

Jairo A. Charris Castañeda
Bernarda Aldana Gómez
Primitivo B. Acosta Humaney

ALGEBRA I

Fundamentos y teoría de los grupos

ACADEMIA COLOMBIANA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES
COLECCIÓN JULIO CARRIZOSA VALENZUELA No. 13
EDICIÓN CONJUNTA CON LA UNIVERSIDAD SERGIO ARBOLEDA

ACADEMIA COLOMBIANA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES
COLECCIÓN JULIO CARRIZOSA VALENZUELA No. 13

EDICIÓN CONJUNTA CON LA
UNIVERSIDAD SERGIO ARBOLEDA



UNIVERSIDAD
SERGIO ARBOLEDA

ALGEBRA I

Fundamentos y teoría de los grupos

Jairo A. Charris Castañeda

Universidad Sergio Arboleda, Academia Colombiana de Ciencias Exactas,
Físicas y Naturales

Bernarda Aldana Gómez

Escuela Colombiana de Ingeniería, Universidad Sergio Arboleda

Primitivo B. Acosta Humanéz

Universidad Sergio Arboleda, Universidad Pedagógica Nacional

Bogotá, D.C., Colombia
2005

© **Academia Colombiana de Ciencias Exactas, Físicas y Naturales**
Transversal 27 No. 39A-63, Apartado 44763, Bogotá, D.C., Colombia

© **Universidad Sergio Arboleda**
Calle 74 No. 14-14. Teléfono 3257500

Catalogación en la publicación Academia Colombiana de Ciencias Exactas,
Físicas y Naturales

Charris Castañeda, Jairo / Aldana Gómez, Bernarda / Umanez, Primitivo B.
Algebra I. Fundamentos y teoría de los grupos / Jairo Charris Castañeda /
Bernarda Aldana Gómez / Primitivo B. Umanez - Bogotá: Academia
Colombiana de Ciencias Exactas, Físicas y Naturales / Universidad Sergio
Arboleda, 2005

X, 274 p il. (Colección Julio Carrizosa Valenzuela, No. 13)

ISBN: 958-9205-28-3 Obra completa

ISBN: 958-9205-64-X Volumen

1. Algebra 2. Teoría de los grupos

CDD-20 512.22/2005

Diseño de la carátula tomado de Rothman, T.: Evariste Galois,
Temas 1. Grandes Matemáticas.

Esta publicación cuenta con el apoyo financiero del Ministerio de Educación Nacional

República de Colombia
MINISTERIO DE EDUCACIÓN NACIONAL



Libertad y Orden

Impresión:
Editora Guadalupe Ltda.
Tel.: 2690788
Bogotá, D.C., Colombia

Índice general

Introducción	VII
I Fundamentos y estructuras clásicas	1
1. Conjuntos, funciones y sistemas numéricos	3
1.1. Conjuntos y funciones	3
1.2. Los números reales	12
1.3. Los números naturales	18
1.4. Números enteros y aritmética elemental	21
1.5. Los números racionales	29
1.6. Dos notaciones útiles	31
1.7. Los números irracionales	32
1.8. Los números complejos	35
1.9. Sistemas numéricos, dominios y campos	44
1.10. Polinomios sobre los sistemas numéricos	47
1.11. Conjuntos finitos e infinitos	70
II Teoría elemental de los grupos	97
2. Grupos	99
3. Subgrupos	115
4. Subgrupos Normales	127
5. Homomorfía e isomorfía	135
6. Los teoremas de isomorfía	145

7. Productos finitos de grupos	159
8. El grupo simétrico	171
III Grupos y resultados especiales	193
9. Grupos de operadores	195
10. La teoría de Sylow	207
11. Grupos del tipo (p, q) y grupos diedros	219
12. Nilpotencia y resolubilidad	233

Introducción

El texto que sigue es una elaboración y ampliación por los dos últimos autores de las notas de clase presentadas por el primero a estudiantes del curso de Algebra Abstracta del Programa de Pregrado en Matemáticas de la Universidad Sergio Arboleda de Bogotá. El presente volumen está básicamente dedicado a la teoría elemental de los grupos.

De hecho, sólo la segunda parte, capítulos 2 a 8, fue presentada detalladamente en las clases. La primera parte, capítulo 1, fue redactada para los propósitos de referencia, y contiene las nociones básicas indispensables para el resto del trabajo sobre la teoría de los conjuntos y los sistemas numéricos clásicos (números naturales, enteros, racionales, reales y complejos), incluyendo nociones elementales de aritmética. Esta primera parte suministra, además de instrumentos, ejemplos concretos del material más abstracto de las segunda y tercera partes, y puede constituir de por sí la base para un curso de un semestre sobre los temas citados arriba y sobre la generación de estructuras abstractas. Es razonable suponer, sin embargo, que su contenido es suficientemente bien conocido por los estudiantes del primer curso de Algebra. La tercera parte, capítulos 9 a 12, dedicada a grupos y resultados especiales, es de un nivel más elevado que el de las otras dos y fue incluida para beneficio de los estudiantes más sobresalientes del curso, que pueden encontrar en ella técnicas y resultados relativamente avanzados que, sin embargo, constituyen aún material indispensable para una comprensión aceptable de los métodos de la teoría moderna de los grupos, y que, de ser cubierto totalmente en un curso, haría de éste un primer curso al nivel de posgrado.

La segunda parte pretende familiarizar al estudiante con las nociones y desarrollos básicos de la teoría de los grupos (grupos, subgrupos, subgrupos normales, grupos producto y grupos cociente, homomorfía e isomorfía), con algunas consideraciones sobre el problema de la existencia y las propiedades estructurales de los grupos abelianos finitos, y con un examen más o menos detallado de los grupos finitos de permutaciones, que no sólo suministran ejemplos significativos de grupos no abelianos, sino que son indispensables en cualquier estudio serio tanto de estos últimos objetos como de muchas otras partes del álgebra moderna. También incursionamos en esta parte en la teoría de Sylow en el caso conmutativo, más accesible de lo que lo es en el caso general. La exposición de esta segunda parte es, dados sus objetivos, pausada, detallada y rigurosa: todos los resultados que se mencionan, y

sobre todo aquellos que son indispensables en desarrollos posteriores, se demuestran cuidadosamente. Hemos procurado que cada capítulo contenga al menos un resultado significativo y no del todo trivial, pues un primer curso de álgebra, y especialmente uno dedicado a la teoría de los grupos, es un marco excelente para ir familiarizando a los estudiantes con el poder y omnipresencia del método deductivo en matemáticas y con algunas de sus características más relevantes. Asimilar las nociones y resultados básicos de esta parte es, como lo hemos mencionado, indispensable para cualquier estudio posterior de la teoría de los grupos y, de hecho, para el de muchas otras partes del álgebra. En particular, es indispensable para una buena comprensión de la tercera parte.

Debemos advertir al lector que hemos dejado por fuera de nuestras consideraciones al menos dos capítulos notables de la teoría de los grupos. El concerniente a las llamadas series de composición y los importantes resultados de Schreier, Zassenhaus y Jordan-Hölder sobre las mismas (aunque algo mencionamos de ellas en el capítulo 12), y el relacionado con los denominados grupos libres (sobre los cuales algo decimos en el capítulo 11). La razón para excluir estos temas tiene que ver con el grado de exigencia de los mismos. Del primero, no tanto en su desarrollo (al fin y al cabo, aplicaciones ingeniosas de los teoremas de isomorfía) como en su significado y objetivos (describir en forma precisa cualquier grupo en términos de los llamados grupos simples, algo que los principiantes pueden no estar listos para apreciar en toda su dimensión), y del segundo, no tanto en su significado y objetivos (construir, o lo que es equivalente, establecer la existencia de grupos sobre medida), como en su desarrollo (notablemente abstracto: alfabetos, palabras, generadores y relaciones, etc.). De usarse el presente documento como base para un curso de posgrado, algo habría que hacer con respecto a estas omisiones.

Cada capítulo contiene un número apreciable de ejercicios, la mayor parte de los cuales se resuelve por aplicación directa de los desarrollos del capítulo que los incluye y de los resultados más básicos de los capítulos previos. Algunos contienen ejemplos y contraejemplos que es conveniente conocer. Es razonable esperar que el lector intente resolver algunos de ellos, con el fin de poner a prueba su comprensión del material tratado. Los más difíciles (en el criterio de los autores, lo cual no deja de ser subjetivo) están marcados con un asterisco (*) y, a veces, con dos (**). En opinión de los autores, estos ejercicios pueden omitirse en un curso de pregrado, pero sería aconsejable que se los considerara siempre en uno de posgrado. (En gene-

ral, un asterisco previo a un lema, teorema, corolario, etc., indica que este presenta alguna característica que puede hacer conflictiva su comprensión o asimilación en un primer contacto con tal material.)

La presentación que hacemos (y que esperamos que ocupe un justo medio entre un texto divulgativo y un tratado sobre los grupos, compartiendo las virtudes pero no los defectos de tal tipo de documentos) ha sido altamente influida por la de los excelentes libros de I. N. Herstein [15] y [16]. De hecho, puede decirse que la nuestra es en esencia una elaboración del material de estas obras, presentándolo en forma algo más detallada, con el fin de adaptarlo a las necesidades de nuestros estudiantes y al estilo de los cursos en nuestras universidades. Esperamos así haber comunicado suficientes conocimientos técnicos sobre el tema para permitir autonomía de pensamiento en el mismo sin pretender crear un erudito. Otros textos han tenido también influencia, como es fácilmente detectable, aunque de una manera más local. Esto es evidente de los magníficos libros de T. W. Hungerford [17], S. Lang [20], J. Rotman [22] y B. L. Van der Waerden [26], aunque todos ellos son de un nivel más avanzado que el nuestro. También se han consultado, con gran beneficio, el texto de J. F. Caycedo [6] y las notas del curso que sobre la teoría de los grupos imparte el Profesor V. S. Albis en la Universidad Nacional en Bogotá, a quien agradecemos habernos puesto a nuestra disposición el contenido total de las mismas, incluyendo material aún no publicado.

Hemos procurado que tanto la notación como la terminología sean las más usuales. En cuanto a la primera, tal vez sólo las expresiones $A := B$ o $B =: A$, que indican que *A se define en términos de B*, son algo exóticas. En cuanto a la segunda, hemos preferido el lenguaje clásico, tal vez un poco anticuado, de los años 30 y 40 del Siglo XX, antes de la teoría de las categorías y el álgebra homológica hicieran su impacto (a comienzos de los años 50).

Es de esperar que el presente libro, que sólo contiene el primero de dos cursos de Álgebra Abstracta que la Universidad Sergio Arboleda ofrece a sus estudiantes de pregrado, sea seguido por un volumen adicional que contenga lo esencial del segundo curso y para el cual también se elaboraron notas de clase. Algo se ha planeado al respecto, y *la teoría de las extensiones algebraicas de los campos numéricos, incluyendo las teorías de Galois y de las extensiones construibles*, constituirán seguramente una de sus primeras partes. Otras partes estudiarán las estructuras abstractas básicas, anillos y cuerpos, así como sus propiedades aritméticas (lo cual generalizaría y

unificaría temas ya explorados para las estructuras numéricas), para terminar, probablemente con la teoría de Galois de los cuerpos finitos.

Parte I

Fundamentos y estructuras clásicas

Capítulo 1

Conjuntos, funciones y sistemas numéricos

En este capítulo fijaremos el lenguaje fundamental, el de los conjuntos, y revisaremos las propiedades básicas de los sistemas numéricos clásicos. Trataremos de ser breves, pues suponemos que las nociones aquí introducidas son en alguna medida conocidas por los lectores, pero no sacrificaremos la precisión necesaria.

La presentación que daremos se inspira en diversas fuentes, que no excluyen el Libro I del tratado de Bourbaki [25] (véase también [9]), pero es mucho más informal y muy cercana a la dada en [5], aunque más elaborada en ciertos puntos.

1.1. Conjuntos y funciones

La noción matemática básica es la de *conjunto*. Los conjuntos son agrupaciones o colecciones de objetos que deseamos considerar a su vez como objetos autónomos. Los representaremos usualmente con letras mayúsculas $A, B, C, D, E, F, G, X, Y, Z$, etc. Es también frecuente referirse a ellos como *clases*. Si X es un conjunto, $a \in X$ significará que a es un *objeto*, un *elemento*, o un *miembro* de X , y se dice que a *pertenece* a X . Si a no es un objeto de X , escribiremos $a \notin X$. Si X, Y son conjuntos, $X \subseteq Y$, que se lee *X está contenido en Y* , significará que *todo objeto de X es también un objeto de Y* . Se dice entonces que X es un *subconjunto* de Y , es usual

escribir también $Y \supseteq X$, y expresarlo diciendo que Y contiene a X . La notación $X \not\subseteq Y$, o lo que es lo mismo, la $Y \not\supseteq X$, indicará que X no es un subconjunto de Y , y será equivalente a afirmar que *existe* $a \in X$ tal que $a \notin Y$.

Aunque a veces se les da un significado diferente (véase, al respecto, [17], Apéndice), y aunque preferiremos el término conjunto, nosotros consideraremos que los términos *clase* y *conjunto* son sinónimos. Sólo usaremos esporádicamente el término *clase* y usualmente en el contexto de *conjunto de conjuntos* (parece más elegante hablar de una *clase de conjuntos*).

Dos conjuntos X, Y son *iguales*, $X = Y$, si tienen los mismos elementos, es decir, si $X \subseteq Y$ y $Y \subseteq X$. Si X y Y no son iguales, es decir, si $X \not\subseteq Y$ o $Y \not\subseteq X$, se dice que X y Y son *diferentes*, y se escribe $X \neq Y$.

Si a es un objeto, $\{a\}$ denotará el conjunto cuyo único elemento es a . Así, si $A = \{a\}$, $x \in A$ si y sólo si $x = a$. Debe distinguirse entre el objeto a y el conjunto $\{a\}$. Si a, b son objetos, denotaremos con $\{a, b\}$ el conjunto cuyos únicos elementos son a y b , así que $B = \{a, b\}$ significará que $x \in B$ si y sólo si $x = a$ o $x = b$. Si $a = b$ y sólo en este caso será $\{a, b\} = \{a\}$. De la misma manera, si $a_1, a_2, \dots, a_n$ son objetos, $A = \{a_1, a_2, \dots, a_n\}$ denotará el conjunto cuyos elementos son $a_1, a_2, \dots, a_n$. Entonces $x \in A$ si y sólo si $x = a_i$ para algún $i = 1, 2, \dots, n$. Si $P(x)$ es una condición sobre una variable x y existe un conjunto A tal que $a \in A$ si y sólo si $P(a)$ es una afirmación verdadera, usaremos las notaciones $A = \{x : P(x)\}$ o $A = \{x \mid P(x)\}$ para representar tal conjunto. Se dice que A es el *conjunto de los objetos que verifican* $P(x)$ y que $P(x)$ es una *relación colectivizante*, es decir, *que forma conjunto*. Véase, al respecto, la nota *relación colectivizante* 1.5. Así, $\{a\} = \{x : x = a\}$, $\{a, b\} = \{x : x = a \text{ o } x = b\}$, de tal manera que " $x = a$ " y " $x = a \text{ o } x = b$ " son colectivizantes. Si $P(x)$ es una condición en x y X es un conjunto, admitiremos que el conjunto A de los objetos que verifican la condición " $x \in X$ y $P(x)$ " siempre existe y es un subconjunto de X ; es decir, admitiremos que " $x \in X$ y $P(x)$ " es siempre colectivizante. En lugar de $A = \{x : x \in X \text{ y } P(x)\}$ es corriente escribir $A = \{x \in X : P(x)\}$. Denotaremos con $\emptyset$ el *conjunto vacío*, el cual es un conjunto sin elementos.

La razón de introducir un conjunto vacío es en muchos aspectos análoga a la de introducir el número 0 en la aritmética elemental. Permite además interpretar 0, en forma semejante a 1, 2, 3, etc., como el número de elementos (cardinal) de un conjunto: 0 es el número de elementos de $\emptyset$. Evidentemente

$\emptyset$ es un subconjunto de cualquier conjunto A (pues de no ser así, existiría $a \in \emptyset$ tal que $a \notin A$, lo cual es absurdo). Esto asegura que existe un único conjunto vacío (pues si hay dos, $\emptyset$ y $\emptyset'$, con el mismo argumento anterior se verifica que $\emptyset \subseteq \emptyset'$ y $\emptyset' \subseteq \emptyset$). Decir que $A = \emptyset$ es equivalente a decir que *no existe ningún objeto a tal que* $a \in A$. A su vez, $A \neq \emptyset$ garantiza la *existencia de un a tal que* $a \in A$. Claramente $A = \emptyset$ si y sólo si $A \subseteq \emptyset$. Si no existe un objeto a tal que $P(a)$ sea verdadera, admitiremos que $P(x)$ es colectivizante y que $\{x : P(x)\} = \emptyset$. Por ejemplo, $\{x : x \neq x\} = \emptyset$. Si A y B son conjuntos, $A \cup B$ (la *unión* de A y B) será el *conjunto de los objetos que están al menos en uno de* A o B , esto es $A \cup B = \{x : x \in A \text{ o } x \in B\}$, y $x \in A \cup B$ si y sólo si $x \in A$ ó $x \in B$. A su vez, $A \cap B$ (la *intersección* de A y B) será el *conjunto de los elementos comunes a* A y B , esto es $A \cap B = \{x : x \in A \text{ y } x \in B\}$, y $x \in A \cap B$ si y sólo si $x \in A$ y $x \in B$. Si $A \cap B = \emptyset$, se dice que A y B son *conjuntos disyuntos*. Claramente $A \subseteq A \cup B$ y $B \subseteq A \cup B$, $A \cap B \subseteq A$ y $A \cap B \subseteq B$.

Otras propiedades son:

$$\begin{aligned} 1. & A \cup A = A, A \cap A = A, A \cup B = B \cup A, \\ & A \cap B = B \cap A, A \cup \emptyset = A, A \cap \emptyset = \emptyset, \\ 2. & A \cup B = A \text{ si y sólo si } B \subseteq A, \\ & A \cap B = B \text{ si y sólo si } B \subseteq A, \\ 3. & A \cup (B \cup C) = (A \cup B) \cup C, \\ & A \cap (B \cap C) = (A \cap B) \cap C, \\ 4. & A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \\ & A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \end{aligned} \tag{1.1}$$

Si A y B son conjuntos, $A \setminus B$, la *diferencia* de A y B , el conjunto A *menos* B , o el *complemento de* B en A , será el *conjunto de los elementos de* A que *no están en* B , esto es $A \setminus B = \{x \in A : x \notin B\}$, y $x \in A \setminus B$ si y sólo si $x \in A$ y $x \notin B$. Claramente $A \setminus A = \emptyset$, $A \setminus \emptyset = A$, $A \setminus B = A \setminus (A \cap B)$, $A \setminus B = \emptyset$ si y sólo si $A \subseteq B$. Si A y B son subconjuntos de X , $A \cap B = \emptyset$ si y sólo si $A \subseteq X \setminus B$. Además,

$$\begin{aligned} 1. & X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B), \\ 2. & X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B). \end{aligned} \tag{1.2}$$

Verificaremos la segunda de tales igualdades: si $x \in X \setminus (A \cap B)$ entonces $x \in X$ y $x \notin (A \cap B)$, así que $x \in X$ y $x \notin A$ o $x \notin B$; esto es $x \in X \setminus A$ o $x \in X \setminus B$, y entonces $x \in (X \setminus A) \cup (X \setminus B)$; recíprocamente, si $x \in (X \setminus A) \cup (X \setminus B)$, se tendrá que $x \in X \setminus A$ o $x \in X \setminus B$, de lo cual $x \in X$ y $x \notin A$ o $x \notin B$; esto implica que $x \in X$ y $x \notin (A \cap B)$, de lo cual $x \in X \setminus (A \cap B)$.

Definición 1.1. Si a y b son objetos,

$$(a, b) := \{\{a\}, \{a, b\}\} \quad (1.3)$$

será la *pareja ordenada de primera coordenada a y segunda coordenada b* .

Teorema 1.1. $(a, b) = (c, d)$ si y sólo si $a = c$ y $b = d$.

Demostración. La condición es obviamente suficiente. Para ver que es necesaria, supongamos primero $a = b$, así que $(a, b) = \{\{a\}\}$. Como $\{c, d\} \in (a, b)$, será $\{c, d\} = \{a\}$, así que $c = d = a$. Esto implica $a = c$ y $b = d$. Supongamos ahora $a \neq b$. Claramente $\{a\} = \{c\}$, así que $a = c$. Por otra parte $\{a, b\} = \{c, d\}$, así que $d = a$ o $d = b$. Pero, si fuera $d = a$ se tendría que $d = c$, de lo cual, por el argumento anterior, sería $a = b = c = d$. Entonces $d \neq a$, y deberá ser $d = b$. $\square$

Se deduce que, en general, $(a, b) \neq (b, a)$. De hecho, $(a, b) = (b, a)$ si y sólo si $a = b$.

Definición 1.2. Si X y Y son conjuntos, el conjunto

$$X \times Y := \{(x, y) : x \in X, y \in Y\} \quad (1.4)$$

se denomina el *producto cartesiano* de X y Y .

Evidentemente $\emptyset \times Y = X \times \emptyset = \emptyset$. En general $X \times Y \neq Y \times X$.

Si $a_1, a_2, \dots, a_n$ son objetos, $n > 2$, se define “inductivamente”

$$(a_1, a_2, \dots, a_n) = ((a_1, a_2, \dots, a_{n-1}), a_n). \quad (1.5)$$

El conjunto $(a_1, a_2, \dots, a_n)$ se denomina la *n -pla ordenada de coordenadas $a_1, a_2, \dots, a_n$* . En particular, $(a, b, c) = ((a, b), c)$ será la *tripla ordenada de coordenadas a, b, c* . Como es natural, diremos que la pareja (a, b) será la *dupla ordenada de coordenadas a, b* . Se tiene que $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$ si y sólo si $a = b_1, a_2 = b_2, \dots, a_n = b_n$. Si $X_1, X_2, \dots, X_n, n \geq 2$, son conjuntos, $X_1 \times X_2 \times \dots \times X_n$ será el conjunto de las *n -plas ordenadas $(x_1, x_2, \dots, x_n)$* donde $x_i \in X_i, i = 1, 2, \dots, n$. Si $n > 2$, podemos considerar que $X_1 \times X_2 \times \dots \times X_n = (X_1 \times X_2 \times \dots \times X_{n-1}) \times X_n$.

Definición 1.3. Un subconjunto G de $X \times Y$ se denomina una *gráfica*. Si $G \subseteq X \times Y$ es una gráfica y $x \in X$, el *corte de G con x* , $G(x)$, es

$$G(x) := \{y \in Y : (x, y) \in G\}. \quad (1.6)$$

Definición 1.4. Si $G \subseteq X \times Y$ es una gráfica, se dice que la tripla $R = (X, G, Y)$ es una *relación entre elementos de X y de Y* . Se dice entonces que G es la *gráfica de R* . El conjunto X se denomina el *conjunto de definición* o de *partida* de R y Y , el de *llegada*. Si $(x, y) \in G$, es usual escribir xRy y decir que x y y están relacionados por R .

Los conjuntos

$$\text{Dom}(R) := \{x \in X : G(x) \neq \emptyset\}, \quad \text{Cod}(R) := \bigcup_{x \in X} G(x) \quad (1.7)$$

(así que $\text{Dom}(R) = \{x \in X : \text{existe } y \in Y \text{ con } (x, y) \in G\}$ y $\text{Cod}(R) = \{y \in Y : \text{existe } x \in X \text{ con } (x, y) \in G\}$), se denominan respectivamente el *dominio* y el *codominio* de R . Si para todo $x \in X$, $G(x)$ es vacío o se reduce a un punto, se dice que G es una *gráfica funcional* y que R es una *relación funcional*. Esto equivale a decir que no existen en G dos parejas distintas con la misma primera coordenada, o, lo que es lo mismo, que si xRy y xRy' entonces $y = y'$. Puede suceder, sin embargo, que exista $x \in X$ que no figure en ninguna pareja de G , es decir, que $G(x) = \emptyset$, así que es posible que $\text{Dom}(R) \neq X$.

Definición 1.5. Si $f = (X, G, Y)$ es una relación funcional y $\text{Dom}(f) = X$, se dice que f es una *aplicación* o una *función* de X en Y .

Si $f = (X, G, Y)$ es una función de X en Y , es usual escribir simplemente $f : X \rightarrow Y$, sin mencionar a G . La razón para esto radica en que G puede describirse fácilmente en términos de f . En efecto, para todo $x \in X$, $G(x)$ tiene un único elemento, el cual se denomina la *imagen de x por f* y se denota con $f(x)$, así que $G(x) = \{f(x)\}$, y entonces $G = \{(x, f(x)) : x \in X\}$. Intuitivamente, una *función $f : X \rightarrow Y$* es una *ley que a cada $x \in X$ asigna un único elemento $f(x) \in Y$* (una máquina que transforma a x en $f(x)$). La noción de función que hemos dado, aunque menos “dinámica” que esta interpretación intuitiva, contiene, sin embargo, toda la información pertinente acerca de ésta: conjunto de definición, conjunto de llegada, gráfica, dominio, codominio, etc. De hecho, cuando a una persona se le pide que hable de una función, su primer impulso es generalmente el de fijar su dominio y dibujar su gráfica.

Si $A \subseteq X, B \subseteq Y$ y $f : X \rightarrow Y$ es una función,

$$f(A) := \{f(x) \in Y : x \in A\}, \quad f^{-1}(B) := \{x \in X : f(x) \in B\}$$

se denominan respectivamente la *imagen directa* de A y la *imagen recíproca* de B por f . Obviamente $y \in f(A)$ si y sólo si existe $x \in A$ tal que $y = f(x)$ (lo cual no excluye que exista $x' \notin A$ tal que $y = f(x')$, así que $f(x) \in f(A)$ no garantiza que $x \in A$), y $x \in f^{-1}(B)$ si y sólo si $f(x) \in B$.

Es claro que $\text{Dom}(f) = f^{-1}(Y)$ y $\text{Cod}(f) = f(X)$. Es costumbre en este último caso denominar también a $f(X)$ la *imagen* o el *recorrido* de f y denotarlos con $\text{Im}(f)$. Si $\text{Im}(f) = Y$, se dice que f es *sobreyectiva*. Decir que f es *sobreyectiva* equivale entonces a decir que todo elemento de Y es la imagen de algún elemento de X , es decir, que para todo $y \in Y$ existe $x \in X$ tal que $y = f(x)$.

Si $B = \{b\}$, es frecuente escribir simplemente $f^{-1}(b)$ en lugar de $f^{-1}(B)$ (o sea, de $f^{-1}(\{b\})$). Esto puede ser causa de confusión y lo evitaremos, pero es una práctica usual.

Si $a \in \text{Dom}(f)$, se dice que f está definida en a ; si $A \subseteq \text{Dom}(f)$, que f está definida en A o sobre A .

Si $f : X \rightarrow Y$ y $g : Y \rightarrow Z$, $g \circ f : X \rightarrow Z$ es la función dada por

$$g \circ f(x) := g(f(x)), \quad x \in X. \quad (1.8)$$

Si $f = (X, G, Y)$ y $g = (Y, G', Z)$, la gráfica de $g \circ f$ se denota con $G' \circ G$. Nótese que

$$G' \circ G = \{(x, g(f(x))) : x \in X\}$$

y $g \circ f = (X, G' \circ G, Z)$. Se dice que $g \circ f$ es la *función compuesta* de g y f y que $G' \circ G$ es la *gráfica compuesta* de sus respectivas gráficas.

Si $G \subseteq X \times Y$ es una gráfica,

$$G^{-1} := \{(y, x) : (x, y) \in G\} \subseteq Y \times X \quad (1.9)$$

es también una gráfica, denominada la *gráfica inversa* de G . Si $R = (X, G, Y)$, $R^{-1} := (Y, G^{-1}, X)$ se denomina la *relación inversa* de R . Si $f = (X, G, Y)$ es una función y G^{-1} es una gráfica funcional, o sea, si $(y, x), (y, x') \in G^{-1}$ implican $x = x'$, o, lo que es lo mismo, si $f(x) = f(x')$ implica $x = x'$, se dice que f es una *aplicación* o una *función inyectiva* de X en Y . Aún si f es inyectiva, puede ser que $f^{-1} = (Y, G^{-1}, X)$ no sea una función, pues puede suceder que $\text{Dom}(f^{-1}) = f(X) \neq Y$.

Si tanto f como f^{-1} son funciones, lo cual ocurre si y sólo si f es tanto *sobreyectiva* como *inyectiva*, en cuyo caso se dice que f es *biyectiva*, f^{-1} se denomina la *función inversa* de f . Nótese que entonces $y = f(x)$ es equivalente a $f^{-1}(y) = x$. Además, $f^{-1} \circ f(x) = x$ y $f \circ f^{-1}(y) = y$, cualesquiera que sean $x \in X, y \in Y$.

Si Z es un conjunto, $\Delta_Z = \{(z, z) : z \in Z\}$ se denomina la *diagonal* de Z (o, más precisamente, de $Z \times Z$). Evidentemente Δ_Z es una gráfica funcional, e $i_Z = (Z, \Delta_Z, Z)$ es una función, que se denomina la *función idéntica* de Z . Nótese que $i_Z(x) = x$ para todo $x \in Z$. Como es claro, $\Delta_Z^{-1} = \Delta_Z$ e $i_Z^{-1} = i_Z$. Si $f : X \rightarrow Y$ es biyectiva, así que $f^{-1} : Y \rightarrow X$ es también una función, se tiene entonces que $f^{-1} \circ f = i_X$ y $f \circ f^{-1} = i_Y$. En tal caso, f^{-1} es también biyectiva y $(f^{-1})^{-1} = f$.

Nota 1.1. Al definirlos, hemos admitido implícitamente que garantizada la existencia de los conjuntos X, Y y de los objetos a, b , podemos garantizar la existencia de los conjuntos $X \cup Y, X \cap Y, X \setminus Y, \{a\}, \{a, b\}, (a, b), X \times Y$, etc. También hemos admitido, menos evidentemente, que si X y Y son conjuntos no vacíos y existe alguna regla que a cada elemento $x \in X$ asocia un único elemento $\tau(x)$ de Y , existe entonces $f : X \rightarrow Y$ tal que $f(x) = \tau(x)$. En efecto, podemos formar, según lo dicho en el cuarto párrafo de esta sección, el conjunto $G = \{(x, y) : (x, y) \in X \times Y \text{ y } y = \tau(x)\}$ y la tripla (X, G, Y) .

Nota 1.2. La notación f^{-1} para la función inversa de f puede ser causa de alguna confusión. Por ejemplo, de acuerdo con la práctica usual, si $b \in Y$, $f^{-1}(b)$ denota a la vez el conjunto $f^{-1}(b)$ y a su único elemento. Esperamos que el contexto evite siempre esta posible confusión. Análogamente, es quizá más natural llamar corte de una gráfica $G \subseteq X \times Y$ con un punto $x \in X$ al conjunto $\{x\} \times G(x)$ que al $G(x)$ (hágase un dibujo), pero las convenciones de lenguaje son difíciles de cambiar. Además, $G(x)$ es más útil que $\{x\} \times G(x)$. Si X es un conjunto, $f = (\emptyset, \emptyset, X)$ es una aplicación inyectiva de $\emptyset$ en X (pues no existen $x, x' \in \emptyset, x \neq x'$, tales que $f(x) = f(x')$). Si $X = \emptyset, f = f^{-1} = i_\emptyset$ es la única aplicación de $\emptyset$ sobre sí mismo, y es biyectiva.

Nota 1.3. Si $R = (X, G, Y)$ es una relación y $R^{-1} = (Y, G^{-1}, X)$ es su relación inversa, es claro que $\text{Dom}(R^{-1}) = \text{Cod}(R)$ y que $\text{Cod}(R^{-1}) = \text{Dom}(R)$. Para una relación $R = (X, G, Y)$ puede suceder que $G(x) = \emptyset$ para algún $x \in X$ (en cuyo caso $x \notin \text{Dom}(R)$ y $\text{Dom}(R) \neq X$) o que

$G(x)$ contenga más de un punto. En general $\text{Cod}(R) \neq Y$, aún si R es una función. Si R es una relación funcional, $(\text{Dom}(R), G, Y)$ es una función.

Nota 1.4. Sean X, Y conjuntos, $X \neq \emptyset \neq Y$. Entonces podemos garantizar, según lo dicho en la nota 1.1, que existen $a \in X$ y $b \in Y$, de lo cual, también $(a, b) \in X \times Y$, así que $X \times Y \neq \emptyset$. Recíprocamente, si $X \times Y \neq \emptyset$, existe $(a, b) \in X \times Y$, de lo cual $a \in X$, $b \in Y$, y entonces $X \neq \emptyset \neq Y$. Inductivamente se verifica también que si $n > 2$, $X_1 \times \cdots \times X_n = \emptyset$ si y sólo si $X_i = \emptyset$ para algún $i = 1, 2, \dots, n$.

