{n+m} = x^n x^m$ y $(x^n)^m = x^{nm}$.*
6. *La igualdad $(xy)^2 = x^2y^2$ se verifica si y sólo si $xy = yx$ (decimos en este caso que x e y* conmutan*).*
7. *Si todos los elementos de G verifican $x^2 = 1$ entonces G es abeliano.*

El siguiente resultado nos ahorrará trabajo a la hora de verificar que ciertos ejemplos que se nos presentarán son grupos.

Lema 5.1.3 *Sea G un conjunto con una operación asociativa $(\cdot)$ y un elemento $e \in G$ tales que:*

1. *e es un neutro por la derecha; es decir, $xe = x$ para cada $x \in G$.*
2. *Existen inversos por la derecha; es decir, para cada $x \in G$ existe $\hat{x} \in G$ tal que $x\hat{x} = e$.*

Entonces $(G, \cdot)$ es un grupo.

Demostración. Observamos primero que hay "cancelación por la derecha": Si $ax = bx$ entonces $a = b$, pues

$$a = ae = a(x\hat{x}) = (ax)\hat{x} = (bx)\hat{x} = b(x\hat{x}) = be = b.$$

Ahora, para cualquier x, se tiene

$$(ex)\hat{x} = e(x\hat{x}) = ee = e = x\hat{x},$$

y cancelando $\hat{x}$ deducimos que $ex = x$, de modo que e es un elemento neutro para la operación. Por último, $\hat{x}$ también verifica $\hat{x}x = e$, como se ve cancelando en

$$(\hat{x}x)\hat{x} = \hat{x}(x\hat{x}) = \hat{x}e = \hat{x} = e\hat{x}.$$

□

Proposición 5.1.4 *Sea G un conjunto no vacío con una operación asociativa $(\cdot)$. Entonces las siguientes condiciones son equivalentes:*

1. *$(G, \cdot)$ es un grupo.*
2. *Dados $a, b \in G$, cada una de las ecuaciones $aX = b$ e $Ya = b$ tiene una única solución en G.*

Demostración. 1 implica 2. Es claro que $X = a^{-1}b$ e $Y = ba^{-1}$ son soluciones de las ecuaciones dadas, y son las únicas porque podemos cancelar.

2 implica 1. Como G no es vacío existe $a \in G$. Si denotamos por $e \in G$ a la única solución de la ecuación $aX = a$, entonces e es un neutro por la derecha, pues dado $b \in G$ la ecuación $Ya = b$ tiene una solución única $Y = y$; es decir, $ya = b$, de donde

$$be = (ya)e = y(ae) = ya = b.$$

El hecho de que toda ecuación de la forma $aX = e$ tenga solución significa que todo elemento de G tiene inverso por la derecha, y entonces el resultado es consecuencia del Lema 5.1.3. □

Aunque más tarde desarrollaremos con detalle la noción de homomorfismo de grupos, damos aquí la definición con el objetivo de poder manejar ya el concepto de isomorfismo de grupos.

Definición 5.1.5 *Sean $(G,\cdot)$ y $(H,*)$ dos grupos. Un* homomorfismo de grupos *entre G y H es una aplicación $f: G \to H$ que conserva las operaciones; es decir, tal que*

$$f(a \cdot b) = f(a) * f(b)$$

para cualesquiera $a, b \in G$. Si f es un homomorfismo biyectivo, decimos que es un isomorfismo *de grupos, y que G y H son* isomorfos. *Las nociones de endomorfismo y automorfismo se definen como en el caso de anillos.*

Ejercicio 5.1.6 *Demostrar que, si $f: G \to H$ es un isomorfismo de grupos, entonces la aplicación inversa $f^{-1}: H \to G$ es también un isomorfismo de grupos.*

Como ocurrió con los isomorfismos de anillos, si existe un isomorfismo entre dos grupos éstos pueden considerarse como básicamente iguales.

Ejercicio 5.1.7

1. *Demostrar que, si $\{1, a\}$ es un grupo (con neutro 1), entonces su operación viene forzosamente dada por $a^2 = 1$ (en el resto de productos aparece el neutro y, en consecuencia, no es necesario describirlos). En particular, el grupo es abeliano.*

2. *Demostrar que, si $G = \{1_G, g\}$ y $H = \{1_H, h\}$ son grupos (con neutros 1_G y 1_H), entonces la aplicación $f: G \to H$ dada por $1_G \mapsto 1_H$ y $g \mapsto h$ es un isomorfismo de grupos. Es decir, cualesquiera dos grupos con dos elementos son isomorfos. Se dice que "salvo isomorfismos, sólo hay un grupo con dos elementos". Como $\mathbb{Z}_2$ es uno de ellos (en notación aditiva la condición $a^2 = 1$ se traduce en $a + a = 0$), deducimos que, salvo isomorfismos, $\mathbb{Z}_2$ es el único grupo con dos elementos.*

3. *Demostrar que, si $\{1, a, b\}$ es un grupo con neutro 1, entonces su operación viene dada por $a^2 = b$, $ab = ba = 1$, $b^2 = a$. En particular, el grupo es abeliano.*

4. *Demostrar que, si $G = \{1_G, g, g'\}$ y $H = \{1_H, h, h'\}$ son grupos con neutros 1_G y 1_H, entonces la aplicación $f: G \to H$ dada por $1_G \mapsto 1_H$, $g \mapsto h$ y $g' \mapsto h'$ es un isomorfismo de grupos (¿hay algún otro isomorfismo entre G y H?). Deducir que, salvo isomorfismos, $\mathbb{Z}_3$ es el único grupo con tres elementos.*

5.2 Ejemplos

Como hemos comentado después de la Definición 5.1.1, ya contamos con numerosos ejemplos de grupos abelianos provenientes de anillos. Por ejemplo, los grupos aditivos $(\mathbb{Z},+)$, $(\mathbb{Z}_n,+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, y los grupos multiplicativos $(\mathbb{Z}_n^*,\cdot)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$. Por brevedad, a partir de ahora $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$... denotarán los correspondientes grupos aditivos, y $\mathbb{Z}^*$, $\mathbb{Z}_n^*$, $\mathbb{Q}^*$... denotarán los correspondientes grupos multiplicativos. Los vectores de un espacio vectorial con la suma proporcionan otro ejemplo de grupo. En esta sección presentaremos ejemplos de grupos no abelianos, pero antes observemos que hay una manera fácil de obtener grupos nuevos a partir de otros, lo que multiplicará el número de ejemplos a nuestra disposición.

Ejemplo 5.2.1 *Producto directo de grupos.*
Si $(G,*)$ y $(H,\star)$ son grupos entonces $(G \times H,\cdot)$ es un grupo, donde la operación $\cdot$ está definida componente a componente a partir de $*$ y $\star$; es decir,

$$(g,h)\cdot(g',h') = (g * g', h \star h').$$

Este grupo $G \times H$ se llama el *producto directo* de los grupos G y H, y es abeliano si y sólo si lo son G y H. Su neutro es $(1_G, 1_H)$, donde 1_G y 1_H son los neutros de G y de H, y el inverso de (g,h) es (g^{-1}, h^{-1}).

La construcción anterior se generaliza al producto cartesiano de cualquier familia de grupos, finita o infinita. El producto de una familia de grupos $\{G_i : i \in I\}$ se denota $\prod_{i\in I} G_i$ y si $I = \mathbb{N}_n$ es finito, entonces se denota $G_1 \times G_2 \times \cdots \times G_n$.

El ejemplo más clásico de grupo no abeliano es el siguiente:

Definición 5.2.2 *Sea A un conjunto no vacío. Llamamos* permutación *o* sustitución *de A a cualquier aplicación biyectiva $f : A \to A$, y denotamos el conjunto de todas las permutaciones de A por $S(A)$. Cuando $A = \mathbb{N}_k = \{1, 2, \ldots, k\}$ (o, más generalmente, cuando A es un conjunto finito con k elementos) escribimos S_k en lugar de $S(A)$.*

La composición de aplicaciones es una operación en el conjunto $S(A)$ que lo dota de estructura de grupo: la composición siempre es asociativa, el elemento neutro es la aplicación identidad, y el inverso de una aplicación es su aplicación inversa en el sentido usual. Llamamos a este grupo el grupo simétrico *sobre A; a S_k se le suele llamar el* grupo simétrico *en k elementos.*

Si A sólo tiene 1 elemento entonces $S(A)$ se reduce a la aplicación identidad y por tanto es el grupo trivial (en el sentido de los Ejemplos 2.2.2). Si A sólo tiene 2 elementos, $A = \{x, y\}$, entonces $S(A)$ consiste en la identidad y en la aplicación que intercambia x con y, y es claramente un grupo abeliano isomorfo a $\mathbb{Z}_2$. Si A contiene al menos tres elementos distintos x, y, z entonces $S(A)$ no es abeliano: sea $f \in S(A)$ la permutación que intercambia x con y y deja fijos al resto de elementos, y sea $g \in S(A)$ la permutación que intercambia x con z y deja fijos al resto de elementos. Entonces $f(g(x)) = f(z) = z$ y $g(f(x)) = g(y) = y$, y por lo tanto $f \circ g \neq g \circ f$.

Ejercicio 5.2.3 *Si X e Y son conjuntos entre los que existe una biyección, demostrar que los grupos de permutaciones $S(X)$ y $S(Y)$ son isomorfos.*

Ejercicio 5.2.4 *Demostrar que S_n tiene $n!$ elementos.*

Ejemplo 5.2.5 *El grupo simétrico sobre tres elementos: S_3.*

Por el Ejercicio 5.2.4, S_3 tiene 6 elementos. Denotemos por e a la permutación identidad, por τ a la que intercambia 1 con 2 y fija 3, y por σ la permutación circular que lleva cada elemento al siguiente, y el último al primero.

Daremos la lista de los elementos de S_3 escribiendo cada aplicación biyectiva $f : \mathbb{N}_3 \to \mathbb{N}_3$ en la forma siguiente:

$$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}.$$

Con esta escritura, los 6 elementos de S_3 son los siguientes (recuérdese que, al componer dos aplicaciones, la que actúa en primer lugar se escribe a la derecha):

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Haciendo los cálculos directos, que se simplifican usando adecuadamente la igualdad $\tau\sigma = \sigma^2\tau$, podemos construir una "tabla de multiplicar" para el grupo S_3:

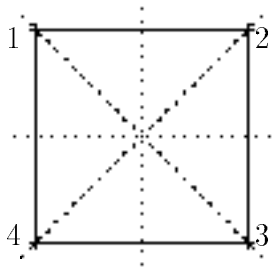
$\circ$	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	e	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	e	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	e	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	e

Obsérvese que, en cada fila y en cada columna de la tabla, cada elemento del grupo aparece exactamente una vez. Esto es un hecho cierto en la tabla de cualquier grupo, ¿por qué?

Ejercicio 5.2.6 *Escribir las tablas de los grupos $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$, y deducir que no son isomorfos. El segundo de ellos se conoce como el* grupo de Klein.

Ejemplo 5.2.7 *Los giros y simetrías del cuadrado: el grupo diédrico D_4.*

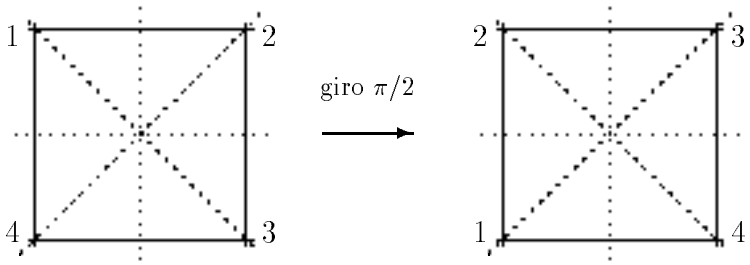
Imaginemos un cuadrado de vértices 1, 2, 3 y 4. Podemos suponer que el cuadrado está centrado en el origen de un sistema de referencia cartesiano del plano real.



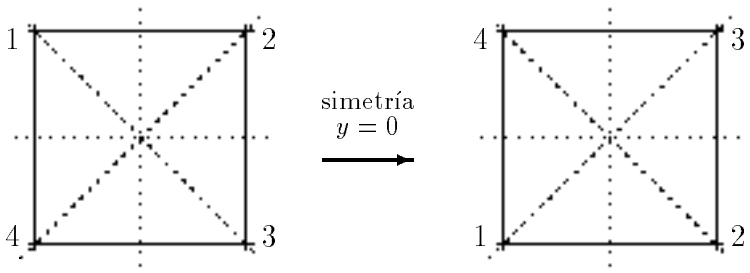
Consideremos ahora, en el plano, los giros (en sentido antihorario) alrededor de un punto y las simetrías respecto de rectas que llevan el cuadrado sobre sí mismo: por ejemplo, si r es un giro de ángulo $\pi/2$ (en radianes) alrededor del origen, entonces el cuadrado se transforma en un cuadrado en la misma posición, aunque el vértice 1 se haya movido hasta ocupar el punto donde antes estaba el 4, etc. Tales giros y simetrías son exactamente ocho:

- El giro de ángulo 0, que deja fijo cada punto del cuadrado. Lo denotaremos por e.

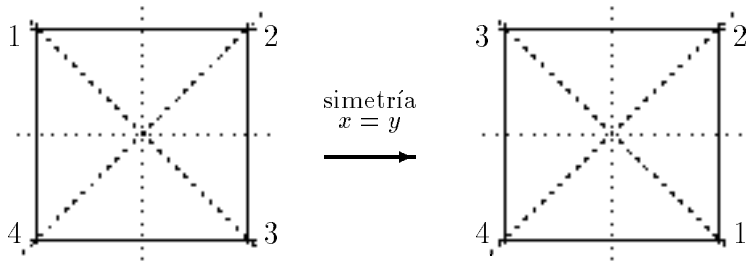
- Los giros de ángulos $\pi/2$, π y $3\pi/2$.



- Las simetrías con respecto a los ejes horizontal ($y = 0$) y vertical ($x = 0$).



- Las simetrías con respecto a las dos diagonales del cuadrado (rectas $x = y$ ó $x = -y$): estas dejan dos vértices opuestos fijos e intercambian los otros dos.



Llamemos D_4 a este conjunto. Vamos a dotarlo de una estructura de grupo cuya operación será la composición de movimientos; esto es, dados dos movimientos α y β en D_4, escribiremos $\alpha\beta$ para designar al movimiento que resulta cuando aplicamos primero β y después α. Esta operación es asociativa, pues podemos interpretarla como una composición de aplicaciones. Para ver que D_4 es un grupo, antes de nada hemos de ver que la operación es interna, lo que conseguimos calculando directamente la tabla.

Claramente, e es el neutro de la operación. Como en el Ejemplo 5.2.5, vamos a destacar dos elementos r y s a partir de los cuales podremos describir el resto. El elemento r será el giro de ángulo $\pi/2$, y el elemento s será la simetría de eje $x = y$.

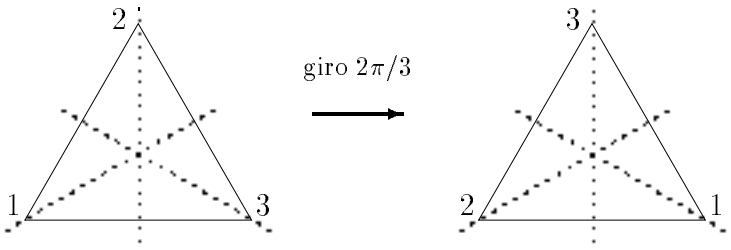
Está claro que r^2 es el giro de ángulo π, que r^3 el de ángulo $3\pi/2$, y que $r^4 = e$. Además, rs es la simetría respecto del eje vertical $x = 0$, r^2s es la simetría respecto del eje $y = -x$, y r^3s es la simetría respecto del eje horizontal $y = 0$. Como en el Ejemplo 5.2.5, la igualdad $sr = r^3s$ (que se comprueba fácilmente) resulta útil para construir la tabla:

$\cdot$	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	e	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	e	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	e

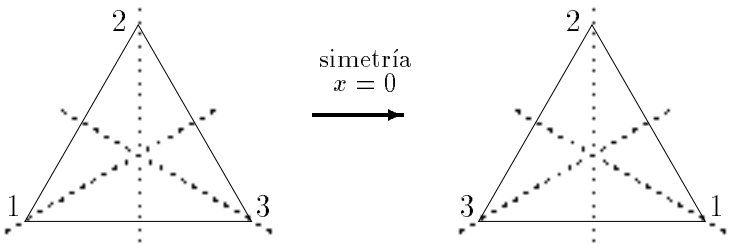
Completada la tabla, vemos que la operación es interna y que cada elemento tiene un inverso, por lo que D_4 es un grupo.

Ejemplo 5.2.8 *Los giros y simetrías del triángulo equilátero: el grupo diédrico D_3.*

Veamos un ejemplo análogo al anterior, referido ahora al triángulo equilátero. Denotaremos por D_3 al siguiente conjunto de movimientos que dejan invariante el triángulo equilátero: la identidad e, los giros centrados en el centro del triángulo de ángulos $2\pi/3$ y $4\pi/3$:



y las simetrías con respecto a las tres bisectrices de los ángulos:



Como en el ejemplo anterior, consideraremos como operación en D_3 la composición de movimientos, que es asociativa y tiene a e por elemento neutro. Si r denota el giro de ángulo $2\pi/3$ y s denota la simetría de eje vertical, es claro que r^2 es el giro de ángulo $4\pi/3$ y que $r^3 = e$, y es fácil verificar que rs y r^2s son las simetría con respecto a las bisectrices que pasan por 3 y por 1, respectivamente. Observando además que $sr = r^2s$, se puede construir la tabla de la operación:

$\cdot$	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

En particular, la operación es interna y todo elemento tiene un inverso, por lo que D_3 es un grupo.

Aunque los grupos S_3 y D_3 se han construido de manera distinta, desde el punto de vista de la Teoría de Grupos son esencialmente iguales, como podrá comprobar el lector resolviendo el siguiente ejercicio.

Ejercicio 5.2.9 *Describir un isomorfismo entre S_3 y D_3.*

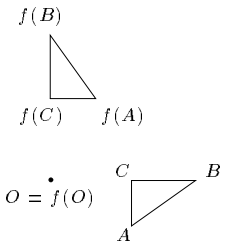
En vista de los dos ejemplos anteriores, es natural preguntarse si, en general, el conjunto D_n de los giros y simetrías de un n-ágono regular es un grupo con la composición. Si tratamos de desarrollar este caso general como los anteriores, nos encontramos con el problema de demostrar que la composición es una operación interna en D_n. Esto lo hemos resuelto, para D_3 y D_4, dando explícitamente la tabla del grupo, pero este método no es razonable en el caso general. Para resolver este problema vamos a dar una descripción alternativa de D_n, que además hará aparecer de modo natural el concepto de subgrupo, al que dedicaremos la próxima sección.

Ejemplo 5.2.10 *Isometrías del plano.*
Una *isometría* del plano euclídeo $\mathbb{R}^2$ es una biyección $f : \mathbb{R}^2 \to \mathbb{R}^2$ que conserva la distancia, es decir

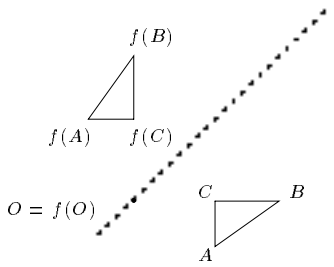
$$d(x, y) = d(f(x), f(y))$$

para todo $x, y \in \mathbb{R}^2$. Claramente la composición de dos isometrías es una isometría y la inversa de una isometría es una isometría, por tanto el conjunto $\mathrm{Isom}(\mathbb{R}^2)$ de las isometrías del plano es un grupo.

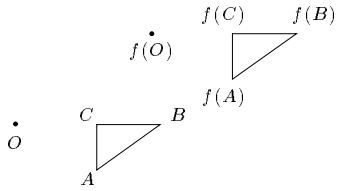
Ejemplos de isometrías son los giros alrededor de puntos,



las reflexiones respecto de rectas,



y las traslaciones.



Si fijamos un punto O de $\mathbb{R}^2$, entonces las isometrías que dejan fijo el punto O forman también un grupo. Un resultado que se verá en Álgebra Lineal y Geometría Euclídea asegura que las isometrías que dejan fijo el punto O son precisamente los giros alrededor de O y las reflexiones respecto de rectas que pasan por O.

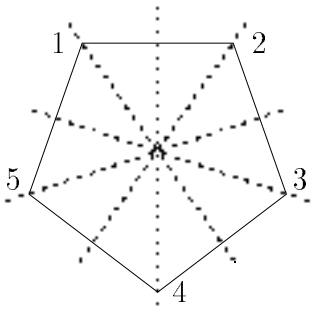
Ejemplo 5.2.11 *Las isometrías de un n-ágono regular: el grupo diédrico D_n.*

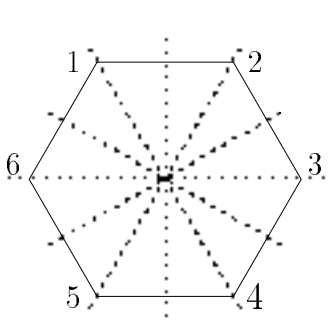
Sea $V = \{v_1, v_2, \ldots, v_n\}$ el conjunto de los vértices de un n-ágono regular P del plano real ($n \geq 3$). Denotamos por O el centro de P, y suponemos que los vértices están ordenados en sentido horario. Llamamos D_n al conjunto de las isometrías del plano que dejan invariante el polígono regular P globalmente (aunque no necesariamente punto a punto). Como la composición de isometrías que dejen P invariante y el inverso de una de ellas tienen la misma propiedad, D_n es un grupo, que llamamos el n-ésimo *grupo diédrico*. Claramente el centro O de P es invariante por todos los elementos de D_n y por tanto los elementos de D_n son o giros alrededor de O o reflexiones a través de rectas que pasan por O.

Claramente los únicos giros alrededor de O que dejan fijo el polígono son los de ángulos que sean múltiplos enteros de $2\pi/n$. Por otro lado las rectas de simetría pueden ser de tres tipos: Si n es impar cada recta de simetría pasa por un vértice y el punto medio del lado opuesto. Si n es par, entonces hay dos tipos de rectas de simetría unas pasan por dos vértices opuestos y las otras pasan por los puntos medios de lados opuestos. En cualquier caso D_n está formado por

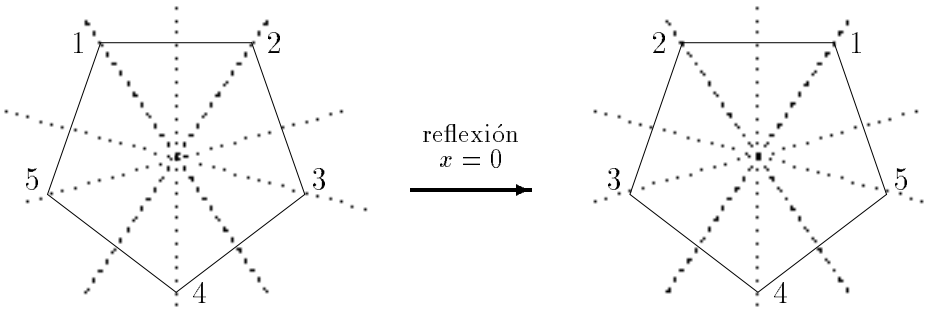
- Las rotaciones (o giros) en torno al centro O de ángulos $k\frac{2\pi}{n}$, con $k = 0, 1, \ldots, n-1$. Para $k = 0$ obtenemos la aplicación identidad e, y en general el inverso de la rotación de ángulo $k\frac{2\pi}{n}$ es la rotación de ángulo $(n-k)\frac{2\pi}{n}$.

- Las reflexiones respecto de rectas que pasan por O y llevan a V sobre sí mismo. Es claro que cada reflexión es su propia inversa. Siempre hay exactamente n ejes de simetría. Si n es impar, cada uno va de un vértice al punto medio del lado opuesto; y si n es par hay $n/2$ ejes que unen vértices opuestos, y otros $n/2$ ejes que unen puntos medios de lados opuestos. Para los casos $n = 5$ y $n = 6$, se tienen las siguientes rectas de simetría:

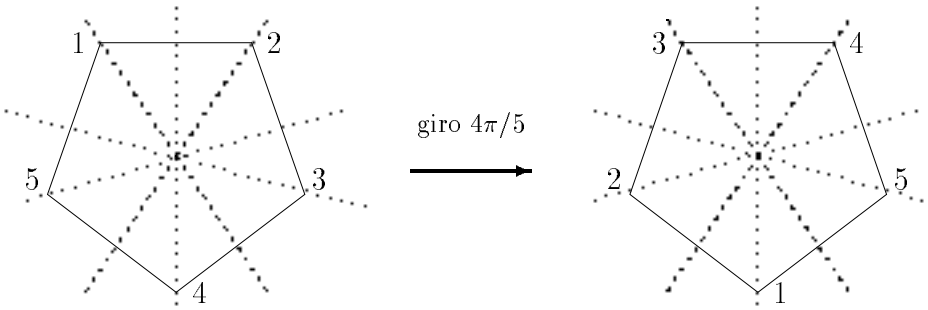




Es claro que las n rotaciones son elementos distintos de D_n, y también es claro que las n reflexiones son distintas entre sí. Además, una reflexión nunca puede ser una rotación, pues las primeras invierten el orden de los vértices (de antihorario a horario y viceversa), por ejemplo:



mientras que las segundas lo conservan:



Consideremos ahora en D_n los siguientes elementos: R es la rotación de ángulo $2\pi/n$, y S es una reflexión, arbitraria pero fija. Es claro que $R^n = e$, que $S^2 = e$ y que $R^0 = e, R, R^2, \ldots, R^{n-1}$ son las n distintas rotaciones de D_n. Por otra parte, los elementos $S, RS, R^2S, \ldots, R^{n-1}S$ son distintos entre sí (podemos cancelar S) y son reflexiones (invierten el orden de los vértices), de modo que

$$D_n = \{e, R, R^2, \ldots, R^{n-1}, S, RS, R^2S, \ldots, R^{n-1}S\}.$$

Como R^kS es una reflexión, se tiene $e = (R^kS)^2 = R^k(SR^kS)$, por lo que $SR^kS = (R^k)^{-1} = R^{n-k}$; multiplicando a la derecha por S obtenemos $SR^k = R^{n-k}S$, y en particular $SR = R^{-1}S$. Usando adecuadamente las relaciones

$$R^n = e, \qquad S^2 = e \qquad \text{y} \qquad SR^k = R^{n-k}S,$$

podemos expresar cualquier producto de elementos de D_n en la forma R^k ó R^kS con $k \in \{0, 1, \ldots, n-1\}$. Por ejemplo, en D_7 se tiene

$$(R^5S)R^3 = R^5SR^3 = R^5R^4S = R^9S = R^2S$$

ó

$$(R^3S)(R^2S) = R^3(SR^2)S = R^3(R^5S)S = R^8S^2 = R.$$

Dejamos como ejercicio para el lector la comprobación de que, usando sólo las relaciones $R^n = e = S^2$ y $SR = R^{-1}S$ y el hecho de que D_n es un grupo, es posible deducir que

$$D_n = \{e, R, R^2, \ldots, R^{n-1}, S, RS, R^2S, \ldots, R^{n-1}S\}$$

y que $SR^k = R^{n-k}S$ para cada $k \in \mathbb{N}_n$. Como acabamos de ver, esto identifica totalmente al grupo; es decir, al conjunto y a su operación. Este hecho se expresa diciendo que D_n está generado por los elementos R y S sujetos a esas tres relaciones[2], y se simboliza por

$$D_n = \langle R, S \ : \ R^n = e, S^2 = e, SRS = R^{-1} \rangle.$$

Ejercicio 5.2.12 *Con la notación del Ejemplo 5.2.11, supongamos que S es la reflexión con respecto a la recta que une el centro O con el vértice v_n. Se pide:*

1. *Comprobar que, para cada $i \in \mathbb{N}_n$, se tiene $R(v_i) = v_{i+1}$ y $S(v_i) = v_{n-i}$.*
2. *Determinar cuál es el eje de la reflexión R^kS. (Indicación: Si n es impar, el eje pasa por un vértice que depende de k y del inverso de 2 módulo n. Si n es par, el eje pasa por dos vértices si k es par, y por los puntos medios de dos lados si k es impar.)*

Terminamos la sección con un ejemplo de naturaleza distinta a los anteriores. En particular, este grupo puede ser infinito (de hecho lo es precisamente si el cuerpo K que se considera es infinito).

Ejemplo 5.2.13 *El grupo lineal* $\mathrm{GL}_n(K)$.
Sea K un cuerpo. El conjunto de todas las matrices de $M_n(K)$ con determinante no nulo (es decir, invertibles) es un grupo no abeliano (para $n \geq 2$) con el producto usual de matrices. Su elemento neutro es la matriz identidad y el inverso de una matriz A es su matriz inversa en el sentido usual. Le llamamos el *grupo lineal general* de matrices $n \times n$ sobre K, y lo denotamos por $\mathrm{GL}_n(K)$.

5.3 Subgrupos

La definición de subgrupo de un grupo es similar a la que usamos en el caso de subanillos:

Definición 5.3.1 *Sea $(G, \cdot)$ un grupo. Un* subgrupo *de G es un subconjunto H de G cerrado para la operación $\cdot$ y tal que $(H, \cdot)$ es un grupo (se dice que la operación de G* induce una estructura *de grupo en H).*

Consideremos la tabla del grupo D_4 construida en el Ejemplo 5.2.7. Si nos fijamos en las cuatro primeras filas y en las cuatro primeras columnas, observamos que $H = \{1, r, r^2, r^3\}$ es un subgrupo. En general, este es un método poco efectivo de determinar si un subconjunto es o no un subgrupo, y los siguientes resultados constituyen una simplificación notable de este problema. La demostración del primero es esencialmente igual que la de la Proposición 2.3.2.

Proposición 5.3.2 *Sea G un grupo y sea H un subconjunto. Las siguientes condiciones son equivalentes:*

1. *H es subgrupo de G.*
2. *$1 \in H$ y H es cerrado para el producto y para inversos (es decir, si $a, b \in H$ entonces $ab \in H$ y $a^{-1} \in H$).*
3. *H no es vacío y, si $a, b \in H$, entonces $ab^{-1} \in H$.*

Decidir cuándo un subconjunto finito es un subgrupo es algo más fácil; como la mayoría de nuestros ejemplos serán de grupos finitos, el resultado que sigue será de gran utilidad:

[2] Existe una definición rigurosa del concepto de grupo expresado en función de generadores y relaciones que no veremos en este curso.

Corolario 5.3.3 *Sea G un grupo. Si H es un subconjunto finito de G, no vacío y cerrado para el producto, entonces H es subgrupo de G.*

Demostración. Por la proposición anterior, basta ver que H contiene al 1 y es cerrado para inversos. Como H no es vacío, existe un elemento $a \in H$. Entonces $a, a^2, \ldots, a^n, \ldots$ están en H por la hipótesis y, como H es finito, deben existir enteros positivos distintos n, m con $a^n = a^m$. Podemos suponer que $n > m$, de modo que $r = n - m > 0$. Cancelando se obtiene $a^r = 1$, igualdad de la que deducimos que $1 \in H$ (por la hipótesis) y que $a^{-1} = a^{r-1}$ está en H. □

Ejemplos 5.3.4 *Subgrupos.*

1. Sea G un grupo cualquiera. Entonces $\{1\}$ y el propio G son subgrupos de G, llamados respectivamente el *subgrupo trivial* y el *subgrupo impropio* de G. Los subgrupos distintos de $\{1\}$ se llaman *no triviales* y los subgrupos distintos de G se llaman *propios*.

2. Los ideales de un anillo son subgrupos de su grupo aditivo. Para el anillo $\mathbb{Z}$ no hay más subgrupos, ya que multiplicar a por un elemento de $\mathbb{Z}$ equivale a sumar a ó $-a$ varias veces consigo mismo.

3. El conjunto $\mathbb{R}^+$ de los números reales positivos es un subgrupo del grupo multiplicativo $\mathbb{R}^*$.

4. El conjunto de los números complejos de módulo 1 es un subgrupo del grupo multiplicativo $\mathbb{C}^*$.

5. Pueden revisarse las tablas de los grupos finitos considerados en la sección anterior para encontrar subgrupos de D_4, S_3 ó D_3. Así, el conjunto de las rotaciones en D_3 (esto es, $\{1, r, r^2\}$) es un subgrupo. Otro subgrupo de D_3 es $\{e, s\}$.

6. En el grupo lineal $\mathrm{GL}_n(\mathbb{R})$, el subconjunto de las matrices cuyo determinante es 1 es un subgrupo, como se comprueba fácilmente a partir de la igualdad $\det(A \cdot B) = \det(A) \cdot \det(B)$ y usando la Proposición 5.3.2. Este subgrupo se llama el *grupo lineal especial* y se denota por $\mathrm{SL}_n(\mathbb{R})$.

   Un argumento semejante prueba que el conjunto de las matrices en $\mathrm{GL}_n(\mathbb{R})$ cuyo determinante tiene valor absoluto 1 es también un subgrupo de $\mathrm{GL}_n(\mathbb{R})$, que denotaremos por $\widehat{\mathrm{SL}}_n(\mathbb{R})$.

7. Dado un entero positivo $k \geq 3$, consideremos el grupo simétrico S_k. Dentro de S_k podemos tomar todas aquellas permutaciones de $\mathbb{N}_k$ que dejan fijos algunos elementos de $\mathbb{N}_k$; por ejemplo, sea $T \subseteq S_k$ el conjunto de las permutaciones que dejan fijos los números $k-1, k$. Es claro que la composición de dos elementos de T está en T, luego T es un subgrupo de S_k por el Corolario 5.3.3. Es fácil establecer un isomorfismo entre los grupos T y S_{k-2}.

8. Sea $G = S(\mathbb{R}^2)$ el grupo simétrico sobre el plano real. El subconjunto $\mathrm{Isom}(\mathbb{R}^2)$ de G formado por las isometrías del plano es un subgrupo de G. Otro subgrupo de G (y de $\mathrm{Isom}(\mathbb{R}^2)$) está formado por las isometrías que fijan un cierto punto.

9. Sea $\{G_i : i \in I\}$ una familia de grupos y sea $G = \prod_{i \in I} G_i$ el grupo producto. Entonces

$$\oplus_{i \in I} G_i = \{(a_i)_{i \in I} \in \prod_{i \in I} G_i : a_i = 0, \text{ para casi todo } i \in I\}$$

   es un subgrupo de G, llamado la *suma directa* de los subgrupos $\{G_i : i \in I\}$. Si I es finito, entonces la suma directa coincide con el producto directo.

Cerramos esta sección con algunos ejemplos que tendrán interés teórico.

Ejemplo 5.3.5 *El centro de un grupo.*

Dado un grupo G, definimos su *centro* como el subconjunto

$$Z(G) = \{a \in G : ag = ga \text{ para cada } g \in G\}.$$

Es fácil comprobar que $Z(G)$ es subgrupo de G. Además G es abeliano si y sólo si $Z(G) = G$.

Si se conoce la tabla de un grupo, un elemento está en el centro si y sólo si, en su fila y en su columna, los elementos de G aparecen en el mismo orden; por tanto $Z(S_3) = \{e\}$, $Z(D_3) = \{1\}$ y $Z(D_4) = \{1, r^2\}$.

Ejercicio 5.3.6 *Demostrar que el centro de D_n es trivial si n es impar, y es $\{e, R^{n/2}\}$ si n es par.*

Ejercicio 5.3.7 *Si G es un grupo, se define el* centralizador *en G de un elemento $x \in G$ como el subconjunto*

$$\mathrm{Cen}_G(x) = \{g \in G : gx = xg\}.$$

1. *Demostrar que $\mathrm{Cen}_G(x)$ es un subgrupo de G.*
2. *Demostrar que $Z(G) = \cap_{x \in G} \mathrm{Cen}_G(x)$.*
3. *Demostrar que $x \in Z(G) \Leftrightarrow \mathrm{Cen}_G(x) = G$.*
4. *Calcular $\mathrm{Cen}_G(x)$ para cada $x \in G$, cuando G es S_3 ó D_4.*

Ejemplo 5.3.8 *Automorfismos.*

Si G es un grupo, los isomorfismos de grupos $G \to G$ se llaman *automorfismos* de G. En general, la composición de dos isomorfismos y el inverso de un isomorfismo siguen siendo isomorfismos, y por tanto el conjunto $\mathrm{Aut}(G)$ de todos los automorfismos de G es un subgrupo del grupo de permutaciones $S(G)$, llamado *grupo de automorfismos* de G.

Análogamente, si en lugar de los automorfismos de un grupo consideramos los de un espacio vectorial o los de un anillo (con las definiciones obvias), obtendremos subgrupos de los correspondientes grupos de permutaciones. En el caso de un espacio vectorial V de dimensión finita n sobre un cuerpo K, la conocida relación entre las aplicaciones lineales $V \to V$ y las matrices $n \times n$ sobre K (para una base fija de V) nos da un isomorfismo de grupos entre el grupo de los automorfismos de V (como espacio vectorial) y el grupo lineal $\mathrm{GL}_n(K)$ del Ejemplo 5.2.13.

5.4 Operaciones con subgrupos

En adelante, para denotar que H es un subgrupo de un grupo G escribiremos $H \leq G$. En esta sección examinaremos diversas construcciones dentro de un grupo que dan lugar a subgrupos. El primer resultado es de esperar, en vista de los que obtuvimos para anillos, y aparte del interés que tiene en sí mismo, resulta necesario para las construcciones que siguen.

Ejercicio 5.4.1 *Demostrar que la intersección de cualquier familia de subgrupos de un grupo G es un subgrupo de G.*

Definición 5.4.2 *Sea G un grupo y sea S un subconjunto de G. Llamamos* subgrupo *de G* generado *por S, y lo denotamos por $\langle S \rangle$, a la intersección de todos los subgrupos de G que contienen a S; es decir,*

$$\langle S \rangle = \cap \{H : H \leq G \text{ y } S \subseteq H\}.$$

Es claro que $\langle S \rangle$ es el menor subgrupo de G que contiene a S; es decir, $\langle S \rangle$ es un subgrupo de G y todos los subgrupos de G que contienen a S también contienen a $\langle S \rangle$.

Ejemplos 5.4.3 *Subgrupos generados.*

Sea G un grupo arbitrario; entonces:

1. El subgrupo generado por $\emptyset$ es el subgrupo trivial, $\langle \emptyset \rangle = \{1\}$.
2. Si S es un subgrupo de G entonces $\langle S \rangle = S$.
3. Si $x \in G$, entonces $\langle \{x\} \rangle = \{x^n : n \in \mathbb{Z}\}$. Usualmente denotaremos este subgrupo por $\langle x \rangle$. La descripción dada no implica que $\langle x \rangle$ sea infinito, puesto que los valores de x^n se pueden repetir para distintos n. Por ejemplo, el subgrupo de $\mathbb{C}^*$ generado por i es $\{1, i, -1, -i\}$.

   Si se usa notación aditiva entonces $\langle x \rangle = \{nx : n \in \mathbb{Z}\}$. Por tanto, los subgrupos de $\mathbb{Z}$ son precisamente los de la forma $\langle n \rangle$ con $n \in \mathbb{N}$ (son todos infinitos, excepto el trivial).

Veamos ahora una manera más explícita de identificar el subgrupo generado por un conjunto, que además generaliza el último de los ejemplos anteriores. Dado $S \subseteq G$, pondremos

$$S^{-1} = \{x \in G : x^{-1} \in S\} = \{x^{-1} : x \in S\} \qquad \text{y} \qquad \widehat{S} = S \cup S^{-1}.$$

Empleando esta notación se tiene:

Proposición 5.4.4 *Sea G un grupo y sea $S \subseteq G$ un subconjunto. Los elementos del subgrupo generado por S son todos los productos finitos de elementos de $\widehat{S}$. Esto es,*

$$\langle S \rangle = \{x_1 x_2 \cdots x_t \ : \ t \geq 0 \text{ y cada } x_i \in \widehat{S}\},$$

donde interpretamos un producto vacío (con 0 factores) como el neutro 1. También se verifica

$$\langle S \rangle = \{x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r} \ : \ r \geq 0, \text{ cada } x_i \in S \text{ y cada } n_i \in \mathbb{Z}\}.$$

Demostración. Las dos expresiones del enunciado son iguales porque podemos pasar de una del segundo tipo a una del primero sustituyendo x^k por $x \cdots x$ o por $x^{-1} \cdots x^{-1}$ ($|k|$ veces) según el signo de k.

Llamemos H al conjunto $\{x \in G : x = x_1 x_2 \cdots x_t$, con $t \geq 0$ y cada $x_i \in \widehat{S}\}$ y veamos que H es el menor subgrupo de G que contiene a S. Considerando productos de un solo elemento es claro que H contiene a S; también es claro que H contiene al 1 y que es cerrado para productos; además es cerrado para inversos por el Ejercicio 5.1.2, por lo que H es un subgrupo de G (Proposición 5.3.2). Por último, si un subgrupo K de G contiene a cada elemento de S entonces, de nuevo por la Proposición 5.3.2, K contiene a todo H, de modo que, en efecto, H es el menor subgrupo de G que contiene a S. □

Observación 5.4.5 *Si G es abeliano y usamos notación aditiva, el subgrupo generado por S es*

$$\langle S \rangle = \left\{ \sum_{s \in S} n_s s \ : \ n_s \in \mathbb{Z} \text{ para todo } s \in S \text{ y } n_s = 0 \text{ para casi todo } s \in S \right\}.$$

Definición 5.4.6 *Dado un subgrupo H del grupo G, pueden existir diversos subconjuntos $S \subseteq G$ tales que $\langle S \rangle = H$. Cada uno de estos se llama un* sistema generador (o de generadores) *del subgrupo H, y en muchos casos nos interesarán los sistemas generadores del subgrupo impropio G.*

Un grupo es cíclico *si posee un sistema generador unitario (es decir, formado por un solo elemento), y es* finitamente generado *si posee un sistema generador finito.*

Ejercicio 5.4.7 *Demostrar que todo grupo cíclico es abeliano.*

Todo subgrupo H de G tiene al menos un sistema generador: el propio H. Sin embargo, la idea que hay detrás del concepto es poder expresar todos los elementos de un grupo a partir de unos pocos, así que, en general, nos interesan los sistemas generadores que tengan el menor número posible de elementos.

Ejemplos 5.4.8 *Sistemas generadores.*

1. El grupo abeliano $\mathbb{Z}$ es cíclico generado por el 1 (usando notación aditiva). El -1 también es un generador, y no hay otros conjuntos generadores unitarios. El conjunto $\{2, 3\}$ también es un sistema generador de $\mathbb{Z}$.

2. Los grupos abelianos $\mathbb{Z}_n$ son cíclicos generados por $[1]_n$. De hecho, dado $a \in \mathbb{Z}$, el elemento $[a]_n$ genera a $\mathbb{Z}_n$ si y sólo si a es coprimo con n (¿por qué?).

3. El grupo producto $\mathbb{Z} \times \mathbb{Z}$ (notación aditiva) está claramente generado por $\{(1, 0), (0, 1)\}$, pero no es cíclico (¿por qué?).

4. El grupo de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$ no es cíclico, y está generado por cualesquiera dos de sus elementos distintos del neutro.

5. El grupo multiplicativo $\mathbb{Z}_8^*$ no es cíclico, pues tiene 4 elementos y cada uno de ellos genera un subgrupo que sólo tiene 1 ó 2 elementos.

6. Como S_3 no es abeliano, no es cíclico. Sin embargo, es fácil ver que todo conjunto de dos elementos de S_3 que no contenga al neutro y no sea $\{\sigma, \sigma^2\}$ es un sistema generador.

7. Como D_n no es abeliano ($n \geq 3$), no es cíclico. Por la descripción dada en el Ejemplo 5.2.11, D_n está generado por el conjunto $\{R, S\}$.

Ejemplo 5.4.9 *El grupo de los cuaterniones Q_8.*
Se conoce con este nombre, y se denota por Q_8, al subgrupo de $\mathrm{GL}_2(\mathbb{C})$ generado por las matrices

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Si denotamos por I la matriz identidad de tamaño 2×2, es elemental verificar las siguientes relaciones

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -I \qquad \mathbf{ij} = \mathbf{k} = -\mathbf{ji} \qquad \mathbf{jk} = \mathbf{i} = -\mathbf{kj} \qquad \mathbf{ki} = \mathbf{j} = -\mathbf{ik},$$

que en particular muestran que cualesquiera dos de las tres matrices $\mathbf{i}, \mathbf{j}, \mathbf{k}$ generan a la otra, de modo que podemos eliminar una cualquiera de ellas del sistema generador inicial sin alterar el subgrupo definido. Por otra parte, esas relaciones también muestran que

$$Q_8 = \{I, \mathbf{i}, \mathbf{j}, \mathbf{k}, -I, -\mathbf{i}, -\mathbf{j}, -\mathbf{k}\},$$

y que la tabla de operación en Q_8 es

$\cdot$	I	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$-I$	$-\mathbf{i}$	$-\mathbf{j}$	$-\mathbf{k}$
I	I	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$-I$	$-\mathbf{i}$	$-\mathbf{j}$	$-\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	$-I$	$\mathbf{k}$	$-\mathbf{j}$	$-\mathbf{i}$	I	$-\mathbf{k}$	$\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$-I$	$\mathbf{i}$	$-\mathbf{j}$	$\mathbf{k}$	I	$-\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	$-I$	$-\mathbf{k}$	$-\mathbf{j}$	$\mathbf{i}$	I
$-I$	$-I$	$-\mathbf{i}$	$-\mathbf{j}$	$-\mathbf{k}$	I	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$-\mathbf{i}$	$-\mathbf{i}$	I	$-\mathbf{k}$	$\mathbf{j}$	$\mathbf{i}$	$-I$	$\mathbf{k}$	$-\mathbf{j}$
$-\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	I	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{k}$	$-I$	$\mathbf{i}$
$-\mathbf{k}$	$-\mathbf{k}$	$-\mathbf{j}$	$\mathbf{i}$	I	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	$-I$

En general, la unión de dos subgrupos H y K de un grupo G no es un subgrupo de G. El subgrupo que genera su unión, $\langle H \cup K \rangle$, se suele denotar por $H \vee K$ y es el menor subgrupo de G que contiene tanto a H como a K. Como es claro que $\widehat{H \cup K} = H \cup K$, la Proposición 5.4.4 nos dice que

$$H \vee K = \langle H \cup K \rangle = \{x_1 \cdot x_2 \cdots x_n \ : \ n \geq 1 \text{ y cada } x_i \in H \text{ ó } x_i \in K\}.$$

Recuérdese que, cuando considerábamos ideales en anillos, el ideal generado por una unión de ideales era la suma de esos ideales (Proposición 2.5.7). Esto sugiere la definición del producto de dos subgrupos H y K de un grupo G como el subconjunto

$$HK = \{hk \ : \ h \in H, k \in K\},$$

pero en general este subconjunto no es un subgrupo de G. Por ejemplo, si $G = S_3$ entonces, con la notación del Ejemplo 5.2.5, $H = \{e, \tau\}$ y $K = \{e, \sigma\tau\}$ son subgrupos, pero su producto $HK = \{e, \tau, \sigma\tau, \sigma^2\}$ no lo es (¿por qué?).

El siguiente ejercicio muestra que HK es un subgrupo en cuanto hay "un poco de conmutatividad".

Ejercicio 5.4.10 *Demostrar que, si H y K son subgrupos de un grupo G, entonces HK es un subgrupo de G si y sólo si $HK = KH$. En este caso, HK es el menor subgrupo de G que contiene a H y a K; es decir, $HK = H \vee K$.*

Otro resultado útil sobre estos productos de subgrupos es el siguiente:

Lema 5.4.11 *Sean A y B dos subgrupos finitos de un grupo G (no es necesario asumir que AB es un subgrupo de G). Entonces*

$$|AB| \cdot |A \cap B| = |A| \cdot |B|.$$

Demostración. En el conjunto $A \times B$ definimos la relación $(a,b) \sim (c,d) \Leftrightarrow ab = cd$, que es claramente de equivalencia. Si C denota el conjunto cociente de $A \times B$ por esa relación, es claro que la aplicación $\phi : C \to AB$ dada por $\phi(a,b) = ab$ está bien definida (no depende de representantes) y es biyectiva. Además, la clase de equivalencia de $(a,b) \in A \times B$ para esta relación es $\{(ax^{-1}, xb) : x \in A \cap B\}$. En efecto, es obvio que un elemento de la forma (ax^{-1}, xb) está en la clase de (a,b); y si $(c,d) \sim (a,b)$ entonces $x = c^{-1}a = db^{-1}$ está en $A \cap B$ y se tiene $(c,d) = (ax^{-1}, xb)$. Como cada una de estas clases tiene cardinal $|A \cap B|$, hemos demostrado que $A \times B$ se divide en $|AB|$ clases de equivalencia, cada una de ellas con $|A \cap B|$ elementos, y por tanto $|A| \cdot |B| = |A \times B| = |AB| \cdot |A \cap B|$. □

5.5 Clases laterales y Teorema de Lagrange

En el Capítulo 2 vimos que si I es un ideal de un anillo A, entonces existe una partición de A formada por los conjuntos de la forma $a+I = \{a+x : x \in I\}$ con $a \in A$. En realidad, sólo utilizamos la estructura aditiva de A para construir esta partición. Estas particiones se pueden construir de forma análoga a partir de un grupo G y un subgrupo suyo H. Pero la posible no conmutatividad de la operación del grupo hace que la versión de la relación de equivalencia que utilizábamos para construir las clases $a + I$ ($a \equiv b \bmod I \Leftrightarrow a - b \in I$) tenga dos definiciones alternativas en el caso de grupos:

$$a \equiv_i b \bmod H \Leftrightarrow a^{-1}b \in H; \qquad a \equiv_d b \bmod H \Leftrightarrow ab^{-1} \in H.$$

Ejercicio 5.5.1 *Demostrar que, para cualquier grupo G y cualquier subgrupo H, las dos relaciones binarias recién definidas son de equivalencia en G.*

Las relaciones $\equiv_i$ y $\equiv_d$ inducen particiones en G. Veamos cómo son las clases de equivalencia: La clase de equivalencia de $a \in G$ por la relación $\equiv_i \bmod H$ es

$$\{x \in G : a \equiv_i x \bmod H\} = \{x \in G : a^{-1}x \in H\} = \{ah \in G : h \in H\} = aH,$$

y análogamente la clase de equivalencia de a por la relación $\equiv_d$ es

$$Ha = \{ha : h \in H\}.$$

Los conjuntos aH se llaman *clases laterales por la izquierda* de G *módulo* H y los conjuntos Ha se llaman *clases laterales por la derecha* de G *módulo* H. El conjunto de las clases laterales por la izquierda se denota G/H y el conjunto de las clases laterales por la derecha por $H\backslash G$. Es decir,

$$G/H = \{gH : g \in G\} \qquad \text{y} \qquad H\backslash G = \{Hg : g \in G\}.$$

Es claro que, para todo $a, b \in G$, se tiene

$$aH = bH \Leftrightarrow a \in bH \Leftrightarrow b \in aH \Leftrightarrow a^{-1}b \in H \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH \cap bH \neq \emptyset$$

y

$$Ha = Hb \Leftrightarrow a \in Hb \Leftrightarrow b \in Ha \Leftrightarrow ba^{-1} \in H \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha \cap Hb \neq \emptyset.$$

En particular $H = 1H$ y

$$aH = H \Leftrightarrow a \in H \Leftrightarrow Ha = H.$$

Ejemplos 5.5.2 *Clases laterales.*

1. Si I es un ideal de un anillo A, entonces I es un subgrupo del grupo $(A, +)$ y las clases laterales (por la izquierda y por la derecha) coinciden con las definidas en el Capítulo 2.

2. Consideremos en D_4 el subgrupo de las rotaciones $K = \langle r \rangle = \{1, r, r^2, r^3\}$. Como $Ks = sK = \{s, rs, r^2s, r^3s\}$, vemos que en este caso $G/K = K\backslash G = \{K, Ks\}$; es decir, sólo hay dos clases por la derecha y coinciden con las dos clases por la izquierda.

   Podemos también calcular las clases laterales módulo el subgrupo $H = \{1, s\}$; en este caso las clases por la derecha son

   $$H1 = Hs = \{1, s\} \quad Hr = Hr^3s = \{r, r^3s\} \quad Hr^2 = Hr^2s = \{r^2, r^2s\} \quad Hr^3 = Hrs = \{r^3, rs\},$$

   mientras que las clases por la izquierda son

   $$1H = sH = \{1, s\} \quad rH = rsH = \{r, rs\} \quad r^2H = r^2sH = \{r^2, r^2s\} \quad r^3H = r^3sH = \{r^3, r^3s\}.$$

   En particular, hay elementos tales que $aH \neq Ha$ y los conjuntos G/H y $H\backslash G$ son distintos.

La siguiente proposición estudia los cardinales de cada clase lateral de G módulo H, y también los de G/H y $H\backslash G$.

Proposición 5.5.3 *Si H es un subgrupo de G, entonces:*

1. *La aplicación $H \to Ha$ dada por $h \mapsto ha$ es una biyección con inversa $x \mapsto xa^{-1}$. En particular, si H es finito entonces todas las clases por la derecha módulo H tienen cardinal $|H|$.*

   La aplicación $H \to aH$ dada por $h \mapsto ah$ es una biyección con inversa $x \mapsto a^{-1}x$. En particular, si H es finito entonces todas las clases por la izquierda módulo H tienen cardinal $|H|$.

2. *La aplicación $H\backslash G \to G/H$ dada por $Ha \mapsto a^{-1}H$ es una biyección con inversa $bH \mapsto Hb^{-1}$. En particular, $H\backslash G$ es finito si y sólo si lo es G/H, y en ese caso sus cardinales coinciden.*

Demostración. El primer apartado es claro, y el segundo lo será si vemos que las aplicaciones dadas están bien definidas. Pero esto es así pues $Ha = Hb$ implica que $ab^{-1} = (a^{-1})^{-1}b^{-1} \in H$, por lo que $a^{-1}H = b^{-1}H$. □

Definición 5.5.4 *Se llama* orden *de un grupo finito G a su cardinal $|G|$.*

Si G es un grupo arbitrario con un subgrupo H, decimos que H tiene índice finito *en G si el cardinal común de $H\backslash G$ y G/H es finito; llamamos* índice *de H en G a ese cardinal, y lo denotamos por $[G : H]$.*

Es evidente que todo subgrupo de un grupo finito tiene índice finito. Por su parte, un grupo infinito tiene al menos un subgrupo de índice infinito (el trivial), y puede tener subgrupos impropios de índice finito: por ejemplo, si $n \geq 1$ entonces $[\mathbb{Z} : n\mathbb{Z}] = n$.

El siguiente teorema es fundamental en el estudio de un grupo finito G, pues establece una relación entre el orden de G y el de sus subgrupos; a saber, el orden de cualquier subgrupo divide al orden del grupo. En general, la relación entre divisores de $|G|$ y subgrupos de G es profunda y complicada, y éste es el primer paso que daremos para desentrañarla.

Teorema 5.5.5 (Teorema de Lagrange) *Si G es un grupo finito y H es un subgrupo de G, entonces el orden de H y el índice de H en G son ambos divisores del orden de G. De hecho, se tiene*

$$|G| = |H| \cdot [G : H] \qquad (\textit{o sea,} \quad |G/H| = [G : H] = |G|/|H|).$$

Demostración. Por los dos resultados anteriores, G se divide en $|G/H| = [G : H]$ clases por la derecha módulo H, cada una de ellas con $|H|$ elementos, lo que nos da las igualdades postuladas. □

Del Teorema de Lagrange se deduce que un subgrupo de un grupo finito es tanto mayor cuanto menor es su índice. Por lo tanto el índice de H en G sirve para medir lo grande que es H "dentro de G": si $[G : H] = 1$ entonces H es todo G, si $[G : H] = 2$ entonces H es "la mitad de grande" que G, etcétera.

Como hemos dicho, el Teorema de Lagrange es un instrumento poderoso para estudiar los grupos finitos en función de su cardinal. Un ejemplo es el siguiente, que es el primero de un tipo de resultados que perseguiremos a lo largo del curso, en los que se trata de deducir propiedades de un grupo finito en función únicamente de su orden.

Corolario 5.5.6 *Si G es un grupo finito de orden primo p, entonces G es cíclico (generado por cualquier elemento distinto del neutro) y no tiene más subgrupos que el trivial y el impropio.*

Demostración. Como los únicos divisores positivos de $|G| = p$ son 1 y p, cualquier posible subgrupo de G ha de tener orden 1 ó p. Pero el único subgrupo de orden 1 es el trivial, y el único de orden p es todo G, luego estos son los únicos subgrupos de G.

Por otra parte, G contiene un elemento $a \neq 1$ (pues $|G| = p > 1$), luego $\langle a \rangle$ es un subgrupo no trivial; del párrafo anterior deducimos que $G = \langle a \rangle$; es decir, G es cíclico (y está generado por cualquier elemento distinto del neutro). □

Ejercicio 5.5.7 *Si G es un grupo finito con subgrupos H y K tales que $H \subseteq K$, demostrar que se tiene*

$$H = K \Leftrightarrow |H| = |K| \Leftrightarrow [G : H] = [G : K].$$

Ejercicio 5.5.8 *Por el teorema de Lagrange, los posibles subgrupos propios y no triviales de $\mathbb{Z}_6$ o de S_3 han de tener orden 2 ó 3, y los de $\mathbb{Z}_8$ o de D_4 deben tener orden 2 ó 4. Determinar todos los subgrupos en cada caso.*

5.6 Subgrupos normales y grupos cociente

En esta sección abordamos la construcción del grupo cociente de un grupo G por un subgrupo N definiendo de forma natural un producto entre las clases laterales módulo N. Esta construcción no es válida para cualquier subgrupo, y en lo que sigue se describen los subgrupos para los que sí lo es.

Dados subconjuntos A y B de un grupo G, pondremos $AB = \{ab : a \in A, b \in B\}$. Si $X = \{x\}$ pondremos xA en lugar de XA y Ax en lugar de AX, lo que es consistente con la notación usada para las clases laterales. Por otra parte, la asociatividad de G implica que $(AB)C = A(BC)$ para subconjuntos A, B y C arbitrarios, lo que nos permite escribir ABC sin ambigüedad; obviamente $ABC = \{abc : a \in A, b \in B, c \in C\}$.

Proposición 5.6.1 *Las condiciones siguientes son equivalentes para un subgrupo N de un grupo G:*

1. *$N\backslash G = G/N$.*
2. *Para cada $x \in G$ se tiene $Nx = xN$ (o equivalentemente $x^{-1}Nx = N$).*
3. *Para cada $x \in G$ se tiene $Nx \subseteq xN$ (o equivalentemente $x^{-1}Nx \subseteq N$).*
4. *Para cada $x \in G$ se tiene $xN \subseteq Nx$ (o equivalentemente $xNx^{-1} \subseteq N$).*
5. *Para cualesquiera $a, b \in G$ se tiene $aNbN = abN$.*
6. *Para cualesquiera $a, b \in G$ se tiene $NaNb = Nab$.*

Demostración. Es obvio que 2 implica 1. El recíproco es cierto pues, dado $x \in G$, la hipótesis 1 implica que existe $y \in G$ tal que $Nx = yN$, por lo que $x \in yN$ y así $xN = yN = Nx$.

A continuación demostramos de forma cíclica la equivalencia entre 2, 5 y 3. El lector puede ver de forma análoga que 2, 6 y 4 son equivalentes, lo que concluirá la demostración. Usaremos dos hechos de fácil comprobación: Por ser N subgrupo, se tiene $NN = N$, y si $A \subseteq B$, entonces $xA \subseteq xB$ y $Ax \subseteq Bx$.

2 implica 5. Asumiendo 2 y tomando $a, b \in G$, se tiene $aNbN = abNN = abN$.

5 implica 3. Dados $n \in N$ y $x \in G$ se tiene $nx = 1nx1 \in 1NxN = 1xN = xN$, por lo que $Nx \subseteq xN$.

3 implica 2. Fijemos $x \in G$ y veamos que $xN \subseteq Nx$. Como 3 vale para cualquier elemento de G, se tiene $Nx^{-1} \subseteq x^{-1}N$, y multiplicando a la derecha por x en ambos lados de la igualdad obtenemos la inclusión deseada. □

Supongamos que se cumplen las condiciones de la Proposición 5.6.1. Entonces el producto de dos elementos de G/N (o de $N\backslash G$) es un elemento de G/N, y es elemental comprobar que esta operación dota a G/N de una estructura de grupo. Obsérvese que, para realizar un producto $aN \cdot bN$ en G/N, no necesitamos describir el conjunto resultante, pues éste queda determinado por cualquier representante suyo, por ejemplo ab. El elemento neutro de G/N es la clase $N = 1N$, y el inverso de aN es $a^{-1}N$.

Definición 5.6.2 *Un subgrupo N de un grupo G es un* subgrupo normal *de G (también se dice que N es* normal en G*) si verifica las condiciones equivalentes de la Proposición 5.6.1. En ocasiones escribiremos $N \trianglelefteq G$ (respectivamente $N \triangleleft G$) para indicar que N es un subgrupo normal (respectivamente normal y propio) de G.*

Si N es normal en G, el grupo G/N recién descrito se llama grupo cociente *de G módulo N.*

Ejemplos 5.6.3 *Subgrupos normales.*

1. Es claro que, en un grupo abeliano, todo subgrupo es normal. De hecho, si I es un ideal de un anillo A, entonces el grupo cociente A/I es el grupo aditivo del anillo cociente.

2. Si G es un grupo y H es un subgrupo contenido en el centro $Z(G)$, entonces H es normal en G. En particular, el centro es un subgrupo normal.

3. Si H es un subgrupo de G de índice 2, entonces H es normal en G. En efecto, como las clases por la derecha módulo H constituyen una partición de G, sólo hay dos, y una de ellas es H, la otra ha de ser el complementario $\{g \in G : g \notin H\}$. El mismo argumento vale para las clases por la izquierda y en consecuencia $G/N = N\backslash G$.

4. Sea $G = \mathrm{GL}_n(\mathbb{R})$ el grupo lineal general sobre $\mathbb{R}$. Usando el hecho de que, si $a, b \in G$, entonces

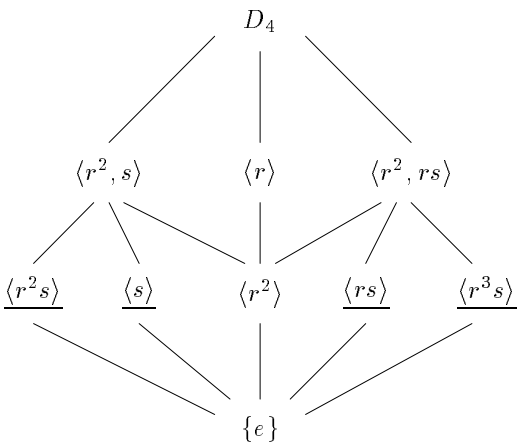
$$\det(ba) = \det(b)\det(a) = \det(a)\det(b) = \det(ab),$$

   es fácil ver que tanto el grupo lineal especial $S = \mathrm{SL}_n(\mathbb{R})$ como el grupo $\hat{S} = \widehat{\mathrm{SL}}_n(\mathbb{R})$ (ver los Ejemplos 5.3.4) son subgrupos normales de G. Vamos a describir el grupo cociente G/S.

   Sean $m, x \in G$ y sea $\alpha = \det(m)$. Si $x \in mS$ entonces $x = ms$ con $s \in S$, por lo que $\det(x) = \det(m)\det(s) = \alpha$. Recíprocamente, si $\det(x) = \alpha$ entonces $\det(m^{-1}x) = \alpha^{-1}\alpha = 1$ y así $m^{-1}x \in S$, o sea $x \in mS$. En consecuencia, la clase mS consiste en todas las matrices de G cuyo determinante es α, y la denotaremos por $\bar{\alpha}$. Como para cada $\alpha \in \mathbb{R}^*$ hay matrices con determinante α (¡muestra una!), deducimos que $G/S = \{\bar{\alpha} : \alpha \in \mathbb{R}^*\}$. Además, si $\alpha\beta = \gamma$ en $\mathbb{R}^*$ entonces $\bar{\alpha}\bar{\beta} = \bar{\gamma}$ en G/S, como se comprueba fácilmente. En consecuencia, la aplicación $\mathbb{R}^* \to G/S$ dada por $\alpha \mapsto \bar{\alpha}$ es un isomorfismo de grupos, y tenemos un ejemplo de grupo no abeliano con cociente abeliano.

   Dejamos que el lector establezca un isomorfismo de grupos entre $\mathbb{R}^+$ y el cociente $G/\hat{S}$.

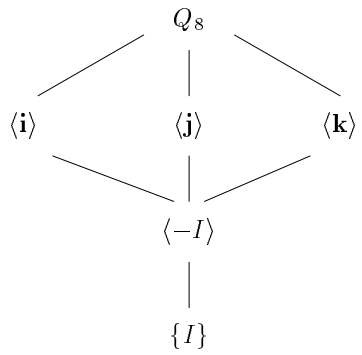
5. El siguiente es el diagrama de todos los subgrupos de D_4 ordenados por inclusión: una línea entre dos subgrupos significa que el de arriba contiene al de abajo. Los subgrupos de la segunda fila tienen orden 4, y los de la tercera fila tienen orden 2. En el diagrama están subrayados los subgrupos que *no* son normales en D_4, que son precisamente los subgrupos generados por cada una de las simetrías:



Los que aparecen son subgrupos y las relaciones de inclusión son claras, pero el lector deberá comprobar esos subgrupos son distintos entre sí y que no hay más, así como la normalidad de los subgrupos no subrayados. Otro ejercicio interesante consiste en demostrar que los subgrupos $\langle r^2, s\rangle$ y $\langle r^2, rs\rangle$ no son cíclicos.

Obsérvese que cualquier subgrupo del diagrama es normal en cualquiera de los subgrupos que lo contengan y estén en el nivel inmediatamente superior. Por ejemplo, $\langle s\rangle \trianglelefteq \langle r^2, s\rangle$ y $\langle r^2, s\rangle \trianglelefteq D_4$; como $\langle s\rangle$ no es normal en D_4, este ejemplo muestra que la relación "ser normal en" no es transitiva.

6. El diagrama de los subgrupos de Q_8 es el siguiente.



Obsérvese que todos son normales (¿por qué?).

Sea $Z = Z(Q_8) = \{I, -I\}$. Los elementos del grupo cociente Q_8/Z son Z, $Z\mathbf{i} = \{\mathbf{i}, -\mathbf{i}\}$, $Z\mathbf{j} = \{\mathbf{j}, -\mathbf{j}\}$ y $Zk = \{\mathbf{k}, -\mathbf{k}\}$, y su tabla es la siguiente:

$\cdot$	Z	$Z\mathbf{i}$	$Z\mathbf{j}$	$Z\mathbf{k}$
Z	Z	$Z\mathbf{i}$	$Z\mathbf{j}$	$Z\mathbf{k}$
$Z\mathbf{i}$	$Z\mathbf{i}$	Z	$Z\mathbf{k}$	$Z\mathbf{j}$
$Z\mathbf{j}$	$Z\mathbf{j}$	$Z\mathbf{k}$	Z	$Z\mathbf{i}$
$Z\mathbf{k}$	$Z\mathbf{k}$	$Z\mathbf{j}$	$Z\mathbf{i}$	Z

Obsérvese que Q_8 es un grupo no abeliano pero es "casi abeliano" en dos sentidos: todos sus subgrupos son normales, y todos los subgrupos propios dan cocientes abelianos. Por otra parte, en vista de la tabla, es sencillo establecer un isomorfismo entre el grupo cociente Q_8/Z y el grupo de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Ejercicio 5.6.4 *Demostrar que un grupo cociente de un grupo finitamente generado es finitamente generado.*

Acabamos la sección con una versión para grupos del Teorema de la Correspondencia (2.4.8).

Teorema 5.6.5 (Teorema de la Correspondencia) *Sea N un subgrupo normal de un grupo G. La asignación $H \mapsto H/N$ establece una biyección entre el conjunto $\mathcal{A}$ de los subgrupos de G que contienen a N y el conjunto $\mathcal{B}$ de los subgrupos de G/N.*

Además, esta biyección conserva las inclusiones, las intersecciones y la normalidad. Es decir, dados $H, K \in \mathcal{A}$, se tiene:

1. *$H \subseteq K$ si y sólo si $(H/N) \subseteq (K/N)$.*
2. *$(H \cap K)/N = (H/N) \cap (K/N)$.*
3. *$H \trianglelefteq G$ si y sólo si $(H/N) \trianglelefteq (G/N)$.*

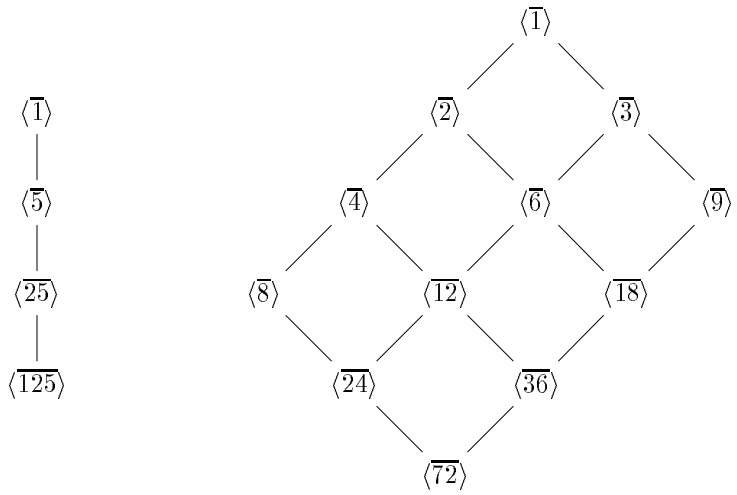
Demostración. Si H está en $\mathcal{A}$ entonces es claro que N es un subgrupo normal de H, por lo que podemos considerar el grupo cociente H/N, que es un subgrupo de G/N (¡compruébese!). Llamemos $\Phi : \mathcal{A} \to \mathcal{B}$ a la aplicación dada por $\Phi(H) = H/N$, y veamos que es inyectiva y suprayectiva.