Nota 1.5. La noción intuitiva de conjunto, tal como la hemos presentado hasta el momento (véase [14] para un tratamiento similar) puede conducir a inconsistencias (contradicciones) desagradables. Por ejemplo, el suponer descuidadamente que cualquier relación es colectivizante implica en particular que la relación $x \notin x$ lo es, lo cual nos lleva a hablar del "conjunto" $A = \{x : x \notin x\}$, el cual conduce a la contradicción $A \in A$ si y sólo si $A \notin A$. Naturalmente, podemos salir del impase diciendo simplemente que $x \notin x$ no es colectivizante, así que no existe un conjunto A tal que $a \in A$ si y sólo si $a \notin a$. Pero entonces ¿es colectivizante la relación $x = x$? Es decir, ¿existe un conjunto A tal que $A = \{x : x = x\}$? El admitirlo, de hecho, nos lleva también a contradicciones. Para evitar esta incertidumbre, lo más conveniente es imponer ciertas limitaciones a la noción intuitiva de conjunto, lo cual se hace exigiendo que éstos satisfagan ciertas restricciones, llamadas axiomas o postulados de los conjuntos. Uno de estos axiomas es el siguiente, que no sólo evita ciertas contradicciones, sino que tiene otras consecuencias útiles (véase el ejercicio 1.11):

Axioma de los conjuntos (A.C.). Si X es un conjunto, $X \neq \emptyset$, existe $A \in X$ tal que $A \cap X = \emptyset$.

Por ejemplo, del axioma (A.C.) se deduce que si A es un conjunto entonces $A \notin A$. En efecto, si $A \in A$ y $X = \{A\}$, no podría existir $B \in X$ tal que $B \cap X = \emptyset$, pues necesariamente serían $B = A$ y $B \cap X = \{A\} \neq \emptyset$. Tal axioma implica de paso que dado un conjunto A siempre existe un objeto a tal que $a \notin A$ (tómese $a = A$), lo cual puede ser importante. Del Axioma (A.C.) se deduce que la relación $x \notin x$ no es colectivizante. En efecto, si $A = \{x : x \notin x\}$ fuera un conjunto, dado que $A \notin A$, se tendría que $A \in A$, lo cual es absurdo. De la misma manera se verifica (ejercicio 1.11) que $x = x$ no es colectivizante. Nosotros no proseguiremos esta discusión, la cual es el objeto de las teorías axiomáticas de los conjuntos (véanse [9], [19], [24], [5]).

Definición 1.6. Si X es un conjunto, el conjunto de los subconjuntos de X es

$$\wp(X) := \{A : A \subseteq X\}. \quad (1.10)$$

Claramente $\emptyset, X \in \wp(X)$, con $\wp(\emptyset) = \{\emptyset\}$. El conjunto $\wp(X)$ se conoce también como el conjunto de las partes de X .

Definición 1.7. Una familia de conjuntos con índices en el conjunto I es un aplicación $f : I \rightarrow C$, donde C es un conjunto (clase) de conjuntos. Si $A_i = f(i)$, es usual escribir $f = (A_i)_{i \in I}$.

Si $(A_i)_{i \in I}$ es una familia de conjuntos, $\bigcup_{i \in I} A_i$ (la unión de los A_i) será el conjunto de los elementos que están al menos en uno de los A_i (con $\bigcup_{i \in I} A_i = \emptyset$ si $I = \emptyset$). Decir entonces que $x \in \bigcup_{i \in I} A_i$ es equivalente a decir que existe $i \in I$ tal que $x \in A_i$. A su vez, si $I \neq \emptyset$, $\bigcap_{i \in I} A_i$ (la intersección de los A_i) será el conjunto de aquellos objetos que están en todos los A_i , y decir que $x \in \bigcap_{i \in I} A_i$ es equivalente a afirmar que $x \in A_i$ para todo $i \in I$. Las relaciones

$$\begin{aligned} 1. \quad X \setminus \bigcup_{i \in I} A_i &= \bigcap_{i \in I} (X \setminus A_i), \\ 2. \quad X \setminus \bigcap_{i \in I} A_i &= \bigcup_{i \in I} (X \setminus A_i), \end{aligned} \quad (1.11)$$

válidas si $I \neq \emptyset$, y conocidas como leyes de De Morgan, serán útiles en el futuro. Verificaremos la primera de ellas. El argumento es típico de los usados para este tipo de comprobación: sea $x \in X \setminus \bigcup_{i \in I} A_i$; entonces $x \in X$ y $x \notin \bigcup_{i \in I} A_i$, así que $x \in X$ y, para todo $i \in I$, $x \notin A_i$; entonces $x \in X \setminus A_i$ para todo $i \in I$, y será $x \in \bigcap_{i \in I} (X \setminus A_i)$; recíprocamente, si $x \in \bigcap_{i \in I} (X \setminus A_i)$, será $x \in X \setminus A_i$ para todo $i \in I$, y, por lo tanto, $x \in X$ y, para todo $i \in I$, $x \notin A_i$; se concluye que $x \in X$ y $x \notin \bigcup_{i \in I} A_i$, así que $x \in X \setminus \bigcup_{i \in I} A_i$.

Nota 1.6. Tal como en la nota 1.1, admitimos que al definir un conjunto a partir de ciertos objetos o de otros conjuntos, este conjunto existe (aunque puede ser vacío). Así, si X es un conjunto, $\wp(X)$ existe y es un conjunto, y si I y los A_i , $i \in I$, son conjuntos, también $\bigcup_{i \in I} A_i$ y $\bigcap_{i \in I} A_i$ son conjuntos, éste último si $I \neq \emptyset$. Si $I = \emptyset$, $\bigcap_{i \in I} A_i$ no está definido; sin embargo, frecuentemente se conviene en darle cierto significado: por ejemplo, si todos los A_i son subconjuntos de un mismo conjunto X , es usual (y en cierta forma natural) tomar $\bigcap_{i \in \emptyset} A_i = X$ (pues si $x \in X$, no existe $i \in I$ tal que $x \notin X_i$).

1.2. Los números reales

Supondremos que el lector está familiarizado en alguna medida con las propiedades básicas del sistema $(\mathbb{R}, +, \cdot, \mathbb{R}_+)$ de los números reales. Este sistema se define pidiendo en primer lugar que la adición (+) y la multiplicación ($\cdot$) sean *leyes de composición interna en $\mathbb{R}$* , el llamado *conjunto de los números reales* (es decir, que sean aplicaciones de $\mathbb{R} \times \mathbb{R}$ en $\mathbb{R}$). Así que $x+y$ y $x \cdot y$ (es también costumbre escribir xy en lugar de $x \cdot y$) son números reales si x y y lo son. Se pide además que existan en $\mathbb{R}$ dos elementos privilegiados distintos 0 y 1 tales que

$$x + 0 = x, \quad x \cdot 1 = x, \quad x \in \mathbb{R}; \quad (1.12)$$

que para todo $x \in \mathbb{R}$ exista $(-x) \in \mathbb{R}$ tal que

$$x + (-x) = 0 \quad (1.13)$$

y también, cuando $x \neq 0$, exista x^{-1} tal que

$$x \cdot x^{-1} = 1. \quad (1.14)$$

Se pide finalmente que tales leyes satisfagan las relaciones

$$\begin{aligned} 1. \quad x + (y + z) &= (x + y) + z, \\ 2. \quad x + y &= y + x, \end{aligned} \quad (1.15)$$

$$\begin{aligned} 3. \quad x \cdot (y \cdot z) &= (x \cdot y) \cdot z, \\ 4. \quad x \cdot y &= y \cdot x, \end{aligned} \quad (1.16)$$

$$5. \quad x \cdot (y + z) = x \cdot y + x \cdot z. \quad (1.17)$$

Se dice entonces que 0 es el *elemento neutro aditivo* y que $(-x)$ es el *inverso aditivo* de x . La ecuación $a + x = b$ tendrá entonces la única solución $x = b + (-a)$ (la cual se denota también con $b - a$), pues $a + (b + (-a)) = (a + (-a)) + b = 0 + b = b$, de lo cual $c = b - a$ es solución. La unicidad resulta de observar que si también $a + c = a + c'$, entonces $c = c'$, ya que $c = (-a) + (a + c) = ((-a) + a) + c' = 0 + c' = c'$, lo cual se conoce como *ley de cancelación de la adición*. Se deduce que si $a + x = a$, necesariamente $x = 0$, y si $a + x = 0$ entonces $x = (-a)$. En particular, $-(-a) = a$, pues ambos, a y $-(-a)$, son soluciones de $(-a) + x = 0$.

De $a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 = a \cdot 0$ se deduce que $a \cdot 0 = 0$ cualquiera que sea $a \in \mathbb{R}$ (pues ambos, $a \cdot 0$ y 0 resuelven la ecuación $a \cdot 0 + x = a \cdot 0$). Entonces

$(-a)b = -ab$, ya que ambos $(-a)b$ y $-ab$ son soluciones de $ab + x = 0$. De la misma manera $a(-b) = -ab$, y también $(-a)(-b) = ab$, ya que ambos resuelven $(-a)b + x = 0$. Por otra parte, $x \cdot y \neq 0$ si $x \neq 0$ y $y \neq 0$, pues $x \cdot y = 0$ implica, si $y \neq 0$, que $(x \cdot y) \cdot y^{-1} = 0 \cdot y^{-1} = 0 = x \cdot (y \cdot y^{-1}) = x \cdot 1 = x$. Esto garantiza que $(\cdot)$ es una ley de composición interna en $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ (es decir, una aplicación de $\mathbb{R}^* \times \mathbb{R}^*$ en $\mathbb{R}^*$). Si $a \in \mathbb{R}^*$, la ecuación $ax = b$ tendrá entonces la solución única $x = ba^{-1} = a^{-1}b$ (escrita también $c = \frac{b}{a}$ o $c = b/a$). En efecto, $a(a^{-1}b) = (aa^{-1})b = 1b = b$, y si también $ac = ac'$ entonces $c = a^{-1}(ac') = (a^{-1}a)c' = c'$ (propiedad cancelativa de la multiplicación). Nótese que si $a \neq 0$ entonces $a/a = 1$ y $1/a = a^{-1}$. Además, si $a \neq 0$ entonces $a^{-1} \neq 0$ (pues $a \cdot a^{-1} = 1 \neq 0$) y $(a^{-1})^{-1} = a$, pues ambos resuelven $a^{-1}x = 1$; y si también $b \neq 0$, entonces $(ab)^{-1} = b^{-1}a^{-1}$, pues $b^{-1}a^{-1}$ y $(ab)^{-1}$ son ambos solución de $(ab)x = 1$. Se dice que 1 es el *elemento neutro multiplicativo* y, si $a \neq 0$, que a^{-1} es el *inverso multiplicativo* de a .

Las relaciones (1.12) a (1.17) se conocen como los *axiomas algebraicos* de $\mathbb{R}$. La *estructura de orden* de $\mathbb{R}$ está determinada por el conjunto $\mathbb{R}_+$ de los números reales positivos. Si para $A, B \subseteq \mathbb{R}$ definimos

$$\begin{aligned} A + B &:= \{x + y : x \in A, y \in B\}, \\ AB &:= \{xy : x \in A, y \in B\}, \\ -A &:= \{-x : x \in A\}, \end{aligned}$$

se pide que el conjunto $\mathbb{R}_+$ tenga las propiedades fundamentales siguientes:

$$\begin{aligned} 1. \quad \mathbb{R}_+ \cap (-\mathbb{R}_+) &= \{0\}, \\ 2. \quad \mathbb{R} &= \mathbb{R}_+ \cup (-\mathbb{R}_+), \\ 3. \quad \mathbb{R}_+ + \mathbb{R}_+ &\subseteq \mathbb{R}_+, \\ 4. \quad \mathbb{R}_+ \mathbb{R}_+ &\subseteq \mathbb{R}_+. \end{aligned} \quad (1.18)$$

Estas relaciones se conocen como los *axiomas algebraicos del orden* de $\mathbb{R}$ (posteriormente daremos otro axioma de orden, de naturaleza más compleja). Si $a, b \in \mathbb{R}$, la notación $a \leq b$ (léase *a es menor o igual que b*) significará que $b - a \in \mathbb{R}_+$, y la $a \geq b$ (léase *a es mayor o igual que b*), que $b \leq a$. Como es claro, $a \geq 0$ equivale a que $a \in \mathbb{R}_+$. Decir que $a \in (-\mathbb{R}_+)$ es equivalente a decir que $a = -b$, $b \in \mathbb{R}_+$, o, lo que es lo mismo, a que $-a \in \mathbb{R}_+$; esto último equivale, dado que $-a = 0 - a$, a que $a \leq 0$, y se dice en tal caso que a es un *número real negativo*. $\mathbb{R}_- := (-\mathbb{R}_+)$ se denomina el *conjunto de los números reales negativos*. Es útil recordar que si $a \in \mathbb{R}$

entonces $a \in \mathbb{R}_+$ o $a \in \mathbb{R}_-$, y que $a \in \mathbb{R}_-$ si y sólo si $(-a) \in \mathbb{R}_+$, $a \in \mathbb{R}_+$ si y sólo si $(-a) \in \mathbb{R}_-$. Las dos primeras propiedades en (1.18) se traducen en

1. Si $a \leq 0$ y $a \geq 0$, entonces $a = 0$.
 2. Si $a \in \mathbb{R}$, entonces $a \leq 0$ ó $a \geq 0$.
- (1.19)

Las dos últimas se sintetizan en

$$\text{Si } a \geq 0 \text{ y } b \geq 0, \text{ entonces } a + b \geq 0, ab \geq 0. \quad (1.20)$$

Las afirmaciones en (1.19) son aún respectivamente equivalentes a las

$$\text{Si } a \leq b \text{ y } b \leq a, \text{ entonces } a = b, \quad (1.21)$$

y

$$\text{Dados } a, b \in \mathbb{R}, \quad a \leq b \text{ ó } b \leq a, \quad (1.22)$$

lo cual se verifica inmediatamente.

Teorema 1.2. La relación $\leq$ tiene además las siguientes propiedades:

1. $a \leq a$,
 2. Si $a \leq b$ y $b \leq c$, entonces $a \leq c$,
- (1.23)

cualesquiera que sean a, b, c en $\mathbb{R}$.

Demostración. (1) es clara, pues $a - a = 0 \in \mathbb{R}_+$. Ahora, las hipótesis de (2) garantizan que $b - a$ y $c - b$ están en $\mathbb{R}_+$, y como $c - a = (c - b) + (b - a)$, (1.20) asegura que $c - a \in \mathbb{R}_+$. $\square$

Nota 1.7. Las afirmaciones (1.21) y (1.23) expresan que $\leq$ es una *relación de orden*. Si se añade (1.22), esta relación es lo que se conoce como una *relación de orden total* o un *orden lineal* (dos elementos cualesquiera de $\mathbb{R}$ están siempre relacionados o son siempre comparables). La relación (1.20) expresa que $\leq$ es en cierta forma compatible con la adición y la multiplicación.

Nota 1.8. Para un número real a se tiene que $a \in \mathbb{R}_+$ o $(-a) \in \mathbb{R}_+$. Esto implica que $a^2 = a \cdot a \in \mathbb{R}_+$, pues $a^2 = a \cdot a = (-a)(-a)$. En particular, $1 = 1 \cdot 1 \in \mathbb{R}_+$. Nótese que si $a \in (-\mathbb{R}_+)$ y $b \in \mathbb{R}_+$ entonces $a \leq b$ (pues $a \leq 0$ y $0 \leq b$).

Nota 1.9. Si $a, b \in \mathbb{R}$, $a < b$ (léase a es estrictamente menor que b) significa que $a \leq b$ y $a \neq b$. Como es claro, $a \leq b$ si y sólo si $a < b$ o $a = b$. En

lugar de $a < b$ es también corriente escribir $b > a$ (léase b es estrictamente mayor que a). Si $a > 0$, se dice que a es *estrictamente positivo*. Si $a < 0$, que a es *estrictamente negativo*.

Si A es un subconjunto de $\mathbb{R}$, un elemento a de $\mathbb{R}$ tal que $a \geq x$ para todo $x \in A$ se denomina una *cota superior* de A (si $a \leq x$ para todo $x \in A$, a es una *cota inferior* de A). Si $a \in A$ y es cota superior de A , se dice que a es un *máximo* de A (un *mínimo* si $a \in A$ y es cota inferior de A). Si a, b son ambos máximos o mínimos de A , $a \leq b$ y $b \leq a$, así que $a = b$. Es decir, un conjunto A tiene, si lo tiene, un único máximo: $\max A$ (y, también un único mínimo: $\min A$). Si $a, b \in \mathbb{R}$, es claro que $\max\{a, b\} = a$ o $\max\{a, b\} = b$. De igual manera, $\min\{a, b\} = a$ o $\min\{a, b\} = b$.

Si $A \subseteq \mathbb{R}$, A^+ denotará el conjunto de las cotas superiores de A y A^- el de sus cotas inferiores. Decir que $a \in A^+$ (respectivamente, $a \in A^-$) es equivalente a decir que no existe $b \in A$ tal que $a < b$ (respectivamente, $b < a$). Por ejemplo, $\mathbb{R}^+ = \mathbb{R}_+^+ = \emptyset$ (si $a \in \mathbb{R}$, no puede ser $a \geq x$ para todo $x \in \mathbb{R}_+$, pues serían $a \in \mathbb{R}_+$, $a + 1 \in \mathbb{R}_+$ y $a + 1 \leq a$, lo cual es absurdo). También $\mathbb{R}^- = \emptyset$, y $\emptyset^+ = \emptyset^- = \mathbb{R}$ (pues dado $a \in \mathbb{R}$, no existe $b \in \emptyset$ tal que $a < b$ o $b < a$). Por otra parte, $(-\mathbb{R}_+)^+ = \mathbb{R}_+$, $\mathbb{R}_+^- = -\mathbb{R}_+$, y 0 es máximo de $(-\mathbb{R}_+)$ y mínimo de $\mathbb{R}_+$.

Definición 1.8. Si $A \subseteq \mathbb{R}$ y $A^+ \neq \emptyset$, se dice que A es *acotado superiormente* (respectivamente, *inferiormente*, si $A^- \neq \emptyset$). Si $A^+ \neq \emptyset \neq A^-$, se dice que A es *acotado*.

Teorema 1.3. Un subconjunto A de $\mathbb{R}$ es acotado si y sólo si existe $a \geq 0$ tal que $-a \leq x \leq a$ para todo $x \in A$.

Demostración. Supóngase que A es acotado. Si $A = \emptyset$, sea $a = 1$ (como no existe $x \in A$ tal que $x > 1$ o que $x < -1$, entonces $-1 \leq x \leq 1$ para todo $x \in A$). Si existe $x \in A$, sean $c \in A^+$, $d \in A^-$. Como $d \leq x$ y $c \geq x$ entonces $d \leq c$. Sea entonces a el máximo de $\{-d, c\}$: $a = \max\{-d, c\}$. Como $c \leq a$, es claro que $x \leq a$ para todo $x \in A$. A su vez, $-x \leq -d \leq a$ para todo $x \in A$, así que $x \geq -a$ para tales x . Lo recíproco es trivial. $\square$

Definición 1.9. Si $a \in \mathbb{R}$, el *valor absoluto* de a es $|a| := \max\{a, -a\}$.

Nótese que si $a \in \mathbb{R}$, $a \leq \max\{a, b\}$, $b \leq \max\{a, b\}$. Como $|a| = \max\{a, -a\}$, es claro entonces que $a \leq |a|$ y $-a \leq |a|$. Por lo tanto,

$$1. -|a| \leq a \leq |a|.$$

De 1, se deduce que $|a| \geq -|a|$, de modo que

$$2. |a| \geq 0.$$

Evidentemente $|0| = \max\{0, 0\} = 0$. Por otra parte, de 1, se tiene que si $|a| = 0$ entonces $0 \leq a \leq 0$, de modo que $a = 0$. En resumen,

$$3. |a| = 0 \text{ si y sólo si } a = 0.$$

Como $\max\{-(-a), -a\} = \max\{a, -a\}$, se tiene que

$$4. |-a| = |a|.$$

Si $|a| \leq b$ entonces $\max\{-a, a\} \leq b$, así que $-a \leq b$ y $a \leq b$, o sea $-b \leq a \leq b$. Por otra parte, si $-b \leq a \leq b$ entonces $-a \leq b$ y $a \leq b$, de lo cual $|a| = \max\{-a, a\} \leq b$. Luego

$$5. |a| \leq b \text{ si y sólo si } -b \leq a \leq b.$$

Como evidentemente, de (1), $-(|a| + |b|) \leq a + b \leq |a| + |b|$, se obtiene que

$$6. |a + b| \leq |a| + |b|,$$

y de 6, se deduce $|a| = |(a - b) + b| \leq |a - b| + |b|$, así que $|a| - |b| \leq |a - b|$. Igualmente $|b| - |a| \leq |b - a| = |a - b|$, de lo cual se obtiene que $|a - b| \leq |a| - |b| \leq |a - b|$. De modo que 5, implica que

$$7. ||a| - |b|| \leq |a - b|.$$

Como es obvio, $a \geq 0$ si $a = |a|$. Por otra parte, si $a \geq 0$ entonces $-a \leq 0$, así que $-a \leq a$ y $|a| = \max\{-a, a\} = a$. Es decir,

$$8. |a| = a \text{ si y sólo si } a \geq 0.$$

De 8, se deduce, en particular, que $||a|| = a$. Como $|-a| = |a|$, se tiene también que

$$9. |a| = -a \text{ si y sólo si } a \leq 0.$$

Teniendo en cuenta entonces que $(-a)(-b) = ab$, se concluye que si $ab \geq 0$ entonces $|ab| = ab = (-a)(-b) = |a||b|$. Y si $ab < 0$, de $(-a)b > 0$ se obtiene también que $|ab| = |(-a)b| = |-a||b| = |a||b|$. En consecuencia,

$$10. |ab| = |a||b|.$$

Nótese finalmente que $|a|^2 = |a||a| = a \cdot a = a^2$ y que $|a + b| = |a| + |b|$ si y sólo si $|a + b|^2 = (|a| + |b|)^2$, lo cual ocurre si y sólo si $ab = |a||b|$, es decir, si y sólo si $ab \geq 0$. También se comprueba fácilmente que, $|a - b| = ||a| - |b||$ si y sólo si $ab \geq 0$.

Es claro que $A \subseteq \mathbb{R}$ es acotado si y sólo si existe $b \in \mathbb{R}$ tal que $|a| \leq b$ para todo $a \in A$.

Las propiedades (axiomas) tanto algebraicas como de orden que hemos supuesto hasta ahora para $\mathbb{R}$ son intuitivas y muy razonables para describir un sistema del cual se espera que sea tan rico como los números reales de nuestra experiencia cotidiana. Hay, sin embargo, muchos sistemas numéricos que satisfacen todas las propiedades anteriores y que pueden ser muy distintos de $\mathbb{R}$. El sistema $(\mathbb{R}, +, \cdot, \mathbb{R}_+)$ tiene, sin embargo, una última propiedad que lo caracteriza (véase, al respecto, el ejercicio 1.39), y cuya naturaleza es algo más sutil que la de las otras.

Axioma de caracterización de los reales (A.C.R.). Si A es un subconjunto no vacío de $\mathbb{R}$ y $A^+ \neq \emptyset$, A^+ tiene un mínimo.

El axioma (A.C.R.) se atribuye a Arquímedes y se conoce también como el *axioma de completéz del orden de los reales*. No es un axioma algebraico, pues no es una afirmación sobre una operación binaria, ni sobre el resultado de efectuar una tal operación sobre los elementos de $\mathbb{R}$. Sus implicaciones, incluyendo las algebraicas, son, sin embargo, múltiples.

Si A^+ tiene un mínimo y $a = \min A^+$, se dice que a es el *extremo superior* de A : $a = \sup A := \min A^+$. Claramente $a \geq x$ para todo $x \in A$, es decir, a es *cota superior* de A ; y si $b < a$, debe existir $x \in A$ tal que $b < x$. Estas dos propiedades caracterizan completamente a $\sup A$. Análogamente si A^- tiene un máximo a , se dice que tal máximo es el *extremo inferior* de A : $a = \inf A := \max A^-$.

Nota 1.10. Si $A \neq \emptyset$ y $A^- \neq \emptyset$, de $A^- = -(-A)^+$ se deduce que $(-A)^+ \neq \emptyset$. También $(-A) \neq \emptyset$, y como $-\min(-A)^+ = \max(A^-)$, se deduce que si A y A^- son no vacíos, A^- tiene un máximo. Es decir, A tiene un extremo inferior. Se tiene además que $\inf(A) = \max(A^-) = -\min(-A)^+ = -\sup(-A)$.

Nota 1.11. En el axioma de caracterización de los reales es necesario hacer dos hipótesis sobre A , $A \neq \emptyset$, $A^+ \neq \emptyset$, para poder asegurar la existencia de $\sup A$. Por ejemplo, $\emptyset^+ = \mathbb{R}$ y $\mathbb{R}$ no tiene un mínimo, así que $\sup \emptyset$ no existe. Tampoco existen $\sup \mathbb{R}$ y $\sup \mathbb{R}_+$, pues $\mathbb{R}^+ = \mathbb{R}_+^+ = \emptyset$. A su vez, para asegurar la existencia de $\inf A$ hay que suponer que $A \neq \emptyset$ y $A^- \neq \emptyset$. Para garantizar la existencia simultánea de $\inf A$ y $\sup A$ se debe entonces suponer que A es acotado y no vacío.

1.3. Los números naturales

Definición 1.10. Un subconjunto A de $\mathbb{R}$ es (finitamente) inductivo si

1. $0 \in A$, y
 2. Si $a \in A$, entonces $a + 1 \in A$.
- (1.24)

Los conjuntos $\mathbb{R}$ y $\mathbb{R}_+$ son inductivos. Si $(A_i)_{i \in I}$ es una familia de subconjuntos inductivos de $\mathbb{R}$ con $I \neq \emptyset$, obviamente $A = \bigcap_{i \in I} A_i$ es inductivo.

Definición 1.11. El conjunto intersección de todos los subconjuntos inductivos de $\mathbb{R}$ se denomina el conjunto de los números naturales y se denota con $\mathbb{N}$.

Evidentemente $\mathbb{N} \subseteq \mathbb{R}_+$. De hecho $\mathbb{N} \subseteq A$ si A es inductivo, y si A es inductivo y $A \subseteq \mathbb{N}$, necesariamente $A = \mathbb{N}$. Como $\mathbb{N}$ contiene, por ejemplo, el conjunto $\mathbb{N}'$ formado por 0 y por los números de la forma $n + 1$ con $n \in \mathbb{N}$, y este conjunto es inductivo ($0 \in \mathbb{N}'$, y si $n \in \mathbb{N}$ y $m = n + 1 \in \mathbb{N}'$ entonces $m + 1 = (n + 1) + 1 \in \mathbb{N}'$, pues $n + 1 \in \mathbb{N}$), se deduce que $\mathbb{N} = \mathbb{N}'$. Es decir, $\mathbb{N} = \{0\} \cup \{n + 1 : n \in \mathbb{N}\}$, y como $n + 1 = 0$, $n \in \mathbb{N}$, implica que $1 \in (-\mathbb{N}) \subseteq \mathbb{R}_-$, de lo cual $1 \in \mathbb{R}_+ \cap \mathbb{R}_-$, y así $1 = 0$, que es absurdo, se deduce que la unión es disyunta. Esta observación se debe a G. Peano, y se expresa usualmente diciendo que todo número natural $m \neq 0$ es el sucesor de algún otro ($m = n + 1$), pero 0 no es el sucesor de ningún otro natural. Algunos elementos de $\mathbb{N}$ son entonces $0, 1 = 0 + 1, 2 := 1 + 1, 3 := 2 + 1, 4 := 3 + 1, \dots$, etc. Se obtiene entonces el siguiente teorema.

Teorema 1.4. Si m es un número natural entonces $m \geq 0$ y si $m > 0$, necesariamente $m \geq 1$. Es decir, no existen números naturales m tales que $0 < m < 1$.

Demostración. La primera afirmación es clara, pues $\mathbb{N} \subseteq \mathbb{R}_+$. Si $m > 0$ entonces $m \neq 0$, así que $m = n + 1$, $n \in \mathbb{N}$, de lo cual $m - 1 \in \mathbb{R}_+$ y $m \geq 1$. $\square$

Teorema 1.5. Si m y n son números naturales, $m + n$ es un número natural.

Demostración. Sea $\mathbb{N}''$ el conjunto de los números naturales m tales que $m + n \in \mathbb{N}$ para todo $n \in \mathbb{N}$. Evidentemente $0 \in \mathbb{N}''$, y si $m \in \mathbb{N}''$, también $m + 1 \in \mathbb{N}''$, pues $(m + 1) + n = (m + n) + 1 \in \mathbb{N}$ para todo $n \in \mathbb{N}$. Entonces $\mathbb{N}'' \subseteq \mathbb{N}$ y $\mathbb{N}''$ es inductivo, así que $\mathbb{N} = \mathbb{N}''$. $\square$

Teorema 1.6. Si $m \geq n$ son naturales, $m - n$ es un natural.

Demostración. Sea $\mathbb{N}'''$ el conjunto de los naturales n tales que si $m \in \mathbb{N}$ y $n \leq m$, existe $p \in \mathbb{N}$ con $n + p = m$. Evidentemente $0 \in \mathbb{N}'''$ y si $n \in \mathbb{N}'''$ y $n + 1 \leq m$, $m \in \mathbb{N}$, dado que $m = p + 1$, $p \in \mathbb{N}$ (pues $m \neq 0$), se tiene que $n \leq p$. Existirá entonces $q \in \mathbb{N}$ tal que $n + q = p$, de lo cual $(n + 1) + q = m$. Entonces $\mathbb{N}''' = \mathbb{N}$, pues $\mathbb{N}'''$ es inductivo. $\square$

Corolario 1.1. Si $m < n$ son naturales entonces $m + 1 \leq n$. Lo mismo, si $m < n + 1$, entonces $m \leq n$.

Demostración. Si fuera $n < m + 1$, sería $0 < n - m < 1$, lo cual es absurdo, pues $n - m \in \mathbb{N}$. $\square$

Teorema 1.7. (Principio de buena ordenación de $\mathbb{N}$). Si $A \subseteq \mathbb{N}$ es no vacío, A tiene un mínimo. De hecho, $\inf A = \min A$.

Demostración. Como $0 \in A^-$, $A^- \neq \emptyset$. Sean $a = \inf A$ y $m \in A$ tal que $m < a + 1$. Entonces $m - 1 < a$, de lo cual $m - 1 < n$ para todo $n \in A$, o sea $m \leq n$ para todo $n \in A$, así que $m = \min A$. Además $m = a$, pues $a \leq m$ ya que $m \in A$, y $m \leq a$, pues $m \in A^-$ y $a = \max A^-$. $\square$

Teorema 1.8. (Arquímedes). El conjunto $\mathbb{N}$ no es acotado superiormente. Si a, b son reales y $a > 0$, existe $n \in \mathbb{N}$ tal que $na > b$.

Demostración. Si fuera $\mathbb{N}^+ \neq \emptyset$, existiría $a = \sup \mathbb{N}$. Esto es absurdo, pues existiría $n \in \mathbb{N}$ tal que $a - 1 < n$, de lo cual $a < n + 1 \in \mathbb{N}$. Ahora, si fuera $na \leq b$ para todo $n \in \mathbb{N}$, se tendría que $b/a \in \mathbb{N}^+$. $\square$

Nota 1.12. Del teorema 1.8 se deduce que si $a \in \mathbb{R}$ y $a > 0$, existe $n \in \mathbb{N}$, $n > 0$, tal que $1/n < a$. Si $A \subseteq \mathbb{N}$ es superiormente acotado y no vacío, y si $a = \sup A$, necesariamente $a \in A$; es decir, $a = \max A$. En efecto, existirá $n \in A$, $n > a - 1$, así que $n \geq m$ para todo $m \in A$. Entonces, $n = \max A$, y como $n \in A$, $n \leq a$. Por otra parte, como $n \in A^+$ y $a = \min A^+$, también $a \leq n$.

Un método frecuente de demostración está basado en el siguiente teorema.

Teorema 1.9. (Principio de inducción). Si $P(x)$ es una afirmación sobre una variable x , y si

1. $P(0)$ es verdadera, y
2. $P(n+1)$ se deduce de $P(n)$ para todo $n \in \mathbb{N}$,

entonces $P(n)$ es verdadera para todo n en $\mathbb{N}$.

Demostración. Sea $\tilde{N} = \{n \in \mathbb{N} : P(n)\}$. Claramente $0 \in \tilde{N}$, y si $n \in \tilde{N}$, de modo que $P(n)$ es verdadera, también $P(n+1)$, al deducirse de $P(n)$, lo será. Entonces $n+1 \in \tilde{N}$, y será $\tilde{N} = \mathbb{N}$. $\square$

Ejemplo 1.1. Como aplicación del teorema anterior demostraremos que si $m \in \mathbb{N}$ entonces $mn \in \mathbb{N}$ para todo $n \in \mathbb{N}$. Sea $m \in \mathbb{N}$ arbitrario pero fijo, y sea $P(x)$ la condición " $mx \in \mathbb{N}$ ". Entonces $P(0)$ es verdadera (pues $m \cdot 0 = 0 \in \mathbb{N}$), y si suponemos que $P(n)$ es verdadera también lo será $P(n+1)$, puesto que $m(n+1) = mn + m \in \mathbb{N}$ se deduce del teorema 1.5.

La siguiente forma del teorema 1.9 será también usada en lo que sigue.

Corolario 1.2. Sean $P(x)$ una afirmación sobre una variable x , $m \in \mathbb{N}$. Supóngase que

1. $P(m)$ es verdadera.
2. De la validez de $P(k)$ para todo los $k \in \mathbb{N}$, $m \leq k < n$, se deduce la validez de $P(n)$.

Entonces, $P(n)$ es válida para todo $n \in \mathbb{N}$, $n \geq m$.

Demostración. Sea X el conjunto de los $k \in \mathbb{N}$, $k \geq m$, tales que $P(k)$ es falsa (es decir, que " $\text{no } P(k)$ " es verdadera). Demostraremos que $X = \emptyset$. En efecto, si fuera $X \neq \emptyset$, existiría $n = \min X$ (pues $X \subseteq \mathbb{N}$). Como $n \in X$, $P(n)$ es falsa. Además $m < n$, pues $P(m)$ es verdadera. De hecho, $P(k)$ es verdadera para todo $m \leq k < n$. Pero esto implica que $P(n)$ es verdadera, lo cual es absurdo. Entonces $X = \emptyset$, y $P(k)$ es verdadera para todo $k \in \mathbb{N}$, $k \geq m$. $\square$

Usaremos el teorema 1.9 y el Corolario 1.1 sin mencionarlos explícitamente.

1.4. Números enteros y aritmética elemental

Definición 1.12. El conjunto $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ se denomina el conjunto de los números enteros. Si $a \in \mathbb{Z}$, se dice que a es un número entero.

Como es claro, decir que $m \in \mathbb{Z}$ es equivalente a decir que $m \in \mathbb{N}$ o $-m \in \mathbb{N}$. Por lo tanto, $m \in \mathbb{Z}$ si y sólo si $m \in \mathbb{R}$ y $|m| \in \mathbb{N}$.

Una de las propiedades más notables e importantes del conjunto $\mathbb{Z}$ de los enteros se establece en el siguiente teorema.

Teorema 1.10. (Euclides). Si $m, n \in \mathbb{Z}$, $n \neq 0$, existen $q, r \in \mathbb{Z}$, $0 \leq r < |n|$, únicos, tales que $m = nq + r$.

Demostración. Nótese que r es siempre un número natural. Podemos suponer también que n es un natural, pues si $m = nq + r$, también $m = (-n)(-q) + r$. Supongamos primero que m es un natural y razonemos por inducción. Si $m = 0$, la afirmación es evidente con $q = r = 0$. Supongamos entonces que $m = nq + r$, $0 \leq r < n$, así que $0 < r + 1 \leq n$. Si $r + 1 < n$, la afirmación en $m + 1$ es clara, pues $m + 1 = nq + (r + 1)$. Si $r + 1 = n$, entonces $m + 1 = n(q + 1) + 0$, es también de la forma deseada. Esto demuestra la afirmación para todo $m \in \mathbb{N}$. Ahora, si $m < 0$ y $(-m) = nq + r$, $0 \leq r < n$, será $m = n(-q)$ si $r = 0$ y $m = n(-q - 1) + (n - r)$ si $r > 0$. Esto completa la demostración de existencia, pues $0 < n - r < n$. La unicidad resulta de observar que si $m, n > 0$ son enteros entonces $nm \geq n$, de lo

cual $nq + r = nq' + r'$, que equivale a $n(q - q') = r' - r < n$, es imposible con $q > q'$. $\square$

Se concluye que todo número entero m es de una y sólo una de las formas $m = 2k$ o $m = 2k + 1$, donde $k \in \mathbb{Z}$. En el primer caso se dice que m es par; en el segundo, que es impar.

Si $m, n \in \mathbb{Z}$ y $q, r \in \mathbb{Z}$ son tales que $m = qn + r$ con $0 \leq r < n$, se dice que q es el cociente de dividir m por n y que r es el resto de tal división. Es usual escribir $q = q(m, n)$ y $r = r(m, n)$. Nótese que si $m, n \in \mathbb{N}$, también $q \in \mathbb{N}$.

Si $a, b \in \mathbb{Z}$ entonces $a + b \in \mathbb{Z}$. Esto es claro si $a, b \in \mathbb{N}$; y si $a, b \in (-\mathbb{N})$ entonces $-(a + b) = (-a) + (-b) \in \mathbb{N}$, de lo cual $a + b \in (-\mathbb{N})$. Por último, si $a, b \in \mathbb{N}$ entonces $a + (-b) = a - b \in \mathbb{N}$ si $a \geq b$ y $a + (-b) = -(b + (-a)) = -(b - a) \in (-\mathbb{N})$ si $a < b$. También $ab \in \mathbb{Z}$ si $a, b \in \mathbb{Z}$, como resulta de las relaciones $ab = (-a)(-b)$ y $-ab = (-a)b = a(-b)$. Como es claro, $0, 1 \in \mathbb{Z}$.

Definición 1.13. Sean $a, b \in \mathbb{Z}$. Se dice que a divide b , que a es un divisor de b , o que a es un factor de b , y se escribe $a \mid b$, si

1. $a \neq 0$
2. Existe $c \in \mathbb{Z}$ tal que $b = ac$.

Se dice también que b es un múltiplo de a .

Como se verifica inmediatamente, $a \mid b$ es equivalente a cualquiera de las afirmaciones siguientes: $a \mid |b|$, $|a| \mid |b|$, $|a| \mid b$, $a \mid (-b)$, $(-a) \mid b$, $(-a) \mid (-b)$.

Si $a = 0$ o si a no es un divisor de b , escribiremos $a \nmid b$ (a no divide b). Es claro que si $a \neq 0$ entonces $a \mid 0$ (pues $a \cdot 0 = 0$) y que $a \mid b$ si y sólo si $r(b, a) = 0$.

Es evidente que si $a, b, c \in \mathbb{Z}$, entonces

1. $a \mid a$ (si $a \neq 0$).
2. Si $a \mid b$ y $b \neq 0$ entonces $|a| \leq |b|$.
3. Si $a \mid b$ y $b \mid a$ entonces $|a| = |b|$.
4. Si $a \mid b$ y $b \mid c$ entonces $a \mid c$.

Definición 1.14. Sean $a, b \in \mathbb{Z}$ tales que $a^2 + b^2 > 0$. Se dice que d es un máximo común divisor de a y b , si

1. $d > 0$,
2. $d \mid a$ y $d \mid b$,
3. $c \mid a$ y $c \mid b$ implica $c \mid d$.

La propiedad (2) expresa que d es un divisor común de a y b . La propiedad (3) implica que cualquier divisor de a y b debe ser menor o igual que d , de lo cual el nombre dado a d .

Si $a, b \in \mathbb{Z}$, no es evidente que exista un $d \in \mathbb{Z}$, máximo común divisor de a y b . Sin embargo, de lo dicho anteriormente se deduce que, si existe, es único. En efecto, si d' es otro, entonces $d \mid d'$ y $d' \mid d$, de lo cual $d = d'$.

Teorema 1.11. (Bezout). Si $a, b \in \mathbb{Z}$ y $a^2 + b^2 > 0$, existe $d \in \mathbb{Z}$, el cual es máximo común divisor de a y b . Más aún

$$d = ma + nb, \quad (1.25)$$

donde $m, n \in \mathbb{Z}$.

Demostración. Sea $A = \{xa + yb > 0 : x, y \in \mathbb{Z}\}$. Es claro que $A \subseteq \mathbb{N}$, y tomando $x = a$, $y = b$ se deduce que $A \neq \emptyset$ (pues $a^2 + b^2 > 0$). Sea $d = \min A$ (teorema 1.7). Como $d \in A$, es claro que $d > 0$, y existen además $m, n \in \mathbb{Z}$ tales que $d = ma + nb$, relación que asegura que si $c \mid a$ y $c \mid b$ entonces $c \mid d$. Veamos que $d \mid a$ y $d \mid b$, lo cual completará la demostración. Si suponemos, por ejemplo, $d \nmid a$, se tiene que $a = qd + r$ con $0 < r < d$, así que $r = (1 - qm)a + (-qn)b$, lo cual es absurdo, pues implica que $r \in A$. De la misma manera se razona si $d \nmid b$. Esto demuestra el teorema. $\square$

En vista de su existencia y unicidad, denotaremos con $\text{mcd}(a, b)$ el máximo común divisor de a y b (cuando $a^2 + b^2 > 0$). La relación

$$\text{mcd}(a, b) = ma + nb$$

dada en el teorema 1.11 se denomina una *relación de Bezout para* $\text{mcd}(a, b)$. En general m y n no son únicos (véase el ejercicio 1.29).

Corolario 1.3. Si $a, b \in \mathbb{Z}$, $a^2 + b^2 > 0$ y $d > 0$, $d = \text{mcd}(a, b)$ si y sólo si d es un divisor común de a y b y existen $m, n \in \mathbb{Z}$ tales que $d = ma + nb$.

Demostración. Del teorema 1.11 sabemos que si $d = \text{mcd}(a, b)$ entonces $d > 0$, d es un divisor común de a y b y existen $m, n \in \mathbb{Z}$ que verifican (1.25). Sólo resta por demostrar que si $d > 0$ es un divisor común de a y b , y $d = ma + nb$, $m, n \in \mathbb{Z}$, entonces $d = \text{mcd}(a, b)$. Pero esto es obvio, pues si $c | a$ y $c | b$, de $d = ma + nb$ se deduce que $c | d$. $\square$

Nota 1.13. Si $a, b \in \mathbb{Z}$, el solo hecho de que $d = ma + nb > 0$, $m, n \in \mathbb{Z}$, no asegura que $d = \text{mcd}(a, b)$. Se necesita que $d | a$ y $d | b$. Por ejemplo, $2 = 3 \cdot 5 + (-1) \cdot 13$, pero $2 \neq \text{mcd}(5, 13) = 1$. Mas generalmente, si $\text{mcd}(a, b) = 1$, en cuyo caso $1 = ma + nb$, $m, n \in \mathbb{Z}$, para todo $d > 0$ se tiene que $d = (md)a + (nd)b$, y ningún real $d > 1$ puede ser $\text{mcd}(a, b)$. Obsérvese, sin embargo, que si $1 = ma + nb$, $m, n \in \mathbb{Z}$, entonces $1 = \text{mcd}(a, b)$, pues $1 | a$ y $1 | b$.

Nota 1.14. Si $a^2 + b^2 > 0$ y $d > 0$ es un divisor común de a y b , entonces $d \geq c$ para todo divisor común c de a y b si y sólo si $d = \text{mcd}(a, b)$ (pues si $d \geq c$ para todo divisor c , entonces $\text{mcd}(a, b) \leq d$, y como $d | \text{mcd}(a, b)$, por ser un divisor, también $d \leq \text{mcd}(a, b)$. Por otra parte, ya hemos visto que si $d = \text{mcd}(a, b)$ entonces $d \geq c$ para todo divisor c de a y b).

Evidentemente, $5 = \text{mcd}(10, 15)$ y $5 = (-1)10 + 15$; $2 = \text{mcd}(14, 22)$ y $2 = 2 \cdot 22 + (-3) \cdot 14$; $1 = \text{mcd}(3, 5)$ y $1 = 2 \cdot 3 + (-1) \cdot 5$. Sin embargo, $7 = 14 \cdot 3 + (-7) \cdot 5$, pero $7 \neq \text{mcd}(3, 5)$. Nótese también que $\text{mcd}(a, b) = \text{mcd}(a, |b|) = \text{mcd}(|a|, b) = \text{mcd}(|a|, |b|) = \text{mcd}(-a, b) = \text{mcd}(a, -b) = \text{mcd}(-a, -b)$.

Teorema 1.12. Si $d = \text{mcd}(a, b)$ y $c > 0$, entonces $\text{mcd}(ca, cb) = cd$. Si además $c | a$ y $c | b$, entonces $d/c = \text{mcd}(a/c, b/c)$.

Demostración. En efecto, $d = ma + nb$, $m, n \in \mathbb{Z}$, y $cd = m(ca) + n(cb)$. Como obviamente $cd | ca$ y $cd | cb$, entonces $cd = \text{mcd}(ca, cb)$. También $d/c = m(a/c) + n(b/c)$, y como $d/c \in \mathbb{Z}$, $d/c | a/c$ y $d/c | b/c$, entonces $d/c = \text{mcd}(a/c, b/c)$. $\square$

Corolario 1.4. Si $a^2 + b^2 > 0$ y $d = \text{mcd}(a, b)$, entonces $\text{mcd}(a/d, b/d) = 1$.

Definición 1.15. Si $\text{mcd}(a, b) = 1$, se dice que a y b son números primos relativos.

Nota 1.15. Como es claro, a y b son primos relativos si y sólo si existen $m, n \in \mathbb{Z}$ tales que $1 = ma + nb$. En tal caso se deduce que si $c | a$, también $\text{mcd}(c, b) = 1$ (pues $1 = (mq)c + nb$ para algún $q \in \mathbb{Z}$).

Por ejemplo, 3 y 5 son primos relativos, y lo mismo es cierto de 8 y 21, pues $2 \cdot 3 + (-1) \cdot 5 = 1$ y $8 \cdot 8 + (-3) \cdot 21 = 1$. También 4 y 21 son primos relativos, pues $16 \cdot 4 + (-3) \cdot 21 = 1$. Nótese que $7 | 21$ y que $1 = 16 \cdot 4 + (-9) \cdot 7 = 2 \cdot 4 + (-1) \cdot 7$.

Nota 1.16. Es claro que si $d \neq 0$ entonces $d | a$ si y sólo si $\text{mcd}(d, a) = |d|$. En particular, $\text{mcd}(1, a) = 1$.

Los siguientes resultados son de gran importancia en la teoría elemental de los números, y a lo largo de todo este curso.

Teorema 1.13. Si $a | bc$ y $\text{mcd}(a, b) = 1$, entonces $a | c$.

Demostración. Evidentemente existen $m, n, q \in \mathbb{Z}$ tales que $1 = ma + nb$ y $bc = qa$, de lo cual $c = (mc)a + n(bc) = (mc + nq)a$. $\square$

Corolario 1.5. Si $\text{mcd}(a, b) = \text{mcd}(a, c) = 1$, entonces $\text{mcd}(a, bc) = 1$. En particular, si $|a| > 1$, entonces $a \nmid bc$.

Demostración. Si $d = \text{mcd}(a, bc)$ entonces $d | bc$, y como también $d | a$, entonces $\text{mcd}(d, b) = 1$ (nota 1.15). Se concluye que $d | c$, así que $d = \text{mcd}(d, c) = 1$ (pues $d | a$ y $\text{mcd}(a, c) = 1$). $\square$

El corolario anterior se puede generalizar.

Corolario 1.6. Si $\text{mcd}(a, a_i) = 1$, $i = 1, \dots, n$, entonces $\text{mcd}(a, a_1 a_2 \cdots a_n) = 1$. Si $|a| > 1$, entonces $a \nmid a_1 a_2 \cdots a_n$.

Demostración. La afirmación es evidente si $n = 1, 2$. Y si $n > 2$, resulta de un argumento inductivo, observando que $a_1 \cdots a_n = (a_1 \cdots a_{n-1}) a_n$. $\square$

Nota 1.17. Se deduce que si $a | (a_1 \cdots a_n) a_{n+1}$, y $\text{mcd}(a, a_i) = 1$, $i = 1, 2, \dots, n$, entonces $a | a_{n+1}$ (pues $\text{mcd}(a, a_1 a_2 \cdots a_n) = 1$, y basta aplicar el teorema 1.13).

Teorema 1.14. Si $a | c$, $b | c$ y $\text{mcd}(a, b) = 1$, entonces $ab | c$.

Demostración. Sean a', b' tales que $c = aa'$, $c = bb'$ y $m, n \in \mathbb{Z}$ tales que $1 = ma + nb$. Entonces $c = mac + nbc = (mb' + na')(ab)$. $\square$

Definición 1.16. Sea $p \in \mathbb{Z}$ tal que

1. $p > 1$.
2. Si $q \mid p$ entonces $|q| = p$ o $|q| = 1$.

Se dice entonces que p es un *número primo*. Es decir, p es un primo si y sólo si $p > 1$ y sus únicos divisores son ± 1 y $\pm p$.

Teorema 1.15. Si $p > 1$, entonces p es un primo si y sólo si para todo entero a , $p \mid a$ ó $\text{mcd}(p, a) = 1$, y las dos posibilidades son mutuamente excluyentes. Por otra parte, si $p > 1$ no es primo, existen $m > 1$ y $n > 1$ en $\mathbb{Z}$ tales que $p = mn$.

Demostración. Si $p > 1$ es primo y $a \in \mathbb{Z}$ entonces $p \mid a$ ó $p \nmid a$. Si $p \nmid a$ entonces $d = \text{mcd}(p, a) \neq p$, y como $d \mid p$, necesariamente $d = 1$. Supóngase recíprocamente que p no es primo. Entonces existe $a \in \mathbb{Z}$, $1 < a < p$, tal que $a \mid p$. Como es claro, $p \nmid a$, y sin embargo, $\text{mcd}(a, p) = a \neq 1$. La última afirmación es trivial. $\square$

Nota 1.18. Evidentemente 2 y 3 son primos, y no es difícil verificar que también 5 y 7 lo son.

Corolario 1.7. Sean p un primo y a, b enteros. Si $p \mid ab$, entonces $p \mid a$ o $p \mid b$. Más generalmente, si $a_1, \dots, a_n$ son enteros y $p \mid a_1 \cdots a_n$, entonces $p \mid a_i$ para algún i , $1 \leq i \leq n$.

Demostración. Si $p \nmid a_i$ para $i = 1, 2, \dots, n$, entonces $\text{mcd}(p, a_i) = 1$, así que (corolario 1.5) $\text{mcd}(p, a_1 \cdots a_n) = 1$. Entonces, $p \nmid a_1 \cdots a_n$. $\square$

Nota 1.19. Es claro que si p y q son primos, $p \mid q$ si y sólo si $p = q$.

Lema 1.1. Sea $a \in \mathbb{Z}$, $a > 1$. Entonces, existen números primos $p_1 \leq \dots \leq p_n$, $n \geq 1$, tales que

$$a = p_1 \cdots p_n. \quad (1.26)$$

En particular, existe al menos un primo p tal que $p \mid a$.

Demostración. Sea X el conjunto de los $a > 1$ en $\mathbb{Z}$ para los cuales no existen primos $p_1 \leq \dots \leq p_n$, $n \geq 1$, tales que $a = p_1 \cdots p_n$. Si $X \neq \emptyset$, existe $a = \min X$. Claramente $a > 1$ y no es primo, así que existen $b > 1$, $c > 1$ tales que $a = bc$. Como $b, c < a$, entonces $b, c \notin X$, y existirán primos que dividen b y primos que dividen c . Sea p_1 el mínimo de tales primos (tal mínimo existe, pues el conjunto de los primos es un subconjunto de $\mathbb{N}$).

Claramente $p_1 \mid a$ y $a/p_1 \notin X$, pues $a/p_1 < a$. Existirán entonces primos $p_2 \leq \dots \leq p_n$, $n \geq 2$, tales que $a/p_1 = p_2 \cdots p_n$, y como $p_2 \mid a$, p_2 dividirá b o c , así que $p_1 \leq p_2$. Entonces $a = p_1 \cdots p_n$ y $a \in X$, lo cual es absurdo. Entonces $X = \emptyset$, y el lema queda demostrado. $\square$

Teorema 1.16. Si $a \in \mathbb{Z}$ y $a > 1$, existen primos $p_1 < \dots < p_n$, $n \geq 1$, y enteros $\alpha_1, \dots, \alpha_n$, $\alpha_i > 0$ para todo i , tales que

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}. \quad (1.27)$$

Tal factorización de a es además única, en el sentido de que si $q_1 < \dots < q_m$, $m \geq 1$, son primos, $\beta_1, \dots, \beta_m$ son enteros, $\beta_i > 0$ para todo i , y también $a = q_1^{\beta_1} \cdots q_m^{\beta_m}$, entonces $m = n$ y $p_i = q_i$, $\alpha_i = \beta_i$, $i = 1, 2, \dots, n$.

Demostración. Agrupando primos iguales, la existencia de una factorización (1.27) es consecuencia obvia de (1.26). Demostraremos la unicidad, haciendo inducción sobre a . Ahora, si $a = p_1$ es primo y también $a = q_1^{\beta_1} \cdots q_m^{\beta_m}$, entonces $p_1 \mid q_i$ para algún i (corolario 1.6), así que $p_1 = q_i$, de lo cual $p_1 \geq q_1$, y si fuera $p_1 > q_1$ se tendría que $q_1 \neq 1$, $q_1 \neq p_1$ y $q_1 \mid p_1$, lo cual es absurdo. Entonces $p_1 = q_1$. Esto implica además que $1 = q_1^{\beta_1-1} q_2^{\beta_2} \cdots q_m^{\beta_m}$, lo cual es también absurdo si $m \geq 2$ o $\beta_1 > 1$. Entonces $m = 1$ y $\beta_1 = 1$. Supongamos ahora que la afirmación es cierta para todo $1 < b < a$, y demostrémosla para a . Supongamos $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n} = q_1^{\beta_1} \cdots q_m^{\beta_m}$. De nuevo $p_1 \mid q_1^{\beta_1} \cdots q_m^{\beta_m}$ (pues $p_1 \mid a$), así que $p_1 = q_i$ para algún $1 \leq i \leq m$, de lo cual $p_1 \geq q_1$. Análogamente $q_1 = p_j$ para algún $1 \leq j \leq n$, de lo cual $q_1 \geq p_1$. Entonces $i = j = 1$ y $q_1 = p_1$, así que $b = p_1^{\alpha_1-1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} = q_1^{\beta_1-1} q_2^{\beta_2} \cdots q_m^{\beta_m}$. Como $1 < b < a$, esto implica que $m = n$, que $\alpha_1 - 1 = \beta_1 - 1$, $\alpha_2 = \beta_2, \dots, \alpha_n = \beta_n$ y que $p_1 = q_1, \dots, p_n = q_n$. Entonces $m = n$, $p_i = q_i$ y $\alpha_i = \beta_i$, $i = 1, 2, \dots, n$. $\square$

Dada su importancia, el teorema anterior se conoce como el *teorema fundamental de la aritmética*.

Nota 1.20. Es claro que del teorema 1.16 se deduce la unicidad de la factorización (1.26), pues agrupando términos iguales, una factorización (1.26) es obviamente equivalente a una (1.27).

Nota 1.21. Si $a \neq 0, 1$, $|a|$ admite una factorización única de la forma $|a| = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, $n \geq 1$, $p_1 < \dots < p_n$, $\alpha_i > 0$ para todo i . Se dice que tal descomposición es la *factorización de a en potencias de primos* o, también, la *descomposición primaria de a* (si $a \neq 0$, un *factor primario* de

a es un divisor m de a de la forma $m = p^n$, donde p es un primo y $n \geq 1$ es un entero). A su vez, la factorización $|a| = p_1 \cdots p_m$, donde $m \geq 1$ y $p_1 \leq \dots \leq p_m$ son primos, se denomina su *descomposición en factores primos* o, simplemente, su *descomposición prima*. Nótese que si $a < -1$, $a = -p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ y $a = -p_1 \cdots p_m$.

Nota 1.22. Si $|a| > 1$ y el conjunto $\{p_1, \dots, p_n\}$ contiene los factores primos de a , $|a|$ puede escribirse en la forma

$$|a| = p_1^{\alpha_1} \cdots p_n^{\alpha_n}, \quad \alpha_i \geq 0, \quad i = 1, 2, \dots, n. \quad (1.28)$$

Como es claro, $\alpha_i > 0$ en (1.28) si y sólo si p_i es un factor primo de a .

Del teorema 1.16 se deduce el siguiente corolario.

Corolario 1.8. Si $|a| = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ y $|b| = p_1^{\beta_1} \cdots p_n^{\beta_n}$, donde los p_i son primos y $\alpha_i \geq 0, \beta_i \geq 0$ para todo $i = 1, 2, \dots, n$, entonces

$$\text{mcd}(a, b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n} \quad (1.29)$$

donde $\gamma_i = \min\{\alpha_i, \beta_i\}$, $i = 1, 2, \dots, n$.

Demostración. Si $c = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$, es claro que $c \mid a$ y $c \mid b$, y si $a' = a/c, b' = b/c$, es también claro que si $p_i \mid a'$ entonces $p_i \nmid b'$, y recíprocamente, así que ningún primo p divide simultáneamente a a' y b' . Esto implica que $\text{mcd}(a', b') = 1$ y así $\text{mcd}(a, b) = c$. $\square$

Si $a, b \in \mathbb{Z}$ y $ab \neq 0$, se define el *mínimo común múltiplo* $\text{mcm}(a, b)$ de a y b por

$$\text{mcm}(a, b) = \frac{|ab|}{\text{mcd}(a, b)}, \quad (1.30)$$

así que si $|a| = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ y $|b| = p_1^{\beta_1} \cdots p_n^{\beta_n}$, donde los p_i son primos y $\alpha_i \geq 0, \beta_i \geq 0$, entonces

$$\text{mcm}(a, b) = p_1^{\mu_1} \cdots p_n^{\mu_n}, \quad \mu_i = \max\{\alpha_i, \beta_i\}, \quad 1 \leq i \leq n, \quad (1.31)$$

como resulta inmediatamente de observar que $\max\{\alpha_i, \beta_i\} + \min\{\alpha_i, \beta_i\} = \alpha_i + \beta_i$, $i = 1, 2, \dots, n$.

Teorema 1.17. Si $a, b \in \mathbb{Z}$ y $ab \neq 0$, $m = \text{mcm}(a, b)$ es un múltiplo tanto de a como de b ; y si n es un múltiplo tanto de a como de b , n es un múltiplo de m . En particular, $m \leq |n|$.

Demostración. Evidentemente $m = \text{mcm}(a, b)$ es un múltiplo de a y de b , pues si $d = \text{mcd}(a, b)$, entonces $m = a(\pm b/d) = (\pm a/d)b$. Además, si $n > 0$ es un múltiplo tanto de a como de b entonces $d \mid n$, y tanto (a/d) como (b/d) dividen a (n/d) . Como además $\text{mcd}(a/d, b/d) = 1$, también $\frac{|ab|}{d^2} = \frac{m}{d}$ divide a (n/d) (teorema 1.14). Entonces $m \mid n$, y así $m \leq n$. $\square$

El teorema anterior explica la razón del nombre *mínimo común múltiplo*. Es frecuente convenir en que $\text{mcm}(a, 0) = \text{mcm}(0, 0) = 0$ para todo $a \in \mathbb{Z}$.

Es de esperar que el lector esté familiarizado desde sus estudios básicos con los procedimientos para obtener las descomposiciones prima y primaria de un entero y para calcular los máximos divisores y los mínimos múltiplos comunes. Para finalizar esta sección, presentamos el siguiente famoso teorema de Euclides.

Teorema 1.18 (Euclides). El conjunto de los números primos es infinito.

Demostración. Supóngase, por el contrario, que sólo existen finitos primos $p_1, \dots, p_n$, y sea $a = (p_1 \cdots p_n) + 1$. Debe existir al menos un primo p tal que $p \mid a$ (lema 1.1). Pero evidentemente $p \neq p_i$, $i = 1, 2, \dots, n$, pues $p \nmid 1$. Esto es absurdo. Entonces, deben existir infinitos primos. $\square$

Para las nociones precisas de conjunto finito e infinito, véase la sección 1.11. Para un tratamiento de los enteros, análogo al que hemos dado, véase [15].

1.5. Los números racionales

El subconjunto $\mathbb{Q} = \{a/b : a, b \in \mathbb{Z}, b \neq 0\}$ de $\mathbb{R}$ se denomina el *sistema de los números racionales*. Si $r \in \mathbb{Q}$, diremos que r es un *número racional*. Recordamos que $a/b = \frac{a}{b} = ab^{-1}$. Supóngase un momento que a, b, c, d son números enteros. Nótese que $a/b = (-a)/(-b)$, lo cual implica que todo número racional se escribe en la forma a/b con $b > 0$. Como es claro, $a/b = c/d$ si y sólo si $ad = bc$ (con $bd \neq 0$). Como

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad (1.32)$$

y

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad (1.33)$$

se deduce que $(+)$ y $(\cdot)$ son clausurativas en $\mathbb{Q}$, es decir, que $r + r'$ y rr' están en $\mathbb{Q}$ si r y r' lo están. Notese que $1 = 1/1 \in \mathbb{Q}$ y $0 = 0/1 \in \mathbb{Q}$. Como $-(a/b) = (-a)/b$, se deduce que si $r \in \mathbb{Q}$ entonces $(-r) \in \mathbb{Q}$. Como también $(a/b)^{-1} = b/a$ si $a/b \neq 0$, o sea, si $a \neq 0$, entonces $r^{-1} \in \mathbb{Q}$ si $r \in \mathbb{Q}$ y $r \neq 0$. Finalmente como $ac/bc = a/b$ si $c \neq 0$, se tiene que si $\text{mcd}(a, b) = d$ entonces $a/b = ad^{-1}/bd^{-1}$ y, como es claro, $\text{mcd}(ad^{-1}, bd^{-1}) = 1$. Es decir, todo número racional r se escribe en la forma a/b con $b > 0$ y $\text{mcd}(a, b) = 1$. Se dice en tal caso que a/b es la forma reducida de r .

Lema 1.2. Si $A \subseteq \mathbb{Z}$ es superiormente acotado y no vacío, y si $a = \sup A$, entonces $a \in A$; es decir $a = \max A$.

Demostración. En efecto, $a - 1$ no es cota superior de A , así que existe $n \in A$ con $a - 1 < n$, de lo cual $a < n + 1$. Esto implica que $m < n + 1$, o sea que $m \leq n$, para todo $m \in A$, así que $n = \max A$. Pero $a \leq n$, pues n es cota superior de A ; y también $n \leq a$, pues $n \in A$. Entonces $a = n \in A$ y $a = \max A$. $\square$

Definición 1.17. Si $a \in \mathbb{R}$, definimos

$$[a] := \sup\{m \in \mathbb{Z} : m \leq a\}. \quad (1.34)$$

Se dice que $[a]$ es el mayor entero en a . También, que $[a]$ es la parte entera de a .

Nota 1.23. Nótese que como no es posible que $a < m$ para todo $m \in \mathbb{Z}$ (pues sería $-a > -m$ para todo $m \in \mathbb{Z}$ y, por lo tanto, $-a$ sería, en particular, una cota superior de $\mathbb{N}$), siempre existirá $m \in \mathbb{Z}$, $m \leq a$, así que el conjunto en (1.34) es no vacío. Como además a es cota superior de tal conjunto, $[a]$ está bien definido y, en virtud de lema 2, $[a]$ pertenece al conjunto de la derecha en (1.34). Se tiene entonces que $[a] \in \mathbb{Z}$, y que $[a] \leq a < [a] + 1$, o sea que $a - 1 < [a] \leq a$. De hecho, $m = [a]$ si y sólo si $m \in \mathbb{Z}$ y $m \leq a < m + 1$ o, lo que es lo mismo, si y sólo si $m \in \mathbb{Z}$ y $a - 1 < m \leq a$. En efecto, esta última relación implica obviamente que $[a] - 1 < m \leq [a]$, o sea, que $[a] \leq m \leq [a]$.

Teorema 1.19. Si $a, b \in \mathbb{R}$ y $a < b$, existe $r \in \mathbb{Q}$ tal que $a < r < b$.