Sean H y K elementos de $\mathcal{A}$ tales que $\Phi(H) = \Phi(K)$. Entonces, si $h \in H$, se tiene $Nh \in H/N = K/N$ y en consecuencia existe $k \in K$ tal que $Nh = Nk$, luego $hk^{-1} \in N \subseteq K$; multiplicando por k se obtiene $h \in K$. En consecuencia $H \subseteq K$, y análogamente se prueba que $K \subseteq H$, lo que nos dice que Φ es inyectiva. Por otra parte, si $X \in \mathcal{B}$ entonces $H = \{x \in G : Nx \in X\}$ es un elemento de $\mathcal{A}$ tal que $\Phi(H) = X$ (la comprobación de los detalles se deja al lector), lo que demuestra que Φ es suprayectiva.

La demostración de la segunda parte del enunciado se deja como ejercicio para el lector. □

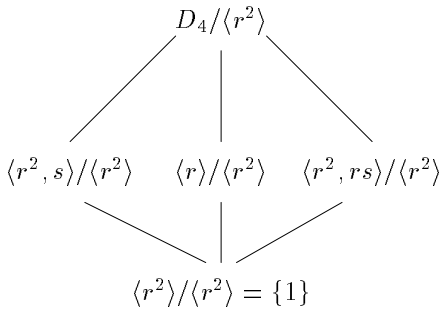
Ejemplos 5.6.6 *Aplicaciones del Teorema de la Correspondencia.*

1. Dado un entero positivo $n \in \mathbb{Z}^+$, vamos a describir los subgrupos del grupo cociente $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$. Escribiremos $\overline{a} = a + \langle n\rangle$. Sabemos que los subgrupos de $\mathbb{Z}$ son precisamente los de la forma $\langle d\rangle$ con $d \geq 0$, y que $\langle d\rangle \subseteq \langle d'\rangle$ si y sólo si $d' \mid d$. Por tanto, los subgrupos de $\mathbb{Z}_n$ son precisamente los de la forma $\frac{\langle d\rangle}{\langle n\rangle} = \langle \overline{d}\rangle$, donde d es un divisor positivo de n, y además $\langle \overline{d}\rangle \subseteq \langle \overline{d'}\rangle$ si y sólo si $d' \mid d$. Así, el diagrama de los subgrupos de $\mathbb{Z}_n$ puede construirse de modo elemental a partir de los divisores de n como muestran los siguientes diagramas (en el de la izquierda se ha tomado $n = 125$, y en el de la derecha $n = 72$):



En general, si r es el número de divisores primos distintos de n, se necesita un diagrama en r dimensiones; por ejemplo, para $n = 180$ necesitaríamos un diagrama tridimensional. Obsérvese que, si $n = dt$, entonces $\langle \overline{d}\rangle = \{\overline{0}, \overline{d}, \overline{2d}, \ldots, \overline{(t-1)d}\}$ tiene t elementos. Por tanto, si t es cualquier divisor positivo de n y tomamos $d = n/t$, entonces $\langle \overline{d}\rangle$ es el único subgrupo de $\mathbb{Z}_n$ con t elementos. Es decir, $\mathbb{Z}_n$ verifica el "recíproco del Teorema de Lagrange" con una condición extra de unicidad.

2. Aplicando el Teorema de la Correspondencia al diagrama de los subgrupos de D_4 (Ejemplos 5.6.3), obtenemos el siguiente diagrama de los subgrupos de $D_4/\langle r^2\rangle$.



5.7 Homomorfismos y Teoremas de Isomorfía

Aunque ya hemos usado la noción de homomorfismo e isomorfismo de grupos, es en esta sección donde las estudiamos de modo sistemático. Comenzamos repitiendo las definiciones:

Definición 5.7.1 *Un* homomorfismo *del grupo $(G,\cdot)$ en el grupo $(H,*)$ es una aplicación $f: G \to H$ que conserva la operación; es decir, que verifica*

$$f(a \cdot b) = f(a) * f(b)$$

para cualesquiera $a, b \in G$. Si $G = H$ decimos que f es un endomorfismo *de G.*

Si $f: G \to H$ es un homomorfismo biyectivo, diremos que es un isomorfismo *y que los grupos G y H son* isomorfos. *Un isomorfismo de G en G se dirá un* automorfismo *de G.*

Dado un homomorfismo de grupos $f: G \to H$, se definen su imagen *y su* núcleo *como*

$$\text{Im } f = f(G) = \{f(x) : x \in G\} \subseteq H \qquad \text{Ker } f = f^{-1}(1_H) = \{x \in G : f(x) = 1_H\} \subseteq G.$$

Ejercicio 5.7.2 *Sea $f: G \to H$ un homomorfismo de grupos. Demostrar que se verifican las siguientes propiedades para $a, a_1, \ldots, a_n \in G$:*

1. *(f conserva el neutro) $f(1_G) = 1_H$.*
2. *(f conserva inversos) $f(a^{-1}) = f(a)^{-1}$.*
3. *(f conserva productos finitos) $f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$.*
4. *(f conserva potencias) Si $n \in \mathbb{Z}$ entonces $f(a^n) = f(a)^n$.*
5. *Si f es un isomorfismo entonces la aplicación inversa $f^{-1}: H \to G$ también lo es.*
6. *Si $g: H \to K$ es otro homomorfismo de grupos entonces $g \circ f: G \to K$ es un homomorfismo de grupos.*
7. *Si H_1 es un subgrupo de H entonces $f^{-1}(H_1) = \{x \in G : f(x) \in H_1\}$ es un subgrupo de G.*

   Si además H_1 es normal en H entonces $f^{-1}(H_1)$ es normal en G; en particular, Ker f *es un subgrupo normal de G.*
8. *f es inyectivo si y sólo si* Ker $f = \{1\}$.
9. *Si G_1 es un subgrupo de G entonces $f(G_1)$ es un subgrupo de H; en particular,* Im f *es un subgrupo de H.*

   Si además G_1 es normal en G y f es suprayectiva entonces $f(G_1)$ es normal en H.
10. *La hipótesis de suprayectividad en la propiedad anterior no es superflua; es decir, dar un ejemplo de un homomorfismo de grupos $f: G \to H$ y un subgrupo normal G_1 de G, tal que $f(G_1)$ no es normal en H.*

Ejemplos 5.7.3 *Homomorfismos de grupos.*

1. Si H es un subgrupo de G, la inclusión de H en G es un homomorfismo inyectivo.
2. Si N es un subgrupo normal de G, la aplicación $\pi: G \to G/N$ dada por $\pi(x) = xN$ es un homomorfismo suprayectivo que recibe el nombre de *proyección canónica* de G sobre G/N. Su núcleo es Ker $\pi = N$.
3. Dados dos grupos G y H, la aplicación $f: G \to H$ dada por $f(a) = 1_H$ para cada $a \in G$ es un homomorfismo llamado *homomorfismo trivial* de G en H. Su núcleo es todo G.
4. La aplicación $f: \mathbb{Z} \to \mathbb{Z}$ dada por $f(n) = 2n$ es un homomorfismo inyectivo y no suprayectivo.
5. Si G es cualquier grupo y $x \in G$ es cualquier elemento, la aplicación $\mathbb{Z} \to G$ dada por $n \mapsto x^n$ es un homomorfismo de grupos; como en $\mathbb{Z}$ usamos notación aditiva y en G multiplicativa, la afirmación anterior es equivalente al hecho, que ya conocemos, de que $x^{n+m} = x^n x^m$.

6. Otro ejemplo en el que se mezclan las notaciones aditiva y multiplicativa es el siguiente: Fijado un número real positivo α, la aplicación $\mathbb{R} \to \mathbb{R}^+$ dada por $r \mapsto \alpha^r$ es un isomorfismo de grupos cuya inversa es la aplicación $\mathbb{R}^+ \to \mathbb{R}$ dada por $s \mapsto \log_\alpha s$.

Claramente, si $f : G \to H$ es un homomorfismo inyectivo de grupos entonces $f : G \to \text{Im } f$ es un isomorfismo de grupos que nos permite ver a G como un subgrupo de H. El siguiente teorema nos dice que todo grupo finito puede verse como un subgrupo de un grupo simétrico.

Teorema 5.7.4 (Cayley) *Todo grupo G es isomorfo a un subgrupo del grupo de permutaciones $S(G)$. En particular, todo grupo finito G de orden n es isomorfo a un subgrupo de S_n.*

Demostración. Por el comentario anterior, se trata de establecer la existencia de un homomorfismo inyectivo $\phi : G \to S(G)$. Si, para cada $g \in G$, definimos $\phi(g)$ como la permutación de G dada por $x \mapsto gx$ (es una biyección con inversa $\phi(g^{-1})$), es elemental ver que ϕ es el homomorfismo buscado. La segunda parte se sigue del hecho de que, si $|G| = n$, entonces $S(G)$ es isomorfo a S_n (Ejercicio 5.2.3). □

El siguiente ejercicio puede considerarse como una versión del Teorema de la Correspondencia.

Ejercicio 5.7.5 *Sea N un subgrupo normal de un grupo G y sea $\pi : G \to G/N$ la proyección canónica. Demostrar que:*

1. *Si H es un subgrupo de G, entonces HN es un subgrupo de G que contiene a N, y se tiene $\pi(H) = HN/N$. Además, HN es normal en G si lo es H.*
2. *Si H es un subgrupo de G que contiene a N, entonces $\pi(H) = H/N$ es la imagen de H por la aplicación Φ del Teorema de la Correspondencia (5.6.5).*

Los Teoremas de Isomorfía que vimos para anillos tienen una versión para grupos. Las demostraciones son análogas, de modo que sólo indicamos sus líneas generales.

Teorema 5.7.6 (Primer Teorema de Isomorfía) *Sea $f : G \to H$ un homomorfismo de grupos. Entonces existe un único isomorfismo de grupos $\bar{f} : G/\text{Ker } f \to \text{Im } f$ que hace conmutativo el diagrama*

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/\text{Ker } f & \xrightarrow{\quad \bar{f} \quad} & \text{Im } f \end{array}$$

es decir, $i \circ \bar{f} \circ p = f$, donde i es la inclusión y p es la proyección canónica. En particular

$$\frac{G}{\text{Ker } f} \cong \text{Im } f.$$

Demostración. Si $K = \text{Ker } f$, la aplicación $\bar{f} : G/K \to \text{Im } f$ dada por $\bar{f}(xK) = f(x)$ satisface las propiedades del enunciado. □

Usando el Teorema de la Correspondencia se obtiene el siguiente corolario.

Corolario 5.7.7 *En la situación del Primer Teorema de Isomorfía, $\bar{f}$ induce una biyección entre el conjunto de los subgrupos de G que contienen a* Ker f *y el de los subgrupos de H contenidos en* Im f.

Teorema 5.7.8 (Segundo Teorema de Isomorfía) *Sean N y H subgrupos normales de un grupo G con $N \subseteq H$. Entonces H/N es un subgrupo normal de G/N y se tiene*

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

En particular, si G/N es finito, se tiene

$$[G/N : H/N] = [G : H].$$

Demostración. La aplicación $f : G/N \to G/H$ dada por $f(xN) = xH$ es un homomorfismo suprayectivo con núcleo H/N. □

Teorema 5.7.9 (Tercer Teorema de Isomorfía) *Sean G un grupo, H un subgrupo de G y N un subgrupo normal de G. Entonces $N \cap H$ es un subgrupo normal de H y se tiene*

$$\frac{H}{N \cap H} \cong \frac{NH}{N}.$$

Demostración. La aplicación $f : H \to G/N$ dada por $f(x) = Nx$ es un homomorfismo con núcleo $H \cap N$ e imagen NH/N. □

Ejemplos 5.7.10 *Aplicaciones de los Teoremas de Isomorfía.*

1. Consideremos los grupos multiplicativos $\mathbb{C}^*$ y $\mathbb{R}^*$, y la aplicación norma $\delta : \mathbb{C}^* \to \mathbb{R}^*$ dada por $\delta(a+bi) = a^2 + b^2$. Entonces δ es un homomorfismo que tiene por núcleo a la circunferencia de radio 1 en $\mathbb{C}$, y por imagen a $\mathbb{R}^+$. Por tanto, el grupo cociente de $\mathbb{C}^*$ por la circunferencia de radio 1 es isomorfo a $\mathbb{R}^+$.

2. La aplicación $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ que lleva una matriz a su determinante es un homomorfismo suprayectivo de grupos con núcleo $\mathrm{SL}_n(\mathbb{R})$. Esto nos dice que el cociente de $\mathrm{GL}_n(\mathbb{R})$ por $\mathrm{SL}_n(\mathbb{R})$ es isomorfo a $\mathbb{R}^*$, cosa que ya habíamos visto por métodos más elementales (pero con más trabajo).

   Usando la aplicación "valor absoluto del determinante" se demuestra con la misma facilidad que el cociente de $\mathrm{GL}_n(\mathbb{R})$ por $\widehat{\mathrm{SL}}_n(\mathbb{R})$ es isomorfo a $\mathbb{R}^+$.

   Por último, la aplicación $\det : \widehat{\mathrm{SL}}_n(\mathbb{R}) \to \mathbb{R}^*$ tiene núcleo $\mathrm{SL}_n(\mathbb{R})$ e imagen $\{1, -1\}$, luego el cociente de $\widehat{\mathrm{SL}}_n(\mathbb{R})$ por $\mathrm{SL}_n(\mathbb{R})$ es isomorfo a $\mathbb{Z}_2$. Cuando $n = 2$, podemos tomar como representantes de cada una de las clases laterales a las matrices $a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ y $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

3. Sea n un entero positivo. Hemos visto (Ejemplos 5.6.6) que todo subgrupo de $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ es de la forma $\langle \overline{d}\rangle = \langle d\rangle/\langle n\rangle$, para cierto divisor positivo d de n. El Segundo Teorema de Isomorfía nos permite identificar el cociente $\mathbb{Z}_n/\langle \overline{d}\rangle$, pues

$$\frac{\mathbb{Z}_n}{\langle \overline{d}\rangle} = \frac{\mathbb{Z}/\langle n\rangle}{\langle d\rangle/\langle n\rangle} \cong \frac{\mathbb{Z}}{\langle d\rangle} = \mathbb{Z}_d.$$

5.8 Órdenes de elementos y grupos cíclicos

Definición 5.8.1 *Sea G un grupo. El* orden *de un elemento $g \in G$, denotado por $o(g)$, es el cardinal del subgrupo $\langle g\rangle$ generado por g. Si $\langle g\rangle$ es infinito escribimos $o(g) = \infty$.*

Recordemos que, en general, $\langle g\rangle = \{g^n : n \in \mathbb{Z}\}$ (ó $\{ng : n \in \mathbb{Z}\}$ si usamos notación aditiva). Aunque los posibles exponentes sean infinitos, estos conjuntos pueden ser finitos si los g^n se repiten. De hecho es claro que, en un grupo finito, todo elemento tiene orden finito.

Ejemplos 5.8.2 *Órdenes de elementos.*

1. Es claro que $o(g) = 1$ si y sólo si g es el neutro de G.

2. Cualquier elemento no nulo de $\mathbb{Z}$ tiene orden infinito.

3. En $\mathbb{R}^*$, el elemento -1 tiene orden 2, y cualquier elemento distinto de ± 1 tiene orden infinito.

4. En $\mathbb{C}^*$, los elementos $-1, \omega = \frac{-1+\sqrt{3}i}{2}$ e i tienen órdenes $2, 3$ y 4, respectivamente. Más generalmente, el número complejo $e^{\frac{2\pi i}{k}} = \cos\frac{2\pi}{k} + i\,\mathrm{sen}\,\frac{2\pi}{k}$ tiene orden k. Un elemento cuya norma no sea 1 tiene orden infinito.

5. En $\mathrm{GL}_2(\mathbb{R})$, la matriz $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ tiene orden 4, y la matriz $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ tiene orden infinito pues, como se demuestra fácilmente por inducción, $a^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

6. Si n es un entero positivo, los siguientes elementos tienen orden n: el elemento $[1]_n$ en $\mathbb{Z}_n$; el giro de ángulo $2\pi/n$ en D_n; el elemento $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$ en S_n.

En las dos proposiciones siguientes damos diversas interpretaciones alternativas del concepto de orden de un elemento, separando los casos finito e infinito. Dado un elemento g de un grupo G, denotaremos por $\mu_g : \mathbb{Z} \to G$ al homomorfismo dado por $\mu_g(n) = g^n$. Es obvio que $\mathrm{Im}\,(\mu_g) = \langle g \rangle$ y que $\mathrm{Ker}\,(\mu_g) = \{n \in \mathbb{Z} : g^n = 1\}$.

Proposición 5.8.3 *Las condiciones siguientes son equivalentes para un elemento g de un grupo G y un entero positivo n:*

1. $o(g) = n$.
2. *El subgrupo $\langle g \rangle$ es isomorfo a $\mathbb{Z}_n$.*
3. $\mathrm{Ker}\,(\mu_g) = n\mathbb{Z}$.
4. *Para un entero arbitrario m se tiene $g^m = 1$ si y sólo si $n \mid m$.*
5. *n es el menor entero positivo m tal que $g^m = 1$.*
6. $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$ *con los g^i distintos dos a dos cuando $0 \leq i < n$.*

Demostración. Por el Primer Teorema de Isomorfía se tiene $\langle g \rangle = \mathrm{Im}\,(\mu_g) \cong \mathbb{Z}/\mathrm{Ker}\,(\mu_g)$, y además sabemos que $\mathrm{Ker}\,(\mu_g)$ es de la forma $n\mathbb{Z}$ para un único $n \geq 0$ y que $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ tiene exactamente n elementos si $n > 0$ y es infinito si $n = 0$. Usando esto, la equivalencia entre 1, 2 y 3 es clara. También es obvio a partir de las definiciones que 3 es equivalente a 4. Dejaremos que el lector compruebe que 4 implica 5 y que 5 implica 3. Como es obvio que 6 implica 1, sólo falta demostrar que 3 implica 6.

Supongamos pues que se verifica 3. Entonces los g^i son distintos dos a dos cuando $0 \leq i < n$, pues una relación $g^i = g^j$ con $0 \leq i < j < n$ implicaría que $0 < j - i < n$ y que $j - i \in \mathrm{Ker}\,(\mu_g) = n\mathbb{Z}$, lo cual es absurdo. Además, todo elemento $g^m \in \langle g \rangle$ está en $\{1, g, g^2, \dots, g^{n-1}\}$, pues dividiendo con resto encontramos $q, i \in \mathbb{Z}$ con $m = nq + i$ y $0 \leq i < n$, y entonces tenemos $g^m = (g^n)^q g^i = 1^q g^i = g^i$. Por tanto, se verifica la condición 6. □

Aplicando el Teorema de Lagrange se obtiene:

Corolario 5.8.4 *Si G es un grupo finito entonces el orden de cualquier elemento g de G es finito y divide al orden de G. En particular se tiene $g^{|G|} = 1$.*

Obsérvese que el Teorema de Euler (1.8.1) puede obtenerse como una consecuencia inmediata de este último resultado.

Proposición 5.8.5 *Las condiciones siguientes son equivalentes para un elemento g de un grupo G:*

1. $o(g) = \infty$.
2. *$\mu_g : \mathbb{Z} \to G$ es inyectiva.*
3. *Los elementos g^m (con $m \in \mathbb{Z}$) son distintos dos a dos.*
4. $\mathrm{Ker}\,(\mu_g) = 0$*; es decir, $g^m \neq 1$ para todo $m \geq 1$.*
5. *El subgrupo $\langle g \rangle$ es isomorfo a $\mathbb{Z}$.*

Demostración. De la Proposición 5.8.3 deducimos que 1 implica 2, pues si μ_g no fuera inyectiva entonces se tendría Ker $(\mu_g) = n\mathbb{Z}$ con $n \geq 1$, lo que implicaría $o(g) = n < \infty$. La equivalencia entre 2, 3 y 4 es evidente, y también lo es que 4 implica 5. Por último, como $\mathbb{Z}$ es infinito, 5 implica 1. □

Nuestros primeros ejemplos de grupos cíclicos fueron $\mathbb{Z}$ y los $\mathbb{Z}_n$ con $n \geq 1$. Una consecuencia inmediata de los resultados precedentes es que, esencialmente, no hay otros ejemplos:

Teorema 5.8.6 (Clasificación de los Grupos Cíclicos) *Salvo isomorfismos, $\mathbb{Z}$ es el único grupo cíclico infinito y $\mathbb{Z}_n$ es el único grupo cíclico finito con n elementos ($n \in \mathbb{Z}^+$). En otras palabras, todo grupo cíclico infinito es isomorfo a $\mathbb{Z}$, y todo grupo cíclico finito G es isomorfo a $\mathbb{Z}_{|G|}$.*

Esto, a su vez, nos permite refinar el Corolario 5.5.6, con lo que avanzamos en nuestro objetivo de describir los grupos en términos de su orden.

Teorema 5.8.7 *Si p es un entero positivo primo entonces, salvo isomorfismos, $\mathbb{Z}_p$ es el único grupo finito de orden p.*

Vamos a obtener otros dos corolarios del Teorema 5.8.6 usando las descripciones de los subgrupos y cocientes de $\mathbb{Z}$ y de los $\mathbb{Z}_n$ que hemos obtenido en los Ejemplos 5.4.3, 5.6.6 y 5.7.10. El segundo corolario nos dice que los grupos cíclicos finitos verifican el recíproco del Teorema de Lagrange con una condición extra de unicidad.

Corolario 5.8.8 *Los subgrupos y los grupos cociente de un grupo cíclico son cíclicos.*

Corolario 5.8.9 *Sea $G = \langle g \rangle$ un grupo cíclico de orden finito n. Entonces, para cada divisor positivo m de n, existe un único subgrupo de orden m en G; a saber, $\langle g^k \rangle$ con $k = n/m$.*

Ejercicio 5.8.10 *Mostrar un grupo finito G que tenga al menos un subgrupo de orden m para cada divisor m de $|G|$ y tenga más de uno para cierto divisor.*

Una consecuencia más del Teorema de Clasificación de los Grupos Cíclicos (5.8.6) es la siguiente:

Proposición 5.8.11 *Sea g un elemento de un grupo G; entonces:*

1. *Si $o(g)$ es infinito entonces los únicos elementos de $\langle g \rangle$ que generan todo $\langle g \rangle$ son g y g^{-1}.*
2. *Si $o(g) = n$ es finito y k es cualquier entero, entonces*

$$o(g^k) = \frac{n}{\text{mcd}(n,k)}.$$

En consecuencia, los elementos de $\langle g \rangle$ que generan todo $\langle g \rangle$ son exactamente los g^k en los que k es coprimo con n.

Demostración. Por el Teorema 5.8.6, si $o(g)$ es infinito podemos suponer que $\langle g \rangle = \mathbb{Z}$ y que $g = 1$, y el apartado 1 es entonces evidente. Supongamos pues que $o(g)$ es finito y vale n. Podemos suponer que $\langle g \rangle = \mathbb{Z}_n$ y que $g = [1]$. Sólo hay entonces que demostrar que el orden de $[k]$ en $\mathbb{Z}_n$ es n/d, donde $d = \text{mcd}(n,k)$. El subgrupo de $\mathbb{Z}_n$ generado por $[k]$ es $\langle k, n \rangle / \langle n \rangle = \langle d \rangle / \langle n \rangle$, que, como vimos en los Ejemplos 5.6.6, tiene n/d elementos, con lo que el resultado queda demostrado. □

5.9 Conjugación y Ecuación de Clases

El concepto de elementos conjugados y de clases de conjugación es muy importante en Teoría de Grupos, y lo emplearemos con frecuencia en el resto del curso. En esta sección, además de las definiciones y propiedades elementales, establecemos la Ecuación de Clases, que es una herramienta fundamental para contar elementos en un grupo finito, y la empleamos para demostrar algunos resultados en los que se establecen propiedades de un grupo en función sólo de su orden.

Definición 5.9.1 *Sea G un grupo y sean $a, x \in G$. El* conjugado *de a por x es el elemento $a^x = x^{-1}ax$; un elemento $b \in G$ es un conjugado de a si es de la forma $b = a^x$ para algún $x \in G$. Si A es un subconjunto de G llamamos* conjugado *de A por x al subconjunto $A^x = \{a^x : a \in A\}$.*

La notación a^x para el producto $x^{-1}ax$ es útil en muchas situaciones. Aunque aparentemente puede confundirse con la notación introducida al principio de la Sección 5.1, la naturaleza del exponente (elemento del grupo multiplicativo que estemos manejando o número entero) nos sacará de dudas en cada caso concreto.

En un grupo abeliano es claro que $a^x = a$ para cada x, luego en el contexto abeliano la conjugación no tiene interés. Las propiedades elementales de la conjugación son fáciles de demostrar, y las proponemos como ejercicio.

Ejercicio 5.9.2 *Sea G un grupo y sean $a, b, x \in G$. Demostrar que:*

1. $(a^x)^{-1} = (a^{-1})^x$.
2. $(ab)^x = a^x b^x$.
3. $o(a^x) = o(a)$.
4. *Si H es un subgrupo de G entonces H^x es un subgrupo de G del mismo orden que H (los subgrupos de este tipo se dice que son* conjugados *de H).*
5. *Si A y B son subconjuntos de G entonces $A \subseteq B \Leftrightarrow A^x \subseteq B^x$.*
6. $a^x = a \Leftrightarrow ax = xa$.
7. $b = a^x \Leftrightarrow xb = ax \Leftrightarrow a = b^{(x^{-1})}$.
8. $a^{xy} = (a^x)^y$.
9. *La relación "ser conjugados" es una relación de equivalencia en G.*

Ejercicio 5.9.3 *Dados un grupo G y un subgrupo N, demostrar que las siguientes condiciones son equivalentes:*

1. *N es normal en G.*
2. *$N^x = N$ para cada $x \in G$ (es decir, N coincide con todos sus conjugados).*
3. *$N^x \subseteq N$ para cada $x \in G$ (es decir, N contiene a todos sus conjugados).*

Ejercicio 5.9.4 *Dado un grupo G, demostrar que:*

1. *Dado $x \in G$, la aplicación $t_x : G \to G$ dada por $t_x(a) = xax^{-1}$ (*conjugación *por x^{-1}) es un automorfismo de G, con inverso $t_{x^{-1}}$, llamado* automorfismo interno (o interior) *de G inducido por x. Los elementos fijados por t_x son precisamente los que pertenecen al centralizador* $\mathrm{Cen}_G(x)$.
2. *El conjunto* $\mathrm{Inn}(G)$ *de los automorfismos internos de G es un subgrupo normal del grupo* $\mathrm{Aut}(G)$ *(Ejemplo 5.3.8) que se denomina* grupo de los automorfismos internos *de G.*
3. *La aplicación $t : G \to \mathrm{Aut}(G)$ dada por $x \mapsto t_x$ es un homomorfismo de grupos con imagen* $\mathrm{Inn}(G)$ *y núcleo $Z(G)$ (el centro de G). En consecuencia,* $\mathrm{Inn}(G) \cong G/Z(G)$.

Las clases de equivalencia para la relación "ser conjugados" en un grupo G se llaman *clases de conjugación* de G, de modo que G es la unión disjunta de sus clases de conjugación. La clase de conjugación de a se denota por a^G; es decir,

$$a^G = \{a^x : x \in G\}.$$

Obsérvese que todos los elementos de una clase de conjugación tienen el mismo orden.

Proposición 5.9.5 (Ecuación de Clases) *Sea G un grupo arbitrario y sea $a \in G$. Entonces:*

1. *La clase de conjugación de a es unitaria (es decir, sólo contiene al propio a) si y sólo si $a \in Z(G)$.*
2. *$|a^G| = [G : \mathrm{Cen}_G(a)]$ (donde $\mathrm{Cen}_G(a)$ es el centralizador de a). En particular, $|a^G| \cdot |\mathrm{Cen}_G(a)| = |G|$, y por tanto $|a^G|$ divide a $|G|$.*
3. *Si G es finito y Ω es un conjunto de representantes de las clases de conjugación no unitarias de G, entonces*
$$|G| = |Z(G)| + \sum_{b \in \Omega} |b^G| = |Z(G)| + \sum_{b \in \Omega} [G : \mathrm{Cen}_G(b)].$$
Esta igualdad se conoce con el nombre de Ecuación de Clases *de G.*

Demostración. 1. Es claro, pues $a^x = a$ si y sólo si $ax = xa$.

2. Pongamos $H = \mathrm{Cen}_G(a)$. Como $[G : H]$ es el cardinal del conjunto $H\backslash G$ de las clases por la derecha módulo H, el resultado estará probado si vemos que la aplicación $H\backslash G \to a^G$ dada por $Hx \mapsto a^x$ es una biyección. Las equivalencias

$$Hx = Hy \Leftrightarrow xy^{-1} \in H \Leftrightarrow axy^{-1} = xy^{-1}a \Leftrightarrow x^{-1}ax = y^{-1}ay \Leftrightarrow a^x = a^y$$

muestran que la aplicación está bien definida y es inyectiva, mientras que la suprayectividad es obvia.

3. Como las clases de conjugación constituyen una partición de G, el cardinal $|G|$ es la suma de los cardinales de cada clase de conjugación, y la ecuación de clases lo único que hace es recoger la suma de los cardinales de las clases unitarias en $|Z(G)|$ (por el apartado 1), y el resto en la suma $\sum[G : \mathrm{Cen}_G(b)]$ (por el apartado 2). □

Ejemplo 5.9.6 *Clases de conjugación en D_n.*

Sea R la rotación de ángulo $2\pi/n$ en D_n. Como $\langle R\rangle \subseteq \mathrm{Cen}_{D_n}(R^i)$ para todo i, y $\langle R\rangle$ tiene índice 2 en D_n, tenemos dos opciones:

$$\mathrm{Cen}_{D_n}(R^i) = D_n \qquad \text{ó} \qquad \mathrm{Cen}_{D_n}(R^i) = \langle R\rangle.$$

Por la Proposición 5.9.5, la clase de conjugación R^{iD_n} tiene uno o dos elementos. El primer caso se da si R^i es central, o sea, por el Ejercicio 5.3.6, si $i = 0$ o si n es par e $i = n/2$. En el segundo caso, $R^{iD_n} = \{R^i, R^{-i}\}$.

Para calcular las demás clases de conjugación, obsérvese que un elemento de D_n es una simetría respecto de una recta precisamente si deja fija una recta de $\mathbb{R}^2$. Si $g \in D_n$ y S es la simetría respecto de cierta recta L, entonces gSg^{-1} deja fija la recta gL, y por tanto es otra simetría. Si L pasa por un vértice, entonces gL también pasa por un vértice, porque g permuta los vértices. Utilizando esto, se ve fácilmente que, si n es impar, las simetrías respecto de rectas forman una clase de conjugación. Sin embargo, si n es par, las simetrías se dividen en dos clases de conjugación: una está formada por las simetrías respecto de rectas que unen dos vértices, y otra por las simetrías que unen puntos medios de lados opuestos.

El lector puede tratar de obtener los mismos resultados empleando sólo la operación en D_n, en lugar de usar argumentos geométricos.

La Ecuación de Clases nos da información sobre $|G|$, y cuando este entero tiene una factorización cómoda es posible sacarle bastante partido. Un tipo de enteros con factorización especialmente cómoda son las potencias de números primos; veamos qué cosas se pueden decir sobre este tipo de grupos:

Proposición 5.9.7 *Si $|G| = p^n$ para cierto entero primo p y cierto $n \geq 1$, entonces $Z(G) \neq \{1\}$.*

Demostración. La ecuación de clases nos dice que $p^n = |Z(G)| + \sum[G : \mathrm{Cen}_G(a)]$, y como p divide a cada $[G : \mathrm{Cen}_G(a)]$ y a p^n deducimos que p divide a $|Z(G)|$, lo que nos da el resultado. □

Cuando el orden del grupo G es p^2 se puede afirmar algo más contundente: G es abeliano. El resultado se basa en este lema, que tiene interés por sí mismo.

Lema 5.9.8 *Si $G/Z(G)$ es cíclico entonces G es abeliano (luego $G/Z(G)$ es trivial). En particular, $[G : Z(G)]$ no puede ser un entero primo para ningún grupo G.*

Demostración. Sea $Z = Z(G)$. Si G/Z es cíclico y aZ es un generador de G/Z, entonces todo elemento de G es de la forma $a^n z$, con $n \in \mathbb{Z}$ y $z \in Z$, y es elemental ver que dos elementos de esta forma conmutan. □

Proposición 5.9.9 *Si p es un entero primo, entonces todo grupo finito G de orden p^2 es abeliano.*

Demostración. Por el Teorema de Lagrange, el orden de $Z(G)$ sólo puede ser 1, p ó p^2. Como $|Z(G)| \neq 1$ por la Proposición 5.9.7, y $|Z(G)| \neq p$ por el Lema 5.9.8, ha de ser $|Z(G)| = p^2$, de modo que $G = Z(G)$. □

La Ecuación de Clases nos permite encontrar una condición que garantiza la normalidad de ciertos subgrupos de un grupo de orden p^n.

Proposición 5.9.10 *Sea G un grupo finito de orden p^n, con p primo y $n \geq 1$. Si H es un subgrupo de G de orden p^{n-1}, entonces H es normal en G.*

Demostración. Haremos inducción sobre n. Para $n = 1$, el resultado es obvio, de modo que supondremos $n > 1$. Por la Proposición 5.9.7 y el Teorema de Lagrange se tiene $|Z| = p^s$ para cierto s con $1 \leq s \leq n$. Es obvio que $ZH = HZ$, luego éste es un subgrupo de G que contiene a H (Ejercicio 5.4.10), y en consecuencia sólo hay dos opciones: o bien $HZ = H$ o bien $HZ = G$.

En el segundo caso H es normal en G. En efecto, dado $g \in G = HZ$ se tiene $g = hz$ con $h \in H$ y $z \in Z$, luego $H^g = (H^h)^z = H^h = H$.

Por tanto, podemos asumir que $HZ = H$. Entonces Z es un subgrupo normal de H, y así

$$|G/Z| = \frac{|G|}{|Z|} = \frac{p^n}{p^s} = p^{n-s} \qquad \text{y} \qquad |H/Z| = \frac{|H|}{|Z|} = \frac{p^{n-1}}{p^s} = p^{n-s-1}.$$

Si aplicamos la hipótesis de inducción al grupo $\frac{G}{Z}$ observamos que $\frac{H}{Z}$ es normal en $\frac{G}{Z}$, y ahora el resultado es consecuencia del Teorema de la Correspondencia (5.6.5). □

Grupos de orden pequeño

Como parece apreciarse por los resultados obtenidos hasta ahora, en general podremos describir mejor los grupos de orden n cuanto más sencilla sea la factorización de n en primos. En este párrafo vamos a recopilar lo que ya sabemos para algunos valores bajos de n, y a plantear algunos objetivos para el futuro.

1. Consideremos los siguientes grupos de orden 4: el grupo cíclico $\mathbb{Z}_4$, el producto $\mathbb{Z}_2 \times \mathbb{Z}_2$ y el grupo cociente Q_8/N de los Ejemplos 5.6.3. No es difícil dar explícitamente un isomorfismo entre $\mathbb{Z}_2 \times \mathbb{Z}_2$ y Q_8/N. Por otra parte, en estos dos grupos todo elemento a verifica $o(a) \mid 2$, cosa que no ocurre en $\mathbb{Z}_4$. Esto nos dice que hay al menos dos grupos de orden 4 no isomorfos, y sabemos que cualquier otro debe ser abeliano (Proposición 5.9.9). Veremos en el Capítulo 7 que de hecho no hay más.

2. Consideremos los siguientes grupos de orden 6: el grupo cíclico $\mathbb{Z}_6$, el producto $\mathbb{Z}_2 \times \mathbb{Z}_3$, S_3 y D_3. Ya vimos que los dos últimos son isomorfos (Ejercicio 5.2.9), y los dos primeros también lo son (¿por qué?). Por otra parte, $\mathbb{Z}_6$ es abeliano y S_3 no, luego no pueden ser isomorfos. Esto nos dice que hay al menos dos grupos no isomorfos de orden 6 ($\mathbb{Z}_6$ y D_3), y veremos en el Capítulo 8 que no hay más.

3. Consideremos los siguientes grupos de orden 8: el grupo cíclico $\mathbb{Z}_8$, los productos $\mathbb{Z}_2 \times \mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, y los grupos no abelianos D_4 y Q_8. Entre ellos no hay dos isomorfos: Ninguno de los abelianos puede ser isomorfo a uno de los no abelianos; D_4 y Q_8 no son isomorfos porque en el segundo sólo hay un elemento de orden 2 y en el primero hay cuatro; dejamos que el lector use argumentos de este tipo para ver que tampoco puede haber isomorfismos entre los abelianos. Esto nos dice que hay al menos cinco grupos no isomorfos de orden 8, y veremos en el Capítulo 8 que no hay más.

4. Consideremos los siguientes grupos de orden 9: el grupo cíclico $\mathbb{Z}_9$ y el producto $\mathbb{Z}_3 \times \mathbb{Z}_3$ (no los hay no abelianos por la Proposición 5.9.9). No son isomorfos porque en el segundo no hay elementos de orden 9 y en el primero sí. Veremos en el Capítulo 7 que, salvo isomorfismos, no hay más grupos de orden 9.

5. Consideremos los siguientes grupos de orden 10: el grupo cíclico $\mathbb{Z}_{10}$, el producto $\mathbb{Z}_2 \times \mathbb{Z}_5$, y el grupo no abeliano D_5. Los dos primeros son isomorfos, y desde luego no son isomorfos al no abeliano. En cuanto a grupos de orden 14 tenemos $\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7 \ncong D_7$. Veremos en el Capítulo 8 que, salvo isomorfismos, sólo hay estos dos grupos de cada uno de los órdenes 10 y 14.

6. Veremos en el Capítulo 8 que, salvo isomorfismos, sólo hay un grupo de orden 15 (¿cuál crees que va a ser?), y hay exactamente 5 grupos de orden 12.

5.10 Problemas

1. Decir cuáles de los siguientes conjuntos y operaciones son grupos.
   (a) El conjunto $\mathbb{N}$ con la operación máximo común divisor.
   (b) El conjunto $\mathbb{N}$ con la operación mínimo común múltiplo.
   (c) El conjunto $\mathbb{R}$ con la operación $a * b = a + b + ab$.
   (d) El conjunto $A = \{x \in \mathbb{R} : -1 < x < 1\}$, con la operación $x * y = \frac{x+y}{1+xy}$.

2. Construir la tabla de multiplicación de los siguientes grupos.
   (a) Los grupos de unidades de $\mathbb{Z}_7$ y $\mathbb{Z}_{16}$.
   (b) $\mathrm{GL}_2(\mathbb{Z}_2)$.
   (c) El subgrupo de $\mathrm{GL}_2(\mathbb{C})$ generado por las matrices
   $$a = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$
   (d) El subgrupo de $\mathrm{GL}_2(\mathbb{C})$ generado por las matrices
   $$a = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
   donde $\omega = \frac{1+\sqrt{-3}}{2}$.
   (e) El subgrupo de $\mathrm{GL}_2(\mathbb{Q})$ generado por las matrices
   $$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$
   (f) El grupo cociente $G/\langle -I \rangle$, donde G es el grupo del apartado anterior e I es la matriz identidad.
   (g) El grupo de los automorfismos del grupo $\mathbb{Z}_5$.

(h) El subgrupo del grupo de la permutaciones de $A = \mathbb{R} \setminus \{0, 1, 2\}$ generado por f y g, donde

$$f(x) = 2 - x \qquad \text{y} \qquad g(x) = \frac{2}{x}.$$

(i) $\mathbb{Z}_{16}$ con la operación $x * y = x + (-1)^x + y$.

Decidir si alguno de estos grupos es isomorfo a algún otro grupo conocido.

3. Construir el diagrama de los subgrupos de los grupos anteriores, indicando cuáles de ellos son normales.

4. Sea $f : G \to H$ un isomorfismo de grupos. Demostrar (mientras no se considere una pérdida de tiempo) que:

(a) Los elementos a y a' conmutan en G si y sólo si $f(a)$ y $f(a')$ conmutan en H.

(b) G es abeliano si y sólo si H es abeliano.

(c) El orden de a en G coincide con el orden de $f(a)$ en H.

(d) Un subconjunto K de G es un subgrupo de G si y sólo si $f(K)$ es un subgrupo de H. En este caso, los índices $[G : K]$ y $[H : f(K)]$ coinciden.

(e) Un subconjunto N de G es un subgrupo normal de G si y sólo si $f(N)$ es un subgrupo normal de H.

(f) Un subconjunto X de G genera el subgrupo K si y sólo si el subconjunto $f(X)$ de H genera el subgrupo $f(K)$.

(g) G es cíclico si y sólo si H es cíclico.

(h) Si Z es el centro de G entonces $f(Z)$ es el centro de H.

(i) Si C es el centralizador de a en G entonces $f(C)$ es el centralizador de $f(a)$ en H.

(j) Un subconjunto C de G es una clase de conjugación de G si y sólo si $f(C)$ es una clase de conjugación de H.

5. Probar que todo grupo G de orden menor o igual a cinco es abeliano.

6. Sean H, K y L subgrupos de un grupo G con $H \subseteq L$. Probar que $(HK) \cap L = H(K \cap L)$. Esta identidad de conoce como *identidad de Dedekind*.

7. Sea G un grupo. Para cada una de las dos afirmaciones que siguen, dar una demostración o poner un contraejemplo:

(a) Para cada $a \in G$, existe un $a' \in G$ tal que $aa'a = 1$.

(b) Para cada $a \in G$, existe un $a' \in G$ tal que $a'aa' = 1$.

(c) G posee a lo sumo un elemento a que verifica $a^2 = a$.

8. Sea G un grupo. Probar que las siguientes afirmaciones son equivalentes:

(a) G es abeliano.

(b) $(ab)^2 = a^2b^2$ para cualesquiera $a, b \in G$.

(c) $(ab)^{-1} = a^{-1}b^{-1}$ para cualesquiera $a, b \in G$.

(d) $(ab)^n = a^nb^n$ para todo $n \in \mathbb{N}$ y para cualesquiera $a, b \in G$.

(e) [*] $(ab)^n = a^nb^n$ para tres enteros consecutivos fijos y para cualesquiera $a, b \in G$.

Probar, además, que la última condición no es equivalente a las demás si se sustituye "tres" por "dos".

9. Mostrar que la unión de dos subgrupos de un grupo no es necesariamente un subgrupo. Aún más, probar que un grupo nunca puede expresarse como unión de dos subgrupos propios.

10. Para $n = 1, \ldots, 10$, determinar cuáles de los grupos $\mathbb{Z}_n^*$ son cíclicos.

11. Supongamos que H y K son dos subgrupos de un grupo G, tales que existe una clase lateral por la derecha de G módulo H que es igual a otra de G módulo K. Probar que $H = K$.

12. Sea G un grupo arbitrario. Mostrar que si K y L son subgrupos de G de índice finito y $K \subseteq L$ entonces $[G : K] = [G : L] \cdot [L : K]$.

13. Sea G un grupo con subgrupos H y K. Demostrar que, si la intersección de dos clases laterales Hx y Ky no es vacía, entonces es una clase lateral módulo $H \cap K$. Deducir que si H y K tienen índice finito en G, entonces también lo tiene $H \cap K$.

14. Calcular el orden de cada elemento de los grupos D_n.

15. Calcular el orden en S_5 de la permutación $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$.

16. Demostrar las siguientes variantes del Teorema Chino de los Restos:

    (a) Si $G_1, \ldots, G_r$ son grupos cíclicos finitos de órdenes $n_1, \ldots, n_r$, entonces $G = G_1 \times \ldots \times G_r$ es cíclico (de orden $n_1 \cdots n_r$) precisamente si los n_i son coprimos dos a dos.

    (b) Si a y b son dos elementos de un grupo que conmutan entre si y tienen órdenes finitos n y m, entonces $\langle a, b\rangle$ es cíclico de orden nm precisamente si $\mathrm{mcd}(n, m) = 1$.

17. ¿Es cíclico el producto directo de dos grupos cíclicos infinitos?

18. Sea K un cuerpo. Demostrar que:

    (a) El subconjunto G de $\mathrm{GL}_2(K)$ formado por las matrices invertibles de la forma $\begin{pmatrix} \mathrm{a} & \mathrm{b} \\ 0 & \mathrm{d} \end{pmatrix}$ es un subgrupo.

    (b) El subconjunto N de las matrices de la forma $\begin{pmatrix} 1 & \mathrm{b} \\ 0 & 1 \end{pmatrix}$ es subgrupo normal de G.

    (c) El cociente G/N es abeliano.

19. Demostrar que la intersección de una familia de subgrupos normales de un grupo también es un subgrupo normal.

20. Sea H un subgrupo de un grupo G. Demostrar que $\cap_{g \in G} g^{-1}Hg$ es el mayor subgrupo normal de G contenido en H y el subgrupo generado por $\cup_{g \in G} g^{-1}Hg$ es el menor subgrupo normal de G que contiene a H.

21. Sea $\mathcal{P}$ una partición de un grupo G con la propiedad de que para cualquier par de elementos A, B de la partición, el producto $AB = \{ab : a \in A, b \in B\}$ es otro elemento de la partición. Sea N el elemento de la partición que contiene al neutro $1 \in G$. Probar que N es un subgrupo normal de G y que $\mathcal{P}$ consiste en las clases laterales de G módulo N.

22. Demostrar que la propiedad de "ser normal" no es transitiva. Es decir, dar un ejemplo de un grupo G con subgrupos H y K tales que H sea normal en K, K sea normal en G, y H no sea normal en G.

23. Un grupo se dice que es *simple* si no tiene ningún subgrupo normal propio no trivial. Un *subgrupo normal maximal* del grupo G es un subgrupo normal propio de G que no está contenido propiamente en ningún subgrupo normal propio de G. Demostrar que N es un subgrupo normal maximal de G si y sólo si G/N es simple. Demostrar que si N es un subgrupo normal maximal de G y H es un subgrupo de G que no está contenido en N, entonces $N \cap H$ es un subgrupo normal maximal de H.

24. Encontrar todos los grupos cíclicos G, salvo isomorfismos, que tengan exactamente dos generadores (es decir, tales que existan exactamente dos elementos $x \in G$ con $G = \langle x\rangle$).

25. Sean a, b dos elementos en un grupo G y sea $c = [a, b] = aba^{-1}b^{-1}$ su *conmutador*. Probar que, si c conmuta con a y con b, entonces se verifica, para todo par r, s de enteros positivos, $[a^r, b^s] = c^{rs}$.

26. Probar que todo grupo de orden par posee un elemento de orden 2.

27. Sean H y K subgrupos de un grupo G, y sea $g \in G$ cualquiera. El conjunto $HgK = \{x \in G : x = hgk$ para ciertos $h \in H, k \in K\}$ se llama una *doble clase lateral*.

    (a) Probar que las dobles clases laterales son una partición de G.

    (b) ¿Es cierto que todas las dobles clases laterales tienen el mismo cardinal?

28. Sean N y M subgrupos normales de un grupo G tales que $N \cap M = \{1\}$. Probar que $nm = mn$ para todo $n \in N$ y $m \in M$.

29. Sea N un subgrupo normal de índice n de un grupo G. Demostrar que $g^n \in N$ para todo $g \in G$, y dar un ejemplo que muestre que esta propiedad falla si N no es normal en G.

30. Si N es un subgrupo normal en un grupo G y $a \in G$ tiene orden n, probar que el orden de Na en G/N es un divisor de n.

31. Si G y H son grupos, $\mathrm{Hom}(G, H)$ denota el conjunto de los homomorfismos de G a H.

    (a) Demostrar que si H es abeliano, entonces $\mathrm{Hom}(G, H)$ es un grupo con la operación natural:

    $$(\varphi\phi)(g) = \varphi(g)\phi(g), \quad (g \in G).$$

    (b) Demostrar que si G es abeliano, entonces $\mathrm{Hom}(\mathbb{Z}, G) \cong G$ y $\mathrm{Hom}(\mathbb{Z}_n, G) \cong \{g \in G : g^n = e\}$.

    (c) Calcular $\mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_8)$ y $\mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_{21})$.

    (d) Probar que $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.

    (e) Mostrar que, aun cuando G sea cíclico, $\mathrm{Aut}(G)$ no tiene por qué ser cíclico.

    (f) Describir $\mathrm{Aut}(\mathbb{Z})$.

32. Probar que si $n \mid m$ entonces existen un homomorfismo inyectivo $\mathbb{Z}_n \to \mathbb{Z}_m$ y un homomorfismo suprayectivo $\mathbb{Z}_m \to \mathbb{Z}_n$.

33. Demostrar que, si el grupo G no es abeliano, entonces existe un subgrupo abeliano de G que contiene estrictamente al centro $Z(G)$.

34. Demostrar que si H es un subgrupo de G y $g \in G$, entonces $H^g = \{h^g : h \in H\}$ es un subgrupo de H tal que $|H| = |H^g|$. Demostrar además que H es normal en G si y sólo si lo es cualquier H^g.

35. Un subgrupo H del grupo G es *característico* si, para cualquier automorfismo f de G, se verifica $f(H) \subseteq H$. Se pide:

    (a) Demostrar que todo subgrupo característico de G es un subgrupo normal de G.

    (b) Dar un ejemplo de un grupo con un subgrupo normal que no sea característico.

    (c) Si H es un subgrupo característico de G y K es un subgrupo característico de H, demostrar que K es un subgrupo característico de G.

    (d) Demostrar que el centro de un grupo es un subgrupo característico.

36. Supongamos que H es un subgrupo de un grupo G, y que ningún otro subgrupo de G contiene un subgrupo del mismo cardinal que H. Demostrar que H es un subgrupo característico (y por tanto normal) de G.

37. Sea G un grupo finito con un subgrupo normal H tal que $|H|$ y $[G : H]$ son coprimos. Si $|H| = n$, probar que H es el único subgrupo de G de orden n.

38. [*] Sea G un grupo para el que existe un $n > 1$, tal que la aplicación $x \mapsto x^n$ es un automorfismo. Probar que x^{n-1} está en el centro de G para todo $x \in G$.

39. Sean N_1 y N_2 dos subgrupos normales de dos grupos G_1 y G_2. Demostrar que $N_1 \times N_2$ es un subgrupo normal de $G_1 \times G_2$ y que

$$(G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2.$$

40. Sea $f : G \to H$ un homomorfismo de grupos y sean G_1 y H_1 dos subgrupos normales de G y H, respectivamente, tales que $f(G_1) \subseteq H_1$. Demostrar que existe un único homomorfismo de grupos $\bar{f} : G/G_1 \to H/H_1$ que hace conmutativo el siguiente diagrama, donde las flechas verticales designan las proyecciones canónicas:

$$\begin{array}{ccc} G & \stackrel{f}{\to} & H \\ \downarrow & & \downarrow \\ G/G_1 & \stackrel{\bar{f}}{\to} & H/H_1 \end{array}$$

Identificar Ker $(\bar{f})$ e Im $(\bar{f})$ en función de G_1, H_1, Ker (f) e Im (f).

41. Sean H y N subgrupos de G. Supongamos que H tiene orden finito, que N tiene índice finito en G y que $|H|$ y $[G : N]$ son coprimos. Se pide:

    (a) Mostrar que si N es normal en G, entonces $H \subseteq N$.

    (b) Mostrar que si H es normal en G, entonces $[NH : N] = [H : N \cap H]$.

    (c) Deducir que si H es normal en G, entonces $H \subseteq N$.

42. Sea K un subgrupo normal finito de un grupo G, sea n un entero positivo coprimo con $|K|$, y sea $x \in G$. Probar:

    (a) Si $o(x) = n$ entonces el orden de xK en el grupo cociente G/K es también n.

    (b) Si el orden de xK en el cociente es n, entonces existe $y \in G$ de orden n tal que $xK = yK$.

43. [*] Sean a y p enteros con p primo impar. Demostrar que el polinomio $X^2 - [a]_p$ tiene una raíz en $\mathbb{Z}_p$ precisamente si $a^{(p+1)/2} \equiv a \bmod p$.

44. Sea p un entero primo. Comprobar que $\mathbb{Z}_{p^\infty} = \{a/b + \mathbb{Z} \in \frac{\mathbb{Q}}{\mathbb{Z}} : a, b \in \mathbb{Z}, b = p^n \text{ para algún } n \in \mathbb{N}\}$ es un subgrupo infinito de $\mathbb{Q}/\mathbb{Z}$ en el que el orden de cada elemento es una potencia de p.

45. Demostrar que, si G el grupo diédrico D_4 o el de cuaterniones Q_8, entonces $Z(G) \cong \mathbb{Z}_2$ y $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, y sin embargo $D_4 \ncong Q_8$.

46. Probar que, salvo isomorfismos, sólo hay dos grupos no abelianos de orden 8. ¿Cuáles son?

47. Probar que todo grupo no abeliano de orden 6 es isomorfo a S_3.

48. Sean N_1 y N_2 subgrupos normales de G_1 y G_2 respectivamente. Dar ejemplos que muestren que cada una de las siguientes implicaciones es falsa.

    (a) $G_1 \cong G_2, N_1 \cong N_2 \Rightarrow G_1/N_1 \cong G_2/N_2$.

    (b) $G_1 \cong G_2, G_1/N_1 \cong G_2/N_2 \Rightarrow N_1 \cong N_2$.

    (c) $N_1 \cong N_2, G_1/N_1 \cong G_2/N_2 \Rightarrow G_1 \cong G_2$.

49. Probar las siguientes afirmaciones sobre el grupo abeliano $\mathbb{Q}$ de los números racionales.

    (a) Si un subgrupo H de $\mathbb{Q}$ es finitamente generado, entonces H es cíclico.

    (b) $\mathbb{Q}$ no es cíclico; ni siquiera es finitamente generado.

50. Demostrar que si H es un subgrupo abeliano de un grupo G tal que $HZ(G) = G$, entonces G es abeliano. Deducir que si $G/Z(G)$ es cíclico, entonces G es abeliano.

51. Describir todos los subgrupos normales del grupo diédrico D_n.

52. [*] Demostrar que el grupo de automorfismos de D_n tiene $n\phi(n)$ elementos, donde ϕ denota la función de Euler.

53. Calcular los centros de $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$, $\mathrm{SL}_n(\mathbb{R})$ y $\mathrm{SL}_n(\mathbb{C})$.

54. Demostrar que un grupo es finito precisamente si tiene un número finito de subgrupos.

55. Si p es primo, probar que el centro de cualquier grupo no abeliano de orden p^3 tiene orden p.

56. Sea G un grupo con un subgrupo N. Demostrar que N es normal en G si y sólo si N es la unión de ciertas clases de conjugación de G.

57. [*] Sea G un grupo abeliano finito en el que, para cada $n \in \mathbb{Z}^+$, la ecuación $x^n = e$ tiene a lo sumo n soluciones. Demostrar que G es cíclico. Deducir que un subgrupo finito del grupo de unidades de un dominio es cíclico. (Indicación: Elegir un elemento de orden máximo y observar que para cada $g \in G$ de orden n, el subgrupo $\langle g \rangle$ contiene n soluciones de la ecuación $x^n = e$.)

Bibliografía del capítulo

Allenby [1], Clark [9], Delgado-Fuertes-Xambó [11], Dorronsoro-Hernández [13], Herstein [20], Jacobson [23], Rotman [30].

Capítulo 6

Grupos de permutaciones

Se estudian los grupos de permutaciones en un conjunto finito y sus subgrupos alternados.

Introducción

El grupo simétrico S_n (grupo de permutaciones de un conjunto finito de n elementos) no es sólo un ejemplo relevante de grupos no abelianos finitos, sino que tiene una gran importancia teórica e histórica en el desarrollo de las Ciencias que se manifiesta en muy diversas situaciones. Nosotros ya conocemos el Teorema de Cayley, y de hecho representaremos en la práctica algunos grupos finitos como subgrupos de grupos simétricos. La aplicación teórica fundamental de los grupos simétricos se verá en la asignatura Ecuaciones Algebraicas de Tercer Curso.

El primer objetivo de este capítulo es conseguir una representación cómoda de los elementos de S_n que nos permita operarlos con facilidad. Para ello describimos unos elementos sencillos de S_n, los ciclos, y demostramos que toda permutación de S_n admite una expresión, única salvo el orden, como producto de ciclos "disjuntos". Esta expresión, fácil de obtener en la práctica, permite calcular automáticamente el orden y la clase de conjugación de un elemento de S_n, y proporciona diversos sistemas generadores cómodos de S_n.

En la segunda parte del capítulo definimos el signo (o la paridad) de una permutación y estudiamos el subgrupo alternado de S_n, formado por las permutaciones pares. Los grupos alternados A_n nos permiten obtener un contraejemplo para el recíproco del Teorema de Lagrange (cuando $n = 4$) y nos proporcionan una familia de grupos simples (cuando $n \geq 5$) que, en el curso de Ecuaciones Algebraicas, se usarán para demostrar un importante teorema sobre la irresolubilidad por radicales de ecuaciones polinómicas de grado ≥ 5.

Objetivos del capítulo

- Saber expresar una permutación σ de S_n como producto de ciclos disjuntos, y calcular a partir de esa expresión el orden y la clase de conjugación de σ, así como el conjugado de σ por cada elemento τ de S_n.

- Conocer el concepto de signo de una permutación, sus propiedades y las formas de calcularlo.

- Conocer el grupo alternado y sus propiedades básicas.

- Conocer distintos sistemas generadores de los grupos simétricos y alternados.

- Conocer el concepto de grupo simple y el Teorema de Abel sobre la simplicidad de los grupos alternados A_n para $n \geq 5$.

Desarrollo de los contenidos

6.1 Ciclos y trasposiciones

Recordemos que, para cada número natural n, S_n denota el grupo simétrico sobre $\mathbb{N}_n$; es decir, el grupo de las aplicaciones biyectivas $f : \mathbb{N}_n \to \mathbb{N}_n$ con la composición de aplicaciones como operación. Generalizando la notación que introdujimos en el Ejercicio 5.2.5, describiremos a veces un elemento $f \in S_n$ dando la lista de sus imágenes en la forma

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

Esta notación puede ser bastante incómoda, y en esta primera sección la simplificamos destacando ciertos elementos que además nos proveen con sistemas de generadores "cómodos" de S_n.

Definición 6.1.1 *Diremos que una permutación $\sigma \in S_n$* fija *un entero $i \in \mathbb{N}_n$ si $\sigma(i) = i$; en caso contrario diremos que σ* cambia *o* mueve *i, y denotaremos por $M(\sigma)$ al conjunto de los enteros cambiados por σ:*

$$M(\sigma) = \{i \in \mathbb{N}_n : \sigma(i) \neq i\}.$$

Es claro que $M(\sigma)$ es vacío si y sólo si $\sigma = 1$, y que $M(\sigma)$ no puede tener exactamente un elemento.

Diremos que dos permutaciones σ y τ de S_n son disjuntas *si lo son los conjuntos $M(\sigma)$ y $M(\tau)$. Es decir, si todos los elementos que cambia una de ellas son fijados por la otra.*

Cuando digamos que ciertas permutaciones $\sigma_1, \dots, \sigma_r$ son disjuntas entenderemos que lo son dos a dos.

Ejercicio 6.1.2 *Sean $\sigma, \tau \in S_n$. Demostrar que $M(\sigma) = M(\sigma^{-1})$, y que si σ y τ son disjuntas entonces conmutan ($\sigma\tau = \tau\sigma$) y se tiene $M(\sigma\tau) = M(\sigma) \cup M(\tau)$.*

Definición 6.1.3 *La permutación $\sigma \in S_n$ es un* ciclo *de longitud s (o un s-ciclo) si $M(\sigma)$ tiene s elementos y éstos pueden ordenarse de manera que se tenga $M(\sigma) = \{i_1, i_2, \dots, i_s\}$ y*

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \dots \quad \sigma(i_{s-1}) = i_s, \quad \sigma(i_s) = i_1.$$

Obsérvese que para cualquier $i \in M(\sigma)$ se tiene $M(\sigma) = \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{s-1}(i)\}$.

Por ejemplo, los siguientes elementos de S_4 son ciclos de longitudes 2, 3 y 4, respectivamente:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \qquad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

Buscamos una representación más sencilla de las permutaciones, y ésta depende de probar que toda permutación es producto de ciclos, cosa que haremos pronto, y de encontrar una representación adecuada para los ciclos. Esto último es fácil: como está claro que un ciclo σ queda determinado por la descripción de $M(\sigma)$ en el orden adecuado, denotaremos el ciclo general de la Definición 6.1.3 por

$$\sigma = (i_1\ i_2\ i_3\ \dots\ i_s) \qquad \text{ó} \qquad \sigma = (i_1, i_2, i_3, \dots, i_s).$$

Obsérvese que esta representación no es única. Por ejemplo, los ciclos de S_4 que hemos dado como ejemplo se escribirán así (lo que ayuda a justificar el nombre de ciclo):

$$\alpha = (1\ 4) = (4\ 1) \qquad \beta = (2\ 4\ 3) = (4\ 3\ 2) = (3\ 2\ 4) \qquad \gamma = (1\ 3\ 4\ 2) = (3\ 4\ 2\ 1) = (4\ 2\ 1\ 3) = (2\ 1\ 3\ 4).$$

Ejercicio 6.1.4 *Sea $\sigma = (i_1 \dots i_s)$ un ciclo de longitud s en S_n. Demostrar que:*

1. *Para cada $t \in \{2, \dots, s\}$ se tiene $\sigma = (i_t \dots i_s\ i_1 \dots i_{t-1})$.*
2. *Para cada $t \in \{2, \dots, s\}$ se tiene $i_t = \sigma^{t-1}(i_1)$.*
3. *El orden de σ coincide con su longitud s.*

El resultado que nos da la representación buscada de las permutaciones de S_n es el siguiente:

Teorema 6.1.5 *Toda permutación $\sigma \neq 1$ de S_n se puede expresar de forma única (salvo el orden) como producto de ciclos disjuntos.*

Demostración. Definimos en $M(\sigma) \neq \emptyset$ la siguiente relación binaria:

$$i \equiv j \Leftrightarrow \text{ existe } n \in \mathbb{Z} \text{ tal que } \sigma^n(i) = j.$$

Dejamos que el lector compruebe que $\equiv$ es una relación de equivalencia.

Fijado $i \in M(\sigma)$, sea s el menor entero positivo tal que $\sigma^s(i) = i$ (¿por qué existe uno?). Entonces la clase de equivalencia que contiene a i es $\{i, \sigma(i), \sigma^2(i), \ldots, \sigma^{s-1}(i)\}$ (¿por qué son distintos?). En particular, $s \geq 2$, y s es el cardinal de la clase de equivalencia que contiene a i.

Sea ahora $\{i_1, \ldots, i_k\}$ un conjunto de representantes de las clases de equivalencia de $\equiv$; es decir, el conjunto tiene exactamente un elemento de cada clase de equivalencia. Para cada $j = 1, \ldots, k$, sea s_j el cardinal de la clase de i_j. Entonces $\sigma = \tau_1 \cdots \tau_k$ es la factorización buscada, donde

$$\tau_j = (i_j, \sigma(i_j), \sigma^2(i_j), \ldots, \sigma^{s_j-1}(i_j)).$$

El orden de los ciclos se puede alterar por la propia demostración o por el Ejercicio 6.1.2, y también de la demostración se deduce la unicidad salvo el orden, pues si $\sigma = \tau_1 \cdots \tau_k$ es una factorización de σ en producto de ciclos disjuntos, entonces las clases de equivalencia de $\equiv$ son los conjuntos $M(\tau_1), \ldots, M(\tau_k)$. □

Ejemplo 6.1.6 *Factorización de una permutación como producto de ciclos disjuntos.*
Consideremos la permutación de S_{11}

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 6 & 5 & 1 & 4 & 2 & 7 & 3 & 8 & 11 & 9 & 10 \end{pmatrix}.$$

Elegimos un elemento arbitrario cambiado por σ, por ejemplo el 1, y calculamos sus imágenes sucesivas por σ:

$$\sigma(1) = 6,\ \sigma^2(1) = \sigma(6) = 7,\ \sigma^3(1) = \sigma(7) = 3,\ \sigma^4(1) = \sigma(3) = 1.$$

Entonces (1 6 7 3) es uno de los factores de σ. Elegimos ahora un elemento de $M(\sigma)$ que no haya aparecido aún, por ejemplo el 2, y le volvemos a seguir la pista, lo que nos da un nuevo factor (2 5). Empezando ahora con el 9 obtenemos un tercer ciclo (9 11 10) que agota el proceso (el 4 y el 8 son fijados por σ) y nos dice que $\sigma = (1\ 6\ 7\ 3)(2\ 5)(9\ 11\ 10)$.

Veamos cómo se puede calcular el orden de una permutación en términos de su factorización como producto de ciclos disjuntos:

Proposición 6.1.7 *Sea $\sigma = \tau_1 \cdots \tau_k$ la factorización de una permutación σ como producto de ciclos disjuntos, y sea s_i la longitud del ciclo τ_i. Entonces*

$$o(\sigma) = \text{mcm}(s_1, \ldots, s_k).$$

Demostración. Sea $m \in \mathbb{N}$. Como los τ_i conmutan entre sí, se tiene $\sigma^m = \tau_1^m \cdots \tau_k^m$. Por otra parte, para cada i se tiene $M(\tau_i^m) \subseteq M(\tau_i)$ y por tanto los τ_i^m son disjuntos. Esto implica, por la unicidad en el Teorema 6.1.5, que $\sigma^m = 1$ precisamente si cada $\tau_i^m = 1$, y entonces el resultado es claro, pues s_i es el orden de τ_i. □

A continuación vamos a describir las clases de conjugación de S_n.

Definición 6.1.8 *El* tipo *de una permutación $\sigma \neq 1$ de S_n es la lista $[s_1, \ldots, s_k]$ de las longitudes de los ciclos que aparecen en su factorización en ciclos disjuntos, ordenadas en forma decreciente. Por convenio, la permutación identidad tiene tipo* [1].

Por ejemplo, el tipo de un s-ciclo es $[s]$, el de la permutación $(1\ 2)(3\ 4\ 5)(6\ 7) \in S_7$ es $[3,2,2]$, y el de la permutación de S_{11} del Ejemplo 6.1.6 es $[4,3,2]$.

Teorema 6.1.9 *Dos elementos de S_n son conjugados precisamente si tienen el mismo tipo. En consecuencia, cada clase de conjugación de S_n está formada por todos los elementos de un mismo tipo.*

Demostración. Fijemos una permutación α. Para un s-ciclo $\tau = (i_1\ i_2\ \ldots\ i_s)$, se comprueba fácilmente que

$$\tau^\alpha = (i_1\ i_2\ \ldots\ i_s)^\alpha = (\alpha^{-1}(i_1)\ \alpha^{-1}(i_2)\ \ldots \alpha^{-1}(i_s)), \tag{6.1.1}$$

y en particular τ^α es un s-ciclo. También es fácil ver que, si dos ciclos τ_1 y τ_2 son disjuntos, entonces lo son τ_1^α y τ_2^α. Como, en general, $(\tau_1 \cdots \tau_k)^\alpha = \tau_1^\alpha \cdots \tau_k^\alpha$, es claro que dos elementos conjugados de S_n tienen el mismo tipo.

Recíprocamente, supongamos que σ y σ' tienen el mismo tipo. Entonces las descomposiciones de σ y σ' en producto de ciclos disjuntos son de la forma $\sigma = \tau_1\tau_2\cdots\tau_k$ y $\sigma' = \tau_1'\tau_2'\cdots\tau_k'$ donde τ_i y τ_i' tienen la misma longitud. Por tanto existen biyecciones $\alpha_i : M(\tau_i') \to M(\tau_i)$ que conservan la estructura de los ciclos; es decir, si $\tau_i = (j_1\ j_2\ \ldots\ j_s)$ y $\tau_i' = (j_1'\ j_2'\ \ldots\ j_s')$, entonces $\alpha_i(j_t') = j_t$, para todo t. Además, como $|M(\sigma)| = |M(\sigma')|$, existe una biyección $\beta : \mathbb{N}_n \setminus M(\sigma') \to \mathbb{N}_n \setminus M(\sigma)$. Sea ahora $\alpha \in S_n$ la biyección que se obtiene "pegando" las α_i y β. Es decir, $\alpha(x) = \alpha_i(x)$ si $x \in M(\tau_i')$ y $\alpha(x) = \beta(x)$ si $x \notin M(\sigma')$. De 6.1.1 se deduce que $\tau_i' = \tau_i^\alpha$, para todo i y, por tanto $\sigma' = \sigma^\alpha$. □

Observación 6.1.10 *De la primera parte de la demostración anterior se deduce que la factorización en ciclos disjuntos de σ^α se obtiene sustituyendo, en la de σ, cada elemento $i \in \mathbb{N}_n$ por $\alpha^{-1}(i)$.*

Por ejemplo, si $\alpha = (1\ 4\ 3)(2\ 5\ 6)$ y $\sigma = (1\ 3)(2\ 4\ 7)$, entonces $\sigma^\alpha = (3\ 4)(6\ 1\ 7)$.

Ejemplo 6.1.11 *Clases de conjugación de S_n.*

Las 6 permutaciones de S_3 se dividen en una permutación de tipo [1] (la identidad), tres 2-ciclos o permutaciones de tipo [2] (a saber, (1 2), (1 3) y (2 3)), y dos 3-ciclos o permutaciones de tipo [3] (a saber, (1 2 3) y (1 3 2)).