Demostración. Sea $m \in \mathbb{N}$ tal que $m(b - a) > 1$. Entonces $[ma] \leq ma \leq mb - 1$, de lo cual $ma < [ma] + 1 < mb$, y así $a < ([ma] + 1)/m < b$. $\square$

El teorema 1.19 tiene implicaciones importantes en diversas áreas de la matemática (especialmente en el denominado análisis matemático).

1.6. Dos notaciones útiles

Sean $a_1, a_2, \dots, a_n$ números reales, $n \geq 1$. Escribiremos

$$\sum_{k=1}^n a_k = a_1 + a_2 + \dots + a_n. \quad (1.35)$$

En particular, $\sum_{k=1}^1 a_k = a_1$, $\sum_{k=1}^2 a_k = a_1 + a_2$.
Convendremos en que

$$\sum_{k=n}^1 a_k = \sum_{k=1}^n a_k. \quad (1.36)$$

Si $1 \leq l \leq m \leq n$, entonces $\sum_{k=l}^m a_k = a_l + a_{l+1} + \dots + a_m$.

De igual manera definimos

$$\prod_{k=1}^n a_k = a_1 \cdot a_2 \cdot \dots \cdot a_n. \quad (1.37)$$

En particular, $\prod_{k=1}^1 a_k = a_1$, $\prod_{k=1}^2 a_k = a_1 \cdot a_2$ y convendremos en que

$$\prod_{k=n}^1 a_k = \prod_{k=1}^n a_k. \quad (1.38)$$

Si $1 \leq l \leq m$, entonces $\prod_{k=l}^m a_k = a_l \cdot a_{l+1} \cdot \dots \cdot a_m$.

1.7. Los números irracionales

Si $a \in \mathbb{R}$, definimos inductivamente

$$a^0 := 1, (a \neq 0); a^n := a^{n-1}a, n = 1, 2, \dots \quad (1.39)$$

Nótese que entonces $a^{n+1} = a^n a$ y $a^{n-1} = a^n a^{-1}$, $n \geq 0$.

También definimos, si $a \neq 0$,

$$a^n := (a^{-1})^{-n}, n = -1, -2, \dots \quad (1.40)$$

Nótese que $(a^{-1})^{-n}$ en (1.40) está ya definido en (1.39), y se deduce que $a^{n+1} = a^n a$, $n < 0$. En efecto, esto es claro si $n = -1$; y si $n < -1$, entonces $a^{n+1} = (a^{-1})^{-n-1} = (a^{-1})^{-n} (a^{-1})^{-1} = a^n a$ (pues $-n > 0$). Si m, n son enteros, es fácil verificar (por inducción sobre n si $n \geq 0$, y usando la relación (1.40) si $n < 0$) que para $a \in \mathbb{R}$,

$$\begin{aligned} 1. & a^n a^{-1} = a^{n-1}, a \neq 0, \\ 2. & a^{m+n} = a^m \cdot a^n, \\ 3. & (a^n)^{-1} = (a^{-1})^n = a^{-n}, \\ 4. & (a^m)^n = a^{mn} = (a^n)^m. \end{aligned} \quad (1.41)$$

Se supone que si alguno de los números m, n es menor que 0 entonces $a \neq 0$.

Demostraremos (1) y (2). Supongamos primero $n \geq 0$ en (1). La afirmación es clara si $n = 0$. Supongámosla para n . Como entonces $a^{n+1} a^{-1} = (a^n a) a^{-1} = a^n = a^{(n+1)-1}$, la afirmación queda demostrada en este caso. Supongamos ahora $n < 0$. Entonces $a^n a^{-1} = (a^{-1})^{-n} a^{-1} = (a^{-1})^{-n+1} = a^{n-1}$ (pues $-n > 0$). Veamos la demostración de (2). Supongamos primero $m \geq 0$ ó $n \geq 0$. Digamos $n \geq 0$. La afirmación es evidente si $n = 0$. Suponiendo entonces la validez de (2) para n , se deduce que $a^{m+(n+1)} = a^{(m+n)+1} = a^{m+n} a = a^m (a^n a) = a^m a^{n+1}$. Si $m \geq 0$, se procede de la misma manera. Queda entonces por considerar el caso $m < 0$, $n < 0$, de modo que $m+n < 0$. Se tiene que $a^{m+n} = (a^{-1})^{-(m+n)} = (a^{-1})^{-m} (a^{-1})^{-n} = a^m a^n$ (pues $-m > 0$ y $-n > 0$).

También

$$(ab)^m = a^m b^m, \quad (1.42)$$

donde $a, b \neq 0$ si $m < 0$. Obviamente $a^{-1} \neq 0$ y $(a^{-1})^{-1} = a$ si $a \neq 0$. Es también fácil verificar (por inducción) que cuando $0 \leq a \leq b$, entonces

$$a^n \leq b^n, n = 0, 1, 2, \dots \quad (1.43)$$

En esta última circunstancia se tiene también que si $a \neq 0$ entonces

$$b^{-n} \leq a^{-n}, n = 0, 1, 2, \dots, \quad (1.44)$$

pues si $a \leq b$, obviamente $b^{-1} \leq a^{-1}$.

Demostraremos ahora un resultado aritmético útil, con una consecuencia sorprendente (por lo menos fue sorprendente para Pitágoras). La demostración requiere sin embargo el axioma (A.C.R.) y no es, por lo tanto, puramente algebraica. Requiere, además, de las dos observaciones preliminares siguientes. En primer lugar, si $x, y \in \mathbb{R}$, entonces

$$x^n - y^n = (x - y) \sum_{k=1}^n x^{n-k} y^{k-1}, n \geq 1. \quad (1.45)$$

Esto resulta inmediatamente de un argumento inductivo basado en la igualdad $x^{n+1} - y^{n+1} = x^n(x - y) + y(x^n - y^n)$. Se deduce que si $0 \leq y \leq x$ entonces

$$ny^{n-1}(x - y) \leq x^n - y^n \leq nx^{n-1}(x - y), \quad (1.46)$$

pues $x^{n-k} y^{k-1} \leq x^{n-k} x^{k-1} = x^{n-1}$, $x^{n-k} y^{k-1} \geq y^{n-1}$.

Teorema 1.20. Si $b > 0$ y $n \in \mathbb{N}$, $n \geq 1$, existe $a \in \mathbb{R}$, $a > 0$, tal que $a^n = b$. Tal a es además único.

Demostración. Supóngase primero que $b \geq 1$, y sea $A = \{x \in \mathbb{R} : x > 0 \text{ y } x^n \leq b\}$. Como $1 \in A$, A es no vacío. Por otra parte $b+1$ es cota superior de A , pues si $x \geq b+1$ entonces $x^n \geq (b+1)^n \geq b+1 > b$, así que si $x \in A$, necesariamente $x < b+1$. Sea entonces $a = \sup A$. Claramente $a > 0$. Si fuera $a^n < b$, podríamos tomar $0 < \varepsilon \leq a$ tal que $\varepsilon < \frac{b - a^n}{2^{n-1}na^{n-1}}$, así que, de (1.46), $(a + \varepsilon)^n \leq n(a + \varepsilon)^{n-1}\varepsilon + a^n \leq (2^{n-1}na^{n-1})\varepsilon + a^n < b$, lo cual implica que $a + \varepsilon \in A$, que es absurdo. Tampoco puede ser $b < a^n$, pues tomando $0 < \varepsilon \leq a$ y $\varepsilon < \frac{a^n - b}{na^{n-1}}$ se obtiene, mediante (1.46), que $a^n - (a - \varepsilon)^n \leq na^{n-1}\varepsilon < a^n - b$, lo cual asegura que $(a - \varepsilon)^n > b$, que es también absurdo, pues obviamente $a - \varepsilon \in A$. Se concluye que $a^n = b$ en este caso. Si ahora suponemos $0 < b < 1$ entonces $b^{-1} > 1$, y si $c \in \mathbb{R}$, $c > 0$,

es tal que $c^n = b^{-1}$, entonces $(c^{-1})^n = (c^n)^{-1} = (b^{-1})^{-1} = b$, y basta tomar $a = c^{-1}$. Esto completa la demostración de la existencia de a . Ahora, si $a^n = c^n = b$ y $0 < c \leq a$ entonces, de (1.46), $0 \leq n(a - c)c^{n-1} \leq 0$, de lo cual $n(a - c)c^{n-1} = 0$, así que $c = a$. Esto establece la unicidad de a y completa la demostración. $\square$

Definición 1.18. Si $b > 0$ y $n \geq 1$ es un número natural, el único $a > 0$ tal que $a^n = b$ se denomina la *raíz n -ésima positiva* de b y se denota con $b^{1/n}$ o con $\sqrt[n]{b}$.

Nota 1.25. Es costumbre escribir simplemente $\sqrt{b}$ en lugar de $\sqrt[2]{b}$. Como es claro, $1^{1/n} = 1$ para todo natural $n \geq 1$. Es también usual convenir en que $0^{1/n} = 0$ (pues $0^n = 0$). Cuando $n = 2$, se dice que $b^{1/2} = \sqrt{b}$ es la *raíz cuadrada positiva* de b . Cuando $n = 3$, que $b^{1/3} = \sqrt[3]{b}$ es la *raíz cúbica* de b . Notese que cuando n es par, también $(-b^{1/n})^n = b$. Por otra parte, si n es impar y $b < 0$, $(-|b|^{1/n})^n = b$.

El siguiente resultado justifica el haber desviado la atención del lector hacia las anteriores consideraciones sobre las raíces de números reales. Para otras justificaciones, véase la sección 1.8, fórmulas (1.54) y (1.85).

Teorema 1.21. Si p es un número primo y $n \geq 2$, $p^{1/n}$ no es un número racional.

Demostración. Supóngase que $p^{1/n} = a/b$, donde $a, b \in \mathbb{N}$ con $\text{mcd}(a, b) = 1$. Entonces $p = a^n/b^n$, así que $p \mid a^n$, de lo cual $p \mid a$ y $a = pc$ para algún $c \in \mathbb{N}$. Se deduce que $p^{n-1}c^n = b^n$, así que $p \mid b^n$, y entonces $p \mid b$. Esto es absurdo, pues $\text{mcd}(a, b) = 1$. $\square$

Se deduce que $\mathbb{R} \setminus \mathbb{Q} \neq \emptyset$. Si $x \in \mathbb{R} \setminus \mathbb{Q}$, se dice que x es un *número irracional*. Tal vez el más famoso de los números irracionales, por ser el primero conocido (Pitágoras), es $\sqrt{2}$ (aunque π y e puedan ser más importantes). Los números irracionales son, en un sentido preciso, más abundantes que los números racionales (véase la sección 1.11). Que no son tan escasos, se puede apreciar en el siguiente teorema.

Teorema 1.22. Si a, b son números reales, con $a < b$, existe un número irracional x tal que $a < x < b$.

Demostración. En virtud del teorema 1.18, podemos suponer que a es racional. Sea entonces $n \in \mathbb{N}$ tal que $n(b - a) > \sqrt{2}$, de lo cual $b >$

$a + \sqrt{2}/n > a$. Como $a + \sqrt{2}/n$ es irracional (si fuera $a + \sqrt{2}/n = r \in \mathbb{Q}$, se tendría que $\sqrt{2} = n(r - a) \in \mathbb{Q}$), el teorema queda demostrado. $\square$

Nota 1.26. Si $b > 0$ y $n \in \mathbb{N}$, $n > 0$, entonces, por definición, $(b^{1/n})^n = b$. Por otra parte $b^n > 0$, y si $(b^n)^{1/n} = a$ entonces $a > 0$ y $b^n = a^n$, de lo cual $a = b$, y también $(b^n)^{1/n} = b$. Es decir, si $b > 0$ entonces $(b^{1/n})^n = (b^n)^{1/n} = b$ para todo $n \in \mathbb{N}$, $n > 0$.

Nota 1.27. Las consideraciones anteriores sobre las raíces permiten dar sentido a b^r para todo $b > 0$ y todo $r \in \mathbb{Q}$. Basta, en efecto, definir

$$b^{m/n} := (b^m)^{1/n} \quad (1.47)$$

para todo par $m, n \in \mathbb{Z}$, $n > 0$. Como se verifica inmediatamente, también $b^{m/n} = (b^{1/n})^m$ (si $(b^{1/n})^m = a$ entonces $a > 0$ y $[(b^{1/n})^m]^n = [(b^{1/n})^n]^m = b^m = a^n$, de lo cual $a = (b^m)^{1/n}$). De esto se deduce sin más que si $b > 0$ entonces $(b^r)^{r'} = b^{rr'} = (b^{r'})^r$ y $b^r b^{r'} = b^{r+r'}$, cualesquiera que sean $r, r' \in \mathbb{Q}$. Si también $a > 0$, entonces $(ab)^r = a^r b^r$ para todo $r \in \mathbb{Q}$. Para una definición de a^r , $a > 0$, r arbitrario en $\mathbb{R}$, véase [7], capítulo 5, nota 5.10, o el ejercicio 1.45 más adelante. No haremos uso de este concepto.

1.8. Los números complejos

El sistema $(\mathbb{C}, +, \cdot)$ de los números complejos se obtiene al dotar $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ de las leyes de composición interna

$$\begin{aligned} 1. \quad (a, b) + (c, d) &= (a + c, b + d), \\ 2. \quad (a, b) \cdot (c, d) &= (ac - bd, ad + bc). \end{aligned} \quad (1.48)$$

En lugar de $(a, b) \cdot (c, d)$ es usual escribir simplemente $(a, b)(c, d)$.

Usaremos preferencialmente las letras z, ξ, ζ para denotar los elementos de $\mathbb{C}$, especialmente cuando aparecen como variables. Si $z = (a, b) \in \mathbb{C}$, a se denomina la *parte real* de z : $a = \Re(z)$. A su vez, b es la *parte imaginaria* de z : $b = \Im(z)$. El número complejo $\bar{z} := (a, -b)$ se conoce como el *conjugado* de z .

Es costumbre identificar el número complejo $(a, 0)$ con el número real a :

$$(a, 0) = a. \quad (1.49)$$

Esta identificación permite considerar a $\mathbb{R}$ como un subconjunto de $\mathbb{C}$.

También se definen

$$\begin{aligned} -(a, b) &:= (-a, -b), \\ -(a, b) &:= (-a, -b), \\ (a, b) - (c, d) &:= (a, b) + (-c, d) = (a - c, b - d). \end{aligned} \quad (1.50)$$

El número complejo

$$i := (0, 1), \quad (1.51)$$

que juega un papel importante en la teoría de números complejos, se denomina la *unidad imaginaria*. De hecho, un número complejo de la forma $(0, b)$ se denomina un *número imaginario*. Dado que $(0, b) = (b, 0)(0, 1) = bi$, como resulta inmediatamente de (1.48) y (1.49), los números imaginarios son los múltiplos reales de i . Se tiene que

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1. \quad (1.52)$$

El tener la relación (1.52) lo que hace interesante el sistema $(\mathbb{C}, +, \cdot)$.

Como

$$(a, b) = (a, 0) + (0, b) = a + bi,$$

todo número complejo z se escribe

$$z = \Re(z) + \Im(z)i. \quad (1.53)$$

Si $z = (a, b)$ es un número complejo, (1.48) y (1.49) implican que $z\bar{z} = a^2 + b^2$, y el número real

$$|z| := \sqrt{z\bar{z}} = \sqrt{a^2 + b^2} \quad (1.54)$$

se denomina *valor absoluto* de z (para la noción de raíz cuadrada de un número positivo, véase la sección 1.7). Claramente $|z| \geq 0$. Nótese que $|z| = \sqrt{z^2}$ si $z \in \mathbb{R}$ (pues $b = 0$ y $z = a$ en 1.53).

Sean z, ξ números complejos. Las siguientes afirmaciones se verifican fácilmente a partir de las definiciones (1.48), (1.50), (1.51) y (1.54), y las de

$\Re(z)$, $\Im(z)$ y $\bar{z}$ (algunas, como (8) y (9), con algo de paciencia):

1. $|i| = 1$,
2. $\Re(z + \xi) = \Re(z) + \Re(\xi)$, $\Im(z + \xi) = \Im(z) + \Im(\xi)$,
3. z es real si y sólo si $\Im(z) = 0$, si y sólo si $z = \Re(z)$,
4. $z + \bar{z} = 2\Re(z)$, $z - \bar{z} = 2\Im(z)i$,
5. z es real si y sólo si $z = \bar{z}$,
6. $\bar{\bar{z}} = z$,
7. $\overline{z + \xi} = \bar{z} + \bar{\xi}$,
8. $\overline{z\xi} = \bar{z}\bar{\xi}$,
9. $z\bar{z} = |z|^2$,
10. $|z| = 0$ si y sólo si $z = 0$,
11. $|z| = |\bar{z}| = |-z|$,
12. $|\Re z| \leq |z|$, $|\Im z| \leq |z|$, $|z| = \sqrt{(\Re z)^2 + (\Im z)^2}$,
13. $|z| \leq |\Re z| + |\Im z| \leq \sqrt{2}|z|$
14. $|z\xi| = |z||\xi|$,
15. $z\xi = 0$ si y sólo si $z = 0$ ó $\xi = 0$ (de (10) y (14)),
16. $\Re z = |z|$ si y sólo si $z = |z|$.

(1.55)

Es también claro que $\Re(z) = \Re(\bar{z})$, $\Im(z) = -\Im(\bar{z})$, $\Re(z) = \Im(iz)$ y que $\Im(z) = -\Re(iz)$.

Si z, ξ y ζ son números complejos, se verifica inmediatamente a partir de (1.48) y (1.50) que

1. $(z + \xi) + \zeta = z + (\xi + \zeta)$,
2. $z + \xi = \xi + z$,
3. $z + 0 = z$,
4. $z + (-z) = 0$.

(1.56)

Para $a \neq 0$ real y z complejo, escribiremos

$$a^{-1}z = \frac{z}{a} = z/a = \left(\frac{\Re(z)}{a}, \frac{\Im(z)}{a} \right).$$

Definimos ahora, para $z \in \mathbb{C}$, $z \neq 0$,

$$z^{-1} := \frac{\bar{z}}{|z|^2}. \quad (1.57)$$

Es también usual escribir $z^{-1} = \frac{1}{z} = 1/z$ y $z^{-1}\xi = \frac{\xi}{z} = \xi/z$. Nótese que

$$\frac{\xi}{z} = \frac{\xi\bar{z}}{|z|^2}, \quad (1.58)$$

fórmula que suministra la manera más cómoda de efectuar la división de números complejos.

Con un poco de paciencia se verifica, a partir de (1.48) y (1.57), que

$$\begin{aligned} 1. & (z\xi)\zeta = z(\xi\zeta), \\ 2. & z\xi = \xi z, \\ 3. & z \cdot 1 = z, \\ 4. & zz^{-1} = 1, \quad z \neq 0. \end{aligned} \quad (1.59)$$

Además

$$z \cdot 0 = 0 \quad (1.60)$$

y

$$z(\xi + \zeta) = z\xi + z\zeta. \quad (1.61)$$

Tal como en el caso de los números reales, si $a, b \in \mathbb{C}$, la ecuación $a + x = b$ tiene la solución única $x = b + (-a) = b - a$. De igual manera, si $a \neq 0$, también $ax = b$ tiene la solución única $x = ba^{-1} = b/a$. Las propiedades algebraicas de $(\mathbb{C}, +, \cdot)$ son enteramente similares a las de $(\mathbb{R}, +, \cdot)$. En $\mathbb{C}$ no existe, sin embargo, una relación de orden semejante a la que existe en $\mathbb{R}$, es decir, que sea compatible con $(+)$ y $(\cdot)$. Véase al respecto el ejercicio 1.40.

La siguiente relación es muy importante en la teoría de los números complejos:

$$|z + \xi| \leq |z| + |\xi|. \quad (1.62)$$

En efecto,

$$\begin{aligned} |z + \xi|^2 &= (z + \xi) \overline{(z + \xi)} = |z|^2 + z\bar{\xi} + \bar{z}\xi + |\xi|^2 \\ &= |z|^2 + 2\Re(z\bar{\xi}) + |\xi|^2 \leq |z|^2 + 2|z||\xi| + |\xi|^2 \\ &= (|z| + |\xi|)^2, \end{aligned}$$

como se deduce de (4), (6), (8), (9), (11), (12) y (14) de (1.55). Nótese que de la demostración, la igualdad en (1.62) es cierta si y sólo si $\Re(z\bar{\xi}) = |z\bar{\xi}|$ o, lo que es lo mismo (de (1.55), (16)), si y sólo si $z\bar{\xi} = |z\bar{\xi}|$, que se da si y sólo si $\xi = 0$, o $\xi \neq 0$ y $z = a\xi$, $a \in \mathbb{R}$, $a \geq 0$ (tómese $a = |z|/|\xi|$). En total, (1.62) es una igualdad si y sólo si z, ξ están sobre una misma semi-recta que parta del origen (es decir, sobre un conjunto de la forma $\{az : a \in \mathbb{R}_+\}$, $z \in \mathbb{C}$, $z \neq 0$). De (1.62) se deduce inmediatamente, teniendo en cuenta que si a y x son reales entonces $|x| \leq a$ si y sólo si $-a \leq x \leq a$, que

$$||z| - |\xi|| \leq |z - \xi|. \quad (1.63)$$

En efecto, $|z| \leq |z - \xi| + |\xi|$ y $|\xi| \leq |z - \xi| + |z|$, de lo cual $-|z - \xi| \leq |z| - |\xi| \leq |z - \xi|$.

Tal como lo hicimos para los números reales, definimos inductivamente, para $z \in \mathbb{C}$,

$$\begin{aligned} 1. & z^0 = 1, \\ 2. & z^n = z^{n-1}z, \quad n = 1, 2, 3, \dots \end{aligned} \quad (1.64)$$

También,

$$z^n = (z^{-1})^{-n}, \quad z \neq 0, \quad n = -1, -2, -3, \dots \quad (1.65)$$

Obsérvese que $(z\xi)^{-1} = z^{-1}\xi^{-1}$ cuando $z\xi \neq 0$. Si m, n son enteros, es fácil verificar (por inducción sobre n si $n \geq 0$, y usando la relación (1.65) si $n < 0$) que

$$\begin{aligned} 1. & z^n z^{-1} = z^{n-1}, \\ 2. & z^{m+n} = z^m z^n, \\ 3. & (z^n)^{-1} = z^{-n}, \\ 4. & (z^m)^n = z^{mn} \end{aligned} \quad (1.66)$$

para todo $z \in \mathbb{C}$ ($z \neq 0$, si alguno de los números m o n es menor que cero). Demostraremos (3) y (4) suponiendo que (1) y (2) ya han sido demostrados (véase al respecto la sección 1.7). Para (3) obsérvese que, de (2), $z^n z^{-n} = z^{n+(-n)} = z^0 = 1$, de lo cual $z^{-n} = (z^n)^{-1}$. Para demostrar (4), supongamos primero que $n \geq 0$. La afirmación es clara si $n = 0$. Supongámosla para n . Entonces $(z^m)^{n+1} = (z^m)^n z^m = z^{mn} z^m = z^{mn+m} = z^{m(n+1)}$, y la afirmación es válida para todo $n \geq 0$. Ahora, si $n < 0$, entonces $(z^m)^n = [(z^m)^{-1}]^{-n} = (z^{-m})^{-n} = z^{(-m)(-n)} = z^{mn}$ (pues $-n > 0$). Se tiene también, que

$$(z\xi)^m = z^m \xi^m \quad (1.67)$$

donde $z\xi \neq 0$ si $m < 0$. Esto es obvio, por inducción, si $m \geq 0$. Y si $m < 0$ entonces $(z\xi)^m = [(z\xi)^{-1}]^{-m} = (\xi^{-1}z^{-1})^{-m} = (\xi^{-1})^{-m} (z^{-1})^{-m} = z^m \xi^m$, pues $-m > 0$. Obviamente $z^{-1} \neq 0$ si $z \neq 0$, y

$$(z^{-1})^{-1} = z, \quad (z\xi)^{-1} = \xi^{-1}z^{-1}, \quad z, \xi \neq 0, \quad (1.68)$$

lo cual usamos en la demostración de (1.67). Si $m = 2q + r$, $r = 0, 1$, la relación

$$i^m = (-1)^q i^r \quad (1.69)$$

es ocasionalmente útil.

Las siguientes relaciones obvias son frecuentemente útiles:

$$\begin{aligned} 1. & |z^{-1}| = |z|^{-1}, \\ 2. & \left| \frac{\xi}{z} \right| = \frac{|\xi|}{|z|}, \quad z \neq 0. \end{aligned} \quad (1.70)$$

La primera resulta de observar que $|z^{-1}| |z| = |z^{-1}z| = |1| = 1$. La segunda, de $|\xi z^{-1}| = |\xi| |z|^{-1}$. También,

$$|z^m| = |z|^m, \quad m \in \mathbb{Z} \quad (z \neq 0 \text{ si } m < 0), \quad (1.71)$$

cuya verificación es inmediata (por inducción si $m \geq 0$ y usando la relación (1.65) si $m < 0$).

Si $z = (a, b)$ es un número complejo, $|z| = \sqrt{a^2 + b^2}$; y si $z \neq 0$, $z/|z| = (a/\sqrt{a^2 + b^2}, b/\sqrt{a^2 + b^2})$, el cual es un punto sobre el círculo unidad $x^2 + y^2 = 1$. Por lo tanto, existe $0 \leq \theta < 2\pi$ tal que

$$\frac{z}{|z|} = (\cos\theta, \sin\theta) = \cos\theta + i\sin\theta, \quad 0 \leq \theta < 2\pi. \quad (1.72)$$

Este es un hecho aceptado como obvio, pero la demostración formal requiere conocimientos básicos de trigonometría, los cuales, por definición, "trascienden" los dominios del álgebra (para una presentación rigurosa, véase [9], capítulo 1, sección 1.5), pero una cierta familiaridad con las nociones intuitivas usuales puede ser suficiente para nuestros propósitos. La exclusión del valor 2π en (1.72) se hace con el fin de tener unicidad para θ (pues $\cos 2\pi = \cos 0$, $\sin 2\pi = \sin 0$). El número θ se denomina el *argumento* (natural) de z y se denota con $\text{Arg}(z)$. Nótese que, por definición, $0 \leq \text{Arg}(z) < 2\pi$.

Si para $\theta \in \mathbb{R}$ definimos

$$e^{i\theta} := \cos\theta + i\sin\theta, \quad (1.73)$$

es claro entonces que

$$z = |z| e^{i\text{Arg}(z)}, \quad (1.74)$$

lo cual se conoce como la *forma polar* de z . El término de la izquierda en (1.73), a pesar de sugerir la presencia del número e , (lo cual a la larga es cierto), es en principio solamente una notación abreviada, muy conveniente, del término de la derecha. Como veremos a continuación, esta notación es plenamente justificable desde un punto de vista estrictamente matemático.

Ejemplo 1.2. Si z es real y $z > 0$, es claro que $\text{Arg}(z) = 0$. A su vez, $\text{Arg}(-1) = \pi$, como se deduce de la evidente pero curiosa fórmula

$$e^{\pi i} + 1 = 0, \quad (1.75)$$

debida a Euler, la cual involucra los números más notables de la matemática: $0, 1, e, \pi, i$. También $\text{Arg}(i) = \pi/2$, mientras que $\text{Arg}(-i) = 3\pi/2$.

Obsérvese que si $z \neq 0$,

$$\text{Arg}(z) = \text{Arg}\left(\frac{z}{|z|}\right). \quad (1.76)$$

Las relaciones

$$\begin{aligned} 1. & |e^{i\theta}| = 1, \\ 2. & e^{-i\theta} := \cos\theta - i\sin\theta = \overline{e^{i\theta}} = (e^{i\theta})^{-1} \\ 3. & e^{i\theta} e^{i\theta'} = e^{i(\theta+\theta')} \end{aligned} \quad (1.77)$$

son consecuencia de identidades trigonométricas elementales. En este caso, de $\sin^2\theta + \cos^2\theta = 1$, $\cos(-\theta) = \cos\theta$, $\sin(-\theta) = -\sin\theta$, $\cos(\theta + \theta') = \cos\theta\cos\theta' - \sin\theta\sin\theta'$, y $\sin(\theta + \theta') = \sin\theta\cos\theta' + \cos\theta\sin\theta'$. Las relaciones (1.77) justifican la notación $e^{i\theta}$ para el número complejo $\cos\theta + i\sin\theta$ (pues implican que $e^{i\theta}$ se comporta en gran medida como lo haría e^θ , el número e elevado a la potencia θ , cuando $\theta \in \mathbb{R}$. Debe entenderse, sin embargo, que aunque (1.73) define bien $e^{i\theta}$, $\theta \in \mathbb{R}$, en ninguna forma permite definir el número real e ni dar sentido a lo que puede significar e^θ , cuando $\theta \in \mathbb{R}$ (sobre todo, si $\theta \notin \mathbb{Q}$). Este no es un problema fácil. De hecho, una definición razonable de e (o de e^x , $x \in \mathbb{R}$) es imposible dentro del ámbito restringido del álgebra, requiriendo, en una forma u otra, la ayuda de procesos infinitos: límites, derivadas, integrales, series o semejantes). Véase, al respecto de todo esto, [7], capítulo 1, sección 1.5 y capítulo 5, nota 5.10). Nótese, en particular, que (1.77), (3) implica inductivamente que

$$(e^{i\theta})^n = e^{in\theta}, \quad n \in \mathbb{N}. \quad (1.78)$$

De hecho, (1.77), (1) (2) y (3) implican conjuntamente, por vía de (1.65) que esta relación vale para todo $n \in \mathbb{Z}$. Nótese que (1.78) dice en realidad que

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta \quad (1.79)$$

para todo $n \in \mathbb{N}$ (de hecho, para todo $n \in \mathbb{Z}$), lo cual tiene una apariencia menos trivial que (1.78), a la cual es, sin embargo, equivalente.

De (1.73) es claro que

$$e^{i\theta} = 1 \text{ si y sólo si } \theta = 2k\pi, \quad k \in \mathbb{Z}, \quad (1.80)$$

pues $\cos\theta = 1$ implica que $\theta = 2k\pi$, $k \in \mathbb{Z}$, en cuyo caso, $\sin\theta = 0$. Esto implica que $e^{i\theta} = e^{i\theta'}$ si y sólo si $\theta = \theta' + 2k\pi$, $k \in \mathbb{Z}$. En particular, si $z \neq 0$, $z = |z|e^{i\theta}$ si y sólo si $\theta = \text{Arg}(z) + 2k\pi$, $k \in \mathbb{Z}$, así que si $z = |z|e^{i\theta}$, $\theta = \text{Arg}(z)$ si y sólo si $0 \leq \theta < 2\pi$.

Las siguientes relaciones son frecuentemente útiles. Si $\text{Arg}(z) = \theta$ y $\text{Arg}(z') = \theta'$, entonces

$$\text{Arg}(zz') = \begin{cases} \theta + \theta', & 0 \leq \theta + \theta' < 2\pi, \\ \theta + \theta' - 2\pi, & 2\pi \leq \theta + \theta'. \end{cases} \quad (1.81)$$

$$\text{Arg}(z^{-1}) = \text{Arg}(\bar{z}) = \begin{cases} 0, & \text{Arg}(z) = 0, \\ 2\pi - \text{Arg}(z), & \text{Arg}(z) \neq 0. \end{cases} \quad (1.82)$$

Finalmente,

$$\text{Arg}(-z) = \begin{cases} \text{Arg}(z) + \pi, & \text{Arg}(z) \neq \pi, \\ 0, & \text{Arg}(z) = \pi. \end{cases} \quad (1.83)$$

Nótese también que si $n \in \mathbb{Z}$, y que si $z = re^{i\theta}$, $r \neq 0$, entonces

$$z^n = r^n e^{in\theta}, \quad n \in \mathbb{Z}. \quad (1.84)$$

Las relaciones (1.78) (1.79) y (1.84) se conocen como las fórmulas de De Moivre.

Nota 1.28. Usando las propiedades ya establecidas de los números complejos, y en particular la relación $i^2 = -1$, se obtiene que

$$\begin{aligned} (a+bi)(c+di) &= a(c+di) + bi(c+di) \\ &= ac + adi + bci + bdi^2 \\ &= (ac - bd) + (ad + bc)i \\ &= (ac - bd, ad + bc) = (a.b)(c, d), \end{aligned}$$

que es la segunda de las fórmulas en la definición (1.48). Es decir, las propiedades de la adición y la multiplicación de números complejos, una vez establecidas, permiten recuperar la definición de esta última operación, haciendo innecesario el tener que memorizarla.

Sean finalmente $n > 0$ un entero y $z \neq 0$ un número complejo. Supóngase que $z = re^{i\theta}$, $r > 0$. Si para $k = 0, 1, 2, \dots, n-1$, definimos

$$z_k = r^{1/n} e^{i\frac{\theta+2k\pi}{n}} \quad (1.85)$$

($r^{1/n}$ ha sido definido en la sección 1.7), entonces $z_k^n = re^{i(\theta+2k\pi)} = re^{i\theta} e^{2k\pi i} = re^{i\theta} = z$, así que los z_k son raíces n -ésimas de z . Tales raíces son distintas, pues si $z_k = z_j$, $0 \leq k, j \leq n-1$, $k \neq j$, entonces $z_k z_j^{-1} = e^{\frac{2(k-j)\pi}{n}i} \neq 1$, ya que $(k-j)/n$ no es un entero. Sea ahora

$$w_n = e^{\frac{2\pi}{n}i}. \quad (1.86)$$

Es claro que $w_n^k = e^{\frac{2\pi k}{n}i}$, $k = 0, 1, 2, \dots, n-1$, y que $w_n^n = 1$, así que también $(w_n^k)^n = (w_n^n)^k = 1$, $1 \leq k \leq n-1$. Por lo tanto, las w_n^k son n raíces n -ésimas de 1, distintas entre sí. Nótese que

$$z_k = r^{1/n} e^{i\frac{\theta}{n}} w_n^k, \quad k = 0, 1, \dots, n-1, \quad (1.87)$$

así que las raíces z_k de z pueden obtenerse a partir de la raíz particular $r^{1/n} e^{i\frac{\theta}{n}}$ de z y de las w_n^k , (sin embargo, el cálculo de las z_k es en general más fácil a partir de (1.85) que de (1.87)).

Queremos demostrar que las z_k son las únicas raíces n -ésimas posibles de z , lo cual implicará que las w_n^k , $k = 0, 1, \dots, n-1$, son las únicas raíces n -ésimas posibles de 1. Ahora, si $\xi^n = z$ y $\xi = se^{i\varphi}$, donde $s = |\xi|$, entonces $s^n = r$, así que $s = r^{1/n}$ y $e^{i\theta} = e^{i(n\varphi)}$, o sea que $n\varphi - \theta = 2m\pi$, $m \in \mathbb{Z}$, de lo cual $\varphi = \theta/n + 2(l+k/n)\pi$, donde $m = ln+k$, $l, k \in \mathbb{Z}$, $0 \leq k < n$ (teorema 1.10). Entonces $\xi = z_k$, como se quería establecer. Hemos demostrado entonces el siguiente teorema.

Teorema 1.23. Si para $n = 1, 2, \dots$, w_n está dada por (1.86), las w_n^k , $0 \leq k \leq n-1$, son n raíces n -ésimas distintas de la unidad, y las únicas posibles. Si además $z = re^{i\theta}$, donde $z \neq 0$ y $r = |z|$, y

$$z_k = r^{1/n} e^{i\frac{\theta+2k\pi}{n}} = r^{1/n} e^{i\frac{\theta}{n}} w_n^k, \quad k = 0, 1, \dots, n-1, \quad (1.88)$$

las z_k son n raíces n -ésimas distintas de z , y las únicas posibles.

Ejemplo 1.3. Así, $w_3 = w_3^1 = e^{2\pi i/3} = -1/2 + \sqrt{3}i/2$, $w_3^0 = 1$ y $w_3^2 = e^{4\pi i/3} = -1/2 - \sqrt{3}i/2$ son todas las raíces cúbicas de 1. Como $i = e^{i\pi/2}$, y $e^{i\pi/6} = \sqrt{3}/2 + i/2$, las raíces cúbicas de $z = i$ serán $z_0 = e^{i\pi/6} = \sqrt{3}/2 + i/2$,

$z_1 = e^{i\pi/6} (-1/2 + \sqrt{3}i/2) = (\sqrt{3}/2 + i/2) (-1/2 + \sqrt{3}i/2) = -\sqrt{3}/2 + i/2$,
 $z_2 = (\sqrt{3}/2 + i/2) (-1/2 - \sqrt{3}i/2) = -i$. Naturalmente, es más cómodo calcular directamente $e^{i\pi/6}$, $e^{5\pi i/6}$, $e^{3\pi i/6}$.

Nota 1.29. Si $n \geq 1$ es un entero y $w_n = e^{2\pi i/n}$ es como en el teorema 1.23, no sobra recalcar que si $k \in \mathbb{Z}$ entonces $w_n^k = 1$ si y sólo si $n \mid k$, pues $w_n^r \neq 1$ para $r = 1, 2, \dots, n-1$ (teorema 1.23), y si $n \nmid k$ entonces $k = ln + r$ con $l, r \in \mathbb{Z}$, $1 \leq r \leq n-1$, de lo cual $w_n^k = 1 = w_n^r$, que es absurdo.

Nota 1.30. Si $n \geq 1$, la raíz w_n genera al conjunto de todas las raíces n -ésimas de 1, en el sentido de que cualquier otra raíz n -ésima de 1 es de la forma w_n^k , $k \in \mathbb{Z}$ (teorema 1.23). Más generalmente, si w es una raíz n -ésima de 1 tal que $\{w^k : k \in \mathbb{Z}\}$ es el conjunto de todas las posibles raíces n -ésimas de 1, se dice que w es una *raíz primitiva n -ésima de la unidad*. Evidentemente 1 es una raíz primitiva n -ésima de la unidad si y sólo si $n = 1$, y si $n > 1$ y w es una tal raíz, del teorema 1.23 se deduce que $w = w_n^k$, $1 \leq k \leq n-1$ ($w_n = e^{2\pi i/n}$). Como entonces $w_n = w^l = w_n^{kl}$ para algún $l \in \mathbb{Z}$, deberá tenerse que $kl - 1 = mn$ para algún $m \in \mathbb{Z}$ (nota 1.29), así que $1 = kl + (-m)n$, de lo cual $1 = \text{mcd}(k, n)$. Recíprocamente, si $1 \leq k \leq n-1$ y $1 = \text{mcd}(k, n) = kl + mn$, $l, k \in \mathbb{Z}$, entonces $(w_n^k)^l = w_n \cdot (w_n^n)^{(-m)} = w_n$, lo cual implica que $w = w_n^k$ es una raíz primitiva n -ésima de la unidad. Es decir, si $w_n = e^{2\pi i/n}$, w es una raíz primitiva n -ésima de la unidad si y sólo si $w = w_n^k$, donde $1 \leq k \leq n-1$ y $\text{mcd}(k, n) = 1$. Nótese, por ejemplo, que i es una raíz cuarta primitiva de 1, mientras que (-1) no lo es; pero i no es una raíz octava primitiva de 1 (sin embargo $w = (\sqrt{2} + i\sqrt{2})/2$ y $w = (\sqrt{2} - i\sqrt{2})/2$ si lo son).

1.9. Sistemas numéricos, dominios y campos

Consideraremos en esta sección algunas estructuras que se generan naturalmente dentro de los números complejos: *sistemas, dominios y campos numéricos*. Estas han estado en la génesis de muchas de las estructuras abstractas que constituyen la esencia del álgebra moderna. Pensamos que estudiarlas en su contexto propio puede ser conveniente e instructivo, tanto más cuanto que este contexto es excepcionalmente rico.

Si $S \subseteq \mathbb{C}$ es tal que

i. $0, 1 \in S$,

ii. Dados $a, b \in S$, también $a + b$ y $ab \in S$,

se dice que $(S, +, \cdot)$ es un *sistema numérico*. Por ejemplo, $(\mathbb{N}, +, \cdot)$ es un *sistema numérico*. Por otra parte, si $(S, +, \cdot)$ es un sistema numérico entonces $0, 1 \in S$, y si $n \in \mathbb{N}$ es tal que $n \in S$, (ii) implica que también $n + 1 \in S$. Luego S es inductivo, así que $\mathbb{N} \subseteq S$; es decir, *todo sistema numérico contiene los números naturales*. Otros sistemas numéricos son $(\mathbb{R}_+, +, \cdot)$ y $(\mathbb{Q}_+, +, \cdot)$, donde $\mathbb{Q}_+ = \mathbb{Q} \cap \mathbb{R}_+$.

Si $(S, +, \cdot)$ es un sistema numérico tal que

iii. $-S = \{-a : a \in S\} \subseteq S$,

así que $-S = S$, se dice que $(S, +, \cdot)$ es un *sistema aditivamente simétrico*, o un *dominio numérico*, o, simplemente, que es un *dominio*. Un dominio es entonces un *sistema numérico que contiene los inversos aditivos de sus elementos*. Es claro, por ejemplo que $(\mathbb{Z}, +, \cdot)$ es un *dominio*, y que si $(S, +, \cdot)$ es un dominio entonces $\mathbb{Z} \subseteq S$ (pues, como $\mathbb{N} \subseteq S$, también $(-\mathbb{N}) \subseteq S$) así que *todo dominio contiene los enteros*. Un dominio interesante es, como veremos más adelante, $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$, denominado el *dominio de los enteros de Gauss*, el cual no está exento de importancia.

Si $(K, +, \cdot)$ es un dominio y $K^* = K \setminus \{0\}$ es tal que

$$(K^*)^{-1} = \{a^{-1} : a \in K^*\} \subseteq K^*,$$

o sea, que $(K^*)^{-1} = K^*$, se dice que $(K, +, \cdot)$ es un *dominio multiplicativamente simétrico*, que es un *campo numérico* o, simplemente, que es un *campo*. Por ejemplo $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ son campos, y si $(K, +, \cdot)$ es un campo, entonces $\mathbb{Q} \subseteq K$. En efecto, $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\} \subseteq K^*$, así que si $a, b \in \mathbb{Z}$, $b \neq 0$, entonces $b^{-1} \in K$, y, en virtud de (ii), también $a/b = ab^{-1} \in K$. Un campo es entonces un *dominio que contiene, junto con sus elementos no nulos, los inversos multiplicativos de estos*. Como es claro, el dominio $(\mathbb{Z}, +, \cdot)$, no es un campo.

Si K, L son campos numéricos y $K \subseteq L$, se dice que K es un *subcampo* de L o que L es una *extensión* de K . En vista de lo anterior, *todo campo es un subcampo de $\mathbb{C}$ y una extensión de $\mathbb{Q}$* . Es claro, por ejemplo, que

$$\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \quad (1.89)$$

es un campo numérico, el cual es un subcampo de $\mathbb{R}$ (ejercicio 1.56), mientras que

$$\mathbb{Q}[i] := \{a + bi : a, b \in \mathbb{Q}, i^2 = -1\} \quad (1.90)$$

es también un campo que extiende propiamente a $\mathbb{Q}$ pero no es un subcampo de $\mathbb{R}$ (ejercicio 1.56). Por el contrario,

$$\tilde{\mathbb{Q}} := \{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\} \quad (1.91)$$

no es un campo (véase el ejercicio 1.58), mientras que

$$\mathbb{Q}[\sqrt[3]{2}] := \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\} \quad (1.92)$$

sí lo es (véase ejercicio 1.57). Nótese que

$$\mathbb{C} = \mathbb{R}[i] := \{a + bi : a, b \in \mathbb{R}, i^2 = -1\} \quad (1.93)$$

Teorema 1.24. Si $(S, +, \cdot)$ es un dominio, existe un campo $(\hat{S}, +, \cdot)$ tal que

1. $S \subseteq \hat{S}$,
2. Si K es un campo y $S \subseteq K$, entonces $\hat{S} \subseteq K$.

Demostración. Como se verifica inmediatamente, si $S^* = S \setminus \{0\}$, entonces

$$\hat{S} := \{a/b : a \in S, b \in S^*\} \quad (1.94)$$

es un campo que satisface (1) y (2). $\square$

Definición 1.19. Si $(S, +, \cdot)$ es un dominio, se dice que $(\hat{S}, +, \cdot)$ es el campo de cocientes de $(S, +, \cdot)$.

Nota 1.31. Si $(S, +, \cdot)$ es un sistema numérico, siempre existe un dominio numérico $(\tilde{S}, +, \cdot)$ tal que

1. $S \subseteq \tilde{S}$,
2. Si $(S', +, \cdot)$ es un dominio numérico y $S \subseteq S'$, entonces $\tilde{S} \subseteq S'$.

Basta, en efecto, tomar $\tilde{S} = S \cup (-S)$. Se dice que $\tilde{S}$ es el dominio de saldos o el dominio de activos y pasivos de S (este lenguaje proviene de la contabilidad, oficio en el cual se originó el concepto). Nótese que $\tilde{\mathbb{N}} = \mathbb{Z}$ y que $\tilde{\mathbb{Z}} = \mathbb{Q}$. Si S es ya un dominio, es claro que $\tilde{S} = S$. Y si S es un campo, entonces $\hat{S} = S$.

1.10. Polinomios sobre los sistemas numéricos

La teoría de los polinomios sobre los dominios y campos abstractos es el corazón del álgebra moderna. Sobre los dominios y campos numéricos lo es, igualmente, del álgebra clásica. Como en la sección anterior, pensamos que considerar estos casos especiales, particularmente ricos, puede ser una excelente motivación para el estudio de sus contrapartes abstractas. Las analogías entre ambos casos pueden ser, además, de gran ayuda para la comprensión de estas últimas. Los conceptos y resultados de esta sección no serán indispensables en los capítulos 2 y 3 de este trabajo (sólo en el capítulo 11 tendrán algún papel), pero serían fundamentales en muchas partes de un posible segundo curso. Dada la similitud de muchos de los resultados de esta sección con los de secciones previas, similitud que no es gratuita, hemos considerado apropiado incluirla en este punto.

Sean $(S, +, \cdot)$ un dominio numérico y $x \notin \mathbb{C}$ un objeto fijo. El conjunto de las sumas "formales"

$$f(x) = \sum_{k=0}^{\infty} a_k x^k \quad (1.95)$$

tales que para algún $m \geq 0$, $a_k = 0$ para todo $k \geq m$, así que la suma en (1.95) es realmente finita), se denomina el sistema de los polinomios sobre S en la indeterminada x y se denota con $S[x]$. Se entiende que

$$\sum_{k=0}^{\infty} a_k x^k = \sum_{k=0}^{\infty} b_k x^k$$

si y sólo si $a_k = b_k$ para todo $k \geq 0$.

Nota 1.32. A pesar de la notación funcional utilizada, $f(x) \in S[x]$ no es, en principio, una función (nótese que x es un objeto fijo, no una variable). Sin embargo, $f(x)$ define de manera natural una función $f : S \rightarrow S$, por

$$f(s) = \sum_{k=0}^{\infty} a_k s^k. \quad (1.96)$$

Nótese que la suma de la derecha en (1.96) es finita y define efectivamente un elemento de S . Aunque en el caso de los sistemas numéricos no es muy importante distinguir entre el polinomio $f(x)$ y la función f , es mejor hacerlo, así sea por las razones siguientes: en primer lugar, si $(K, +, \cdot)$ es

otro dominio tal que $S \subseteq K$, también $S[x] \subseteq K[x]$, así que $f(x) \in K[x]$, y por lo tanto, $f(x)$ define también, de manera natural, una aplicación de K en sí mismo, por medio de (1.96), la cual se denotaría aún con f . Así la función f definida por $f(x)$ *no está unívocamente determinada*. Por otra parte, no se puede excluir, a priori, que exista otro polinomio $g(x) \in S[x]$, $g(x) \neq f(x)$, tal que $g(s) = f(s)$ para todo $s \in S$ (esto no se da en el caso de los polinomios sobre los sistemas numéricos, pero puede darse en el de los polinomios sobre dominios finitos, a los cuales extenderemos, en el futuro, la noción de polinomio).

Si $f(x)$ es como en (1.95) y $a_k = 0$ para $k > m$, es usual escribir

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m. \quad (1.97)$$

Nótese que esto sugiere que $x^0 = 1$ y $x^1 = x$, lo cual aceptaremos en lo que sigue, y no excluye que $a_k = 0$ para $k \leq m$. Definimos

$$0(x) = \sum_{k=0}^{\infty} a_k x^k, \quad a_k = 0 \text{ para todo } k, \quad (1.98)$$

y

$$1(x) := \sum_{k=0}^{\infty} b_k x^k, \quad b_0 = 1, \quad b_k = 0 \text{ para todo } k > 0, \quad (1.99)$$

así que, según (1.97),

$$0(x) = 0, \quad 1(x) = 1 \quad (1.100)$$

lo cual identifica los polinomios $0(x)$ y $1(x)$, respectivamente, con los números 0 y 1. De hecho, S puede considerarse como un subconjunto de $S[x]$, identificando $a \in S$ con el polinomio $a + 0x + 0x^2 + \cdots$ ($a_0 = a$, $a_k = 0$ para todo $k > 0$). Para $f(x)$ como en (1.97), definimos

$$-f(x) = (-f)(x) := \sum_{k=0}^{\infty} (-a_k) x^k. \quad (1.101)$$

Es claro que $(-f)(x) \in S[x]$.

Si $f(x) = \sum_{k=0}^{\infty} a_k x^k$ y $g(x) = \sum_{k=0}^{\infty} b_k x^k$ están en $S[x]$, definimos también

$$f(x) + g(x) := \sum_{k=0}^{\infty} (a_k + b_k) x^k. \quad (1.102)$$

Obsérvese que

$$f(x) + g(x) \in S[x], \quad (1.103)$$

pues si $a_k = 0$ para $k > m$ y $b_k = 0$ para $k > n$, entonces

$$a_k + b_k = 0, \quad k > \max\{m, n\} \quad (1.104)$$

Nótese también que

$$f(x) + 0(x) = f(x) + 0 = f(x) = 0 + f(x) = 0(x) + f(x). \quad (1.105)$$

Por otra parte,

$$f(x) + (-f)(x) = (-f)(x) + f(x) = 0(x). \quad (1.106)$$

También es obvio que

$$(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x)) \quad (1.107)$$

y que

$$f(x) + g(x) = g(x) + f(x). \quad (1.108)$$

Definamos ahora

$$f(x) \cdot g(x) = f(x)g(x) := \sum_{k=0}^{\infty} c_k x^k, \quad (1.109)$$

donde

$$c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i=0}^k a_{k-i} b_i = \sum_{i+j=k} a_i b_j. \quad (1.110)$$

Nótese que si $i + j = k > m + n$ entonces $i > m$ o $j > n$, así que

$$c_k = 0, \quad k > m + n; \quad c_{m+n} = a_m b_n. \quad (1.111)$$

La segunda relación en (1.111) resulta de observar que si $i + j = m + n$ e $i < m$ entonces $j > n$, y si $j < n$ entonces $i > m$. Además, $i = m$ si y sólo si $j = n$. Entonces

$$f(x) \cdot g(x) \in S[x], \quad (1.112)$$

y, como es obvio,

$$f(x) \cdot 1(x) = f(x) \cdot 1 = f(x) = 1 \cdot f(x) = 1(x) \cdot f(x). \quad (1.113)$$

Veamos que

$$(f(x)g(x))h(x) = f(x)(g(x)h(x)). \quad (1.114)$$

Escribamos $f(x) = \sum_{k=0}^{\infty} a_k x^k$, $g(x) = \sum_{k=0}^{\infty} b_k x^k$, $h(x) = \sum_{k=0}^{\infty} c_k x^k$, y supongamos que $f(x)(g(x)h(x)) = \sum_{k=0}^{\infty} d_k x^k$ y $(f(x)g(x))h(x) = \sum_{k=0}^{\infty} l_k x^k$. Entonces

$$\begin{aligned} d_m &= \sum_{i=0}^m a_{m-i} \left(\sum_{j=0}^i b_{i-j} c_j \right) = \sum_{(i,j) \in T} a_{m-i} b_{i-j} c_j \\ &= \sum_{j=0}^m \sum_{i=j}^m a_{m-i} b_{i-j} c_j = \sum_{j=0}^m \left(\sum_{k=0}^{m-j} a_{m-j-k} b_k \right) c_j, \end{aligned}$$

donde $T = \{(i, j) : 0 \leq i \leq m, 0 \leq j \leq i\} = \{(i, j) : 0 \leq j \leq m, j \leq i \leq m\}$ (véase Figura 1.1) y $k = i - j$, j fijo. Entonces, $d_m = l_m$, $m \geq 0$. Esto demuestra la afirmación.

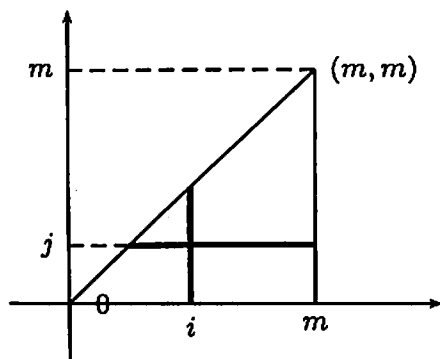


Figura 1.1

La región de sumación es el triángulo de vértices 0 , m , (m, m) . (Para cada $0 \leq i \leq m$, la suma es sobre el segmento vertical. Para cada $0 \leq j \leq m$, fijo, sobre el segmento horizontal).

Es también claro que

$$f(x) \cdot 0(x) = f(x) \cdot 0 = 0 = 0 \cdot f(x) = 0(x) \cdot f(x). \quad (1.115)$$

y que

$$\begin{aligned} f(x)(g(x) + h(x)) &= f(x)g(x) + f(x)h(x), \\ (g(x) + h(x))f(x) &= g(x)f(x) + h(x)f(x). \end{aligned} \quad (1.116)$$

De (1.110) se deduce finalmente que

$$f(x)g(x) = g(x)f(x). \quad (1.117)$$

Nota 1.33. Las propiedades (1.103) a (1.108) y (1.112) a (1.116) son básicas para una teoría coherente de los polinomios. Cuando $(S, +, \cdot)$ es sólo un sistema numérico, (1.101) puede no tener sentido, y tampoco lo tendría (1.106). Por esta razón sólo definimos $S[x]$ cuando S es, como mínimo, un dominio numérico.

Aunque podría hacerse, la multiplicación de polinomios no se efectúa generalmente mediante (1.110) sino según los procedimientos usuales del álgebra elemental (véanse, [6] y [1]). La validez de estos procedimientos es consecuencia de las propiedades establecidas arriba, especialmente de las (1.113), (1.114), (1.115) y (1.117) (y hace, en cierta forma, innecesario recordar la fórmula (1.110)).

Sean $(S, +, \cdot)$ un dominio numérico, y $f(x) = \sum_{k=0}^{\infty} a_k x^k \in S[x]$. Entonces, existe $m \geq 0$ tal que $a_k = 0$ para todo $k > m$. Si $a_m \neq 0$, se dice que $f(x)$ tiene *grado* m , o que es un *polinomio de grado* m . Se dice también que m es el *grado* de $f(x)$:

$$\text{grad}(f(x)) := m$$

Sólo hemos definido arriba el grado de un polinomio $f(x)$ cuando $f(x) \neq 0(x)$, en cuyo caso

$$\text{grad}(f(x)) := \max\{k : a_k \neq 0\} \geq 0. \quad (1.118)$$

Convendremos en que

$$\text{grad}(0(x)) := -\infty. \quad (1.119)$$

Esta convención es útil teniendo en cuenta que, como se acepta usualmente, $-\infty < a$ y $-\infty + a = a + (-\infty) = -\infty$, para todo $a \in \mathbb{R}$.

Teorema 1.25. Si $(S, +, \cdot)$ es un dominio y $f(x), g(x) \in S[x]$, entonces

$$\text{grad}(f(x) + g(x)) \leq \max(\text{grad}(f(x)), \text{grad}(g(x))) \quad (1.120)$$

y

$$\text{grad}(f(x)g(x)) = \text{grad}(f(x)) + \text{grad}(g(x)). \quad (1.121)$$

Demostración. Resulta inmediatamente de las relaciones (1.104) y (1.111). Obsérvese que (1.120) es aún válida si $f(x) + g(x) = 0$ y que (1.121) también lo es si $f(x)g(x) = 0$, pues, como se deduce de (1.111) y (1.115), $f(x)g(x) = 0$ si y sólo si $f(x) = 0$ ó $g(x) = 0$. $\square$

Nota 1.34. De (1.121) se deduce también que

$$\text{grad}(f(x)) \leq \text{grad}(f(x)g(x)) \quad (1.122)$$

cualquiera que sea $g(x) \in S[x]$, $g(x) \neq 0$. Es claro además que $\text{grad}(f(x)) = 0$ si y sólo si $f(x) = a \in S$, $a \neq 0$.

Definición 1.20. Sean $f(x), g(x) \in S[x]$. Se dice que $f(x)$ divide a $g(x)$ en $S[x]$, que $f(x)$ es un divisor de $g(x)$ en $S[x]$, o que $f(x)$ es un factor de $g(x)$ en $S[x]$, si $f(x) \neq 0$, y existe $h(x) \in S[x]$ tal que $g(x) = f(x)h(x)$. Se escribe $f(x) \mid g(x)$ en $S[x]$. Si $f(x) = 0$, o si $f(x)$ no es un divisor de $g(x)$, escribiremos $f(x) \nmid g(x)$.

Nota 1.35. El escribir $f(x) \mid g(x)$ asegura entonces que $f(x) \neq 0$.

Sean $(S, +, \cdot)$ un dominio y $f(x), g(x), h(x) \in S[x]$. Si $f(x) \neq 0$ entonces $f(x) \mid 0$, y si $f(x) \mid g(x)$ y $g(x) \neq 0$ se tiene que $\text{grad}(f(x)) \leq \text{grad}(g(x))$. También

$$f(x) \mid f(x), \quad f(x) \neq 0 \quad (1.123)$$

y

$$\text{Si } f(x) \mid g(x) \text{ y } g(x) \mid h(x), \text{ entonces } f(x) \mid h(x). \quad (1.124)$$

Además,

$$\text{Si } f(x) \mid g(x) \text{ y } g(x) \mid f(x), \text{ entonces } f(x) = ag(x), \quad (1.125)$$

donde $a \in S$ es tal que $a^{-1} \in S$.

Si $(S, +, \cdot)$ un dominio y $a \in S$ es tal que $a^{-1} \in S$, se dice que a es multiplicativamente invertible en S o que a es una unidad de S . El elemento unidad 1 de S es una unidad de S . Sin embargo, no toda unidad de S es un elemento unidad de S . Por ejemplo, si $S = \mathbb{Z}$, 1, -1 son (las únicas) unidades de S , y -1 no es un elemento unidad de S . Si $(S, +, \cdot)$ es un campo, todo elemento no nulo de S es de hecho una unidad. Si $S = \mathbb{Z}[i]$ es el dominio de los enteros de Gauss, las únicas unidades de S son ± 1 y $\pm i$. Esto se deduce de observar que si $a + bi \in \mathbb{Z}[i]$ y $a + bi \neq 0$, el inverso de $a + bi$ en

$\mathbb{C}$ es $(a - bi) / (a^2 + b^2)$, y como $a/a^2 + b^2$ y $b/a^2 + b^2$ deben ser enteros, si queremos que $(a + bi)^{-1} \in \mathbb{Z}[i]$, esto sólo es posible cuando $a = \pm 1$ y $b = 0$ o $a = 0$ y $b = \pm 1$.

Definición 1.21. Si $f(x), g(x) \in S[x]$ y $f(x) = ag(x)$ donde a es una unidad de S , se dice que $f(x)$ y $g(x)$ están o son asociados en $S[x]$, y se escribe $f(x) \sim g(x) \pmod{S}$.

Es claro que si $f(x) \mid h(x)$ y $g(x) \sim f(x) \pmod{S}$, también $g(x) \mid h(x)$. Además, si $f(x)g(x) \neq 0$,

$$f(x) \mid g(x) \text{ y } g(x) \mid h(x) \text{ si y sólo si } f(x) \sim g(x) \pmod{S}. \quad (1.126)$$

La teoría de la divisibilidad de polinomios sobre un dominio numérico S presenta características que son frecuentemente mejor comprendidas si se tiene en cuenta que $S[x] \subseteq \widehat{S}[x]$, donde $\widehat{S}$ es el campo de cocientes de S , como será claro más adelante (véase la nota 1.56). De hecho, la teoría de la divisibilidad de polinomios sobre campos es más rica, accesible y útil de lo que suele serlo la teoría sobre dominios. Por esta razón haremos mayor énfasis, en lo que sigue, en los polinomios sobre campos, aunque algo diremos, cuando sea fácil hacerlo, acerca de los polinomios sobre dominios. Dejaremos, sin embargo, muchos aspectos de la teoría sobre dominios a la consideración de capítulos posteriores y, algunas veces, inclusive, a la de cursos más avanzados de álgebra.

El teorema siguiente, por ejemplo, marca una diferencia notable entre el comportamiento de los polinomios sobre dominios y sobre campos.

Teorema 1.26 (Euclides). Sean $f(x), g(x) \in K[x]$ donde K es un campo numérico. Si $g(x) \neq 0$, existen polinomios $q(x), r(x) \in K[x]$ tales que $\text{grad}(r(x)) < \text{grad}(g(x))$ y que

$$f(x) = q(x)g(x) + r(x). \quad (1.127)$$

Además, $q(x)$ y $r(x)$ están unívocamente determinados por $f(x)$ y $g(x)$.

Demostración. La validez de (1.127) es evidente en cualquiera de las dos siguientes circunstancias: (i), $\text{grad}(f(x)) < \text{grad}(g(x))$ (tómese $q(x) = 0$ y $r(x) = f(x)$), y (ii), $g(x) = b \in K$, $b \neq 0$ (con $q(x) = b^{-1}f(x)$ y $r(x) = 0$). Supongamos entonces que $\text{grad}(f(x)) \geq \text{grad}(g(x)) \geq 1$, e, inductivamente, que (1.127) vale para todo polinomio cuyo grado es estrictamente menor que

$\text{grad}(f(x))$. Si entonces $f(x) = a_m x^m + \cdots + a_0$ y $g(x) = b_n x^n + \cdots + b_0$ con $a_m b_n \neq 0$ y $m \geq n \geq 1$, al definir

$$\hat{f}(x) = f(x) - b_n^{-1} a_m x^{m-n} g(x)$$

se obtiene que $\text{grad}(\hat{f}(x)) < \text{grad}(f(x))$, así que

$$\hat{f}(x) = \hat{q}(x) g(x) + \hat{r}(x)$$

donde $\hat{q}(x), \hat{r}(x) \in K[x]$ y $\text{grad}(\hat{r}(x)) < \text{grad}(g(x))$, de lo cual se deduce que

$$f(x) = q(x) g(x) + r(x)$$

con $q(x) = b_n^{-1} a_m x^{m-n} + \hat{q}(x)$ y $r(x) = \hat{r}(x)$. Esto establece (1.127). Para demostrar la unicidad de $q(x)$ y $r(x)$, supóngase que también $f(x) = q'(x) g(x) + r'(x)$ con $\text{grad}(r'(x)) < \text{grad}(g(x))$. Entonces

$$(q(x) - q'(x)) g(x) = r'(x) - r(x),$$

lo cual, dado que $g(x) \neq 0$ y que $\text{grad}(r'(x) - r(x)) < \text{grad}(g(x))$, sólo es posible si $q(x) = q'(x)$, en cuyo caso, también $r(x) = r'(x)$. Esto demuestra el teorema. $\square$

Si $q(x)$ y $r(x)$ son como en (1.127), se dice que $q(x)$ es el *cociente* y que $r(x)$ es el *residuo* (o *resto*) de dividir $f(x)$ por $g(x)$ en $K[x]$. Escribiremos

$$q(x) = q(f(x), g(x)), \quad r(x) = r(f(x), g(x)). \quad (1.128)$$

En lugar de (1.127) es también corriente escribir

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}. \quad (1.129)$$

Así,

$$\frac{x^2 - 1}{x - 1} = x + 1 + \frac{0}{x - 1} = x + 1,$$

$$\frac{x^2 - 5x + 6}{x - 1} = x - 4 + \frac{2}{x - 1}$$

Nota 1.36. El teorema 1.26 se conoce como el *algoritmo euclídeo de la división*. El proceso de demostración de (1.127) es en efecto algorítmico (repetitivo de los mismos pasos un número finito de veces), y consiste, básicamente, en reducir el problema al caso $\text{grad}(f(x)) < \text{grad}(g(x))$ (la afirmación es inmediata si $g(x) = b \in K$, $b \neq 0$). Por esta razón se sustrae

$b_n^{-1} a_m x^{m-n} g(x)$ de $f(x)$ para obtener $\hat{f}(x) = c_{m-k} x^{m-k} + \cdots + c_0$, $k \geq 1$, y, si aún $m - k > n$, se repetirá este paso y se sustraerá $b_n^{-1} c_{m-k} x^{m-k-n} g(x)$, y así sucesivamente. El propósito se logrará en un número finito de pasos. Para conocer como se ordenan las cosas para llevar esto a cabo sistemáticamente, consúltese cualquier texto de álgebra elemental. Por ejemplo [4] o [24].