En S_4 hay más variedad, y en particular aparecen permutaciones que no son ciclos. Sus 24 permutaciones se dividen en los siguientes tipos:

Tipo	Permutaciones
[1]	1
[2]	(1 2), (1 3), (1 4), (2 3), (2 4), (3 4)
[3]	(1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3)
[4]	(1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)
[2,2]	(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)

Por tanto, cada fila de elementos a la derecha de la barra es una clase de conjugación de S_4.

Además de los ciclos, en S_5 hay permutaciones de los tipos $[2,2]$ y $[3,2]$; y en S_6 las hay de los tipos $[2,2]$, $[3,2]$, $[2,2,2]$ y $[3,3]$. En estos casos, por el gran número de elementos en los grupos, es pesado construir tablas como la que acabamos de dar para S_4, pero se puede al menos calcular cuántas permutaciones hay de cada tipo (véase el Problema 13).

Como consecuencia del Teorema 6.1.5, sabemos que el grupo simétrico S_n está generado por el conjunto de todos los ciclos. Vamos a terminar la sección mostrando otros conjuntos generadores de S_n más económicos. En particular, encontraremos uno con 2 elementos, que para $n \geq 3$ es lo menos que podemos esperar puesto que S_n no es abeliano en tal caso.

Definición 6.1.12 *Llamaremos* trasposición *de S_n a cualquier ciclo de longitud* 2.

Así, una trasposición cambia exactamente dos elementos, permutándolos entre sí. Por el Teorema 6.1.9, el conjunto de todas las trasposiciones es una clase de conjugación en S_n.

Proposición 6.1.13 *Para $n > 2$, los siguientes son conjuntos generadores de S_n:*

1. *El conjunto de todos los ciclos.*
2. *El conjunto de todas las trasposiciones.*
3. *El conjunto de $n-1$ trasposiciones: $\{(1\ 2), (1\ 3), (1\ 4), \ldots, (1\ n-1), (1\ n)\}$.*
4. *El conjunto de $n-1$ trasposiciones: $\{(1\ 2), (2\ 3), (3\ 4), \ldots, (n-1\ n)\}$.*
5. *El conjunto de una trasposición y un n-ciclo: $\{(1\ 2), (1\ 2\ 3\ \ldots\ n-1\ n)\}$.*

Demostración. 1. Es una consecuencia inmediata del Teorema 6.1.5.

Para demostrar el resto de apartados bastará con comprobar que los elementos del conjunto dado en cada apartado se expresan como productos de los elementos del conjunto del apartado siguiente.

2. Cada ciclo $\sigma = (i_1\ i_2\ \ldots\ i_s)$ puede escribirse como producto de trasposiciones (no disjuntas):

$$\sigma = (i_1\ i_s)(i_1\ i_{s-1}) \cdots (i_1\ i_3)(i_1\ i_2).$$

3. Es consecuencia de la igualdad $(i\ j) = (1\ i)(1\ j)(1\ i)$.

4. Dado $j \geq 2$, sea $\alpha = (2\ 3)(3\ 4)(4\ 5) \cdots (j-1\ j)$. Usando la Observación 6.1.10 se obtiene $(1\ 2)^\alpha = (1\ j)$.

5. Sean $\tau = (1\ 2)$ y $\sigma = (1\ 2\ \ldots\ n-1\ n)$. Como σ^{j-1} lleva $1 \mapsto j$ y $2 \mapsto j+1$, la Observación 6.1.10 nos dice que $\sigma^{j-1}\tau\sigma^{1-j} = (j, j+1)$. □

Aunque toda permutación de S_n se puede expresar como un producto de trasposiciones, estas expresiones no tienen las buenas propiedades que vimos en las descomposiciones en ciclos. Por una parte, no podemos esperar que una permutación arbitraria sea producto de trasposiciones disjuntas (tendría orden 2). Por otra, tampoco se tiene conmutatividad (por ejemplo, $(1\ 3)(1\ 2) \neq (1\ 2)(1\ 3)$) ni unicidad, ni siquiera en el número de factores; por ejemplo

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

Nótese que en todas estas factorizaciones de $(1\ 2\ 3)$ hay un número par de trasposiciones; esto es consecuencia de un hecho general que analizaremos en la sección siguiente (Proposición 6.2.3).

6.2 Grupos alternados

Fijemos un entero positivo $n \geq 2$ y una permutación $\sigma \in S_n$. Por la Propiedad Universal de los Anillos de Polinomios, existe un homomorfismo de anillos $\bar{\sigma} : \mathbb{Z}[X_1, \ldots, X_n] \to \mathbb{Z}[X_1, \ldots, X_n]$ tal que $\bar{\sigma}(X_i) = X_{\sigma(i)}$ para cada i (Ejemplos 4.7.4). Es decir, dado un polinomio Q, su imagen $\bar{\sigma}(Q)$ se obtiene sustituyendo cada X_i por $X_{\sigma(i)}$ en la expresión de Q.

En lo que sigue, P designará al polinomio de $\mathbb{Z}[X_1, \ldots, X_n]$ dado por

$$P = \prod_{i<j}(X_j - X_i) = (X_2 - X_1)(X_3 - X_1) \cdots (X_n - X_1)(X_3 - X_2) \cdots (X_n - X_2) \cdots (X_n - X_{n-1}).$$

La condición $i < j$ implica que cada diferencia entre dos indeterminadas distintas aparece, en cierto orden, exactamente una vez en esa factorización. Como $\bar{\sigma}$ es un homomorfismo de anillos, se tiene

$$\bar{\sigma}(P) = \prod_{i<j} \bar{\sigma}(X_j - X_i) = \prod_{i<j}(X_{\sigma(j)} - X_{\sigma(i)}).$$

Como σ es una biyección, cada diferencia entre dos indeterminadas distintas sigue apareciendo, en cierto orden, exactamente una vez en esta factorización. Fijados $i < j$ pueden ocurrir dos cosas:

- Que sea $\sigma(i) < \sigma(j)$, en cuyo caso el factor $X_{\sigma(j)} - X_{\sigma(i)}$ aparece en $\bar{\sigma}(P)$ igual que en P.
- Que sea $\sigma(i) > \sigma(j)$, en cuyo caso el factor $X_{\sigma(j)} - X_{\sigma(i)}$ aparece en $\bar{\sigma}(P)$ en el orden contrario que en P; en este caso diremos que σ *presenta una inversión* para el par (i, j).

Como cada inversión se traduce en un cambio de signo en $\bar{\sigma}(P)$ con respecto a P, se tiene $\bar{\sigma}(P) = \pm P$, donde el signo es + si y sólo si el número de pares (i, j) (con $i < j$) para los que σ presenta una inversión es par. Esto sugiere las definiciones que siguen:

Definición 6.2.1 *La permutación $\sigma \in S_n$ es* par *si $\bar{\sigma}(P) = P$; es decir, si σ presenta un número par de inversiones; y es* impar *si $\bar{\sigma}(P) = -P$; es decir, si σ presenta un número impar de inversiones.*

El signo *de σ se define como $\mathrm{sg}(\sigma) = (-1)^k$, donde k es el número de inversiones que presenta σ. Es decir, $\mathrm{sg}(\sigma) = 1$ si σ es par y $\mathrm{sg}(\sigma) = -1$ si σ es impar. Por el comentario previo a esta definición se tiene $\bar{\sigma}(P) = \mathrm{sg}(\sigma)P$.*

Proposición 6.2.2 *La "aplicación signo" $\mathrm{sg} : S_n \to \mathbb{Z}^* = \{1, -1\}$ es un homomorfismo de grupos.*

Demostración. Sean $\sigma, \tau \in S_n$. Es claro que $\bar{\sigma} \circ \bar{\tau} = \overline{\sigma \circ \tau}$, y por tanto

$$\mathrm{sg}(\sigma \circ \tau)P = \overline{\sigma \circ \tau}(P) = \bar{\sigma}(\bar{\tau}(P)) = \bar{\sigma}(\mathrm{sg}(\tau)P) = \mathrm{sg}(\tau)\bar{\sigma}(P) = \mathrm{sg}(\tau)\mathrm{sg}(\sigma)P,$$

y por tanto $\mathrm{sg}(\sigma \circ \tau) = \mathrm{sg}(\sigma)\mathrm{sg}(\tau)$. □

Proposición 6.2.3 *En S_n se verifica:*

1. *El signo de una permutación σ es el mismo que el de su inversa σ^{-1} y que el de cualquiera de sus conjugadas σ^α.*
2. *Toda trasposición es impar.*
3. *Si $\sigma = \tau_1 \cdots \tau_r$, donde las τ_i son trasposiciones, entonces $\mathrm{sg}(\sigma) = (-1)^r$.*
4. *Una permutación σ es par (respectivamente impar) si y sólo si es producto de un número par (respectivamente impar) de trasposiciones.*
5. *Un ciclo de longitud s tiene signo $(-1)^{s-1}$; es decir, un ciclo de longitud par es impar, y viceversa.*
6. *La paridad de una permutación coincide con la del número de componentes pares de su tipo.*

Demostración. Por la Proposición 6.2.2, $\mathrm{sg}(\sigma)\mathrm{sg}(\sigma^{-1}) = 1$ y $\mathrm{sg}(\tau^{-1}\sigma\tau) = \mathrm{sg}(\tau)^{-1}\mathrm{sg}(\sigma)\mathrm{sg}(\tau) = \mathrm{sg}(\sigma)$, de donde se deduce 1. Ahora, como toda trasposición es conjugada de (1 2) y ésta es impar (presenta exactamente una inversión), el apartado 2 se sigue del 1, y entonces 3 y 4 son claros puesto que toda permutación es producto de trasposiciones y sg es un homomorfismo. Finalmente, el apartado 3 aplicado a la igualdad $(i_1\ i_2\ \ldots\ i_s) = (i_1\ i_s)(i_1\ i_{s-1}) \cdots (i_1\ i_3)(i_1\ i_2)$ nos da el apartado 5 y 6 es una consecuencia inmediata de 5. □

Ejemplo 6.2.4 *Calculando la paridad en función del tipo.*
Del Ejemplo 6.1.11 y del último apartado de la Proposición 6.2.3 se deduce que, además de la identidad, las permutaciones pares de S_3 son las de tipo [3]; las de S_4 son las de los tipos [3] ó [2, 2]; las de S_5 son las de los tipos [3], [5] ó [2, 2]; y las de S_6 son las de los tipos [3], [5], [2, 2] ó [3, 3].

Definición 6.2.5 *El* grupo alternado *en n elementos, denotado por A_n, es el núcleo del homomorfismo $\mathrm{sg} : S_n \to \mathbb{Z}^* = \{1, -1\}$. Es decir, es el subgrupo de S_n formado por las permutaciones pares.*

Proposición 6.2.6 *A_n es un subgrupo normal de S_n, y para $n \geq 2$ se tiene:*

$$[S_n : A_n] = 2, \qquad |A_n| = \frac{n!}{2}, \qquad y \qquad \frac{S_n}{A_n} \cong \{1, -1\} \cong \mathbb{Z}_2.$$

Demostración. Al estar definido como el núcleo de un homomorfismo, A_n es normal en S_n. El resto es consecuencia del Primer Teorema de Isomorfía si vemos que, para $n \geq 2$, el homomorfismo sg es suprayectivo, para lo que basta notar que $\mathrm{sg}(1) = 1$ y $\mathrm{sg}(1\ 2) = -1$. □

Es elemental ver que A_2 es el grupo trivial y que A_3 es el subgrupo cíclico de S_3 generado por el 3-ciclo (1 2 3), y por tanto $A_3 \cong \mathbb{Z}_3$. En el caso general, tenemos dos maneras sencillas de describir conjuntos de generadores de A_n.

Proposición 6.2.7 *Los siguientes son sistemas de generadores de A_n:*

1. *El conjunto de todos los productos de dos trasposiciones (disjuntas o no).*
2. *El conjunto de todos los 3-ciclos.*

Demostración. El apartado 1 es una consecuencia inmediata del apartado 4 de la Proposición 6.2.3. Por la misma proposición, todos los 3-ciclos están en A_n; por tanto, usando 1, para ver 2 sólo hay que probar que cada producto de dos trasposiciones distintas (disjuntas o no) se puede escribir como producto de 3-ciclos, lo que se sigue de las igualdades

$$(i\ j)(i\ k) = (i\ k\ j) \qquad \text{e} \qquad (i\ j)(k\ l) = (j\ l\ k)(i\ k\ j),$$

donde asumimos que i, j, k, l son distintos dos a dos. □

Obsérvese que, como el conjunto vacío genera el subgrupo trivial, la Proposición 6.2.7 es válida incluso cuando $n = 1$ ó $n = 2$.

A continuación describimos los subgrupos de A_4. Esto nos dará un ejemplo en el que no se verifica el recíproco del Teorema de Lagrange: A_4 tiene orden 12, pero no tiene subgrupos de orden 6.

Ejemplo 6.2.8 *Subgrupos de A_4.*
En virtud del Ejemplo 6.2.4, la siguiente es la lista completa de los elementos de A_4:

1	$\sigma = (1\ 2)(3\ 4)$	$\tau = (1\ 3)(2\ 4)$	$\eta = (1\ 4)(2\ 3)$
$\alpha = (1\ 2\ 3)$	$\beta = (1\ 2\ 4)$	$\gamma = (1\ 3\ 4)$	$\delta = (2\ 3\ 4)$
$\alpha^2 = (1\ 3\ 2)$	$\beta^2 = (1\ 4\ 2)$	$\gamma^2 = (1\ 4\ 3)$	$\delta^2 = (2\ 4\ 3)$

Por el Teorema de Lagrange, los subgrupos propios y no triviales de A_4 han de tener orden 2, 3, 4, ó 6. Los de orden 2 han de estar generados por elementos de orden 2, y por tanto son:

$$\langle\sigma\rangle = \{1, \sigma\} \qquad \langle\tau\rangle = \{1, \tau\} \qquad \langle\eta\rangle = \{1, \eta\}.$$

Como $\sigma^\alpha = \tau \notin \langle\sigma\rangle$, deducimos que $\langle\sigma\rangle$ no es normal en A_4, y del mismo modo se ve que no lo son $\langle\tau\rangle$ ni $\langle\eta\rangle$. Los subgrupos de orden 3 han de estar generados por elementos de orden 3, y por tanto son:

$$\langle\alpha\rangle = \langle\alpha^2\rangle = \{1, \alpha, \alpha^2\} \qquad \langle\beta\rangle = \langle\beta^2\rangle = \{1, \beta, \beta^2\} \qquad \langle\gamma\rangle = \langle\gamma^2\rangle = \{1, \gamma, \gamma^2\} \qquad \langle\delta\rangle = \langle\delta^2\rangle = \{1, \delta, \delta^2\}.$$

Un subgrupo de orden 4 no puede contener a ninguno de los elementos de orden 3; como el resto de elementos forman un subgrupo

$$N = \{1, \sigma, \tau, \eta\},$$

éste es el único subgrupo de orden 4, que además es normal en S_n por el Teorema 6.1.9. Por último, veamos que no hay subgrupos de orden 6. Un tal subgrupo H sería normal en A_4 por tener índice 2, por lo que también $N \cap H$ sería normal en A_4. Además se tendría $NH = A_4$ (¿por qué?) y en consecuencia $|N \cap H| = 2$ (Lema 5.4.11), en contra del hecho de que ninguno de los subgrupos de orden 2 de A_4 es normal.

Terminamos el capítulo con un resultado de notable importancia histórica, pues es una de las claves que permitió demostrar la inexistencia de una fórmula general para calcular "por radicales" las raíces de polinomios de grado 5 o superior (ver la nota al pie en el Ejemplo 9.2.2). Se trata del *Teorema de Abel*, que afirma que los grupos alternados A_n son simples cuando $n \geq 5$. Por supuesto, necesitamos la definición de grupo simple.

Definición 6.2.9 *Un grupo no trivial G es* simple *si sus únicos subgrupos normales son $\{1\}$ y G.*

Por ejemplo, todo grupo de orden primo es simple. El recíproco se verifica para grupos abelianos:

Ejercicio 6.2.10 *Demostrar que un grupo abeliano es simple precisamente si su orden es primo.*

Los grupos simples no abelianos son escasos[1]. De hecho, el grupo simple no abeliano de menor tamaño es A_5, que tiene 60 elementos (Teorema 8.4.11). Es decir, si G es un grupo simple finito entonces o bien $|G|$ es primo o bien $|G| \geq 60$.

Obsérvese que A_3 es simple, pero A_4 no lo es, como muestra el Ejemplo 6.2.8. Para demostrar el anunciado Teorema de Abel necesitamos un lema:

Lema 6.2.11 *Si un subgrupo normal H de A_n ($n \geq 5$) contiene un 3-ciclo, entonces $H = A_n$.*

Demostración. Sea σ un 3-ciclo en H. Por la Proposición 6.2.7, basta ver que cualquier otro 3-ciclo σ' está en H. Sabemos por el Teorema 6.1.9 que existe $\alpha \in S_n$ tal que $\sigma' = \sigma^\alpha$, de modo que si $\alpha \in A_n$ entonces $\sigma' \in H$, por la normalidad de H en A_n; en consecuencia, podemos suponer que α es una permutación impar. Como σ sólo cambia 3 elementos y $n \geq 5$, existe una trasposición β disjunta con σ, por lo que $\sigma^\beta = \sigma$. Por tanto

$$\sigma^{\beta\alpha} = (\sigma^\beta)^\alpha = \sigma^\alpha = \sigma',$$

y como $\beta\alpha$ está en A_n por ser el producto de dos permutaciones impares, la normalidad de H en A_n implica que $\sigma' \in H$, como queríamos ver. □

Teorema 6.2.12 (Abel) *Si $n \geq 5$, entonces A_n es un grupo simple.*

Demostración. Supongamos que $H \neq \{1\}$ es un subgrupo normal de A_n y veamos que $H = A_n$. Por el Lema 6.2.11, bastará probar que H contiene un 3-ciclo.

Por el Axioma de Buena Ordenación, podemos elegir un elemento $1 \neq \sigma \in H$ que cambie el menor número posible de elementos de $\mathbb{N}_n$; es decir, existen $1 \neq \sigma \in H$ y $r \in \mathbb{Z}^+$ tales que σ cambia exactamente r elementos, y cualquier otro $1 \neq \nu \in H$ cambia al menos r elementos. Ahora veremos que debe tenerse $r = 3$, por lo que σ será un 3-ciclo en H y habremos terminado.

Desde luego, no puede ser $r = 1$ porque ninguna permutación cambia exactamente un elemento, ni tampoco $r = 2$ porque todas las permutaciones de H son pares. Supongamos pues, en busca de una contradicción, que $r > 3$. Se tienen entonces dos posibilidades:

1. Que, en la factorización de σ en ciclos disjuntos, aparezca alguno de longitud ≥ 3.

2. Que σ sea un producto de (al menos dos) trasposiciones disjuntas.

En el primer caso, σ debe cambiar al menos 5 elementos (si sólo cambiase 4, como al menos aparece un 3-ciclo, σ sería un 4-ciclo, lo que contradice el hecho de que $\sigma \in A_n$). Podemos suponer, sin pérdida de generalidad (¿por qué?), que $1, 2, 3, 4, 5 \in M(\sigma)$ y que alguno de los ciclos disjuntos que componen σ es de la forma (1 2 3 ...) (con longitud al menos 3). Sea $\alpha = (3\ 4\ 5)$. Como $\alpha \in A_n$ y H es normal en A_n, deducimos que $\sigma^\alpha \in H$, y así $\beta = \sigma^{-1}\sigma^\alpha \in H$. Si $\sigma(i) = i$ entonces $i > 5$ y por tanto $\alpha(i) = i$, de donde se sigue que $\beta(i) = i$; por tanto $M(\beta) \subseteq M(\sigma)$, y la inclusión es estricta pues $\sigma(1) = 2$ mientras que $\beta(1) = 1$. En consecuencia, $\beta \in H$ cambia menos de r elementos, así que debe ser $\beta = 1$, por la elección de r. Esto significa que $\sigma^\alpha = \sigma$, y por tanto $\alpha\sigma = \sigma\alpha$. Pero esto es falso, pues $\alpha\sigma(2) = 4$ y $\sigma\alpha(2) = 3$, de manera que la primera de las dos posibilidades consideradas nos lleva a una contradicción.

Pasamos al segundo caso. Reordenando los elementos de $\mathbb{N}_n$ podemos asumir que $\sigma = (1\ 2)(3\ 4)\cdots$ (puede haber más trasposiciones en el producto o no). Sea de nuevo $\alpha = (3\ 4\ 5)$. Como antes, tomamos $\beta = \sigma^{-1}\sigma^\alpha \in H$. Si $i \neq 5$ y $\sigma(i) = i$ entonces $i \neq 3, 4, 5$ y por tanto $\alpha(i) = i$, de donde se sigue que $\beta(i) = i$; por tanto $M(\beta) \subseteq M(\sigma) \cup \{5\}$. Pero el 1 y el 2 son fijados por β y cambiados por σ, de modo que β cambia menos de r elementos y así $\beta = 1$, o sea $\sigma\alpha = \alpha\sigma$. Pero se tiene $\sigma\alpha(3) = 3 \neq 5 = \alpha\sigma(3)$. En cualquier caso, pues, llegamos a la contradicción que buscábamos. □

[1] La clasificación de todos los grupos simples finitos está considerada como el mayor trabajo colectivo que se ha hecho en Matemáticas. La "demostración" de este resultado, conocido como el "Teorema Enorme", se esparce en numerosos artículos de investigación y se estima que ocuparía unas 15.000 páginas. La mayoría de estos grupos se distribuyen en 4 familias infinitas con alguna característica común; dos de ellas son la familia de los grupos cíclicos de orden primo y la de los grupos alternados A_n con $n \geq 5$. Los grupos simples finitos que no pertenecen a ninguna de estas familias se llaman "esporádicos". Hay exactamente 26 grupos esporádicos; el menor tiene orden $2^4 \cdot 3^5 \cdot 5 \cdot 11 = 7.920$, y el mayor, conocido como el "grupo monstruo", tiene orden algo mayor que $8 \cdot 10^{53}$ (exactamente $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$).

6.3 Problemas

1. Se pide, para las siguientes permutaciones:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}, \quad \gamma = (4\ 5\ 6)(5\ 6\ 7)(1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5).$$

   (a) Expresarlas como producto de ciclos disjuntos.

   (b) Calcular sus órdenes.

   (c) Expresarlas como producto de las trasposiciones $(1\ 2), (2\ 3), \ldots, (n-1\ n)$.

   (d) Expresarlas como producto de las trasposiciones $(1\ 2), (1\ 3), \ldots, (1\ n-1), (1\ n)$.

   (e) Expresarlas como producto de las permutaciones $(1\ 2)$ y $(1\ 2 \cdots n-1\ n)$.

   (f) Calcular su paridad.

   (g) Expresar las que sean pares como producto de ciclos de longitud 3.

2. Calcular $\sigma\tau\sigma^{-1}$, donde

   (a) $\sigma = (1\ 3\ 5)(1\ 2)$, $\tau = (1\ 5\ 7\ 9)$.

   (b) $\sigma = (5\ 7\ 9)$, $\tau = (1\ 2\ 3)$.

3. Determinar la paridad de las siguientes permutaciones:

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

   (b) $(1\ 2\ 3\ 4\ 5)(1\ 2\ 3)(4\ 5)$.

   (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 6 & 4 & 1 & 3 & 2 \end{pmatrix}$.

4. Calcular σ^{1000}, donde $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 5 & 2 & 6 & 1 & 7 & 4 & 0 & 9 & 11 & 8 \end{pmatrix}$.

5. Se pide:

   (a) Resolver la ecuación $x(1\ 2)(3\ 4)x^{-1} = (5\ 6)(1\ 3)$ en S_6.

   (b) Probar que la ecuación $x(1\ 2\ 3)x^{-1} = (1\ 3)(5\ 7\ 8)$ no tiene solución en S_8.

   (c) Encontrar, si existen, las soluciones en S_5 de la ecuación $x(1\ 2)x^{-1} = (3\ 4)(1\ 5)$.

6. Encuentra los 13 pares para los que la permutación $\sigma = (2\ 7\ 8)(1\ 4)$ de S_8 presenta inversiones.

7. Dada la permutación $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 9 & 8 & 2 & 3 & 4 & 6 & 7 \end{pmatrix}$, calcular el orden de σ^2.

8. Probar que si $\sigma \in S_n$ es un d-ciclo y $\sigma(x) \neq x$ entonces $\sigma = (x\ \sigma(x) \cdots\ \sigma^{d-1}(x))$.

9. Sea $\sigma \neq 1$ una permutación de S_n; entonces:

   (a) σ es un ciclo si y sólo si, para cualesquiera $j, k \in M(\sigma)$, existe un entero m tal que $\sigma^m(j) = k$.

   (b) Si σ es producto de dos o más ciclos disjuntos, entonces σ no es un ciclo.

10. Probar que para toda permutación $\sigma \in S_n$ se cumple $\sigma(i_1 \cdots i_r)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_r))$.

11. Demostrar que una permutación tiene orden primo p si y sólo si se factoriza como un producto de ciclos disjuntos, cada uno de longitud p.

12. Demostrar que para todo $1 \leq k < n$, S_n tiene al menos $\binom{n}{k}$ subgrupos isomorfos a $S_k \times S_{n-k}$ y que todos son conjugados; es decir, para dos de estos grupos H y K existe $\sigma \in G$ tal que $H^\sigma = K$.

13. Dados dos números naturales n y k con $n \geq k \geq 2$, se pide:

    (a) Demostrar que, para cada subconjunto A de $\mathbb{N}_n$ de cardinal k, el número de k-ciclos σ de S_n con $M(\sigma) = A$ es $(k-1)!$.

    (b) Demostrar que el número de k-ciclos en S_n es $\binom{n}{k}(k-1)!$.

    (c) ¿Cuántos elementos de tipo $[2,2]$ hay en S_5? ¿Cuántos de tipo $[2,3]$?

    (d) ¿Cuántos elementos de tipo $[2,2]$ hay en S_6? ¿Cuántos de tipo $[2,3]$? ¿Y de tipo $[3,3]$?

    (e) [*] Calcular en general el número de elementos de S_n de tipo $[k_1, \ldots, k_r]$.

14. Sea G un grupo finito de orden n, y sea $g \in G$ de orden m. Como en la demostración del Teorema de Cayley (5.7.4), se define $\phi_g : G \to G$ por $\phi_g(x) = gx$. Viendo a ϕ_g como un elemento de S_n, demostrar que:

    (a) ϕ_g es un producto de n/m ciclos de longitud m.

    (b) La paridad de ϕ_g coincide con la paridad del entero $(m-1)\frac{n}{m}$.

    (c) Si $(m-1)\frac{n}{m}$ es impar, entonces G tiene un subgrupo normal de índice 2.

15. Demostrar que el centralizador de la permutación $\sigma = (1, 2, \ldots, n)$ en S_n es $\langle \sigma \rangle$.

16. Demostrar que el grupo alternado A_n es un subgrupo característico del grupo simétrico S_n.

17. Sea $n \geq 2$ y sea $f : S_n \to S_{n+2}$ la aplicación dada por $f(\sigma) = \sigma^*$, donde σ^* actúa igual que σ sobre los elementos $1, 2, \ldots, n$, y σ^* fija (respectivamente, intercambia) $n+1$ y $n+2$ cuando σ es par (respectivamente, impar). Demostrar que f es un homomorfismo inyectivo de grupos y que su imagen está contenida en A_{n+2}. Deducir que todo grupo finito es isomorfo a un subgrupo de un grupo alternado.

18. Probar que si P es un subgrupo de orden 4 del grupo alternado A_5, entonces P es isomorfo al grupo de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$.

19. Demostrar que D_n es isomorfo al subgrupo $\langle \rho, \sigma \rangle$ de S_n, donde $\rho = (1, 2, \ldots, n-1, n)$ y σ es el producto de las trasposiciones $(i, n+1-i)$, donde i varía desde 1 hasta la parte entera de $n/2$. ¿Para qué valores de n se tiene $\langle \rho, \sigma \rangle \subseteq A_n$?

20. Probar que si todo $\sigma \in S_n$ es producto de ciclos disjuntos de orden 2 entonces $n \leq 2$.

21. Probar que para todo $H \leq S_n$, con $n > 2$, se tiene, o bien $H \leq A_n$ o bien $[H : H \cap A_n] = 2$.

22. Dado $f \in \mathrm{Aut}(S_3)$, probar que f induce una permutación del conjunto $X = \{(1\,2), (1\,3), (2\,3)\} \subset S_3$. Deducir que la aplicación $t : S_3 \to \mathrm{Aut}(S_3)$ que lleva $\sigma \in S_3$ al automorfismo interno t_σ (ver el Ejercicio 5.9.4) es un isomorfismo de grupos.

23. Demostrar que A_n está generado por los 3-ciclos de la forma $(1, 2, i)$ con $i = 3, \ldots, n$.

24. Para $n \geq 5$, demostrar que S_n tiene exactamente tres subgrupos normales.

25. Para $n \geq 2$, demostrar que A_n es el único subgrupo de índice dos de S_n.

26. [*] Sea K un cuerpo. Un *polinomio* $P \in K[X_1, \ldots, X_n]$ se dice que es *simétrico* si, para todo $\sigma \in S_n$, se tiene $\bar{\sigma}(P) = P$ (con la notación de la Sección 6.2). Se llaman *polinomios simétricos elementales* a los siguientes polinomios simétricos:

$$\begin{aligned} \sigma_1 &= \textstyle\sum_{i=1}^{n} X_i \\ \sigma_2 &= \textstyle\sum_{1 \leq i < j \leq n} X_i X_j \\ \sigma_3 &= \textstyle\sum_{1 \leq i < j < k \leq n} X_i X_j X_k \\ &\vdots \\ \sigma_n &= X_1 X_2 \cdots X_n. \end{aligned}$$

(a) Demostrar que, si $r_1, \ldots, r_n$ son las raíces en K del polinomio $P = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$, entonces se tiene

$$a_i = (-1)^i \sigma_i(r_1, \ldots, r_n)$$

para cada $i = 1, \ldots, n$. Esto nos da los coeficientes de un polinomio en función de sus raíces.

(b) Demostrar que el conjunto de los polinomios simétricos de $K[X_1, \ldots, X_n]$ coincide con el subanillo $K[\sigma_1, \ldots, \sigma_n]$ generado por K y los polinomios simétricos elementales. (Indicación: Hacer una doble inducción primero en el número de indeterminadas y segundo en el grado del polinomio simétrico P que se quiere demostrar que pertenece a $K[\sigma_1, \ldots, \sigma_n]$.)

(c) Expresar los siguientes polinomios simétricos como polinomios en los polinomios simétricos elementales:

$$(X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2, \quad X_1^3 + X_2^3 + X_3^3.$$

(d) Demostrar que el homomorfismo de sustitución $S : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]$ dado por $S(P) = P(\sigma_1, \ldots, \sigma_n)$ es inyectivo y deducir que $K[X_1, \ldots, X_n]$ es isomorfo al anillo de los polinomios simétricos elementales.

27. [*] Sea p un primo impar y sea H un subgrupo propio de S_p que contiene una trasposición. Demostrar que existen $i, j \in \mathbb{N}_p$ tales que $\sigma(i) \neq j$ para todo $\sigma \in H$. (Indicación: Considerar en $\mathbb{N}_p$ la relación de equivalencia en la que $i \sim j$ si $i = j$ ó si $(i, j) \in H$, y comparar el número de elementos de las clases de equivalencia.)

28. [*] Sea $S_\infty = S(\mathbb{N})$ el grupo de permutaciones del conjunto numerable $\mathbb{N}$. El *grupo alternado infinito* es el subgrupo A_∞ de S_∞ generado por todos los 3-ciclos (donde un 3-ciclo se define del modo obvio). Demostrar que A_∞ es un grupo simple infinito.

Bibliografía del capítulo

Allenby [1], Delgado-Fuertes-Xambó [11], Lang [24], Rotman [30].

Capítulo 7

Grupos abelianos finitamente generados

Se estudian los grupos abelianos finitamente generados, dando una descripción precisa de su estructura y asignándoles unas listas de invariantes numéricos que los determinan salvo isomorfismos.

Introducción

En este capítulo y en el siguiente, tratamos el problema de clasificar grupos finitos en función de su orden. El objetivo es obtener, para cada entero positivo n, la descripción de todos los grupos de orden n. Por ejemplo, obtendremos resultados como este: "Salvo isomorfismos, hay cinco grupos de orden 8, que son $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4 y Q_8". Esto significa que entre esos grupos de orden 8 no hay dos isomorfos, y que cualquier grupo de orden 8 es isomorfo a uno (y sólo uno) de ellos.

El problema es tremendamente complicado, y de hecho no está resuelto en general. En situaciones como ésta, lo usual es abordar primero el problema con alguna hipótesis extra que lo haga más sencillo, y tratar entonces de extraer consecuencias para el caso general. En este capítulo clasificaremos los grupos abelianos finitos (más generalmente, los finitamente generados), y algunas de las ideas que usaremos nos servirán más tarde para obtener ciertos resultados de clasificación en el caso no abeliano (clasificaremos los grupos de orden n para $n \leq 15$ y para ciertos valores de n con una factorización prima sencilla).

Hay un modo elemental de fabricar grupos abelianos finitamente generados: hacer productos finitos de grupos cíclicos. Vamos a demostrar que, salvo isomorfismos, éstos son todos los grupos abelianos finitamente generados que existen, lo que nos da una descripción muy precisa de esos grupos. Más aún, de forma similar (aunque más sofisticada) al modo en el que la dimensión de un espacio vectorial lo determina salvo isomorfismos, ciertos invariantes numéricos (llamados así porque permanecen invariantes por isomorfismos) asociados a cada grupo abeliano finitamente generado caracterizan su clase de isomorfía, en el sentido de que dos de tales grupos son isomorfos si y sólo si los invariantes de ambos coinciden.

En todo el capítulo usamos notación aditiva. Comenzamos estudiando el concepto de suma directa de subgrupos, que permite establecer isomorfismos entre un grupo abeliano y el producto directo de algunos de sus subgrupos. Después analizamos los grupos abelianos libres, que interpretamos como grupos que cumplen ciertas propiedades análogas a las de los espacios vectoriales, y vemos que se les puede asignar un "rango" que representa en este contexto el papel que tiene la dimensión en el caso vectorial. Definimos entonces el subgrupo de torsión de un grupo, y demostramos que todo grupo abeliano finitamente generado A es suma directa de su subgrupo de torsión $t(A)$, que es finito, y de un subgrupo libre isomorfo al cociente $A/t(A)$. Esta "parte libre" es isomorfa a un producto de r copias de $\mathbb{Z}$, donde r es el rango de $A/t(A)$, por lo que el problema queda reducido al estudio de grupos abelianos finitos. Es fácil ver que tales grupos son sumas directas de subgrupos "indescomponibles", por lo que basta ver que todo grupo finito e indescomponible B es cíclico. Para ello, considerando las p-componentes de un grupo (para cada entero positivo primo p), vemos en un primer paso que el orden de B es una potencia de un primo fijo p, y usando esto obtenemos finalmente el resultado deseado.

Habremos demostrado así que la parte de torsión de A es producto de grupos cíclicos cuyo orden es una potencia de primo. Viendo entonces que esta expresión es esencialmente única (salvo el orden y salvo isomorfismos), la lista formada por el rango de $A/t(A)$ junto con los órdenes (potencias de primo) de esos grupos cíclicos será una lista de invariantes que determina la clase de isomorfía de A (es decir, la clase formada por los grupos isomorfos a A). Será entonces fácil ver que hay una forma alternativa de descomponer A como producto de cíclicos, en la que el orden de cada uno de ellos divide al del siguiente. El capítulo finaliza con un método matricial para obtener estas listas a partir de una presentación del grupo "por generadores y relaciones".

Objetivos del capítulo

- Conocer el concepto de suma directa de subgrupos y su relación con el producto de grupos.
- Conocer los conceptos de conjunto linealmente independiente, base, grupo abeliano libre y rango, así como la Propiedad Universal de las Bases.
- Saber calcular bases y rangos de grupos abelianos libres.
- Saber determinar la parte de torsión y las p-componentes de un grupo abeliano, y saber descomponer éstas como suma directa de subgrupos cíclicos.
- Saber utilizar el Teorema Chino de los Restos para pasar de una descomposición invariante a una descomposición indescomponible, y viceversa.
- Saber usar la notación matricial para obtener los factores invariantes de un grupo abeliano finitamente generado a partir de una presentación por generadores y relaciones.

Desarrollo de los contenidos

7.1 Sumas directas

Un modo habitual de estudiar un objeto matemático consiste en descomponerlo en objetos más sencillos, estudiar éstos y recomponer entonces el objeto inicial. Lo que se entiende por objeto sencillo y la manera de descomponer y recomponer un objeto dependen de cada caso. En este capítulo el objeto estudiado será un grupo abeliano finitamente generado A, y los objetos sencillos serán los grupos cíclicos, que ya conocemos bien. En este contexto, el proyecto sugerido al principio del párrafo funciona porque existe un método muy efectivo para descomponer A de modo que es muy fácil conocer A a partir de sus componentes. Se trata de la suma directa de subgrupos, que analizamos en esta sección.

Proposición 7.1.1 *Sean $\{B_1, \ldots, B_n\}$ subgrupos de un grupo abeliano A. Entonces las condiciones siguientes son equivalentes:*

1. *El 0 se expresa de manera única como suma de elementos de los B_i. Es decir, si $b_1 + \cdots + b_n = 0$ con cada $b_i \in B_i$, entonces se tiene $b_i = 0$ para cada $i = 1, \ldots, n$.*
2. *Cada elemento de $B_1 + \cdots + B_n$ se expresa de manera única como suma de elementos de los B_i. Es decir, si $b_1 + \cdots + b_n = b'_1 + \cdots + b'_n$ con cada $b_i \in B_i$ y cada $b'_i \in B_i$, entonces se tiene $b_i = b'_i$ para cada $i = 1, \ldots, n$.*
3. *Para cada $j = 1, \ldots, n$ se verifica $B_j \cap (\sum_{i \neq j} B_i) = 0$.*

Demostración. La equivalencia entre las dos primeras condiciones se deduce de un argumento típico que el lector conocerá del álgebra lineal, y se deja como ejercicio. Veamos pues que las condiciones 1 y 3 son equivalentes.

Si se verifica 1 y $x \in B_j \cap (\sum_{i \neq j} B_i)$, entonces $x \in B_j$ y existen $b_1, \ldots, b_{j-1}, b_{j+1}, \ldots, b_n$ tales que $x = b_1 + \cdots + b_{j-1} + b_{j+1} + \cdots + b_n$. Haciendo $b_j = -x$ se tiene $b_1 + \cdots + b_n = 0$, luego $b_j = 0$ y así $x = 0$. Recíprocamente, si se verifica 3 y se tiene $b_1 + \cdots + b_n = 0$ con cada $b_i \in B_i$ entonces, para cada índice j, se tiene $b_j = -(b_1 + \ldots + b_{j-1} + b_{j+1} + \ldots + b_n) \in B_j \cap (\sum_{i \neq j} B_i) = 0$, luego $b_j = 0$. $\square$

La Proposición 7.1.1 se puede generalizar a una familia infinita de subgrupos. Explícitamente:

Ejercicio 7.1.2 *Sea $\{B_i : i \in I\}$ una familia de subgrupos de un grupo abeliano A. Entonces las condiciones siguientes son equivalentes:*

1. *El 0 se expresa de manera única como suma de elementos de los B_i. Es decir, si $\sum_{i\in I} b_i = 0$ con cada $b_i \in B_i$ y $b_i = 0$, para casi todo $i \in I$, entonces se tiene $b_i = 0$ para cada $i \in I$.*

2. *Cada elemento de $\sum_{i\in I} B_i$ se expresa de manera única como suma de elementos de los B_i. Es decir, si $\sum_{i\in I} b_i = \sum_{i\in I} b'_i$ con cada $b_i, b'_i \in B_i$, $b_i = 0$ para casi todo $i \in I$ y $b'_i = 0$ para casi todo $i \in I$, entonces se tiene $b_i = b'_i$ para cada $i \in I$.*

3. *Para cada $j \in I$ se verifica $B_j \cap (\sum_{i\neq j} B_i) = 0$.*

Definición 7.1.3 *Si se verifican las condiciones equivalentes de la Proposición 7.1.1 (o del Ejercicio 7.1.2 en el caso infinito), se dice que la familia de subgrupos $\{B_1, \ldots, B_n\}$ es* independiente, *o que los subgrupos B_i son independientes. Su suma, $\sum_{i=1}^n B_i = B_1 + \cdots + B_n$, se llama entonces la* suma directa *de la familia $\{B_1, \ldots, B_n\}$, y se denota por $\oplus_{i=1}^n B_i = B_1 \oplus \cdots \oplus B_n$ (o por $\oplus_{i\in I} B_i$ en el caso infinito).*

La expresión "Sea $A = B_1 \oplus \cdots \oplus B_n$" quiere decir que los B_i son subgrupos independientes del grupo abeliano A y que su suma vale A.

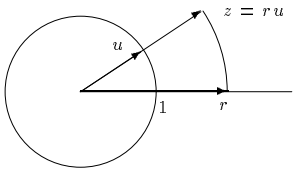
Un subgrupo B de A es un sumando directo *de A si existe otro subgrupo C de A tal que $A = B \oplus C$; es decir, tal que $A = B + C$ y $B \cap C = 0$. En este caso se dice que C es un* complemento directo *de B.*

Ejemplos 7.1.4 *Subgrupos independientes y sumas directas.*

1. En el grupo $A = \mathbb{Z}_6$ los subgrupos $B = \langle 2\rangle$ y $C = \langle 3\rangle$ son independientes y se tiene $A = B \oplus C$.

2. En el grupo multiplicativo $\mathbb{R}^*$ se tiene $\mathbb{R}^* = \langle -1\rangle \oplus \mathbb{R}^+$.

3. En el grupo multiplicativo $\mathbb{C}^*$ los subgrupos $\mathbb{R}^+$ y $U = \{u \in \mathbb{C} : |u| = 1\}$ son independientes y se tiene $\mathbb{C}^* = \mathbb{R}^+ \oplus U$. Eso es precisamente la expresión en forma polar de un número complejo.



4. Si A y B son grupos abelianos, entonces el grupo producto $A \times B$ es la suma directa de los subgrupos $A \times 0$ y $0 \times B$.

5. El complemento directo de un sumando directo no es, en general, único. Por ejemplo, para cualquier $a \in \mathbb{Z}$ se tiene $\mathbb{Z} \times \mathbb{Z} = \langle (1,0)\rangle \oplus \langle (a,1)\rangle$: la intersección es claramente nula, y un elemento arbitrario (x, y) de $\mathbb{Z} \times \mathbb{Z}$ se puede expresar como $(x, y) = y(a, 1) + (x - ya)(1, 0)$.

6. En $\mathbb{Q}$ no hay dos subgrupos no triviales que sean independientes. En efecto, si A y B son subgrupos no nulos y elegimos elementos no nulos $\frac{a}{n} \in A$ y $\frac{b}{m} \in B$, entonces $0 = bn\dfrac{a}{n} - am\dfrac{b}{m}$ nos da una expresión no trivial del 0 como suma de elementos de A y B. En $\mathbb{Z}$ ocurre lo mismo, por un argumento similar.

Ejercicio 7.1.5 *Demostrar las siguientes afirmaciones sobre un grupo abeliano A.*

1. *Toda subfamilia de una familia independiente de subgrupos de A es independiente. Es decir, si $\{B_i : i \in I\}$ es una familia independiente de subgrupos de A y J es un subconjunto del conjunto de índices I, entonces la familia $\{B_i : i \in J\}$ es independiente.*

2. *Una familia de subgrupos es independiente precisamente si toda subfamilia finita suya lo es.*

3. *Si la familia $\{B_i : i \in I\}$ de subgrupos de un grupo abeliano A es independiente y otro subgrupo B_0 de A verifica $B_0 \cap (\oplus_{i\in I} B_i) = 0$, entonces la familia $\{B_0\} \cup \{B_i : i \in I\}$ también es independiente.*

   En particular, si a una familia independiente le añadimos el subgrupo trivial 0 (una o más veces), seguimos teniendo una familia independiente.

4. *Si $A = \oplus_{i\in I} B_i$ entonces cada B_j es un sumando directo de A con complemento $\oplus_{i\neq j} B_i$.*

5. *Si $A = B \oplus C$ y, a su vez, $B = B_1 \oplus \cdots \oplus B_n$ y $C = C_1 \oplus \cdots \oplus C_m$, entonces $A = B_1 \oplus \cdots \oplus B_n \oplus C_1 \oplus \cdots \oplus C_m$.*

6. *Si $A = B \oplus C$ entonces la aplicación $A \to C$ dada por $b + c \mapsto c$ (donde $b + c$ es la expresión única de un elemento arbitrario de A con $b \in B$ y $c \in C$) es un homomorfismo suprayectivo de grupos con núcleo B. En particular, $C \cong A/B$.*

7. *Si B es un sumando directo de A, cualquier complemento directo suyo es isomorfo a A/B. Por tanto, aunque un sumando directo puede tener distintos complementos directos, todos ellos son isomorfos entre sí.*

Cuando sólo consideramos familias finitas, existe una estrecha relación entre los conceptos de suma directa y producto directo de grupos, que describimos a continuación dejando los detalles a cargo del lector.

Supongamos primero que $A = B_1 \oplus \cdots \oplus B_n$. Entonces, viendo cada B_i como grupo y considerando su producto $B_1 \times \cdots \times B_n$, la aplicación $B_1 \times \cdots \times B_n \to A$ dada por $(b_1, \ldots, b_n) \mapsto b_1 + \cdots + b_n$ es un isomorfismo de grupos. Es decir, si A es la suma directa de los B_i, entonces A es isomorfo al producto directo de los B_i.

Recíprocamente, sean $B_1, \ldots, B_n$ grupos abelianos y sea A el grupo producto, $A = B_1 \times \cdots \times B_n$. Si denotamos por $\hat{B}_i$ al subgrupo de A formado por los elementos que llevan ceros en todas las coordenadas excepto tal vez en la i-ésima (o sea $\hat{B}_i = 0 \times \cdots \times 0 \times B_i \times 0 \times \cdots \times 0$), entonces es elemental ver que cada $\hat{B}_i$ es isomorfo a B_i y que $A = \hat{B}_1 \oplus \cdots \oplus \hat{B}_n$. Es decir, si A es el producto directo de los B_i, entonces A es la suma directa de los $\hat{B}_i$, que son isomorfos a los B_i.

En vista de esto, a partir de ahora identificaremos $B_1 \oplus \cdots \oplus B_n$ con $B_1 \times \cdots \times B_n$.

Ejercicio 7.1.6 *Extender la discusión anterior al caso de una familia infinita independiente de subgrupos, sustituyendo el producto directo por el grupo del último apartado de los Ejemplos 5.3.4.*

7.2 Grupos abelianos libres

Definición 7.2.1 *Sea A un grupo abeliano.*

Un subconjunto finito $\{a_1, \ldots, a_n\}$ de A se dice que es linealmente independiente *si la única solución, formada por números enteros $x_1, \ldots, x_n$, de la ecuación*

$$\sum_{i=1}^{n} x_i a_i = 0$$

es $x_1 = \cdots = x_n = 0$. Un subconjunto de A se dice que es linealmente independiente si todo subconjunto finito suyo es linealmente independiente.

Una base *de A es un sistema generador de A que es linealmente independiente. Diremos que A es un* grupo abeliano libre *si tiene una base.*

Ejercicio 7.2.2 *Demostrar que un subconjunto X de un grupo abeliano A es una base precisamente si cada elemento de A se puede expresar de forma única como combinación lineal con coeficientes enteros de los elementos de X. Es decir, si para cada $a \in A$ existe una única familia $\{a_x : x \in X\}$ de enteros, casi todos nulos, tal que $a = \sum_{x\in X} a_x x$.*

Ejemplos 7.2.3 *Grupos abelianos libres.*

1. Sea n un número natural y sea $A = \mathbb{Z}^n$. Entonces el conjunto

$$e_1 = (1, 0, \ldots, 0), \quad e_2 = (0, 1, \ldots, 0), \quad \ldots \quad e_n = (0, 0, \ldots, 1)$$

   es una base de A, llamada *base canónica*.

2. En $A = \mathbb{Z}$, el conjunto $\{2, 3\}$ es un sistema generador minimal (en el sentido de que, si quitamos algún elemento, deja de ser sistema generador) que no es linealmente independiente. Por otra parte, el conjunto $\{2\}$ es un conjunto linealmente independiente maximal (en el sentido de que, en cuanto le añadamos un elemento, dejará de ser independiente) que no es generador.

   Esto no ocurre con los espacios vectoriales: en un espacio vectorial, todo sistema generador minimal es una base (en el sentido de álgebra lineal) y todo conjunto linealmente independiente maximal es una base.

3. Sea I un conjunto y consideremos el grupo $A = \mathbb{Z}^I = \{(a_i)_{i\in I} : a_i \in \mathbb{Z}\}$ con la suma componente a componente (a este grupo se le suele llamar el producto directo de $|I|$ copias de $\mathbb{Z}$). Para cada $i \in I$, sea $e_i = (\delta_{ij})_{j\in I}$, donde $\delta_{ij} = 0$ si $i \neq j$ y $\delta_{ii} = 1$ (este símbolo se conoce como *la delta de Kronecker*). Entonces $E = \{e_i : i \in I\}$ es un conjunto linealmente independiente de A. Sin embargo, E sólo es una base si I es finito. De hecho, el subgrupo generado por E es

$$\mathbb{Z}^{(I)} = \{(a_i)_{i\in I} \in \mathbb{Z}^I : a_i = 0 \text{ para casi todo } i \in I\}.$$

   Luego $\mathbb{Z}^{(I)}$ es un grupo libre y E es una base suya llamada *base canónica*.

4. Sea P el conjunto de los enteros primos positivos. Entonces la aplicación $f : \mathbb{Z}^{(P)} \to \mathbb{Q}^+$ dada por

$$f((n_p)_{p\in P}) = \prod_{p\in P} p^{n_p}$$

   es un isomorfismo. Luego $\mathbb{Q}^+$ es libre con base P.

Ejercicio 7.2.4 *Demostrar que una familia $\{a_i : i \in I\}$ de elementos de un grupo A es linealmente independiente si y sólo si cada a_i tiene orden infinito y la familia $\{\langle a_i\rangle : i \in I\}$ de los subgrupos cíclicos generados por los a_i es independiente.*

En realidad, el apartado 3 del Ejemplo 7.2.3 agota, salvo isomorfismos, todos los posibles ejemplos de grupos libres, como muestra el siguiente ejercicio.

Ejercicio 7.2.5 *Sea X un subconjunto de un grupo abeliano A, y sea $f : \mathbb{Z}^{(X)} \to A$ la aplicación dada por $f((a_x)_{x\in X}) = \sum_{x\in X} a_x x$ (las sumas tienen sentido porque casi todos los sumandos son nulos). Demostrar:*

1. *f es un homomorfismo de grupos.*
2. *f es inyectiva precisamente si X es linealmente independiente.*
3. *f es suprayectiva precisamente si X es un conjunto generador de A.*
4. *X es una base precisamente si f es un isomorfismo. En este caso $A \cong \mathbb{Z}^{(X)}$.*
5. *A es libre precisamente si A es isomorfo a $\mathbb{Z}^{(I)}$ para cierto conjunto I.*

Los conceptos de linealmente independiente, generador y base nos recuerdan a los correspondientes de álgebra lineal. En el siguiente ejercicio vemos algunas relaciones entre nuestro concepto y el de álgebra lineal.

Ejercicio 7.2.6 *Sea I un conjunto. Consideremos $A = \mathbb{Z}^{(I)}$ como un grupo abeliano libre y $V = \mathbb{Q}^{(I)}$ como un espacio vectorial sobre $\mathbb{Q}$. Demostrar las siguientes propiedades para un subconjunto S de A:*

1. *S es linealmente independiente como subconjunto del grupo A precisamente si S es linealmente independiente como subconjunto del espacio vectorial V.*
2. *Si S es un sistema generador del grupo A, entonces S es un sistema generador del espacio vectorial V.*
3. *Dar un ejemplo de un subconjunto de A que sea generador de V pero que no sea generador de A.*
4. *Demostrar que todas las bases de A tienen el mismo cardinal, a saber $|I|$. Deducir que si J es otro conjunto, entonces $\mathbb{Z}^{(I)} \cong \mathbb{Z}^{(J)}$ precisamente si $|I| = |J|$.*

Definición 7.2.7 *El cardinal de una base (cualquier base) de un grupo abeliano libre A se llama rango de A y se denota $r(A)$.*

De los Ejercicios 7.2.5 y 7.2.6 se deduce que el rango es un invariante que caracteriza los grupos abelianos libres salvo isomorfismos; es decir:

Proposición 7.2.8 *Si A y B son grupos abelianos libres, entonces $A \cong B$ si y sólo si $r(A) = r(B)$.*

Los grupos abelianos libres que más nos interesan son los finitamente generados. Obviamente, los grupos de la forma $\mathbb{Z}^n$ son grupos abelianos libres finitamente generados. De hecho no hay más, salvo isomorfismos, ya que si $\{a_1 = (a_{1i})_{i\in I}, \ldots, a_n = (a_{ni})_{i\in I}\}$ es un conjunto generador de $A = \mathbb{Z}^{(I)}$, entonces $F = \{i \in I : a_{ki} \neq 0 \text{ para algún } k = 1, \ldots, n\}$ es un subconjunto finito de I. Vamos a ver que $I = F$. Si $i \in I \setminus F$, entonces la coordenada i-ésima de todo elemento de la forma $\sum_{k=1}^{n} m_k a_k$ es 0. Como en $\mathbb{Z}^{(I)}$ hay elementos cuya coordenada i-ésima no es 0 (¡encuentra uno!), eso nos lleva a una contradicción, de donde deducimos que $I = F$ y, por tanto I es finito. Junto con la Proposición 7.2.8, esto demuestra que:

Corolario 7.2.9 *Todo grupo abeliano libre finitamente generado A es isomorfo a $\mathbb{Z}^n$, donde $n = r(A)$.*

Un grupo abeliano libre finitamente generado también se dice que es un grupo abeliano libre de *tipo finito* o de *rango finito*. Como consecuencia del Ejercicio 7.2.5 se deduce:

Proposición 7.2.10 *Sea A un grupo abeliano.*

1. *A es isomorfo a un cociente de un grupo abeliano libre.*
2. *A es finitamente generado precisamente si es isomorfo a un cociente de un grupo abeliano libre de tipo finito.*
3. *A es cíclico precisamente si es isomorfo a un cociente de $\mathbb{Z}$.*

Demostración. Sea A un grupo abeliano, y sea I un conjunto generador de A (¿existe siempre?). Entonces la aplicación $f : \mathbb{Z}^{(I)} \to A$ del Ejercicio 7.2.5 es un epimorfismo. Por el Primer Teorema de Isomorfía se tiene $A \cong \mathbb{Z}^{(I)}/\text{Ker } f$, lo que demuestra la primera afirmación y la condición necesaria de las otras dos afirmaciones. Las condiciones suficientes son evidentes. □

Del isomorfismo evidente $\mathbb{Z}^n \times \mathbb{Z}^m \cong \mathbb{Z}^{n+m}$ se deduce:

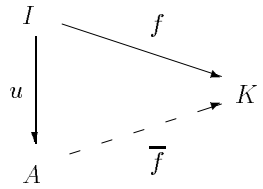
Proposición 7.2.11 *Si A y B son grupos abelianos libres de tipo finito entonces $A \times B$ es también libre, y se tiene $r(A \times B) = r(A) + r(B)$.*

El lector puede probar que el producto directo de un número finito de grupos libres (no necesariamente de tipo finito) es libre. No es cierto que el producto directo infinito de grupos libres sea libre. Por ejemplo, $\mathbb{Z}^{\mathbb{N}}$ no es libre, pero la demostración de este hecho excede los objetivos del curso.

Las bases de los grupos abelianos libres verifican una propiedad análoga a las bases de espacios vectoriales, en el sentido de que podemos describir homomorfismos que salgan de un grupo abeliano libre eligiendo arbitrariamente (en el grupo imagen) las imágenes de los elementos de la base. Explícitamente:

Proposición 7.2.12 (Propiedad Universal de las Bases) *Sea A un grupo abeliano libre y sea I una base de A. Si B es un grupo abeliano y $f : I \to B$ es una aplicación, entonces existe un único homomorfismo de grupos $\bar{f} : A \to B$ que extiende f (es decir, tal que $\bar{f}(i) = f(i)$ cuando $i \in I$).*

Obsérvese que, si $u : I \to A$ es la inclusión, entonces el homomorfismo $\bar{f}$ completa el siguiente diagrama



Demostración. Por el Ejercicio 7.2.5 existe un isomorfismo $g : A \to \mathbb{Z}^{(I)}$ tal que $g(i) = e_i$, donde $\{e_i : i \in I\}$ es la base canónica de $\mathbb{Z}^{(I)}$. Sea $\bar{f} : \mathbb{Z}^{(I)} \to B$ la aplicación dada por $\bar{f}((a_i)_{i\in I}) = \sum_{i\in I} a_i f(i)$. Por el Ejercicio 7.2.5, $\bar{f}$ es un homomorfismo de grupos y la composición $g \circ \bar{f} : A \to B$ satisface las condiciones requeridas. La unicidad es consecuencia del hecho obvio de que dos homomorfismos que toman los mismos valores en un conjunto generador son iguales. □

Lema 7.2.13 *Un subgrupo B de un grupo A es un sumando directo de A si y sólo si existe un homomorfismo $\rho : A \to B$ que es la identidad en B; es decir, tal que $\rho(b) = b$ para cada $b \in B$. Si tal ρ existe, entonces $A = B \oplus \operatorname{Ker} \rho$.*

Demostración. La condición necesaria es consecuencia del Ejercicio 7.1.5. Sea $\rho : A \to B$ un homomorfismo suprayectivo que es la identidad en B. Entonces $B \cap \operatorname{Ker} \rho = 0$ y, si $a \in A$, entonces $\rho(a - \rho(a)) = \rho(a) - \rho(a) = 0$ y

$$a = \rho(a) + a - \rho(a) \in B + \operatorname{Ker} \rho.$$

Luego $A = B \oplus \operatorname{Ker} \rho$. □

Corolario 7.2.14 *Sea $f : A \to L$ un homomorfismo suprayectivo de grupos abelianos. Si L es libre, entonces existe un subgrupo B de A isomorfo a L tal que $A = B \oplus \operatorname{Ker} f$.*

Demostración. Sea I una base de L y, para cada $i \in I$, sea $a_i \in A$ tal que $f(a_i) = i$. Por la Proposición 7.2.12, existe un único homomorfismo de grupos $g : L \to A$ tal que $g(i) = a_i$, para todo $i \in I$. Entonces $f \circ g = 1_L$ (¿por qué?); por tanto g es inyectiva y así $B = \operatorname{Im} g \cong L$. Entonces, la composición $p = g \circ f : A \to B$ es la identidad sobre B, pues un elemento $b \in B$ es de la forma $b = g(x)$ con $x \in L$ y entonces

$$p(b) = p(g(x)) = g(f(g(x))) = g(1_L(x)) = g(x) = b.$$

Ahora el resultado es una consecuencia inmediata del Lema 7.2.13. □

Teorema 7.2.15 *Sea A un grupo abeliano libre de tipo finito y sea B un subgrupo de A. Entonces B es libre de tipo finito y $r(B) \leq r(A)$.*

Demostración. Sea $n = r(A)$. Por el Corolario 7.2.9, podemos suponer que $A = \mathbb{Z}^n$. Razonamos por inducción sobre n, con el caso $n = 1$ resuelto por el Corolario 5.8.8. Supongamos pues que $n > 1$ y que se verifica el teorema para grupos abelianos libres de rango menor que n. Sea $e_1, \ldots, e_n$ la base canónica de A. Sean $A_1 = \langle e_1, \ldots, e_{n-1}\rangle$ y $B_1 = B \cap A_1$. Obviamente, A_1 es libre de rango $n - 1$, y por la hipótesis de inducción B_1 es libre de rango $\leq n - 1$. Sea $f : A \to \mathbb{Z}$ el homomorfismo dado por $f(x_1, \ldots, x_n) = x_n$, sea $C = f(B)$ y sea $g : B \to C$ la restricción de f a B. Entonces C es un grupo abeliano libre de rango ≤ 1 y $\operatorname{Ker} g = B_1$. Del Corolario 7.2.14 se deduce que $B = B_1 \oplus C_1$, donde C_1 es un subgrupo de B isomorfo a C. Aplicando la Proposición 7.2.11 se deduce que B es libre de rango menor o igual que n. □

7.3 Grupos de torsión y libres de torsión

Definición 7.3.1 *Sea A un grupo abeliano.*

El subgrupo de torsión *de A es el conjunto $t(A)$ formado por los elementos de orden finito de A:*

$$t(A) = \{a \in A : \text{ existe } 0 \neq n \in \mathbb{Z} \text{ tal que } na = 0\}.$$

Se dice que A es un grupo de torsión *si $t(A) = A$. Es decir, si para cada $a \in A$ existe $0 \neq n \in \mathbb{Z}$ tal que $na = 0$.*

Se dice que A es un grupo libre de torsión *si $t(A) = 0$. Es decir, si para cada $0 \neq a \in A$, el único $n \in \mathbb{Z}$ tal que $na = 0$ es $n = 0$ (lo que equivale a que el conjunto $\{a\}$ sea linealmente independiente).*

Si un entero n verifica $na = 0$ para todo $a \in A$, escribiremos $nA = 0$. Si existe algún $n \geq 1$ con $nA = 0$, llamamos periodo *de A al menor entero positivo con esa propiedad. Si no existe tal entero positivo, decimos que A tiene periodo 0. Denotaremos con $p(A)$ al periodo de A.*

Dejamos que el lector compruebe algunas propiedades elementales de los conceptos recién definidos, y en particular las relaciones entre ellos.

Ejercicio 7.3.2 *Si A es un grupo abeliano, demostrar que:*

1. *El conjunto $t(A)$ es un subgrupo de A que es de torsión, y el grupo cociente $A/t(A)$ es libre de torsión.*
2. *Si A es finito entonces $p(A) \neq 0$.*
3. *Si $p(A) \neq 0$ entonces A es de torsión.*
4. *Si A es libre entonces A es libre de torsión.*
5. *Si A es libre de torsión y no trivial, entonces $p(A) = 0$.*
6. *Si A es cíclico y $p(A) = n$ entonces $A \cong \mathbb{Z}_n$ (incluidos los casos $n = 0$ y $n = 1$).*
7. *Si A es de torsión y B es un subgrupo de A entonces B y A/B también son de torsión.*
8. *Si A es libre de torsión entonces cualquier subgrupo B es también libre de torsión; ¿lo es A/B?*
9. *Si $A = B \oplus C$ entonces $t(A) = t(B) \oplus t(C)$.*
10. *Si $p(A) = n \neq 0$ y $m \in \mathbb{Z}$ entonces $ma = 0$ para cada $a \in A$ si y sólo si $n \mid m$.*
11. *Si $A = B_1 \oplus \cdots \oplus B_n$ entonces $p(A) = \text{mcm}(p(B_1), \ldots, p(B_n))$.*
12. *Si A es de torsión y $\{a_i : i \in I\}$ es un sistema generador entonces $p(A) = \text{mcm}\{o(a_i) : i \in I\}$.*

Ejemplos 7.3.3 *Torsiones y periodos.*

1. El grupo $A = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$ (producto numerable de copias de $\mathbb{Z}_2$) tiene periodo 2. Esto nos da un contraejemplo para el recíproco del apartado 2.
2. El grupo $\mathbb{Q}/\mathbb{Z}$ es de torsión, pues cada $\frac{a}{b} + \mathbb{Z}$ es anulado por $b \neq 0$. Además este grupo tiene periodo 0, pues dado $n \neq 0$ en $\mathbb{Z}$ se tiene $n(\frac{1}{p} + \mathbb{Z}) \neq 0$, donde p es cualquier primo que no divide a n. Esto nos da un contraejemplo para los recíprocos de los apartados 3 y 5.
3. Existen grupos abelianos libres de torsión que no son libres; por ejemplo $\mathbb{Q}$ (cualquier subconjunto linealmente independiente tiene un solo elemento, y por tanto no es un sistema generador). Esto nos da un contraejemplo para el recíproco del apartado 4.
4. Existen grupos abelianos que no son de torsión ni libres de torsión; por ejemplo, $\mathbb{Q}^*$, $\mathbb{R}^*$ ó $\mathbb{C}^*$.
5. Si $A = \mathbb{Z} \times \mathbb{Z}_n$, con $n > 0$, entonces $t(A) = 0 \times \mathbb{Z}_n$.
6. Si $A = \prod_p \mathbb{Z}_p$, donde p recorre el conjunto de los enteros positivos primos, entonces $t(A) = \oplus_p \mathbb{Z}_p$. Este subgrupo $t(A)$ es otro ejemplo de grupo de torsión con periodo 0.

7. Sea $z \in \mathbb{C}^*$. Si $r = |z|$ entonces se tiene $z = re^{\alpha i} = r(\cos\alpha + i\text{sen }\alpha)$, donde α es el argumento de z. Entonces $z^n = r^n e^{n\alpha i}$, con lo que $z^n = 1$ precisamente si $r = 1$ y $n\alpha = 2k\pi$ para algún $k \in \mathbb{Z}$. Por tanto
$$t(C^*) = \{e^{2\pi qi} : q \in \mathbb{Q},\ 0 \leq q < 1\}.$$
O sea, $t(C^*)$ está formado por los vértices de los polígonos regulares centrados en el origen con un vértice en el punto 1 (el lector puede representar gráficamente, por ejemplo, todos los elementos de orden ≤ 10.) Obsérvese que la aplicación $f : \mathbb{Q} \to \mathbb{C}^*$ dada por $f(q) = e^{2\pi qi}$ es un homomorfismo de grupos tal que $t(C^*) = \text{Im } f$ y $\text{Ker } f = \mathbb{Z}$, con lo que $t(C^*) \cong \mathbb{Q}/\mathbb{Z}$.

Los siguientes tres resultados nos dicen que, para grupos abelianos finitamente generados, todo lo relativo a la torsión se simplifica: Ser de torsión equivale a ser finito, ser libre de torsión equivale a ser libre y el subgrupo de torsión es un sumando directo[1].

Proposición 7.3.4 *Las condiciones siguientes son equivalentes para un grupo abeliano finitamente generado A:*

1. *A es finito.*
2. *$p(A) \neq 0$.*
3. *A es de torsión.*

Demostración. Por el Ejercicio 7.3.2, basta ver que 3 implica 1. Supongamos pues que A es de torsión, con un sistema generador $\{a_1, \ldots, a_k\}$, y sea $n_i = o(a_i) < \infty$. Obviamente, la familia de los elementos de A de la forma $r_1a_1 + \cdots + r_ka_k$ con $0 \leq r_i < n_i$ para cada $i = 1, \ldots, k$, es finita (tal vez incluso se repitan elementos), y las condiciones implican que cada elemento de A es uno de esos, luego A es un conjunto finito. □

Teorema 7.3.5 *Un grupo abeliano finitamente generado es libre de torsión precisamente si es libre.*

Demostración. Todo grupo libre es libre de torsión, por el Ejercicio 7.3.2. Sea A un grupo abeliano finitamente generado y libre de torsión. Sea $X = \{a_1, \ldots, a_n\}$ un conjunto de generadores de A. Entre todos los subconjuntos de X que sean linealmente independientes elegimos uno maximal Y; podemos suponer, reordenando los a_i si es necesario, que $Y = \{a_1, \ldots, a_k\}$. Sea $L = \langle Y \rangle$, que claramente es libre.

Sea $i \in \{k+1, k+2, \ldots, n\}$. Por la maximalidad de Y, el conjunto $\{a_1, \ldots, a_k, a_i\}$ es linealmente dependiente, luego hay una relación
$$t_{i1}a_1 + \cdots + t_{ik}a_k + t_ia_i = 0$$
donde los coeficientes son enteros, no todos nulos. Como Y es linealmente independiente, se tiene $t_i \neq 0$. Sea $t = t_{k+1} \cdots t_n$. Entonces cada $ta_i \in L$ y la aplicación $a \mapsto ta$ es un homomorfismo de grupos $f : A \to L$. Como A es libre de torsión y $t \neq 0$, la aplicación f es inyectiva y, por tanto A es isomorfo a un subgrupo de L. Del Teorema 7.2.15 se deduce que A es libre. □

Corolario 7.3.6 *Sea A un grupo abeliano finitamente generado. Entonces $A = t(A) \oplus L$ para un subgrupo abeliano libre L de A. Además $t(A)$ es finito y L es isomorfo a $A/t(A)$, y por tanto L es único salvo isomorfismos.*

Demostración. $A/t(A)$ es libre de torsión por el Ejercicio 7.3.2, y es finitamente generado por serlo A, luego es libre por el Teorema 7.3.5. Sea $\pi : A \to A/t(A)$ la proyección canónica. Del Corolario 7.2.14 se deduce que $A = t(A) \oplus L$, donde L es un subgrupo de A isomorfo a $A/t(A)$, luego L es un grupo abeliano libre. Además $t(A)$ es finitamente generado (es isomorfo al cociente A/L por el Ejercicio 7.1.5) y de torsión, luego es finito (Proposición 7.3.4). □

[1] Existen grupos abelianos A tales que $t(A)$ no es un sumando directo de A. Un ejemplo de esta situación es el grupo $\prod_p \mathbb{Z}_p$ del apartado 6 de los Ejemplos 7.3.3, pero no es sencillo comprobar esta propiedad.