Nota 1.37. Como es fácil comprobarlo, el teorema 1.26 es aún válido si $K = \mathbb{Z}$, o, de hecho, si K es cualquier dominio numérico, cuando $g(x) = b_n x^n + \cdots + b_0$ con $n \geq 0$ y $b_n = 1$. Por ejemplo,

$$\frac{x^5 - 3x^4 + 2x^3 - 3x^2 + 2x + 1}{x^2 - 3x + 2} = x^3 - 3 + \frac{(-7)x + 7}{x^2 - 3x + 2}.$$

Si $b_n \neq 1$, el resultado puede ser, sin embargo, falso. Por ejemplo, no existen $q(x), r(x) \in \mathbb{Z}[x]$ tales que $x^2 - 1 = q(x)(2x) + r(x)$ con $r(x) \in \mathbb{Z}$.

Nota 1.38. Si L es una extensión de K entonces $K[x] \subseteq L[x]$, y si $f(x), g(x) \in K[x]$, también $f(x), g(x) \in L[x]$. Como es claro, $q(f(x), g(x))$ y $r(f(x), g(x))$ son independientes de donde se efectúe la división: $K[x]$ ó $L[x]$.

Nota 1.39. Como es también claro, si K es un campo, $g(x) \mid f(x)$ en $K[x]$ si y sólo si $r(f(x), g(x)) = 0$.

El siguiente corolario simple del teorema 1.26 es, sin embargo, de gran importancia. Recordamos que si $f(x) = a_m x^m + \cdots + a_0 \in K[x]$, $f(x)$ define una aplicación $f: K \rightarrow K$ dada por

$$f(s) = a_m s^m + \cdots + a_0 \quad (1.130)$$

para todo $s \in K$

Corolario 1.9. Si K es un campo, $a \in K$ y $f(x) \in K[x]$, entonces

$$f(x) = g(x)(x - a) + f(a) \quad (1.131)$$

donde $g(x) \in K[x]$.

Demostración. Según (1.127), $f(x) = g(x)(x - a) + r(x)$ donde $g(x), r(x) \in K[x]$ y $\text{grad}(r(x)) < \text{grad}(x - a) = 1$, así que $r(x) = b \in K$. Como $f(a) = g(a)(a - a) + b = 0 + b = b$, la afirmación queda demostrada. $\square$

Definición 1.22. Si K es un dominio numérico, $f(x) \in K[x]$, y $a \in K$ es tal que $f(a) = 0$, se dice que a es una raíz de $f(x)$ en K .

Del corolario 1.9 se deduce entonces que

Corolario 1.10. Si K es un campo, $a \in K$ y $f(x) \in K[x]$, a es una raíz de $f(x)$ en K si y sólo si existe $g(x) \in K[x]$ tal que

$$f(x) = g(x)(x - a). \quad (1.132)$$

Esto implica, por otra parte, que:

Teorema 1.27. Si K es un campo, $f(x) \in K[x]$ y $\text{grad}(f(x)) = n \geq 0$, entonces $f(x)$ tiene a lo sumo n raíces distintas en K .

Demostración. La afirmación es clara si $\text{grad}(f(x)) = 0, 1$. Puede suceder que $f(x)$ no tenga raíces en K cuando $n > 1$, con lo cual la afirmación del teorema es trivialmente cierta. Pero si $f(x)$ tiene al menos una raíz $a \in K$, es posible escoger $g(x) \in K[x]$ tal que $f(x) = g(x)(x - a)$, y cualquier raíz de $f(x)$ distinta de a será una raíz de $g(x)$. Como $\text{grad}(g(x)) = n - 1$, razonando inductivamente podemos suponer que $g(x)$ tiene a lo sumo $n - 1$ raíces distintas en K . Entonces $f(x)$ tendrá a lo sumo n raíces distintas en K . $\square$

Nota 1.40. Como es claro, si $f(x) \in K[x]$ y $\text{grad}(f(x)) = n \geq 0$, $f(x)$ tendrá a lo sumo n raíces distintas en cualquier extensión L de K . Puede suceder, sin embargo, que $f(x)$ tenga una o más raíces en L y ninguna en K . Por ejemplo, $f(x) = x^2 + 1 \in \mathbb{R}[x]$ no tiene ninguna raíz en $\mathbb{R}$, pero i y $-i$ son raíces de $f(x)$ en $\mathbb{C}$. Nótese, sin embargo, que toda raíz de $f(x)$ en K es una raíz de $f(x)$ en L . Se deduce también que si $f(x) \in K[x]$ y $\text{grad}(f(x)) < n$, $f(x)$ tendrá n o más raíces en K si y sólo si $f(x) = 0$, en cuyo caso todo elemento de K es raíz. Esto implica que si $f(x), g(x) \in K[x]$, $f(x), g(x)$ definen la misma función $\varphi : L \rightarrow L$ ($\varphi(a) = f(a) = g(a)$ para todo $a \in L$) en alguna extensión L de K si y sólo si $f(x) = g(x)$ (pues $h(x) = f(x) - g(x)$ tendría infinitas soluciones en L).

Nota 1.41. Como es fácil de verificar, los corolarios 1.8 y 1.9, así como el teorema 1.27, son aún válidos si K es simplemente un dominio. Obsérvese también que si $z \in \mathbb{C}$ y $n \geq 1$, el teorema 1.27 aplicado al polinomio $x^n - z \in \mathbb{C}[x]$ asegura que z tiene a lo sumo n raíces n -ésimas distintas en $\mathbb{C}$, y como las z_k , $k = 0, 1, \dots, n - 1$ son n raíces n -ésimas de z , distintas entre sí, se

concluye, de manera distinta de la usada en la demostración del teorema 1.23, que z tiene exactamente n raíces n -ésimas (distintas) en $\mathbb{C}$.

Definición 1.23. Se dice que un campo numérico K es *algebraicamente cerrado*, o, simplemente, que es *cerrado*, si todo polinomio $f(x) \in K[x]$ con $\text{grad}(f(x)) \geq 1$, tiene al menos una raíz $a \in K$.

Ni $\mathbb{Q}$ ni $\mathbb{R}$ son cerrados, pues $x^2 + 1 \in \mathbb{Q}[x] \subseteq \mathbb{R}[x]$, pero ninguna de sus raíces, $i, -i$, está en $\mathbb{Q}$ ó $\mathbb{R}$.

Teorema 1.28. Un campo numérico K es algebraicamente cerrado si y sólo si todo polinomio $f(x) \in K[x]$, con $\text{grad}(f(x)) = n \geq 1$, se escribe en la forma

$$f(x) = a(x - a_1) \cdots (x - a_n), \quad (1.133)$$

donde $a \neq 0$ y los a_k , $k = 1, \dots, n$, están en K .

Demostración. Supongamos primero que K es cerrado y que $f(x) \in K[x]$ tiene grado $n \geq 1$. Si $n = 1$, así que $f(x) = ax + b$, $a, b \in K$, $a \neq 0$, entonces $f(x) = a(x - a_1)$, con $a_1 = -b/a \in K$. Supongamos entonces que $n > 1$, y sea $a_n \in K$ tal que $f(a_n) = 0$. En virtud de (1.132), corolario 1.8, existe $g(x) \in K[x]$ tal que $f(x) = g(x)(x - a_n)$, y como $\text{grad}(g(x)) = n - 1 \geq 1$, podemos suponer inductivamente que existen $a \in K$, $a \neq 0$, y $a_1, \dots, a_{n-1} \in K$, tales que $g(x) = a(x - a_1) \cdots (x - a_{n-1})$. Entonces, $f(x)$ satisface (1.133). Recíprocamente, si todo polinomio $f(x) \in K[x]$ con $\text{grad}(f(x)) = n \geq 1$ satisface una relación (1.133), entonces $f(a_k) = 0$, $k = 1, 2, \dots, n$, $a_k \in K$, y K será, así, algebraicamente cerrado. $\square$

Corolario 1.11. Si K es algebraicamente cerrado y $f(x) \in K[x]$ tiene grado $n \geq 1$, existen $a'_1, \dots, a'_m \in K$, $1 \leq m \leq n$, $a'_k \neq a'_j$ si $k \neq j$, y $\alpha_k \in \mathbb{Z}$, $1 \leq \alpha_k \leq n$, $k = 1, \dots, m$, tales que

$$f(x) = a(x - a'_1)^{\alpha_1} \cdots (x - a'_m)^{\alpha_m}, \quad (1.134)$$

donde $a \in K$ y $a \neq 0$. Además,

$$\alpha_1 + \cdots + \alpha_m = n. \quad (1.135)$$

Demostración. La relación (1.134) se obtiene de la (1.133) agrupando factores iguales. La relación (1.135) es consecuencia de la (1.121). $\square$

Nota 1.42. La relación (1.133) se expresa diciendo que $f(x)$ tiene en K n raíces (no necesariamente distintas). La (1.134), diciendo que $f(x)$ tiene en K m raíces distintas $a'_1, \dots, a'_m$, con a'_k de multiplicidad α_k , $k = 1, \dots, m$. De hecho, si $(x - a)^\alpha \mid f(x)$, donde $a \in K$ y $\alpha \in \mathbb{Z}$, $\alpha \geq 0$, son tales que $(x - a)^{\alpha+1} \nmid f(x)$, se dice que a es una raíz de $f(x)$ en K de multiplicidad α . Nótese que según nuestra demostración de (1.134), α_k es simplemente el número de veces que a'_k aparece como raíz de $f(x)$ en (1.133). Cuando $\alpha_k = 1$, se dice que a'_k es una raíz simple de $f(x)$. Si $\alpha_k = 2$, se dice que a'_k es una raíz doble, etc. Nótese que si $\alpha_k = 0$, a_k no es, realmente, una raíz de $f(x)$ (una raíz de multiplicidad 0).

Establecer la existencia de campos numéricos algebraicamente cerrados es en general un problema difícil cuya solución requiere usualmente instrumentos matemáticos avanzados y, no puramente algebraicos. Tal vez el resultado más notable en esta dirección es el siguiente, debido a C. F. Gauss, el cual es conocido, por su importancia, como el *teorema fundamental del álgebra*, y el cual enunciamos sin demostración.

Teorema 1.29 (Gauss). El campo $(\mathbb{C}, +, \cdot)$ de los números complejos es algebraicamente cerrado.

A partir del teorema 1.29 es posible establecer, en forma puramente algebraica, la existencia de otros campos numéricos algebraicamente cerrados, aunque esto último requiere, en general, conocimientos elementales de Álgebra Lineal. Nosotros usaremos libremente el teorema 1.29 para propósitos más modestos. Demostraciones del teorema 1.29 pueden encontrarse en [7], [17], [23] y [1].

Nota 1.43. Es posible que aún si K no es algebraicamente cerrado, un polinomio dado $f(x) \in K[x]$ se escriba en la forma (1.133) con a y los a_k , $k = 1, 2, \dots, n$, en K . Si éste es el caso, en ninguna extensión L de K puede existir $b \in L$, distinto de los a_k , tal que $f(b) = 0$; es decir, $A = \{a_1, \dots, a_n\}$ es un conjunto completo de raíces de $f(x)$ en cualquier extensión L de K , ya que las hipótesis sobre b garantizan que $f(b) = a(b - a_1) \cdots (b - a_n) \neq 0$. Esto implica obviamente que la descomposición (1.133) es la única posible de $f(x)$ como producto de polinomios de grado 1, y no sólo en K , sino en cualquier extensión L de K , y lo mismo será cierto de la descomposición (1.134).

Las descomposiciones de un polinomio como producto de polinomios de grado menor pueden suministrar información valiosa sobre éste. Desafortunadamente, una descomposición como la (1.133), la mejor posible, puede

no existir si K no es algebraicamente cerrado. En lo que sigue daremos, sin embargo, respuestas parciales, válidas aún si K no es algebraicamente cerrado. Necesitaremos algunas nociones adicionales.

Definición 1.24. Sean K un campo numérico, $f(x) \in K[x]$. Si $f(x) = a_m x^m + \cdots + a_0$, donde $m \geq 0$ y $a_m = 1$, es decir, si $f(x) = 1$ o $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$, $m \geq 1$, diremos que $f(x)$ es un polinomio mónico.

Nótese que si $f(x)$ es mónico entonces $\text{grad}(f(x)) \geq 0$. Claramente $f(x) = 1$ es el único polinomio mónico de grado 0. Por otra parte, si K es un campo, todo polinomio no nulo en $K[x]$ está asociado con un único polinomio mónico.

Nota 1.44. La Definición 1.24 tiene aún sentido cuando K es simplemente un dominio, y para todo $m \geq 0$ hay polinomios mónicos en $K[x]$ de grado m . Sin embargo, no todo polinomio no nulo en $K[x]$ está asociado con un polinomio mónico. Por ejemplo en $\mathbb{Z}[x]$, $2x + 1$ no está asociado con ningún polinomio mónico.

En lo que sigue nos limitaremos, salvo advertencia expresa de lo contrario, a polinomios sobre campos.

Definición 1.25. Sean K un campo numérico, $f(x), g(x) \in K[x]$, uno al menos de los cuales es no nulo. Se dice que $d(x) \in K[x]$ es un máximo común divisor de $f(x)$ y $g(x)$, si:

1. $d(x)$ es mónico,
2. $d(x) \mid f(x)$ y $d(x) \mid g(x)$,
3. Si $h(x) \mid f(x)$ y $h(x) \mid g(x)$, donde $h(x) \in K[x]$, entonces $h(x) \mid d(x)$.

La propiedad (2) expresa que $d(x)$ es un divisor común de $f(x)$ y $g(x)$. La (3) asegura que todo divisor común $h(x)$ de $f(x)$ y $g(x)$ en $K[x]$ debe ser un divisor de $d(x)$, y deberá tenerse entonces que $\text{grad}(h(x)) \leq \text{grad}(d(x))$. En este sentido, $d(x)$ es un máximo común divisor de $f(x)$ y $g(x)$.

De la Definición 1.25 no se deduce la existencia de máximos comunes divisores, aunque si su unicidad, en caso de que existan (pues si también $d'(x)$ es un máximo común divisor de $f(x)$ y $g(x)$ entonces $d(x) \mid d'(x)$

y $d'(x) \mid d(x)$, así que $d(x) = ad'(x)$, $a \in K$, $a \neq 0$, y, necesariamente, $a = 1$). El siguiente teorema garantiza la existencia de máximos comunes divisores.

Teorema 1.30 (Bezout). Sean K un campo numérico, $f(x)$ y $g(x)$ polinomios en $K[x]$, uno al menos de los cuales es no nulo. Entonces, existe $d(x) \in K[x]$, el cual es máximo común divisor de $f(x)$ y $g(x)$. Más aún, $d(x)$ se escribe en la forma

$$d(x) = m(x)f(x) + n(x)g(x), \quad (1.136)$$

donde $m(x), n(x) \in K[x]$.

Demostración. Sea $A = \{p(x)f(x) + q(x)g(x) \neq 0 : p(x), q(x) \in K[x]\}$. Claramente $A \neq \emptyset$, pues si $f(x) \neq 0$ entonces $f(x) \in A$ (ya que $f(x) = 1 \cdot f(x) + 0 \cdot g(x)$), y un resultado análogo vale si $f(x) = 0$ pero $g(x) \neq 0$. Sean $m = \min\{\text{grad}(h(x)) : h(x) \in A\}$, $D(x) \in A$ con $\text{grad}(D(x)) = m$, y $a \in K$ tal que $d(x) = aD(x)$ sea mónico. Nótese que $m \geq 0$. Evidentemente $d(x)$ se escribe en la forma (1.136), lo cual implica que si $h(x) \in K[x]$, $h(x) \mid f(x)$ y $h(x) \mid g(x)$, entonces $h(x) \mid d(x)$. Veamos entonces que $d(x) \mid f(x)$ y $d(x) \mid g(x)$, lo cual demostrará la afirmación. Supongamos que $d(x) \nmid f(x)$, así que $f(x) = q(x)d(x) + r(x)$ con $0 \leq \text{grad}(r(x)) < \text{grad}(d(x))$. Pero entonces

$$r(x) = (1 - q(x)m(x))f(x) + (-q(x)n(x))g(x),$$

lo cual asegura que $r(x) \in A$. Esto es absurdo, pues $r(x) \neq 0$ y $\text{grad}(r(x)) < \text{grad}(d(x))$. Entonces, $d(x) \mid f(x)$. El argumento para demostrar que $d(x) \mid g(x)$ es análogo. $\square$

Si $f(x), g(x) \in K[x]$ y no son ambos nulos, escribiremos

$$d(x) = \text{mcd}(f(x), g(x))$$

para denotar el máximo común divisor de $f(x)$ y $g(x)$. La relación

$$\text{mcd}(f(x), g(x)) = m(x)f(x) + n(x)g(x) \quad (1.137)$$

dada por el teorema 1.30 se denomina una *Relación de Bezout para* $\text{mcd}(f(x), g(x))$. En general $m(x)$ y $n(x)$ no están unívocamente determinados (ejercicios 1.66 y 1.67). Como es claro, si $d(x) = \text{mcd}(f(x), g(x))$, existen $m(x), n(x) \in K[x]$ tales que $d(x) = m(x)f(x) + n(x)g(x)$,

pero el sólo hecho de que esta última relación sea válida no garantiza que $d(x) = \text{mcd}(f(x), g(x))$. Por ejemplo, en $\mathbb{Q}[x]$, $x^2 = x^2(x+1) + (-x^2)x$, pero $x^2 \neq \text{mcd}(x+1, x)$. De hecho, $\text{mcd}(x+1, x) = 1$. Obsérvese, sin embargo, que si $1 = m(x)f(x) + n(x)g(x)$ donde $m(x), n(x) \in K[x]$, necesariamente $1 = \text{mcd}(f(x), g(x))$ pues $1 \mid f(x)$ y $1 \mid g(x)$. Obsérvese también que si $f(x), g(x) \in K[x]$, $d(x) = \text{mcd}(f(x), g(x))$ en $K[x]$ si y sólo si esto es también válido en $L[x]$, cualquiera que sea la extensión L de K . En efecto, si (1.136) es válida en $K[x]$, también lo es en $L[x]$, y si $d(x) \mid f(x)$ y $d(x) \mid g(x)$ en $K[x]$, esto también será cierto en $L[x]$. Por otra parte, si $f(x), g(x) \in K[x]$ y $d(x) = \text{mcd}(f(x), g(x))$ en $K[x]$, $d'(x) = \text{mcd}(f(x), g(x))$ en $L[x]$, entonces $d(x) \mid d'(x)$ pues $d(x)$ es un divisor de $f(x)$ y $g(x)$ en $L[x]$, y $d'(x) \mid d(x)$ en $L[x]$, ya que $d(x)$ satisface una relación de Bezout en $L[x]$, así que $d(x) = d'(x)$. Sin embargo, una relación de Bezout para $d(x)$ en $L[x]$ puede no ser válida en $K[x]$.

Nota 1.45. Aunque la labor de determinar el máximo común divisor es más ardua en el caso de los polinomios (véase el ejercicio 1.70), el lector debe haber observado la analogía existente entre las nociones y resultados anteriores y los de la sección 1.4. Esta analogía persistirá a lo largo de la sección y nos permitirá, de hecho, ser breves y concisos en nuestras consideraciones y en las demostraciones de muchos de los resultados. Por ejemplo, las demostraciones de los siguientes resultados son completamente análogas a las de algunos de los establecidos en la sección 1.4, y las omitiremos, dejándolas como ejercicio al lector.

Teorema 1.31. Si $d(x) = \text{mcd}(f(x), g(x))$ y $h(x)$ es mónico, entonces $\text{mcd}(h(x)f(x), h(x)g(x)) = h(x)d(x)$. Si además $h(x) \mid f(x)$ y $h(x) \mid g(x)$ entonces $d(x)/h(x) = \text{mcd}(f(x)/h(x), g(x)/h(x))$.

Corolario 1.12. Si $d(x) = \text{mcd}(f(x), g(x))$ entonces $\text{mcd}(f(x)/d(x), g(x)/d(x)) = 1$.

Definición 1.26. Si $f(x), g(x) \in K[x]$, y $\text{mcd}(f(x), g(x)) = 1$, se dice que $f(x)$ y $g(x)$ son *primos relativos* en $K[x]$.

Teorema 1.32. Para que $f(x)$ y $g(x)$ en $K[x]$ sean primos relativos es necesario y suficiente que existan $m(x), n(x) \in K[x]$ tales que

$$1 = m(x)f(x) + n(x)g(x) \quad (1.138)$$

Corolario 1.13. Si $f(x)$ y $g(x)$ son primos relativos en $K[x]$ y $h(x) \mid f(x)$, entonces $h(x)$ y $g(x)$ son aún primos relativos en $K[x]$.

Teorema 1.33. Si $f(x)$ y $g(x)$ son primos relativos en $K[x]$ y $f(x) \mid g(x)h(x)$, entonces $f(x) \mid h(x)$ en $K[x]$.

Corolario 1.14. Si $g(x)$ y $h(x)$ son primos relativos con $f(x)$, también lo es $g(x)h(x)$. En tales circunstancias, si $\text{grad}(f(x)) > 0$, entonces $f(x) \nmid g(x)h(x)$.

Más generalmente:

Corolario 1.15. Si $\text{mcd}(f(x), g_i(x)) = 1$, $i = 1, 2, \dots, n$, entonces $\text{mcd}(f(x), g_1(x)g_2(x) \cdots g_n(x)) = 1$. Si $\text{grad}(f(x)) > 0$, entonces $f(x) \nmid g_1(x)g_2(x) \cdots g_n(x)$. Dicho de otra manera: si $\text{mcd}(f(x), g_i(x)) = 1$, $i = 1, 2, \dots, n$, y $f(x) \mid g_1(x)g_2(x) \cdots g_n(x)g_{n+1}(x)$, entonces $f(x) \mid g_{n+1}(x)$.

Teorema 1.34. Si $f(x) \mid h(x)$, $g(x) \mid h(x)$ y $f(x), g(x)$ son primos relativos, entonces $f(x)g(x) \mid h(x)$.

Nota 1.46. Obsérvese que si $f(x), g(x) \in K[x]$, $f(x)$ y $g(x)$ son primos relativos en $K[x]$ si y sólo si lo son en $L[x]$, cualquiera que sea la extensión L de K .

Definición 1.27. Se dice que $p(x) \in K[x]$ es un *polinomio irreducible* de $K[x]$ si $p(x) \notin K$ y los únicos divisores de $p(x)$ en $K[x]$ son los elementos no nulos de K y los polinomios $f(x) = ap(x)$ con $a \in K$, $a \neq 0$ (es decir las constantes no nulas de K y los polinomios asociados con $p(x)$). Si $p(x)$ es mónico e irreducible, se dice que $p(x)$ es un *polinomio primo* de $K[x]$.

Nota 1.47. Si $p(x), f(x) \in K[x]$ y $p(x)$ es irreducible en $K[x]$, decir que $p(x) \nmid f(x)$ es equivalente a decir que $p(x)$ y $f(x)$ son primos relativos.

Todo polinomio irreducible tiene grado al menos 1, y todo polinomio de grado 1 es irreducible y asociado de un polinomio primo. De hecho, todo polinomio irreducible es asociado de un polinomio primo. Si $f(x) \in K[x]$ no es irreducible y $f(x) \notin K$, se dice que $f(x)$ es *reducible* en $K[x]$. Como es claro, $f(x)$ es reducible en $K[x]$ si y sólo si $\text{grad}(f(x)) \geq 2$ y existe $g(x) \in K[x]$ con $0 < \text{grad}(g(x)) < \text{grad}(f(x))$ tal que $g(x) \mid f(x)$.

Nota 1.48. Es claro que si $p(x), q(x) \in K[x]$ son irreducibles, $p(x) \mid q(x)$ si y sólo si $p(x) \sim q(x) \pmod{K}$, y que si $p(x), q(x)$ son primos, $p(x) \mid q(x)$ si y sólo si $p(x) = q(x)$. Dos polinomios primos distintos son primos relativos.

Nota 1.49. El hecho de que $p(x) \in K[x]$ sea irreducible en $K[x]$ depende de K , es decir, si $p(x)$ es irreducible en $K[x]$ y L es una extensión de K , puede ser que $p(x)$ no sea irreducible en $L[x]$. Así $x^2 + 1$ es irreducible en $\mathbb{R}[x]$, como se verifica fácilmente, pero no en $\mathbb{C}[x]$, pues $x + i$ y $x - i$ son divisores de $x^2 + 1$ en $\mathbb{C}[x]$.

Nota 1.50. Como se deduce del teorema 1.28, un campo K es algebraicamente cerrado si y sólo si los únicos polinomios irreducibles de $K[x]$ son los de grado 1. Así, los únicos polinomios primos en $\mathbb{C}[x]$ son los de la forma $x - a$ con $a \in \mathbb{C}$.

Nota 1.51. En cualquier campo K , un polinomio de grado 2 es irreducible si y sólo si no tiene raíces en K (ejercicio 1.68). De esto se deduce que un polinomio $f(x)$ de grado 2 en $\mathbb{R}[x]$ es irreducible si y sólo si $f(x) = ax^2 + bx + c$, $a, b, c \in \mathbb{R}$, con $b^2 - 4ac < 0$. De hecho éstos son los únicos polinomios irreducibles de $\mathbb{R}[x]$ con grado mayor que 1. Para demostrar esto obsérvese que si $f(x) \in \mathbb{R}[x]$ y $\alpha \in \mathbb{C}$, entonces $\overline{f(\alpha)} = f(\bar{\alpha})$, así que si $\alpha \in \mathbb{C}$ es raíz de $f(x)$, también $\bar{\alpha}$ lo es. Ahora, si $f(x)$ tiene grado mayor que 1 y una raíz real, $f(x)$ es reducible (corolario 1.9). Entonces, si $f(x) \in \mathbb{R}[x]$, $\text{grad}(f(x)) > 1$ y $f(x)$ es irreducible en $\mathbb{R}[x]$, sus raíces son todas complejas no reales, y si α es una de ellas, también lo será $\bar{\alpha}$. Como $g_\alpha(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 + bx + c$ con $b = -2\Re(\alpha)$ y $c = |\alpha|^2$, se tiene que $g_\alpha(x) \in \mathbb{R}[x]$ y, de esto, que $f(x) = h(x)g_\alpha(x)$, donde $h(x) \in \mathbb{R}[x]$. Pero como $f(x)$ es irreducible y $h(x) \in \mathbb{R}[x]$, necesariamente $h(x) = a \in \mathbb{R}$, $a \neq 0$, así que $f(x) = ag_\alpha(x)$. Como evidentemente $(a\Re(\alpha))^2 - (a|\alpha|)^2 = a^2((\Re(\alpha))^2 - |\alpha|^2) < 0$, pues $|\Re(\alpha)| < |\alpha|$, ya que $\Im(\alpha) \neq 0$, esto demuestra la afirmación.

Nota 1.52. Por el contrario, en $\mathbb{Q}[x]$ pueden existir polinomios irreducibles de cualquier grado, como demostraremos al final de esta sección (teorema 1.36).

Nuestro siguiente teorema es completamente análogo al lema 1.1 de la sección 1.4 y da una descripción de cualquier polinomio sobre un campo K en términos de polinomios irreducibles (en general, de grado menor), lo cual puede dar valiosa información sobre la estructura del polinomio. Nótese que si $p(x)$ es primo en $K[x]$ y $p(x) \nmid f_i(x)$, $i = 1, 2, \dots, n$, el hecho de que $p(x) \mid f_1(x) \cdots f_n(x)f_{n+1}(x)$ asegura que $p(x) \mid f_{n+1}(x)$ (pues, corolario 1.14, $\text{mcd}(p(x), f_i(x)) = 1$, $i = 1, 2, \dots, n$).

Teorema 1.35. Si K es un campo, $f(x) \in K[x]$ y $\text{grad}(f(x)) \geq 1$, existen polinomios primos $p_1(x), \dots, p_n(x)$ en $K[x]$, $n \geq 1$, y $a \in K$, tales que

$$f(x) = ap_1(x) \cdots p_n(x). \quad (1.139)$$

Tal descomposición es además única, en el sentido de que si también

$$f(x) = bq_1(x) \cdots q_n(x) \quad (1.140)$$

donde $b \in K$ y los $q_i(x)$, $i = 1, 2, \dots, n$, son polinomios primos en $K[x]$, entonces $a = b$, $m = n$, y existe una aplicación biyectiva σ de $\{1, 2, \dots, n\}$ en sí mismo tal que

$$p_i(x) = q_{\sigma(i)}(x), \quad i = 1, 2, \dots, n. \quad (1.141)$$

Si $f(x)$ es mónico, se puede tomar $a = 1$ en (1.139).

Demostración. Sea A el conjunto de los polinomios en $K[x]$ con grado mayor o igual que 1 y para los cuales no es posible una descomposición (1.139). Supóngase que $A \neq \emptyset$ y sea $f(x) \in A$ de mínimo grado posible. Claramente $\text{grad}(f(x)) \geq 1$ y no es irreducible, pues, en tal caso, existirían $a \in K$ y $p_1(x) \in K[x]$, primo, tales que $f(x) = ap_1(x)$. Pero entonces, existen $g(x), h(x) \in K[x]$, con $1 \leq \text{grad}(g(x)), \text{grad}(h(x)) < \text{grad}(f(x))$, tales que $f(x) = g(x)h(x)$, y, por definición de A , $g(x) \notin A$ y $h(x) \notin A$. Esto da, para cada uno de $g(x), h(x)$, y por tanto para $f(x)$, una descomposición de la forma (1.139). Esto es absurdo, así que $A = \emptyset$, y la afirmación sobre la existencia de una representación (1.139) para todo polinomio $f(x) \in K[x]$ con $\text{grad}(f(x)) \geq 1$ queda asegurada. En cuanto a la unicidad, supóngase que (1.139) y (1.140) valen para $f(x)$. Entonces $p_1(x) \mid q_1(x) \cdots q_m(x)$, así que existe $\sigma(1) = 1, 2, \dots, m$ tal que $p_1(x) \mid q_{\sigma(1)}(x)$. Esto es consecuencia del corolario 1.13. Entonces $p_1(x) = q_{\sigma(1)}(x)$, y se tendrá que

$$g(x) := ap_2(x) \cdots p_n(x) = bq_1(x) \cdots \widehat{q_{\sigma(1)}}(x) \cdots q_m(x), \quad (1.142)$$

donde el símbolo $\widehat{}$ significa que $q_{\sigma(1)}(x)$ debe omitirse. Podemos ahora razonar por inducción, suponiendo que la afirmación es válida para todo polinomio $g(x) \in K[x]$ con $1 \leq \text{grad}(g(x)) < \text{grad}(f(x))$. Nótese que es obviamente cierta si $\text{grad}(f(x)) = 1$, pues en tal caso $m = n = 1$ (si no, una al menos de las dos descomposiciones debería tener grado mayor que 1), y de $ap_1(x) = bq_1(x)$ se deduce que $a = b$ y $p_1(x) = q_1(x)$. Obsérvese que es también válida si $n = 1$ en (1.139), pues (1.142) implicaría que

$ab^{-1} = q_1(x) \cdots \widehat{q_{\sigma(1)}}(x) \cdots q_m(x)$, lo cual es absurdo si $m > 1$ (compárense los grados), e implica de nuevo que $a = b$ y que $p_1(x) = q_{\sigma(1)}(x) = q_1(x)$. Pero entonces, si $\text{grad}(g(x)) \geq 1$ en (1.142), la hipótesis de inducción garantiza que $m = n$, que $a = b$ es el coeficiente de grado máximo de $f(x)$, y que existe $\sigma : \{2, \dots, n\} \rightarrow \{1, \dots, n\} \setminus \{\sigma(1)\}$, biyectiva, tal que $q_{\sigma(i)}(x) = p_i(x)$, $i = 2, \dots, n$. Esto demuestra el teorema. $\square$

Nota 1.53. El teorema anterior se expresa frecuentemente en términos de polinomios irreducibles (en lugar de primos), diciendo que si $f(x) \in K[x]$ y $\text{grad}(f(x)) \geq 1$, existen $p_1(x), \dots, p_n(x)$, irreducibles en $K[x]$, tales que $f(x) = p_1(x) \cdots p_n(x)$, $n \geq 1$, y que si también $f(x) = q_1(x) \cdots q_m(x)$ con los $q_i(x)$ irreducibles en $K[x]$, entonces $m = n$ y existe σ como antes tal que $p_i(x) \sim q_{\sigma(i)}(x) \pmod{K}$ para todo $i = 1, 2, \dots, n$. Claramente esto es equivalente al enunciado del teorema 1.35, y en este momento parece superfluo. Sin embargo, existen algunas razones para esto (véase, la nota 1.56, más adelante).

Del teorema 1.35 se deduce sin más el siguiente corolario.