Ejemplos 7.3.7 *La torsión como sumando directo.*

1. Si $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_6 \times \mathbb{Z}_{36}$, entonces$t(A) = 0 \times 0 \times \mathbb{Z}_6 \times \mathbb{Z}_{36}$, y podemos tomar $L = \mathbb{Z} \times \mathbb{Z} \times 0 \times 0$.

2. Ya hemos visto que $\mathbb{R}^* = \langle -1 \rangle \oplus \mathbb{R}^+$, y es claro que $\langle -1 \rangle = t(\mathbb{R}^*)$.

3. Sea G el subgrupo de $\mathbb{C}^*$ generado por $\{2, i\}$. Por los Ejemplos 7.3.3, si $z = 2^n i^m \in t(G)$ (con $n, m \in \mathbb{Z}$), entonces $1 = |z| = 2^n$, lo que implica que $n = 0$. O sea $t(G) = \langle i \rangle$. Como $\langle 2 \rangle$ es libre de torsión, $G = \langle 2 \rangle \oplus \langle i \rangle$ es la descomposición del Corolario 7.3.6.

4. Sea R un anillo. En el anillo cociente $R[X]/(X^2)$, es claro que cada elemento tiene un único representante de la forma $r + sX$ con $r, s \in R$. Dados $r + sX + (X^2)$ y $r' + s'X + (X^2)$ en $R[X]/(X^2)$, se tiene

$$[r + sX + (X^2)] + [r' + s'X + (X^2)] = (r + r') + (s + s')X + (X^2)$$

y

$$[r + sX + (X^2)] \cdot [r' + s'X + (X^2)] = (rr') + (rs' + r's)X + (X^2).$$

Por tanto, podemos identificar $R[X]/(X^2)$ con el anillo cuyo grupo abeliano subyacente es $R \times R$ y en el que el producto viene dado por

$$(r, s) \cdot (r', s') = (rr', rs' + r's).$$

El elemento identidad de este anillo es $(1, 0)$.

Si (r, s) es invertible en este anillo, es claro que $r \in R^*$. Recíprocamente, si $r \in R^*$ entonces $(r^{-1}, -sr^{-2})$ es el inverso de (r, s) en este anillo. En consecuencia, el grupo multiplicativo de sus unidades, que denotaremos con $R^* \propto R$, es el conjunto $R^* \times R$ con el producto definido en el párrafo anterior.

Vamos a determinar el orden de un elemento $(r, s) \in R^* \propto R$. Si $n \in \mathbb{Z}^+$, es fácil ver (bien por inducción o bien considerando la fórmula del binomio de Newton en $R[X]/(X^2)$) que

$$(r, s)^n = (r^n, nr^{n-1}s).$$

Como r es invertible en R, se tiene $(r, s)^n = (1, 0)$ precisamente si $r^n = 1$ y $ns = 0$. Por tanto, (r, s) tiene orden finito en $R^* \propto R$ precisamente si r tiene orden finito en $(R^*, \cdot)$ y s tiene orden finito en $(R, +)$. Es decir, $t(R^* \propto R) = t(R^*) \times t(R)$. Además, si $(r, s) \in t(R^* \propto R)$ entonces

$$o(r, s) = \text{mcm}(o_m(r), o_a(s)),$$

donde $o_m(r)$ es el orden de r en el grupo multiplicativo R^* y $o_a(s)$ es el orden de s en el grupo aditivo R.

Pasemos a un caso concreto: Sea $A = \mathbb{Z}^* \propto \mathbb{Z}$ (recuérdese que $\mathbb{Z}^* = \{1, -1\}$). Por el párrafo anterior se tiene $t(A) = \{(1, 0), (-1, 0)\}$. Por otra parte, $L = \langle (1, 1) \rangle$ es un subgrupo libre de A, y el lector puede ahora comprobar que se tiene $A = t(A) \oplus L$.

Por el Teorema 7.2.15, todo subgrupo B de un grupo abeliano libre A es libre y $r(B) \leq r(A)$. Los resultados anteriores nos permiten determinar cuándo se da la igualdad entre los rangos.

Proposición 7.3.8 *Sea A un grupo abeliano libre finitamente generado y B un subgrupo de A. Entonces $r(A) = r(B)$ precisamente si A/B es un grupo finito.*

Demostración. Como A es finitamente generado, lo es también A/B, así que A/B es finito si y sólo si es de torsión (Proposición 7.3.4). Se trata pues de ver que A/B es de torsión si y sólo si $r(B) = r(A)$. Sean $n = r(A)$ (por lo que podemos asumir que $A = \mathbb{Z}^n$) y $k = r(B)$, y fijemos una base $b_1, \ldots, b_k$ de B. Es fácil ver que, para un elemento $a \in A$, el elemento $a + B \in A/B$ tiene orden infinito si y sólo si los elementos $b_1, \ldots, b_k, a$ son linealmente independientes en A. Podemos ya demostrar la equivalencia:

Si A/B no es de torsión, existe un elemento $a + B$ en A/B de orden infinito, luego $b_1, \ldots, b_k, a$ son linealmente independientes en A y así $k < k + 1 \leq n$. Y si $k < n$ y vemos a $A = \mathbb{Z}^n$ dentro del espacio vectorial racional $V = \mathbb{Q}^n$, entonces existe $\alpha \in V$ tal que $b_1, \ldots, b_k, \alpha$ son linealmente independientes en V, y además existe un entero no nulo t tal que $a = t\alpha \in A$. Como $t \neq 0$, los elementos $b_1, \ldots, b_k, a$ son linealmente independientes en V y, por el Ejercicio 7.2.6, también lo son en A, por lo que $a + B$ tiene orden infinito y así A/B no es de torsión. □

7.4 Grupos indescomponibles y p-grupos

Como hemos comentado en la introducción del capítulo, nuestro objetivo es descomponer un grupo abeliano finitamente generado A como suma directa de subgrupos con algunas propiedades especiales. Con las herramientas desarrolladas en las secciones anteriores, en ésta veremos primero que A es suma directa de subgrupos que no pueden descomponerse más (indescomponibles), y a continuación demostraremos que estos subgrupos indescomponibles son cíclicos, de lo que deduciremos que A es suma directa de subgrupos cíclicos. Comenzamos definiendo con precisión los grupos indescomponibles.

Definición 7.4.1 *Un grupo abeliano no nulo se dice que es* indescomponible *si no es suma directa de dos subgrupos propios. Es decir A es indescomponible si $A = X \oplus Y$ implica $X = 0$ ó $Y = 0$ (y por tanto $X = A$ ó $Y = A$).*

Ejemplos 7.4.2 *Grupos Indescomponibles.*

1. $\mathbb{Z}$ y $\mathbb{Q}$ son indescomponibles, por un argumento usado en los Ejemplos 7.1.4.
2. Por el Corolario 7.2.9 y el Teorema 7.3.5, $\mathbb{Z}$ es, salvo isomorfismos, el único grupo abeliano libre de torsión y finitamente generado que es indescomponible.
3. Si p es un número primo entonces $\mathbb{Z}_p$ es indescomponible, pues no tiene subgrupos propios no triviales. De hecho, $\mathbb{Z}_{p^n}$ es indescomponible para cada $n \geq 1$. En efecto, por el Teorema de la Correspondencia, los subgrupos de $\mathbb{Z}_{p^n}$ forman una cadena (Ejemplos 5.6.6), y es claro que cualquier grupo cuyos subgrupos estén linealmente ordenados es indescomponible.
4. Sean $n, m \geq 2$ dos enteros coprimos; por el Teorema Chino de los Restos se tiene $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$, por lo que $\mathbb{Z}_{nm}$ no es indescomponible (recuérdese la relación entre entre suma directa y producto directo descrita al final de la Sección 7.1). En consecuencia, los grupos cíclicos finitos indescomponibles son exactamente aquellos cuyo orden es p^r para cierto primo p y cierto entero $r \geq 1$.

Como consecuencia inmediata del Corolario 7.3.6 se obtiene:

Corolario 7.4.3 *Un grupo abeliano finitamente generado indescomponible es de torsión (y por tanto finito) o libre de torsión.*

Proposición 7.4.4 *Todo grupo abeliano finitamente generado y no nulo A es una suma directa de subgrupos indescomponibles.*

Demostración. Por el Corolario 7.3.6, y teniendo en cuenta que los grupos abelianos libres de rango finito son sumas directas de copias de $\mathbb{Z}$ (Corolario 7.2.9) y que los grupos abelianos finitamente generados de torsión son finitos (Proposición 7.3.4), basta demostrar la afirmación para grupos abelianos finitos. Sea A un grupo abeliano finito. Razonamos por inducción en $|A|$, con el caso $|A| = 2$ trivial. Si A es indescomponible no hay nada que demostrar. En caso contrario $A = B \oplus C$ y los cardinales de B y C son estrictamente menores que el de A. Por hipótesis de inducción, B y C son sumas directas de grupos indescomponibles, y "pegando" las descomposiciones de B y C como en el Ejercicio 7.1.5 obtenemos una descomposición de A como suma directa de grupos indescomponibles. □

En los Ejemplos 7.4.2 han aparecido dos tipos de grupos finitamente generados e indescomponibles: $\mathbb{Z}$ y los cíclicos de orden p^n ($\mathbb{Q}$ no es finitamente generado por el Problema 49 del Capítulo 5). El resto de esta sección lo dedicaremos a ver que, salvo isomorfismos, no hay otros. Para ello, será importante considerar ciertos grupos que comparten una característica con $\mathbb{Z}_{p^n}$, y que definimos a continuación:

Lema 7.4.5 *Dados un grupo abeliano finito A y un entero positivo primo p, las siguientes condiciones son equivalentes:*

1. *El orden de A es una potencia de p.*
2. *El orden de cada elemento de A es una potencia de p.*

Demostración. Si $|A| = p^n$ entonces cada $a \in A$ tiene orden p^m con $m \leq n$ por el Teorema de Lagrange. Demostraremos el recíproco por inducción en el orden $|A|$, con el caso $|A| = 1$ trivial. Si $|A| > 1$ entonces existe $0 \neq b \in A$, y si ponemos $B = \langle b \rangle$ entonces tenemos $|B| = o(b) = p^m$ para cierto $m \geq 1$. El grupo cociente A/B tiene cardinal menor que $|A|$, y es elemental ver que el orden de todos sus elementos es una potencia de p. Por la hipótesis de inducción se tiene $|A/B| = p^n$ para cierto $n \geq 0$, y en consecuencia $|A| = |B| \cdot |A/B| = p^{m+n}$, como queríamos ver. □

Definición 7.4.6 *Un grupo abeliano finito que verifique las condiciones equivalentes del Lema 7.4.5 se llama un* p-grupo.

Esta definición la extenderemos a grupos no abelianos en la Definición 8.3.3.

Como en la definición no se excluyen las potencias de exponente 0, el grupo trivial es un p-grupo para cualquier primo p. Un ejemplo más sofisticado es $\mathbb{Z}_{25} \times \mathbb{Z}_{625} \times \mathbb{Z}_{625}$, que es un 5-grupo.

Definición 7.4.7 *Dados un grupo abeliano A y un entero primo p, el* subgrupo de p-torsión *de A es*

$$t_p(A) = \{a \in A : \text{ existe } n \in \mathbb{N} \text{ tal que } p^n a = 0\} = \{a \in A : o(a) \text{ es una potencia de } p\}.$$

Dejamos que el lector compruebe que ambos conjuntos son iguales y que forman un subgrupo de A. De hecho, si A es finito, $t_p(A)$ es claramente el mayor *p-subgrupo* de A (es decir, el mayor subgrupo de A que es un p-grupo).

Proposición 7.4.8 *Sea A un grupo abeliano finito y sean $p_1, \ldots, p_k$ los divisores primos de $|A|$. Entonces*

$$A = t_{p_1}(A) \oplus \cdots \oplus t_{p_k}(A),$$

con cada $t_{p_i}(A) \neq 0$.

Demostración. Sea $a \in A$ y sea $o(a) = n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (¿por qué no pueden aparecer otros primos en la factorización de n?). Para cada $i = 1, \ldots, k$ sea $q_i = n/p_i^{\alpha_i}$. Es claro que ningún primo divide a la vez a todos los q_i, por lo que $\text{mcd}(q_1, \ldots, q_k) = 1$ y por tanto existen $m_1, \ldots, m_k \in \mathbb{Z}$ tales que $m_1 q_1 + \cdots + m_k q_k = 1$. Como $p_i^{\alpha_i} q_i a = 0$, se tiene $q_i a \in t_{p_i}(A)$, luego

$$a = m_1 q_1 a + \cdots + m_k q_k a \in t_{p_1}(A) + \cdots + t_{p_k}(A).$$

En consecuencia, $A = t_{p_1}(A) + \cdots + t_{p_k}(A)$.

Para ver que la suma es directa, supongamos que $a_1 + \cdots + a_k = 0$ con cada $a_i \in t_{p_i}(A)$. Por tanto, para cada $i = 1, \ldots, k$, existe β_i tal que $p_i^{\beta_i} a_i = 0$. Sea $m = p_1^{\beta_1} \cdots p_k^{\beta_k}$. Para cada índice i ponemos $t_i = m/p_i^{\beta_i}$, de modo que $t_i a_j = 0$ cuando $i \neq j$, y así

$$t_i a_i = -t_i \sum_{j \neq i} a_j = 0.$$

Entonces $o(a_i)$ divide a t_i y a $p_i^{\beta_i}$, y como éstos son coprimos, se tiene $o(a_i) = 1$ y por tanto $a_i = 0$. Esto prueba que la familia es independiente.

Por último, de la igualdad $A = t_{p_1}(A) \oplus \cdots \oplus t_{p_k}(A)$ se deduce que $|A| = |t_{p_1}(A)| \cdots |t_{p_k}(A)|$. Como el orden de cada $t_{p_i}(A)$ es una potencia de p_i (Lema 7.4.5) y cada p_i divide a $|A|$, deducimos que ese orden es mayor que 1 y por tanto $t_{p_i}(A) \neq 0$. □

El siguiente corolario es inmediato:

Corolario 7.4.9 *Un grupo finito e indescomponible es un p-grupo para cierto primo p.*

Ejemplos 7.4.10 *Descomposición en suma directa de p-grupos*

1. Sea $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ una factorización prima irredundante del entero n. Por el Teorema Chino de los Restos, $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$ y claramente los factores de esta descomposición van a corresponder con los factores $t_p(\mathbb{Z}_n)$ de la descomposición de la Proposición 7.4.8. Más concretamente, si $q_i = n/p_i^{\alpha_i}$ para cada $i = 1, \ldots, k$, entonces $\overline{q_i} = q_i + n\mathbb{Z}$ genera un grupo de orden $p_i^{\alpha_i}$, y por tanto $t_{p_i}(\mathbb{Z}_n) = \langle \overline{q_i} \rangle$.

2. Sea $A = \mathbb{Z}_{12}^* \propto \mathbb{Z}_{12}$ (véanse los Ejemplos 7.3.7 para la definición de este grupo). Como $|\mathbb{Z}_{12}^*| = 4$ y $|\mathbb{Z}_{12}| = 12$, se tiene $|A| = 48 = 2^4 \cdot 3$. Usando la descripción del orden de cada elemento que se dio en los Ejemplos 7.3.7, se tiene

$$t_3(A) = \{(1,b) : b = 0,4,8\} \qquad \text{y} \qquad t_2(A) = \{(a,b) : b = 0,3,6,9\}$$

(donde identificamos cada entero con su clase módulo 12).

Sea B un subgrupo del grupo abeliano A, y sea $a \in A$. Si $na = 0$ (con $n \in \mathbb{N}$), entonces, en A/B, se tiene $n(a+B) = 0$. Eso implica que el orden de $a+B$ divide al orden de a. En general estos órdenes no coinciden; por ejemplo, no lo hacen si a es un elemento no nulo de B. Se dice entonces que a "baja de orden" en el cociente A/B. El siguiente lema muestra que, en algunas clases laterales, podemos elegir un representante que no baja el orden.

Lema 7.4.11 *Sea A un p-grupo finito. Entonces:*

1. *Existe $a \in A$ tal que $o(a) = p(A)$.*
2. *Si $B = \langle a \rangle$ (donde a es el del apartado anterior) entonces todo elemento del cociente A/B tiene un representante que no baja de orden. Es decir, para todo $\gamma \in A/B$ existe $x \in A$ tal que $x + B = \gamma$ y $o(x) = o(\gamma)$.*

Demostración. El primer apartado se tiene porque el periodo de un grupo abeliano es el mínimo común múltiplo de los ordenes de sus elementos (Ejercicio 7.3.2).

Para el segundo, comenzaremos eligiendo un representante cualquiera de γ, y veremos que podemos sustituirlo por otro con la propiedad requerida. Sea pues $y \in A$ tal que $y + B = \gamma$. Supongamos que $o(a) = p(A) = p^m$, $o(y) = p^s$ y $o(\gamma) = p^k$. Por el párrafo anterior al lema, se tiene $k \leq s \leq m$. Si $k = s$, tomamos $x = y$ y hemos terminado. Supongamos pues que $k < s$. Como $p^k(y+B) = p^k\gamma = 0$, se tiene que $p^k y \in B = \langle a \rangle$; es decir, $p^k y = qa$, para algún $q \in \mathbb{Z}$. Dividiendo q por la mayor potencia posible de p, podemos poner $q = rp^t$ con $\text{mcd}(p,r) = 1$. Entonces

$$p^{m+k-t}y = p^{m-t}p^k y = p^{m-t}qa = rp^m a = 0$$

y, por tanto, $s \leq m + k - t$. Por otro lado,

$$p^{m+k-t-1}y = p^{m-t-1}qa = rp^{m-1}a \neq 0,$$

de donde se deduce que $s = m + k - t$. Sea ahora $x = y - rp^{m-s}a$; entonces $x + B = y + B = \gamma$, y por tanto $o(\gamma) = p^k$ divide a $o(x)$. Pero además, $p^k x = p^k y - rp^{m+k-s}a = p^k y - rp^t a = 0$, de donde se deduce que $o(x) = p^k = o(\gamma)$, como queríamos ver. □

Ahora podemos caracterizar los grupos abelianos finitamente generados que son indescomponibles.

Proposición 7.4.12 *Las siguientes condiciones son equivalentes para un grupo abeliano finitamente generado A:*

1. *A es indescomponible.*
2. *A es isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}_{p^n}$ con p primo y $n \in \mathbb{Z}^+$.*

Demostración. Ya hemos observado (Ejemplos 7.4.2) que los grupos del apartado 2 son indescomponibles. Supongamos pues que A es indescomponible y veamos que es isomorfo a uno de ellos.

Por el Corolario 7.4.3, A es libre de torsión o de torsión. En el primer caso A es isomorfo a $\mathbb{Z}$ por el Teorema 7.3.5 y el Corolario 7.2.9. Supongamos pues que A es de torsión, por lo que debe ser un p-grupo finito (Proposición 7.3.4 y Corolario 7.4.9) y en consecuencia $|A| = p^n$ para cierto $n \geq 1$. Sólo falta demostrar que A es cíclico, cosa que vamos a hacer por inducción sobre n.

El caso $n = 1$ lo resuelve el Teorema 5.8.7. En el caso general, por el Lema 7.4.11, A contiene un elemento a cuyo orden coincide con el periodo de A. Sean $B = \langle a \rangle$ y $C = A/B$. Por la Proposición 7.4.4 se tiene $C = C_1 \oplus \cdots \oplus C_k$ para ciertos $C_1, \ldots, C_k$ indescomponibles. Por hipótesis de inducción, cada C_i es cíclico. Es decir, existen $x_1, \ldots, x_k \in A$ tales que $C_i = \langle x_i + B \rangle$ para cada i, y por el Lema 7.4.11

podemos suponer que $o(x_i) = o(x_i+B)$ para cada i. Claramente $A = B+\langle x_1\rangle+\langle x_2\rangle+\cdots+\langle x_k\rangle$. Vamos a ver que esta suma es directa. Sean $b \in B$ y $m_1, \ldots, m_k \in \mathbb{Z}$ tales que $b + m_1x_1 + \cdots + m_kx_k = 0$. Entonces $0 = m_1(x_1 + B) + \cdots + m_k(x_k + B)$ y, por tanto, cada $m_i(x_i + B) = 0$. De aquí se deduce que m_i es múltiplo de $o(x_i + B) = o(x_i)$ y por tanto $m_ix_i = 0$ y $b = 0$. Como A es indescomponible y $B \neq 0$, deducimos que $A = B = \langle a\rangle$ es cíclico. □

Combinando las Proposiciones 7.4.4 y 7.4.12 se obtiene:

Corolario 7.4.13 *Todo grupo abeliano finitamente generado es suma directa de subgrupos cíclicos (y los que sean finitos se pueden tomar de manera que su orden sea potencia de primo).*

7.5 Descomposiciones primarias e invariantes

El Corolario 7.4.13 va a ser fundamental para clasificar los grupos abelianos finitamente generados salvo isomorfismos. La idea es que cada clase de isomorfía de grupos abelianos finitamente generados estará dada por una lista de números que van a representar los cardinales de los factores que aparecen en una descomposición de cualquiera de los elementos de la clase como suma directa de grupos cíclicos. Vamos a elegir dos tipos de listas de números: En la primera los números que admitimos son potencias de primos y 0; en la segunda los números van a ser números naturales arbitrarios pero con la exigencia de que cada uno de ellos divida a los anteriores.

Definición 7.5.1 *Sea A un grupo abeliano finitamente generado. Una* descomposición primaria *o* indescomponible *de A es una expresión de A como suma directa de subgrupos indescomponibles. Como cada uno de estos sumandos es isomorfo a $\mathbb{Z}$ ó a $\mathbb{Z}_{p^n}$, con p primo y $n \geq 1$, siempre podemos reordenarlos de modo que se tenga*

$$\begin{aligned} A &= (\oplus_{j=1}^{n} A_j) \oplus (\oplus_{j=1}^{m_1} A_{1j}) \oplus \cdots \oplus (\oplus_{j=1}^{m_k} A_{kj}) \\ &= A_1 \oplus A_2 \oplus \cdots \oplus A_n \oplus \\ &\quad A_{11} \oplus A_{12} \oplus \cdots \oplus A_{1m_1} \oplus \\ &\quad \cdots \\ &\quad A_{k1} \oplus A_{k2} \oplus \cdots \oplus A_{km_k} \end{aligned}$$

con $p(A_i) = 0$ (es decir, A_i es cíclico infinito) y $p(A_{ij}) = p_i^{\alpha_{ij}}$ para ciertos enteros primos positivos $p_1 < p_2 < \cdots < p_k$ y ciertos enteros positivos α_{ij} con $\alpha_{i1} \geq \alpha_{i2} \geq \cdots \geq \alpha_{im_i} \geq 1$ para cada $i = 1, \ldots, k$.

Con esta terminología, la Proposición 7.4.4 se reenuncia como:

Teorema 7.5.2 *Todo grupo abeliano finitamente generado tiene una descomposición primaria.*

Para obtener una descomposición primaria de un grupo abeliano finitamente generado seguimos los pasos indicados en la sección anterior; es decir, dado un grupo abeliano finitamente generado A:

1. Se calcula $T = t(A)$ y un subgrupo libre de torsión L de A tal que $A = T \oplus L$ (Corolario 7.3.6).

2. Se busca una base $b_1, \ldots, b_n$ de L y por tanto se tiene $L = \langle b_1\rangle \oplus \cdots \oplus \langle b_n\rangle \cong \mathbb{Z}^n$. Esta es la "primera fila" en la ordenación de los sumandos que se propone en la Definición 7.5.1.

3. Se calcula $t_p(T)$ para cada divisor primo de $|T|$; entonces $T = t_{p_1}(T) \oplus \cdots \oplus t_{p_k}(T)$ (Proposición 7.4.8).

4. Para cada divisor primo p de $|T|$ se calcula $a \in t_p(T)$ tal que $o(a)$ coincida con el periodo de $t_p(T)$ (Proposición 7.4.11) y pasamos a estudiar $t_p(T)/\langle a\rangle$, que tiene orden menor que el de $t_p(T)$. Por recurrencia vamos pasando a grupos de orden cada vez más pequeño hasta obtener un grupo cíclico. Volvemos para atrás siguiendo la demostración de la Proposición 7.4.12 y así obtendremos una descomposición primaria de $t_p(T)$, que ocupará una fila en la ordenación de los sumandos según la Definición 7.5.1.

Ejemplos 7.5.3 *Descomposiciones primarias.*

1. Sea $A = \langle 2, i\rangle$ el grupo del Ejemplo 7.3.7. Ya vimos que $t(A) = \langle i\rangle$ y $A = \langle i\rangle \oplus \langle 2\rangle$. Como $\langle i\rangle$ es cíclico de orden 4, hemos obtenido una descomposición primaria de A.

2. Sea $A = \mathbb{Z}^* \propto \mathbb{Z}$. Vimos que $t(A) = \langle(-1,0)\rangle$ y $A = \langle(-1,0)\rangle \oplus \langle(1,1)\rangle$. Como $\langle(-1,0)\rangle$ es cíclico de orden 2, la anterior es una descomposición primaria de A.

3. Sea $A = \mathbb{Z}_{12}^* \propto \mathbb{Z}_{12}$. Como este grupo es finito, no hay que dar los dos primeros pasos, y el tercero lo habíamos dado en el Ejemplo 7.4.10. Claramente $t_3(A) = \{(1,b) : b = 0,4,8\}$ es cíclico de orden 3, generado por $(1,4)$. Sin embargo $t_2(A) = \{(a,b) : b = 0,3,6,9\}$ no es cíclico ya que su cardinal es 16 y su periodo 4. Un elemento de orden 4 es $(1,3)$. Pongamos

$$B = \langle(1,3)\rangle = \{(1,0),(1,3),(1,6),(1,9)\}$$

y $C = t_2(A)/B$, que tiene orden 4. Obsérvese que $x^2 \in B$ para todo $x \in t_2(A)$. Por tanto $C \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, de donde se deduce que si C_1 y C_2 son dos subgrupos C de orden 2 y distintos, entonces $C = C_1 \oplus C_2$ es una descomposición primaria de C. Uno de estos subgrupos puede ser $\langle(-1,3)B\rangle$ (notación multiplicativa), pero como $(-1,3)$ no tiene orden 2 en A, es necesario cambiarlo, como hicimos en la demostración del Lema 7.4.11, por otro elemento de la misma clase módulo B que no baje el orden, por ejemplo $(-1,3)(1,3) = (-1,0)$ está en $(-1,3)B$ y tiene orden 2. El otro subgrupo puede ser $\langle(5,0)B\rangle$, de donde se obtiene que $C = \langle(-1,0)B\rangle \oplus \langle(5,0)B\rangle$ y, por tanto,

$$t_2(A) = \langle(1,3)\rangle \oplus \langle(-1,0)\rangle \oplus \langle(5,0)\rangle.$$

Uniendo toda la información obtenemos

$$A = \langle(1,3)\rangle \oplus \langle(-1,0)\rangle \oplus \langle(5,0)\rangle \oplus \langle(1,4)\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Definición 7.5.4 *Sea A un grupo abeliano finitamente generado. Una* descomposición invariante *de A es una expresión del tipo*

$$A = \oplus_{i=1}^n A_i,$$

donde cada A_i es un grupo cíclico no trivial y se verifica $p(A_i) \mid p(A_{i-1})$ para cada $i = 2,\ldots,n$.

Ejercicio 7.5.5 *Demostrar que, si $A = \oplus_{i=1}^n C_i$ es una descomposición invariante A y el subíndice k es tal que $p(C_k) = 0 \neq p(C_{k+1})$, entonces el subgrupo de torsión de A es $t(A) = \oplus_{i=k+1}^n C_i$.*

Utilizando el Teorema 7.5.2 podemos obtener también:

Teorema 7.5.6 *Todo grupo abeliano finitamente generado tiene una descomposición invariante.*

Demostración. Sea A un grupo abeliano finitamente generado. Añadiendo sumandos triviales a una descomposición primaria suya, tenemos

$$\begin{aligned} A \;=\; & A_1 \oplus A_2 \oplus \cdots \oplus A_n \oplus \\ & A_{11} \oplus A_{12} \oplus \cdots \oplus A_{1m} \oplus \\ & \cdots \\ & A_{k1} \oplus A_{k2} \oplus \cdots \oplus A_{km}, \end{aligned}$$

donde cada sumando es cíclico y se tiene $p(A_i) = 0$ y $p(A_{ij}) = p_i^{\alpha_{ij}}$, para ciertos primos positivos distintos $p_1, p_2, \ldots, p_k$ y ciertos enteros α_{ij} tales que, para cada i,

$$\alpha_{11} \geq \alpha_{12} \geq \ldots \geq \alpha_{1m} \geq 0. \tag{7.5.1}$$

Los α_{ij} que valen cero se corresponden con los sumandos triviales que hemos añadido para que, en cada fila de la descomposición de A, a partir de la segunda, haya el mismo número de sumandos.

Para obtener la descomposición primaria basta con "agrupar los sumandos por columnas", a partir de la segunda fila. Explícitamente, para cada $j = 1,\ldots,m$, sea

$$B_j = A_{1j} \oplus A_{2j} \oplus \cdots \oplus A_{kj}.$$

Entonces

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_n \oplus B_1 \oplus B_2 \oplus \cdots \oplus B_m$$

y, por el Teorema Chino de los Restos, cada B_j es cíclico de orden $d_j = p^{\alpha_{1j}} p^{\alpha_{2j}} \cdots p^{\alpha_{mj}}$. Como consecuencia de las desigualdades (7.5.1) se tiene que $d_j \mid d_{j-1}$ para todo $j = 2, \ldots, n$. □

La demostración del Teorema 7.5.6 nos dice cómo se obtiene una descomposición invariante a partir de una descomposición primaria.

Ejemplos 7.5.7 *Descomposiciones invariantes a partir de descomposiciones primarias.*

1. Supongamos dada una descomposición primaria de A, digamos

$$A = (A_1 \oplus A_2) \oplus (A_{21} \oplus A_{22} \oplus A_{23} \oplus A_{24}) \oplus (A_{31} \oplus A_{32}) \oplus (A_{71} \oplus A_{72} \oplus A_{73}),$$

donde $A_{ij} = \langle a_{ij} \rangle$ y los ordenes de los respectivos sumandos son (por este orden) 0,0,16, 4, 2, 2, 27, 3, 7, 7, 7. Entonces:

- $B_1 = A_{21} \oplus A_{31} \oplus A_{71} = \langle a_{21} + a_{31} + a_{71} \rangle$ es cíclico de orden $16 \cdot 27 \cdot 7 = 3.024$;
- $B_2 = A_{22} \oplus A_{32} \oplus A_{72} = \langle a_{22} + a_{32} + a_{72} \rangle$ es cíclico de orden $4 \cdot 3 \cdot 7 = 84$;
- $B_3 = A_{23} \oplus A_{73} = \langle a_{23} + a_{73} \rangle$ es cíclico de orden $2 \cdot 7 = 14$ y
- $B_4 = A_{24}$ es cíclico de orden 2.

Entonces

$$A = A_1 \oplus A_2 \oplus B_1 \oplus B_2 \oplus B_3 \oplus B_4 \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_{3.024} \times \mathbb{Z}_{84} \times \mathbb{Z}_{14} \times \mathbb{Z}_2$$

es una descomposición invariante de A.

2. Sea $A = \mathbb{Z}_{12}^* \propto \mathbb{Z}_{12}$. En los Ejemplos 7.5.3 vimos que

$$A = \langle (1,3) \rangle \oplus \langle (-1,0) \rangle \oplus \langle (5,0) \rangle \oplus \langle (1,4) \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$$

es una descomposición primaria de A. Por tanto

$$A = \langle (1,7) \rangle \oplus \langle (-1,0) \rangle \oplus \langle (5,0) \rangle \cong \mathbb{Z}_{12} \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

es una descomposición invariante de A.

También es fácil sacar consecuencias de la demostración del Teorema 7.5.6 para obtener descomposiciones primarias a partir de descomposiciones invariantes.

Ejemplo 7.5.8 *Descomposiciones primarias a partir de descomposiciones invariantes.*
Sea

$$A = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \langle a_3 \rangle \oplus \langle a_4 \rangle \cong \mathbb{Z}_{2.025} \times \mathbb{Z}_{135} \times \mathbb{Z}_9$$

(donde el isomorfismo es componente a componente). Observando que $2.025 = 3^4 \cdot 5^2$ y $135 = 3^3 \cdot 5$, definimos

$$\begin{array}{ll} B_{31} = \langle 25a_1 \rangle \cong \mathbb{Z}_{81}, & B_{51} = \langle 81a_1 \rangle \cong \mathbb{Z}_{25} \\ B_{32} = \langle 5a_2 \rangle \cong \mathbb{Z}_{27}, & B_{52} = \langle 27a_2 \rangle \cong \mathbb{Z}_5 \\ B_{33} = \langle a_4 \rangle \cong \mathbb{Z}_9. & \end{array}$$

Entonces $A = B_{31} \oplus B_{32} \oplus B_{33} \oplus B_{51} \oplus B_{52}$ es una descomposición primaria de A.

Por supuesto, es posible descomponer un grupo abeliano finito como suma directa de subgrupos cíclicos sin ajustarse a ninguno de los "formatos" de las descomposiciones primarias o invariantes. Por ejemplo, si $A = \mathbb{Z}_6 \times \mathbb{Z}_3 \times \mathbb{Z}_2$ entonces la descomposición

$$A = \langle (1,0,0) \rangle \oplus \langle (0,1,0) \rangle \oplus \langle (0,0,1) \rangle$$

no es de ninguno de esos dos tipos, aunque no es difícil obtener una descomposición primaria

$$A = \langle (2,0,0)\rangle \oplus \langle (3,0,0)\rangle \oplus \langle (0,1,0)\rangle \oplus \langle (0,0,1)\rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2$$

y una invariante

$$A = \langle (1,0,0)\rangle \oplus \langle (0,1,1)\rangle \cong \mathbb{Z}_6 \times \mathbb{Z}_6.$$

Lo importante de estas descomposiciones es que presentan buenas condiciones de unicidad. En efecto, como vamos a ver, cualesquiera dos descomposiciones primarias de un grupo A (abeliano y finitamente generado) son "esencialmente iguales", lo que nos permite asignarle a un tal grupo una lista de números enteros (los periodos de los sumandos que aparecen en una de esas descomposiciones). Otro tanto podrá decirse de las descomposiciones invariantes. Además, estas listas de números determinan salvo isomorfismos al grupo A, en el mismo sentido en el que la dimensión determina salvo isomorfismos a un espacio vectorial de dimensión finita. Aunque el caso que nos ocupa es más sofisticado, en ambos somos capaces de asociar a un objeto (grupo o espacio vectorial) una lista de números (uno sólo, la dimensión, en el caso vectorial) de tal modo que dos objetos son isomorfos si y sólo si tienen la misma lista.

Definición 7.5.9 *Sean A y B dos grupos abelianos finitamente generados.*

Dos descomposiciones primarias de A y B son semejantes *si los sumandos que intervienen son isomorfos dos a dos. Si ordenamos las descomposiciones como se ha indicado en la Definición 7.5.1, digamos*

$$A = (\oplus_{j=1}^{n} A_j) \oplus (\oplus_{j=1}^{m_1} A_{1j}) \oplus \cdots \oplus (\oplus_{j=1}^{m_k} A_{kj})$$

y

$$B = (\oplus_{j=1}^{n'} B_j) \oplus (\oplus_{j=1}^{m'_1} B_{1j}) \oplus \cdots \oplus (\oplus_{j=1}^{m'_{k'}} B_{k'j}),$$

es claro que éstas son semejantes si y sólo si $n = n'$, $k = k'$, cada $m_i = m'_i$ y $p(A_{ij}) = p(B_{ij})$ para cada posible par de índices.

Dos descomposiciones invariantes $A = \oplus_{i=1}^{n} A_i$ y $B = \oplus_{i=1}^{n'} B_i$ son semejantes *si los sumandos que intervienen son isomorfos dos a dos, lo que claramente equivale a que tengan el mismo número de sumandos ($n = n'$) y las mismas listas de periodos ($p(A_i) = p(B_i)$ para todo $i = 1, \ldots, n$).*

Es fácil ver que, si A y B tienen descomposiciones primarias (o invariantes) semejantes, entonces A y B son isomorfos. El siguiente teorema nos dice, esencialmente, que se verifica el recíproco:

Teorema 7.5.10 *Sea A un grupo abeliano finitamente generado. Entonces:*

1. *Todas las descomposiciones primarias de A son semejantes.*
2. *Todas las descomposiciones invariantes de A son semejantes.*

Demostración. En vista de que se puede pasar de una descomposición primaria a una invariante y viceversa, bastará con demostrar una de las dos afirmaciones. Demostraremos la primera.

Sea

$$A = (\oplus_{j=1}^{n} A_j) \oplus (\oplus_{j=1}^{m_1} A_{1j}) \oplus \cdots \oplus (\oplus_{j=1}^{m_k} A_{kj})$$

una descomposición primaria de A con $p(A_i) = 0$ y $p(A_{ij}) = p_i^{\alpha_{ij}}$ para ciertos enteros primos positivos $p_1 < p_2 < \cdots < p_k$ y ciertos enteros positivos α_{ij} con $\alpha_{i1} \geq \alpha_{i2} \geq \cdots \geq \alpha_{im_i} \geq 1$ para cada $i = 1, \ldots, k$. Obsérvese que $\oplus_{j=1}^{n} A_j \cong A/t(A)$, por lo que n es el rango del grupo libre $A/t(A)$ y por tanto está determinado por A (no depende de la descomposición particular elegida). Por otro lado, es claro que, para cada $i = 1, \ldots, k$, se tiene

$$\oplus_{j=1}^{m_i} A_{ij} = t_{p_i}(A),$$

por lo que estos subgrupos también están determinados por A. En consecuencia, podemos limitarnos a demostrar la unicidad asumiendo que A es un p-grupo finito.

En esta situación, dos descomposiciones primarias de A serán de la forma

$$A = A_1 \oplus \cdots \oplus A_n = B_1 \oplus \cdots \oplus B_m,$$

donde cada sumando es cíclico y, si ponemos $p(A_i) = p^{\alpha_i}$ y $p(B_i) = p^{\beta_i}$, se tiene $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$ y $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_m$. Vamos a ver, por inducción en i, que $\alpha_i = \beta_i$ para cada i.

Obsérvese que $p^{\alpha_1} = p(A) = p^{\beta_1}$, lo que resuelve el caso $i = 1$. Supongamos pues que $\alpha_j = \beta_j$ para cada $j = 1, \ldots, i-1$, y veamos que $\alpha_i = \beta_i$. Podemos suponer sin pérdida de generalidad que $\alpha_i \leq \beta_i$.

Observemos lo siguiente: Sea C un grupo cíclico de orden p^r y sea $s \in \mathbb{N}$. Se tiene $p^s C = 0$ si y sólo si $s \geq r$. Por otra parte, si $s \leq r$, entonces $p^s C$ es cíclico de orden p^{r-s} por la Proposición 5.8.11. En consecuencia, si ponemos $q = p^{\alpha_i}$, se tiene

$$\begin{aligned} qA &\cong qA_1 \oplus \cdots \oplus qA_{i-1} \\ &\cong (qB_1 \oplus \cdots \oplus qB_{i-1}) \oplus (qB_i \oplus \cdots \oplus qB_m). \end{aligned}$$

Como $qA_1 \oplus \cdots \oplus qA_{i-1}$ y $qB_1 \oplus \cdots \oplus qB_{i-1}$ tienen el mismo cardinal, deducimos que $qB_i \oplus \cdots \oplus qB_m = 0$. En particular $0 = qB_i = p^{\alpha_i} B_i$, de modo que $\alpha_i \geq \beta_i$, y por tanto $\alpha_i = \beta_i$, como queríamos ver. □

Definición 7.5.11 *Sea A un grupo abeliano finitamente generado. Sea*

$$A = \oplus_{i=1}^{n} A_i \tag{7.5.2}$$

una descomposición primaria ordenada como en la Definición 7.5.1. Entonces la lista $(p(A_1), \ldots, p(A_n))$ (que no depende de la descomposición primaria elegida, por el Teorema 7.5.10) se conoce como la lista de los divisores elementales *de A.*

Análogamente, si (7.5.2) es una descomposición invariante, entonces la lista $(p(A_1), \ldots, p(A_n))$ (que tampoco depende de la descomposición invariante elegida) se conoce como la lista de los factores invariantes *de A.*

En ambas listas, cada sumando cíclico infinito aporta un 0 al principio de la lista. A menudo se simplifica la notación escribiendo $(m; p(A_{m+1}), \ldots, p(A_n))$, donde m es el número de ceros en la lista original.

Ejemplos 7.5.12 *Listas de divisores elementales y factores invariantes.*

1. Si A es el grupo del primer apartado de los Ejemplos 7.5.7, la lista de sus divisores elementales es $(2; 16, 4, 2, 2, 27, 3, 7, 7, 7)$, y la de sus factores invariantes es $(2; 3.024, 84, 14)$.

2. Para el grupo $\mathbb{Z}^* \propto \mathbb{Z}$, las listas de divisores elementales y de factores invariantes coinciden, y son $(0, 2)$. ¿Para qué tipo de grupos coinciden ambas listas?

3. Los divisores elementales de $\mathbb{Z}_{12}^* \propto \mathbb{Z}_{12}$ son $(4, 2, 2, 3)$, y sus factores invariantes son $(12, 2, 2)$.

Todo lo visto en esta sección se resume en el siguiente Teorema:

Teorema 7.5.13 (Teorema de Estructura de Grupos Abelianos Finitamente Generados)

1. *Todo grupo abeliano finitamente generado tiene una descomposición primaria y una descomposición invariante.*

2. *Las siguientes condiciones son equivalentes para dos grupos abelianos:*

   (a) *Son isomorfos.*

   (b) *Tienen descomposiciones primarias semejantes.*

   (c) *Tienen descomposiciones invariantes semejantes.*

   (d) *Tienen la misma lista de divisores elementales.*

   (e) *Tienen la misma lista de factores invariantes.*

Ejercicio 7.5.14

1. *Demostrar que, si $n \in \mathbb{Z}^+$ es libre de cuadrados, entonces todo grupo abeliano finito de orden n es cíclico (y por tanto isomorfo a $\mathbb{Z}_n$).*

2. *Si p es un primo positivo, demostrar que, salvo isomorfismos, los únicos grupos abelianos de orden p^2 son $\mathbb{Z}_{p^2}$ y $\mathbb{Z}_p \times \mathbb{Z}_p$. Además se puede borrar "abelianos".*

3. *Describir, salvo isomorfismos, todos los grupos abelianos de órdenes 8, 12, 16, 20 y 24.*

Ejercicio 7.5.15 *Demostrar el recíproco del Teorema de Lagrange para grupos abelianos finitos. Es decir, demostrar que un grupo abeliano de orden n tiene un subgrupo de orden m para cada divisor m de n.*

Ejemplos 7.5.16 *Algunas decomposiciones invariantes y primarias.*

1. Los grupos multiplicativos $\mathbb{Z}_5^*$, $\mathbb{Z}_{10}^*$ y $\mathbb{Z}_{12}^*$ tienen 4 elementos (pues $\phi(5) = \phi(10) = \phi(12) = 4$). Los dos primeros son cíclicos (busca un generador), y por tanto isomorfos entre sí. El tercero no es cíclico (tiene periodo 2), y por el ejercicio anterior debe ser isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ (da un isomorfismo explícito).

2. Los grupos multiplicativos $\mathbb{Z}_{15}^*$, $\mathbb{Z}_{16}^*$, $\mathbb{Z}_{20}^*$, $\mathbb{Z}_{24}^*$ y $\mathbb{Z}_{30}^*$ tienen 8 elementos, por lo que han de ser isomorfos a uno de estos tres: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ ó $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Considerando los órdenes de los elementos se deduce que ninguno es cíclico, que $\mathbb{Z}_{24}^*$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ y que los otros cuatro son isomorfos a $\mathbb{Z}_4 \times \mathbb{Z}_2$.

3. Vamos a calcular todos los grupos abelianos de orden 420 salvo isomorfismos y sus descomposiciones invariantes y primarias. Como $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, las posibles listas de divisores elementales son $(4, 3, 5, 7)$ ó $(2, 2, 3, 5, 7)$. Por tanto, salvo isomorfismos, los grupos abelianos de orden 420 son

$$A = \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \quad \text{y} \quad B = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7.$$

   Éstas son sus descomposiciones primarias. Sus descomposiciones invariantes serán

$$A = \mathbb{Z}_{420} \quad \text{y} \quad B = \mathbb{Z}_{210} \times \mathbb{Z}_2.$$

Por el Teorema de Estructura 7.5.13, todo grupo abeliano finitamente generado es suma directa de cíclicos. Esto no es cierto para grupos abelianos en general, considérese $\mathbb{Q}$; ni siquiera para grupos abelianos de torsión, como muestra el siguiente ejemplo.

Ejemplo 7.5.17 *Un grupo abeliano de torsión que no es suma directa de grupos cíclicos.*
Sea p un número primo. El conjunto X_p de los números racionales de la forma $\frac{m}{p^n}$, donde $m \in \mathbb{Z}$ y n es un entero no negativo, es un subgrupo de $\mathbb{Q}$. Además $\mathbb{Z}$ es un subgrupo de X_p. Se define $\mathbb{Z}_{p^\infty} = X_p/\mathbb{Z}$. Para cada entero no negativo n, sea A_n el subgrupo de $\mathbb{Z}_{p^\infty}$ generado por $a_n = \frac{1}{p^n} + \mathbb{Z}$. Como a_n tiene orden p^n, entonces A_n es isomorfo a $\mathbb{Z}_{p^n}$. Además $0 = A_0 \subset A_1 \subset A_2 \subset \cdots$ y $\cup_{n \in \mathbb{N}} A_n = \mathbb{Z}_{p^\infty}$.

Vamos a ver que todo subgrupo propio H de $\mathbb{Z}_{p^\infty}$ es igual a A_n para algún $n \in \mathbb{N}$. El conjunto de los números naturales n tales que $a_n \in H$ está acotado (¿por qué?). Sea n el máximo de dicho conjunto. Entonces $A_n \subseteq H$. Si $\frac{m}{p^t} + \mathbb{Z} \in H$, con $\mathrm{mcd}(m, p) = 1$, entonces existen $x, y \in \mathbb{Z}$ tales que $xm + yp^t = 1$. Luego $a_t = \frac{1}{p^t} + \mathbb{Z} = x\frac{m}{p^t} + y + \mathbb{Z} = x(\frac{m}{p^t} + \mathbb{Z}) \in H$, y por tanto $t \leq n$, de donde se concluye que $\frac{m}{p^t} + \mathbb{Z} = mp^{n-t}a_n \in A_n$. Deducimos que $H = A_n$, como queríamos.

La conclusión final es que $\mathbb{Z}_{p^\infty}$ es indescomponible y, como no es cíclico, tampoco es suma directa de grupos cíclicos.

7.6 Presentaciones por generadores y relaciones

Sea L un grupo abeliano libre con base $\{a_1, \ldots, a_n\}$ y sea S un subgrupo de L. Sabemos que S ha de estar generado por un conjunto finito $\{r_1, \ldots, r_m\}$ de elementos de L; es decir, cada r_i será una combinación lineal con coeficientes enteros de los a_j, digamos

$$r_i = k_{i1}a_1 + \cdots + k_{in}a_n \qquad (k_{ij} \in \mathbb{Z}).$$

Consideremos ahora el grupo cociente L/S. Abusando de la notación, escribiremos $a_j = a_j + S$. Entonces $\{a_1, \ldots, a_n\}$ es un conjunto generador de L/S, y para cada $i = 1, \ldots, m$ se tiene

$$k_{i1}a_1 + \cdots + k_{in}a_n = 0 \qquad (\text{en } L/S).$$

Estas igualdades se llaman "relaciones" entre los generadores $a_1, \ldots, a_n$ del grupo L/S. Es decir, los a_i son generadores "libres" (linealmente independientes, sin relaciones no triviales) cuando los vemos en L, pero satisfacen ciertas relaciones en el cociente L/S.

Por la Proposición 7.2.10, todo grupo abeliano finitamente generado A es isomorfo a uno de la forma recién descrita, y de hecho es usual encontrar grupos abelianos dados de esa manera. Dados L y S en la situación anterior y tales que $A \cong L/S$, escribiremos

$$A = \langle a_1, \ldots, a_n \mid r_1, \ldots, r_m \rangle,$$

y diremos que ésta es una *presentación de A por generadores y relaciones.*

Un resultado básico para el manejo de las presentaciones por generadores y relaciones es el siguiente:

Ejercicio 7.6.1 *Sea A un grupo abeliano que es suma directa de subgrupos: $A = A_1 \oplus \cdots \oplus A_n$. Para cada $i = 1, \ldots, n$, sea B_i un subgrupo de A_i. Entonces la familia $B_1, \ldots, B_n$ es independiente y, si $B = B_1 \oplus \cdots \oplus B_n$, se verifica*

$$\frac{A}{B} \cong \frac{A_1}{B_1} \times \cdots \times \frac{A_n}{B_n}$$

donde, si algún B_i coincide con A_i, el correspondiente factor es trivial y se puede eliminar del producto. (Indicación: Usar el Primer Teorema de Isomorfía.)

Como consecuencia, las presentaciones en las que cada relación es un múltiplo entero de un generador nos permiten ver al grupo en cuestión como suma directa de cíclicos de modo inmediato. Explícitamente, el hecho de que A tenga una presentación del tipo

$$A = \langle a_1, \ldots, a_r \mid d_1a_1, \ldots, d_sa_s \rangle$$

(con $s \leq r$ y cada $d_i \in \mathbb{Z}^+$) equivale a decir que

$$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

con $r - s$ factores iguales a $\mathbb{Z}$, y podemos eliminar los factores con $d_i = 1$. Por ejemplo, las siguientes son varias expresiones por generadores y relaciones de grupos abelianos finitamente generados:

$$\mathbb{Z}^n = \langle a_1, \ldots, a_n \rangle, \qquad \mathbb{Z}_n = \langle a \mid na \rangle, \qquad \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle a, b, c \mid 2b, 3c \rangle.$$

Un grupo puede tener diversas presentaciones. Por ejemplo, $\mathbb{Z} = \langle a \rangle = \langle a, b \mid b \rangle$ o, utilizando el Teorema Chino de los Restos, $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle a, b \mid 2a, 3b \rangle = \langle c \mid 6c \rangle$. En esta sección veremos cómo conseguir, a partir de una presentación por generadores y relaciones de un grupo abeliano finitamente generado A, otras presentaciones más manejables, con el objetivo último de obtener una presentación del tipo $\langle a_1, \ldots, a_r \mid d_1a_1, \ldots, d_sa_s \rangle$ con $d_1 \mid d_2 \mid \cdots \mid d_s$, lo que nos dará la descomposición invariante de A.

La segunda herramienta básica para la manipulación de las presentaciones es:

Ejercicio 7.6.2 *Sean $a_1, a_2, \ldots, a_n$ elementos de un grupo abeliano A. Si, o bien $a_1' = a_1 + ta_2$, donde $t \in \mathbb{Z}$, o bien $a_1' = -a_1$, entonces:*

1. *$\langle a_1, a_2, \ldots, a_n \rangle = \langle a_1', a_2, \ldots, a_n \rangle$.*
2. *El conjunto $\{a_1, a_2, \ldots, a_n\}$ es linealmente independiente si y sólo si lo es $\{a_1', a_2, \ldots, a_n\}$.*

En otras palabras, si en un conjunto sumamos a un elemento un múltiplo entero de otro, o si cambiamos de signo un elemento, no cambian ni el subgrupo generado ni la dependencia o independencia lineal. Aplicando reiteradamente el Ejercicio 7.6.2, vemos que la afirmación sigue valiendo si sumamos a un elemento una combinación lineal (con coeficientes enteros) del resto de elementos.

Veamos con un ejemplo cómo pueden usarse estos resultados para simplificar las presentaciones:

Ejemplo 7.6.3 *Simplificación de una presentación por generadores y relaciones.*
Sea $A = \langle a, b, c \mid 2a + b + 6c,\ 2a + 2b + 2c \rangle$. Esto significa que $A \cong L/S$, donde $\{a, b, c\}$ es base de L y $S = \langle 2a + b + 6c, 2a + 2b + 2c \rangle$. Si hacemos $b' = 2a + b + 6c$, entonces $\{a, b', c\}$ sigue siendo base de L y se tiene $2a + 2b + 2c = -2a + 2b' - 10c$, luego $S = \langle b', -2a + 2b' - 10c \rangle$; restando al segundo generador el doble del primero, y cambiando luego el signo del resultado, obtenemos $S = \langle b', 2a + 10c \rangle$. Por tanto, $A = \langle b', a, c \mid b', 2a + 10c \rangle$. Podemos simplificar más, haciendo $a' = a + 5c$. Entonces $\{b', a', c\}$ sigue siendo base de L y además $S = \langle b', 2a' \rangle$, de modo que $A = \langle b', a', c \mid b', 2a' \rangle = \langle a', c' \mid 2a' \rangle$. Por tanto $A \cong \mathbb{Z}_2 \times \mathbb{Z}$.

En lo que sigue vemos cómo las ideas usadas en el Ejemplo 7.6.3 son suficientes para simplificar cualquier presentación. Lo primero que haremos será adoptar una notación matricial para las presentaciones que las hace más manejables. Supongamos que partimos de una expresión de un grupo por generadores y relaciones $A = \langle a_1, \ldots, a_n \mid r_1, \ldots, r_m \rangle$, donde las relaciones vienen dadas por las combinaciones lineales

$$r_i = k_{i1}a_1 + \cdots + k_{in}a_n \qquad (k_{ij} \in \mathbb{Z}). \tag{7.6.3}$$

Representamos este conjunto de relaciones por una matriz $K = (k_{ij})$. Recíprocamente, a cada matriz K de números enteros con m filas y n columnas, le asociaremos el grupo cuya presentación por generadores y relaciones es $\langle a_1, \ldots, a_n \mid r_1, \ldots, r_m \rangle$, donde cada r_i viene dado por la igualdad (7.6.3). En particular, una matriz $m \times n$ de la forma

$$\begin{pmatrix} d_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & d_m & 0 & \cdots & 0 \end{pmatrix} \tag{7.6.4}$$

se corresponde con el grupo abeliano $A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, con $n - m$ factores iguales a $\mathbb{Z}$.

Comenzaremos notando que ciertas transformaciones en una matriz no alteran el grupo que define, y después veremos cómo combinar esas transformaciones para alcanzar una matriz del tipo (7.6.4).

Lema 7.6.4 *Si K es una matriz de números enteros y K' es una matriz obtenida a partir de K mediante una de las operaciones que siguen, entonces los grupos asociados a K y K' son isomorfos.*

F0: Eliminar una fila formada por ceros.

F1: Reordenar las filas.

F2: Cambiar el signo a todos los elementos de una fila.

F3: Sumar a una fila un múltiplo entero de otra.
(Si a la fila i-ésima le sumamos la j-ésima multiplicada por t, escribiremos $F_i + tF_j$).

C1: Reordenar las columnas.

C2: Cambiar el signo a todos los elementos de una columna.

C3: Sumar a una columna un múltiplo entero de otra.
(Si a la columna i-ésima le sumamos la j-ésima multiplicada por t, escribiremos $C_i + tC_j$).

Demostración. Con la notación L/S que venimos usando, las operaciones en las filas se traducen en manipulaciones de los generadores de S (o sea, de las relaciones en L/S) que no afectan al subgrupo: quitar un generador nulo, reordenar los generadores, sustituir uno por su opuesto, o sumarle a uno un múltiplo de otro.

Vemos ahora que la operación C3 no afecta a L ni a S, y dejamos que el lector analice por qué son también admisibles las operaciones de los tipos C1 y C2. Supongamos, para simplificar, que la operación es $C_1 + tC_2$. Si $\{a_1, \ldots, a_n\}$ es la base de L y ponemos $a_2' = a_2 - ta_1$, entonces $\{a_1, a_2', \ldots, a_n\}$ también es base de L. Si la matriz de partida es (k_{ij}) entonces el generador r_i es

$$\begin{aligned} r_i &= k_{i1}a_1 + k_{i2}a_2 + k_{i3}a_3 + \cdots + k_{in}a_n \\ &= k_{i1}a_1 + k_{i2}(a_2' + ta_1) + k_{i3}a_3 + \cdots + k_{in}a_n \\ &= (k_{i1} + tk_{i2})a_1 + k_{i2}a_2' + k_{i3}a_3 + \cdots + k_{in}a_n, \end{aligned}$$

por lo que la matriz obtenida al aplicar C3 representa a los mismos generadores de S, aunque expresados en una base distinta. En conclusión, la operación C3 no supone ningún cambio en L ni en S. □

A continuación describimos un método para pasar, mediante operaciones de los tipos anteriores, de una matriz cualquiera con coeficientes enteros a una matriz del tipo (7.6.4) en la que $d_1 \mid d_2 \mid \cdots \mid d_m$. Cada vez que hablemos de "la matriz K" nos estaremos refiriendo a la última matriz obtenida a partir de la inicial mediante las operaciones que se hayan descrito.

Comencemos notando el siguiente hecho: Sea a una entrada no nula de K con el menor valor absoluto (podemos suponer que $a > 0$, cambiando si hace falta el signo de su fila), y supongamos que a no divide a todas las entradas de K. Entonces podemos transformar K hasta hacer aparecer una entrada r con $0 < r < a$. Para ello, comenzamos haciendo operaciones F1 y C1 para poner a en la entrada $(1,1)$; este paso lo damos sólo por comodidad en la notación. Supongamos que a no divide a cierta entrada de la primera fila, digamos k_{1j} (con $j \neq 1$). Dividiendo con resto, encontramos $q, r \in \mathbb{Z}$ con $0 < r < a$ y $k_{1j} = aq + r$. Entonces la operación $C_j - qC_1$ nos da una matriz con r en la entrada $(1,j)$, como queríamos. Si a no divide a una entrada de la primera columna procedemos de modo análogo, operando esta vez por filas. Podemos pues suponer que a divide a todas las entradas de la primera fila y a todas las de la primera columna, pero no divide a cierto k_{ij} con $i, j \neq 1$. Por hipótesis, existen enteros b y c tales que $k_{1j} = ba$ y $k_{i1} = ca$. Haciendo primero la operación $F_i - cF_1$ (para poner un 0 en la entrada $(i,1)$) y después la operación $F_1 - F_i$, obtenemos una matriz con a en la entrada $(1,1)$ y $ba + bca - k_{ij}$ en la entrada $(1,j)$. Como a no divide a esta entrada de la primera fila, procedemos como al principio de este párrafo para obtener una entrada r con $0 < r < a$.

Como el valor absoluto no puede bajar indefinidamente, repitiendo el proceso anterior llegará un momento en el que K tendrá una entrada $a > 0$ que dividirá al resto de entradas de K, y podemos llevar a hasta el lugar $(1,1)$. Ponemos entonces ceros en el resto de los lugares $(i,1)$ de la primera columna: Tomamos $q \in \mathbb{Z}$ tal que $k_{i1} = qa$ y hacemos la operación $F_i - qF_1$. Hecho esto, podemos cambiar todas las entradas de la primera fila, excepto la $(1,1)$, por ceros (¿por qué?).

Hemos llegado pues a una matriz de la forma

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

en la que a es positivo y divide a cada b_{ij}. A partir de ahora no haremos operaciones con la primera fila ni con la primera columna, por lo que ni a ni los ceros de esos lugares van a variar. De hecho, podemos eliminar esa fila y esa columna de la matriz y "apuntar" el valor de a (incluso olvidarlo, si $a = 1$). Además, las operaciones que podemos hacer no van a cambiar el hecho de que todas las entradas que se obtengan sean múltiplos de a (¿por qué?). Pues bien, procediendo con la submatriz (b_{ij}) como se acaba de describir, podremos llegar a una matriz del tipo

$$\begin{pmatrix} a & 0 & 0 & \cdots & 0 \\ 0 & b & 0 & \cdots & 0 \\ 0 & 0 & c_{33} & \cdots & c_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & c_{m3} & \cdots & c_{mn} \end{pmatrix}$$

en la que a divide a b y b divide a los c_{ij}. Continuando de este modo, y eliminando las filas de ceros que puedan aparecer, conseguiremos la matriz que buscamos. Por supuesto, el proceso se puede simplificar por procedimientos heurísticos.

Ejemplos 7.6.5 *Transformaciones en la matriz de generadores y relaciones.*

1. Sea A el grupo abeliano con generadores a, b, c, d, e, f y relaciones:

$$\begin{array}{rcrcrcrcrcrcl} 4a & + & 13b & & & & & + & 3e & + & f & = & 0 \\ 5a & - & 7b & + & 6c & & & + & & - & f & = & 0 \\ 3a & + & 3b & & & + & 3d & + & & & & = & 0 \\ 3a & + & 6b & & & & & + & 3e & & & = & 0 \\ a & + & 7b & & & & & & & + & f & = & 0 \end{array}$$

La matriz asociada a dicho grupo es

$$\begin{pmatrix} 4 & 13 & 0 & 0 & 3 & 1 \\ 5 & -7 & 6 & 0 & 0 & -1 \\ 3 & 3 & 0 & 3 & 0 & 0 \\ 3 & 6 & 0 & 0 & 3 & 0 \\ 1 & 7 & 0 & 0 & 0 & 1 \end{pmatrix}$$

En este ejemplo veremos que no es necesario seguir estrictamente los pasos descritos anteriormente. Por ejemplo, el papel que antes ha representado la entrada de arriba a la izquierda lo asumirá ahora la entrada de abajo a la derecha. Observamos que la primera fila es combinación lineal de las dos últimas. Luego, restando a la primera la suma de las dos últimas (lo que representaremos por $F_1 - F_4 - F_5$) obtenemos:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & -7 & 6 & 0 & 0 & -1 \\ 3 & 3 & 0 & 3 & 0 & 0 \\ 3 & 6 & 0 & 0 & 3 & 0 \\ 1 & 7 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Eliminando la primera fila, y haciendo sucesivamente $F_1 + F_4$ (con la nueva numeración), $C_1 - C_6$ y $C_2 - 7C_6$, obtenemos

$$\begin{pmatrix} 6 & 0 & 6 & 0 & 0 & 0 \\ 3 & 3 & 0 & 3 & 0 & 0 \\ 3 & 6 & 0 & 0 & 3 & 0 \\ 1 & 7 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 6 & 0 & 6 & 0 & 0 & 0 \\ 3 & 3 & 0 & 3 & 0 & 0 \\ 3 & 6 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Podemos eliminar la última fila y última columna, y haciendo entonces (con la nueva numeración) $C_1 - C_3 - C_4 - C_5$ y $C_2 - C_4 - 2C_5$, obtenemos por fin la matriz

$$\begin{pmatrix} 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix},$$

de la que se deduce que $A \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_6 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ es la descomposición invariante de A. A partir de ésta podemos obtener la descomposición indescomponible $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

2. Sea A un grupo abeliano con matriz de generadores y relaciones dada por

$$\begin{pmatrix} 0 & 12 & 24 & 0 \\ 4 & 10 & 12 & 6 \\ 4 & 8 & 0 & 4 \end{pmatrix}$$

Es claro que, por más que operemos, las entradas van a ser siempre pares. Por otra parte, no es difícil conseguir que una sea 2, por ejemplo, haciendo $F_2 - F_3$ (escriba el lector las matrices que se van obteniendo). De los dos "2" que aparecen, el más cómodo es de la última columna. Podemos poner ceros en el resto de esa columna haciendo $F_3 - 2F_2$, siguiendo el método descrito, pero es más fácil hacer $C_4 - C_1$. Ahora podemos poner ceros en la segunda fila, haciendo $C_2 - C_4$ y $C_3 - 6C_4$. Pasando entonces la primera fila al último lugar, y pasando después la última columna al primer lugar, habremos puesto el 2 en la entrada $(1,1)$. Haciendo entonces, sucesivamente, $C_3 - 2C_2$ y $C_4 - 2C_3$, se obtiene por fin

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix},$$

por lo que $A \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}$.

7.7 Problemas

1. Sea $f : A \to B$ un isomorfismo entre dos grupos abelianos. Demostrar (hasta aburrirse) que:
   (a) La familia $\{A_i\}_{i\in I}$ de subgrupos de A es independiente si y sólo si la familia $\{f(A_i)\}_{i\in I}$ de subgrupos de B es independiente.
   (b) Un subgrupo C de A es un sumando directo de A si y sólo si el subgrupo $f(C)$ es un sumando directo de B.
   (c) A es indescomponible si y sólo si B es indescomponible.
   (d) La familia $\{a_i\}_{i\in I}$ de elementos de A es linealmente independiente si y sólo si la familia $\{f(a_i)\}_{i\in I}$ de elementos de B es linealmente independiente.
   (e) A es libre si y sólo si B es libre.
   (f) Si T es el subgrupo de torsión de A entonces $f(T)$ es el subgrupo de torsión de B.
   (g) A es de torsión si y sólo si B es de torsión.
   (h) A es libre de torsión si y sólo si B es libre de torsión.
2. Sea A un grupo abeliano libre de rango n. Decidir sobre la verdad o falsedad de las siguientes afirmaciones:
   (a) Todo subconjunto linealmente independiente de A tiene a lo sumo n elementos.
   (b) Todo subconjunto generador de A tiene al menos n elementos.
   (c) Todo subconjunto linealmente independiente de A con n elementos es una base de A.
   (d) Todo subconjunto generador de A con n elementos es una base de A.
3. Sean L, M, N grupos abelianos finitamente generados con $L \oplus N \cong M \oplus N$. Demostrar que $L \cong M$.
4. Determinar el subgrupo de torsión de los siguientes grupos aditivos: $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Z} \oplus \mathbb{Z}_n$, $\mathbb{Q}/\mathbb{Z}$, $\mathbb{R}/\mathbb{Z}$.
5. Determinar el subgrupo de torsión del grupo de las unidades de los anillos $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[i]$ y $\mathbb{Z}[\sqrt{2}]$.
6. Sea P un polinomio mónico de $\mathbb{Z}[X]$ de grado n. Demostrar que el grupo aditivo de $\mathbb{Z}[X]/(P)$ es libre de rango n. ¿Puede fallar el resultado si P no es mónico?
7. Probar que si A es un grupo abeliano libre y $n \in \mathbb{N}$, entonces A tiene un subgrupo de índice n.
8. Encontrar un subgrupo B de $A = \mathbb{Z}_{16}^*$ tal que $A/B \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
9. Sea A el subconjunto de $\mathbb{Z} \times \mathbb{Z}$ formado por las parejas de números enteros (a, b) tales que $a \equiv b \bmod 10$. Demostrar que A es un subgrupo de $\mathbb{Z} \times \mathbb{Z}$ y determinar una base de A.
10. Para un grupo abeliano arbitrario A, demostrar que la familia $\{t_p(A)\}$, donde p recorre el conjunto de todos los enteros primos positivos, es independiente, y que su suma directa es $t(A)$.
11. Demostrar que $t_p(\mathbb{Q}/\mathbb{Z})$ es el subgrupo $\mathbb{Z}_{p^\infty}$ del Ejemplo 7.5.17, y que $\mathbb{Q}/\mathbb{Z} = \oplus_p \mathbb{Z}_{p^\infty}$, donde p recorre el conjunto de todos los enteros primos positivos.
12. Demostrar que el grupo aditivo $(A, +)$ de un anillo A es de torsión precisamente si la característica de A es diferente de 0. Si A es un dominio, demostrar que las condiciones son equivalentes a que $(A, +)$ no sea libre de torsión. El anillo $\mathbb{Z}[X]/(2X)$ muestra que, en la segunda parte, la hipótesis de que A sea un dominio no es superflua, ¿por qué?
13. Encontrar bases para los siguientes subgrupos de grupos abelianos libres:
   (a) $\langle 3a, 4b, 6a + 2b\rangle$, siendo a, b generadores de un grupo abeliano libre de rango 2.
   (b) $\langle x + 2y + 4z, 3x + 6y + 12z, -12x - 24y - 48z, -2x + y + 7z\rangle$, siendo x, y, z generadores de un grupo libre de rango 3.

14. Demostrar que el grupo aditivo de los números racionales es indescomponible.

15. Calcular las descomposiciones primaria e invariante de los siguientes grupos abelianos:

    (a) $\mathbb{Z}_{20} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{108}$

    (b) $\mathbb{Z}_{21}^*$.

    (c) $\langle a, b \mid 3a + 6b = 9a + 24b = 0 \rangle$.

    (d) $\langle a, b, c \mid 2a + b = 3a + c = 0 \rangle$.

    (e) $\langle a, b, c \mid -4a + 2b + 6c = -6a + 2b + 6c = 7a + 4b + 15c = 0 \rangle$.

    (f) $\langle a, b, c \mid a + 2b + 4c = 3a + 6b + 12c = -2a + b + 7c = 0 \rangle$.

16. Clasificar el grupo abeliano presentado por los generadores y relaciones dados:

    (a) Generadores a, b, c y relaciones

$$\begin{array}{rcrcrcr} 7a & + & 8b & + & 9c & = & 0 \\ 4a & + & 5b & + & 6c & = & 0 \\ a & + & 2b & + & 3c & = & 0 \end{array}$$

    (b) Generadores a, b, c, d, e y relaciones

$$\begin{array}{rcrcrcrcrcr} a & - & 7b & - & 21c & + & 14d & & & = & 0 \\ 5a & - & 7b & - & 2c & + & 10d & - & 15e & = & 0 \\ 3a & - & 3b & - & 2c & + & 6d & - & 9e & = & 0 \\ a & - & b & & & + & 2d & - & 3e & = & 0 \end{array}$$

17. Encontrar todos los grupos abelianos, salvo isomorfismos, de órdenes 30, 60, 72, 90, 180, 360, 720 y 1830, calculando para cada uno de ellos las descomposiciones primaria e invariante.

18. Determinar salvo isomorfismos todos los grupos abelianos de orden ≤ 30 y dar la lista de sus divisores elementales y factores invariantes.

19. Demostrar que la lista de factores invariantes de $\mathbb{Z}_n \oplus \mathbb{Z}_m$ es (nm) ó $(\text{mcm}(n, m), \text{mcd}(n, m))$.

20. Demostrar que si A es un p-grupo abeliano que es la suma directa de n grupos cíclicos no nulos, entonces la ecuación $px = 0$ tiene exactamente p^n soluciones.

21. Sea G un p-grupo abeliano finito en el que la ecuación $px = 0$ tiene a lo sumo p soluciones. Demostrar que G es cíclico. Demostrar que también es cíclico un grupo abeliano finito (no necesariamente un p-grupo) en el que la ecuación $px = 0$ tenga a lo sumo p soluciones para todo primo p.

22. Resolver el Problema 57 del Capítulo 5 usando los resultados de este capítulo.

23. Del Ejercicio 7.5.15 se deduce que, si G es un grupo abeliano finito y p es un divisor primo de $|G|$, entonces G contiene un elemento de orden p. Demostrar que este resultado sigue siendo válido si G no es abeliano. Éste es el Teorema de Cauchy que demostraremos en el capítulo siguiente con otros métodos. (Indicación: Usar el Ejercicio 7.5.15, la Ecuación de Clases e inducción en $|G|$.)

24. Sea p primo. Demostrar que si G es un grupo abeliano finito en el que todo elemento no nulo tiene orden p, entonces $G \cong \mathbb{Z}_p^n$ para algún n.

25. Demostrar que todo grupo abeliano finito no cíclico contiene un subgrupo isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$ para algún primo p.

26. Sea B un subgrupo de un grupo abeliano finito A. Demostrar que A contiene un subgrupo isomorfo a A/B. ¿Es cierto el resultado si A es infinito?

27. Sea A un grupo abeliano finito y sea a un elemento de A orden máximo. Demostrar que $\langle a \rangle$ es un sumando directo de A.

28. Se pide:

    (a) Encontrar un número natural n tal que existan exactamente 5 grupos abelianos de orden n salvo isomorfismos.

    (b) [*] Encontrar todos los números naturales n tales que, salvo isomorfismos, existen exactamente 6 grupos abelianos de orden n.

    (c) [*] Demostrar que para ningún número natural n hay exactamente 13 grupos abelianos de orden n salvo isomorfismos.

29. [*] Un subgrupo propio H de un grupo G que no está contenido en ningún otro subgrupo propio de G se dice que es *maximal* (en G). Para un grupo abeliano finito A, demostrar:

    (a) Los subgrupos maximales son precisamente los de índice primo.

    (b) A tiene exactamente 2 subgrupos maximales si y sólo si A es cíclico y $|A|$ tiene exactamente dos divisores primos.

30. Sea G el grupo abeliano definido por los generadores $g_1, \ldots, g_n$ y las relaciones $\sum_{j=1}^{n} a_{ij} g_i = 0$ $(i = 1, \ldots, n)$, con $a_{ij} \in \mathbb{Z}$. Demostrar que G es finito precisamente si el determinante de la matriz (a_{ij}) es diferente de 0 y que, en tal caso, el orden de G coincide con el valor absoluto de dicho determinante.

Bibliografía del capítulo

Artin [4], Delgado-Fuertes-Xambó [11], Dorronsoro-Hernández [13], Herstein [20], Jacobson [23], Rotman [30].

Capítulo 8

Estructura de los grupos finitos

Se estudian los grupos finitos usando las acciones de grupos en conjuntos como principal herramienta. Se demuestran los Teoremas de Sylow y, como consecuencia de estos resultados y otras técnicas auxiliares, se clasifican todos los grupos con 15 o menos elementos.

Introducción

La noción de acción de un grupo en un conjunto, cuya definición abre este capítulo, es una de las más importantes en Teoría de Grupos. De hecho, históricamente, las acciones fueron usadas antes incluso de la formalización del concepto de grupo. No es exagerado afirmar que, en gran medida, los grupos son importantes en Matemáticas porque actúan, de formas muy variadas y casi siempre muy naturales, sobre otros conjuntos. Los conceptos de órbita y estabilizador de un elemento surgen también de modo natural y se relacionan de modo que, en el caso de grupos finitos, son muy útiles para hacer argumentos de recuento.

En la parte central del capítulo usamos técnicas basadas en acciones para demostrar los Teoremas de Cauchy y Sylow, que constituyen recíprocos parciales del Teorema de Lagrange. Éste afirma que el orden de cualquier subgrupo de un grupo finito G debe dividir a $|G|$, pero sabemos que pueden existir divisores d de $|G|$ tales que G no posea ningún subgrupo de orden d. Podemos preguntarnos si podrá imponerse una condición extra sobre el divisor d de $|G|$ que garantice la existencia de subgrupos de orden d en G. Un primer paso en esta dirección lo proporciona el Teorema de Cauchy, que responde afirmativamente a la pregunta cuando $d = p$ es primo. Esto permite deducir diversas propiedades de los p-grupos (grupos cuyo orden es una potencia del primo p), en particular el hecho de que verifican el "recíproco del Teorema de Lagrange". El Primer Teorema de Sylow va más allá, y responde afirmativamente a la pregunta cuando $d = p^n$ es cualquier potencia de primo que divide a $|G|$. Los otros dos Teoremas de Sylow tratan sobre los subgrupos de orden p^n en los que el exponente n es lo mayor posible, llamados p-subgrupos de Sylow de G. El segundo afirma que todos ellos son conjugados entre sí; en particular, si G posee un único p-subgrupo de Sylow (para cierto primo p), éste es normal. El tercero nos da información, muy útil en la práctica, sobre el número de p-subgrupos de Sylow de G, y de él se deduce un criterio de no simplicidad que nos permite demostrar que ningún grupo simple no abeliano tiene menos de 60 elementos (recuérdese que el grupo alternado A_5 es simple y tiene 60 elementos).

El final del capítulo lo dedicamos a obtener resultados sobre la estructura de los grupos de orden bajo, para lo que necesitaremos usar información obtenida a lo largo de todos los capítulos sobre grupos y dos últimos recursos técnicos: Uno de ellos es la descripción de ciertas situaciones en las que un grupo es isomorfo a un producto directo de dos de sus subgrupos, y otro es el concepto de producto semidirecto de grupos. Con estos recursos, clasificamos salvo isomorfismos todos los grupos de orden menor o igual que 15. Estos resultados muestran que, en general, la clasificación de los grupos finitos es muy laboriosa y requiere de toda la teoría de la que se pueda disponer. Clasificar grupos es un tema todavía abierto a la investigación y está muy lejos de resolverse.

Objetivos del capítulo

- Conocer el concepto de acción de un grupo sobre un conjunto, así como los de órbita y estabilizador y sus propiedades básicas.
- Conocer las acciones por traslaciones, por conjugación y por conjugación en subgrupos, y sus consecuencias teóricas.
- Conocer el Teorema de Cauchy y sus aplicaciones a p-grupos.
- Conocer los Teoremas de Sylow, y saber emplearlos para analizar la estructura de ciertos grupos en función de su orden.
- Conocer algunos criterios de no simplicidad para grupos.
- Conocer el concepto de producto semidirecto de grupos.
- Conocer algunas técnicas de clasificación de grupos de orden bajo.

Desarrollo de los contenidos

8.1 Acción de un grupo sobre un conjunto

Definición 8.1.1 *Sean G un grupo y Ω un conjunto. Una* acción por la izquierda *de G en Ω (o sobre Ω) es una aplicación $G \times \Omega \to \Omega$ tal que, si denotamos la imagen del par (g, α) por $g\alpha$, se verifica:*

1. *$1\alpha = \alpha$ para cada $\alpha \in \Omega$.*
2. *$h(g\alpha) = (hg)\alpha$ para cualesquiera $h, g \in G$ y $\alpha \in \Omega$.*

La segunda condición es una "asociatividad formal" que permite escribir $hg\alpha$ sin ambigüedad. Observando en qué conjuntos están los elementos que se operan, no debe haber confusión sobre si se está usando el producto de G o la acción.

Ocasionalmente, en lugar de $g\alpha$ se emplean otras notaciones como ${}^{g}\alpha$ para designar a la imagen de (g, α) por la acción que se considere. Las condiciones de la Definición 8.1.1 son entonces:

$$ {}^{1}\alpha = \alpha \qquad \text{y} \qquad {}^{g}({}^{h}\alpha) = {}^{gh}\alpha. $$

Dada una acción $G \times \Omega \to \Omega$ de un grupo G sobre un conjunto Ω, cada $g \in G$ determina una aplicación $\phi_g : \Omega \to \Omega$ dada por $\phi_g(\alpha) = g\alpha$. Combinando las dos propiedades de la definición se observa que la aplicación $\phi_{g^{-1}}$ es la inversa de ϕ_g, por lo que ésta es una permutación de Ω. Además, si g y h son elementos de G, es claro que $\phi_h \circ \phi_g = \phi_{hg}$. Con esto hemos probado:

Proposición 8.1.2 *Dada una acción $G \times \Omega \to \Omega$ de un grupo G sobre un conjunto Ω, la aplicación $\phi : G \to S(\Omega)$ dada por $\phi(g) = \phi_g$ es un homomorfismo de grupos.*

Llamaremos *núcleo de la acción* al núcleo de este homomorfismo ϕ, y diremos que la acción es *fiel* si ϕ es inyectivo.

La proposición anterior admite una recíproca de demostración elemental:

Proposición 8.1.3 *Dados un conjunto Ω, un grupo G y un homomorfismo de grupos $\phi : G \to S(\Omega)$, la aplicación $G \times \Omega \to \Omega$ dada por $(g, \alpha) \mapsto \phi(g)(\alpha)$ es una acción por la izquierda de G sobre Ω.*

De las dos proposiciones anteriores resulta que las acciones de un grupo G sobre un conjunto Ω y los homomorfismos $G \to S(\Omega)$ se determinan mutua y biyectivamente, por lo que pueden ser considerados como conceptos equivalentes.

Todo lo expuesto hasta aquí puede traducirse sin dificultad para las acciones "por la derecha". Una *acción por la derecha* de un grupo G sobre un conjunto Ω es una aplicación $\Omega \times G \to \Omega$, en la que la imagen del par (α, g) se escribe αg, que verifica

$$ \alpha 1 = \alpha \qquad \text{y} \qquad (\alpha g)h = \alpha gh $$

para cualesquiera $\alpha \in \Omega$ y $g, h \in G$. A menudo, la imagen del par (α, g) se denota por α^g, y entonces las condiciones anteriores se traducen en

$$\alpha^1 = \alpha \qquad \text{y} \qquad (\alpha^g)^h = \alpha^{gh}.$$

Como antes, se demuestra que dar una acción por la derecha de G sobre Ω es equivalente a dar un *antihomomorfismo* de G en $S(\Omega)$; es decir, una aplicación $\phi : G \to S(\Omega)$ que verifica $\phi(gh) = \phi(h)\phi(g)$ cuando $g, h \in G$. Definiendo el núcleo de un antihomomorfismo del modo obvio, podemos definir el núcleo de una acción por la derecha y el concepto de acción por la derecha fiel.

En realidad, la diferencia entre acciones por la izquierda y por la derecha es meramente formal. En efecto, si $\theta : G \to G$ es la aplicación dada por $g \mapsto g^{-1}$, entonces la asignación $\phi \mapsto \phi \circ \theta$ define una biyección entre el conjunto de los homomorfismos de G en $S(\Omega)$ y el conjunto de los antihomomorfismos de G en $S(\Omega)$ (la biyección inversa también se obtiene componiendo con θ). Por lo dicho anteriormente, esta biyección se traduce en una biyección entre las acciones por la izquierda de G sobre Ω y las correspondientes acciones por la derecha. Explícitamente, esta biyección lleva una acción por la izquierda dada por $(g, \alpha) \mapsto g\alpha$ a la acción por la derecha dada por $(\alpha, g) \mapsto \alpha g^{-1}$.

Cada resultado o ejemplo, por su naturaleza (o en muchos casos para respetar costumbres notacionales), sugiere el uso de acciones por uno u otro lado. Por tanto, es conveniente usar ambos conceptos, y eso haremos en lo que sigue.

Ejemplos 8.1.4 *Acciones.*

1. Para un número natural n, la aplicación $S_n \times \mathbb{N}_n \to \mathbb{N}_n$ dada por $\sigma i = \sigma(i)$ es una acción por la izquierda del grupo simétrico S_n en el conjunto $\mathbb{N}_n$, y el homomorfismo asociado $S_n \to S(\mathbb{N}_n)$ es la identidad.

   Más generalmente, si Ω es un conjunto arbitrario y G es un subgrupo del grupo simétrico $S(\Omega)$, entonces la aplicación $(\sigma, x) \mapsto \sigma(x)$ es una acción por la izquierda fiel de G sobre Ω.

2. Sea G un grupo y sea $\Omega = G$. La aplicación $(g, x) \mapsto gx$ es una acción de G sobre sí mismo. Se denomina *acción de G sobre sí mismo por traslaciones por la izquierda*, y es claramente fiel. ¿Qué relación guarda este ejemplo con el Teorema de Cayley 5.7.4?

   Análogamente, la aplicación dada por $(x, g) \mapsto xg$ es una acción fiel por la derecha de G sobre sí mismo *por traslaciones por la derecha.*

3. Sean G un grupo, H un subgrupo de G y Ω el conjunto G/H de las clases laterales por la izquierda módulo H. La aplicación $(g, xH) \mapsto gxH$ es una acción por la izquierda de G sobre Ω, que también se llama *acción por traslaciones por la izquierda* de G en G/H. Cuando $H = 1$ tenemos la acción del apartado anterior.

   El lector podrá describir una *acción por traslaciones por la derecha* de G sobre el conjunto $H\backslash G$ de las clases laterales por la derecha de G módulo H.

4. Dado un grupo G, la aplicación $(a, x) \mapsto a^x = x^{-1}ax$ es una acción por la derecha de G sobre sí mismo. Más generalmente, si H y N son subgrupos de G y N es normal en G, la conjugación induce una acción por la derecha de H sobre N que se denomina *acción de H sobre N por conjugación.* ¿Cuándo es fiel esta acción?

   La acción por la izquierda de H sobre N asociada a la anterior viene dada por $(x, a) \mapsto {}^x a = xax^{-1}$ (conjugación por x^{-1}). En este caso, la imagen del homomorfismo $H \to S(N)$ está contenida en $\mathrm{Aut}(N)$.

8.2 Órbitas y estabilizadores

Definición 8.2.1 *Sea G un grupo que actúa por la izquierda sobre un conjunto Ω, y sean $\alpha, \beta \in \Omega$.*

Se dice que α y β son equivalentes para la acción *cuando existe $g \in G$ tal que $g\alpha = \beta$. Se propone como ejercicio la comprobación de que la anterior es una relación de equivalencia en Ω. Las correspondientes clases de equivalencia reciben el nombre de* órbitas. *Así, la órbita de α es el conjunto*

$$G\alpha = \{g\alpha : g \in G\}.$$

El estabilizador *de α en G es el conjunto*

$$\mathrm{Estab}_G(\alpha) = E(\alpha) = \{g \in G : g\alpha = \alpha\}$$

(escribiremos $E(\alpha)$ cuando no haya riesgo de confusión en cuanto a la acción considerada).

Es claro que la órbita de α es unitaria; es decir, $G\alpha = \{\alpha\}$, precisamente si $\mathrm{Estab}_G(\alpha) = G$*, pues ambas condiciones equivalen a que se tenga $g\alpha = \alpha$ para cada $g \in G$. Cuando esto ocurre decimos que α es un* punto fijo *para la acción.*

Cuando todos los elementos están en la misma órbita se dice que la acción es transitiva*, o que G* actúa transitivamente *en Ω.*

Si usamos la notación ${}^g\alpha$, o si trabajamos con acciones por la derecha, haremos los cambios pertinentes en la notación. Por ejemplo, las órbitas se denotarán por ${}^G\alpha$, αG ó α^G.

Ejercicio 8.2.2 *Dada una acción de G sobre Ω, demostrar que el estabilizador de cada elemento de Ω es un subgrupo de G, y que la intersección de todos los estabilizadores es el núcleo de la acción.*

Ejemplos 8.2.3 *Órbitas y estabilizadores.*

1. Sea G el subgrupo cíclico de S_6 generado por la permutación $\sigma = (1\ 2\ 3)(4\ 5)$, y consideremos la acción $G \times \mathbb{N}_6 \to \mathbb{N}_6$ definida en los Ejemplos 8.1.4. Entonces las órbitas son $\{1,2,3\}$, $\{4,5\}$ y $\{6\}$, el único punto fijo de $\mathbb{N}_6$ es el 6, y los estabilizadores son

$$E(1) = E(2) = E(3) = \{1, \sigma^3\}, \quad E(4) = E(5) = \{1, \sigma^2, \sigma^4\}, \quad E(6) = G.$$

2. La acción natural del subgrupo $G = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ de S_4 sobre $\mathbb{N}_4$ es transitiva, y cada elemento de $\mathbb{N}_4$ tiene estabilizador trivial.

3. La acción de un grupo G sobre sí mismo por traslaciones por la izquierda (o por la derecha) es transitiva, pues cada ecuación $aX = b$ tiene solución única en G. También lo es la acción de G en G/H por traslaciones por la izquierda.

Como las órbitas son clases de equivalencia, forman una partición de Ω. Cuando éste es finito se tiene

$$|\Omega| = \sum_{\alpha \in \Omega'} |G\alpha|, \tag{8.2.1}$$

donde Ω' es un conjunto de representantes de las órbitas (es decir, en Ω' hay exactamente un elemento de cada órbita). Esta igualdad se conoce con el nombre de *Ecuación de Órbitas*.

Ejercicio 8.2.4 *Se considera la acción (por la derecha) de un grupo G sobre sí mismo por conjugación:*

1. *Comprobar que las órbitas son las clases de conjugación, que el estabilizador de un elemento g es su centralizador $\mathrm{Cen}_G(g)$, que los puntos fijos de la acción son los elementos de $Z(G)$, que la acción es fiel precisamente si $Z(G) = \{1\}$, y que la acción es transitiva precisamente si $G = \{1\}$.*

2. *Interpretar la Ecuación de Clases (Proposición 5.9.5) como un caso particular de la Ecuación de Órbitas (8.2.1).*

Proposición 8.2.5 *Sea G un grupo que actúa por la izquierda sobre un conjunto Ω y sea $\alpha \in \Omega$. Entonces:*

1. *$[G : E(\alpha)] = |G\alpha|$.*

2. *Si la acción es transitiva entonces $E(\alpha)$ es el grupo trivial para cualquier $\alpha \in \Omega$.*

3. *Si G es finito se tiene $|G| = |G\alpha| \cdot |E(\alpha)|$; por tanto, el cardinal de cualquier órbita divide a $|G|$.*

4. *$E(g\alpha) = g \cdot E(\alpha) \cdot g^{-1}$ (para cada $g \in G$).*

Demostración. Para ver 1, notemos que dados $g, h \in G$ se tiene

$$g\alpha = h\alpha \Leftrightarrow h^{-1}g\alpha = \alpha \Leftrightarrow h^{-1}g \in E(\alpha) \Leftrightarrow gE(\alpha) = hE(\alpha).$$

En consecuencia, la aplicación $E(\alpha)\backslash G \to G\alpha$ dada por $gE(\alpha) \mapsto g\alpha$ está bien definida y es inyectiva. Como es obviamente suprayectiva, tenemos una biyección que nos da la igualdad entre cardinales buscada. Los apartados 2 y 3 se siguen del 1 y del Teorema de Lagrange. El 4 se tiene por las equivalencias

$$h \in E(g\alpha) \Leftrightarrow hg\alpha = g\alpha \Leftrightarrow g^{-1}hg\alpha = \alpha \Leftrightarrow g^{-1}hg \in E(\alpha) \Leftrightarrow h \in gE(\alpha)g^{-1}.$$

□

En el siguiente ejercicio, dado un subgrupo H de un grupo finito G, describimos el mayor subgrupo de H que es normal en G y damos una condición bajo la cual el propio H es normal en G (esta condición generaliza el hecho de que todo subgrupo de índice 2 es normal).

Ejercicio 8.2.6 *Sea G un grupo con un subgrupo H, y consideremos la acción por traslaciones por la derecha de G en $H\backslash G$ descrita en los Ejemplos 8.1.4. Demostrar que:*

1. *La acción es transitiva.*
2. $\mathrm{Estab}_G(H) = H$, *por lo que* $\mathrm{Estab}_G(Hg) = H^g$ *para cada* $g \in G$.
3. *El núcleo de la acción, que denotaremos por $c(H)$ (se suele llamar el* corazón *de H), es la intersección de todos los conjugados de H en G; es decir,*

$$c(H) = \bigcap_{g \in G} H^g.$$

4. *$c(H)$ es el mayor subgrupo normal de G contenido en H.*
5. *Si H tiene índice finito n en G, existe un homomorfismo inyectivo de grupos $\frac{G}{c(H)} \to S_n$.*
6. *Si G es finito y $[G : H] = p$, donde p es el menor divisor primo de $|G|$ (esto significa que H tiene el mayor orden posible entre los subgrupos propios de G), entonces H es normal en G. (Indicación: usar el apartado anterior para probar que $[H : c(H)]$ divide a $(p-1)!$).*
7. *Si $|G| = m$, $[G : H] = n > 1$ y $m \nmid n!$ entonces $c(H) \neq \{1\}$ y por tanto G no es simple.*

A continuación damos un nuevo ejemplo de acción del que se extraen consecuencias teóricas interesantes:

Ejemplo 8.2.7 *Acción por conjugación en subgrupos; normalizadores.*
Sea G un grupo y sea Ω el conjunto de todos los subgrupos de G. La asignación $(H, g) \mapsto H^g = g^{-1}Hg$ define una acción por la derecha de G en Ω llamada *acción por conjugación en subgrupos*. La órbita del subgrupo H está formada por los subgrupos conjugados de H, y es claro que los subgrupos normales de G son precisamente los puntos fijos para esta acción; es decir, los que tienen estabilizador G. Este hecho se generaliza en el ejercicio que sigue.

Ejercicio 8.2.8 *Sea H un subgrupo de un grupo G, y consideremos el conjunto*

$$N_G(H) = \{g \in G : H = H^g\},$$

que recibe el nombre de normalizador *de H en G. Demostrar que:*

1. *$N_G(H)$ es el estabilizador de H para la acción de Ejemplo 8.2.7.*
2. *$N_G(H)$ es el mayor subgrupo de G en el que H es normal. Es decir, H es un subgrupo normal de $N_G(H)$ y, si K es un subgrupo de G tal que H es un subgrupo normal de K, entonces $K \subseteq N_G(H)$.*
3. *Si $N_G(H)$ tiene índice finito en G, entonces $[G : N_G(H)]$ coincide con el número de subgrupos conjugados de H en G.*

8.3 Teorema de Cauchy y p-grupos

Sea p un entero primo positivo. Los grupos cuyo orden es una potencia de p han tenido un papel destacado en la descripción de los grupos abelianos finitos (Sección 7.4), y también aparecieron en la Sección 5.9. En el caso abeliano, vimos que un grupo G tiene orden potencia de p si y sólo si lo mismo le ocurre a todos sus elementos, lo que dio lugar a la definición de los p-grupos.

Por otra parte, hemos visto que no se verifica el "recíproco del Teorema de Lagrange": Si G es un grupo finito y m es un divisor de $|G|$, en general no es cierto que G tenga un subgrupo de orden m (por ejemplo, no lo es si $G = A_4$ y $m = 6$). Sin embargo, este resultado es cierto cuando m es una potencia de primo, como veremos en la sección siguiente. En esta sección damos un primer paso en la demostración de ese resultado. Es el Teorema de Cauchy, que se ocupa del caso en que m es primo y nos permite extender la definición de los p-grupos al caso no abeliano. En el Problema 23 del Capítulo 7 propusimos una demostración alternativa de este teorema.

Teorema 8.3.1 (Cauchy) *Sea G un grupo finito. Si p es un divisor primo de $|G|$, entonces G posee un elemento de orden p.*

Demostración. Sea Ω el conjunto de las p-tuplas de elementos de G cuyo producto es 1:

$$\Omega = \{(x_1, \ldots, x_p) : x_i \in G \text{ para cada } i \text{ y } x_1 \cdots x_p = 1\}.$$

Es claro que una p-tupla $(x_1, \ldots, x_p)$ de elementos de G está en Ω si y sólo si $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$. Por tanto, para dar un elemento de Ω podemos elegir sus $p-1$ primeras componentes arbitrariamente en G, y la última queda entonces determinada por éstas. En consecuencia se tiene $|\Omega| = |G|^{p-1}$, y en particular p divide a $|\Omega|$.

Sea $C = \langle c \rangle$ un grupo cíclico de orden p, y consideremos su acción por la izquierda en Ω dada por

$$(c, (x_1, \ldots, x_p)) \mapsto (x_p, x_1, x_2 \ldots, x_{p-1}).$$

Los puntos fijos para esta acción son los elementos de Ω de la forma $(x, x, \ldots, x)$, que se corresponden con los elementos de G tales que $x^p = 1$. Por tanto, el resultado quedará demostrado si vemos que Ω contiene algún punto fijo distinto del $(1, 1, \ldots, 1)$.

Sea pues $k \geq 1$ el número de órbitas unitarias (o de puntos fijos) para la acción dada, y sea q el número de órbitas no unitarias. Por la Proposición 8.2.5, cada órbita no unitaria tiene cardinal p, y así $|\Omega| = k + pq$. Como p divide a $|\Omega|$ deducimos que p divide a k, y como $k \neq 0$ deducimos que hay puntos fijos diferentes del $(1, 1, \ldots, 1)$, como queríamos ver. □

Como consecuencia de los Teoremas de Lagrange y Cauchy se tiene:

Ejercicio 8.3.2 *Dados un grupo finito G y un entero positivo primo p, demostrar la equivalencia de las siguientes condiciones:*

1. *El orden de G es una potencia de p.*
2. *El orden de cada elemento de G es una potencia de p.*

Definición 8.3.3 *Un grupo finito que verifique las condiciones equivalentes del Ejercicio 8.3.2 se llama un* p-grupo.

Otra consecuencia notable del Teorema de Cauchy es la siguiente:

Proposición 8.3.4 *Los p-grupos verifican el recíproco del Teorema de Lagrange. Es decir, un p-grupo G posee un subgrupo de orden d para cada divisor d de $|G|$.*

Demostración. Sea $|G| = p^n$ con $n \geq 1$, y procedamos por inducción en n, con el caso $n = 1$ trivial. En el caso general, el divisor d ha de ser de la forma p^m con $m \leq n$. Por la Proposición 5.9.7, el centro $Z = Z(G)$ no es trivial, y por tanto contiene un elemento g de orden p. El subgrupo $N = \langle g \rangle$ es normal en G (¿por qué?), y el cociente G/N tiene orden p^{n-1}. Por tanto p^{m-1} divide a $|G/N|$, y la hipótesis de inducción nos dice que G/N posee un subgrupo X de orden p^{m-1}. Por el Teorema de la Correspondencia, existe un subgrupo H de G que contiene a N y tal que $X = H/N$, y entonces se tiene $|H| = |X| \cdot |N| = p^{m-1}p = p^m$, luego H es el subgrupo que buscábamos. □

8.4 Los Teoremas de Sylow

Acabamos de ver que los p-grupos verifican el recíproco del Teorema de Lagrange. En este sentido, el Primer Teorema de Sylow constituirá un "recíproco parcial" del Teorema de Lagrange: afirmará que, dado un grupo finito $|G|$, para cada divisor d de $|G|$ que sea potencia de un primo, existe un subgrupo de G de orden d. Obsérvese que estos subgrupos son precisamente los subgrupos de G que son p-grupos para algún primo p (les llamaremos p-subgrupos de G). El resto de los Teoremas de Sylow profundizarán más en el estudio de los subgrupos de este tipo.

Particularmente importantes serán los p-subgrupos de G que tengan el mayor orden posible, y esto nos llevará a menudo a la siguiente situación: Si p es un divisor primo de $|G|$, podemos poner

$$|G| = p^n r \quad \text{con} \quad n \geq 1 \quad \text{y} \quad p \not| r;$$

es decir, p^n es la mayor potencia de p que divide a $|G|$, y entonces p^n es el mayor orden que puede tener un p-subgrupo de G.

Definición 8.4.1 *Sea G un grupo finito y sea p un entero primo positivo. Un subgrupo de G que sea un p-grupo se llama un* p-subgrupo *de G. Por el Teorema de Lagrange, G sólo puede poseer p-subgrupos no triviales si p divide a $|G|$.*

Si $|G| = p^n r$ con $p \not| r$, un subgrupo de G de orden p^n (es decir, un p-subgrupo del mayor orden posible) se llama un p-subgrupo de Sylow *de G.*

Para grupos abelianos finitos, los subgrupos de Sylow han aparecido con otro nombre:

Ejercicio 8.4.2 *Sea G un grupo abeliano finito y sea p un divisor primo de $|G|$. Demostrar que $t_p(G)$ es el único p-subgrupo de Sylow de G.*

El Primer Teorema de Sylow

Teorema 8.4.3 (Primer Teorema de Sylow) *Sea G un grupo finito y sea p un divisor primo de $|G|$. Entonces G contiene algún p-subgrupo de Sylow.*

Demostración. Sea $m = |G|$ y pongamos $m = p^n r$ con $p \not| r$. Se trata de demostrar que G tiene un subgrupo de orden p^n, y lo hacemos por inducción sobre m. Como p divide a m, el menor caso posible es $m = p$ y el resultado es entonces trivial. Así, supondremos que $m > p$ y que el enunciado del teorema es válido para cualquier grupo de orden menor que m. Distinguiremos dos casos:

Si existe $g \in G \setminus Z(G)$ tal que p no divide a $[G : \mathrm{Cen}_G(g)]$ entonces, por el Teorema de Lagrange y el Teorema Fundamental de la Aritmética, p^n divide a $|\mathrm{Cen}_G(g)|$. Como éste es un subgrupo propio de G, la hipótesis de inducción implica que $\mathrm{Cen}_G(g)$ posee un subgrupo de orden p^n, y por tanto G también.

En otro caso, se tiene que p divide a $[G : \mathrm{Cen}_G(g)]$ para cada $g \in G \setminus Z(G)$. Aplicando la Ecuación de Clases (Proposición 5.9.5) se deduce que p ha de dividir a $Z(G)$. Por el Teorema de Cauchy (8.3.1), $Z(G)$ contiene un subgrupo N de orden p, que será normal en G. Como $|G/N| = m/p < m$ y p^{n-1} es la mayor potencia de p que divide a $|G/N|$, la hipótesis de inducción nos dice que existe un subgrupo X de G/N tal que $|X| = p^{n-1}$. Por el Teorema de la Correspondencia (5.6.5) se tiene $X = H/N$ para algún subgrupo H de G que contiene a N. Entonces $|H| = |N| \cdot |X| = p^n$, y por tanto H es el subgrupo que buscábamos. □

Aplicando ahora la Proposición 8.3.4 a un subgrupo de Sylow de G se tiene:

Corolario 8.4.4 *Un grupo finito posee p-subgrupos de todos los órdenes posibles. Es decir, si G es un grupo finito y k es un entero tal que p^k divide a $|G|$, entonces G contiene algún subgrupo de orden p^k.*

Estos resultados nos dan información sobre la existencia de ciertos subgrupos de los grupos finitos. Por ejemplo, sea G un grupo del que sabemos que $|G| = 28.600 = 2^3 \cdot 5^2 \cdot 11 \cdot 13$. Entonces G tiene subgrupos de cualquiera de los órdenes 2, 4, 8, 5, 25, 11 ó 13.

¿Qué pasa con los subgrupos de otros órdenes? Los resultados anteriores no afirman nada sobre su existencia, y de hecho no es posible hacer ninguna afirmación general en ese sentido. Por ejemplo, si $|G| = 12$, lo anterior nos dice que G tiene subgrupos de órdenes 2, 3 y 4 (y por supuesto 1 y 12); en cuanto a los subgrupos de orden 6, existen para el grupo cíclico $G = \mathbb{Z}_{12}$ o para el grupo diédrico D_6, pero no existen para el grupo alternado $G = A_4$ (Ejemplo 6.2.8).

El Segundo Teorema de Sylow

A lo largo de este párrafo suponemos que $|G| = p^n r$ con $p \not| r$. Por el Primer Teorema (8.4.3) podemos fijar un p-subgrupo de Sylow P de G; es decir, un subgrupo tal que $|P| = p^n$.

Denotaremos por S_P el conjunto de todos los subgrupos de G que son conjugados de P; es decir, todos los subgrupos de la forma $P^x = x^{-1}Px$, para algún $x \in G$. Como "conjugar por x" es un automorfismo de G, todos los subgrupos de S_P tienen el mismo cardinal que P y, en consecuencia, son p-subgrupos de Sylow de G. Una parte del Segundo Teorema de Sylow afirma que, recíprocamente, todo p-subgrupo de Sylow de G está en S_P (es decir, es conjugado de P). Para demostrar esto necesitamos un par de lemas previos.

Lema 8.4.5 *Con la notación anterior, $|S_P|$ es un divisor de r (es decir, $|S_P|$ es un divisor de $|G|$ que no es múltiplo de p).*

Demostración. Consideraremos la acción por la derecha por conjugación de G sobre el conjunto Ω de todos los subgrupos de G, y usaremos la notación y los resultados del Ejemplo 8.2.7 y del Ejercicio 8.2.8. Entonces S_P es la órbita de P, y $N = N_G(P)$ es un subgrupo de G que contiene a P y verifica $|S_P| = [G : N]$, de donde $|G| = |N| \cdot |S_P|$. De aquí se deduce inmediatamente que $|S_P|$ divide a $|G|$. Además, como $p^n = |P|$ divide a $|N|$ (pues $P \subseteq N$), p no puede dividir a $|S_P|$ pues de lo contrario p^{n+1} dividiría a $|G|$, lo cual es imposible por la elección de n. □

El lema que sigue contiene esencialmente la demostración del Segundo Teorema de Sylow, pero lo enunciamos separadamente porque sus apartados serán usados también en el Tercer Teorema.

Lema 8.4.6 *Sea H un p-subgrupo de G. Entonces:*

1. *La aplicación $S_P \times H \to S_P$ dada por $(Q, x) \mapsto Q^x$ es una acción por la derecha de H en S_P.*
2. *Esta acción tiene puntos fijos.*
3. *Un elemento Q de S_P es un punto fijo para la acción si y sólo si $H \subseteq Q$.*

Demostración. El apartado 1 es elemental y se deja como ejercicio.

2. Apliquemos la Ecuación de Órbitas (8.2.1) a esta acción: tenemos

$$|S_P| = \sum |Q^H| = \sum [H : \mathrm{Estab}_H(Q)],$$

donde Q recorre un conjunto de representantes de las órbitas. Por el Lema 8.4.5, p no divide a $|S_P|$ y en consecuencia p no divide a $[H : \mathrm{Estab}_H(Q)]$ para cierto $Q \in S_P$. Como H es un p-grupo, ese índice debe valer 1 y así $\mathrm{Estab}_H(Q) = H$; es decir, Q es un punto fijo.

3. Si $x \in Q$ entonces $Q^x = Q$, por lo que los elementos de S_P que contienen a H son puntos fijos para la acción. Recíprocamente, supongamos que Q es un punto fijo de S_P para esa acción. La hipótesis nos dice que $xQ = Qx$ para cada $x \in H$, por lo que $HQ = QH$ y así HQ es un subgrupo de G que contiene a Q y a H (Ejercicio 5.4.10). Además, como H y Q son p-grupos y se tiene $|HQ| = \dfrac{|H| \cdot |Q|}{|H \cap Q|}$ (Lema 5.4.11), deducimos que HQ es un p-subgrupo de G. Como Q es maximal entre los p-subgrupos de G, entonces $HQ = Q$ y por tanto $H \subseteq Q$. □

Podemos ya demostrar el Segundo Teorema de Sylow.

Teorema 8.4.7 (Segundo Teorema de Sylow) *Sean G un grupo finito, p un divisor primo de $|G|$, P un p-subgrupo de Sylow de G y H un p-subgrupo de G. Entonces H está contenido en algún subgrupo conjugado de P.*

En particular, todos los p-subgrupos de Sylow de G son conjugados entre sí.

Demostración. La acción del Lema 8.4.6 tiene al menos un punto fijo Q, y éste es un conjugado de P que contiene a H. Si, además, H es un p-subgrupo de Sylow de G, entonces la inclusión $H \subseteq Q$ es una igualdad (¿por qué?), y en consecuencia H es un conjugado de P. □

El siguiente corolario se usa a menudo para contar elementos de un grupo.

Corolario 8.4.8 *Sea G un grupo finito y sea p un divisor primo de $|G|$. La unión de todos los p-subgrupos de Sylow de G coincide con el conjunto de todos los elementos de G cuyo orden es una potencia de p.*

Demostración. Es claro que el orden de cualquier elemento de esa unión es una potencia de p (incluyendo al neutro, cuyo orden es p^0). Recíprocamente, si $o(x) = p^k$ entonces x está en el p-subgrupo $\langle x \rangle$, y por tanto está en algún p-subgrupo de Sylow por el Segundo Teorema. □

El Tercer Teorema de Sylow

Una consecuencia inmediata del Segundo Teorema de Sylow es el hecho de que S_P es el conjunto de *todos* los p-subgrupos de Sylow de G, y también el conjunto de los conjugados de *cualquier* p-subgrupo de Sylow de G (no sólo de un p-subgrupo de Sylow prefijado). En particular, si denotamos por n_p al número de p-subgrupos de Sylow de G, se tiene

$$n_p = |S_P|.$$

El Tercer Teorema de Sylow establece ciertas condiciones que debe cumplir el número n_p recién definido.

Teorema 8.4.9 (Tercer Teorema de Sylow) *Sea G un grupo finito, sea p un divisor primo de $|G|$ y sea $|G| = p^n r$ con $p \not| r$. Entonces el número n_p de p-subgrupos de Sylow de G verifica:*

1. *n_p divide a r.*
2. *$n_p \equiv 1 \bmod p$.*
3. *$n_p = 1$ si y sólo si algún p-subgrupo de Sylow de G es normal en G.*

Demostración. 1. Es consecuencia del Lema 8.4.5 y de la igualdad $n_p = |S_P|$.

2. Sea H un p-subgrupo de Sylow de G; la acción del Lema 8.4.6 tiene al menos un punto fijo, y de hecho no tiene más porque ahora, para un elemento Q de S_P, contener a H equivale a coincidir con H (por la igualdad de cardinales). Por tanto, en la Ecuación de Órbitas (8.2.1)

$$|S_P| = \sum |Q^H| = \sum [H : \mathrm{Estab}_H(Q)],$$

exactamente uno de los índices $[H : \mathrm{Estab}_H(Q)]$ vale 1, y cada uno de los otros es múltiplo de p por ser un divisor de $|H|$ distinto de 1. En consecuencia, $n_p \equiv 1 \bmod p$.

3. Puesto que S_P es el conjunto de todos los conjugados de cualquier p-subgrupo de Sylow de G, el resultado es una consecuencia directa del hecho de que un subgrupo es normal si y sólo si coincide con todos sus conjugados (Ejercicio 5.9.3). □

Criterios de no simplicidad

En este párrafo usaremos los Teoremas de Sylow para obtener un criterio que nos permite afirmar que ciertos grupos no son simples. Este resultado, junto con otros del mismo tipo que se han visto antes, nos permitirá demostrar que no hay grupos simples no abelianos con menos de 60 elementos.

Proposición 8.4.10 *Sea G un grupo finito con $|G| = pq$ ó $|G| = pq^2$, donde p, q son dos primos distintos. Entonces se tiene $n_p = 1$ ó $n_q = 1$, y en consecuencia G no es un grupo simple.*

Demostración. Usaremos en varias ocasiones el Tercer Teorema de Sylow (8.4.9). Si $|G| = pq$ podemos asumir que $p < q$, luego $p \not\equiv 1 \bmod q$ y en consecuencia $n_q \neq p$, por lo que $n_q = 1$. Suponemos pues que $|G| = pq^2$, y distinguimos tres casos:

Si $p < q$ entonces $p \not\equiv 1 \bmod q$, y por tanto $n_q = 1$.

Si $p > q^2 (> q)$ entonces $q, q^2 \not\equiv 1 \bmod p$ y en consecuencia $n_p \neq q, q^2$, por lo que $n_p = 1$.

Por último, si $q < p < q^2$ entonces $q \not\equiv 1 \bmod p$ y en consecuencia $n_p \neq q$. Por tanto o bien $n_p = 1$, y hemos terminado, o bien $n_p = q^2$, y basta ver que esta última opción implica que $n_q = 1$. Supongamos

pues que $n_p = q^2$. Entonces el número de elementos de orden p que hay en el grupo G es $q^2(p-1)$, pues cada subgrupo de orden p aporta $p-1$ elementos de orden p que no se repiten, ya que dos subgrupos distintos de orden p tienen intersección trivial. Por tanto, el número de elementos de G cuyo orden no es p es

$$pq^2 - q^2(p-1) = q^2.$$

Sea ahora K un q-subgrupo de Sylow de G; como $|K| = q^2$ y K no contiene elementos de orden p, K debe consistir en los q^2 elementos de orden distinto de p, lo que muestra que K es el único q-subgrupo de Sylow de G y así $n_q = 1$. □

Teorema 8.4.11

1. *El menor entero positivo n para el que existe un grupo simple no abeliano de orden n es $n = 60$.*
2. *Si G es un grupo simple y $|G| < 60$, entonces $G \cong \mathbb{Z}_p$ para cierto número primo p.*

Demostración. Por el Ejercicio 6.2.10, el apartado 2 será consecuencia del 1, por lo que nos limitamos a demostrar éste. Además, como A_5 es un grupo simple con 60 elementos, basta ver un grupo no abeliano con menos de 60 elementos no es simple.

Si p y q son primos distintos, ya sabemos que los grupos de orden p son abelianos y que los de órdenes p^n (con $n > 1$), pq y pq^2 no son simples (Proposiciones 5.9.7 y 8.4.10). Esto resuelve todos los casos excepto los de órdenes 24, 30, 36, 40, 42, 48 y 56.

Por el Tercer Teorema de Sylow 8.4.9, si si $|G| = 40$ entonces $n_5 = 1$, y si $|G| = 42$ entonces $n_7 = 1$, por lo que ningún grupo de esos órdenes puede ser simple.

Por el Primer Teorema de Sylow 8.4.3, todo grupo de orden 24 tiene un subgrupo de índice 3; todo grupo de orden 36 tiene un subgrupo de índice 4; y todo grupo de orden 48 tiene un subgrupo de índice 3. Por el último apartado del Ejercicio 8.2.6, ningún grupo de esos órdenes puede ser simple.

Supongamos ahora que $|G| = 30 = 2 \cdot 3 \cdot 5$. Del Tercer Teorema de Sylow se deduce que n_3 puede valer 1 ó 10, y que n_5 puede valer 1 ó 6. Si $n_3 = 10$ entonces, como cada par de 3-subgrupos de Sylow tiene intersección trivial, la unión de todos ellos tiene $10 \cdot 2 = 20$ elementos distintos del neutro, todos de orden 3. Análogamente, si $n_5 = 6$ entonces hay $6 \cdot 4 = 24$ elementos de orden 5 en G. Por tanto, no puede tenerse a la vez $n_3 = 10$ y $n_5 = 6$, por lo que uno de ellos vale 1 y por tanto G no es simple.

Sólo nos queda por estudiar el caso $|G| = 56 = 2^3 7$, que estará resuelto si vemos que o bien $n_7 = 1$ o bien $n_2 = 1$. Supongamos que $n_7 \neq 1$ y veamos que $n_2 = 1$. Del Tercer Teorema de Sylow se deduce que $n_7 = 8$. Como en el párrafo anterior, G contiene $8 \cdot 6 = 48$ elementos de orden 7. Sólo quedan pues el neutro y 7 elementos de orden 2 para formar los 2-subgrupos de Sylow (de orden $2^3 = 8$), por lo que ha de ser $n_2 = 1$. □

8.5 Productos directo y semidirecto de subgrupos

En el Capítulo 7 hemos visto que, si un grupo abeliano A es la suma directa de dos subgrupos B y C, entonces A es isomorfo al producto directo $B \times C$. En esta sección describiremos situaciones en las que un grupo (no necesariamente abeliano) es isomorfo al producto directo de dos subgrupos, y estudiaremos una construcción que generaliza el producto directo, y que nos permitirá encontrar nuevos ejemplos de grupos.

Sean H y K dos grupos y sea $G = H \times K$ su producto directo. Si a cada $h \in H$ le asociamos el elemento $\hat{h} = (h, 1)$ de G, a cada $k \in K$ le asociamos $\hat{k} = (1, k) \in G$, y hacemos $\hat{H} = \{\hat{h} : h \in H\}$ y $\hat{K} = \{\hat{k} : k \in K\}$, se comprueba fácilmente que:

- $\hat{H}$ y $\hat{K}$ son subgrupos normales de G.
- Si $\hat{h} \in \hat{H}$ y $\hat{k} \in \hat{K}$, entonces $\hat{h}\hat{k} = \hat{k}\hat{h}$.
- $\hat{H} \cap \hat{K} = \{1\}$.
- $G = \hat{H}\hat{K}$, y si son finitos entonces $|G| = |\hat{H}| \cdot |\hat{K}|$.

Los resultados que siguen muestran que algunas de estas condiciones son suficientes para que un grupo sea isomorfo al producto directo de dos de sus subgrupos.

Lema 8.5.1 *Sea G un grupo finito con subgrupos H y K. Si se verifican las condiciones siguientes:*

1. *H y K* conmutan elemento a elemento*; es decir, si $h \in H$ y $k \in K$ entonces $hk = kh$.*
2. *$H \cap K = \{1\}$.*
3. *$|G| = |H| \cdot |K|$.*

Entonces existe un isomorfismo $G \cong H \times K$.

Demostración. La condición 1 implica que la aplicación $\phi : H \times K \to G$ dada por $\phi(h,k) = hk$ es un homomorfismo de grupos. La condición 2 implica que ϕ es inyectivo, pues si $1 = \phi(h,k) = hk$ (con $h \in H$ y $k \in K$) entonces $k = h^{-1} \in H \cap K$, luego $(h,k) = (1,1)$. Por tanto, Im ϕ es un subgrupo de G isomorfo $H \times K$ y en consecuencia su cardinal es $|H \times K| = |H| \cdot |K|$; la condición 3 nos dice entonces que ϕ es suprayectivo, lo que termina la demostración. □

Ejemplo 8.5.2 *Si n es impar, D_{2n} es el producto directo de D_n y $\mathbb{Z}_2$.*
Consideremos el grupo diédrico $D_{2n} = \langle r, s : r^{2n} = 1, s^2 = 1, srs = r^{-1} \rangle$ y el subgrupo $H = \langle r^2, s \rangle$. Como $o(r^2) = n$ y $sr^2s = (r^2)^{-1}$, se tiene $H \cong D_n$. Por el Ejercicio 5.3.6, se tiene $Z(D_{2n}) = \langle r^n \rangle \cong \mathbb{Z}_2$. Como n es impar, $r^n \notin H$. Ahora es evidente que H y $Z(D_{2n})$ verifican las hipótesis del Lema 8.5.1 y por tanto $D_{2n} \cong D_n \times \mathbb{Z}_2$.

Lema 8.5.3 *Sea G un grupo finito con subgrupos H y K. Si se verifican las condiciones siguientes:*

1. *H y K son normales en G.*
2. *$H \cap K = \{1\}$.*
3. *$|G| = |H| \cdot |K|$.*

Entonces existe un isomorfismo $G \cong H \times K$.

Demostración. Por el Lema 8.5.1, basta ver que H y K conmutan elemento a elemento. Sean pues $h \in H$ y $k \in K$. Por la condición 1 se tiene $h^k \in H$ y $(k^{-1})^h \in K$, y así

$$h^{-1}k^{-1}hk = h^{-1}h^k \in H \qquad \text{y} \qquad h^{-1}k^{-1}hk = (k^{-1})^h k \in K.$$

La condición 2 implica entonces que $h^{-1}k^{-1}hk = 1$, por lo que $hk = kh$, como queríamos ver. □

La generalización del concepto de producto directo prometida al principio de la sección es la siguiente:

Definición 8.5.4 *Sean H y N dos grupos y sea $\phi : H \to \mathrm{Aut}(N)$ un homomorfismo de grupos. Denotamos por ϕ_g la imagen de $g \in H$ por ϕ y definimos en el producto cartesiano $N \times H$ la operación*

$$(x,g)(y,h) = (x\phi_g(y), gh).$$

Esta operación dota a $N \times H$ de una estructura de grupo llamado producto semidirecto *de N por H con* acción *ϕ, que denotaremos por $N \rtimes H$, o por $N \rtimes_\phi H$ si puede haber confusión con respecto a ϕ.*

Ejercicio 8.5.5 *Dados H, N y $\phi : H \to \mathrm{Aut}(N)$ como antes, se pide:*

1. *Comprobar que el producto semidirecto $N \rtimes H$ es un grupo. Identificar el neutro y el inverso de cada elemento.*
2. *Si ϕ es el homomorfismo trivial (es decir, $\phi_g(x) = x$ para todo $g \in H$ y $x \in N$) entonces $N \rtimes H$ es el producto directo $N \times H$.*

3. *Demostrar que $N \rtimes H$ tiene un subgrupo $\hat{H}$ isomorfo a H y un subgrupo normal $\hat{N}$ isomorfo a N tales que $\hat{H} \cap \hat{N}$ es el subgrupo trivial y $\hat{H}\hat{N} = N \rtimes H$.*

4. *¿Cuándo es $N \rtimes H$ abeliano?*

Como ha ocurrido con el producto directo, ciertas condiciones en dos subgrupos de un grupo G nos permiten ver a éste como un producto semidirecto de aquéllos:

Lema 8.5.6 *Sea G un grupo finito con subgrupos N y H. Si se verifican las condiciones siguientes:*

1. *N es normal en G.*
2. *$N \cap H = \{1\}$.*
3. *$|G| = |N| \cdot |H|$.*

Entonces existe un isomorfismo $G \cong N \rtimes_\phi H$, donde $\phi : H \to \mathrm{Aut}(N)$ lleva $g \in H$ al automorfismo $\phi_g : N \to N$ dado por $\phi_g(x) = gxg^{-1}$ (conjugación por g^{-1}).

Demostración. Es claro que ϕ es un homomorfismo de grupos; de hecho, es el homomorfismo asociado a la acción por la izquierda de H sobre N descrita en los Ejemplos 8.1.4. La aplicación $\beta : N \rtimes_\phi H \to G$ dada por $\beta(x, g) = xg$ es un homomorfismo de grupos pues

$$\beta((x,g)(y,h)) = \beta(x\phi_g(y), gh) = xgyg^{-1}gh = xgyh = \beta(x,g)\beta(y,h),$$

y es inyectivo pues $\beta(x, g) = 1$ implica que $x = g^{-1} \in N \cap H = \{1\}$ y por tanto $(x, g) = (1, 1)$. Ahora la condición 3 implica que β es suprayectivo, y por tanto es el isomorfismo que buscamos. □

Para dar ejemplos de productos semidirectos, es interesante estudiar los grupos de automorfismos $\mathrm{Aut}(N)$ cuando N es un grupo sencillo.

Ejercicio 8.5.7 *Demostrar que:*

1. *Si N es un grupo abeliano entonces $\theta(y) = y^{-1}$ (para cada $y \in N$) define un automorfismo de N, y se tiene $\theta^2 = 1$ en $\mathrm{Aut}(N)$.*
2. *Sea $N = \langle x \rangle$ un grupo cíclico finito de orden n. Entonces cada homomorfismo $\eta : N \to N$ queda determinado por el valor de $\eta(x)$, y η es un automorfismo si y sólo si $\eta(x) = x^i$ con $\mathrm{mcd}(n, i) = 1$. De hecho, hay un isomorfismo de grupos $\mathrm{Aut}(N) \cong \mathbb{Z}_n^*$.*
3. *Si N es cíclico de orden 3 ó 4, entonces $\mathrm{Aut}(N) = \{1, \theta\}$, donde θ es el automorfismo del apartado 1.*
4. *Si $N = \{1, a, b, c\}$ es el grupo de Klein, entonces cada automorfismo de N induce una permutación de $\{a, b, c\}$, y de hecho esto define un isomorfismo $\mathrm{Aut}(N) \cong S_3$. Los elementos de orden 2 de $\mathrm{Aut}(N)$ son los que fijan exactamente uno de los elementos a, b ó c.*

Ejemplos 8.5.8 *Productos semidirectos.*
En todos los ejemplos, θ es el automorfismo del Ejercicio 8.5.7.

1. Sean $H = \langle g \rangle$ y $N = \langle x \rangle$ dos grupos cíclicos de ordenes 2 y 3, respectivamente, y sea $\phi : H \to \mathrm{Aut}(N)$ el homomorfismo dado por $g \mapsto \theta$. Entonces es fácil ver que $N \rtimes H \cong S_3$.
2. Más generalmente, si N es un grupo abeliano y $H = \langle g \rangle$ es cíclico de orden 2, entonces el homomorfismo $\phi : H \to \mathrm{Aut}(N)$ dado por $\phi_g = \theta$ induce un producto semidirecto. Si N es cíclico de orden n, es fácil dar un isomorfismo $D_n \cong N \rtimes H \cong Z_n \rtimes_\phi \mathbb{Z}_2$. Si N es cíclico infinito, el grupo obtenido se llama *diédrico infinito*.
3. Sean $H = \langle g \rangle$ y $N = \langle x \rangle$ grupos cíclicos de ordenes 4 y 3, respectivamente. El producto semidirecto asociado al homomorfismo $\phi : H \to \mathrm{Aut}(N)$, dado por $\phi(g) = \theta$, es un grupo de orden 12 que denotaremos por $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$.

Ejercicio 8.5.9 *Sea $H = \langle g \rangle$ un grupo cíclico de orden 3 y sea $N = \langle x_1, x_2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Demostrar que existe un homomorfismo de grupos $\phi : H \to \mathrm{Aut}(N)$ tal que $\phi_g(x_1) = x_2$ y $\phi_g(x_2) = x_1x_2$, y describir un isomorfismo explícito entre $N \rtimes H$ y A_4.*

8.6 Grupos de orden bajo

En esta sección obtenemos información acerca de la estructura de ciertos grupos finitos cuyo orden tiene una factorización en primos sencilla, y a partir de ellos describimos todos los grupos de orden menor o igual que 15.

Proposición 8.6.1 *Sea G un grupo finito con $|G| = p^r q^s$, donde p y q son primos distintos y $r, s \in \mathbb{Z}^+$. Si G tiene un único p-subgrupo de Sylow H y un único q-subgrupo de Sylow K, entonces $G \cong H \times K$.*

Demostración. Bastará ver que H y K verifican las tres condiciones del Lema 8.5.3. La primera se verifica por el Tercer Teorema de Sylow (8.4.9); la segunda porque $|H \cap K|$ debe ser un divisor común de $|H| = p^r$ y de $|K| = q^s$; y la tercera es evidente. □

Proposición 8.6.2 *Sea G un grupo finito con $|G| = pq$, donde $p < q$ son primos y $q \not\equiv 1 \bmod p$. Entonces G es un grupo cíclico.*

Demostración. Sea n_p el número de p-subgrupos de Sylow de G. El Tercer Teorema de Sylow (8.4.9) y la hipótesis $q \not\equiv 1 \bmod p$ implican que $n_p = 1$. Es decir, G tiene un único p-subgrupo de Sylow H, que tiene orden p y por tanto $H \cong \mathbb{Z}_p$. Como la relación $p < q$ implica que $p \not\equiv 1 \bmod q$, se ve del mismo modo que G tiene un único q-subgrupo de Sylow $K \cong \mathbb{Z}_q$. Por la Proposición 8.6.1 y el Teorema Chino de los Restos se tiene $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$, como queríamos ver. □

Proposición 8.6.3 *Si p es un primo impar, entonces un grupo de orden $2p$ o bien es cíclico o bien es isomorfo al grupo diédrico D_p.*

Demostración. Si G es abeliano el resultado es claro, considerando su descomposición invariante. Supongamos pues que G no es abeliano. Con la notación usual se tiene $n_p = 1$, de modo que G posee un subgrupo normal N de orden p. Como p es primo, existe $x \in G$ tal que $N = \langle x \rangle$. Por otra parte, G contiene algún subgrupo $H = \langle g \rangle$ de orden 2. Como $G = \langle x, g \rangle$ (¿por qué?) y no es abeliano, se tiene $xg \neq gx$. Es claro que el orden de xg no es 1, y no es $2p$ pues G no es cíclico. Tampoco es p pues, al ser $\langle x \rangle$ el único p-subgrupo de Sylow, eso nos daría $xg \in \langle x \rangle$ y por tanto $g \in \langle x \rangle$, que es absurdo. En conclusión, debe ser $(xg)^2 = 1$, o sea $gxg^{-1} = x^{-1}$. Ahora el Lema 8.5.6 y los Ejemplos 8.5.8 nos dan el resultado. □

Podemos ya iniciar la descripción de los grupos de orden menor o igual que 15. De hecho ya tenemos descritos casi todos esos grupos desde hace tiempo, y lo que nos permiten los últimos resultados es asegurarnos de que no hay más.

Grupos de orden 2, 3, 5, 7, 11 ó 13.

Si n vale 2, 3, 5, 7, 11 ó 13 el único grupo (salvo isomorfismos) de orden n es $\mathbb{Z}_n$ (Proposición 5.5.6).

Grupos de orden 4 ó 9.

Si $|G| = p^2$ con p primo, la Proposición 5.9.9 nos dice que G es abeliano y entonces, por el Teorema de Estructura 7.5.13, G es isomorfo a $\mathbb{Z}_{p^2}$ o a $\mathbb{Z}_p \times \mathbb{Z}_p$. Así, hay solamente dos grupos de orden 4 (el grupo cíclico $\mathbb{Z}_4$ y el grupo de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$); y dos grupos de orden 9 ($\mathbb{Z}_9$ y $\mathbb{Z}_3 \times \mathbb{Z}_3$).

Grupos de orden 6, 10 ó 14.

Por la Proposición 8.6.3 hay exactamente dos grupos (salvo isomorfismos) de cada uno de esos órdenes: el cíclico y el diédrico. Es decir, los únicos grupos de orden 6 son $\mathbb{Z}_6$ y D_3; los únicos grupos de orden 10 son $\mathbb{Z}_{10}$ y D_5; y los únicos grupos de orden 14 son $\mathbb{Z}_{14}$ y D_7.

Grupos de orden 8.

Conocemos cinco grupos distintos y no isomorfos de orden 8 (ver el final de la Sección 5.8): son los grupos abelianos $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ y $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$; y los grupos no abelianos D_4 y Q_8. Por el Teorema de Estructura 7.5.13 no hay más grupos abelianos de orden 8. Por tanto, para ver que ésos son todos los grupos de orden 8, hemos de probar que un grupo G no abeliano y de orden 8 debe ser isomorfo a D_4 ó a Q_8.

Como G no contiene elementos de orden 8 (¿por qué?) y no todos sus elementos pueden tener orden ≤ 2 (¿por qué?), G debe contener un elemento x de orden 4. Como $\langle x \rangle$ tiene índice 2, es normal en G y $G/\langle x \rangle \cong \mathbb{Z}_2$. Si fijamos ahora $y \notin \langle x \rangle$, se tiene $G = \langle x, y \rangle$, y en consecuencia $xy \neq yx$. Como además $x^y \in \langle x \rangle$ (por la normalidad) y $o(x^y) = o(x) = 4$, ha de ser $x^y = x$ ó $x^y = x^3$, pero la primera posibilidad equivale a $xy = yx$ y por tanto se ha de dar la segunda: $x^y = x^3 = x^{-1}$.

Por otra parte, como $G/\langle x \rangle \cong \mathbb{Z}_2$, se tiene $y^2 \in \langle x \rangle$. Si fuera $y^2 = x$ ó $y^2 = x^3$ deduciríamos que $o(y) = 8$, por lo que ha de ser $y^2 = 1$ ó $y^2 = x^2$. La primera posibilidad nos lleva a la situación

$$G = \langle x, y \rangle, \qquad x^4 = 1, \qquad y^2 = 1, \qquad y^{-1}xy = x^{-1},$$

y es entonces claro que $G \cong D_4$. La segunda posibilidad nos lleva a la situación

$$G = \langle x, y \rangle, \qquad x^4 = 1, \qquad y^2 = x^2, \qquad y^{-1}xy = x^{-1},$$

y entonces es fácil establecer un isomorfismo $G \cong Q_8$ que lleve $x \mapsto \mathbf{i}$ e $y \mapsto \mathbf{j}$.

Grupos de orden 15.

Por la Proposición 8.6.2, el único grupo de orden 15 es $\mathbb{Z}_{15}$.

Grupos de orden 12.

Conocemos cinco grupos de orden 12. Por los resultados del Capítulo 7, hay exactamente dos que son abelianos, $\mathbb{Z}_{12}$ y $\mathbb{Z}_6 \times \mathbb{Z}_2$. Otros tres no son abelianos; se trata del grupo alternado A_4, del grupo diédrico D_6 y del grupo $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ de los Ejemplos 8.5.8 (producto semidirecto de $\mathbb{Z}_3 = \langle x \rangle$ por $\mathbb{Z}_4 = \langle g \rangle$ con homomorfismo $\phi : \langle g \rangle \to \mathrm{Aut}(\langle x \rangle)$ dado por $\phi_g(x) = x^{-1}$). Éstos no son isomorfos entre sí porque A_4 no tiene subgrupos de orden 6, D_6 tiene elementos de orden 6 y $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ tiene elementos de orden 4.

Vamos a demostrar que no hay más grupos no abelianos de orden 12. Para ello, basta con demostrar que un grupo G no abeliano y de orden 12 debe ser isomorfo a D_6, A_4 ó $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$.

Sea G un tal grupo, y sean H un 2-subgrupo de Sylow (de orden 4) y K un 3-subgrupo de Sylow (de orden 3). Como H y K son abelianos y G no lo es, de las Proposiciones 8.4.10 y 8.6.1 se deduce que exactamente uno de estos dos subgrupos es normal en G. Como $|K| = 3$, existe $k \in G$ de orden 3 tal que $K = \langle k \rangle$. Para H tenemos dos opciones: o bien es cíclico, $H = \langle h \rangle$ con $o(h) = 4$, o bien es isomorfo al grupo de Klein, $H = \langle h_1, h_2 \rangle$ con $o(h_1) = o(h_2) = 2$ y $h_1h_2 = h_2h_1$. Distinguiremos casos según cuál de los subgrupos sea normal y según sea H cíclico o no.

Supongamos primero que H es normal en G. Por el Lema 8.5.6 se tiene $G \cong H \rtimes_\phi K$ para el homomorfismo $\phi : K \to \mathrm{Aut}(H)$ tal que ϕ_k es conjugar por k^{-1}. Como ϕ no es trivial (de lo contrario $G \cong H \times K$ sería abeliano) y K es simple, ϕ debe ser inyectivo y por tanto ϕ_k tiene orden 3 en $\mathrm{Aut}(H)$. Por los dos últimos apartados del Ejercicio 8.5.7, deducimos que H ha de ser el grupo de Klein y que podemos elegir los generadores h_1 y h_2 de H de modo que se tenga $\phi(h_1) = h_2$ y $\phi(h_2) = h_1h_2$. Entonces el Ejercicio 8.5.9 nos dice que $G \cong A_4$.

Supongamos ahora que K es normal en G. Por el Lema 8.5.6 se tiene $G \cong K \rtimes_\phi H$ para el homomorfismo no trivial $\phi : H \to \mathrm{Aut}(K)$ tal que ϕ_g es conjugar por g^{-1}, para cada $g \in H$. Por el Ejercicio 8.5.7 se tiene $\mathrm{Aut}(K) = \{1, \theta\}$ con $\theta(k) = k^{-1}$. Si $H = \langle h \rangle$ es cíclico entonces debe ser $\phi_h = \theta$, y por tanto G es el grupo $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ de los Ejemplos 8.5.8. Supongamos por último que H es el grupo de Klein. Entonces el núcleo de ϕ tiene dos elementos y, eligiendo adecuadamente los generadores de H, podemos poner $H = \langle h_1, h_2 \rangle$ con $\phi_{h_1}(k) = k^{-1}$ y $\phi_{h_2}(k) = k$. Entonces $D = \langle k, h_1 \rangle$ es un subgrupo de G isomorfo a D_3. Comprobando que D y $E = \langle h_2 \rangle \cong \mathbb{Z}_2$ verifican las hipótesis del Lema 8.5.1, deducimos que $G \cong D \times E \cong D_3 \times \mathbb{Z}_2$, y por tanto $G \cong D_6$ por el Ejemplo 8.5.2.

Resumen: Grupos de orden menor o igual que 15.

La siguiente tabla resume la clasificación de los grupos de orden menor o igual que 15 (excepto los de orden primo). En la primera columna aparecen los posibles órdenes, en la segunda el número N de grupos no isomorfos de cada orden, con el número de abelianos entre paréntesis, en la tercera se da la lista de los abelianos, y en la cuarta la de los no abelianos.

$\|G\|$	N	Abelianos	No abelianos
4	2 (2)	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$	
6	2 (1)	$\mathbb{Z}_6$	D_3
8	5 (3)	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_4, Q_8
9	2 (2)	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$	
10	2 (1)	$\mathbb{Z}_{10}$	D_5
12	5 (2)	$\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$	D_6, A_4, $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$
14	2 (1)	$\mathbb{Z}_{14}$	D_7
15	1 (1)	$\mathbb{Z}_{15}$	

Clasificar grupos de órdenes mayores puede ser muy laborioso (por ejemplo, existen 14 grupos distintos de orden 16), aunque ya hemos visto que es sencillo cuando el orden tiene una factorización adecuada (Teorema 5.8.7 y Proposiciones 5.9.9 y 8.6.3). Con las técnicas vistas en este capítulo resulta fácil clasificar los grupos de órdenes $18, 20, 21$ ó 30. En el libro *Group Tables*, de A. Thomas y G. Wood (Shiva Math. Series), se describen todos los grupos de orden menor o igual que 32, y para cada uno de ellos se da la tabla y se describen todos sus subgrupos y sus clases de conjugación.

8.7 Problemas

1. Sea $\Omega = \{A, B, C, D\}$ el conjunto de los vértices de un cuadrado, y sea $S(\Omega)$ su grupo de permutaciones. Se pide:

   (a) Describir un homomorfismo inyectivo $D_4 \to S(\Omega)$.

   (b) Describir las órbitas y los estabilizadores de la correspondiente acción por la izquierda de D_4 en Ω.

   (c) Determinar todas las órbitas y los estabilizadores de la restricción de esta acción al subgrupo de las rotaciones.

2. Considérese S_3 actuando en el conjunto Ω de sus subgrupos por conjugación. Determinar la órbita y el estabilizador de $< (12) >$.

3. Sea $\omega = \frac{-1+\sqrt{-3}}{2}$ una raíz cúbica de 1. Demostrar que $D_3 = \langle a, b \mid a^3 = b^2 = e, bab = a^{-1} \rangle$ actúa en la circunferencia unidad C que identificaremos con $C = \{z \in \mathbb{C} : |z| = 1\}$ de forma que

   $$b \cdot z = \bar{z} \quad a \cdot z = \omega z.$$

   Calcular las órbitas de esta acción. Generalizar esta acción a una acción del grupo diédrico D_n en C.

4. Verificar que, para grupos no abelianos, la acción por conjugación gxg^{-1} es una acción por la izquierda pero no por la derecha, y viceversa para $g^{-1}xg$.

5. Sean x e y elementos conjugados en un grupo finito G. Probar que el número de elementos $g \in G$ tales que $x^g = y$ es igual al orden del subgrupo $\mathrm{Cen}_G(x)$.

6. Probar que si en un grupo G existe un elemento que tiene exactamente dos conjugados entonces G posee un subgrupo normal propio y no trivial.

7. [*] Sea G un grupo finito y sea p el menor divisor primo de $|G|$. Demostrar que si H es subgrupo normal de G de orden p entonces $H \subseteq Z(G)$. (Indicación: Considerar G actuando por conjugación sobre H.)

8. [*] Sea G un grupo finito que actúa sobre un conjunto finito Ω. Para cada $g \in G$, designamos por Ω_g al conjunto $\{\alpha \in \Omega : g\alpha = \alpha\}$ de los punto fijados por g. Demostrar que el número de órbitas de G en Ω es
$$\frac{1}{|G|}\sum_{g\in G}|\Omega_g|;$$
es decir, el promedio del número de puntos fijados por los elementos de G. (Indicación: Contar el número de elementos del conjunto $\{(g,\alpha) \in G \times \Omega : g\alpha = \alpha\}$ de dos maneras distintas.)

9. [*] Sea G un grupo finito que actúa en un conjunto finito X. Sea k el número de órbitas. Para cada $g \in G$ sea $v(g)$ el cardinal del conjunto $\{x \in X : g \cdot x \neq x\}$. Demostrar:
   (a) $\sum_{g\in G} v(g) = |G|(|X| - k)$.
   (b) Si $k = 1$, entonces $|G| = |X|$ si y sólo si para todo $g \in G \setminus \{1\}$ y todo $x \in X$, $g \cdot x \neq x$.