Corolario 1.16. Si K es un campo y $f(x) \in K[x]$ es tal que $\text{grad}(f(x)) \geq 1$, existen $a \in K$, polinomios primos distintos $p_1(x), \dots, p_n(x)$ en $K[x]$, y enteros $\alpha_i > 0$, $i = 1, \dots, n$, tales que

$$f(x) = ap_1^{\alpha_1}(x) \cdots p_n^{\alpha_n}(x). \quad (1.143)$$

Además, tal descomposición es única, salvo por el orden de los factores.

Demostración. Obviamente (1.139) y (1.143) son, después de agrupar factores iguales, equivalentes. $\square$

Definición 1.28. Las factorizaciones de $f(x)$ dadas en (1.139) y (1.143) se denominan, respectivamente, las *descomposiciones prima y primaria* de $f(x)$.

Como en el caso de los enteros, si $f(x), g(x) \in K[x]$, $f(x)g(x) \neq 0$, y

$$f(x) = ap_1^{\alpha_1}(x) \cdots p_n^{\alpha_n}(x) = bp_1^{\beta_1}(x) \cdots p_n^{\beta_n}(x),$$

donde $a, b \in K$, los $p_i(x)$ son primos, y $\alpha_i, \beta_i \geq 0$ para $i = 1, \dots, n$ entonces

$$\text{mcd}(f(x), g(x)) = p_1^{\gamma_1}(x) \cdots p_n^{\gamma_n}(x), \quad \gamma_i = \min(\alpha_i, \beta_i), \quad i = 1, \dots, n. \quad (1.144)$$

Y si

$$\text{mcm}(f(x), g(x)) := \frac{(ab)^{-1} f(x) g(x)}{\text{mcd}(f(x), g(x))} \quad (1.145)$$

(el mínimo común múltiplo de $f(x)$ y $g(x)$), entonces

$$\text{mcm}(f(x), g(x)) = p_1^{\mu_1}(x) \cdots p_n^{\mu_n}(x), \quad \mu_i = \max(\alpha_i, \beta_i), \quad i = 1, \dots, n. \quad (1.146)$$

Nota 1.54. Si K es un dominio, las propiedades (1.103), (1.105), (1.106), (1.107), (1.108), (1.112), (1.113), (1.114), (1.115), (1.116), (1.117), y el hecho de que

$f(x)g(x) = 0$ si y sólo si $f(x) = 0$ o $g(x) = 0$, sugiere que, salvo porque $K[x] \not\subseteq \mathbb{C}$, $K[x]$ podría considerarse como un dominio (lo es, en el sentido abstracto), aunque no como un campo (aún si K lo es), pues, por ejemplo, x^{-1} carece de sentido.

Nota 1.55. La noción de máximo común divisor de dos enteros se generaliza a un número finito de ellos (no todos nulos): $d = \text{mcd}(a_1, \dots, a_n)$ (véase la sección 1.4). La noción de máximo común divisor de dos polinomios sobre un campo K también se generaliza a un número finito de ellos (no todos nulos), y es claro aún que $d(x) = \text{mcd}(f_1(x), \dots, f_n(x))$ si y sólo si $d(x) \mid f_i(x)$ y existen $m_i(x) \in K[x]$, $i = 1, 2, \dots, n$, tales que

$$d(x) = m_1(x)f_1(x) + \cdots + m_n(x)f_n(x). \quad (1.147)$$

A su vez, si ninguno de los $f_i(x)$ es nulo y $a \in K$ es tal que $af_1(x) \cdots f_n(x)$ es mónico, se define aún

$$\text{mcm}(f_1(x), \dots, f_n(x)) := \frac{af_1(x) \cdots f_n(x)}{\text{mcd}(f_1(x), \dots, f_n(x))}. \quad (1.148)$$

Incursionaremos ahora, brevemente, en la teoría de los polinomios sobre $\mathbb{Z}$ y sobre dominios más generales.

Definición 1.29. Si $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, $f(x) \neq 0$, se define

$$c(f(x)) = \text{mcd}(a_0, \dots, a_n). \quad (1.149)$$

Se dice que $c(f(x))$ es el *contenido* de $f(x)$. Si $c(f(x)) = 1$, se dice que $f(x)$ es un *polinomio primitivo* de $\mathbb{Z}[x]$, o un *polinomio primitivo sobre $\mathbb{Z}$* .

Evidentemente $c(f(x)) \in \mathbb{Z}$ y $c(f(x)) \geq 1$. Todo polinomio mónico es obviamente primitivo. Si $a \in \mathbb{Z}$, $a \neq 0$ y $f(x) \in \mathbb{Z}[x]$, $f(x) \neq 0$, entonces

$$c(af(x)) = |a|c(f(x)), \quad (1.150)$$

pues $\text{mcd}(aa_0, \dots, aa_n) = |a|\text{mcd}(a_0, \dots, a_n)$. Además, claramente $f(x) = c(f(x))\hat{f}(x)$, donde $\hat{f}(x)$ es primitivo, y no es difícil demostrar que si $f(x), g(x) \in \mathbb{Z}[x]$ son primitivos, también $f(x)g(x)$ lo es (ejercicio 1.80). Esto implica que si $f(x), g(x) \in \mathbb{Z}[x]$ son no nulos entonces

$$c(f(x)g(x)) = c(f(x))c(g(x)). \quad (1.151)$$

En efecto, $f(x) = c(f(x))\hat{f}(x)$, $g(x) = c(g(x))\hat{g}(x)$, donde $\hat{f}(x)$ y $\hat{g}(x)$ son primitivos, de lo cual $c(f(x)g(x)) = c(f(x))c(g(x))c(\hat{f}(x)\hat{g}(x)) = c(f(x))c(g(x))$, pues $c(\hat{f}(x)\hat{g}(x)) = 1$. La relación (1.151), que juega un papel importante en la teoría de los polinomios sobre dominios, se debe a Gauss. Nótese que (1.150) es un caso especial de (1.151).

Supóngase ahora que $f(x) \in \mathbb{Z}[x]$, con $\text{grad}(f(x)) \geq 1$. Como $f(x) \in \mathbb{Q}[x]$, $f(x)$ se escribe en la forma

$$f(x) = aq_1(x) \cdots q_n(x) \quad (1.152)$$

donde $a \in \mathbb{Z}$ y $q_k(x) \in \mathbb{Q}[x]$ es, para todo $k = 1, 2, \dots, n$, un polinomio primo en $\mathbb{Q}[x]$. Sea ahora $b_k \in \mathbb{Z}$ tal que $p_k(x) = b_k q_k(x) \in \mathbb{Z}[x]$, $k = 1, 2, \dots, n$ (tómese, por ejemplo, b_k igual al mínimo común múltiplo de los denominadores de los coeficientes no nulos de $q_k(x)$). Claramente $p_k(x)$ es aún un polinomio irreducible de $\mathbb{Q}[x]$, y si $\hat{p}_k(x) = c(p_k(x))^{-1}p_k(x)$, también $\hat{p}_k(x)$ es irreducible en $\mathbb{Q}[x]$. Pero entonces, como es obvio, $\hat{p}_k(x)$ es irreducible en $\mathbb{Z}[x]$. Ahora,

$$b_1 \cdots b_n f(x) = ap_1(x) \cdots p_n(x),$$

de lo cual $|b_1 \cdots b_n|c(f(x)) = |a|c(p_1(x)) \cdots c(p_n(x))$, así que, si $\hat{f}(x) = c(f(x))^{-1}f(x)$, entonces $\hat{f}(x) = a\hat{p}_1(x) \cdots \hat{p}_n(x)$. Se deduce que

$$f(x) = c(f(x)) \cdot \hat{p}_1(x) \cdots \hat{p}_n(x).$$

Por otra parte, si $p \in \mathbb{Z}$, es claro que p es irreducible en $\mathbb{Z}[x]$ si y sólo si también lo es en $\mathbb{Z}$. Se deduce que si $c(f(x)) = up_1 \cdots p_m$, $u = \pm 1$, es la descomposición prima de $c(f(x))$, entonces

$$f(x) = up_1 \cdots p_m \cdot \hat{p}_1(x) \cdots \hat{p}_n(x), \quad (1.153)$$

así que $f(x)$ es producto de irreducibles en $\mathbb{Z}[x]$. Obsérvese que si un polinomio $p(x)$ es irreducible en $\mathbb{Z}[x]$, necesariamente $p(x)$ es primitivo (si no, $c(p(x)) \neq 1$, será entonces producto de irreducibles de $\mathbb{Z}$, y como $p(x) = c(p(x))\hat{p}(x)$ con $\hat{p}(x)$ primitivo, $p(x)$ no será irreducible). Esta observación implica, como se verifica fácilmente, que la descomposición (1.153) de $f(x) \in \mathbb{Z}[x]$ es única, salvo por asociados y orden de los factores. Por esta razón se dice que $\mathbb{Z}[x]$ es un *dominio de descomposición factorial única*, o, simplemente, un *dominio factorial*. Si K es un dominio arbitrario, puede suceder que $K[x]$ no sea un dominio factorial, pues, de hecho, K mismo puede no serlo (véase el ejercicio 1.55). Si $K = \mathbb{Z}[i]$ es el anillo de los enteros de Gauss, es posible demostrar que tanto K como $K[x]$ son dominios factoriales. De hecho, bastaría demostrar esto para K , pues trabajando entonces en $\hat{K}[x]$ ($\hat{K}$ es el campo de cocientes de K), es posible usar argumentos completamente análogos a los usados más arriba para establecer que también $K[x]$ lo es. Sin embargo, no demostraremos por ahora que $\mathbb{Z}[i]$ es un dominio factorial, dejándolo para más adelante.

Demostraremos ahora el criterio de irreducibilidad de Eisenstein, previamente mencionado.

Teorema 1.36 (Criterio de Eisenstein). Sea $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ y supóngase que existe un primo p tal que

$$p \nmid a_n, \quad p \mid a_k, \quad k = 0, 1, \dots, n-1, \quad p^2 \nmid a_0. \quad (1.154)$$

Entonces, $f(x)$ es irreducible en $\mathbb{Q}[x]$.

Demostración. No hay pérdida de generalidad al suponer, para los propósitos a la vista, que $f(x)$ es primitivo, ya que si $f(x) = c(f(x))\hat{f}(x)$, los coeficientes de $\hat{f}(x)$ satisfacen las mismas condiciones (1.154) que los de $f(x)$, pues $p \nmid c(f(x))$. Supongamos entonces que $f(x)$ es reducible en $\mathbb{Q}[x]$ y que $f(x) = g_0(x)h_0(x)$, donde $g_0(x), h_0(x) \in \mathbb{Q}[x]$ con $1 \leq \text{grad}(g_0(x))$, $\text{grad}(h_0(x)) < \text{grad}(f(x))$, y sean $b, c \in \mathbb{Z}$ tales que $g(x) = bg_0(x)$, $h(x) = ch_0(x)$, estén en $\mathbb{Z}[x]$. Como $bcf(x) = g(x)h(x)$, se deduce que $|bc| = c(g(x)h(x))$, de lo cual $f(x) = \hat{g}(x)\hat{h}(x)$, donde $\hat{g}(x), \hat{h}(x) \in \mathbb{Z}[x]$ son primitivos. Supongamos que $\hat{g}(x) = b_0 + b_1x + \cdots + b_r x^r$, $\hat{h}(x) = c_0 + c_1x + \cdots + c_s x^s$, siendo $r > 0$ y $s > 0$ los grados respectivos de $\hat{g}(x)$ y $\hat{h}(x)$. Suponemos $b_i = 0, i > r; c_i = 0, i > s$. Nótese que $a_0 = b_0c_0$, y como $p \mid a_0$ entonces $p \mid b_0$ o $p \mid c_0$. Como $p^2 \nmid a_0$, podemos suponer que $p \nmid c_0$. Ahora, $p \nmid b_r$ y $p \nmid c_s$, pues $p \nmid a_n$ (y $a_n = b_r c_s$). Sea $k = \min\{i : p \nmid b_i, i = 0, 1, \dots, r\}$. Como $p \mid b_0$ entonces $k \geq 1$ y $p \mid b_i$ para

todo $i = 0, 1, \dots, k-1$. Pero $a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k$ y $p \mid a_k$, lo cual contradice el hecho de que $p \nmid b_k c_0$. Esta contradicción asegura que la factorización $f(x) = \hat{g}(x)\hat{h}(x)$ no es posible, así que $f(x)$ es irreducible en $\mathbb{Q}[x]$. $\square$

Nota 1.57. Nótese que si en el teorema 1.36, $f(x)$ es primitivo, entonces $f(x)$ también es irreducible en $\mathbb{Z}[x]$.

El siguiente corolario del teorema 1.36 asegura la existencia de polinomios primos sobre $\mathbb{Q}$ de cualquier grado.

Corolario 1.17. Si p es un primo, $x^n - p$ es irreducible sobre $\mathbb{Q}$ para todo $n \geq 1$.

Demostración. Teniendo en cuenta que $a_{n-1} = a_{n-2} = \cdots = a_1 = 0$, la afirmación es consecuencia obvia del teorema. $\square$

El siguiente resultado es útil en la teoría de las llamadas *extensiones ciclotómicas* que serán examinadas en el segundo curso de álgebra. Véase, al respecto, la sección 1.7, relación (1.45).

Corolario 1.18. Si p es un primo, el polinomio

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1 \quad (1.155)$$

es irreducible sobre $\mathbb{Q}$.

Demostración. Demostraremos que $f(x+1)$ es irreducible sobre $\mathbb{Q}$. Esto es suficiente, pues si $f(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{Q}[x]$, también $f(x+1) = g(x+1)h(x+1)$, y es claro que $g(x+1), h(x+1) \in \mathbb{Q}[x]$. Pero

$$f(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{k=1}^p \binom{p}{k} x^{k-1} \quad (1.156)$$

(véase el ejercicio 1.44), y evidentemente $\binom{p}{p} = 1$ y $p \mid \binom{p}{k}$, $1 \leq k < p$, pues $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, mientras que $p^2 \nmid \binom{p}{1}$, pues $\binom{p}{1} = p$. $\square$

1.11. Conjuntos finitos e infinitos

Para terminar este ya largo capítulo, revisaremos brevemente las nociones de *conjunto finito e infinito*, y estableceremos algunas de sus propiedades más elementales, las cuales serán, sin embargo, útiles en el futuro (y de hecho, suficientes para casi todas las necesidades básicas de la matemática). Algo diremos también sobre la noción de cardinal y sobre la interpretación cardinal del número natural. Los argumentos de esta sección son simples, pero a veces engorrosos. Aconsejamos al lector asimilar las definiciones y comprender los enunciados de los teoremas, y luego recurrir más a su intuición que a las demostraciones.

Definición 1.30. Se dice que un conjunto X es *infinito*, si existe una aplicación inyectiva y no sobreyectiva de X en sí mismo. En caso contrario se dice que X es *finito*.

La anterior característica de la infinitud parece ser la única importante en matemáticas (Cantor). Si existe otra, no entraremos a investigarla.

Ejemplo 1.4. El conjunto $\mathbb{N}$ de los números naturales es infinito. La aplicación $f(n) = n + 1$ de $\mathbb{N}$ en sí mismo es inyectiva pero no sobreyectiva (no existe $n \in \mathbb{N}$ tal que $f(n) = 0$). El conjunto vacío y el conjunto reducido a un único elemento son finitos.

Para poder establecer algunas propiedades básicas de los conjuntos infinitos necesitaremos el siguiente axioma de la teoría de conjuntos.

Axioma de elección (A.E.) Si $(A_i)_{i \in I}$ es una familia de conjuntos no vacíos tales que $A_i \cap A_j = \emptyset$ si $i \neq j$, y si $I \neq \emptyset$, existe una aplicación $f : I \rightarrow \bigcup_{i \in I} A_i$ tal que $f(i) \in A_i$ para todo $i \in I$.

Se dice que f es una *función de elección*. El enunciado anterior es equivalente al siguiente: *existe un conjunto A que tiene con cada A_i exactamente un elemento en común*. En efecto, si (A.E.) es válido y f es una función de elección, sea $A = f(I)$. Recíprocamente, si el enunciado anterior es válido, sea $f : I \rightarrow \bigcup_{i \in I} A_i$ dada por $f(i)$ igual al único elemento en $A_i \cap A$ (nota 1.1). Si $I \neq \emptyset$ y $A_i \neq \emptyset$ para todo $i \in I$, el axioma (A.E.) asegura, aún si los A_i no son dos a dos disyuntos (no necesariamente $A_i \cap A_j = \emptyset$ si $i \neq j$), la existencia de una función de elección ($f(i) \in A_i$ para todo $i \in I$). Basta,

en efecto, tomar $f = p \circ g$, donde $g : I \rightarrow \bigcup_{i \in I} A_i \times \{i\}$ tal que $g(i) \in A_i \times \{i\}$ para todo $i \in I$ está dada por (A.E.), y $p : X \times I \rightarrow X$, $X = \bigcup_{i \in I} A_i$, es $p((a, i)) = a$.

El axioma (A.E.) asegura la existencia de un mecanismo que permite elegir un punto de cada conjunto de una familia no vacía ($I \neq \emptyset$) de conjuntos no vacíos, *sea ésta finita o infinita*. Frecuentemente este mecanismo está involucrado en la descripción misma de la familia (por ejemplo, si $(A_i)_{i \in I}$ es una familia de subconjuntos no vacíos de $\mathbb{N}$, una función de elección está automáticamente dada por $f(i) = \min A_i$), pero el axioma (A.E.) asegura que aún si este no es el caso, la elección es posible. El axioma (A.E.) tiene implicaciones importantes en todas las áreas de la matemática. Las que estudiaremos en este capítulo tienen que ver con la distinción entre conjuntos finitos e infinitos.

Lema 1.3. Sean X, Y conjuntos. Entonces:

- (a) Si $X \neq \emptyset$ y $f : X \rightarrow Y$, para que exista $g : Y \rightarrow X$ tal que $g \circ f = i_X$ es necesario y suficiente que f sea inyectiva.
- (b) Si $f : X \rightarrow Y$, para que exista $g : Y \rightarrow X$ tal que $f \circ g = i_Y$ es necesario y suficiente que f sea sobreyectiva.

Demostración. (a) Si existe $g : Y \rightarrow X$ tal que $g \circ f = i_X$, necesariamente f es inyectiva, pues si $f(x) = f(x')$ entonces $x = g(f(x)) = g(f(x')) = x'$. Supongamos ahora que f sea inyectiva. Si $f(X) = Y$, sea $g : Y \rightarrow X$ dada por $g(y)$ igual al único elemento de $f^{-1}(\{y\})$ para todo $y \in Y$. Si $f(X) \neq Y$, sean $a \in X$ y $f : Y \rightarrow X$ dada por

$$g(y) = \begin{cases} a, & \text{si } y \in Y \setminus f(X), \\ \text{único elemento de } f^{-1}(\{y\}), & \text{si } y \in f(X). \end{cases}$$

Evidentemente $g(f(x)) = x$ para todo $x \in X$. (b) Si $f \circ g = i_Y$, necesariamente f es sobreyectiva, pues si $y \in Y$ entonces $f(g(y)) = y$. Supongamos, recíprocamente, que f es sobreyectiva. La afirmación es obvia si $Y = \emptyset$, pues también deberá ser $X = \emptyset$, y bastará tomar $f = g = (\emptyset, \emptyset, \emptyset)$. Supongamos entonces que $Y \neq \emptyset$, así que también $X \neq \emptyset$, y sea $g : Y \rightarrow X$ tal que $g(y) \in f^{-1}(\{y\})$ para todo $y \in Y$. La función g está dada por el axioma (A.E.), es decir, es una función de elección para la familia $(f^{-1}(\{y\}))_{y \in Y}$. Evidentemente $f(g(y)) = y$ para todo $y \in Y$. $\square$

Corolario 1.19. Las afirmaciones siguientes para un conjunto X son equivalentes:

- (a) Existe $f : X \rightarrow X$, inyectiva y no sobreyectiva.
- (b) Existe $g : X \rightarrow X$, sobreyectiva y no inyectiva.

Demostración. Nótese que ambas condiciones aseguran que $X \neq \emptyset$. La demostración resulta entonces del lema 1.3. En efecto, si f es inyectiva y no sobreyectiva, existe $g : X \rightarrow X$ tal que $g \circ f = i_X$, así que g es sobreyectiva; y no es inyectiva, pues si lo fuera, sería $f = g^{-1}$, y f sería sobreyectiva. Recíprocamente, si g es sobreyectiva y no inyectiva, y si $g \circ f = i_X$, f es inyectiva y no sobreyectiva. $\square$

Nota 1.58. Por lo tanto, si toda aplicación inyectiva de X en sí mismo es sobreyectiva, toda aplicación sobreyectiva $g : X \rightarrow X$ será automáticamente inyectiva.

Corolario 1.20. Un conjunto X es infinito si y sólo si existe $g : X \rightarrow X$, sobreyectiva y no inyectiva.

Corolario 1.21. Las afirmaciones siguientes son equivalentes:

- (1) X es finito.
- (2) Toda aplicación inyectiva $f : X \rightarrow X$ es sobreyectiva.
- (3) Toda aplicación sobreyectiva $f : X \rightarrow X$ es inyectiva.

Definición 1.31. Si $m, n \in \mathbb{N}$, $m \leq n$, se define

$$\langle m, n \rangle = \{q \in \mathbb{N} : m \leq q \leq n\}. \quad (1.155)$$

Así, $\langle m, m \rangle = \{m\}$, $\langle m, m+1 \rangle = \{m, m+1\}$, etc.

Lema 1.4. Si existe $f : \langle 0, n \rangle \rightarrow \langle 0, m \rangle$, inyectiva, entonces $n \leq m$. Si además f no es sobreyectiva, $n < m$.

Demostración. Todo es claro si $n = 0$. Haremos inducción sobre n . Supongamos que $f : \langle 0, n+1 \rangle \rightarrow \langle 0, m \rangle$ es inyectiva. Entonces $f(\langle 0, n+1 \rangle) \subseteq \langle 0, m \rangle$, así que $f(\langle 0, n+1 \rangle)$ es no vacío y superiormente acotado. Entonces

(nota 1.23), existe $0 \leq p \leq n+1$, único, tal que $f(p) = \max f(\langle 0, n+1 \rangle)$. Sea $i : \langle 0, n \rangle \rightarrow \langle 0, n+1 \rangle$ dada por $i(k) = k$, $k < p$, $i(k) = k+1$, $k \geq p$. Claramente $f \circ i$ es inyectiva, y aplica $\langle 0, n \rangle$ en $\langle 0, m-1 \rangle$, puesto que $f(k) < f(p) \leq m$ si $k \neq p$ y $f \circ i(\langle 0, n \rangle) = f(\langle 0, n+1 \rangle - \{p\}) \subseteq \langle 0, f(p)-1 \rangle$. Entonces $n \leq m-1$, y $n+1 \leq m$. Supongamos ahora que f no es sobreyectiva. Si $f \circ i$ lo fuera, se tendría que $f(p) = m$ y $f(\langle 0, n+1 \rangle) = \langle 0, m \rangle$, lo cual es absurdo. Entonces $n < m-1$, y $n+1 < m$. $\square$

Corolario 1.22. Si $f : \langle 0, n \rangle \rightarrow \langle 0, m \rangle$ es sobreyectiva entonces $m \leq n$. Si además f no es inyectiva, $m < n$.

Demostración. Consecuencia de los lemas 1.3 y 1.4. $\square$

Corolario 1.23. Los conjuntos $\langle 0, n \rangle$, $n \in \mathbb{N}$, son finitos. Para que exista una aplicación biyectiva $f : \langle 0, n \rangle \rightarrow \langle 0, m \rangle$ es necesario y suficiente que $m = n$.

Corolario 1.24. Si X es infinito y $n \in \mathbb{N}$, no existe ninguna aplicación sobreyectiva $f : \langle 0, n \rangle \rightarrow X$.

Demostración. Supóngase lo contrario y sea n mínimo para el cual existe tal f . Entonces $n \geq 1$ y f es inyectiva (pues si $f(i) = f(j)$, $0 \leq i < j \leq n$ y $\varphi : \langle 0, n-1 \rangle \rightarrow \langle 0, n \rangle$ se define por $\varphi(k) = k$, $k < i$, $\varphi(k) = k+1$, $k \geq i$, es claro que $f \circ \varphi$ es aún sobreyectiva). Sean entonces $g : X \rightarrow \langle 0, n \rangle$ inyectiva y $h : X \rightarrow X$ inyectiva y no sobreyectiva. Claramente $g \circ h \circ f : \langle 0, n \rangle \rightarrow \langle 0, n \rangle$ es inyectiva y no sobreyectiva. $\square$

Corolario 1.25. Si X es infinito, existe $f : \mathbb{N} \rightarrow X$, inyectiva.

Demostración. Como $X \neq \emptyset$, existe $f_0 : \langle 0, 0 \rangle \rightarrow X$, y como X es infinito, f_0 no es sobreyectiva. Sean $x_1 \in X \setminus f_0(\langle 0, 0 \rangle)$ y $f_1 : \langle 0, 1 \rangle \rightarrow X$ dada por $f_1(0) = f_0(0)$, $f_1(1) = x_1$. Haremos inducción sobre $n \geq 1$, suponiendo que existe $f_n : \langle 0, n \rangle \rightarrow X$, inyectiva, tal que $f_n(k) = f_{n-1}(k)$ si $k \in \langle 0, n-1 \rangle$. Como f_n no es sobreyectiva, podemos definir entonces $f_{n+1} : \langle 0, n+1 \rangle \rightarrow X$ tal que $f_{n+1}(k) = f_n(k)$, $k \in \langle 0, n \rangle$, $f_{n+1}(n+1) \in X \setminus f_n(\langle 0, n \rangle)$. Claramente f_{n+1} es inyectiva. Sea ahora $f : \mathbb{N} \rightarrow X$ definida por $f(n) = f_n(n)$, $n = 0, 1, 2, \dots$. Es fácil verificar que f es inyectiva. $\square$

Corolario 1.26. Si X es infinito, existe $g : X \rightarrow \mathbb{N}$, sobreyectiva.

Si un conjunto X tiene un subconjunto infinito Y , X mismo es infinito, pues si $g : Y \rightarrow Y$ es inyectiva y no sobreyectiva, $f : X \rightarrow X$, definida por $f(x) = x$, $x \in X \setminus Y$; $f(x) = g(x)$, $x \in Y$, es inyectiva y no sobreyectiva. Se concluye que si X es finito y $Y \subseteq X$, también Y es finito. Es también evidente que si X es infinito y $f : X \rightarrow Y$ es inyectiva, $f(X)$ es infinito. Por lo tanto, si existe f inyectiva de $\mathbb{N}$ en X , o g sobreyectiva de X en $\mathbb{N}$, X es necesariamente infinito. Esto implica el siguiente teorema.

Teorema 1.37. Si X es finito y $f : X \rightarrow \mathbb{N}$ entonces $f(X)$ es acotado.

Demostración. Si no, existirían $n_0 < n_1 < \dots < n_k \dots$ en $f(X)$ y $h : \mathbb{N} \rightarrow f(X)$, definida por $h(k) = n_k$, sería inyectiva. Esto suministraría una aplicación sobreyectiva g de $f(X)$ en $\mathbb{N}$ y $g \circ f : X \rightarrow \mathbb{N}$ sería también sobreyectiva. $\square$

Corolario 1.27. Si X es finito y no vacío, existen $n \in \mathbb{N}$ y $f : \langle 0, n \rangle \rightarrow X$, sobreyectiva.

Demostración. Si no, razonando como en el corolario 1.23, se podría construir $f : \mathbb{N} \rightarrow X$, inyectiva. $\square$

Corolario 1.28. Si X es finito y no vacío, existen un único n y una aplicación biyectiva $f : \langle 0, n \rangle \rightarrow X$.

Demostración. Sea n , mínimo, para el cual existe $f : \langle 0, n \rangle \rightarrow X$, sobreyectiva. Entonces f es inyectiva. $\square$

Definición 1.32. Si X es finito y no vacío y n es como en el corolario 1.26, se dice que X tiene $n + 1$ elementos, o que el cardinal de X es $n + 1$. Se escribe $\text{Card}(X) = n + 1$. Se dice también que $\emptyset$ tiene 0 elementos y que su cardinal es 0: $\text{Card}(\emptyset) = 0$.

Si X es finito, existe un único $n \in \mathbb{N}$ tal que $n = \text{Card}(X)$. Si existe f biyectiva de $\langle 0, n \rangle$ sobre X , X es finito con $n + 1$ elementos. En efecto, si existe $\varphi : X \rightarrow X$ inyectiva y no sobreyectiva, $f^{-1} \circ \varphi \circ f : \langle 0, n \rangle \rightarrow \langle 0, n \rangle$ sería inyectiva y no sobreyectiva.

El siguiente concepto precisa la noción de enumerar un conjunto: *asignar un número natural distinto a cada uno de sus elementos*.

Definición 1.33. Si existe $f : X \rightarrow \mathbb{N}$, inyectiva, se dice que X es enumerable.

Todo conjunto finito es enumerable, pues si $f : \langle 0, n \rangle \rightarrow X$, $n \in \mathbb{N}$, es biyectiva, f^{-1} puede verse como una aplicación inyectiva de X en $\mathbb{N}$. Decir que $X \neq \emptyset$ es enumerable equivale a decir que existe una aplicación sobreyectiva $g : \mathbb{N} \rightarrow X$.

Nota 1.59. Si X, Y son enumerables, también lo es $X \times Y$. En efecto, si $\phi : X \rightarrow \mathbb{N}$, $\varphi : Y \rightarrow \mathbb{N}$ son inyectivas, $f : X \times Y \rightarrow \mathbb{N}$, dada por $f(x, y) = 2^{\phi(x)} 3^{\varphi(y)}$ (véase el ejercicio 1.32), es inyectiva. En particular $\mathbb{N} \times \mathbb{N}$ es enumerable, y existirá $\phi : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$, sobreyectiva. El anterior resultado implica que si $(A_n)_{n \in \mathbb{N}}$ es una familia de conjuntos enumerables, $A = \bigcup_{n \in \mathbb{N}} A_n$ es enumerable. En efecto, si para todo $m \in \mathbb{N}$, $f_m : \mathbb{N} \rightarrow A_m$ es sobreyectiva, $f : \mathbb{N} \times \mathbb{N} \rightarrow A$ dada por $f(m, n) = f_m(n)$ es sobreyectiva, y también lo será $f \circ \phi : \mathbb{N} \rightarrow A$.

Ejemplo 1.5. El conjunto $\mathbb{Z}$ de los números enteros es enumerable, pues la aplicación $\phi : \mathbb{Z} \rightarrow \mathbb{N}$ dada por

$$\phi(k) = \begin{cases} 2k+1, & k \geq 0 \\ -2(k+1), & k < 0 \end{cases} \quad (1.156)$$

es inyectiva (y obviamente, también sobreyectiva). También es enumerable el conjunto $\mathbb{Q}$ de los números racionales, pues la aplicación $\varphi : \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Q}$, $\varphi(m, n) = m/n$, es sobreyectiva.

Nota 1.60. En realidad, X es enumerable infinito si y sólo si existe $f : \mathbb{N} \rightarrow X$, biyectiva. En efecto, si X es enumerable, existe una función sobreyectiva $g : \mathbb{N} \rightarrow X$. Para cada $x \in X$, sea $n(x) = \min g^{-1}(x)$. Si el conjunto $A = \{n(x) : x \in X\}$ fuera finito y m fuera su máximo, sería evidente como definir $X \rightarrow \langle 0, m \rangle$ inyectiva y $\langle 0, m \rangle \rightarrow X$ sobreyectiva. Por lo tanto, si X es infinito, también lo es A . Si ahora definimos $n_0 = \min A$, e inductivamente $n_{m+1} = \min (A \setminus \{n_0, \dots, n_m\})$, y si $\phi : A \rightarrow X$ está dada por $\phi(n(x)) = x$ y $\varphi : \mathbb{N} \rightarrow A$ lo está por $\varphi(m) = n_m$, es claro que ϕ y φ son ambas biyectivas, y basta tomar $f = \phi \circ \varphi$. Lo recíproco es trivial.