10. Sean G un grupo finito, H un subgrupo propio y no trivial de G, X el conjunto de los subgrupos conjugados de H y $S(X)$ el grupo simétrico sobre el conjunto X.
    (a) Demostrar que la aplicación $\varphi : G \to S(X)$ dada por $\varphi(h)(K) = hKh^{-1}$ es un homomorfismo de grupos. Deducir que si G es simple, entonces $|G|$ divide a $|S(X)|$.
    (b) Utilizar el apartado anterior para probar que ningún grupo de orden 300 es simple.

11. Si un grupo G posee un único p-subgrupo de Sylow P, demostrar que P es un subgrupo característico de G.

12. Sea P un p-subgrupo de Sylow de un grupo finito G y sea N un subgrupo normal de G. Probar que PN/N es un p-subgrupo de Sylow de G/N.

13. Demostrar que si H es un subgrupo de índice finito de G entonces $N = \cap_{g\in G} g^{-1}Hg$ tiene índice finito en G. Concluir que si G tiene un subgrupo propio de índice finito, entonces también tiene un subgrupo propio normal de índice finito.

14. Sean G un grupo que actúa sobre dos conjuntos X e Y. Demostrar que
$$g \cdot (x, y) = (g \cdot x, g \cdot y)$$
es una acción de G en $X \times Y$ y que se tiene $G_{(x,y)} = G_x \cap G_y$ para cualesquiera $x, y \in G$. Utilizar esto para demostrar que, si H y K son dos subgrupos de G de índice finito, entonces $H \cap K$ también tiene índice finito en G y $[G : H \cap K] \leq [G : H][G : K]$. Demostrar que si además $[G : H] = [G : K] = r$, entonces $[G : H \cap K] \leq r(r - 1)$.

15. Sea G un grupo que actúa sobre un conjunto X. Demostrar:
    (a) $G_0 = \cap_{x\in X} G_x$ es un subgrupo normal de G.
    (b) La acción de G en X es fiel precisamente si $G_0 = \{e\}$.
    (c) G/G_0 actúa fielmente en X de forma natural.

16. Dados H, N y un homomorfismo $\phi : H \to \mathrm{Aut}(N)$, demostrar que las condiciones siguientes son equivalentes para un elemento (x, g) de $N \rtimes_\phi H$:
    (a) (x, g) está en el centro de $N \rtimes_\phi H$.
    (b) (x, g) conmuta con los elementos de la forma $(1, h)$ y con los de la forma $(y, 1)$.
    (c) $g \in Z(H)$, ϕ_g es la conjugación por x, y $\phi_h(x) = x$ para cada $h \in H$.

17. Demostrar que el conjunto G de las matrices de la forma $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$ tales que $a, b, c \in \mathbb{Z}_5$ y $ac \neq 0$ es un grupo multiplicativo. Determinar su orden, encontrar los elementos de orden 5 y describir los 5-subgrupos de Sylow de G.

18. Sea G un grupo que posee un sistema generador formado por tres elementos a, b, c que satisfacen las siguientes condiciones:

$$o(a) = o(b) = 2,\ o(c) = 3 \qquad ab = ba,\ a^c = b,\ b^c = ab.$$

Demostrar que $|G| = 12$, y determinar todos los subgrupos normales de G. ¿A qué grupo de los que hemos descrito en el texto es isomorfo G?

19. Demostrar que si H y K son dos subgrupos de un grupo que verifican $K \subseteq N_G(H)$ y $H \cap K = \{1\}$, entonces $HK \cong H \rtimes K$ para cierto homomorfismo $K \to \mathrm{Aut}(H)$.

20. Probar que ningún grupo de orden $2p^r$ (donde p es primo y $r \geq 1$) es simple.

21. Sean G un grupo finito, p un divisor primo de $|G|$ y N la intersección de todos los p-subgrupos de Sylow de G. Demostrar que N es el mayor p-subgrupo de G que es normal en G (es decir, N es normal y cualquier otro p-subgrupo que sea normal está contenido en N).

22. Probar que no hay grupos de orden 490 que sean simples.

23. [*] Se pide:

    (a) Demostrar que si a y b son elementos de un grupo con $o(a) = n$ y $o(b) = m$, y si existe un entero i tal que $b^{-1}ab = a^i$, entonces $i^m \equiv 1 \bmod n$.

    (b) Recíprocamente, demostrar que si n, m e i son enteros positivos tales que $i^m \equiv 1 \bmod n$, entonces existe un grupo de orden nm generado por dos elementos a y b tales que $o(a) = n$, $o(b) = m$ y $b^{-1}ab = a^i$.

    (c) Mostrar que las permutaciones $\sigma = (1,2,3,4,5,6,7)$ y $\tau = (1,4,2)(3,5,6)$ de S_7 verifican $\sigma^\tau = \sigma^2$, y describir un subgrupo de S_7 no abeliano de orden 21.

    (d) Demostrar que todos los grupos de orden impar menor que 21 son abelianos.

24. [*] Sean n y m enteros positivos tales que m y $\phi(n)$ son coprimos. Demostrar que si a y b son dos elementos de órdenes n y m de un grupo y $\langle a \rangle$ es un subgrupo normal, entonces $ab = ba$.

25. Probar que todo grupo de orden 255, 455 ó 1645 es cíclico.

26. Probar que ningún grupo tiene un centro de índice 77.

27. Demostrar que dos subgrupos conjugados de un grupo G tienen el mismo índice en G. (Indicación: Considerar G actuando en el conjunto de los subgrupos por traslaciones.)

28. [*] Demostrar que un grupo de orden 108 tiene un subgrupo normal de orden 9 ó 27.

29. Sea H un subgrupo normal de un grupo finito G y p un divisor primo de $|G|$ tal que $[G : H]$ no es múltiplo de p. Demostrar que H contiene todos los p-subgrupos de Sylow de G.

30. Demostrar que si G es un grupo finito de orden pq, con $p < q$ primos y de forma que $q \not\equiv 1 \bmod p$, entonces G es cíclico. Dar un ejemplo de un grupo no cíclico de orden pq con $p < q$ primos.

31. Demostrar que un grupo de orden $p^n q$, con p y q primos distintos y $p^{n-1} < q$, no es simple.

32. Demostrar que un grupo simple no tiene orden p^2q^2 con p y q dos primos distintos. (Indicación: Obsérvese que $q|p+1$ con $p < q$ implica $q = p + 1 = 3$.)

33. Sea G un grupo tal que $|G/Z(G)| = pq$, con $p < q$ primos. Demostrar que $q \equiv 1 \bmod p$.

34. Clasificar los grupos de orden 18, 20 y 30.

35. Calcular el número de p-subgrupos de Sylow de S_p, con p primo y del resultado obtenido deducir el Teorema de Wilson.

36. [*] Sea H un subgrupo propio del grupo alternado A_n, con $n \geq 5$. Demostrar que $[A_n : H] \geq n$. Demostrar que, para cada divisor $m \geq 5$ de 60, A_5 tiene un subgrupo de índice m.

37. Sea $f(x_1, \ldots, x_n)$ una función en n variables y, para cada $\sigma \in S_n$, sea $\sigma(f)$ la función en n variables
$$\sigma(f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$
Demostrar que si $n \geq 5$ y el número k de funciones $\sigma(f)$ distintas es > 2, entonces $k \geq n$.

38. [*] Probar que si G es finito y P es un subgrupo de Sylow de G, entonces todo subgrupo H de G que contenga al normalizador $N_G(P)$ es su propio normalizador; es decir, verifica $H = N_G(H)$. (Indicación: Usar el Segundo Teorema de Sylow aplicado a H.)

39. [*] Demostrar que no hay grupos simples de orden n no primo y $n \neq 60$, para $n < 168$. ¿Hasta donde puedes llegar para $n > 168$?

40. [*] Sea G un grupo simple de orden 60. Demostrar:

    (a) Si G actúa en un conjunto X con menos de 5 elementos entonces lo hace trivialmente; es decir, $g \cdot x = x$, para todo $g \in G$ y $x \in X$. Concluir que G no tiene subgrupos propios de índice menor que 5.

    (b) Si $H_1 \neq H_2$ son 2-subgrupos de Sylow de G, entonces $K = \langle H_1 \cup H_2 \rangle$ tiene índice 1 ó 5.

    (c) Si el número de 2-subgrupos de Sylow de G es 15, entonces al menos dos de ellos H_1 y H_2 se intersecan no trivialmente y en tal caso $K = \langle H_1 \cup H_2 \rangle$ ha de tener índice 5. (Indicación: Para la primera afirmación, contar elementos de orden potencia de 2 y de orden potencia de 5. Para la segunda, observar que K tiene centro no trivial.)

    (d) G actúa de forma no trivial en un conjunto con 5 elementos.

    (e) $G \cong A_5$.

41. [*] Sea G un grupo. Un *G-conjunto* (por la izquierda) es un conjunto X junto con una acción por la izquierda de G en X. Un *homomorfismo de G-conjuntos* es una aplicación $\phi : X_1 \to X_2$ entre dos G-conjuntos X_1 y X_2 tal que $\phi(g \cdot x) = g \cdot \phi(x)$ para cada $x \in X_1$. Demostrar:

    (a) La composición de dos homomorfismos de G-conjuntos es un homomorfismo de G-conjuntos.

    (b) Si $\phi : X_1 \to X_2$ es un homomorfismo de G-conjuntos biyectivo, entonces $\phi^{-1} : X_2 \to X_1$ es un homomorfismo de G-conjuntos. Se dice entonces que ϕ es un *isomorfismo* de G-conjuntos.

    (c) Sea X un G-conjunto. Un G-subconjunto de X es un subconjunto Y de X tal que $Gy \subseteq Y$ para cada $g \in G$ y cada $y \in Y$. En este caso, la restricción a Y de la acción de G dota a Y de una estructura de G-conjunto, y la inclusión $Y \hookrightarrow X$ es un homomorfismo de G-conjuntos.

    (d) Las órbitas de un G-conjunto X son G-subconjuntos de X.

    (e) Si $\{X_i : i \in I\}$ es una familia de G-conjuntos disjuntos, entonces la unión $X = \cup_{i \in I} X_i$ tiene una única estructura de G-conjunto en la que cada X_i es un G-subconjunto. Este G-conjunto se llama *coproducto* y se denota por $\coprod_{i \in I} X_i$.

    (f) Sean X un G-conjunto, $x \in X$ y $H = \mathrm{Estab}_G(x)$. Consideremos la acción por la izquierda por traslaciones de G sobre G/H. Entonces la aplicación $\phi : G/H \to X$ dada por $\phi(gH) = gx$ está bien definida y es un homomorfismo de G-conjuntos.

    (g) Todo G-conjunto (por la izquierda) es isomorfo a un coproducto de G-conjuntos de la forma G/H, donde cada H es un subgrupo de G y G actúa en G/H por traslaciones.

    (h) Sean $H_1, \ldots, H_n, K_1, \ldots, K_m$ subgrupos de G, y sean $X = \coprod_{i=1}^{n} G/H_i$ e $Y = \coprod_{i=1}^{m} G/K_i$ los G-conjuntos coproducto, donde en cada cociente se considera la acción por traslaciones. Demostrar que X e Y son isomorfos si y sólo si $n = m$ y existe una permutación $\sigma \in S_n$ tal que H_i y $K_{\sigma(i)}$ son conjugados para cada $i = 1, \ldots, n$.

Bibliografía del capítulo

Delgado-Fuertes-Xambó [11], Dorronsoro-Hernández [13], Herstein [20], Jacobson [23], Rotman [30].

Capítulo 9

Series normales

Se estudian las series normales de un grupo, y se demuestran las propiedades básicas de los grupos resolubles y de los grupos de longitud finita.

Introducción

Sea G un grupo con un subgrupo normal N, propio y no trivial. Como N y G/N son grupos "más pequeños" que G, puede ser que tengamos cierta información sobre ellos, y entonces es natural tratar de usarla para deducir propiedades de G. Es decir, podemos pensar que G "se descompone" de algún modo en las "piezas" N y G/N, y la tarea es "recomponer" G a partir de esas piezas. Hay que advertir que, en general, N y G/N no determinan a G, pero sí pueden conocerse algunas propiedades de G a partir de las de estas piezas.

A su vez, podemos tratar de estudiar cada pieza descomponiéndola en otras: Si H es un subgrupo normal de N podemos estudiar N a partir de H y N/H, y si K/N es un subgrupo normal de G/N (es decir, si se tiene $N \trianglelefteq K \trianglelefteq G$) podemos estudiar G/N a partir de su subgrupo K/N y del correspondiente cociente $(G/N)/(K/N) \cong G/K$. Globalmente, estamos tratando de conocer G a partir del conocimiento de los grupos H, N/H, K/N y G/K, donde H, N y K son subgrupos de G tales que $H \trianglelefteq N \trianglelefteq K \trianglelefteq G$.

Esto sugiere la definición de una serie normal de un grupo G como una cadena de subgrupos

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{n-1} \trianglerighteq G_n = \{1\}.$$

Dada una tal serie, y generalizando la idea anterior, podemos interpretar que G está compuesto a partir de las piezas (que llamaremos factores de la serie) G_{i-1}/G_i con $i = 1, \ldots, n$. Cuando estos factores son sencillos en algún sentido (por ejemplo, abelianos, cíclicos, simples...), es posible obtener información sobre G a partir de la de los factores, y en este capítulo estudiaremos algunas situaciones de este tipo.

En lugar de comenzar con la definición general de serie normal, analizamos primero un caso concreto. A cada grupo G se le asocia un subgrupo normal G' tal que el cociente G/G' es "el mayor grupo cociente abeliano" de G. Repitiendo este proceso, se obtiene una cadena de subgrupos $G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots$ (la "serie derivada" de G) que, si en algún paso alcanza al subgrupo trivial, proporciona una serie normal de G con factores abelianos (decimos entonces que G es resoluble). Esto motiva nuestra definición general de serie normal, y demostramos entonces que un grupo G es resoluble si y sólo si posee una serie normal con factores abelianos. En el caso de grupos finitos, esto equivale a que exista una serie normal de G con factores cíclicos y, como se verá en la asignatura de Ecuaciones Algebraicas, este hecho hará especialmente relevantes a los grupos resolubles en el estudio de las ecuaciones (de hecho, el nombre se debe a la conexión de estos grupos con la resolubilidad por radicales de las ecuaciones).

Otra clase importante de series normales son las que tienen sus factores simples; es decir, aquéllas en las que no pueden añadirse nuevos términos. Estas series se llaman series de composición, y un grupo que posea una se dice que tiene longitud finita. En el contexto de las series normales, los grupos simples han de considerarse como los "bloques básicos", puesto que no se pueden descomponer en el sentido que estamos considerando en este capítulo. Por tanto, los grupos de longitud finita son los que admiten descomposiciones en términos de estos bloques básicos. En la segunda mitad del capítulo

estudiamos estos grupos hasta demostrar el Teorema de Jordan-Hölder, que afirma que todas las series de composición de un grupo de longitud finita G tienen los mismos factores.

El hecho de que todo grupo finito tenga longitud finita, combinado con la existencia de una descripción (complicada) de todos los grupos simples finitos, puede interpretarse como un teorema de estructura para los grupos finitos. Pero este teorema es mucho menos contundente que el que vimos para grupos abelianos, por dos motivos: Por una parte, los "bloques básicos de estructura" en el caso abeliano (grupos cíclicos) son mucho más sencillos que los grupos simples (a pesar de su nombre). Por otra parte, en cuanto a la manera de "componer" esos bloques básicos, las sumas directas son más manejables que las series normales, y además determinan salvo isomorfismos al grupo en cuestión.

Objetivos del capítulo

- Conocer las propiedades del subgrupo derivado de un grupo.
- Conocer el concepto de serie normal y las distintas caracterizaciones y propiedades de los grupos resolubles y de longitud finita.
- Saber calcular series derivadas y series de composición en ejemplos concretos.
- Conocer las propiedades de la longitud de composición, y saber usarlas para su cálculo en ejemplos.

Desarrollo de los contenidos

9.1 El subgrupo derivado

Dado un grupo no abeliano G, es interesante medir de algún modo lo cerca que está G de ser abeliano. El centro del grupo es útil para esto: cuanto mayor es $Z(G)$ más cerca está G de ser abeliano. En esta sección vamos a desarrollar una herramienta alternativa para evaluar la "falta de abelianidad" de G.

Observemos dos cosas: Por una parte, un elemento de la forma $aba^{-1}b^{-1}$ vale 1 precisamente cuando a y b conmutan, por lo que tales elementos (y el subgrupo que generan) serán interesantes para nuestro propósito. Por otra parte, es obvio que G tiene grupos cociente abelianos (al menos G/G, que es trivial), y será interesante considerar los mayores de ellos; es decir, los que se obtienen tomando el cociente por un subgrupo lo menor posible. En lo que sigue vemos cómo estas dos ideas confluyen en el concepto de subgrupo derivado de G.

Definición 9.1.1 *Sea G un grupo. El* conmutador *de los elementos $a, b \in G$ es el elemento*

$$[a, b] = aba^{-1}b^{-1}.$$

El subgrupo de G generado por los conmutadores se llama subgrupo derivado *de G y se denota por G'.*

Las siguientes propiedades se verifican fácilmente:

Ejercicio 9.1.2 *Dados un grupo G y elementos $a, b \in G$, demostrar que:*

1. *G es abeliano si y sólo si $G' = \{1\}$.*
2. *$[a, b]^{-1} = [b, a]$.*
3. *G' consiste en los productos finitos de conmutadores.*
4. *Si $f : G \to H$ es un homomorfismo de grupos entonces $f([a, b]) = [f(a), f(b)]$.*
5. *En particular, si N es normal en G, entonces $[a, b]N = [aN, bN]$ en G/N.*
6. *$[a, b]^x = [a^x, b^x]$ para cada $x \in G$.*

Ejemplo 9.1.3 *El subgrupo derivado de S_n.*

Vamos a demostrar que $S_n' = A_n$. En efecto, como la "aplicación signo" $S_n \to \{1, -1\}$ es un homomorfismo, es claro que todo conmutador es par, y en consecuencia $S_n' \subseteq A_n$. Recíprocamente, la igualdad

$$(ijk) = (ij)(ik)(ij)(ik) = [(ij), (ik)]$$

nos dice que cada ciclo de longitud 3 de S_n está en S_n', y como tales ciclos generan A_n (Proposición 6.2.7) deducimos que $A_n \subseteq S_n'$, lo que nos da la igualdad buscada.

La propiedad básica del subgrupo derivado es la siguiente.

Teorema 9.1.4 *Dado un grupo G, su subgrupo derivado G' es el menor subgrupo normal de G que da un cociente abeliano; es decir, se verifican:*

1. *G' es un subgrupo normal de G.*
2. *El cociente G/G' es abeliano.*
3. *Si N es un subgrupo normal de G tal que el cociente G/N es abeliano, entonces $G' \subseteq N$.*

Demostración. 1. Vemos que, si $g \in G'$ y $x \in G$, entonces $g^x \in G'$. En efecto, por el Ejercicio 9.1.2, se tiene $g = [a_1, b_1] \cdots [a_n, b_n]$ para ciertos elementos de G, y por tanto

$$g^x = [a_1, b_1]^x \cdots [a_n, b_n]^x = [a_1^x, b_1^x] \cdots [a_n^x, b_n^x] \in G'.$$

2. Es una consecuencia inmediata del Ejercicio 9.1.2.

3. Si N es como en el enunciado y $a, b \in G$, entonces $[a, b]N = [aN, bN] = N$, luego $[a, b] \in N$. Es decir, N contiene a cada conmutador de G y en consecuencia contiene a G'. □

El Teorema 9.1.4 nos dice que, en cierto sentido, G' convierte a G en un grupo abeliano perdiendo la menor información posible (si entendemos que al hacer el cociente por G' se pierde la información sobre G', pues sus elementos representan al neutro en el cociente). Podemos decir que, cuanto más pequeño es G', más cerca está G de ser abeliano. En la próxima sección consideraremos una manera más precisa de medir lo lejos que está G de ser abeliano. Concluimos ésta con un ejemplo.

Ejemplo 9.1.5 *El subgrupo derivado de Q_8.*

Sabemos que el grupo de los cuaterniones Q_8 no es abeliano y que todos sus subgrupos son normales (Ejemplos 5.6.3). En particular lo es el subgrupo $Z = \{I, -I\}$, y el cociente Q_8/Z es abeliano por tener orden 4. Como el único subgrupo menor que Z es el trivial, que no da un grupo abeliano al pasar al cociente, el Teorema 9.1.4 nos dice que $G' = Z = \{I, -I\}$.

Obsérvese que, en este caso, el subgrupo derivado coincide con el centro; ¿es esto cierto en general?

9.2 La serie derivada; grupos resolubles

Consideremos el último ejemplo: Q_8 no es abeliano, pero sí lo es su derivado Q_8'. De este modo, Q_8 se "descompone" mediante un subgrupo normal abeliano Q_8' y el cociente correspondiente Q_8/Q_8', que también es abeliano (Teorema 9.1.4). En este sentido podríamos decir que, aunque Q_8 no es abeliano (su derivado no es trivial), está próximo a serlo: el derivado de su derivado es trivial.

Análogamente, podríamos considerar grupos para los que el derivado del derivado de su derivado es trivial, etc. Todos estos grupos se pueden considerar como pertenecientes a una clase amplia de grupos "parecidos a los abelianos"; el grado de parecido vendría dado por el número de veces que hace falta calcular el derivado para llegar a obtener el subgrupo trivial.

Sistematizamos estas observaciones a continuación. Recordemos que $N \trianglelefteq G$ (ó $G \trianglerighteq N$) significa que N es un subgrupo normal de G, mientras que $N \triangleleft G$ (ó $G \triangleright N$) significa que N es un subgrupo normal y propio de G.

Definición 9.2.1 *Sea G un grupo. Se define por recurrencia el* t-ésimo derivado *del grupo G, denotado $G^{(t)}$ (donde $t \in \mathbb{Z}^+$) del modo siguiente:*

- $G^{(1)} = G'$, *el derivado de G.*
- $G^{(t+1)} = G^{(t)\prime}$, *el derivado de $G^{(t)}$.*

La cadena de subgrupos

$$G \trianglerighteq G' \trianglerighteq G^{(2)} \trianglerighteq \cdots$$

se conoce como la serie derivada *de G, y se dice que G es* resoluble *si su serie derivada alcanza al grupo trivial; es decir, si existe $t \geq 1$ tal que $G^{(t)} = \{1\}$.*

Es evidente que todo grupo abeliano es resoluble, y el comentario que abrió la sección muestra que el grupo Q_8, no abeliano, es resoluble con serie derivada $Q_8 \rhd \{1, -1\} \rhd \{1\}$. El siguiente ejemplo muestra nuevos grupos resolubles, y también otros que no lo son. Usaremos el hecho obvio de que, en cuanto un término se repite en la serie derivada, ésta *se estabiliza* en ese término; es decir, si $G^{(t)} = G^{(t+1)}$ entonces $G^{(t)} = G^{(t+k)}$ para cualquier $k \geq 1$.

Ejemplos 9.2.2 *Resolubilidad de los grupos simétricos*[1].

1. Hemos visto que $S_n' = A_n$. Cuando $n = 3$ tenemos $S_3' = A_3$, que es abeliano. Por tanto S_3 es resoluble con serie derivada $S_3 \rhd A_3 \rhd \{1\}$.

2. Por el Ejemplo 6.2.8, el único subgrupo normal, propio y no trivial de A_4 es

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

   Como A_4 no es abeliano y A_4/V sí lo es (tiene orden 3), del Teorema 9.1.4 se deduce que $V = A_4' = S_4^{(2)}$. Y como V es abeliano, deducimos que $S_4^{(3)}$ es trivial. En consecuencia, S_4 es resoluble con serie derivada $S_4 \rhd A_4 \rhd V \rhd \{1\}$.

3. Si $n \geq 5$ entonces A_n es simple (Teorema de Abel, 6.2.12) y no abeliano, luego $A_n' = A_n$ por el Teorema 9.1.4. Es decir, la serie derivada de S_n se estabiliza en A_n y nunca alcanza al grupo trivial. En consecuencia, S_n no es resoluble cuando $n \geq 5$.

Vamos a estudiar las propiedades básicas de los grupos resolubles, y comenzamos con un lema.

Lema 9.2.3 *Sea $f : G \to H$ un homomorfismo de grupos. Entonces:*

1. *$f(G') \subseteq H'$; más generalmente, $f(G^{(t)}) \subseteq H^{(t)}$ para cada $t \geq 1$.*
2. *Si f es suprayectiva entonces $f(G') = H'$; más generalmente, $f(G^{(t)}) = H^{(t)}$ para cada $t \geq 1$.*

Demostración. 1. Como $f([a,b]) = [f(a), f(b)]$ para cualesquiera $a, b \in G$, se tiene $f(G') \subseteq H'$. El caso general lo vemos por inducción en t, con el caso $t = 1$ resuelto por lo anterior. Si el resultado vale para cierto entero positivo t entonces f se restringe a un homomorfismo $f : G^{(t)} \to H^{(t)}$, y aplicando a éste el caso inicial deducimos que $G^{(t+1)} \subseteq H^{(t+1)}$, lo que completa la demostración.

2. Supongamos ahora que f es suprayectiva, y sea $[u, v]$ un conmutador en H. Tomando $a, b \in G$ con $f(a) = u$ y $f(b) = v$ se tiene $f([a,b]) = [u, v]$, lo que prueba que $[u, v] \in f(G')$; es decir, $H' \subseteq f(G')$, y el apartado anterior nos da la igualdad. El caso general se demuestra por inducción como antes. □

[1] Es bien conocida la fórmula $(-b \pm \sqrt{b^2 - 4ac})/2a$ para obtener las soluciones de la *ecuación general de segundo grado* $aX^2 + bX + c = 0$. Cuando es posible expresar las soluciones de una ecuación polinómica usando sólo sus coeficientes y las operaciones de suma, resta, producto, división y extracción de raíces, se dice que la ecuación es *resoluble por radicales*.

Un profundo resultado, que se demostrará en la asignatura de Tercer Curso *Ecuaciones Algebraicas*, afirma que la *ecuación general de grado n* (es decir, la ecuación con coeficientes arbitrarios $a_nX^n + \cdots + a_1X + a_0 = 0$) es resoluble por radicales si y sólo si el grupo simétrico S_n es resoluble. Por tanto, los Ejemplos 9.2.2 implican que esto sólo es posible para las ecuaciones lineales, cuadráticas, cúbicas y cuárticas.

También es posible asignar un grupo G_f a cada polinomio particular f (en lugar de considerar polinomios con coeficientes indeterminados) de tal manera que la ecuación $f(X) = 0$ es resoluble por radicales si y sólo si el grupo G_f es resoluble (de ahí el nombre de estos grupos). El grupo G_f es un subgrupo del grupo de permutaciones de las raíces de f en algún cuerpo. De hecho, el origen de la Teoría de Grupos está, en buena medida, en el uso de estos grupos de permutaciones para el estudio de la resolubilidad por radicales de las ecuaciones polinómicas.

Proposición 9.2.4 *Sea G un grupo con un subgrupo H y un subgrupo normal N. Se verifican:*

1. *Si G es resoluble entonces H es resoluble (los subgrupos de resolubles son resolubles).*
2. *Si G es resoluble entonces G/N es resoluble (los cocientes de resolubles son resolubles).*
3. *Si N y G/N son resolubles entonces G es resoluble.*

Demostración. 1. Aplicando el Lema 9.2.3 a la inclusión $H \hookrightarrow G$, tenemos $H^{(t)} \subseteq G^{(t)}$ para cada $t \geq 1$. Si G es resoluble entonces existe un t tal que $G^{(t)} = \{1\}$ y por tanto $H^{(t)} = \{1\}$, por lo que H es resoluble.

2. El Lema 9.2.3 aplicado a la proyección canónica $p : G \to G/N$ nos dice que $p(G^{(t)}) = (G/N)^{(t)}$ para cada $t \geq 1$. Si G es resoluble entonces existe un t tal que $G^{(t)}$ es trivial, y por tanto $(G/N)^{(t)} = p(G^{(t)}) = p(\{1\})$ también es trivial, por lo que G/N es resoluble.

3. Por hipótesis existe $t \geq 1$ tal que $(G/N)^{(t)} = \{1\}$. Aplicando como antes el Lema 9.2.3 deducimos que $p(G^{(t)})$ es trivial, lo que significa que $G^{(t)} \subseteq \operatorname{Ker} p = N$. Por el apartado 1, $G^{(t)}$ es resoluble; es decir, existe $s \geq 1$ tal que $(G^{(t)})^{(s)} = \{1\}$. Como es claro que $(G^{(t)})^{(s)} = G^{(t+s)}$, deducimos que G es resoluble. □

Esto nos permite encontrar otros ejemplos de grupos resolubles:

Proposición 9.2.5 *Todo p-grupo finito G es resoluble.*

Demostración. Por hipótesis se tiene $|G| = p^n$ para cierto $n \geq 1$; demostraremos el resultado por inducción sobre n, con el caso $n = 1$ evidente. En el caso general G tiene un subgrupo N de orden p^{n-1} (Corolario 8.3.4) que es normal en G (Proposición 5.9.10 o Ejercicio 8.2.6). Como G/N es resoluble (de hecho, abeliano) por tener orden primo y N lo es por la hipótesis de inducción, la Proposición 9.2.4 nos dice que G es resoluble. □

La serie derivada de un grupo resoluble sugiere la siguiente definición más general:

Definición 9.2.6 *Sea G un grupo arbitrario. Una* serie normal *de G es una cadena de subgrupos de G de la forma*

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{n-1} \trianglerighteq G_n = \{1\}$$

(es decir, es una cadena descendente finita que empieza en G y termina en $\{1\}$ y en la que cada subgrupo es normal en el anterior). Los grupos G_i se llaman términos *de la serie, el número n es la* longitud *de la serie, y cada grupo cociente G_{i-1}/G_i (para $i = 0, 1, \ldots, n$) se llama un* factor *de la serie.*

Obsérvese que la longitud n mide el número de factores, y no el de términos (que es $n + 1$).

Podemos considerar una serie normal de G como una "descomposición" del grupo G: En efecto, G podría obtenerse "componiendo" de algún modo los grupos G_1 y G/G_1. A su vez, G_1 es "compuesto" de G_2 y G_1/G_2, de modo que G está compuesto a partir de los tres grupos G_2, G_1/G_2 y G/G_1. En general, dada una serie normal como la definición, G está compuesto por los factores de la serie

$$\frac{G}{G_1} = \frac{G_0}{G_1}, \quad \frac{G_1}{G_2}, \quad \frac{G_2}{G_3}, \ldots, \frac{G_{n-2}}{G_{n-1}}, \quad \frac{G_{n-1}}{G_n} = \frac{G_{n-1}}{\{1\}} = G_{n-1}.$$

En particular, si G es resoluble, su serie derivada nos dice que G se puede considerar compuesto a partir de grupos abelianos. El siguiente teorema nos dice que, recíprocamente, todo grupo compuesto a partir de grupos abelianos es resoluble.

Teorema 9.2.7 *Un grupo G es resoluble si y sólo si existe una serie normal de G con todos sus factores abelianos.*

Demostración. Si G es resoluble entonces su serie derivada es una serie normal con factores abelianos, lo que nos da el "sólo si". Recíprocamente, supongamos que G tiene una serie normal como la de la Definición 9.2.6 con todos los factores abelianos, y veamos que G es resoluble por inducción en la longitud n de la serie. Si $n = 1$ entonces G es el único factor de la serie, por lo que es abeliano y en consecuencia resoluble. En el caso general, la hipótesis de inducción aplicada a G_1 nos dice que éste es resoluble (tiene una serie de longitud $n - 1$ con factores abelianos), y como G/G_1 también es resoluble (de hecho es abeliano, por ser un factor de la serie inicial), la Proposición 9.2.4 nos dice que G es resoluble, como queríamos ver. □

9.3 Series de composición; grupos de longitud finita

Supongamos dada una serie normal cualquiera de un grupo G:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{n-1} \trianglerighteq G_n = \{1\} \tag{9.3.1}$$

Desde luego, siempre es posible introducir nuevos términos en esa serie: entre G_i y G_{i+1} podemos intercalar un subgrupo $G_i \trianglerighteq H \trianglerighteq G_{i+1}$ tomando, por ejemplo, $H = G_i$ ó $H = G_{i+1}$. Aparte de este modo trivial de alargar la serie, puede haber otros. Por ejemplo, en la serie $D_4 \triangleright \langle r^2 \rangle \triangleright \{1\}$ podemos introducir otro término de modo no trivial:

$$D_4 \triangleright \langle r \rangle \triangleright \langle r^2 \rangle \triangleright \{1\}.$$

Así, muchas series normales pueden ser "refinadas" como en el caso que acabamos de ver. Introducimos la definición que precisa esta idea.

Definición 9.3.1 *Un* refinamiento *de la serie normal (9.3.1) de un grupo G es otra serie normal de G que incluye a todos los términos de (9.3.1). Si el refinamiento aporta nuevos términos, decimos que es un* refinamiento propio.

Es decir, un refinamiento de (9.3.1) se obtiene intercalando en cada "salto" $G_i \trianglerighteq G_{i+1}$ de la serie original un cierto número finito $r \geq 0$ de subgrupos K_i en la forma

$$G_i \trianglerighteq K_1 \trianglerighteq K_2 \trianglerighteq \cdots \trianglerighteq K_r \trianglerighteq G_{i+1}.$$

En la definición de serie normal no se excluye la posibilidad de que dos términos consecutivos sean iguales, pero es claro que esas repeticiones no aportan nada al conocimiento de G. Por tanto, son especialmente interesantes las series en las que todos los contenidos son estrictos. Por ejemplo, si G es un grupo simple entonces la única serie así que podemos dar en G es $G \triangleright \{1\}$; en otras palabras, esta serie no admite refinamientos propios.

Más generalmente, usando el Teorema de la Correspondencia (5.6.5), es fácil ver que un factor G_i/G_{i-1} de una serie normal es un grupo simple si y sólo si no se pueden intercalar términos entre G_i y G_{i-1} de forma no trivial. Este es el contenido del siguiente ejercicio:

Ejercicio 9.3.2 *Sea G un grupo con subgrupos N y H tales que $N \trianglelefteq H$. Demostrar que el grupo cociente H/N es simple si y sólo si $N \neq H$ (es decir, $N \lhd H$) y los únicos subgrupos K de G que verifican $N \trianglelefteq K \trianglelefteq H$ son $K = N$ y $K = H$.*

Por tanto, si una serie (9.3.1) con contenidos estrictos no admite refinamientos propios, es porque cada uno de los factores G_i/G_{i+1} es un grupo simple. Esta es una buena situación, pues nos da una "descomposición" de G a partir de grupos simples. Destacamos este tipo de series normales mediante una definición.

Definición 9.3.3 *Una* serie de composición *de G es una serie normal con contenidos estrictos*

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{n-1} \triangleright G_n = \{1\}$$

en la que todos los factores G_i/G_{i+1} (para $i = 0, 1, ..., n-1$) son grupos simples, lo que equivale a que la serie no admita refinamientos propios.

Si G posee una serie de composición decimos que G es de longitud finita*, y llamamos* longitud de composición *de G, denotada por $\ell(G)$, al mínimo de las longitudes de sus series de composición.*

Ejemplos 9.3.4 *Series de composición.*

1. Si G es el grupo trivial, entonces $G = G_0 = \{1\}$ es una serie normal con un sólo término, y por tanto sin inclusiones ni factores. Por tanto, el grupo trivial tiene una serie de composición y su longitud de composición es 0.

2. Es claro que todo grupo simple admite una única serie de composición; más aún, los grupos simples son exactamente aquéllos cuya longitud de composición es 1.

3. El grupo aditivo de los enteros no es de longitud finita: Si tuviese una serie de composición, digamos $\mathbb{Z} = G_0 \rhd G_1 \rhd \cdots \rhd G_{t-1} \rhd G_t = \{0\}$, entonces G_{t-1} sería un subgrupo simple de $\mathbb{Z}$, así que basta ver que no existe tal cosa. En efecto, por el Teorema 1.2.11, los subgrupos de $\mathbb{Z}$ son el trivial (que no es simple) y los de la forma $n\mathbb{Z}$ con $n \geq 1$, que no son simples pues tienen por ejemplo a $2n\mathbb{Z}$ como subgrupo (normal) propio y no trivial.

4. Sean $p_1, p_2, \ldots, p_n$ enteros positivos (no necesariamente primos ni distintos) y sea $n = p_1 p_2 \cdots p_n$. Consideraremos el grupo $G = \mathbb{Z}_n$ y abusaremos de la notación identificando cada entero con su clase módulo $n\mathbb{Z}$. Tenemos entonces una serie normal

$$\mathbb{Z}_n = \langle 1 \rangle \rhd \langle p_1 \rangle \rhd \langle p_1 p_2 \rangle \rhd \cdots \rhd \langle p_1 p_2 \cdots p_{n-1} \rangle \rhd \langle p_1 p_2 \cdots p_n \rangle = \{0\}$$

(la normalidad es obvia, pues el grupo es abeliano) cuyos cocientes son $\mathbb{Z}_{p_1}, \mathbb{Z}_{p_2}, \ldots, \mathbb{Z}_{p_n}$ por el Corolario 5.8.9. Por tanto, si $n = p_1 p_2 \cdots p_n$ es una factorización de n en producto de primos positivos, la anterior es una serie de composición de $\mathbb{Z}_n$. Obsérvese que, como en la factorización de n se puede alterar el orden de los p_i, podemos obtener otras series de composición en las que los factores simples que aparecen son los mismos pero en orden distinto.

5. Del apartado 4 deducimos que $\mathbb{Z}_4$ tiene una serie de composición de longitud 2 cuyos dos factores son isomorfos a $\mathbb{Z}_2$. Como $\mathbb{Z}_4$ no es simple, esto implica que $\ell(\mathbb{Z}_4) = 2$.

   Exactamente lo mismo le pasa al grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ (¡compruébalo!), lo que nos dice que dos grupos no isomorfos pueden tener series de composición con la misma longitud y los mismos factores. En otras palabras, las series de composición de un grupo G no determinan a G, ni siquiera salvo isomorfismos.

6. Si p es un entero positivo primo y r es la rotación de ángulo $2\pi/p$ en el grupo diédrico D_p, entonces $D_p \rhd \langle r \rangle \rhd \{1\}$ es serie de composición de D_p. En efecto, $\langle r \rangle$ es normal en D_p por tener índice 2, y los factores $D_p/\langle r \rangle$ y $\langle r \rangle$ son simples por tener orden primo. Como D_p no es simple, se tiene $\ell(D_p) = 2$. ¿Puedes encontrar un grupo abeliano que tenga una serie con los mismos factores?

   Combinando este argumento con el del apartado 4, es fácil ver que, si el entero n es producto de k primos, entonces D_n tiene una serie de composición de longitud $k + 1$.

7. La serie derivada de S_4 es $S_4 \rhd A_4 \rhd V \rhd \{1\}$, donde $V = \{1,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$. Ésta no es una serie de composición porque V no es simple, pero puede refinarse a la serie de composición

$$S_4 \rhd A_4 \rhd V \rhd \langle (1\ 2)(3\ 4) \rangle \rhd \{1\}.$$

   Cambiando $(1\ 2)(3\ 4)$ por cualquiera de los otros dos elementos no triviales de V se obtienen otras formas de refinar la serie normal dada a una serie de composición, pero es claro que las tres series de composición que se obtienen son *esencialmente iguales*.

8. Para $n \geq 5$, la serie $S_n \rhd A_n \rhd \{1\}$ es de composición, por lo que $\ell(S_n) = 2$.

9. El grupo de los cuaterniones Q_8 tiene subgrupos de orden 4 (por ejemplo, $N = \langle \mathbf{i} \rangle = \{I, \mathbf{i}, -I, -\mathbf{i}\}$) y de orden 2 ($\langle -I \rangle$), y es claro que $Q_8 \rhd N \rhd Z \rhd \{I\}$ es una serie de composición.

   Más generalmente, si G es un grupo de orden p^n, con p primo, entonces G tiene una serie de composición de longitud n con factores de orden p (Proposición 8.3.4 y Ejercicio 8.2.6).

Para proseguir con el estudio de las series de composición necesitamos algunas propiedades básicas.

Proposición 9.3.5 *Sea G un grupo con un subgrupo normal N y sea $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$ una serie normal de G. Entonces*

$$N = G_0 \cap N \trianglerighteq G_1 \cap N \trianglerighteq \cdots \trianglerighteq G_n \cap N = \{1\}$$

es una serie normal de N.

Si la serie de G es de composición entonces, eliminando en la de N los términos repetidos, se obtiene una serie de composición de N.

Demostración. Sean H y K dos subgrupos de G tales que $H \lhd K$. Como $K \cap N$ es otro subgrupo de K, el Tercer Teorema de Isomorfía (5.7.9) nos dice que la intersección $H \cap (K \cap N)$ (que, obviamente, coincide con $H \cap N$) es un subgrupo normal de $K \cap N$. Es decir,

$$H \cap N \trianglelefteq K \cap N,$$

lo que claramente implica la primera parte del enunciado. El Tercer Teorema de Isomorfía nos da además un isomorfismo

$$\frac{K \cap N}{H \cap N} \cong \frac{H(K \cap N)}{H},$$

y el mismo teorema aplicado a G, N y K nos dice que $K \cap N \trianglelefteq K$, por lo que $H(K \cap N) \trianglelefteq K$ (Ejercicio 5.7.5) y así

$$\frac{H(K \cap N)}{H} \trianglelefteq \frac{K}{H}$$

(Teorema 5.6.5). Si el cociente K/H es simple, esta última condición implica que $H(K \cap N)/H$ es trivial o simple, y en consecuencia lo mismo le pasa a $(K \cap N)/(H \cap N)$. La demostración de la segunda parte del enunciado a partir de este hecho es ahora evidente. □

Ejemplo 9.3.6 *Intersecando series normales con subgrupos.*
Sea $D_8 = \langle r, s \mid r^8 = s^2 = 1, srs = r^{-1} \rangle$ el grupo diédrico. Entonces $\langle r^2, s \rangle = D_4$. Una serie de composición de D_8 es $D_8 \rhd \langle r \rangle \rhd \langle r^2 \rangle \rhd \langle r^4 \rangle \rhd \{1\}$. Intersecando con D_4 obtenemos la siguiente serie de composición de D_4, que tiene un término menos que la anterior porque, al intersecar con D_4, los términos segundo y tercero de la serie de D_8 se transforman en el mismo:

$$D_4 \rhd \langle r \rangle \cap D_4 = \langle r^2 \rangle \cap D_4 \rhd \langle r^4 \rangle \rhd \{1\}.$$

Proposición 9.3.7 *Sea G un grupo con un subgrupo normal N y sea $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$ una serie normal G. Entonces*

$$\frac{G}{N} = \frac{G_0 N}{N} \trianglerighteq \frac{G_1 N}{N} \trianglerighteq \cdots \trianglerighteq \frac{G_n N}{N} = \{1\}$$

es una serie normal de G/N.

Si la serie de G es de composición entonces, eliminando en la de G/N los términos repetidos, se obtiene una serie de composición de G/N.

Demostración. Sean, como antes, $H \trianglelefteq K$ dos subgrupos de G. Como N es normal en G, los conjuntos HN y KN son subgrupos de G, y obviamente el primero está contenido en el segundo. Afirmamos que, de hecho, $HN \trianglelefteq KN$: En efecto, dados $k \in K$ y $n \in N$, se tiene

$$\begin{aligned} knHN &= kHNn \quad (\text{pues } n \in N \subseteq HN) \\ &= HkNn \quad (\text{pues } H \trianglelefteq K) \\ &= HNkn \quad (\text{pues } N \trianglelefteq G). \end{aligned}$$

El Teorema de la Correspondencia nos dice además que $HN/N \trianglelefteq KN/N$, de donde se sigue fácilmente la primera afirmación.

El Tercer Teorema de Isomorfía aplicado a $HN \trianglelefteq KN$ y a $K \leq KN$ nos dice que $K \cap HN \trianglelefteq K$ y

$$\frac{K}{K \cap HN} \cong \frac{KHN}{HN} = \frac{KN}{HN}.$$

Además, el cociente $K/(K \cap HN)$ es a su vez un cociente de K/H pues, por el Segundo Teorema de Isomorfía,

$$\frac{K}{K \cap HN} \cong \frac{K/H}{(K \cap HN)/H}.$$

Por tanto, si K/H es simple entonces el cociente $K/(K \cap HN)$ es o bien trivial o bien simple, y ahora la segunda parte del enunciado es clara. □

Ejemplo 9.3.8 *Transportando series normales a cocientes.*

Sea $G = \langle g \rangle$ un grupo cíclico de orden 12, y consideremos la serie de composición $G = \langle g \rangle \rhd \langle g^3 \rangle \rhd \langle g^6 \rangle \rhd \langle g^{12} \rangle = \{1\}$. Aplicando la Proposición 9.3.7 con el subgrupo normal $\langle g^4 \rangle$ obtenemos la siguiente serie de composición de $G/\langle g^4 \rangle \cong \mathbb{Z}_4$:

$$G = \langle g, g^4 \rangle / \langle g^4 \rangle = \langle g^3, g^4 \rangle / \langle g^4 \rangle \rhd \langle g^6, g^4 \rangle / \langle g^4 \rangle \rhd \langle g^{12}, g^4 \rangle / \langle g^4 \rangle = \{1\}$$

(nótese que $\langle g, g^4 \rangle = \langle g^3, g^4 \rangle = \langle g \rangle$, que $\langle g^6, g^4 \rangle = \langle g^2 \rangle$ y que $\langle g^{12}, g^4 \rangle = \langle g^4 \rangle$).

Proposición 9.3.9 *Sea G un grupo con un subgrupo normal N, y sean*

$$\frac{G}{N} = \frac{G_0}{N} \rhd \frac{G_1}{N} \rhd \cdots \rhd \frac{G_n}{N} = \{1\} \qquad y \qquad N = G_n \rhd G_{n+1} \rhd \cdots \rhd G_{n+m} = \{1\}$$

series normales de G/N y N. Entonces

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd G_n \rhd G_{n+1} \rhd \cdots \rhd G_{n+m} = \{1\}$$

es una serie normal de G.

Si las series de G/N y de N son de composición, entonces lo es la de G.

Demostración. Observamos primero que, por el Teorema de la Correspondencia, una serie normal de G/N debe ser de la forma dada, donde cada G_i (con $i = 0, 1, \ldots, n$) es un subgrupo de G que contiene a N. El mismo teorema aplicado a la relación $G_{i+1}/N \trianglelefteq G_i/N$ (con $i = 0, 1, \ldots, n-1$) nos dice que $G_{i+1} \trianglelefteq G_i$, lo cual prueba la primera afirmación. Además, por el Segundo Teorema de Isomorfía,

$$\frac{G_i/N}{G_{i+1}/N} \cong \frac{G_i}{G_{i+1}}$$

para $i = 0, 1, \ldots, n-1$, de modo que los factores de la serie de G que hemos construido son los de las dos series iniciales, y ahora la segunda parte del enunciado es clara. □

Como consecuencia de los tres resultados anteriores se obtiene:

Teorema 9.3.10 *Sea G un grupo con un subgrupo normal N. Entonces G es de longitud finita si y sólo si lo son a la vez N y G/N.*

Corolario 9.3.11 *Todo grupo finito G es de longitud finita*[2]*.*

Demostración. Demostramos el resultado por inducción en el orden del grupo. Si $|G| = 1$ el resultado es obvio. Supongamos pues que $|G| > 1$. Si G es simple, entonces $G \rhd \{1\}$ es una serie de composición. En otro caso G posee un subgrupo N normal, propio y no trivial; por hipótesis de inducción, N y G/N tienen longitud finita, y entonces G también la tiene por el Teorema 9.3.10. □

Una serie normal que no sea de composición se puede refinar. Si es posible refinarla hasta un punto en el que no se pueda refinar más, habremos obtenido una serie de composición. Esto no es siempre posible. Por ejemplo, los siguientes refinamientos sucesivos

$$\mathbb{Z} \rhd \{0\}, \qquad \mathbb{Z} \rhd 2Z \rhd \{0\}, \qquad \mathbb{Z} \rhd 2Z \rhd 4Z \rhd \{0\}, \qquad \mathbb{Z} \rhd 2Z \rhd 4Z \rhd 8Z \rhd \{0\}, \ldots$$

nunca darán una serie de composición de $\mathbb{Z}$. Otra consecuencia importante del Teorema 9.3.10 es que este proceso sí tiene fin cuando trabajamos con un grupo de longitud finita:

[2] Como consecuencia de este resultado, clasificar los grupos finitos se divide en las dos siguientes tareas: Clasificar los grupos simples finitos y determinar las posibles maneras de "componer" grupos simples finitos en series de composición. Sobre la primera tarea, véase la nota al pie en la página 156. Como hemos visto en los Ejemplos 9.3.4, existe más de una forma de componer dos grupos, y es todavía un problema abierto conocer cuáles son las posibles formas de componer los grupos simples finitos.

Corolario 9.3.12 *Sea G un grupo de longitud finita. Entonces cualquier serie normal de G puede refinarse a una serie de composición.*

Demostración. Sea $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = \{1\}$ una serie normal de G. Por el Teorema 9.3.10, cada G_i/G_{i+1} tiene una serie de composición

$$\frac{G_i}{G_{i+1}} = \frac{G_{i,0}}{G_{i+1}} \rhd \frac{G_{i,1}}{G_{i+1}} \rhd \cdots \rhd \frac{G_{i,k_i}}{G_{i+1}} \rhd \{1\}$$

(obsérvese que hemos escrito los subíndices de forma que $G_{i,k_i} \neq G_{i+1}$; viendo cómo sigue la demostración, el lector puede analizar la ventaja de esta notación). "Pegando" estas series como en la Proposición 9.3.9, obtenemos la serie

$$\begin{aligned} G \;=\; & G_{00} \rhd G_{01} \rhd \cdots \rhd G_{0k_0} \rhd \\ & G_{10} \rhd G_{11} \rhd \cdots \rhd G_{1k_1} \rhd \\ & \cdots \\ & G_{m0} \rhd G_{m1} \rhd \cdots \rhd G_{mk_m} \rhd \{1\}, \end{aligned}$$

que es un serie de composición de G. □

Corolario 9.3.13 *Un grupo resoluble G es de longitud finita si y sólo si es finito. En este caso G tiene una serie de composición con todos sus factores de orden primo.*

Demostración. Una implicación es consecuencia directa del Corolario 9.3.11. Recíprocamente, supongamos que G es resoluble y de longitud finita. Por el Corolario 9.3.12, su serie derivada se refina a una serie de composición $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$ cuyos factores han de ser abelianos (¿por qué?). Por el Ejercicio 6.2.10, cada uno de esos factores G_{i-1}/G_i (para $i = 1, \ldots, n$) debe tener orden primo p_i, y en particular debe ser finito. Aplicando reiteradamente el Teorema de Lagrange, deducimos que G es finito de orden $p_1 \cdots p_n$. □

Ejemplos 9.3.14 *Series de composición de grupos abelianos y resolubles.*

1. Sea G un grupo abeliano finito con descomposición invariante $G = \langle x \rangle \oplus \langle y \rangle \oplus \langle z \rangle$, donde $o(x) = 12$, $o(y) = 6$, $o(z) = 3$. Entonces

   $$\{0\} \lhd \langle x^6 \rangle \lhd \langle x^2 \rangle \lhd \langle x \rangle \lhd \langle x \rangle \oplus \langle y^3 \rangle \lhd \langle x \rangle \oplus \langle y \rangle \lhd \langle x \rangle \oplus \langle y \rangle \oplus \langle z \rangle = G$$

   es una serie de composición de G. ¿Puedes dar otras series de composición de G usando la misma idea?

2. En los Ejemplos 9.3.4 vimos cómo la serie derivada de S_4 se refinaba a una de composición.

3. Sea $D_8 = \langle r, s \mid r^8 = s^2 = 1, srs = r^{-1} \rangle$ el grupo diédrico. El subgrupo $\langle r^2 \rangle$ es normal, pues $(r^2)^s = r^{-2} \in \langle r \rangle$, y el cociente $D_8/\langle r^2 \rangle$ es abeliano por tener orden 4. Como el cociente $D_8/\langle r^4 \rangle$ no es abeliano (¿por qué?, ¿a qué grupo de los de orden 8 es isomorfo?), deducimos que $D_8 \rhd \langle r^2 \rangle \rhd \{1\}$ es la serie derivada de D_8. Un refinamiento a una serie de composición es

   $$D_8 \rhd \langle r \rangle \rhd \langle r^2 \rangle \rhd \langle r^4 \rangle \rhd \{1\}.$$

Los ejemplos del inicio de esta sección sugieren que puede haber una cierta condición de unicidad sobre las series de composición de un grupo de longitud finita G, especialmente en cuanto al tipo de isomorfía de los grupos simples que aparecen como factores, y desde luego no en cuanto al orden en el que éstos aparecen. El resultado fundamental en este sentido es el Teorema de Jordan-Hölder, que asegura que esa sospecha es cierta. Comencemos definiendo con precisión el concepto de "igualdad salvo el orden" para dos series de composición de un grupo de longitud finita.

Definición 9.3.15 *Si un grupo G tiene series de composición, dos de ellas se dicen* equivalentes *si tienen la misma longitud y, salvo el orden y salvo isomorfismos, los mismos factores. Explícitamente, dos series de composición*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\} \qquad y \qquad G = H_0 \rhd H_1 \rhd \cdots \rhd H_m = \{1\}$$

son equivalentes si $n = m$ y existe una permutación $\sigma \in S_n$ tal que, para cada $i = 0, 1, \ldots, n-1$, existe un isomorfismo

$$\frac{G_i}{G_{i+1}} \cong \frac{H_{\sigma(i)}}{H_{\sigma(i)+1}}.$$

Ejercicio 9.3.16 *Demostrar que la relación recién definida es una relación de equivalencia en el conjunto de todas las series de composición de un grupo de longitud finita.*

Teorema 9.3.17 (Jordan-Hölder) *Si un grupo G tiene longitud finita, entonces todas sus series de composición son equivalentes.*

Demostración. Sea $n = \ell(G)$. Demostraremos el teorema por inducción en n, con el caso $n = 1$ resuelto porque entonces G es simple y $G \rhd \{1\}$ es su única serie de composición.

En el caso general, es claro que la hipótesis de inducción puede enunciarse del modo siguiente: "Si un grupo tiene una serie de composición de longitud menor que n, entonces todas las series de composición de ese grupo son equivalentes". Fijemos una serie de composición de G

$$G = G_0 \rhd G_1 \rhd \ G_2 \rhd \cdots \rhd G_n = \{1\} \tag{9.3.2}$$

de longitud mínima n. Por la transitividad de la relación, el teorema quedará demostrado si vemos que cualquier otra serie de composición de G, digamos

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_m = \{1\}, \tag{9.3.3}$$

es equivalente a la serie (9.3.2). Observemos que

$$G_1 \rhd \ G_2 \rhd \cdots \rhd G_n = \{1\} \tag{9.3.4}$$

$$H_1 \rhd H_2 \rhd \cdots \rhd H_m = \{1\} \tag{9.3.5}$$

son series de composición de G_1 y de H_1, y que la primera de ellas nos permite aplicar la hipótesis de inducción a G_1.

Consideremos primero el caso en el que $G_1 = H_1$. Entonces (9.3.4) y (9.3.5) son dos series de composición de G_1, y por la hipótesis de inducción ambas son equivalentes, de modo que $n - 1 = m - 1$ y así $n = m$. Además, los factores de ambas son los mismos (salvo quizás el orden), y añadiendo el factor $G/G_1 = G/H_1$ vemos que lo son los de las series (9.3.2) y (9.3.3), que por tanto son equivalentes, como queríamos ver.

Supongamos a partir de ahora que $G_1 \neq H_1$, y observemos que esto implica que ninguno de estos grupos contiene al otro: por ejemplo, si fuese $G_1 \subset H_1$, entonces H_1/G_1 sería un subgrupo normal, propio y no trivial del grupo simple G/G_1, lo cual es imposible.

Como G_1 y H_1 son normales en G, también lo es su producto G_1H_1, que contiene estrictamente a G_1 pues lo contrario implicaría que $H_1 \subset G_1$. En consecuencia G_1H_1/G_1 es un subgrupo normal no trivial del grupo simple G/G_1, de donde se sigue que $G_1H_1 = G$.

Sea ahora $K_2 = G_1 \cap H_1$. Éste es un subgrupo normal tanto de G_1 como de H_1, y podemos identificar los correspondientes cocientes:

$$\frac{G_1}{K_2} = \frac{G_1}{G_1 \cap H_1} \cong \frac{G_1H_1}{H_1} = \frac{G}{H_1} \qquad \text{y} \qquad \frac{H_1}{K_2} = \frac{H_1}{G_1 \cap H_1} \cong \frac{G_1H_1}{G_1} = \frac{G}{G_1}.$$

Por la Proposición 9.3.5, K_2 tiene una serie de composición, digamos

$$K_2 \rhd K_3 \rhd \cdots\cdots \rhd K_l = \{1\}. \tag{9.3.6}$$

Como G_1/K_2 y H_1/K_2 son simples, las siguientes son series de composición de G_1 y de H_1:

$$G_1 \rhd K_2 \rhd K_3 \rhd \cdots\cdots \rhd K_l = \{1\}. \tag{9.3.7}$$

$$H_1 \rhd K_2 \rhd K_3 \rhd \cdots\cdots \rhd K_l = \{1\}. \tag{9.3.8}$$

Ahora, la hipótesis de inducción aplicada a G_1 nos dice que las series (9.3.4) y (9.3.7) son equivalentes, y por tanto $n = l$. En consecuencia, la serie (9.3.8) tiene longitud $n-1$ y podemos aplicar la hipótesis de inducción a H_1, por lo que las series (9.3.8) y (9.3.5) son equivalentes; en particular $n-1 = m-1$ y así $n = m$. Por último, las series iniciales (9.3.2) y (9.3.3) son equivalentes pues los siguientes conjuntos van siendo iguales cada uno al siguiente (las justificaciones de todas las igualdades o bien son claras o bien están en los párrafos anteriores; identifícalas):

- Factores de (9.3.2).
- G/G_1 y los factores de (9.3.4).
- G/G_1 y los factores de (9.3.7).
- G/G_1, G_1/K_2 y los factores de (9.3.6).
- G/H_1, H_1/K_2 y los factores de (9.3.6).
- G/H_1 y los factores de (9.3.8).
- G/H_1 y los factores de (9.3.5).
- Factores de (9.3.3).

□

Si el grupo G tiene longitud finita, los grupos simples que aparecen como factores de una (cualquiera) de sus series de composición, con las repeticiones pertinentes, se llaman *factores de composición* de G.

Los dos corolarios que siguen son consecuencias inmediatas del Teorema de Jordan-Hölder (en el segundo hay que usar además la Proposición 9.3.9):

Corolario 9.3.18 *Si un grupo G tiene longitud finita, entonces todas sus series de composición tienen la misma longitud $\ell(G)$.*

Ejercicio 9.3.19 *Sea G un grupo finito y resoluble de orden $p_1 \cdots p_k$, con los p_i primos tal vez repetidos. Demostrar que $\ell(G) = k$.*

Corolario 9.3.20 *Si un grupo G tiene longitud finita y N es un subgrupo normal, propio y no trivial de G, entonces*

$$\ell(G) = \ell(N) + \ell(G/N), \qquad \ell(N) < \ell(G) \quad y \quad \ell(G/N) < \ell(G).$$

Aplicando el Corolario 9.3.12 se obtiene.

Corolario 9.3.21 *Si G es un grupo de longitud finita, cualquier serie normal de G con factores no triviales (es decir, con inclusiones propias) tiene longitud $\leq \ell(G)$.*

9.4 Problemas

1. Sea $f : G \to H$ un isomorfismo de grupos. Demostrar que:
   (a) Si G' es el subgrupo derivado de G entonces $f(G')$ es el subgrupo derivado de H.
   (b) G es resoluble si sólo si lo es H.
   (c) G es de longitud finita si sólo si lo es H. En este caso, $\ell(G) = \ell(H)$.

2. Decidir sobre la verdad o falsedad de las siguientes igualdades para elementos a, b, c de un grupo:

   (a) $[a,[b,c]] = [[a,b],c]$.

   (b) $[a,bc] = [a,c][a,b]^c$.

   (c) $[a,b]^c = [a,b][[a,b],c]$.

3. Demostrar que el subgrupo derivado de un grupo G es un subgrupo característico de G. Deducir que todos los términos de la serie derivada de G son característicos, y por tanto normales, en G.

4. Probar que si G es resoluble y no trivial entonces $G' \neq G$.

5. Probar que si G es simple y resoluble entonces G es cíclico de orden primo.

6. Dado un grupo cíclico $G = \langle g \rangle$ de orden 72, consideremos la serie de composición

$$G = \langle g \rangle \rhd \langle g^2 \rangle \rhd \langle g^6 \rangle \rhd \langle g^{12} \rangle \rhd \langle g^{36} \rangle \rhd \langle g^{72} \rangle = \{1\}.$$

   Calcular la serie de composición de $G/\langle g^{18} \rangle \cong \mathbb{Z}_{18}$ que se obtiene al aplicar la Proposición 9.3.7 con el subgrupo normal $\langle g^{18} \rangle$.

7. Formar todas las series de composición del grupo cíclico de 20 elementos.

8. Dar una serie de composición del grupo de 21 elementos construido en el Problema 23 del Capítulo 8.

9. Probar que, si H y K son dos subgrupos normales de G, entonces $[H,K] = \langle [h,k] : h \in H, k \in K \rangle$ es un subgrupo normal de G que está contenido en $H \cap K$.

10. Demostrar que todo grupo de orden menor que 60 es resoluble.

11. Sea $n \geq 5$ un entero. Encontrar $\sigma, \tau \in A_n$ tales que $[\sigma, \tau] = (1,2,3)$, y usar esto para demostrar que A_n no es resoluble sin utilizar el Teorema de Abel.

12. Probar que si p, q, r son primos distintos tales que $pq < r$ entonces todo grupo finito de orden pqr es resoluble.

13. Probar que todo grupo de orden 56, 63 ó 440 es resoluble.

14. Si G es un grupo resoluble finito cuyo orden se factoriza como

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

    demostrar que la longitud de composición de G es $\ell(G) = \alpha_1 + \alpha_2 + \cdots + \alpha_r$ y que sus factores de composición son los $\mathbb{Z}_{p_i}$, cada uno repetido α_i veces.

15. Sea G un grupo de orden 2925.

    (a) Probar que G tiene al menos dos subgrupos normales.

    (b) Mostrar que G es resoluble.

    (c) Calcular su longitud de composición.

16. Demostrar:

    (a) Todo grupo de orden 45 es abeliano.

    (b) Todo grupo de orden 765 es resoluble.

    (c) Sea G un grupo de orden 765. Construir una serie de composición para G.

17. Sea G un grupo finito con un subgrupo normal N de índice 351 tal que N tiene una serie de composición de longitud 6. Encontrar la longitud de la composición de G.

18. Demostrar que $G \times H$ es resoluble precisamente si G y H lo son.

19. [*] Demostrar que para cada $n \in \mathbb{N}$ existe un grupo resoluble G tal que $G^{(n)} \neq \{1\}$. Utilizar esto para mostrar que el producto directo infinito de grupos resolubles puede no ser resoluble. (Indicación: En la primera parte, usar el isomorfismo $S_3 \cong \mathrm{Aut}(S_3)$).

20. Dar un ejemplo de un grupo resoluble que no sea de longitud finita, y otro de un grupo de longitud finita que no sea resoluble.

21. Dar una serie de composición para cada uno de los grupos de orden ≤ 15.

22. Calcular la serie derivada de cada uno de los grupos de orden ≤ 15.

23. Demostrar que si H es un subgrupo normal de un grupo G de longitud finita, entonces G tiene una serie de composición en la que aparece H.

24. Probar que si un grupo G es resoluble y $G/Z(G)$ es simple entonces G es abeliano.

25. Dado un grupo G de orden $3^3 \cdot 13$, probar que es resoluble y dar una serie de composición.

26. Si G es un grupo de longitud finita y H es un subgrupo de G, ¿es cierto que $\ell(H) \leq \ell(G)$?

27. Demostrar que, si G es un grupo con series de composición y N es un subgrupo normal de G tal que $\ell(N) = \ell(G)$, entonces se tiene $N = G$.

28. Probar que el grupo G del Problema 17 del Capítulo 8 es resoluble y calcular una serie de composición.

29. Encontrar una serie de composición del grupo $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ de orden 12.

30. Escribir la serie derivada de los grupos diédricos D_n y del grupo de cuaterniones.

31. Probar que si G es un grupo no abeliano de orden p^3 (con p primo), entonces $G' = Z(G)$ y $G/G' \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

32. ¿Es cierta la siguiente afirmación? Si todos los subgrupos propios de un grupo G tienen longitud finita, entonces G tiene longitud finita.

33. Demostrar que un grupo finito abeliano tiene una única serie de composición si y sólo si es un p-grupo cíclico, para algún primo p. ¿Es cierto esto si el grupo no es abeliano?

34. Sean H y K dos subgrupos normales de un grupo G. Demostrar que si G/H y G/K son resolubles, entonces $G/H \cap K$ es resoluble.

35. Demostrar que todo grupo de orden p^2q con p y q primos es resoluble.

36. [*] Demostrar que si G es un grupo no resoluble de orden $n < 300$, entonces $n = 60, 120, 168, 180$ ó 240.

37. [*] Sea G un grupo. Para cada $n \in \mathbb{N}$ definimos el *n-ésimo centro* $Z_n(G)$ de G por recurrencia de la siguiente forma: $Z_0(G) = \{1\}$. Supongamos que hemos definido $Z_n(G)$ que resulta ser un subgrupo normal de G. Entonces $Z_{n+1}(G)$ es el único subgrupo (normal) de G que verifica

$$Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G)).$$

En particular, $Z_1(G)$ es el centro de G. La cadena de subgrupos

$$\{1\} = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

se conoce como la *serie central (ascendente)* de G. Se dice que G es *nilpotente* si $Z_n(G) = G$ para algún n; es decir, si la serie central alcanza al grupo G en algún paso. Demostrar:

(a) Todo grupo abeliano es nilpotente.

(b) $Z_n(G) = \{x \in G : [x, y] \in Z_{n-1}(G) \text{ para todo } y \in G\}$.

(c) Todo p-grupo finito (p primo) es nilpotente.

(d) Un grupo G es nilpotente precisamente si tiene una serie normal

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

tal que $G_i/G_{i-1} \subseteq Z(G/G_{i-i})$ para todo $i = 1, 2, \ldots, n$.

(e) Todo grupo nilpotente es resoluble.

(f) Dar un ejemplo de un grupo resoluble que no sea nilpotente.

(g) Si G es nilpotente y H es un subgrupo de G, entonces H es nilpotente.

(h) Si G es nilpotente y N es un subgrupo normal de G, entonces G/N es nilpotente.

(i) Dar un ejemplo de un grupo G con un subgrupo normal N tales que N y G/N sean nilpotentes y G no lo sea.

(j) Demostrar que si G y H son dos grupos nilpotentes, entonces $G \times H$ es un grupo nilpotente.

Bibliografía del capítulo

Allenby [1], Cohn [10], Delgado-Fuertes-Xambó [11], Rotman [30].

Capítulo 10

Formas canónicas de matrices

Se estudia un endomorfismo f de un espacio vectorial V de dimensión finita sobre un cuerpo K. Usando el anillo de polinomios $K[X]$ como principal herramienta, se obtienen diversas representaciones matriciales cómodas de f y se asigna a f una lista de invariantes (polinomios de $K[X]$) que lo determinan salvo semejanza.

Introducción

Muchos problemas, puramente matemáticos o planteados por otras ciencias, llevan a la consideración de un endomorfismo f de un espacio vectorial V de dimensión finita n sobre un cuerpo K. Por Álgebra Lineal sabemos que, para cada base de V, hay una matriz $n \times n$ sobre K que representa a f. En general, hay bases que "se adaptan mejor" a f que otras, lo que se traduce en que las correspondientes matrices son más sencillas, lo que suele dar información sobre el endomorfismo. Por tanto, es importante disponer de métodos para encontrar esas bases adecuadas y esas matrices sencillas, y éste es el principal objetivo del capítulo. En el camino, asociaremos a f unos invariantes que determinarán su clase de semejanza, por lo que tendremos una clasificación de los endomorfismos de V análoga a la clasificación de los grupos abelianos finitamente generados.

En la primera mitad del capítulo nos enfrentamos principalmente a los aspectos teóricos del problema. El camino, salvando las complicaciones técnicas, es muy similar al que seguimos al clasificar grupos abelianos finitamente generados; de hecho, bastará con pensar en grupos abelianos finitos, pues en la analogía que desarrollaremos la "parte libre" será trivial.

Tras recordar algunos resultados de Álgebra Lineal, en particular los conceptos de endomorfismos y matrices semejantes, estudiamos los subespacios de V en los que la restricción de f induce un endomorfismo, llamados subespacios invariantes. Es sencillo ver que V es suma directa de subespacios invariantes indescomponibles, de modo que se plantea el problema de dar una descripción precisa de éstos. Para ello, definimos un producto de polinomios de $K[X]$ por vectores de V, que se comporta en gran medida como el producto de enteros por elementos de un grupo abeliano. Las nociones de orden de un elemento, periodo de un grupo y subgrupo cíclico tienen sus análogos en este contexto: polinomio anulador de un vector ($\mathrm{Anu}_f(v)$), polinomio mínimo del endomorfismo ($\min(f)$) y subespacio cíclico ($K[f]v$), respectivamente. Esta analogía nos permite adaptar los argumentos del Capítulo 7 para demostrar que los subespacios invariantes indescomponibles son precisamente los del tipo $K[f]v$, donde $\mathrm{Anu}_f(v)$ es una potencia de un polinomio irreducible de $K[X]$. Además, en una descomposición de V como suma directa de subespacios invariantes indescomponibles, $V = K[f]v_1 \oplus \cdots \oplus K[f]v_k$, la lista de los anuladores $\mathrm{Anu}_f(v_i)$ determina unívocamente la clase de semejanza de f.

Una descomposición $V = K[f]v_1 \oplus \cdots \oplus K[f]v_k$ como la anterior nos permite formar matrices de f a partir de matrices de sus restricciones a los $K[f]v_i$, y cada una de éstas adopta formas sencillas para bases adecuadas de $K[f]v_i$. Por tanto, el problema de encontrar matrices sencillas (y las correspondientes bases) para f se reduce a saber encontrar esas descomposiciones de V y a elegir bases adecuadas en cada $K[f]v$. A esto dedicamos casi todo el resto del capítulo.

Hay varios modos típicos de construir bases adecuadas para $K[f]v_i$ (siempre a partir de v_i y de $\mathrm{Anu}_f(V_i)$), y según cuál usemos se obtiene una de las llamadas "formas canónicas" de f. Comenzamos describiendo la forma canónica primaria, y la usamos para demostrar el Teorema de Cayley-Hamilton, que nos da un modo práctico para calcular $\min(f)$. Después, describimos las formas canónicas de Jordan y damos algoritmos para su cálculo. Hay una forma canónica "generalizada" que posee cualquier endomorfismo y otra "clásica", más sencilla, pero que sólo poseen los endomorfismos para los que $\min(f)$ se descompone en factores lineales. En particular, todo endomorfismo de un espacio vectorial complejo tiene una forma canónica de Jordan, y la estrecha relación entre $\mathbb{C}$ y $\mathbb{R}$ permite asignar a cada endomorfismo de un espacio vectorial real un nuevo tipo de forma canónica.

El capítulo termina mostrando cómo las formas canónicas de Jordan pueden usarse para calcular potencias de matrices (lo que permite describir el término general de ciertas sucesiones recurrentes) y para encontrar "descomposiciones aditivas" de matrices que son de gran utilidad en el estudio de las ecuaciones diferenciales.

Objetivos del capítulo

- Conocer la noción de subespacio invariante, y entender por qué las descomposiciones en suma directa de subespacios invariantes son útiles para encontrar matrices sencillas de un endomorfismo.
- Conocer los conceptos de polinomio mínimo y característico (de un endomorfismo) y anulador (de un vector), las relaciones entre ellos y métodos para calcularlos.
- Comprender por qué la clase de semejanza de un endomorfismo queda determinada por sus formas canónicas o por sus divisores elementales.
- Saber calcular las distintas formas canónicas de una matriz: primaria, de Jordan generalizada, de Jordan (si existe) y real de Jordan (para endomorfismos de espacios vectoriales reales).
- Saber calcular, a partir de las formas canónicas de Jordan, las potencias de una matriz y la descomposición aditiva de un endomorfismo de un espacio vectorial real o complejo.

Desarrollo de los contenidos

10.1 Representaciones matriciales de endomorfismos

En todo este capítulo, K será un cuerpo y V será un espacio vectorial sobre K, no nulo y de dimensión finita n. Denotaremos por $\mathbf{E} = \mathrm{End}_K(V)$ el conjunto de los *endomorfismos* de V (aplicaciones K-lineales $V \to V$), y por $M_n(K)$ al conjunto de las matrices cuadradas de tamaño n con entradas en K. Usaremos resultados típicos de Álgebra Lineal que serán citados o enunciados sin demostración.

Para cada base ordenada $B = \{v_1, \ldots, v_n\}$ de V hay una biyección

$$\begin{array}{ccc} \mathbf{E} & \to & M_n(K) \\ f & \mapsto & f_B \end{array}$$

que asocia cada endomorfismo $f \in \mathbf{E}$, con la matriz f_B asociada a f en la base B; es decir, la j-ésima columna de f_B está formada por las coordenadas en la base B del vector $f(v_j)$. Diremos que f *está representado* por la matriz f_B o que f_B es la *matriz del endomorfismo* f en la base B. El isomorfismo inverso lleva una matriz $A = (a_{ij})$ al único endomorfismo $f \in \mathbf{E}$ que, sobre cada elemento v_j de la base B, actúa de la forma siguiente:

$$f : v_j \ \mapsto \ \sum_{i=1}^{n} a_{ij} v_i.$$

Obsérvese que el orden en el que se escriban los elementos de la base influye en la representación de una matriz en esa base. Por tanto, consideraremos las bases como conjuntos ordenados, de forma que dos bases formadas por los mismos elementos ordenados de diferente forma se consideran diferentes.

Fijado un endomorfismo $f \in \mathbf{E}$, sus representaciones en distintas bases serán, por lo general, distintas. Algunas de estas matrices pueden ser más sencillas que otras (por ejemplo, porque tengan muchos

ceros), y nuestro objetivo en este capítulo es encontrar una base B de forma que la matriz f_B sea lo más sencilla posible, y ofrezca por tanto una buena información visual de f. Veamos algunos ejemplos:

Ejemplos 10.1.1 *Representaciones sencillas de endomorfismos.*

1. Sea f la homotecia de razón $\alpha \in K$ (es decir, $f(v) = \alpha v$ para cada $v \in V$). Entonces, para cualquier base B, la matriz f_B es la matriz escalar correspondiente a α (con α en cada entrada de la diagonal y ceros en el resto). En este caso, no hay ningún problema que resolver, pues todas las representaciones matriciales de f son iguales.

2. Si V es el plano real $\mathbb{R}^2$, f es la rotación de ángulo $\pi/2$ (antihorario) y B es la base canónica, entonces
$$f_B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$
De hecho, se obtiene la misma matriz para cualquier base formada por dos vectores ortogonales de la misma longitud y ordenados adecuadamente. Podemos decir que estas bases "se ajustan bien" a f, y en general otras bases dan lugar a representaciones más complicadas.

3. Sea $V = K^2$ y sea $f(x, y) = (4y - 7x, 7y - 12x)$. Si B es la base canónica y B' es la base $\{v_1 = (1, 2),\ v_2 = (2, 3)\}$, entonces
$$f_B = \begin{pmatrix} -7 & 4 \\ -12 & 7 \end{pmatrix} \qquad \text{y} \qquad f_{B'} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$
Ahora B' es "mejor base" para f que la base canónica B, y $f_{B'}$ nos permite describir a f como la reflexión sobre la recta $\langle v_1 \rangle$ en la dirección de la recta $\langle v_2 \rangle$.

Además de encontrar bases que nos den representaciones adecuadas de f, deseamos que las matrices sencillas que buscamos sean únicas en cierto sentido, de forma que podamos clasificar los endomorfismos de V a partir de esas matrices (que llamaremos *formas canónicas*).

Pero todavía no hemos dicho qué entendemos por una matriz sencilla. Nuestro modelo inicial de matriz sencilla es una *matriz diagonal*; es decir, una matriz con ceros en las entradas que no están en la diagonal. Obsérvese, por ejemplo, que es muy fácil calcular las potencias de una matriz diagonal, o el producto de una matriz diagonal por una matriz arbitraria. Un vector $v \in V$ es un *vector propio* de f si existe un escalar $\lambda \in K$ (llamado *valor propio* de f asociado al vector propio v) tal que $f(v) = \lambda v$. Es claro que f_B es diagonal si y sólo si cada vector de B es un vector propio de f, de donde se deduce, por ejemplo, que la rotación de los Ejemplos 10.1.1 no puede ser representada por una matriz diagonal (no es *diagonalizable*). Es decir, no todos los endomorfismos pueden representarse por una matriz diagonal, así que tendremos que ampliar (y por lo tanto complicar) nuestro concepto de matriz sencilla.

Existen varias posibilidades para elegir estos modelos de matrices sencillas, y en consecuencia existen distintos tipos de formas canónicas, como veremos. En el desarrollo de la teoría será fundamental el anillo de polinomios $K[X]$ y sus propiedades de divisibilidad, que en algunos aspectos dependen del cuerpo K. Por ejemplo, el caso en el que K es algebraicamente cerrado es especialmente bueno. Dedicaremos una sección especial al caso $K = \mathbb{R}$, que es el de mayor interés en numerosas aplicaciones de la teoría.

El resto de esta primera sección lo dedicaremos a establecer con precisión la relación entre $\mathbf{E}$ y $M_n(K)$. Como ya hemos comentado, muchos de estos resultados son bien conocidos en Álgebra Lineal y nos limitaremos a citarlos.

En $\mathbf{E} = \mathrm{End}_K(V)$ podemos considerar tres operaciones (las dos primeras son internas y en la tercera intervienen elementos de K, a los que llamaremos *escalares*): Dados $f, g \in \mathbf{E}$ y $\alpha \in K$, se definen los elementos $f + g$, fg y αf de $\mathbf{E}$ mediante su acción en elementos $v \in V$ por las fórmulas:

$$\begin{array}{rcll} (f+g)(v) & = & f(v) + g(v) & \text{(suma)} \\ (fg)(v) & = & f(g(v)) & \text{(producto o composición)} \\ (\alpha f)(v) & = & \alpha f(v) & \text{(producto por escalares)} \end{array}$$

La suma y el producto (composición) dotan a $\mathbf{E}$ de una estructura de anillo (no conmutativo salvo que V tenga dimensión 1), mientras que la suma y el producto por escalares lo dotan de una estructura

de K-espacio vectorial. Dado un escalar $\alpha \in K$, representaremos por la misma letra a la *homotecia de razón* α, o sea al elemento de $\mathbf{E}$ dado por $\alpha(v) = \alpha v$ para cada $v \in V$. Esta notación no induce a error, pues el producto αf (con $f \in \mathbf{E}$) no depende de si vemos a α como escalar o como endomorfismo (homotecia). Además, es claro que las homotecias conmutan con los endomorfismos (es decir, $\alpha f = f\alpha$) y que la aplicación $K \to \mathbf{E}$ dada por $\alpha \mapsto \alpha$ es un homomorfismo inyectivo de anillos, por lo que podemos ver a K como un subanillo de $\mathbf{E}$.

Con la notación usual de potencias, si $f \in \mathbf{E}$ entonces f^n (con $n \geq 1$) denotará la composición de f consigo mismo n veces. Es decir, si $v \in V$ entonces $f^2(v) = f(f(v))$, y en general $f^n(v) = f(f^{n-1}(v))$.

Algo similar ocurre en $M_n(K)$ con las operaciones usuales de suma y producto de matrices, y de producto de un escalar por una matriz. De nuevo $M_n(K)$ es un anillo (no conmutativo si $n > 1$) y un K-espacio vectorial. Además, si a cada $\alpha \in K$ se le asigna la *matriz escalar* $\alpha = \alpha I_n$ (con α en cada entrada de la diagonal y ceros en el resto), se tiene un homomorfismo inyectivo de anillos $K \to M_n(K)$ tal que $\alpha A = A\alpha$ para cada $A \in M_n(K)$, independientemente de que lo veamos como producto de matrices o como producto de matriz por escalar.

Para cada base B de V, la aplicación $\mathbf{E} \to M_n(K)$ descrita anteriormente es un isomorfismo de anillos (de hecho, la forma de definir el producto de matrices está pensada para que estas aplicaciones conserven el producto) y un isomorfismo de espacios vectoriales (lo que implica que $\dim_K(\mathbf{E}) = n^2$).

En vista de los objetivos que nos hemos marcado, es esencial describir cómo se relacionan, para dos bases distintas B y B' de V, las matrices f_B y $f_{B'}$. Para ello, denotaremos por $C_{B',B}$ a la matriz del cambio de base de B a B'; es decir, en la j-ésima columna de $C_{B',B}$ aparecen las coordenadas en B' del j-ésimo vector de B. Esta matriz es invertible y su inversa es la matriz del cambio de base de B a B'; es decir, $C_{B',B}^{-1} = C_{B,B'}$. La relación que buscamos es la siguiente (para cualquier $f \in \mathbf{E}$):

$$f_{B'} = C_{B',B} f_B C_{B,B'} = C_{B,B'}^{-1} f_B C_{B,B'}.$$

En particular, si A y A' son dos matrices que representan al mismo endomorfismo, entonces existe una matriz invertible Q tal que $A' = Q^{-1}AQ$.

Dos *endomorfismos* se dice que son *semejantes* si son representables por la misma matriz. Es decir $f, f' \in \mathbf{E}$ son semejantes si y sólo si existen bases B y B' de V tales que $f_B = f'_{B'}$. Dos *matrices* se dice que son *semejantes* si representan el mismo endomorfismo; es decir, $A, A' \in M_n(K)$ son semejantes si existen $f \in \mathbf{E}$ y bases B y B' tales que $f_B = A$ y $f_{B'} = A'$. Claramente dos matrices A y A' son semejantes precisamente si son conjugadas; es decir, si existe una matriz invertible U tal que $A' = U^{-1}AU$. Es fácil ver que las relaciones de semejanza son relaciones de equivalencia en $\mathbf{E}$ y $M_n(K)$. Las correspondientes clases de equivalencia se llaman *clases de semejanza* y la clase de semejanza que contiene a x se denotará por $[x]$, tanto si x es un endomorfismo como si es una matriz. Fijada una base B de V, la aplicación

$$[f] \mapsto [f_B]$$

está bien definida y define una correspondencia biunívoca entre los conjuntos de clases de semejanza de endomorfismos y matrices.

Utilizando esto podemos reescribir nuestros objetivos de las siguientes formas equivalentes:

- Dado un endomorfismo f, queremos encontrar una base B tal que la matriz f_B sea sencilla.

- Dada una matriz A, queremos encontrar una matriz semejante a ella que sea sencilla.

Por lo tanto, nuestro problema consiste en encontrar una base adecuada o una matriz invertible adecuada, lo que técnicamente es la misma cosa.

En las secciones que siguen desarrollaremos la teoría para un endomorfismo f. A menudo se quiere trabajar directamente con una matriz $A \in M_n(K)$, y en este caso no hay más que considerar A como un endomorfismo del modo que sigue: Se toma $V = K^n$ (vectores columna $n \times 1$) y se considera el endomorfismo $A\cdot$ que lleva un vector v al producto Av (que vuelve a ser un vector columna $n \times 1$). De este modo se tiene $A = (A\cdot)_B$, donde B es la base canónica de $V = K^n$.

10.2 Subespacios invariantes

En general, cuando se estudia un objeto con cierto tipo de estructura (grupo, anillo, espacio vectorial...), es interesante considerar los subconjuntos para los que se conserva esa estructura. Ahora estamos estudiando un endomorfismo f de un espacio vectorial V, de modo que nos interesan los subespacios vectoriales W de V para los que f pueda seguir considerándose un endomorfismo. Para eso, necesitamos que los vectores de W sigan en W después de aplicarles f, y ésa es la idea inicial en las siguientes definiciones.

Definición 10.2.1 *Un subespacio vectorial W de V se dice que es* invariante *por el endomorfismo $f \in \mathbf{E}$ (o que W es f-invariante) si $f(W) \subseteq W$. En este caso, la restricción de f a W es un endomorfismo de W; es decir, $f|_W \in \mathrm{End}_K(W)$.*

Cuando trabajemos directamente con matrices, usaremos la siguiente definición análoga: El subespacio W de K^n es invariante *por la matriz $A \in M_n(K)$ si es invariante por el endomorfismo $A\cdot$.*

Una descomposición por subespacios invariantes *de f es una descomposición de V en suma directa de subespacios invariantes*

$$V = V_1 \oplus \cdots \oplus V_n.$$

En este caso, si f_i es la restricción de f a V_i (de modo que $f_i \in \mathrm{End}_K(V_i)$), escribimos

$$f = f_1 \oplus \cdots \oplus f_n$$

y decimos que f es la suma directa *de $f_1, \ldots, f_n$.*

Ejercicio 10.2.2 *Sean V un espacio vectorial, W un subespacio, f un endomorfismo de V y $\{w_1, \ldots, w_m\}$ un sistema generador de W. Demostrar que W es f-invariante si y sólo si $f(w_i) \in W$ para cada $i = 1, \ldots, m$.*

Ejercicio 10.2.3 *Demostrar que los siguientes subespacios de V son invariantes por f:*

1. *$\langle v, f(v), f^2(v), \ldots \rangle$, donde v es cualquier vector de V. En particular, si v es un vector propio de f, entonces $\langle v \rangle$ es una recta invariante.*
2. *$\mathrm{Ker}\, g$, donde g es cualquier endomorfismo de V que conmuta con f, es decir, tal que $fg = gf$.*

A menudo nos encontraremos con sumas directas del tipo $f = f_1 \oplus \cdots \oplus f_n$. Entonces, salvo que se diga lo contrario, V_i representará el dominio de f_i; es decir, f_i es la restricción de f al subespacio V_i de V, que entendemos que es invariante por f. En tal caso, si B_i es una base de V_i para cada i, entonces $B = B_1 \cup \cdots \cup B_n$ es una base de V. Consideramos el orden en B de forma que los elementos de B_i van delante de los de B_{i+1} y el orden dentro de cada B_i se mantiene. La representación matricial de f en la base B adquiere entonces la siguiente forma:

$$f_B = \begin{pmatrix} f_{1B_1} & & & \\ & f_{2B_2} & & \\ & & \ddots & \\ & & & f_{nB_n} \end{pmatrix}$$

donde se entiende que las cajas vacías están formadas por ceros. Cuanto menores sean las dimensiones de los V_i, más cerca estará la matriz f_B de ser diagonal. El caso extremo ocurre cuando todos los V_i tienen dimensión 1, en cuyo caso f_B es diagonal (y por tanto f es diagonalizable), pero ya hemos observado que no siempre es posible conseguir esto. En general, nuestro objetivo es obtener una descomposición de f lo "más fina" posible, lo que nos lleva a considerar los endomorfismo que "no se pueden refinar":

Definición 10.2.4 *Diremos que f es* indescomponible *si V no admite una descomposición por subespacios invariantes de f formada por dos subespacios vectoriales no nulos.*

Una descomposición indescomponible *o* primaria *de f es una descomposición $f = f_1 \oplus \cdots \oplus f_n$ en la que cada f_i es indescomponible.*

Ejercicio 10.2.5 *Demostrar que la rotación de ángulo $\pi/2$ en el plano real es un endomorfismo indescomponible.*

Obsérvese que esta aplicación viene dada por $f(x,y) = (-y,x)$. Comprobar que, si consideramos dicha aplicación en $\mathbb{C}^2$, entonces f es descomponible.

Ejemplos 10.2.6 *Descomposiciones indescomponibles.*

1. Sea $V = K^3$ y sea f el endomorfismo dado por

$$f(x,y,z) = (-x-2y-2z,\ x+y,\ z).$$

Entonces $u = (0,-1,1)$ verifica $f(u) = u$. En consecuencia, $V_1 = \langle u\rangle$ es un subespacio f-invariante de V con base $B_1 = \{u\}$, la restricción $f_1 = f\mid_{V_1}$ es la identidad, y su matriz 1×1 en B_1 es (1).

Por su parte, los vectores $v = (1,0,0)$ y $w = (-1,1,0)$ verifican $f(v) = w$ y $f(w) = -v$. Así, $W = \langle v,w\rangle$ es un subespacio f-invariante con base $B_2' = \{v,w\}$, y es fácil ver que $g = f\mid_W$ es indescomponible si $K = \mathbb{R}$ y no lo es si $K = \mathbb{C}$ (g está en la situación del Ejercicio 10.2.5). Como además $V = V_1 \oplus W$, tenemos la descomposición indescomponible $f = f_1 \oplus g$ para el endomorfismo f si $K = \mathbb{R}$. La matriz asociada a f en la base $B' = B_1 \cup B' = \{u,v,w\}$ es

$$f_{B'} = \left(\begin{array}{c|cc} 1 & & \\ \hline & 0 & -1 \\ & 1 & 0 \end{array}\right).$$

Supongamos ahora que $K = \mathbb{C}$. Si ponemos $v_1 = u$, $v_2 = (1-i,-1,0)$ y $v_3 = (1+i,-1,0)$, entonces $f(v_2) = iv_2$ y $f(v_3) = -iv_3$, y por tanto, $V_2 = \langle v_2\rangle$ y $V_3 = \langle v_3\rangle$ son subespacios f-invariantes. Si f_i es la restricción de f a V_i $(i = 1,2,3)$, entonces $f = f_1 \oplus f_2 \oplus f_3$ es una descomposición indescomponible de f. La matriz asociada a f en la base $B = \{v_1,v_2,v_3\}$ es

$$f_B = \left(\begin{array}{c|c|c} 1 & & \\ \hline & i & \\ \hline & & -i \end{array}\right).$$

2. Sea $f : K^2 \to K^2$ el homomorfismo dado por $f(x,y) = (x+y,y)$. Vamos a ver que f es indescomponible. Si f fuera descomponible, existiría una base $B = \{v_1,v_2\}$ de K^2 formada por vectores propios; es decir, de forma que $f(v_i) = \lambda_i v_i$ para ciertos $\lambda_1,\lambda_2 \in K$. Eso implicaría que, para $i = 1,2$, el sistema homogéneo de ecuaciones lineales

$$\begin{array}{rcrcl} (1-\lambda_i)x & + & y & = & 0 \\ & + & (1-\lambda_i)y & = & 0 \end{array}$$

tiene solución no trivial y por tanto

$$\left|\begin{array}{cc} 1-\lambda_i & 1 \\ 0 & 1-\lambda_i \end{array}\right| = 0;$$

es decir, $\lambda_1 = \lambda_2 = 1$. De aquí se deduce fácilmente que la segunda coordenada de v_1 y v_2 es cero en contra de que la independencia lineal de v_1 y v_2.

3. Sea f el endomorfismo de K^3 dado por $f(x,y,z) = (x,x+y,x+z)$. Si ponemos $v_1 = (0,0,1)$, $v_2 = (0,1,1)$ y $v_3 = (1,1,1)$, entonces $f(v_1) = v_1$, $f(v_2) = v_2$ y $f(v_3) = v_2 + v_3$. Por tanto $U = \langle v_1\rangle$ y $W = \langle v_2,v_3\rangle$ son subespacios f-invariantes. Obsérvese que la matriz asociada a f en la base $B = \{v_1,v_2,v_3\}$ es

$$f_B = \left(\begin{array}{c|cc} 1 & & \\ \hline & 1 & 1 \\ & 0 & 1 \end{array}\right).$$

¿Es $V = U \oplus W$ una descomposición indescomponible?

La existencia de descomposiciones indescomponibles para cualquier endomorfismo está garantizada por la siguiente proposición.

Proposición 10.2.7 *Todo endomorfismo f de un espacio vectorial de dimensión finita n es suma directa de endomorfismos indescomponibles; es decir, tiene una descomposición indescomponible.*

Demostración. Razonaremos por inducción sobre n. Si $n = 1$ entonces V no tiene subespacios vectoriales propios no nulos, y por tanto f es indescomponible. Supongamos que $n > 1$ y la hipótesis de inducción. Si f es indescomponible no hay nada que demostrar. En caso contrario $f = f_1 \oplus f_2$ para ciertos f_i definidos en subespacios vectoriales propios V_1 y V_2. Por hipótesis de inducción $f_1 = g_1 \oplus \cdots \oplus g_k$ y $f_2 = h_1 \oplus \cdots \oplus h_l$ con los g_i y los h_i indescomponibles, y entonces $f = g_1 \oplus \cdots \oplus g_k \oplus h_1 \oplus \cdots \oplus h_l$ es una descomposición indescomponible de f. □

10.3 Endomorfismos indescomponibles

En este momento nos encontramos en una situación muy similar a la que teníamos después de la Proposición 7.4.4. Observemos el paralelismo entre ellas: La Proposición 7.4.4 (respectivamente, la Proposición 10.2.7) muestra que todo grupo abeliano finitamente generado (respectivamente, todo endomorfismo de un espacio vectorial de dimensión finita) admite una descomposición indescomponible. Lo que hicimos a continuación en el Capítulo 7 fue caracterizar los grupos abelianos finitamente generados indescomponibles. Eso es lo que vamos a hacer ahora para los endomorfismos. Recordaremos sucintamente los pasos dados en el Capítulo 7 para un grupo abeliano A:

1. Descomponiendo $A = t(A) \oplus L$ con L libre de torsión (Corolario 7.3.6), observábamos que si A es indescomponible, entonces es de torsión o libre de torsión (Corolario 7.4.3). El caso libre de torsión se resuelve utilizando el Corolario 7.2.9 y pasamos a suponer que A es de torsión y por tanto finito.

2. Descomponiendo A como suma directa de p-grupos (Proposición 7.4.8) observamos que si A es indescomponible, entonces es un p-grupo (Corolario 7.4.9) y pasamos a suponer que A es un p-grupo.

3. Después de demostrar un lema técnico sobre los elementos de orden máximo (Lema 7.4.11), demostramos que los grupos finitos indescomponibles son los cíclicos de orden p^n con p primo o, equivalentemente, los grupos de periodo p^n con un elemento de orden p^n.

Los pasos que vamos a dar para caracterizar los endomorfismos indescomponibles son los mismos, aunque aparecerán algunos problemas técnicos. Para poder aplicar los métodos del Capítulo 7 a endomorfismos necesitamos versiones de los siguientes conceptos: orden, periodo y torsión. Estos tres conceptos vienen asociados a la multiplicación ng de enteros ($n \in \mathbb{Z}$) por elementos del grupo ($g \in A$). La siguiente tabla es un pequeño diccionario de traducción de conceptos que iremos desarrollando poco a poco.

Grupo abeliano A	Endomorfismo $f : V \to V$
Enteros $\mathbb{Z}$	Polinomios $K[X]$
$ng = g + \overset{(n)}{\cdots} + g$	$P \cdot v = P(f)(v)$
Periodo $p(A)$	Polinomio mínimo $\min(f)$
Orden $o(g)$	Polinomio anulador $\mathrm{Anu}_f(v)$
Grupo cíclico $\langle g \rangle$	Subespacio cíclico $K[f]v$

Paso 1

A partir de ahora f denota un endomorfismo del espacio vectorial de dimensión finita V sobre el cuerpo K. El papel que representaba el anillo de los números enteros $\mathbb{Z}$ va a ser representado ahora por el anillo de polinomios $K[X]$. Para ello definimos, para cada $P = p_0 + p_1 X + \cdots + p_n X^n \in K[X]$ y cada $v \in V$, el producto:

$$P \cdot v = p_0 v + p_1 f(v) + \cdots + p_n f^n(v).$$

Podemos ver esto de otra forma: Como f conmuta con las homotecias, la Observación 4.2.2 nos permite aplicar la Propiedad Universal del Anillo de Polinomios al homomorfismo $K \to \mathbf{E}$ (que lleva $\alpha \in K$ a la homotecia α) y X al elemento $f \in \mathbf{E}$. Obtenemos así un homomorfismo de anillos $S_f : K[X] \to \mathbf{E}$ dado por

$$K[X] \ni P = p_0 + p_1 X + \cdots + p_n X^n \quad \mapsto \quad S_f(P) = P(f) = p_0 + p_1 f + \cdots + p_n f^n \in \mathbf{E}.$$

Entonces

$$P \cdot v = P(f)(v) = p_0 v + p_1 f(v) + \cdots + p_n f^n(v).$$

Utilizando que S_f es un homomorfismo de anillos se pueden hacer los siguientes ejercicios:

Ejercicio 10.3.1 *Comprobar que, para cualesquiera $P, Q \in K[X]$ y $v, w \in V$, se verifica:*

1. $P(f)Q(f) = Q(f)P(f)$.
2. $1 \cdot v = v$.
3. $P \cdot (v + w) = P \cdot v + P \cdot w$.
4. $(P + Q) \cdot v = P \cdot v + Q \cdot v$.
5. $(PQ) \cdot v = P \cdot (Q \cdot v)$ *y por tanto,* $P \cdot (Q \cdot v) = Q \cdot (P \cdot v)$.

Ejercicio 10.3.2 *Demostrar que:*

1. *Si $v \in V$ entonces el conjunto $\{P \cdot v : P \in K[X]\}$ coincide con el subespacio $\langle v, f(v), f^2(v), \ldots \rangle$, que es invariante por f por el Ejercicio 10.2.3. Denotaremos este subespacio por $K[f]v$ y lo llamaremos* subespacio cíclico generado por v.
2. *Si $P \in K[X]$ entonces* Ker $P(f)$ *es un subespacio invariante por f (usar el Ejercicio 10.2.3).*

Recordemos que $K[X]$ es un dominio de ideales principales y que los polinomios mónicos (es decir, con coeficiente principal 1) forman un conjunto de representantes salvo asociados de $K[X] \setminus \{0\}$ (Ejercicio 3.1.7). Por tanto, cada ideal no nulo de $K[X]$ está determinado por el único polinomio mónico que lo genera. Como S_f es un homomorfismo de anillos, Ker S_f es un ideal de $K[X]$. Observemos además que S_f es homomorfismo de espacios vectoriales, que la dimensión de $K[X]$ es infinita (el conjunto $\{1, X, X^2, \ldots\}$ es linealmente independiente) y que la dimensión de $\mathbf{E}$ es finita (y vale n^2). Por tanto S_f no puede ser inyectivo, y en consecuencia Ker S_f es un ideal no nulo de $K[X]$.

Definición 10.3.3 *El* polinomio mínimo *de f, denotado por* $\min(f)$, *es el generador mónico de*

$$\text{Ker } S_f = \{Q \in K[X] : Q(f) = 0\}.$$

Es decir, un polinomio $Q \in K[X]$ verifica $Q(f) = 0$ si y solo si Q es múltiplo de $\min(f)$.

Si A es una matriz cuadrada con coeficientes en K entonces llamamos polinomio mínimo *de A,* $\min(A)$, *al polinomio mínimo del endomorfismo $A\cdot$; es decir,* $\min(A) = \min(A\cdot)$.

Si B es una base de V, $A = f_B$ y $P = p_0 + p_1 X + \cdots + p_n X^n \in K[X]$, entonces la matriz asociada a $P(f)$ en la base B es

$$P(A) = p_0 + p_1 A + \cdots + p_n A^n.$$

Por tanto $P(f) = 0$ precisamente si $P(A) = 0$, de donde se deduce:

Lema 10.3.4 *Si A es la matriz asociada a f en una base, entonces* $\min(f) = \min(A)$. *Por tanto, dos endomorfismos semejantes tienen el mismo polinomio mínimo y dos matrices semejantes tienen el mismo polinomio mínimo.*

Ejemplo 10.3.5 *Cálculo del polinomio mínimo.*
Sea f el endomorfismo de K^3 del apartado 3 de los Ejemplos 10.2.6. Como la matriz asociada a f en cierta base es

$$A = f_B = \left(\begin{array}{c|cc} 1 & & \\ \hline & 1 & 1 \\ & 0 & 1 \end{array}\right)$$

y se ve fácilmente que $(A-I)^2 = 0$, deducimos que $\min(f) = (X-1)^2$.

Si interpretamos la torsión de V como el conjunto de los elementos v de V tales que $P \cdot v = 0$ para algún $0 \neq P \in K[X]$, acabamos de ver que todo elemento de V es de torsión. Por tanto el primero de los pasos que dábamos para grupos abelianos no es necesario para endomorfismos. Además el polinomio mínimo representa el papel del periodo.

Paso 2

Primero necesitamos introducir el concepto correspondiente al de orden. Es fácil comprobar que para cada $v \in V$ el conjunto $\{Q \in K[X] : Q \cdot v = 0\}$ es un ideal de $K[X]$, y es no nulo pues claramente contiene a $\min(f)$.

Definición 10.3.6 *El* polinomio anulador *de $v \in V$ por f, denotado por $\mathrm{Anu}_f(v)$, es el generador mónico de*

$$\{Q \in K[X] : Q \cdot v = 0\}.$$

Es decir, un polinomio $Q \in K[X]$ verifica $Q \cdot v = 0$ si y sólo si Q es múltiplo de $\mathrm{Anu}_f(v)$.
Cuando el polinomio f esté claro por el contexto escribiremos $\mathrm{Anu}(v)$ en lugar de $\mathrm{Anu}_f(v)$.

Los ejercicios y ejemplos que siguen son útiles a la hora de calcular en la práctica los polinomios recién definidos. El primer ejercicio dice cómo se puede obtener $\mathrm{Anu}_f(v)$, y cómo se puede usar $\mathrm{Anu}_f(v)$ para estudiar el subespacio invariante cíclico $K[f]v$. El segundo dice que para obtener $\min(f)$ basta con calcular $\mathrm{Anu}_f(v)$ para los vectores de una base.

Ejercicio 10.3.7 *Dados un polinomio mónico $P = p_0 + p_1X + \cdots + p_{m-1}X^{m-1} + X^m$ (de grado m) y un vector $v \in V$, demostrar que las condiciones siguientes son equivalentes:*

1. *$P = \mathrm{Anu}_f(v)$.*
2. *$P \cdot v = 0$ y $Q \cdot v \neq 0$ para todo polinomio no nulo Q con $\mathrm{gr}(Q) < m$.*
3. *$P \cdot v = 0$ y $K[f]v = \langle v, f(v), f^2(v), \ldots\rangle$ tiene dimensión m.*

Asumiendo ahora que se cumplen esas condiciones equivalentes, demostrar que:

1. *$B = \{v, f(v), f^2(v), \ldots, f^{m-1}(v)\}$ es una base de $K[f]v$.*
2. *P es el polinomio mínimo de la restricción de f al subespacio cíclico $K[f]v$ generado por v.*
3. *La matriz asociada a la restricción de f a $K[f]v$ en la base del apartado 1 es*

$$f_B = C(P) = \begin{pmatrix} 0 & 0 & \ldots & 0 & -p_0 \\ 1 & 0 & \ldots & 0 & -p_1 \\ 0 & 1 & \ldots & 0 & -p_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & -p_{m-1} \end{pmatrix}.$$

Esta matriz $C(P)$ se llama matriz compañera *del polinomio P.*

Ejercicio 10.3.8 *Si $B = \{v_1, \ldots, v_n\}$ es una base de V (más generalmente, si es un sistema generador), demostrar que*

$$\min(f) = \mathrm{mcm}(\mathrm{Anu}_f(v_1), \ldots, \mathrm{Anu}_f(v_n)).$$

Ejemplos 10.3.9 *Cálculo del polinomio mínimo.*

1. Sea $V = K^3$ y sea f el endomorfismo del apartado 1 de los Ejemplos 10.2.6. Recordemos que hay una base $B = \{u, v, w\}$ de V tal que

$$f(u) = u, \qquad f(v) = w, \qquad f(w) = -v.$$

Entonces, es claro que $\mathrm{Anu}_f(u) = X - 1$. Por otra parte, se tiene $f^2(v) = -v$, de modo que el polinomio $P = X^2 + 1$ verifica $P \cdot v = 0$. Además, si $Q = aX + b$ verifica $0 = Q \cdot v = -aw + bv$, entonces $Q = 0$ (por la independencia lineal de v y w), y en consecuencia $P = \mathrm{Anu}_f(v)$. Análogamente $P = \mathrm{Anu}_f(w)$, y del Ejercicio 10.3.8 deducimos que

$$\min(f) = \mathrm{mcm}(\mathrm{Anu}_f(u), \mathrm{Anu}_f(v), \mathrm{Anu}_f(w)) = \mathrm{mcm}(X - 1, X^2 + 1) = (X - 1)(X^2 + 1)$$

(excepto si la característica de K es 2, en cuyo caso el mínimo común múltiplo vale $X^2 + 1$).

2. Sea $V = K^3$ y sea f el endomorfismo cuya matriz en la base canónica $B = \{e_1, e_2, e_3\}$ es

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

Como en el apartado anterior, se comprueba que $\mathrm{Anu}_f(e_2) = X - 1$ y que $\mathrm{Anu}_f(e_1) = \mathrm{Anu}_f(e_3) = X^2 - 2X + 2$, por lo que $\min(f) = (X - 1)(X^2 - 2X + 2)$.

Para cada $P \in K[X]$ irreducible sea

$$t_P(V) = \{v \in V : P^i \cdot v = 0 \text{ para algún } i \geq 0\} = \{v \in V : \mathrm{Anu}_f(v) \text{ es una potencia de } P\}.$$

Claramente, $t_P(V)$ es un subespacio vectorial f-invariante de V. De hecho, esto se puede deducir del Ejercicio 10.3.2 y del siguiente:

Ejercicio 10.3.10 *Demostrar que si $P \in K[X]$ es irreducible, entonces $t_P(V) = \mathrm{Ker}\ P^i(f)$, donde P^i es la mayor potencia de P que divide a $\min(f)$.*

La siguiente proposición es la versión de la Proposición 7.4.8 en el contexto de endomorfismos (compárense las demostraciones).

Proposición 10.3.11 *Si $P_1, P_2, \ldots, P_k$ son los polinomios mónicos irreducibles que dividen a $\min(f)$, entonces*

$$V = t_{P_1}(V) \oplus \cdots \oplus t_{P_k}(V)$$

es una descomposición por subespacios invariantes por f en la que cada sumando es no nulo. Además, existen polinomios $F_1, \ldots, F_k \in K[X]$ tales que cada proyección $\pi_i : V \to t_{P_i}(V)$ viene dada por $\pi_i = F_i(f)$.

Demostración. Sea $\min(f) = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ con cada $\alpha_i \geq 1$, y veamos en primer lugar que se tiene $V = t_{P_1}(V) + \cdots + t_{P_k}(V)$. Para ello ponemos $Q_i = P/P_i^{\alpha_i}$, de modo que los Q_i son coprimos y por tanto existen $R_1, \ldots, R_n \in K[X]$ tales que $1 = Q_1R_1 + \cdots + Q_kR_k$. Así, dado $v \in V$ se tiene

$$v = Q_1R_1 \cdot v + \cdots + Q_kR_k \cdot v, \tag{10.3.1}$$

y cada sumando $Q_iR_i \cdot v$ está en $t_{P_i}(V)$ pues

$$P_i^{\alpha_i} \cdot Q_iR_i \cdot v = P_i^{\alpha_i}Q_iR_i \cdot v = R_i \cdot (P \cdot v) = 0.$$

Probemos ahora que la suma es directa; es decir, que si $\sum_{i=1}^k v_i = 0$ con cada $v_i \in t_{P_i}(V)$, entonces cada $v_i = 0$. Como $Q_i \cdot v_i = 0$ (¿por qué?), $\mathrm{Anu}_f(v_i)$ divide a Q_i. Además, $\mathrm{Anu}_f(v_i)$ es una potencia de P_i y $\mathrm{mcd}(P_i, Q_i) = 1$. Por tanto $\mathrm{Anu}_f(v_i) = 1$ o equivalentemente $v_i = 0$, como queríamos ver.

Obsérvese que la ecuación (10.3.1) muestra que $\pi_i = Q_iR_i(f)$.

Veamos por último que los sumandos $t_{P_i}(V)$ no son nulos. En efecto, como Q_i no es múltiplo de $P = \min(f)$ se tiene $Q_i(f) \neq 0$, por lo que existe $v \in V$ tal que $w = Q_i \cdot v \neq 0$. Ahora es claro que w es un elemento no nulo de $t_{P_i}(V)$. □

Ejemplo 10.3.12 *Cálculo de $t_p(V)$.*

Sea f el endomorfismo de $\mathbb{R}^3$ del apartado 1 de los Ejemplos 10.2.6. Ya vimos en el Ejemplo 10.3.9 que $\min(f) = (X-1)(X^2+1)$, $\mathrm{Anu}(v_1) = X-1$ y $\mathrm{Anu}(v) = \mathrm{Anu}(w) = X^2+1$. Por tanto $\langle v_1\rangle \subseteq t_{X-1}(\mathbb{R}^3)$ y $\langle v, w\rangle \subseteq t_{X^2+1}(\mathbb{R}^3)$ y de hecho de la Proposición 10.3.11 se deduce que se dan ambas igualdades.

Usando la Proposición 10.3.11 obtenemos la siguiente condición necesaria para que un endomorfismo sea indescomponible, que es la versión para endomorfismos del Corolario 7.4.9.

Corolario 10.3.13 *Si f es indescomponible entonces* $\min(f)$ *es potencia de un polinomio irreducible.*

El recíproco del Corolario 10.3.13 no se verifica. En efecto, ya vimos en el apartado 3 de los Ejemplos 10.2.6 un endomorfismo descomponible cuyo polinomio mínimo es una potencia de un irreducible (Ejemplo 10.3.5).

Paso 3

Vamos a terminar la caracterización de los endomorfismos indescomponibles. Recordemos que en el Capítulo 7 demostramos que los grupos abelianos finitos que son indescomponibles son los cíclicos con orden una potencia de un primo. Ya hemos demostrado que si un endomorfismo f de un espacio vectorial V es indescomponible, entonces su polinomio anulador es una potencia de un polinomio irreducible. También hemos dado una definición de subespacio cíclico (Ejercicio 10.3.2): Un subespacio de V se dice que es cíclico (con respecto a f) si es de la forma $K[f]v$ para algún $v \in V$. El resultado que vamos a demostrar no puede parecerse más al caso de grupos abelianos finitos:

Proposición 10.3.14 *Un endomorfismo f de un espacio vectorial de dimensión finita V es indescomponible precisamente si* $\min(f)$ *es una potencia de un irreducible y V es cíclico (con respecto a f).*

Antes de demostrar la Proposición 10.3.14 necesitamos el siguiente resultado.

Ejercicio 10.3.15 *Sea f un endomorfismo de V tal que* $\min(f) = P$ *es irreducible en $K[X]$. Consideremos el cuerpo $F = K[X]/(P)$. Denotamos por $\overline{Q}$ la clase $Q + (P)$ de $Q \in K[X]$ en F. Demostrar:*

1. *La operación $\overline{Q}v = Q \cdot v$. dota a V de una estructura de espacio vectorial sobre F.*
2. *Un K-subespacio vectorial de V es un F-subespacio precisamente si es f-invariante.*
3. *Para cada subespacio f-invariante W de V existe otro subespacio f-invariante W' tal que $V = W \oplus W'$.*
4. *f es indescomponible precisamente si* $\dim_F(V) = 1$.

Demostración de la Proposición 10.3.14. Supongamos primero que V es cíclico, pongamos $V = K[f]v$, y que $\min(f) = P^n$ con $P \in K[X]$ irreducible. Si f no es indescomponible, entonces existe una descomposición $V = V_1 \oplus V_2$ en subespacios f-invariantes no triviales. Sea $v = v_1 + v_2$, con $v_i \in V_i$. Como V_i es invariante, $K[f]v_i \subseteq V_i$ y por tanto la dimensión de $K[f]v_i$ es estrictamente menor que la dimensión de V. Por el Ejercicio 10.3.7 el grado de $\mathrm{Anu}_f(v_i)$ coincide con la dimensión de $K[f]v_i$ y el grado de $\mathrm{Anu}_f(v) = P^n$ coincide con la dimensión de $V = K[f]v$. Por tanto, $\mathrm{Anu}_f(v_i) = P^{m_i}$, con $m_i < n$, de donde se deduce que $P^m \cdot v = 0$, con $m = \max\{m_1, m_2\} < n$, de donde se deriva una contradicción. En consecuencia, f es indescomponible.

Supongamos ahora que f es indescomponible. Por la Proposición 10.3.11, el polinomio mínimo $\min(f)$ es una potencia de un irreducible, pongamos $\min(f) = P^n$. Razonamos por inducción sobre n. Si $n = 1$ y $v \in V$ no es cero, entonces del Ejercicio 10.3.15 se deduce que $V = K[f]v$. Supongamos ahora que $n > 1$ y que se verifica la hipótesis de inducción y pongamos $W = P \cdot V = \{P \cdot v : v \in V\}$. Claramente W es un subespacio f-invariante no nulo. Por la Proposición 10.2.7, la restricción g de f a W tiene una descomposición indescomponible y, como $\min(g) = P^{n-1}$, por hipótesis de inducción los subespacios que aparecen en esta descomposición indescomponible son cíclicos. Es decir, existen

$w_1, \ldots, w_k \in W$ tal que $W = K[f]w_1 \oplus \cdots \oplus K[f]w_k (= K[g]w_1 \oplus \cdots \oplus K[g]w_k)$. Para cada $i = 1, \ldots, k$ sea $v_i \in V$ tal que $w_i = P \cdot v_i$ y sea

$$V' = K[f]v_1 + \cdots + K[f]v_k.$$

Vamos a ver que la suma anterior es directa. Si $Q_1 \cdot v_1 + \cdots + Q_k \cdot v_k = 0$, entonces

$$Q_1 \cdot w_1 + \cdots + Q_k \cdot w_k = P \cdot (Q_1 \cdot v_1 + \cdots + Q_k \cdot v_k) = 0$$

y, por tanto, $Q_i w_i = 0$. Eso implica que $\mathrm{Anu}_f(w_i) \mid Q_i$ y como $\mathrm{Anu}_f(w_i)$ es una potencia de P, se deduce que P divide a Q_i. Si ponemos $Q_i = PR_i$, entonces

$$0 = \sum_{i=1}^{n} Q_i \cdot v_i = \sum_{i=1}^{n} R_i \cdot w_i$$

y por tanto $R_i w_i = 0$, de donde deducimos que $Q_i \cdot v_i = R_i P \cdot v_i = R \cdot w_i = 0$. Además $P \cdot V' = P \cdot V$ y, por tanto, $V = V' + \mathrm{Ker}\ P(f)$. La restricción h de f a $\mathrm{Ker}\ P(f)$ satisface las condiciones del Ejercicio 10.3.15. Como $V' \cap \mathrm{Ker}\ P(f)$ es un subespacio h-invariante de $\mathrm{Ker}\ P(f)$, existe un subespacio h-invariante (o sea, f-invariante) K de $\mathrm{Ker}\ P(f)$ tal que $\mathrm{Ker}\ P(f) = (V' \cap \mathrm{Ker}\ P(f)) \oplus K$. Entonces

$$V = V' + \mathrm{Ker}\ P(f) = V' + (V' \cap \mathrm{Ker}\ P(f)) + K = V' + K$$

y

$$V' \cap K = V' \cap \mathrm{Ker}\ P(f) \cap K = 0,$$

de donde obtenemos la siguiente descomposición en suma directa de subespacios f-invariantes:

$$V = V' \oplus K = K[f]v_1 \oplus \cdots \oplus K[f]v_k \oplus K.$$

Como f es indescomponible $K = 0$ y $k = 1$ y el resultado está probado. □

Algunas consecuencias

Algunos de los resultados de los pasos anteriores tienen consecuencias interesantes aparte de la caracterización de los endomorfismos indescomponibles. El resto de esta sección lo dedicamos a ver algunas de ellas.

Corolario 10.3.16 *Un endomorfismo f de un espacio vectorial es diagonalizable precisamente si su polinomio mínimo es de la forma $(X - \alpha_1) \cdots (X - \alpha_k)$ con los α_i distintos dos a dos.*

Demostración. Supongamos que f es diagonalizable y sea $v_1, \ldots, v_n$ una base de vectores propios con valores propios $\lambda_1, \ldots, \lambda_n$. Entonces $\mathrm{Anu}_f(v_i) = X - \lambda_i$, para todo i y por tanto

$$\min(f) = \mathrm{mcm}(\mathrm{Anu}_f(v_1), \ldots, \mathrm{Anu}_f(v_n)) = (X - \alpha_1) \cdots (X - \alpha_k),$$

donde $\alpha_1, \cdots, \alpha_k$ son los diferentes valores propios.

Supongamos que $\min(f) = (X - \alpha_1) \cdots (X - \alpha_k)$ con los α_i distintos. Por la Proposición 10.3.11,

$$V = t_{X-\alpha_1}(V) \oplus \cdots \oplus t_{X-\alpha_k}(V)$$

y la matriz asociada a la restricción de f a $t_{X-\alpha_i}(V)$ es α_i. Por tanto f es diagonalizable. □

Proposición 10.3.17 *Sean $f, g \in \mathbf{E}$ tales que $fg = gf$. Entonces existe una descomposición*

$$V = V_1 \oplus \cdots \oplus V_n$$

y polinomios irreducibles $P_1, \ldots, P_n, Q_1, \ldots, Q_n$ tales que, para cada $i = 1, 2, \ldots, n$ se verifican:

1. *V_i es f-invariante y g-invariante.*
2. *Para todo $v \in V_i$, $\mathrm{Anu}_f(v)$ es una potencia de P_i y $\mathrm{Anu}_g(v)$ es una potencia de Q_i.*

Demostración. Por la Proposición 10.3.11 y el Ejercicio 10.3.10

$$V = \text{Ker } R_1^{\alpha_1}(f) \oplus \cdots \oplus \text{Ker } R_l^{\alpha_l}(f)$$

donde $\min(f) = R_1^{\alpha_1} \cdots R_l^{\alpha_k}$ es la descomposición irredundante de $\min(f)$ en producto de polinomios mónicos irreducibles. Como g conmuta con f, también conmuta con $R_i^{\alpha_i}(f)$ y por tanto Ker $R_i^{\alpha_i}(f)$ es g-invariante (Ejercicio 10.2.3). Sea g_i la restricción de g a Ker $R_i^{\alpha_i}(f)$. Aplicando de nuevo la Proposición 10.3.11 y los Ejercicios 10.3.10 y 10.2.3 a g_i obtenemos que

$$\text{Ker } R_i^{\alpha_i}(f) = V_{i1} \oplus \cdots \oplus V_{ik_i}$$

donde V_{ij} es g-invariante y f-invariante y $\text{Anu}_g(v_{ij})$ es una potencia de un polinomio irreducible para cualesquiera índices i, j y para cada $v \in V_{ij}$. "Pegando" estas descomposiciones se obtiene el resultado deseado. □

Corolario 10.3.18 *Si f y g son dos endomorfismos diagonalizables de V tales que $fg = gf$, entonces existe una base B de V tal que f_B y g_B son diagonales (se dice que f y g son* simultáneamente diagonalizables*).*

Demostración. Sean $V = V_1 \oplus \cdots \oplus V_n$ y $P_1, \ldots, P_n, Q_1, \ldots, Q_n$ como en la demostración de la Proposición 10.3.17. Por el Corolario 10.3.16, para cada $i = 1, \ldots, n$ existen α_i y β_i tal que $\text{Anu}_f(v) = X - \alpha_i$ y $\text{Anu}_g(v) = X - \beta_i$ para todo $v \in V_i$. O sea $f(v) = \alpha_i v$ y $f(v) = \beta_i v$. Pegando bases de los V_i obtenemos una base B de V tal que f_B y g_B son diagonales. □

10.4 Descomposición primaria

Como consecuencia de las Proposiciones 10.2.7 y 10.3.14 se deduce.

Teorema 10.4.1 *Sea f un endomorfismo del espacio vectorial de dimensión finita V sobre K. Entonces $f = f_1 \oplus \cdots \oplus f_n$, donde cada f_i es un endomorfismo de un subespacio invariante cíclico de V y $\min(f_i)$ es una potencia de un polinomio irreducible de $K[X]$.*

Definición 10.4.2 *Una descomposición $f = f_1 \oplus \cdots \oplus f_n$ como la del Teorema 10.4.1 se llama* descomposición primaria *de f. La lista de los polinomios $\min(f_i)$, con sus repeticiones si las hay, se llama la* lista de divisores elementales *de la descomposición primaria.*

Teorema 10.4.3 *Las listas de divisores elementales de todas las descomposiciones primarias de un endomorfismo son iguales salvo el orden. En consecuencia, podemos hablar de la* lista de divisores elementales del endomorfismo*.*

Demostración. Supongamos que

$$\begin{aligned} f &= g_{11} \oplus \cdots \oplus g_{1k_1} \oplus \cdots \oplus g_{p1} \oplus \cdots \oplus g_{pk_p} \\ &= h_{11} \oplus \cdots \oplus h_{1l_1} \oplus \cdots \oplus g_{q1} \oplus \cdots \oplus g_{ql_q} \end{aligned}$$

son dos descomposiciones primarias de f con

$$\min(g_{ij}) = P_i^{m_{ij}} \qquad \text{y} \qquad \min(h_{ij}) = Q_i^{n_{ij}},$$

siendo los P_i polinomios mónicos irreducibles distintos entre sí y los Q_i polinomios mónicos irreducibles distintos entre sí. Por la Proposición 10.3.14 existen

$$v_{11}, \ldots, v_{1k_1}, \ldots, v_{p1}, \ldots, v_{pk_p}, w_{11}, \ldots, w_{1l_1}, \ldots, w_{q1}, \ldots, w_{ql_q} \in V$$

tales que

$$V \quad = \quad \oplus_{i=1}^{p} \oplus_{j=1}^{k_i} K[f]v_{ij} \quad = \quad \oplus_{i=1}^{q} \oplus_{j=1}^{l_i} K[f]w_{ij}$$

con $\mathrm{Anu}_f(v_{ij}) = P_i^{m_{ij}}$ y $\mathrm{Anu}_f(w_{ij}) = Q_i^{n_{ij}}$. Entonces $\min(f) = \mathrm{mcm}(P_i^{m_{ij}} : i,j) = P_1^{m_1} \cdots P_p^{m_p}$, donde $m_i = \max(m_{ij} : j)$. Análogamente, $\min(f) = \mathrm{mcm}(Q_i^{n_{ij}} : i,j) = Q_1^{n_1} \cdots Q_q^{n_q}$ con $n_i = \max(n_{ij} : j)$. Esto muestra que $p = q$ y que, reordenando los Q_i si es necesario, $P_i = Q_i$ y $m_i = n_i$ para todo i.

El lector puede comprobar como ejercicio que para cada $i = 1, \ldots, p$

$$t_{P_i}(V) \quad = \quad \oplus_{j=1}^{k_i} K[f]v_{ij} \quad = \quad \oplus_{j=1}^{l_i} K[f]w_{ij}.$$

Por tanto $f\mid_{t_{P_i}(V)} = \oplus_{j=1}^{k_i} g_{ij} = \oplus_{j=1}^{l_i} h_{ij}$, de manera que, para ver que $m_{ij} = n_{ij}$ para cada par de índices, podemos suponer que $p = 1$; es decir, que $\min(f) = P^m$ para algún polinomio irreducible P. Es decir, podemos poner

$$V = \oplus_{j=1}^{k} K[f]v_j = \oplus_{j=1}^{l} K[f]w_j$$

donde $\mathrm{Anu}_f(v_j) = P^{m_j}$ y $\mathrm{Anu}_f(v_j) = P^{n_j}$. Reordenando los v_j y los w_j, podemos suponer que los m_j y los n_j están en orden decreciente. La demostración estará terminada si vemos que $m_j = n_j$ para cada j, y a continuación vemos esto por inducción en j. Obsérvese que $P^{m_1} = \min(f) = P^{n_1}$, lo que resuelve el caso $j = 1$. Sea $j > 1$ y suponemos que $m_t = n_t$ para todo $t < j$. Podemos suponer, sin pérdida de generalidad que $m_j \leq n_j$. Entonces

$$\begin{array}{rcl} P^{m_j} \cdot V & = & K[f]P^{m_j}v_1 \oplus \cdots \oplus K[f]P^{m_j}v_{j-1} \\ & = & K[f]P^{m_j}w_1 \oplus \cdots \oplus K[f]P^{m_j}w_{j-1} \oplus K[f]P^{m_j}w_j \oplus \cdots \oplus K[f]P^{m_j}w_k. \end{array}$$

Como, para cada $t < j$

$$\dim_K K[f](P^{m_j} \cdot v_t) = \mathrm{gr}(\mathrm{Anu}_f(P^{m_j} \cdot v_t)) = \mathrm{gr}(P^{m_t - m_j}) = \mathrm{gr}(P^{n_t - m_j}) = \dim_K K[f](P^{m_j} \cdot w_t)$$

deducimos que $P^{m_j}w_j = 0$ y, por tanto $m_j = n_j$. □

La demostración de la Proposición 10.4.3 muestra que, para calcular la lista de los divisores elementales de un endomorfismo f, podemos suponer que su polinomio mínimo es potencia de un polinomio irreducible P. En este caso, todos los divisores elementales son potencias de P y se trata sólo de decir cuántos de ellos son el propio P, cuántos son P^2, etcétera. El siguiente resultado nos da una fórmula que resuelve este problema.

Proposición 10.4.4 *Sea f un endomorfismo de V tal que $\min(f) = P^n$ con P irreducible de grado m en $K[X]$. Para cada $t = 1, \ldots, n$ sea*

$$d_t = \dim_K \mathrm{Ker}\ P^t(f) - \dim_K \mathrm{Ker}\ P^{t-1}(f).$$

Entonces el número de divisores elementales de f de la forma P^t es

$$n_t = \frac{d_t - d_{t+1}}{m}.$$

Demostración. Pongamos

$$V = \oplus_{k=1}^{n} \oplus_{i=1}^{n_k} K[f]v_{ki}$$

con $\mathrm{Anu}_f(v_{ki}) = P^k$, para todo i, k. Obsérvese que $\dim_K K[f]v_{ki} = mk$, para todo k e i. Por otro lado, para todo $t = 1, \ldots, n$,

$$P^t \cdot V = \oplus_{k=1}^{n} \oplus_{i=1}^{n_k} K[f](P^t \cdot v_{ki}) = \oplus_{k=t+1}^{n} \oplus_{i=1}^{n_k} K[f](P^t \cdot v_{ki})$$

y $\mathrm{Anu}_f(P^t \cdot v_{ki}) = P^{k-t}$, para todo $k > t$. Luego, $\dim_K K[f](P^t \cdot v_{ki}) = (k-t)m$ y, por tanto,

$$\dim_K P^t(f)(V) = \dim_K P^t \cdot V = \sum_{k=t+1}^{n} \sum_{i=1}^{n_k} \dim_K K[f](P^t \cdot v_{ki}) = \sum_{k=t+1}^{n} n_k(k-t)m,$$

de donde

$$\dim_K \mathrm{Ker}\ P^t(f) = \dim_K V - \dim_K P^t(f)(V) = \dim_K V - \sum_{k=t+1}^{n} n_k(k-t)m$$

y como consecuencia

$$d_t = \sum_{k=t}^{n} n_k(k-t+1)m - \sum_{k=t+1}^{n} n_k(k-t)m = m\sum_{k=t}^{n} n_k,$$

de donde se deduce fácilmente que $mn_t = d_t - d_{t+1}$. □

Sea $f = f_1 \oplus \cdots \oplus f_k$ una descomposición primaria de f asociada a la descomposición $V = V_1 \oplus \cdots \oplus V_k$. Como cada V_i es cíclico, existen vectores v_i tales que $V_i = K[f]v_i$, y pondremos $Q_i = \mathrm{Anu}_f(v_i) = \min(f_i)$, de modo que $Q_1, \ldots, Q_k$ son los divisores elementales de f. Como hemos visto en el Ejercicio 10.3.7, el conjunto $B_i = \{v_i, f(v_i), f^2(v_i), \ldots, f^{m_i-1}(v_i)\}$ es una base de V_i (donde m_i es el grado de Q_i) y se tiene $f_{iB_i} = C(Q_i)$. Por tanto, del Teorema 10.4.1 se deduce:

Corolario 10.4.5 *Para todo endomorfismo f de un espacio vectorial de dimensión finita V existe una base B tal que*

$$f_B = \left(\begin{array}{c|c|c|c} C(Q_1) & & & \\ \hline & C(Q_2) & & \\ \hline & & \ddots & \\ \hline & & & C(Q_k) \end{array}\right) \tag{10.4.2}$$

donde $(Q_1, Q_2, \ldots, Q_k)$ es la lista de los divisores elementales de f y $C(Q_i)$ es la matriz compañera de Q_i. La matriz de (10.4.2) se llama forma canónica primaria *de f.*

A la forma canónica primaria se le puede "dar la vuelta". Supongamos que B es una base de V tal que f_B es de la forma (10.4.2). Si descomponemos la base B de acuerdo con los bloques de la matriz (10.4.2) $B = B_1 \cup B_2 \cup \cdots \cup B_k$, entonces cada $V_i = \langle B_i \rangle$ es un subespacio f-invariante de V. Además, por la forma de la matriz compañera $C(Q_i)$, si v_i es el primer elemento de B_i y m_i es el grado de Q_i, entonces $B_i = \{v_i, f(v_i), f^2(v_i), \ldots, f^{m_i-1}(v_i)\}$. Luego $V_i = K[f]v_i$ y $f_i = f\,|_{V_i}$ es indescomponible y por tanto $f = f_1 \oplus f_2 \oplus \cdots \oplus f_k$ es una descomposición primaria de f. En conclusión, $(Q_1, Q_2, \ldots, Q_k)$ es la lista de divisores elementales de f y tenemos el siguiente corolario:

Corolario 10.4.6 *Dos endomorfismos son semejantes precisamente si sus listas de divisores elementales coinciden salvo el orden, precisamente si sus formas canónicas primarias coinciden salvo el orden en el que escribimos las matrices compañeras.*

Ejercicio 10.4.7 *Demostrar que un endomorfismo es diagonalizable precisamente si su forma canónica primaria es diagonal.*

Ejemplos 10.4.8 *Forma canónica primaria.*

Vamos a obtener la forma canónica primaria de los endomorfismos de los Ejemplos 10.2.6 y 10.3.9.

1. Sea f el endomorfismo de $\mathbb{R}^3$ dado por $f(x,y,z) = (-x-2y-2z,\ x+y,\ z)$. Ya vimos en el Ejemplo 10.2.6 que $\mathbb{R}^3 = \langle u \rangle \oplus \langle v, w \rangle = \mathbb{R}[f]u \oplus \mathbb{R}[f]v$ es una descomposición indescomponible de f, donde $u = (0,-1,1)$, $v = (1,0,0)$ y $w = (-1,1,0)$. También vimos en el Ejemplo 10.3.9 que $\mathrm{Anu}_f(u) = X - 1$ y $\mathrm{Anu}_f(v) = X^2 + 1$. Entonces, la forma canónica primaria de f es

$$\left(\begin{array}{c|c} C(X-1) & \\ \hline & C(X^2+1) \end{array}\right) = \left(\begin{array}{c|cc} 1 & & \\ \hline & 0 & -1 \\ & 1 & 0 \end{array}\right)$$

   Y la base en la que se obtiene la forma canónica primaria es $\{u, v, f(v) = w\}$. De hecho, ya habíamos obtenido esta representación matricial en el Ejemplo 10.2.6.

2. Sea f el mismo endomorfismo del ejemplo anterior pero considerado en $\mathbb{C}^3$. En tal caso, $\mathbb{C}(f)v$ no es indescomponible, como veíamos en el Ejemplo 10.2.6. En dicho ejemplo veíamos que f es diagonalizable, y claramente la forma diagonal es la forma canónica primaria.

3. Sea ahora f el endomorfismo de K^3 dado por $f(x,y,z) = (x, x+y, x+z)$. En el Ejemplo 10.2.6 vimos que $K^3 = \langle v_1\rangle \oplus \langle v_2, v_3\rangle$ es una descomposición indescomponible, donde $v_1 = (1,0,0)$, $v_2 = (0,1,1)$ y $v_3 = (1,1,1)$. Por tanto, $\langle v_2, v_3\rangle = K[f]v$ para algún vector v. Como $f(v_2) = v_2$, $K[f]v_2 = \langle v_2\rangle$ y por tanto el vector v_2 no puede hacer de v. Sin embargo, $f(v_3) = v_2 + v_3$ es linealmente independiente con v_3 y por tanto podemos coger $v = v_3$. Como $f^2(v) = 2v_2 + v_3 = -v_3 + 2f(v)$, la matriz asociada a f en la base $B = \{v_1, v, f(v)\}$ es

$$\left(\begin{array}{c|cc} 1 & & \\ \hline & 0 & 1 \\ & 1 & -2 \end{array}\right).$$

Ésta es la forma canónica primaria de f y sus divisores elementales son $X - 1 = \mathrm{Anu}(v_1)$ y $X^2 - 2X + 1 = (X-1)^2 = \mathrm{Anu}(v)$.

4. Sea ahora f el endomorfismo de K^3 del segundo apartado de los Ejemplos 10.3.9. Ya vimos que el polinomio mínimo de f es $(X-1)(X^2 - 2X + 2)$. Supongamos que $K = \mathbb{R}$. Entonces, los polinomios $X - 1$ y $X^2 - 2X + 2$ son irreducibles y por tanto son los factores invariantes de f y la forma canónica primaria es

$$\left(\begin{array}{c|cc} 1 & & \\ \hline & 0 & -2 \\ & 1 & 2 \end{array}\right)$$

Ya vimos que $X - 1 = \mathrm{Anu}_f(e_2)$ y $X^2 - 2X + 2 = \mathrm{Anu}_f(e_1)$ y por tanto una base en la que se obtiene la forma racional es $\{e_2, e_1, f(e_1) = e_1 + e_2\}$.

La única forma que hemos visto hasta ahora para calcular el polinomio mínimo de un endomorfismo ha consistido en aplicar el Ejercicio 10.3.8. Sin embargo, hay un método más efectivo, al que dedicamos el resto de la sección.

Definición 10.4.9 *Se llama* polinomio característico de una matriz $A \in M_n(K)$ *al polinomio*

$$\chi_A = \det(XI - A),$$

donde $I \in M_n(A)$ representa la matriz identidad.

Dos matrices semejantes tienen el mismo polinomio característico. En efecto, si A y B son matrices semejantes, entonces existe una matriz invertible U tal que $B = U^{-1}AU$. Luego,

$$\begin{array}{rcl} \chi_B & = & \det(XI - B) = \det(XU^{-1}U - U^{-1}AU) = \det(U^{-1}(XI - A)U) \\ & = & \det(U^{-1})\det(XI - A)\det(U) = \det(XI - A) = \chi_A. \end{array}$$

Por tanto todas las representaciones de un endomorfismo tienen el mismo polinomio característico. Se llama *polinomio característico χ_f de un endomorfismo f* al polinomio característico de cualquiera de sus representaciones matriciales.

Ejercicio 10.4.10 *Demostrar que el polinomio característico de la matriz compañera $C(P)$ de un polinomio mónico P es precisamente P.*

Utilizando el Corolario 10.4.5 y el Ejercicio 10.4.10 se demuestra fácilmente el siguiente:

Teorema 10.4.11 (Cayley-Hamilton) *Si f es un endomorfismo entonces $\chi_f(f) = 0$, o equivalentemente* $\min(f) \mid \chi_f$. *Además* $\min(f)$ *y χ_f tienen los mismos divisores irreducibles.*

Ejemplo 10.4.12 *Cálculo de la forma canónica primaria.*
Consideremos el endomorfismo $f = A\cdot$ de $\mathbb{R}^5$, donde

$$A = \begin{pmatrix} -1 & -1 & -1 & -2 & 0 \\ 1 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

El polinomio característico de A es $(X-1)(X^2+1)^2$. En vista del Teorema de Cayley-Hamilton (10.4.11), el polinomio mínimo de A es $(X-1)(X^2+1)$ ó $(X-1)(X^2+1)^2$. Comprobando que $(A-1)(A^2+1)\neq 0$ deducimos que es el segundo y por tanto la forma canónica primaria de f ha de ser

$$J=\left(\begin{array}{c|c} C(X-1) & \\ \hline & C((X^2+1)^2) \end{array}\right)=\left(\begin{array}{c|ccc} 1 & & & \\ \hline & 0 & 0 & 0 & -1 \\ & 1 & 0 & 0 & 0 \\ & 0 & 1 & 0 & -2 \\ & 0 & 0 & 1 & 0 \end{array}\right).$$

Para obtener la descomposición $\mathbb{R}^5=t_{X-1}(\mathbb{R}^5)\oplus t_{X^2+1}(\mathbb{R}^5)$ observamos que las columnas de la matrices $(A^2+I)^2$ y $A-I$ han de pertenecer a $t_{X-1}(\mathbb{R}^5)$ y $t_{X^2+1}(\mathbb{R}^5)$ respectivamente: Como

$$(A^2+I)^2=\begin{pmatrix} 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

una base de $t_{X-1}(\mathbb{R}^5)$ está formada por el vector $e_0=(1,-1,1,-1,1)$. Por otro lado,

$$A-I=\begin{pmatrix} -2 & -1 & -1 & -2 & 0 \\ 1 & -1 & 0 & 2 & 0 \\ 0 & 1 & -1 & -2 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

de donde fácilmente se deduce que una base de $t_{X^2+1}(\mathbb{R}^5)$ está formada por los cuatro primeros vectores de la base canónica $C=\{e_1,\ldots,e_5\}$. Entonces,

$$\begin{array}{rcl} e_1 & = & (1,0,0,0,0) \\ f(e_1) & = & (-1,1,0,0,0) \\ f^2(e_1) & = & (0,-1,1,0,0) \\ f^3(e_1) & = & (0,0,-1,1,0) \end{array}$$

forman una base B de $W=t_{X^2+1}(\mathbb{R}^5)$ y por tanto la restricción de f a W es indescomponible y $W=\mathbb{R}[f]e_1$. La forma canónica primaria de f se obtiene en la base $B=\{e_0,e_1,f(e_1),f^2(e_1),f^3(e_1)\}$. (Compruébese calculando explícitamente AU y UJ, donde $U=C_{CB}$ es la matriz de cambio de base.)

Ejercicio 10.4.13 *Resolver el ejercicio anterior considerando $f=A\cdot$ como un endomorfismo de $\mathbb{C}^5$.*

10.5 Forma Canónica de Jordan

En la sección anterior hemos asociado a cada endomorfismo una matriz canónica llamada forma canónica primaria. En esta sección vamos a ver una nueva forma canónica, llamada forma canónica de Jordan, que tiene más aplicaciones (véase la Sección 10.8). El proceso para conseguir la forma canónica primaria ha consistido en descomponer el endomorfismo f en una suma directa de endomorfismos indescomponibles $f=f_1\oplus\cdots\oplus f_k$ y después, para cada f_i, elegir una base del tipo $v_i,f(v_i),\ldots,f^{n-1}(v_i)$, donde f_i es un endomorfismo de $K[f]v_i$ y n es la dimensión de $K[f]v_i$ (y el grado del polinomio anulador de v_i). Podemos conseguir algo mejor si elegimos la base de otra forma aprovechando que el polinomio anulador es una potencia de un irreducible.

Definición 10.5.1 *Sea f un endomorfismo del espacio vectorial V sobre K. Sea $v\in V$ tal que $\mathrm{Anu}_f(v)=P^n$ con $P\in K[X]$ irreducible y mónico de grado m. Entonces pondremos*

$$\begin{array}{rcl} B(v)=B_f(v) & = & \{X^iP^j\cdot v : 0\leq i<m, 0\leq j<n\} \\ & = & \{v,f(v),f^2(v),\ldots,f^{m-1}(v), \\ & & P(f)(v),(fP(f))(v),(f^2P(f))(v),\ldots,f^{m-1}P(f))(v), \\ & & \ldots, \\ & & P^{n-1}(f)(v),(fP^{n-1}(f))(v),(f^2P^{n-1}(f))(v),\ldots,(f^{m-1}P(f)^{n-1})(v)\} \end{array}$$

Lema 10.5.2 *Sea f un endomorfismo indescomponible de V. Sea $\min(f) = P^n$, con P irreducible y mónico de grado m, y sea $v \in V$ tal que $V = K[f]v$. Entonces $B = B_f(v)$ es una base de V y la matriz asociada a f en $B = B_f(v)$ es*

$$f_B = J_n(P) = \left(\begin{array}{c|c|c|c|c|c} C(P) & & & & & \\ \hline N & C(P) & & & & \\ \hline & N & C(P) & & & \\ \hline & & \ddots & \ddots & & \\ \hline & & & N & C(P) & \\ \hline & & & & N & C(P) \end{array}\right),$$

donde hay $n \times n$ bloques, todos de tamaño $m \times m$, y

$$N = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \in M_m(K).$$

Recíprocamente, si f es representable por una matriz del tipo $J_n(P)$, entonces f es indescomponible y P^n es el polinomio mínimo de f.

Demostración. Por el Ejercicio 10.3.7, la dimensión de V coincide con el grado nm del polinomio mínimo de f. Por tanto, para comprobar que B es una base, basta con demostrar que es un conjunto linealmente independiente. Pero esto es fácil, ya que si

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \alpha_{ij} X^i P^j \cdot v = 0$$

entonces, haciendo $Q = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \alpha_{ij} X^i P^j$, se tiene $Q(f)(v) = 0$. Por tanto, Q es múltiplo de P^n, y como $\mathrm{gr}(Q) < \mathrm{gr}(P^n)$ deducimos que $Q = 0$. Como es claro que los polinomios $\{X_i P^j : 0 \le i < m, 0 \le j < n\}$ son linealmente independientes, deducimos que $\alpha_{i,j} = 0$.

El resto de la demostración lo dejamos como ejercicio. □

Definición 10.5.3 *La matriz $J_n(P)$ del Lema 10.5.2 se llama* matriz de elemental de Jordan generalizada *asociada al polinomio irreducible y mónico P con* multiplicidad n. *Se llama* matriz de Jordan generalizada *a una matriz del tipo*

$$\left(\begin{array}{c|c|c|c} J_{k_1}(P_1) & & & \\ \hline & J_{k_2}(P_2) & & \\ \hline & & \ddots & \\ \hline & & & J_{k_m}(P_m) \end{array}\right) \tag{10.5.3}$$

en la que cada P_i es un polinomio irreducible y mónico de $K[X]$ (los P_i pueden repetirse).

Corolario 10.5.4 *Cada endomorfismo $f \in \mathrm{End}_K(V)$ es representable por una matriz de Jordan generalizada, de forma única salvo permutaciones en las matrices elementales de Jordan generalizadas que la componen. Además, en tal caso, los divisores elementales de f son $P_1^{k_1}, \ldots, P_m^{k_m}$.*

En consecuencia, toda matriz $A \in M_n(K)$ es semejante a una matriz de Jordan generalizada, única salvo permutaciones en las matrices elementales de Jordan generalizadas que la componen.

Demostración. La existencia de una representación por una matriz de Jordan generalizada es consecuencia del Teorema 10.4.1 y del Lema 10.5.2. Por otro lado, del Lema 10.5.2 se deduce que si f es representable por la matriz (10.5.3), entonces los divisores elementales de f son $P_1^{k_1}, \ldots, P_m^{k_m}$. De la unicidad de los divisores elementales (Teorema 10.4.3) se deduce la unicidad de la representabilidad por matrices de Jordan generalizadas. □

Definición 10.5.5 *Se llama* forma canónica de Jordan generalizada *de un endomorfismo (respectivamente, de una matriz) a cualquier matriz de Jordan generalizada que la represente (respectivamente, que sea semejante a ella). No distinguiremos en el orden en el que escribimos las matrices elementales que forman la forma canónica de Jordan generalizada y, por tanto, hablaremos de* la *forma canónica de Jordan generalizada. Dos endomorfismos son semejantes precisamente si sus formas canónicas de Jordan generalizadas son iguales.*

Ejemplo 10.5.6 *Cálculo de la forma de Jordan generalizada.*

Consideremos la matriz A del Ejemplo 10.4.12. Como $\mathrm{Anu}_f(e_1) = (X^2+1)^2$, podemos obtener la forma generalizada de Jordan de f con la base $B' = \{e_0\} \cup B_f(e_1)$ formada por

$$\begin{array}{rcl} e_0 & = & (1,-1,1,-1,1) \\ e_1 & = & (1,0,0,0,0) \\ f(e_1) & = & (-1,1,0,0,0) \\ (f^2+1)(e_1) & = & (1,-1,1,0,0) \\ f(f^2+1)(e_1) & = & (-1,1,-1,1,0). \end{array}$$

Lo cual se puede ver comprobando la igualdad $AU = UJ$ donde U es la matriz (invertible) cuyas columnas están formadas por las coordenadas de la base B' y

$$J = \left(\begin{array}{c|cc|cc} 1 & & & & \\ \hline & 0 & -1 & & \\ & 1 & 0 & & \\ \hline & 0 & 1 & 0 & -1 \\ & 0 & 0 & 1 & 0 \end{array}\right) = \left(\begin{array}{c|c} J_1(X-1) & \\ \hline & J_2(X^2+1) \end{array}\right)$$

es la forma canónica de Jordan generalizada de A.

Cuando los divisores elementales de un endomorfismo son potencias de polinomios lineales (de grado 1), su forma de Jordan generalizada toma un aspecto particularmente agradable.

Definición 10.5.7 *Sean $a \in K$ y $n \in \mathbb{Z}^+$. Se llama* matriz elemental de Jordan *de* valor propio a *y tamaño n a la matriz $J_n(a) \in M_n(K)$ dada por*

$$J_n(a) = \begin{pmatrix} a & & & & \\ 1 & a & & & \\ & 1 & a & & \\ & & \ddots & \ddots & \\ & & & 1 & a \end{pmatrix}$$

es decir, $J_n(a)$ es la matriz elemental de Jordan generalizada asociada al polinomio irreducible $X-a$, con multiplicidad n; en símbolos, $J_n(a) = J_n(X-a)$. Una matriz de Jordan *es una matriz del tipo*

$$\left(\begin{array}{c|c|c|c} J_{n_1}(a_1) & & & \\ \hline & J_{n_2}(a_2) & & \\ \hline & & \ddots & \\ \hline & & & J_{n_k}(a_k) \end{array}\right). \tag{10.5.4}$$

Como consecuencia del Corolario 10.5.4 se obtiene:

Corolario 10.5.8 *Las siguientes condiciones son equivalentes para un endomorfismo f de un espacio vectorial sobre el cuerpo K:*

1. *f tiene una representación matricial que es una forma de Jordan con valores propios en K.*
2. *El polinomio mínimo* $\min(f)$ *es completamente descomponible.*
3. *El polinomio característico χ_f es completamente descomponible.*

Además, si $\min(f) = (X-a_1)^{m_1}\cdots(X-a_k)^{m_k}$, *con* $a_1,\ldots,a_k \in K$ *distintos, entonces los valores propios de una matriz de Jordan* J *que represente a* f *son* $a_1,\ldots,a_k$ *y* m_i *es el máximo de los tamaños de las matrices elementales de Jordan, de valor propio* a_i, *que forman* J.

Finalmente, todas las representaciones de f *por matrices de Jordan son iguales, salvo el orden en que se escriben las matrices elementales de Jordan que las forman.*

Corolario 10.5.9 *Las condiciones siguientes son equivalentes para una matriz* $A \in M_n(K)$.

1. A *es semejante a una matriz de Jordan con valores propios en* K.
2. *El polinomio mínimo* $\min(A)$ *es completamente descomponible en* K.
3. *El polinomio característico* χ_A *es completamente descomponible en* K.

Además, si $\min(f) = (X-a_1)^{m_1}\cdots(X-a_k)^{m_k}$, *con* $a_1,\ldots,a_k \in K$ *distintos, entonces los valores propios de una matriz de Jordan* J *semejante a* A *son* $a_1,\ldots,a_k$ *y* m_i *es el máximo de los tamaños de las matrices elementales de Jordan, de valor propio* a_i, *que forman* J.

Finalmente, todas las matrices de Jordan semejantes a A *son iguales, salvo el orden en que se escriben las matrices elementales de Jordan que las forman.*

Del Corolario 10.5.8 se deduce que no todos los endomorfismos son representables por una matriz de Jordan con valores propios en K (salvo si K es algebraicamente cerrado). Sin embargo, vamos a ver cómo podemos representar cada endomorfismo por una forma de Jordan con valores propios en un cuerpo que contenga a K como subcuerpo.

Sea f un endomorfismo de un espacio vectorial V de dimensión n sobre el cuerpo K. Para simplificar suponemos que $V = K^n$ y que $f = A\cdot$ para una matriz $A \in M_n(K)$. Por el Corolario 4.4.4, existe un cuerpo K' que contiene a K como subcuerpo y tal que $\min(f)$ es completamente descomponible en K'. Si $V_1 = K'^n$, entonces f se puede extender de forma única a un endomorfismo de $\mathrm{End}_{K'}(V_1)$. Este endomorfismo extendido, que también denotaremos por f, será el endomorfismo que tiene por matriz asociada en la base canónica la matriz A. Por el Corolario 10.5.8, f es representable sobre K' por una matriz de Jordan. En resumen, como consecuencia del Corolario 10.5.8, tenemos.

Teorema 10.5.10 *Dado* $f \in \mathrm{End}_K(V)$ *existen: un cuerpo* K' *que contiene a* K *como subcuerpo; un espacio vectorial* V' *sobre* K', *que contiene a* V *como subespacio vectorial sobre* K *y de forma que una base de* V_K *es una base de* $V'_{K'}$; *y un endomorfismo* $f' \in \mathrm{End}_{K'}(V')$ *que se restringe a* f *sobre* V, *tales que* f' *es representable por una matriz de Jordan.*

Corolario 10.5.11 *Para toda matriz* $A \in M_n(K)$ *existe un cuerpo* K' *que contiene a* K *como subcuerpo y tal que* A *es semejante a una única matriz de Jordan sobre* K'.

La matriz de Jordan que representa a un endomorfismo f (o que es semejante a una matriz A) en algún cuerpo K' que contiene a K se llama *forma canónica de Jordan*[1] de f (o de A).

10.6 Cálculo efectivo

En esta sección vamos a ver cómo obtener efectivamente la forma canónica de Jordan de un endomorfismo o de una matriz. Para ello seguimos los pasos del siguiente algoritmo:

Algoritmo de cálculo de la forma de Jordan de un endomorfismo f o una matriz A:

Supondremos que f se descompone en factores lineales, bien por que eso sucede sobre K o porque consideramos un cuerpo K' que contiene a K como subcuerpo y en el que χ_f descompone.

1. Calculamos el polinomio característico: χ_f (ó χ_A).
2. Descomponemos χ_f en la forma $\chi_f = (X-a_1)^{n_1}\cdots(X-a_k)^{n_k}$, donde $a_1,\ldots,a_k$ son distintos.

[1] Aunque pueden existir distintos cuerpos K' que contengan a K y en los que $\min(f)$ se descomponga en factores lineales, es posible demostrar que "el menor K' con esa propiedad" es único salvo isomorfismos. En el caso de mayor interés, $K = \mathbb{R}$, ese cuerpo es $\mathbb{R}$ ó $\mathbb{C}$, dependiendo de si $\min(f)$ se descompone o no en factores lineales en $\mathbb{R}[X]$.

3. Calculamos el polinomio mínimo. Éste será el polinomio $P = (X-a_1)^{m_1}\dots(X-a_k)^{m_k}$ con los m_i mínimos entre los que verifiquen $P(f)=0$. Por el Teorema de Cayley-Hamilon (10.4.11), $1 \le m_i \le n_i$, para todo i.

4. Para cada $i = 1,\dots,k$ calculamos elementos $v_{i1},\dots,v_{it_i}$ de forma que

$$\text{Ker } (f-a_i)^{m_i} = \oplus_{j=1}^{t_i} K[f]v_{ij}$$

Para hacer esto procedemos de la siguiente forma: Para simplificar pongamos $a = a_i$, $m = m_i$ y los elementos $v_{i1},\dots,v_{it_i}$ que vamos a calcular los denotamos $v_1,\dots,v_t$ Pongamos $g = f - a$. Obsérvese que

$$\text{Ker } (g) \subset \text{Ker } (g^2) \subset \cdots \subset \text{Ker } (g^{m-1}) \subset \text{Ker } (g^m) = \text{Ker } (g^{m+1}) = \cdots$$

y que si $x \in \text{Ker } (g^i)$, entonces $g(x) \in \text{Ker } (g^{i-1})$. Además, si $x_1,\dots,x_k \in \text{Ker } (g^i)$ y sus proyecciones en $\text{Ker } (g^i)/\text{Ker } (g^{i-1})$ son linealmente independientes, entonces las proyecciones de $g(x_1),\dots,g(x_k)$ en $\text{Ker } (g^{i-1})/\text{Ker } (g^{i-2})$ son linealmente independientes (¿por qué?).

Elegiremos

$$v_1,\dots,v_{j_1},v_{j_1+1},\dots,v_{j_2},\dots,v_{j_{m-1}+1},\dots,v_{j_m}$$

de forma que en cada fila de la siguiente tabla, las clases de los elementos que aparecen a la izquierda en el espacio vectorial cociente de la derecha forman una base de este espacio:

v_1	$\dots$	v_{j_1}							$\text{Ker } (g^m)/\text{Ker } (g^{m-1})$
$g(v_1)$	$\dots$	$g(v_{j_1})$	v_{j_1+1}	$\dots$	v_{j_2}				$\text{Ker } (g^{m-1})/\text{Ker } (g^{m-2})$
$g^2(v_1)$	$\dots$	$g^2(v_{j_1})$	$g(v_{j_1+1})$	$\dots$	$g(v_{j_2})$	v_{j_2+1}	$\dots$	v_{j_3}	$\text{Ker } (g^{m-2})/\text{Ker } (g^{m-3})$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

5. Cada uno de los v_{ij} proporcionará una matriz elemental de Jordan del tipo $J_{n_{ij}}(a_i)$ donde n_{ij} viene determinado por la propiedad $v_{ij} \in \text{Ker } (f-a_i)^{n_{ij}} \setminus \text{Ker } (f-a_i)^{n_{ij}-1}$.

6. La base en la que la representación matricial de f es su forma canónica de Jordan está formada uniendo los conjuntos de la forma

$$B_f(v_{ij}) = \{v_{ij}, (f-a_i)(v_{ij}), (f-a_i)^2(v_{ij}), \dots, (f-a_i)^{n_{ij}-1}(v_{ij})\}.$$

Obsérvese que cada uno de estos conjuntos corresponde a los elementos de una columna de la tabla del paso 4. Por tanto, los tamaños de las cajas de la forma de Jordan coinciden con las alturas de las columnas de dicha tabla (sin contar las cajas vacías).

7. Si estamos buscando la forma de Jordan de una matriz A, entonces $U^{-1}AU$ es la forma de Jordan, donde U se obtiene poniendo en columna las coordenadas de los elementos de la base descrita en el paso 6.

Ejemplo 10.6.1 *Cálculo de la forma canónica de Jordan.*

Sea

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 1 & 1 & 2 \end{pmatrix}.$$

Entonces

$$\chi_A = \begin{vmatrix} X-2 & 0 & 0 & 0 \\ 1 & X-1 & 0 & 0 \\ 0 & 1 & X & 1 \\ -1 & -1 & -1 & X-2 \end{vmatrix} = (X-1)(X-2)(X^2-2X+1) = (X-1)^3(X-2).$$

Así que los valores propios de A son 1 y 2, de forma que la suma de los tamaños de las matrices elementales de Jordan que forman la forma de canónica Jordan de A con valor propio 1 es 3 y sólo hay

una matriz elemental de Jordan con valor propio 2 y tamaño 1. Por tanto, la forma de Jordan A es una de las tres siguientes:

$$\left(\begin{array}{c|c|c|c} 1 & & & \\ \hline & 1 & & \\ \hline & & 1 & \\ \hline & & & 2 \end{array}\right), \left(\begin{array}{cc|c|c} 1 & 0 & & \\ 1 & 1 & & \\ \hline & & 1 & \\ \hline & & & 2 \end{array}\right), \left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ 1 & 1 & 0 & \\ 0 & 1 & 1 & \\ \hline & & & 2 \end{array}\right).$$

Por el Teorema de Cayley-Hamilton (10.4.11), el polinomio mínimo de A es $(X-1)^n(X-2)$ con $n = 1, 2$ ó 3. Como

$$(A-I)(A-2I) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & -1 & -2 & -1 \\ 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & -1 & -1 & -1 \end{pmatrix} \neq 0$$

y

$$(A-I)^2(A-2I) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & -1 & -2 & -1 \\ 1 & 1 & 1 & 0 \end{pmatrix} = 0,$$

el polinomio mínimo de A es $(X-1)^2(X-2)$. Eso implica que la forma de Jordan de de A es

$$J = \left(\begin{array}{cc|c|c} 1 & 0 & & \\ 1 & 1 & & \\ \hline & & 1 & \\ \hline & & & 2 \end{array}\right).$$

Vamos a encontrar una matriz invertible U tal que $U^{-1}AU = J$. Para ello primero buscamos un elemento en $\mathrm{Ker}\,(A-I)^2 \setminus \mathrm{Ker}\,(A-I)$. El vector $v_1 = (0,1,0,0)$ satisface esta propiedad. Entonces $v_2 = (A-I)v_1 = (0,0,-1,1) \in \mathrm{Ker}\,(A-I)$. Ahora tenemos que completar v_2 con un vector v_3 de forma que v_2 y v_3 formen una base de $\mathrm{Ker}\,(A-I) = \{(0,x_1,x_2,x_3) : x_1+x_2+x_3 = 0\}$. Podemos elegir $v_3 = (0,1,-1,0)$. Finalmente necesitamos un vector $v_4 \in \mathrm{Ker}\,(A-2I)$. Calculando este núcleo observamos que $v_4 = (1,-1,0,1)$ es una base de $\mathrm{Ker}\,(A-2I)$. Por tanto

$$U = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

es la matriz buscada. Compruébese la igualdad $AU = UJ$.

Cálculo de la forma de Jordan generalizada de un endomorfismo f o una matriz A:

El proceso de cálculo de la forma canónica de Jordan generalizada de un endomorfismo o una matriz, en el caso en el que no exista la forma canónica de Jordan, es bastante similar al del caso en el que sí exista. Enumeraremos aquí las diferencias con los siete pasos del algoritmo de cálculo de la forma canónica de Jordan.

2. El momento en el que descubriremos que un endomorfismo no tiene forma canónica de Jordan sobre K será al calcular, en el paso 2, la descomposición del polinomio característico $\chi_f = P_1^{n_1} \cdots P_k^{n_k}$ como producto de polinomios irreducibles de $K[X]$, si algún P_i tiene grado mayor que 1.

3. Entonces, en el paso 3, calcularemos el polinomio mínimo de forma similar, excepto que éste debe tener la forma $P_1^{m_1} \cdots P_k^{m_k}$, con $1 \leq m_i \leq n_i$ para todo i.

4. En el paso 4, debemos calcular $v_{i1}, \ldots, v_{it_i}$ de forma que

$$\mathrm{Ker}\; P_i^{m_i}(f) = \oplus_{j=1}^{t_i} K[f]v_{ij}\,.$$

Supongamos que $P = P_i$ tiene grado n y pongamos $m = m_i$, $v_j = v_{ij}$ y $t = t_i$. Entonces, la búsqueda de $v_1, \ldots, v_t$ se hace de forma similar a la explicada en el paso 4 cambiando en la tabla cada aparición de un v_i por

$$v_i, f(v_i), f^2(v_i), \ldots, f^{n-1}(v_i).$$

5. Cada v_{ij} da lugar a una matriz de Jordan generalizada.

6. La base en la que se obtiene la forma de Jordan generalizada se obtiene "pegando" las bases $B_f(v_{ij})$ de cada $K[f]v_{ij}$. Por tanto, las cajas de la forma de Jordan generalizada tienen tamaño hn donde h es la altura correspondiente al vector v_i en la tabla.

Ejemplo 10.6.2 *Forma canónica de Jordan generalizada.*
Calculemos la forma canónica de Jordan generalizada de la matriz racional

$$A = \begin{pmatrix} 1 & -1 & -3 & 0 \\ 1 & -1 & -2 & 0 \\ 0 & 0 & -2 & -1 \\ 0 & -1 & 3 & 0 \end{pmatrix} \in M_4(\mathbb{Q})$$

Calculamos el polinomio característico y obtenemos

$$\chi_A = \begin{vmatrix} X-1 & 1 & 3 & 0 \\ -1 & X+1 & 2 & 0 \\ 0 & 0 & X+2 & 1 \\ 0 & 1 & -3 & X \end{vmatrix} = (X^2+X+1)^2.$$

Como $P = X^2 + X + 1$ es indescomponible en $\mathbb{Q}[X]$ y en $\mathbb{R}[X]$, A no tiene una forma de Jordan sobre $\mathbb{Q}$ ni sobre $\mathbb{R}$, aunque si la tendrá sobre $\mathbb{C}$. Como

$$P(A) = A^2 + A + 1 = \begin{pmatrix} 2 & -1 & 2 & 3 \\ 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & -1 & -2 \end{pmatrix} \neq 0,$$

el polinomio mínimo de A es P^2. Por tanto, la forma de Jordan generalizada de A es

$$J = \left(\begin{array}{c|c} C(P) & \\ \hline N & C(P) \end{array}\right) = \left(\begin{array}{cc|cc} 0 & -1 & & \\ 1 & -1 & & \\ \hline 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{array}\right).$$

Para encontrar la matriz U tal que $U^{-1}AU = J$, buscamos $v \notin \operatorname{Ker} P(A)$, por ejemplo, $v = (1,0,0,0)$. Entonces, las columnas de V están formadas por $v_1 = v = (1,0,0,0), v_2 = Av = (1,1,0,0), v_3 = P(A)(v) = (2,1,0,-1), v_4 = (AP(A))(v) = (1,1,1,-1)$; es decir,

$$U = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 \end{pmatrix}$$

satisface $U^{-1}AU = J$.

10.7 Matrices reales de Jordan

Como hemos visto, para obtener la forma canónica de Jordan de un endomorfismo de un espacio vectorial (o una matriz) sobre un cuerpo K, a menudo tenemos que considerar un cuerpo mayor que el original. Esto no pasa si el cuerpo K es algebraicamente cerrado, pues el polinomio mínimo es completamente descomponible. Como $\mathbb{R}$ no es algebraicamente cerrado, la forma canónica de Jordan de una matriz

real es a menudo una matriz compleja, pero no real. Sin embargo, como $\mathbb{R}$ y $\mathbb{C}$ están tan cercanos, es fácil obtener una representación matricial real de una matriz real (y por tanto de un endomorfismo de un espacio vectorial real) que es muy parecida a una matriz de Jordan.

En efecto, sea f un endomorfismo de un espacio vectorial real V. Consideramos el espacio vectorial complejo

$$V[i] = \{x + yi : x, y \in V\}$$

con la suma

$$(x_1 + y_1 i) + (x_2 + y_2 i) = (x_1 + x_2) + (y_1 + y_2)i$$

y el producto por escalares

$$(a + bi)(x + yi) = (ax - by) + (ay + bx)i,$$

donde $a, b \in \mathbb{R}$.

Dado $v = x + yi \in V[i]$, pongamos $\mathrm{Re}\,(v) = x$, $\mathrm{Im}\,(v) = y$ y $\overline{v} = x + yi$. Consideramos V contenido en $V[i]$, identificando $x \in V$ con $x+0i$, y extendemos f a un endomorfismo del espacio vectorial complejo $V[i]$ poniendo

$$f(x + yi) = f(x) + f(y)i.$$

Sea W un subespacio de $V[i]$ invariante por f, de forma que la restricción de f a W es indescomponible. Entonces,

$$W = \mathbb{C}[f]v \quad \text{y} \quad \mathrm{Anu}_f(v) = (X - a)^n$$

para ciertos $v \in V[i]$, $a \in \mathbb{C}$ y $n \geq 1$. Así que

$$\overline{W} = \{\overline{v} : v \in W\} = \mathbb{C}[f]\overline{v} \quad \text{y} \quad \mathrm{Anu}_f(\overline{v}) = (X - \overline{a})^n,$$

luego $\overline{W}$ también es un subespacio invariante por f y la restricción de f a $\overline{W}$ es indescomponible. En consecuencia, por cada matriz elemental de Jordan de la forma $J_n(a)$ con $a \in \mathbb{C} \setminus \mathbb{R}$ que aparezca en la forma canónica de Jordan de f, existe otra de la forma $J_n(\overline{a})$. Eso implica que $V[i]$ tiene una descomposición primaria de la forma

$$V[i] = \mathbb{C}[f]u_1 \oplus \cdots \oplus \mathbb{C}[f]u_k \oplus \mathbb{C}[f]v_1 \oplus \mathbb{C}[f]\overline{v_1} \oplus \cdots \oplus \mathbb{C}[f]v_l \oplus \mathbb{C}[f]\overline{v_l}, \tag{10.7.5}$$

donde

$$\begin{array}{llll}
u_j \in V, & \mathrm{Anu}_f(u_j) = (X - a_j)^{p_j} & \text{con } a_j \in \mathbb{R} & (j = 1, \ldots, k) \\
v_j \in V[i] \setminus V, & \mathrm{Anu}_f(v_j) = (X - b_j)^{q_j} & \text{con } b_j \in \mathbb{C} \setminus \mathbb{R} & (j = 1, \ldots, l) \\
\overline{v_j} \in V[i] \setminus V, & \mathrm{Anu}_f(\overline{v_j}) = (X - \overline{b_j})^{q_j} & \text{con } \overline{b_j} \in \mathbb{C} \setminus \mathbb{R} & (j = 1, \ldots, l)
\end{array}$$

Fijemos un índice $j \in \{1, \ldots, l\}$, y pongamos

$$v = v_j, \quad b = b_j = \alpha + \beta i \quad \text{y} \quad q = q_j.$$

Entonces,

$$v, (f - b)(v), \ldots, (f - b)^{q-1}(v), \overline{v}, (f - b)(\overline{v}), \ldots, (f - b)^{q-1}(\overline{v})$$

es una base de $T_v = \mathbb{C}[f]v \oplus \mathbb{C}[f]\overline{v}$. Pero también

$$B_v = \{\mathrm{Re}\,(v), \mathrm{Im}\,(v), \mathrm{Re}\,((f - b)(v)), \mathrm{Im}\,((f - b)(v)), \ldots, \mathrm{Re}\,((f - b)^{q-1}(v)), \mathrm{Im}\,((f - b)^{q-1}(v))\}$$

es una base de $V[i]$ como espacio vectorial sobre $\mathbb{C}$. Además, $B_v \cup B_v i$ es una base de T_v como espacio vectorial sobre $\mathbb{R}$, de forma que B_v es una base de $V \cap T_v$, y la matriz asociada a la restricción de f a $V \cap T_v$ es

$$J_q(\alpha, \beta) = \left(\begin{array}{cc|cc|cc|cc}
\alpha & \beta & & & & & & \\
-\beta & \alpha & & & & & & \\
\hline
1 & 0 & \alpha & \beta & & & & \\
0 & 1 & -\beta & \alpha & & & & \\
\hline
 & & 1 & 0 & \alpha & \beta & & \\
 & & 0 & 1 & -\beta & \alpha & & \\
\hline
 & & & & \ddots & & \ddots & \\
\hline
 & & & & & & 1 & 0 \\
 & & & & & & 0 & 1
\end{array}\right.
\left.\begin{array}{cc}
 & \\
 & \\
 & \\
 & \\
 & \\
 & \\
 & \\
 & \\
\hline
\alpha & \beta \\
-\beta & \alpha
\end{array}\right),$$

donde hay $q \times q$ bloques. Una matriz del tipo $J_q(\alpha, \beta)$ se llama *matriz elemental real de Jordan* de tamaño q y valor propio $\alpha + \beta i$.

Con los vectores u_i de la descomposición (10.7.5) se actúa de igual modo, aunque en este caso sólo hemos de quedarnos con las partes reales. La unión, en el orden adecuado, de las bases así obtenidas nos da una base de V sobre $\mathbb{R}$ en la que la matriz de f es

$$\left(\begin{array}{c|c|c|c|c|c} J_{n_1}(a_1) & & & & & \\ \hline & \ddots & & & & \\ \hline & & J_{n_k}(a_k) & & & \\ \hline & & & J_{m_1}(b_1, c_1) & & \\ \hline & & & & \ddots & \\ \hline & & & & & J_{m_l}(b_l, c_l) \end{array}\right),$$

con $a_1, \ldots, a_k, b_1, c_1, \ldots, b_l, c_l \in \mathbb{R}$. Una matriz de este tipo se llama *matriz real de Jordan*. Como consecuencia, se tiene:

Teorema 10.7.1 *Sea f un endomorfismo de un espacio vectorial real V. Entonces f es representable por una matriz real de Jordan, única salvo permutaciones de las matrices elementales reales de Jordan que la forman. Esta matriz se llama la* forma canónica real de Jordan *de f.*

Ejemplo 10.7.2 *Formas canónicas de Jordan real y compleja.*
Veamos cómo podemos obtener la forma canónica real de Jordan de la matriz del Ejemplo 10.6.2

$$A = \begin{pmatrix} 1 & -1 & -3 & 0 \\ 1 & -1 & -2 & 0 \\ 0 & 0 & -2 & -1 \\ 0 & -1 & 3 & 0 \end{pmatrix}.$$

Ya vimos que el polinomio mínimo de A es

$$(X^2 + X + 1)^2 = (X - \omega)^2 (X - \overline{\omega})^2 \quad \text{con} \quad \omega = \frac{-1 + \sqrt{-3}}{2}.$$

Por tanto la formas de Jordan compleja y real de A son

$$J_{\mathbb{C}} = \left(\begin{array}{cc|cc} \omega & 0 & & \\ 1 & \omega & & \\ \hline & & \overline{\omega} & 0 \\ & & 1 & \overline{\omega} \end{array}\right) \text{ y } J_{\mathbb{R}} = \left(\begin{array}{cc|cc} -1/2 & \sqrt{3}/2 & & \\ -\sqrt{3}/2 & -1/2 & & \\ \hline 1 & 0 & -1/2 & \sqrt{3}/2 \\ 0 & 1 & -\sqrt{3}/2 & -1/2 \end{array}\right).$$

Para obtener una base del bloque con valor propio ω buscamos

$$v \in \text{Ker } (A - \omega)^2 \setminus \text{Ker } (A - \omega).$$

Una forma rápida de obtener v es observar que, como

$$(A - \omega)^2 (A - \overline{\omega})^2 = 0,$$

entonces los elementos de la forma $(A - \overline{\omega})^2 x$ pertenecen a Ker $(A - \omega)^2$. En particular, las columnas de $(A - \overline{\omega})^2$ pertenecen a Ker $(A - \omega)^2$. Calculando

$$(A - \overline{\omega})^2 = \frac{1}{2} \begin{pmatrix} 1 + 3\sqrt{-3} & -2 - 2\sqrt{-3} & 4 - 6\sqrt{-3} & 6 \\ 2 + 2\sqrt{-3} & -3 - \sqrt{-3} & 2 - 4\sqrt{-3} & 4 \\ 0 & 2 & -3 - 3\sqrt{-3} & 2 - 2\sqrt{-3} \\ -2 & -2\sqrt{-3} & -2 + 6\sqrt{-3} & -7 + \sqrt{-3} \end{pmatrix}$$

y

$$(A - \omega)(A - \overline{\omega})^2 = \frac{1}{2} \begin{pmatrix} 4 + 2\sqrt{-3} & -9 - \sqrt{-3} & 4 + 2\sqrt{-3} & -1 + 3\sqrt{-3} \\ 3 + \sqrt{-3} & -6 & 3 + \sqrt{-3} & 2\sqrt{-3} \\ 2 & -3 + \sqrt{-3} & 2 & 1 + \sqrt{-3} \\ -3 - \sqrt{-3} & 6 & -3 - \sqrt{-3} & -2\sqrt{-3} \end{pmatrix},$$

deducimos que cualquiera de las columnas de $(A-\overline{\omega})^2$ pertenece a Ker $(A-\omega)^2 \setminus$ Ker $(A-\omega)$. Tomando

$$v = (1+3\sqrt{-3},\ 2+2\sqrt{-3},\ 0,\ -2),$$

obtenemos que

$$v_1 = v \quad \text{y} \quad v_2 = (A-\omega)v_1 = (4+2\sqrt{-3},\ 3+\sqrt{-3},\ 2,\ -3-\sqrt{-3})$$

forman una base del bloque correspondiente al valor propio ω. Así,

$$\overline{v_1} = (1-3\sqrt{-3},\ 2-2\sqrt{-3},\ 0,\ -2) \quad \text{y} \quad \overline{v_2} = (A-\overline{\omega})\overline{v_1} = (4-2\sqrt{-3},\ 3-\sqrt{-3},\ 2,\ -3+\sqrt{-3})$$

forman una base correspondiente al bloque correspondiente al valor propio $\overline{\omega}$. Por tanto, la matriz

$$U_1 = \begin{pmatrix} 1+3\sqrt{-3} & 4+2\sqrt{-3} & 1-3\sqrt{-3} & 4-2\sqrt{-3} \\ 2+2\sqrt{-3} & 3+\sqrt{-3} & 2-2\sqrt{-3} & 3-\sqrt{-3} \\ 0 & 2 & 0 & 2 \\ -2 & -3-\sqrt{-3} & -2 & -3+\sqrt{-3} \end{pmatrix}$$

satisface la ecuación $U_1^{-1}AU_1 = J_{\mathbb{C}}$.

Tomando las partes reales e imaginarias de los vectores de las bases anteriores obtenemos la base

$$\begin{array}{rcl} u_1 & = & (1,\ 2,\ 0,\ -2) \\ u_2 & = & (3\sqrt{3},\ 2\sqrt{3},\ 0,\ 0) \\ u_3 & = & (4,\ 3,\ 2,\ -3) \\ u_4 & = & (2\sqrt{3},\ \sqrt{3},\ 0,\ -\sqrt{3}). \end{array}$$

Finalmente, vemos que la matriz

$$U = \begin{pmatrix} 1 & 3\sqrt{3} & 4 & 2\sqrt{3} \\ 2 & 2\sqrt{3} & 3 & \sqrt{3} \\ 0 & 0 & 2 & 0 \\ -2 & 0 & -3 & -\sqrt{3} \end{pmatrix}$$

satisface la ecuación $U^{-1}AU = J_{\mathbb{R}}$.

10.8 Aplicaciones

Expresar un endomorfismo o una matriz en su forma canónica de Jordan tiene múltiples aplicaciones y en esta sección veremos algunas de ellas.

Cálculo de potencias

La primera aplicación es el cálculo de potencias del endomorfismo o la matriz. Esto se basa en la sencilla fórmula

$$(U^{-1}AU)^n = U^{-1}A^nU,$$

y en el hecho de que es fácil calcular potencias de matrices de Jordan ya que

$$\left(\begin{array}{c|c|c|c} A_1 & & & \\ \hline & A_2 & & \\ \hline & & \ddots & \\ \hline & & & A_k \end{array}\right)^n = \left(\begin{array}{c|c|c|c} A_1^n & & & \\ \hline & A_2^n & & \\ \hline & & \ddots & \\ \hline & & & A_k^n \end{array}\right)$$

y

$$J_m(a)^n = \begin{pmatrix} a^n & 0 & 0 & 0 & \cdots \\ \binom{n}{1}a^{n-1} & a^n & 0 & 0 & \cdots \\ \binom{n}{2}a^{n-2} & \binom{n}{1}a^{n-1} & a^n & 0 & \cdots \\ \binom{n}{3}a^{n-3} & \binom{n}{2}a^{n-2} & \binom{n}{1}a^{n-1} & a^n & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

El lector puede demostrar esta fórmula por inducción sobre n.

Ejemplo 10.8.1 *Cálculo de las potencias de una matriz.*

Vamos a calcular A^n, donde

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}.$$

Para ello, calcularemos la forma canónica de Jordan de A. Empezamos calculando el polinomio característico de A:

$$\chi_A = (X-1)^4(X^2+1) = (X-1)^4(X-i)(X+i).$$

Así, el polinomio mínimo de A es de la forma $(X-1)^n(X^2+1)$ donde $n \leq 4$. Como se tiene $(A-I)^2(A^2+I) \neq 0$ y $(A-I)^3(A^2+I) = 0$, el polinomio mínimo de A es $(X-1)^3(X^2+1)$. De aquí, las formas canónicas compleja y real de Jordan de A son

$$J = \left(\begin{array}{ccc|c|c|c} 1 & 0 & 0 & & & \\ 1 & 1 & 0 & & & \\ 0 & 1 & 1 & & & \\ \hline & & & 1 & & \\ \hline & & & & i & \\ \hline & & & & & -i \end{array}\right) \quad \text{y} \quad \left(\begin{array}{ccc|c|cc} 1 & 0 & 0 & & & \\ 1 & 1 & 0 & & & \\ 0 & 1 & 1 & & & \\ \hline & & & 1 & & \\ \hline & & & & 0 & 1 \\ & & & & -1 & 0 \end{array}\right).$$

Obtenemos la forma canónica compleja conjugando por la matriz

$$U = \begin{pmatrix} 0 & 1 & 1 & 1 & 1+i & 1-i \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1+i & -1-i \\ 0 & 0 & 0 & 0 & -1-i & -1+i \end{pmatrix}$$

es decir, $U^{-1}AU = J$. Por tanto, $A^n = UJ^nU^{-1}$ donde

$$J^n = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ n & 1 & 0 & 0 & 0 & 0 \\ \binom{n}{2} & n & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & i^n & 0 \\ 0 & 0 & 0 & 0 & 0 & (-i)^n \end{pmatrix}.$$

Término general de una sucesión recurrente

Otra aplicación de la forma canónica de Jordan de una matriz es el cálculo del término general de una *sucesión recurrente*; es decir, de una sucesión de números (a_n) de forma que cada término a_n viene dado en función de los términos anteriores.

Ejemplo 10.8.2 *Cálculo del término general de sucesiones recurrentes.*

Calculamos una fórmula para el término general de la *sucesión de Fibonacci*

$$1, 1, 2, 3, 5, \ldots, a_n = a_{n-1} + a_{n-2}.$$

Obsérvese que se verifica la siguiente fórmula

$$\begin{pmatrix} a_{n-1} \\ a_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a_{n-2} \\ a_{n-1} \end{pmatrix}.$$

Por tanto, si ponemos

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

tendremos

$$\begin{pmatrix} a_{n-1} \\ a_n \end{pmatrix} = A^{n-2} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = A^{n-2} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Vamos a calcular A^n. El polinomio característico de A es $X^2 - X - 1 = (X - \frac{1+\sqrt{5}}{2})(X - \frac{1-\sqrt{5}}{2})$, luego A es diagonalizable. Si ponemos $\alpha = \frac{1+\sqrt{5}}{2}$ y $\beta = \frac{1-\sqrt{5}}{2}$ entonces se comprueban fácilmente las relaciones:

$$\alpha + \beta = 1, \quad \alpha - \beta = \sqrt{5}, \quad \alpha\beta = -1, \quad \alpha^2 = \alpha + 1, \quad \beta^2 = \beta + 1.$$

Si

$$U = \begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}$$

entonces

$$U^{-1}AU = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} = J.$$

Luego

$$\begin{aligned} A^n &= UJ^nU^{-1} = \tfrac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{pmatrix} \begin{pmatrix} -\beta & 1 \\ \alpha & -1 \end{pmatrix} \\ &= \tfrac{1}{\sqrt{5}} \begin{pmatrix} \alpha^{n-1} - \beta^{n-1} & \alpha^n - \beta^n \\ \alpha^n - \beta^n & \alpha^{n+1} - \beta^{n+1} \end{pmatrix} \end{aligned}$$

Luego

$$\begin{aligned} \begin{pmatrix} a_{n-1} \\ a_n \end{pmatrix} &= A^{n-2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ &= \tfrac{1}{\sqrt{5}} \begin{pmatrix} \alpha^{n-3} - \beta^{n-3} & \alpha^{n-2} - \beta^{n-2} \\ \alpha^{n-2} - \beta^{n-2} & \alpha^{n-1} - \beta^{n-1} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \end{aligned}$$

y, por tanto,

$$a_n = \frac{1}{\sqrt{5}}(\alpha^{n-2} - \beta^{n-2} + \alpha^{n-1} - \beta^{n-1}) = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n).$$

Descomposición aditiva de Jordan

Teorema 10.8.3 *Todo endomorfismo que tenga una forma de Jordan se puede escribir de forma única como $f = d + n$, donde d es diagonalizable, n es* nilpotente *(es decir, existe $k \in \mathbb{N}$ tal que $n^k = 0$) y $dn = nd$.*

Demostración. Sea f un endomorfismo de un espacio vectorial V que tenga una forma de Jordan y supongamos que B es una base de V tal que

$$f_B = \left(\begin{array}{c|c|c|c} J_{n_1}(a_1) & & & \\ \hline & J_{n_2}(a_2) & & \\ \hline & & \ddots & \\ \hline & & & J_{n_k}(a_k) \end{array}\right)$$

es la forma canónica de Jordan de A. Cada matriz elemental de Jordan es de la forma

$$J_{n_i}(a_i) = a_i I_{n_i} + J_{n_i}(0).$$

Claramente, la matriz $N_i = J_{n_i}(0)$ es nilpotente. Sean d y n los endomorfismo de V tal que

$$d_B = \left(\begin{array}{c|c|c|c} a_1 I_{n_1} & & & \\ \hline & a_2 I_{n_2} & & \\ \hline & & \ddots & \\ \hline & & & a_k I_{n_k} \end{array}\right) \qquad \text{y} \qquad n_B = \left(\begin{array}{c|c|c|c} N_1 & & & \\ \hline & N_2 & & \\ \hline & & \ddots & \\ \hline & & & N_k \end{array}\right).$$

Como d_B es diagonal y n_B es nilpotente, d es diagonalizable y n es nilpotente. Además, como $f_B = d_B + n_B$ y $d_B n_B = n_B d_B$, entonces $f = d + n$ y $dn = nd$.

Para ver la unicidad, observemos que

$$d(v) = a_1\pi_1(v) + \cdots + a_k\pi_k(v)$$

donde $\pi_i : V \to t_{X-a_i}(V)$ es la proyección de acuerdo con la descomposición de f de la Proposición 10.3.11. Utilizando esta proposición, deducimos que $\pi_i = P_i(f)$ para algún polinomio $P_i \in K[X]$ y por tanto $d = P(f)$ para algún polinomio $P \in K[X]$. Sean ahora d' diagonalizable y n' nilpotente con $f = d' + n'$ y tales que $d'n' = n'd'$. Entonces, tanto d' como n' conmutan con f y, por tanto, también conmutan con $d = P(f)$ y con $n = f - d$. De esto se deduce que $n - n'$ es nilpotente y que d y d' son simultáneamente diagonalizables (Corolario 10.3.18). Luego, $d' - d = n - n'$ es diagonalizable y nilpotente. Esto implica que $d' - d = n - n' = 0$ (¿por qué?) y por tanto $d = d'$ y $n = n'$. □

Corolario 10.8.4 *Sea $A \in M_n(K)$ y K' un cuerpo que contiene a K como subcuerpo tal que A tiene una forma de Jordan en K'. Entonces existen matrices únicas $D, N \in M_n(K')$ tales que:*

1. *$A = D + N$,*
2. *$DN = ND$,*
3. *D es diagonalizable en K'.*
4. *N es nilpotente; es decir, existe un $n \in \mathbb{N}$ tal que $N^n = 0$.*

Las descomposiciones del Teorema 10.8.3 y el Corolario 10.8.4 se llaman *descomposiciones aditivas de Jordan*. A pesar de que existen endomorfismos de espacios vectoriales reales para los que la forma de Jordan se obtiene sobre $\mathbb{C}$ y no sobre $\mathbb{R}$, las descomposiciones aditivas de Jordan de matrices o endomorfismos sobre $\mathbb{R}$ se pueden obtener sobre $\mathbb{R}$, como muestra la siguiente proposición:

Proposición 10.8.5 *Para todo $A \in M_n(\mathbb{R})$ existen matrices únicas $D, N \in M_n(\mathbb{R})$ tales que:*

1. *$A = D + N$,*
2. *$DN = ND$,*
3. *D es diagonalizable en $\mathbb{C}$.*
4. *N es nilpotente.*

Demostración. Como A tiene una forma de Jordan sobre $\mathbb{C}$, A tiene una descomposición de Jordan $A = D + N$ sobre $\mathbb{C}$. Si denotamos por $\overline{X}$ la matriz formada por los conjugados de las entradas de X, entonces $A = \overline{A} = \overline{D} + \overline{N}$, $\overline{D}$ es diagonalizable, $\overline{N}$ es nilpotente y $\overline{D}\,\overline{N} = \overline{N}\,\overline{D}$ (¿por qué?). Luego $A = D + N = \overline{D} + \overline{N}$ son dos descomposiciones aditivas de Jordan de A y, de la unicidad de estas descomposiciones deducimos que $D = \overline{D}$ y $N = \overline{N}$; es decir, $D \in M_n(\mathbb{R})$ y $N \in M_n(\mathbb{R})$. □

Corolario 10.8.6 *Todo endomorfismo de un espacio vectorial real de dimensión finita se puede escribir de forma única como suma de un endomorfismo diagonalizable (en $\mathbb{C}$) y uno nilpotente.*

Ejemplo 10.8.7 *Descomposición aditiva de Jordan.*

Sea A la matriz del Ejemplo 10.8.1 y sean J y U como en dicho ejemplo. Entonces $J = D_1 + N_1$ es la descomposición aditiva de Jordan de J donde

$$D_1 = \left(\begin{array}{ccc|c|c|c} 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ \hline & & & 1 & & \\ \hline & & & & i & \\ \hline & & & & & -i \end{array}\right) \quad \text{y} \quad N_1 = \left(\begin{array}{ccc|c|c|c} 0 & 0 & 0 & & & \\ 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ \hline & & & 0 & & \\ \hline & & & & 0 & \\ \hline & & & & & 0 \end{array}\right).$$

Por tanto la descomposición aditiva de Jordan de A es $A = D + N$, con

$$D = UD_1U^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix} \quad \text{y} \quad N = UN_1U^{-1} = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

10.9 Problemas

1. Demostrar que si una clase de semejanza de un endomorfismo o una matriz contiene un elemento invertible, entonces todos los elementos de dicha clase de semejanza son invertibles.

2. Demostrar que la matriz compañera de un polinomio P es invertible precisamente si $P(0) \neq 0$. Deducir que si P es el polinomio mínimo o el polinomio característico de un endomorfismo f de un espacio vectorial de dimensión finita, entonces f es invertible precisamente si $P(0) \neq 0$. En tal caso, obtener una fórmula para f^{-1} en función de P.

3. Demostrar que si f es un endomorfismo de V, entonces el grado de $\min(f)$ es menor o igual que $\dim V$.

4. Demostrar que si f es un endomorfismo de un espacio vectorial sobre $\mathbb{C}$ tal que $f^n = 1$ para algún $n \geq 1$, entonces f es diagonalizable.

5. Demostrar que las siguientes condiciones son equivalentes para una matriz $A \in M_n(K)$.

   (a) A es nilpotente; es decir, $A^n = 0$ para algún $n \in \mathbb{N}$.

   (b) El polinomio característico χ_A es una potencia de X.

   (c) El polinomio mínimo $\min(A)$ es una potencia de X.

   (d) 0 es el único valor propio de A en cualquier cuerpo que contenga a K como subcuerpo.

   (e) A tiene una forma canónica de Jordan formada por matrices elementales de Jordan con valor propio 0.

6. Sea f un endomorfismo idempotente (es decir, $f^2 = f$) de un espacio vectorial. Demostrar que f es diagonalizable.

7. Sea K un cuerpo. Demostrar que, si una matriz $N \in M_n(K)$ es nilpotente, entonces la *traza* $\mathrm{tr}(N)$ de N (es decir, la suma de los elementos de la diagonal) es 0. Recíprocamente, demostrar que si $\mathrm{tr}(N^k) = 0$ para todo $k \geq 0$, entonces N es nilpotente.

8. Encontrar las formas canónicas de Jordan complejas y reales de las siguientes matrices y encontrar la matriz invertible U tal que $U^{-1}AU$ adquiere cada una de las formas canónicas mencionadas.

(a) $\begin{pmatrix} 0 & -1 & 2 \\ 3 & -4 & 6 \\ 2 & -2 & 3 \end{pmatrix}$ (b) $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}$ (c) $\begin{pmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & 2 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & -3 & 3 \\ 0 & -5 & 6 \\ 0 & 3 & 4 \end{pmatrix}$

(e) $\begin{pmatrix} 2 & 0 & 0 & 0 \\ 3 & 2 & 0 & -2 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix}$ (f) $\begin{pmatrix} 1 & -2 & -1 & 0 \\ 1 & 0 & -3 & 0 \\ -1 & -2 & 1 & 0 \\ 1 & 2 & 1 & 2 \end{pmatrix}$ (g) $\begin{pmatrix} 0 & -1 & -1 & -1 \\ 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$

(h) $\begin{pmatrix} 0 & 1 & -2 & 1 \\ -2 & 1 & -6 & 3 \\ 2 & -3 & 0 & 1 \\ 2 & -3 & -2 & 3 \end{pmatrix}$ (i) $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ -1 & -1 & 1 & -1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 1 \\ 0 & 0 & 0 & 2 & -4 & -4 \end{pmatrix}$

9. Sean $a \in \mathbb{R}$ y $f : \mathbb{R}^3 \to \mathbb{R}^3$ el endomorfismo dado por $f(x, y, z) = (ax, x + ay, b + az)$. Calcular la forma canónica de Jordan de f y la descomposición aditiva de Jordan de f.

10. Estudiar para qué valores de los parámetros a y b la siguiente matriz es diagonalizable

$$\begin{pmatrix} 5 & 0 & 0 \\ 0 & -1 & a \\ 3 & 0 & b \end{pmatrix}$$

11. [*] Sea f un endomorfismo de V tal que $f = f_1 \oplus f_2$, y para $i = 1, 2$ sean V_i el dominio de f_i y $P_i = \min(f_i)$. Supongamos que $\mathrm{mcd}(P_1, P_2) = 1$. Demostrar:

    (a) $\min(f) = P_1 P_2$.

    (b) Si $V_1 = K[f_1]v_1$ y $V_2 = K[f_2]v_2$, entonces $V = K[f](v_1 + v_2)$.

    (c) Si $V = K[f]v$, entonces $V_1 = K[f_1]P_2(f)(v)$ y $V_2 = K[f_2]P_1(f)(v)$.

    (d) Todo endomorfismo de un espacio vectorial sobre K tiene una representación matricial del tipo

$$(P_1, \ldots, P_n) = \left(\begin{array}{c|c|c|c} C(P_1) & & & \\ \hline & C(P_2) & & \\ \hline & & \ddots & \\ \hline & & & C(P_k) \end{array}\right)$$

    con los P_i polinomios mónicos (no necesariamente potencias de irreducibles) de $K[X]$ y $P_{i+1} \mid P_i$ para todo $i < n$.

    (e) Si $C(P_1, \ldots, P_n)$ y $C(Q_1, \ldots, Q_m)$ son dos representaciones matriciales de un endomorfismo satisfaciendo las condiciones anteriores, entonces $n = m$ y $P_i = Q_i$ para todo i. Dichos polinomios se llaman *factores invariantes* de f.

    (Indicación: Observar la similitud con las descomposiciones invariantes de grupos abelianos finitamente generados.)

12. Sea f un endomorfismo de un espacio vectorial sobre un cuerpo K. Encontrar los factores invariantes de f, si sus divisores elementales son:

    (a) $X - 1, X - 1, X - 2, X - 3, (X - 2)^2, X^2 + 1, X^2 + 1, (X - 1)^2$, con $K = \mathbb{Q}$.

    (b) $X - i, X + i, (X - 2)^2, (X - i)^2, X + i$, con $K = \mathbb{C}$.

    (c) $(X + 3)^6, X + i, X - i, X - i$, con $K = \mathbb{C}$.

    (d) $(X - a), (X - a), (X - a), (X - b), (X - b), (X - c)$.

13. Sea f un endomorfismo de un espacio vectorial sobre un cuerpo K. Encontrar los divisores elementales de f si sus factores invariantes son:

    (a) $X^6 - X^4 - 2X^2, X^5 - X - 2X, X^4 - X^2 - 2$, con $K = \mathbb{Q}$.

    (b) $(X + 3)^2(X^2 + 1), X + 3, X + 3$, con $K = \mathbb{Q}$.

    (c) $(X - a)^2(X - b)^2, (X - a)$.

14. Sea f un endomorfismo de un espacio vectorial V. Sean $v_1, v_2 \in V$ tales que

$$V = K[f]v_1 \oplus K[f]v_2, \qquad \mathrm{Anu}_f(v_1) = (X - 1)^2 \qquad \text{y} \qquad \mathrm{Anu}_f(v_2) = (X^3 - 1).$$

    Calcular los divisores elementales de f.

15. Sea f un endomorfismo de un espacio vectorial V sobre un cuerpo K. Calcular todas las posibles combinaciones de divisores elementales de f en los siguientes casos:

    (a) $\dim_K V = 6$, $\min(f) = (X^2 + 1)(X + 3)^2$, $K = \mathbb{R}$ ó $K = \mathbb{C}$.

    (b) $\dim_K V = 6$, $\min(f) = (X - 1)^2(X^2 + X + 1)^2$, $K = \mathbb{R}$ ó $K = \mathbb{C}$.

16. Sea f un endomorfismo de un espacio vectorial V sobre un cuerpo K. Encontrar todas las posibles formas canónicas generalizadas de Jordan de f en los siguientes casos:
    (a) $K = \mathbb{R}$, $\dim_{\mathbb{R}}(V) = 5$ y $\min(f) = (X-1)^2$.
    (b) $K = \mathbb{Q}$, $\min(f) = (X^2-2)(X-1)$ y $\chi_f = (X^2-2)^2(X-1)^3$.
    (c) $K = \mathbb{R}$, $\dim_{\mathbb{R}}(V) = 6$ y $\min(f) = (X^2+1)(X-1)$
    (d) $K = \mathbb{C}$, $\dim_{\mathbb{C}}(V) = 6$ y $\min(f) = (X^2+1)(X-1)$
    (e) $K = \mathbb{Q}$, $\chi_f = (X^4-1)(X^2-1)$.

17. Encontrar todas las posibles formas canónicas de Jordan para matrices complejas de orden 4. ¿Existen dos matrices no semejantes sobre $\mathbb{C}$ de orden 4 que tengan el mismo polinomio mínimo y el mismo polinomio característico?

18. Encontrar todas las formas de Jordan que tienen como polinomio característico $(X-1)^6X^3$ y como polinomio mínimo $(X-1)^3X^2$. Hacer lo mismo para el caso en que el polinomio característico es $(x+2)^7(x-1)^5(x+3)$ y el polinomio mínimo es $(x+2)^3(x-1)^2(x+3)$.

19. Demostrar que si un endomorfismo f de un espacio vectorial V de dimensión finita sobre $\mathbb{Z}_3$ satisface $f^3 = 1$, entonces f tiene una forma de Jordan sobre $\mathbb{Z}_3$. Suponiendo que V tiene dimensión 3, dar la lista de todas las posibles formas de Jordan para endomorfismos de este tipo.

20. Sea f un endomorfismo de un espacio vectorial real con factores invariantes $(X-2)^3(X^2+1)^2$ y $(X-2)^2(X^2+1)$. Calcular el polinomio característico, el polinomio mínimo y las formas canónica de Jordan real y compleja de f.

21. Sean a, b y c tres números reales (no necesariamente distintos). Escribir todas las posibles formas canónicas de Jordan de un endomorfismo que tenga uno de los siguientes polinomios característicos:
    (a) $(X-a)^3(X-b)^2$.
    (b) $(X-a)^5(X-b)^3$.
    (c) $(X-a)(X-b)^2(X-c)^2$.

22. Calcular la forma de Jordan de la matriz $A = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ y una expresión para A^n.

23. Calcular A^{100} para las matrices del Problema 8.

24. Calcular el término general de una sucesión de números en la que cada número es la media aritmética de los dos inmediatamente precedentes y los dos primeros números son 0 y 1/2.

25. Se ha establecido experimentalmente que el gusano cabezón vive dos días, y cada día el número de gusanos que nacen coincide con la mitad del número de gusanos de la población. Establecer el estado estacionario de una población que empezó con 1000 gusanos cabezones recién nacidos.

26. Encontrar la forma aditiva de Jordan de las matrices del Problema 8.

27. [*] Escribir la lista completa de las posibles formas canónicas de Jordan para matrices 2×2 y 3×3 con coeficientes en el cuerpo $\mathbb{Z}_2$. ¿Cuántas clases de semejanza tienen $M_2(\mathbb{Z}_2)$ y $M_3(\mathbb{Z}_2)$? ¿Cuántas de estas clases de semejanza contienen una matriz invertible? Sea $G = \mathrm{GL}_3(\mathbb{Z}_2)$ el grupo de las matrices invertibles de orden 3 sobre $\mathbb{Z}_2$.
    (a) Calcular el cardinal del centralizador en G de cada una las formas canónicas invertibles.
    (b) Calcular el número de elementos de cada clase de conjugación de G.
    (c) Demostrar que $\mathrm{GL}_3(\mathbb{Z}_2)$ es un grupo simple de orden 168. (Indicación: Usar el Problema 56 del Capítulo 5.)

Bibliografía del capítulo

Puerta [27], Spindler [33].

Bibliografía

[1] Allenby, R.B.J.T.: *Rings, Fields and Groups. An Introduction to Abstract Algebra.* Arnold, 1983.

[2] Anzola, M. – Caruncho, J.R. – Pérez–Canales, G.: *Problemas de Álgebra 1: Conjuntos y Grupos.* Autores, 1982.

[3] Anzola, M. – Caruncho, J.R. – Pérez-Canales, G.: *Problemas de Álgebra 2: Anillos, Polinomios y Ecuaciones.* Autores, 1982.

[4] Artin, M.: *Algebra.* Prentice Hall, 1991.

[5] Atiyah, M. – Macdonald, I.G.: *Introducción al Álgebra Conmutativa.* Reverté, 1980.

[6] Baumslag, B. – Chandler, B.: *Teoría de Grupos.* McGraw-Hill, 1972.

[7] Bujalance, E. – Etayo, J.J. – Gamboa, J.M.: *Teoría Elemental de Grupos.* UNED, 1989.

[8] Childs, L.: *A Concerte Introduction to Higer Algebra.* Springer, 1979.

[9] Clark, A.: *Elementos de Álgebra Abstracta.* Alhambra, 1974.

[10] Cohn, P.M.: *Algebra (vol. 1).* Wiley, 1989.

[11] Delgado, F. – Fuertes, C. – Xambó, S.: *Introducción al Álgebra I.* Ed. Complutense, 1993.

[12] Delgado, F. – Fuertes, C. – Xambó, S.: *Introducción al Álgebra II. Anillos, Factorización y Teoría de Cuerpos.* Universidad de Valladolid, 1999.

[13] Dorronsoro, J. – Hernández, E.: *Números, Grupos, Anillos.* Addison-Wesley/UAM, 1996.

[14] Espada, E.: *Problemas resueltos de Álgebra (tomo 1).* Edunsa, 1978.

[15] Espada, E.: *Problemas resueltos de Álgebra (tomo 2).* Edunsa, 1983.

[16] Fraleigh, J.B.: *A First Course in Abstract Algebra.* Addison-Wesley, 1982.
Versión en castellano: *Álgebra Abstracta.* Addison-Wesley Iberoamericana, 1982.

[17] Gamboa, J.M. – Ruiz, J.M.: *Anillos y Cuerpos Conmutativos.* UNED, 1989.

[18] Gardiner, C.F.: *A First Course in Group Theory.* Springer, 1980.

[19] Hartley, B. – Hawkes, T.O.: *Rings, Modules and Linear Algebra.* Chapman & Hall, 1976.

[20] Herstein, I.N.: *Topics in Algebra.* Wiley, 1975.
Versión en castellano: *Álgebra Moderna.* Trillas, 1979.

[21] Hilton, P. – Wu, Y.C.: *Curso de Álgebra Moderna.* Reverté, 1977.

[22] Hungerford, T.W.: *Algebra.* Springer, 1987.

[23] Jacobson, N.: *Basic Algebra I.* Freeman, 1974.

[24] Lang, S.: *Undergraduate Algebra.* Springer, 1987.

[25] Lang, S.: *Álgebra.* Aguilar, 1977.

[26] Macdonald, I.D.: *The Theory of Groups.* Oxford University Press, 1968.

[27] Puerta, F.: *Álgebra Lineal.* Universidad Politécnica de Barcelona - Marcombo, 1981.

[28] Robinson, D.J.: *A Course in the Theory of Groups.* Springer, 1982.

[29] Rose, J.S.: *A Course on Group Theory.* Cambridge University Press, 1978.

[30] Rotman, J.J.: *The Theory of Groups (an Introduction).* Allyn & Bacon, 1973.

[31] Rowen, L.: *Algebra (Groups, Rings and Fields).* Peters, 1994.

[32] Sharpe, D.: *Rings and Factorization.* Cambridge University Press, 1987.

[33] Spindler, K.: *Abstract Algebra with Applications I. Vector Spaces and Groups.* Dekker, 1994.

[34] Spindler, K.: *Abstract Algebra with Applications II. Rings and Fields.* Dekker, 1994.

[35] Suzuki, M.: *Group Theory I.* Springer, 1982.

[36] van der Waerden, B.L.: *Algebra I.* Springer, 1991.

Índice Terminológico

Símbolos usados frecuentemente

$\emptyset$	conjunto vacío
$x \in X$	e es un elemento del conjunto X
$X \subseteq Y$	el conjunto X está contenido en el conjunto Y
$X \subset Y$	el conjunto X está contenido estrictamente en el conjunto Y
$X \cup Y$	unión de los conjuntos X e Y
$X \cap Y$	intersección de los conjuntos X e Y
$X \setminus Y$	diferencia de los conjuntos X e Y (elementos de X que no pertenecen a Y)
$\|X\|$	cardinal de un conjunto / orden de un grupo
$\mathbb{N}$	números enteros
$\mathbb{Z}$	números naturales
$\mathbb{Q}$	números racionales
$\mathbb{R}$	números reales
$\mathbb{C}$	números complejos
$\mathbb{N}_n$	conjunto $\{1, 2, \ldots, n\}$
$a \mid b$	a divide a b
(S)	ideal generado por el conjunto S
$\mathrm{mcd}(a, b)$	máximo común divisor de a y b
$\mathrm{mcm}(a, b)$	mínimo común múltiplo de a y b
$a \equiv b \bmod n$	a y b son congruentes módulo n
$\mathbb{Z}_n$	clases de restos módulo n
$\mathbb{Z}_n^*$	unidades de $\mathbb{Z}_n$
A^*	grupo de las unidades del anillo A
$M_n(A)$	anillo de matrices cuadradas de tamaño $n \times n$ sobre el anillo A
$A[[X]]$	anillo de series de potencias sobre el anillo A
$Q(D)$	cuerpo de fracciones del dominio D
AS^{-1}	anillo de fracciones del anillo A por el subconjunto multiplicativo S
M/N	anillo cociente o grupo cociente
$M \times N$, $\prod_{i \in I} M_i$	producto cartesiano de conjuntos / producto directo de anillos o grupos
$N \rtimes_\phi H$	producto semidirecto de los grupos N y H con acción ϕ
$M + N$, $\sum_{i \in I} M_i$	suma de ideales de un anillo o de subgrupos de un grupo abeliano
$M \oplus N$, $\oplus_{i \in I} M_i$	suma directa de subgrupos de un grupo abeliano
MN	producto de dos ideales, subgrupos o subconjunto de un anillo o un grupo
$M \cong N$	M y N son anillos o grupos isomorfos
$\mathrm{Ker}\ f$	núcleo del homomorfismo f
$\mathrm{Im}\ f$	imagen del homomorfismo f
$\mathbb{Z}[i]$	anillo de los enteros de Gauss
$\mathbb{Z}[\sqrt{m}]$	subanillo de $\mathbb{C}$ formado por los elementos de la forma $a + b\sqrt{m}$, con $a, b \in \mathbb{Z}$
$\mathbb{Q}[\sqrt{m}]$	subanillo de $\mathbb{C}$ formado por los elementos de la forma $a + b\sqrt{m}$, con $a, b \in \mathbb{Q}$
$N(x)$	norma del número complejo x
$A[X]$	anillo de polinomios en una indeterminada sobre el anillo A
$A[X_1, \ldots, X_n]$	anillo de polinomios en n indeterminadas sobre A
$\mathrm{gr}(P)$	grado del polinomio P
$D(P) = P'$	derivada del polinomio P
$P^{(n)}$	derivada n-ésima del polinomio P

$S(X)$	grupo de las permutaciones del conjunto X
S_n	grupo simétrico sobre n elementos
A_n	grupo alternado sobre n elementos
D_n	grupo diédrico de los giros y simetrías del n-ágono regular
Q_8	grupo de los cuaterniones
$\mathrm{Isom}(\mathbb{R}^2)$	grupo de las isometrías del plano $\mathbb{R}^2$
$\mathrm{Aut}(G)$	grupo de automorfismos del grupo G
$\mathrm{Inn}(G)$	grupo de automorfismos internos del grupo G
$\mathrm{GL}_n(K)$	grupo lineal sobre el cuerpo K
$\mathrm{SL}_n(K)$	grupo lineal especial sobre el cuerpo K
$H \leq G$	H es un subgrupo del grupo G
$H \trianglelefteq G$	H es un subgrupo normal del grupo G
$\langle S\rangle,\ \langle a\rangle$	subgrupo generado por el subconjunto S o por el elemento a
$Z(G)$	centro del grupo G
$\mathrm{Cen}_G(x)$	centralizador en el grupo G del elemento x
$N_G(H)$	normalizador de H en G
$aH,\ Ha$	clases laterales módulo un subgrupo H
G/H	conjunto de las clases laterales por la derecha de G módulo H
$H\backslash G$	conjunto de las clases laterales por la izquierda de G módulo H
$[G : H]$	índice de un subgrupo H en el grupo G
$o(g)$	orden de un elemento de un grupo
a^x	conjugado de a por x
a^G	clase de conjugación de a en el grupo G
$(i_1\ i_2\ \ \ldots\ i_n)$	ciclo en un grupo simétrico
$[t_1, t_2, \ldots, t_r]$	tipo de una permutación
$\mathrm{sg}(\sigma)$	signo de la permutación sigma
$r(L)$	rango del grupo abeliano libre L
$t(A)$	subgrupo de torsión del grupo abeliano A
$t_p(A)$	subgrupo de p-torsión del grupo abeliano A
$p(A)$	periodo del grupo abeliano A
$\langle a_1, \ldots, a_n \mid r_1, \ldots, r_m\rangle$	presentación de un grupo abeliano por generadores y relaciones
$G\alpha$ ó α^G	órbita de α en G
$E(\alpha) = \mathrm{Estab}_G(\alpha)$	estabilizador de α en G
n_p	número de p-subgrupos de Sylow en un grupo
$[a, b]$	conmutador de a y b
G'	subgrupo derivado del grupo G
$G^{(t)}$	t-ésimo subgrupo derivado del grupo G
$\ell(G)$	longitud de composición del grupo G
$\mathbf{E} = \mathrm{End}_K(V)$	anillo de endomorfismos del K-espacio vectorial V
f_B	matriz del endomorfismo f en la base B
$C_{B',B}$	matriz del cambio de base de B a B'
$f_1 \oplus \cdots \oplus f_n$	suma directa de endomorfismos
$A\cdot$	endomorfismo consistente en multiplicar vectores columna por la matriz A
$P \cdot v$	producto de polinomio por vector
$K[f]v$	subespacio invariante cíclico generado por v
$\min(f),\ \min(A)$	polinomio mínimo del endomorfismo f o de la matriz A
$\chi_f,\ \chi_A$	polinomio característico del endomorfismo f o de la matriz A
$\mathrm{Anu}_f(v)$	anulador del vector v por el endomorfismo f
$t_P(V)$	vectores de V anulados por potencias del polinomio P
$C(P)$	matriz compañera del polinomio P
$J_n(P)$	matriz elemental de Jordan generalizada asociada al polinomio P
$J_n(a)$	matriz elemental de Jordan de valor propio a
$J_n(\alpha, \beta)$	matriz elemental real de Jordan de valor propio $\alpha + \beta i$