Un número real $a \in [0, 1) = \{t \in \mathbb{R} : 0 \leq t < 1\}$ tiene una expresión decimal de la forma

$$a = 0.a_1a_2a_3 \dots \quad (1.157)$$

donde $0 \leq a_k \leq 9$, $k = 1, 2, \dots$. Además, existe $k \geq 1$ tal que $a_k \neq 0$ y $a_i = 0$ para todo $i > k$ si y sólo si a tiene también la expresión decimal $0.b_1b_2b_3 \dots$, donde $b_i = a_i$, $i = 1, 2, \dots, k-1$, $b_k = a_k - 1 \geq 0$ y $b_i = 9$, $i > k$. En efecto, ambas expresiones decimales representan el mismo número racional

$a = (a_1 a_2 a_3 \dots a_k) / 10^k = (10^{k-1} a_1 + 10^{k-2} a_2 + \dots + a_k) / 10^k$. Esto es obvio en el primer caso, y en el segundo resulta de observar que $10^k a = b_1 b_2 \dots b_k + 0,999\dots$ y que $0,999\dots = 1$ (pues si $b = 0,999\dots$, entonces $10b - b = 9b = (9,999\dots) - (0,999\dots) = 9$). Denominaremos *desarrollo decimal de a* aquel que no contiene sólo nueves a partir de un cierto $k \geq 1$. Todo desarrollo decimal $0.a_1 a_2 a_3 \dots$ es el desarrollo decimal de un número $a \in [0, 1)$. Así $0,44999\dots = 0,45$, pero el desarrollo decimal es $0,45$.

Teorema 1.38. *El intervalo $[0, 1)$ de $\mathbb{R}$, es no enumerable.*

Demostración. Sea $\varphi : \mathbb{N} \rightarrow [0, 1)$, y escribamos $\varphi(n) = 0.a_{1n} a_{2n} a_{3n} \dots$, donde $0.a_{1n} a_{2n} a_{3n} \dots$ es el desarrollo decimal de $\varphi(n)$. No hay pérdida de generalidad al suponer que $\varphi(0) = 0$. Sea entonces $a = 0.b_1 b_2 b_3 \dots$, donde $b_n \neq a_{nn}$ y $b_n \neq 0, 9$, $n \geq 1$. Claramente $a \neq 0$ y difiere de $\varphi(n)$, $n \geq 1$, al menos en $b_n \neq a_{nn}$, lo cual implica que $a \notin \varphi(\mathbb{N})$. Entonces φ no puede ser sobreyectiva. $\square$

Corolario 1.29. *Los conjuntos $\mathbb{R}$ y $\mathbb{C}$ son no enumerables.*

Demostración. Ya sabemos que $[0, 1)$ no es enumerable. Como $\psi : \mathbb{R} \rightarrow [0, 1)$ dada por

$$\psi(a) = \frac{|a|}{1 + |a|} \quad (1.158)$$

es obviamente sobreyectiva, si $\mathbb{R}$ fuera enumerable y $f : \mathbb{N} \rightarrow \mathbb{R}$ fuera sobreyectiva, $\psi \circ f : \mathbb{N} \rightarrow [0, 1)$ sería sobreyectiva, lo cual es absurdo. Entonces, $\mathbb{R}$ no es enumerable. Tampoco $\mathbb{C}$ es enumerable, pues $g : \mathbb{C} \rightarrow \mathbb{R}$, $g(a) = \Re(a)$, es sobreyectiva. $\square$

Definición 1.34. Si X y Y son conjuntos y existe $f : X \rightarrow Y$, inyectiva, se dice que el *cardinal de X* es inferior al *cardinal de Y* , y se escribe

$$\text{Card}(X) \leq \text{Card}(Y). \quad (1.159)$$

Nota 1.61. La relación (1.159) es válida si $X = \emptyset$ (nota 1.2). Y si $X \neq \emptyset$, es válida si y sólo si existe $g : Y \rightarrow X$ sobreyectiva (lema 1.3).

Si $\text{Card}(X) \leq \text{Card}(Y)$ y $\text{Card}(Y) \leq \text{Card}(X)$, se dice que X y Y tienen el mismo cardinal, y se escribe

$$\text{Card}(X) = \text{Card}(Y). \quad (1.160)$$

Se dice también que X y Y son *equinumerosos*.

Nota 1.62. Si existe $f : X \rightarrow Y$, biyectiva, se dice que X y Y son *equipotentes*. Es claro que si X y Y son equipotentes entonces $\text{Card}(X) = \text{Card}(Y)$, es decir, X y Y son *equinumerosos*. Lo recíproco es también cierto, pero como no lo usaremos, no lo demostraremos.

Definición 1.35. Si $\text{Card}(X) \leq \text{Card}(Y)$ pero $\text{Card}(X) \neq \text{Card}(Y)$, diremos que el *cardinal de X* es estrictamente inferior al de Y , y escribiremos

$$\text{Card}(X) < \text{Card}(Y). \quad (1.161)$$

Nota 1.63. Decir que $\text{Card}(X) < \text{Card}(Y)$ equivale a decir que $\text{Card}(X) \leq \text{Card}(Y)$ pero no existen $f : X \rightarrow Y$, sobreyectiva, o $g : Y \rightarrow X$, inyectiva. Esto responde intuitivamente a la idea de que Y puede cubrir a X , pero X no puede cubrir a Y ; o sea, a que, en alguna forma, Y tiene más elementos que X .

Diremos que el *cardinal de $\mathbb{N}$* es $\aleph_0$ (Aleph sub cero): $\aleph_0 = \text{Card}(\mathbb{N})$. Si X es infinito entonces

$$\aleph_0 = \text{Card}(\mathbb{N}) \leq \text{Card}(X). \quad (1.162)$$

Esto resulta del corolario 1.23. Más aún, $\text{Card}(X) = \aleph_0$ si y sólo si X es infinito enumerable, como resulta de lo dicho en la nota 1.60.

Como lo hemos mencionado, la *noción de cardinal generaliza la idea de número de elementos de un conjunto finito a los conjuntos infinitos, y el hecho de que $\text{Card}(X) < \text{Card}(Y)$ sugiere que Y tiene, en alguna forma, más elementos que X* . Ya hemos visto, por ejemplo que $\aleph_0 = \text{Card}(\mathbb{N}) < \text{Card}(\mathbb{R})$, así que hay más números reales que números naturales. También $\aleph_0 < \text{Card}(\mathbb{C})$, y habrá más complejos que naturales. Por otra parte $\aleph_0 \leq \text{Card}(\mathbb{R} \setminus \mathbb{Q})$, pues $\mathbb{R} \setminus \mathbb{Q}$ es infinito ($\frac{\sqrt{2}}{n}$ es irracional para todo $n \in \mathbb{N}$, $n > 0$ (sección 1.7), y $\mathbb{N}$ es infinito), y si fuera $\aleph_0 = \text{Card}(\mathbb{R} \setminus \mathbb{Q})$, o sea, si $\mathbb{R} \setminus \mathbb{Q}$ fuera enumerable, $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$ sería enumerable (nota 1.59), lo cual es absurdo. Entonces,

$$\aleph_0 < \text{Card}(\mathbb{R} \setminus \mathbb{Q}). \quad (1.163)$$

En este sentido, $\mathbb{C}$, $\mathbb{R}$ y $(\mathbb{R} \setminus \mathbb{Q})$ son *más numerosos* que $\mathbb{N}$, y que $\mathbb{Z}$ y $\mathbb{Q}$, pues,

$$\aleph_0 = \text{Card}(\mathbb{N}) = \text{Card}(\mathbb{Z}) = \text{Card}(\mathbb{Q}). \quad (1.164)$$

También $\text{Card}(\mathbb{N}) = \text{Card}(\mathbb{N} \times \mathbb{N}) = \text{Card}(\mathbb{Z} \times \mathbb{Z}) = \text{Card}(\mathbb{Q} \times \mathbb{Q}) = \aleph_0$ (nota 1.59). De hecho, si X es enumerable infinito, $n \geq 2$, y

$$X^n = X \times X \times \cdots \times X \quad (n \text{ factores}), \quad (1.165)$$

un argumento inductivo basado en la nota 1.59 demuestra que

$$\text{Card}(X^n) = \aleph_0,$$

y lo mismo es cierto de todo subconjunto infinito $Y \subseteq X^n$, (pues $\aleph_0 \leq \text{Card}(Y) \leq \text{Card}(X^n) = \aleph_0$). De las consideraciones anteriores y de lo observado en la nota 1.59, se deduce el siguiente teorema, que será útil más adelante.

Teorema 1.39. *El conjunto $\mathbb{Q}[x]$ de los polinomios en x sobre $\mathbb{Q}$ es enumerable.*

Demostración. En efecto, $\mathbb{Q}[x] = \bigcup_{n=1}^{\infty} \mathbb{Q}_n[x]$, donde $\mathbb{Q}_n[x] = \{f(x) \in \mathbb{Q}[x] : \text{grad}(f(x)) \leq n\}$, y obviamente la aplicación $\varphi : \mathbb{Q}^{n+1} \rightarrow \mathbb{Q}_n[x]$ dada por $\varphi(a_1, a_2, \dots, a_{n+1}) = a_1 + a_2x + \cdots + a_{n+1}x^n$ es biyectiva, así que $\text{Card}(\mathbb{Q}_n[x]) = \text{Card}(\mathbb{Q}^{n+1}) = \aleph_0$. Basta ahora aplicar lo dicho en la nota 1.59. $\square$

EJERCICIOS

- 1.1 Verifique las relaciones (1.1).
- 1.2 Verifique la primera de las relaciones (1.2).
- 1.3 Verifique la segunda de las relaciones (1.11).
- 1.4 Sean $(A_i)_{i \in I}$ una familia de subconjuntos de X , $f : X \rightarrow Y$. Verifique que:

$$1. \quad f\left(\bigcup_{i \in I} A_i\right) = \bigcup_{i \in I} f(A_i),$$

$$2. \quad f\left(\bigcap_{i \in I} A_i\right) \subseteq \bigcap_{i \in I} f(A_i),$$

y dé ejemplos de $f : X \rightarrow Y$ y de dos subconjuntos A_1, A_2 de X tales que $f(A_1 \cap A_2) \neq f(A_1) \cap f(A_2)$. Demuestre además que $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ cualesquiera que sean $A_1, A_2 \subseteq X$ si y sólo si f es inyectiva.

- 1.5 Sean $f : X \rightarrow Y$, $(B_i)_{i \in J}$ una familia de subconjuntos de Y . Demuestre que

$$1. \quad f^{-1}\left(\bigcup_{i \in J} B_i\right) = \bigcup_{i \in J} f^{-1}(B_i),$$

$$2. \quad f^{-1}\left(\bigcap_{i \in J} B_i\right) = \bigcap_{i \in J} f^{-1}(B_i).$$

- 1.6 Sean $f : X \rightarrow Y$, $A \subseteq X, B \subseteq Y$. Demuestre que

$$A \subseteq f^{-1}(f(A)), \quad f(f^{-1}(B)) \subseteq B$$

y dé ejemplos en los cuales las inclusiones sean estrictas (es decir, donde no valga la igualdad). ¿En qué circunstancias es válida la igualdad para la primera de estas relaciones para todo $A \subseteq X$? ¿Y, la segunda, para todo $B \subseteq Y$?

- 1.7 Sean f, A y B como en el ejercicio anterior. Verifique que $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$, y que si f es inyectiva, $f(X \setminus A) \subseteq Y \setminus f(A)$.
- 1.8 Sea $G \subseteq X \times Y$ una gráfica. Demuestre que $(G^{-1})^{-1} = G$, y que si $G' \subseteq G$ entonces $(G')^{-1} \subseteq G^{-1}$. Demuestre en detalle que si $f = (X, G, Y)$ es una función, G^{-1} es funcional si y sólo si f es inyectiva, y que (Y, G^{-1}, X) es una función si y sólo si f es biyectiva.
- 1.9 Sean $G \subseteq X \times X$ una gráfica. Se dice que $R = (X, G, X)$ es una *relación de equivalencia* en X si:

- (1) $\Delta_X \subseteq G$ ($(a, a) \in G$ para todo $a \in X$)
- (2) $G \subseteq G^{-1}$ (de lo cual, $G^{-1} = G : (a, b) \in G$ si y sólo si $(b, a) \in G$)
- (3) $G \circ G \subseteq G$ (si $(a, b) \in G$ y $(b, c) \in G$ entonces $(a, c) \in G$).

Aquí, $G \circ G = \{(a, b) \mid a, b \in X \text{ y existe } c \in X \text{ tal que } (a, c), (c, b) \in G\}$.

Demuestre entonces que $x \in G(x)$, así que $G(x) \neq \emptyset$, para todo $x \in X$, que $G(x) \cap G(y) \neq \emptyset$ si y sólo si xRy , en cuyo caso $G(x) = G(y)$, y que $X = \bigcup_{x \in X} G(x)$, de tal manera que $\{G(x) \mid x \in X\}$ es lo que se conoce como una *partición de X* . En lugar de xRy es usual escribir, para una relación de equivalencia R , $x \equiv y \pmod{R}$. Se dice además que $G(x)$ es la *clase de equivalencia módulo R* de x y el conjunto

$\{G(x) : x \in X\}$ de las clases de equivalencia módulo R se denomina el *conjunto cociente* de X por R y se denota con X/R . La aplicación $\varphi : X \rightarrow X/R$ que a x asocia $G(x)$ ($\varphi(x) := G(x)$) se denomina la *aplicación canónica* o la *aplicación cociente* de R .

1.10 Verifique que:

- a) $X \times (Y \cup Z) = (X \times Y) \cup (X \times Z)$.
- b) $X \times (Y \cap Z) = (X \times Y) \cap (X \times Z)$.

*1.11 Es un axioma de la teoría de conjuntos que si A es un conjunto y $A \neq \emptyset$, existe $B \in A$ tal que $B \cap A = \emptyset$. Demuestre que este axioma implica:

- a) Si A es un conjunto, $A \notin A$. (Indicación. Considere $\{A\}$).
- b) Si A y B son conjuntos y $A \in B$ entonces $B \notin A$. (Indicación. Considere $\{A, B\}$).
- c) Explique por qué no existe el *conjunto de todos los conjuntos que pueden definirse en castellano con menos de veinte palabras*.
- d) Demuestre en detalle que las afirmaciones " $x \notin x$ ", " x es un conjunto" y " $x = x$ " no son colectivizantes.
¿Son colectivizantes las afirmaciones $x \in x$, $x \neq x$? (Resp. Si)
- e) Demuestre que si A es un conjunto, siempre existe a tal que $a \notin A$.
- f) Sean A un conjunto, $X = \wp(A)$. Es colectivizante la relación " $x \in X$ y $x \notin x$ ". Si lo es, ¿qué es $\{x : X \text{ y } x \notin x\}$?

1.12 Sea $f : X \rightarrow Y$. Demuestre que si $G = \{(x, y) : f(x) = f(y)\}$ entonces $R_f = (X, G, X)$ es una relación de equivalencia en X (ejercicio 1.9), denominada la *relación de equivalencia asociada a f* , y que si $\varphi : X \rightarrow X/R_f$ es la aplicación canónica de R_f , existe una aplicación inyectiva $\tilde{f} : X/R_f \rightarrow Y$ tal que $\tilde{f} \circ \varphi = f$.

1.13 Sean $f : X \rightarrow Y$, R una relación de equivalencia en X con gráfica G , $\psi : X \rightarrow X/R$ su aplicación canónica.

- (a) Demuestre que $R_\psi = R$ y que para que exista una aplicación $\hat{f} : X/R \rightarrow Y$ tal que $\hat{f} \circ \psi = f$ es necesario y suficiente que $G \subseteq G_f$, donde G_f es la gráfica de R_f . (ejercicio 1.12).
- (b) Demuestre que $\hat{f}$ es inyectiva si y sólo si $G = G_f$.

1.14 Sean X, Y conjuntos, $f : X \rightarrow Y$. La aplicación f induce aplicaciones

$$\begin{array}{ccc} f_* : \wp(X) \rightarrow \wp(Y) & f^* : \wp(Y) \rightarrow \wp(X) \\ A \mapsto f(A) & B \mapsto f^{-1}(B) \end{array}$$

¿Qué relación existe entre $f_*(f^*(B))$ y B y entre $f^*(f_*(A))$ y A ?

1.15 Sean X, Y conjuntos, $f : X \rightarrow Y$. La aplicación f induce aplicaciones

$$f_* : \wp(\wp(X)) \rightarrow \wp(\wp(Y)), \quad f^* : \wp(\wp(Y)) \rightarrow \wp(\wp(X))$$

definidas respectivamente para $A \subseteq \wp(X)$ y $B \subseteq \wp(Y)$ por

$$\begin{aligned} f_*(A) &= \{B \subseteq Y : f^{-1}(B) \in A\}, \\ f^*(B) &= \{f^{-1}(B) : B \in B\}. \end{aligned}$$

Compruebe que $B \subseteq f_*(f^*(B))$ y que $f^*(f_*(A)) \subseteq A$.

1.16 Sean a, b, c números reales. Verifique que

$$\begin{aligned} -(a+b) &= (-a) + (-b), \\ -(a-b) &= b-a, \\ (a+b)-c &= a+(b-c), \\ (a-b)+c &= a-(b-c), \\ (a-b)-c &= a-(b+c) \end{aligned}$$

1.17 Sean a, b, c números reales con $bc \neq 0$. Demuestre que

$$\begin{aligned} (bc)^{-1} &= b^{-1}c^{-1}, \\ (b/c)^{-1} &= c/b, \\ (ab)/c &= a(b/c), \\ (a/b)c &= a/(b/c), \\ (a/b)/c &= a/bc. \end{aligned}$$

Sea $a \in \mathbb{R}$, $a \neq 0$. Demuestre que $a = a^{-1}$ si y sólo si $a = \pm 1$.

1.18 Sean a, b, c, d números reales. Demuestre que

- a) Si $a \leq b$ y $c \leq d$ entonces $a+c \leq b+d$.
- b) Si $0 \leq a \leq b$ y $0 \leq c \leq d$ entonces $ac \leq bd$.
- c) Si $0 \leq a \leq b$ y $c \leq d \leq 0$ entonces $bc \leq ad$.

1.19 Sean a, b, c, d números reales. Demuestre que

- a) $a \leq b$ si y sólo si $a < b$ o $a = b$.
- b) Si $a < b$ y $b \leq c$ entonces $a < c$.
- c) Si $a < b$ entonces $b \not< a$.
- d) Si $a < b$ y $c \leq d$ entonces $a + c < b + d$.
- e) Si $a < b$ y $c > 0$ entonces $ac < bc$.
- f) Si $a < b$ y $c < 0$ entonces $bc < ac$.

1.20 Verifique que $\mathbb{R}_+ + \mathbb{R}_+ = \mathbb{R}_+$, $\mathbb{R}_+ \mathbb{R}_+ = \mathbb{R}_+$.

1.21 Demuestre que si $A \subseteq \mathbb{Z}$ es inferiormente acotado y no vacío, A tiene un mínimo. De hecho, $\inf A = \min A$. Verifique entonces que si $a \in \mathbb{R}$ y $[a] = \min \{m \in \mathbb{Z} : m \geq a\}$, entonces $[a] \in \mathbb{Z}$ y $[a] - 1 < a \leq [a]$ con $a = [a]$ si sólo si $a \in \mathbb{Z}$. Demuestre además que si $m \in \mathbb{Z}$, $m = [a]$ si y sólo si $a \leq m < a + 1$. Se dice que $[a]$ es el *menor entero mayor que a* . Demuestre finalmente que $[a] = [a]$ si $a \in \mathbb{Z}$ y que $[a] = [a] + 1$ si $a \notin \mathbb{Z}$.

1.22 Sean $\psi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}$ la aplicación $\psi(a, b) = a - b$ y $R = R_\psi$ la relación de equivalencia sobre $\mathbb{N} \times \mathbb{N}$ asociada con ψ (ejercicio 1.12). Sean $\tilde{\mathbb{Z}} = \mathbb{N} \times \mathbb{N} / R$, $\varphi : \mathbb{N} \times \mathbb{N} \rightarrow \tilde{\mathbb{Z}}$ la aplicación canónica, $\tilde{\psi} : \tilde{\mathbb{Z}} \rightarrow \mathbb{Z}$ la aplicación obtenida de ψ como en el ejercicio 1.12. Demuestre que $\tilde{\psi}$ es biyectiva. Para cada $(a, b) \in \mathbb{N} \times \mathbb{N}$, sea $[a, b] = \varphi(a, b)$ la clase de equivalencia módulo R de (a, b) . Demuestre que $[a, b] = [c, d]$ si y sólo si $a + d = b + c$ (así que la relación de equivalencia R puede definirse independientemente de ψ por $(a, b) \equiv (c, d) \pmod{R}$ si y sólo si $a + d = b + c$) y que $[a, b] + [c, d] = [a + c, b + d]$ define una ley de composición interna en $\tilde{\mathbb{Z}}$ tal que $\tilde{\psi}([a, b] + [c, d]) = \tilde{\psi}([a, b]) + \tilde{\psi}([c, d])$. Demuestre que también $[a, b][c, d] = [ac + bd, ad + bc]$ define una ley de composición interna en $\tilde{\mathbb{Z}}$ tal que $\tilde{\psi}([a, b][c, d]) = \tilde{\psi}([a, b])\tilde{\psi}([c, d])$.

Identifique $\mathbb{N}$ con $\mathbb{N} \times \{0\}$ y demuestre que $\varphi : \mathbb{N} \rightarrow \tilde{\mathbb{Z}}$ es inyectiva y tal que $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$ (así que identificando a $\mathbb{N}$ con $\tilde{\mathbb{N}} = \varphi(\mathbb{N})$, se puede considerar que $(\mathbb{N}, +, \cdot)$ es un subsistema de $(\tilde{\mathbb{Z}}, +, \cdot)$).

Nota: Se deduce que $(\tilde{\mathbb{Z}}, +, \cdot)$, construido arriba, es esencialmente igual a $(\mathbb{Z}, +, \cdot)$. Cuando se conoce $(\mathbb{N}, +, \cdot)$, por ejemplo axiomáticamente (Peano) o, mejor, a partir de una teoría cardinal u ordinal, pero

no se conoce el sistema $(\mathbb{Z}, +, \cdot)$, éste puede construirse a partir de $(\mathbb{N}, +, \cdot)$ via $(\tilde{\mathbb{Z}}, +, \cdot)$ (definiendo R directamente). Para evitar este tipo de construcciones, evidentemente engorrosas, hemos preferido desarrollar una teoría puramente axiomática de los reales. (En ciertos contextos tales construcciones son, sin embargo, inevitables).

1.23 Demuestre que la relación de inclusión $\subseteq$ es una relación de orden en $\wp(X)$, pero que si X tiene más de un punto, no es una relación de orden total. (nota 1.7).

1.24 Demuestre que $a \mid b$ si y sólo si $a \mid |b|$, $|a| \mid |b|$ o $|a| \mid b$. Verifique además que si $a \mid b$ entonces $|a| \leq |b|$, que $a \mid b$ y $b \mid a$ si y sólo si $|a| = |b|$, y que $\text{mcd}(a, b) = \text{mcd}(a, |b|) = \text{mcd}(|a|, |b|) = \text{mcd}(|a|, b)$.

1.25 Sean a, b números reales. Demuestre que

$$\min\{a, b\} + \max\{a, b\} = a + b.$$

1.26 Sean $a_1, \dots, a_n$ enteros, no todos nulos. Se dice que $d > 0$ es un *máximo común divisor* de $a_1, \dots, a_n$, si es un divisor común de todos los a_i , y si todo divisor común de todos los a_i es también un divisor de d . Demuestre que el máximo común divisor de $a_1, \dots, a_n$, si existe, está unívocamente determinado por éstos números. Se escribe:

$$d = \text{mcd}(a_1, \dots, a_n).$$

Demuestre que $d > 0$ es un máximo común divisor de $a_1, \dots, a_n$ si es un divisor común de todos los a_i y existen enteros $m_1, \dots, m_n$ tales que

$$d = m_1 a_1 + \dots + m_n a_n$$

Demuestre la existencia de d observando que $X = \{c > 0 : c = m_1 a_1 + \dots + m_n a_n, m_i \in \mathbb{Z}\} \neq \emptyset$ y tomando $d = \min(X)$.

A su vez, si $a_1 \cdots a_n \neq 0$, se dice que m es un *mínimo común múltiplo* de $a_1, \dots, a_n$, si $m > 0$, si es un múltiplo de cada a_i , y si todo múltiplo de todos los a_i es divisible por m . Demuestre que si d es como se describe arriba, entonces

$$m = |a_1 a_2 \cdots a_n| / d$$

es un mínimo común múltiplo de $a_1, \dots, a_n$, y el único posible. Demuestre además que si los primos $p_1, \dots, p_l$ son distintos y tales que $a_i = p_1^{\alpha_{i1}} \cdots p_l^{\alpha_{il}}$, $i = 1, 2, \dots, n$, $\alpha_{ik} \geq 0$, $k = 1, \dots, l$, entonces

$$d = p_1^{\alpha_1} \cdots p_l^{\alpha_l}, \quad m = p_1^{\beta_1} \cdots p_l^{\beta_l}$$

donde $\alpha_k = \min \{\alpha_{ik} : i = 1, \dots, n\}$, $\beta_k = \max \{\alpha_{ik} : i = 1, \dots, n\}$.
¿Qué son $\text{mcd}(p_1, \dots, p_n)$ y $\text{mcm}(p_1, \dots, p_n)$?

- 1.27 Con respecto al ejercicio anterior, verifique que si a, b, c son enteros no nulos, entonces

$$\text{mcd}(\text{mcd}(a, b), c) = \text{mcd}(a, b, c),$$

y

$$\text{mcm}(\text{mcm}(a, b), c) = \text{mcm}(a, b, c).$$

- 1.28 Demuestre que si $a > 1$ es un entero no primo, debe existir al menos un primo p tal que $p \mid a$ y $p \leq \sqrt{a}$. Concluya que si ningún primo $p \leq \sqrt{a}$ divide a a , entonces a es primo.

Este ejercicio muestra que para buscar los factores primos de un número a basta buscarlos entre los primos menores o iguales que $\sqrt{a}$. Si uno de tales primos, p_1 , divide a , repítase el proceso con a/p_1 , y así sucesivamente. Llegará un momento en que $a/p_1 \cdots p_n$, $n \geq 1$, es un primo p_{n+1} , o sea que ningún primo $\leq \sqrt{a/p_1 \cdots p_n}$ dividirá $a/p_1 \cdots p_n$. Entonces, $a = p_1 \cdots p_{n+1}$.

- 1.29 Sean $a, b \in \mathbb{Z}$ tales que $a^2 + b^2 > 0$ y sea $d = \text{mcd}(a, b)$. Verifique que si $d = ma + nb$, $m, n \in \mathbb{Z}$, entonces $d = (cb + m)a + (-ca + n)b$ para todo $c \in \mathbb{Z}$, así que no es posible esperar unicidad de m y n en una relación de Bezout.
- 1.30 Sean $\varphi : X \rightarrow \mathbb{N}$ y $\psi : Y \rightarrow \mathbb{N}$ aplicaciones inyectivas. Demuestre que $f : X \times Y \rightarrow \mathbb{N}$ dada por $f(x, y) = 2^{\varphi(x)} 3^{\psi(y)}$ es también inyectiva.
- 1.31 Sea p un primo impar (i.e., $p > 2$). Demuestre que p es de la forma $4n + 1$ o $4n + 3$, $n \in \mathbb{N}$, y que el número de primos de la forma $4n + 3$ es infinito. (Indicación. Si $p_1, \dots, p_m$ son primos de la forma $4n + 3$, demuestre que $P = p_1 \cdots p_m$ es de la forma $4n + 1$ o $4n + 3$. Concluya que en el primer caso debe existir un primo $p \neq p_1, \dots, p_m$ y de la forma $4n + 3$ tal que $p \mid P + 2$, y en el segundo, un primo p de las mismas características tal que $p \mid P + 4$). Demuestre, de la misma manera, que todo primo ≥ 5 es de la forma $6n + 1$ o $6n + 5$, y que el número de primos de la forma $6n + 5$ es infinito.
- 1.32 Sean $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, $\psi : \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Q}$ la aplicación $\psi(a, b) = a/b$, $R = R_\psi$ la relación de equivalencia en $\mathbb{Z} \times \mathbb{Z}^*$ asociada con ψ (ejercicio 1.12). Sean $\tilde{\mathbb{Q}} = \mathbb{Z} \times \mathbb{Z}^* / R$, $\varphi : \mathbb{Z} \times \mathbb{Z}^* \rightarrow \tilde{\mathbb{Q}}$ la aplicación

canónica, $\tilde{\psi} : \tilde{\mathbb{Q}} \rightarrow \mathbb{Q}$ la aplicación obtenida de ψ como en el ejercicio 1.12. Demuestre que $\tilde{\psi}$ es biyectiva. Demuestre además que $(a, b) \equiv (c, d) \pmod{R}$ si y sólo si $ad = bc$ (lo cual permite definir R independientemente de ψ). Sea $[a, b] = \varphi(a, b)$. Demuestre que $[a, b] + [c, d] = [ad + bc, bd]$ y $[a, b] [c, d] = [ac, bd]$ definen leyes de composición interna en $\tilde{\mathbb{Q}}$ y que $\tilde{\psi}([a, b] + [c, d]) = \tilde{\psi}([a, b]) + \tilde{\psi}([c, d])$, $\tilde{\psi}([a, b] [c, d]) = \tilde{\psi}([a, b]) \tilde{\psi}([c, d])$, (así que $(\tilde{\mathbb{Q}}, +, \cdot)$ es esencialmente lo mismo que $(\mathbb{Q}, +, \cdot)$). Demuestre también que si $\mathbb{Z}$ se identifica con $\mathbb{Z} \times \{1\}$, $\varphi : \mathbb{Z} \rightarrow \tilde{\mathbb{Q}}$ es inyectiva, $\varphi(a + b) = \varphi(a) + \varphi(b)$ y $\varphi(ab) = \varphi(a) \varphi(b)$ (así que $\mathbb{Z}$ puede considerarse como un subconjunto de $\tilde{\mathbb{Q}}$).

Nota. Evidentemente, la construcción anterior de $(\tilde{\mathbb{Q}}, +, \cdot)$ es completamente análoga a la de $(\tilde{\mathbb{Z}}, +, \cdot)$ en el ejercicio 1.22. Ambas se originan en las ideas introducidas en el ejercicio 1.12. Generalmente $(\tilde{\mathbb{Q}}, +, \cdot)$ se construye en segunda etapa, a partir de $(\tilde{\mathbb{Z}}, +, \cdot)$, ya construido a partir de $(\mathbb{N}, +, \cdot)$ como en tal ejercicio.

- 1.33 Compruebe que el sistema $(\mathbb{Q}, +, \cdot, \mathbb{Q}_+)$, donde $\mathbb{Q}_+ = \mathbb{Q} \cap \mathbb{R}_+$, satisface los axiomas algebraicos y los axiomas algebraicos del orden de $\mathbb{R}$. Compruebe, sin embargo, que el conjunto $A = \{x \in \mathbb{Q} : x^2 \leq 2\}$ es acotado superiormente en $\mathbb{Q}$ pero no tiene extremo superior en $\mathbb{Q}$.
- 1.34 Demuestre que si $A \subseteq \mathbb{Q}$ es tal que $A \cup (-A) = \mathbb{Q}$, $A \cap (-A) \subseteq \{0\}$, $A + A \subseteq A$ y $AA \subseteq A$, entonces $A = \mathbb{Q}_+ := \mathbb{Q} \cap \mathbb{R}_+$. (Indicación. Demuestre primero que $0, 1 \in A$ y concluya que $\mathbb{N} \subseteq A$).
- 1.35 Demuestre que si $A \subseteq \mathbb{R}$ es tal que $A \cup (-A) = \mathbb{R}$, $A \cap (-A) \subseteq \{0\}$, $A + A \subseteq A$ y $AA \subseteq A$, entonces $A = \mathbb{R}_+$.
- 1.36 Sean $A \subseteq \mathbb{R}$, $A^* := A^+ \cap \mathbb{Q} = \{a \in \mathbb{Q} : a \geq x \text{ para todo } x \in A\}$. Si $A \neq \emptyset \neq A^*$ y $A \cap A^* = \emptyset$, se dice que (A, A^*) es una *cortadura de Dedekind* de $\mathbb{Q}$. Para cada $a \in \mathbb{R}$, sea $A_a = \{x \in \mathbb{Q} : x < a\}$. Verifique que (A_a, A_a^*) es una *cortadura de Dedekind* de $\mathbb{Q}$ y que si $\tilde{\mathbb{R}}$ es el conjunto de todas las cortaduras de Dedekind de $\mathbb{Q}$, $\psi : \mathbb{R} \rightarrow \tilde{\mathbb{R}}$ dada por $\psi(a) = (A_a, A_a^*)$ es biyectiva. Defina en $\tilde{\mathbb{R}}$ la relación de orden $(A, A^*) \leq (B, B^*)$ si y sólo si $A \subseteq B$. Con los significados obvios, verifique que si $A \subseteq \mathbb{R}$ es superiormente acotado y no vacío, A tiene un extremo superior.

Nota. Este ejercicio apunta en la misma dirección que los ejercicios 1.23 y 1.34. Se trata ahora de construir $\mathbb{R}$ a partir de $\mathbb{Q}$ via $\tilde{\mathbb{R}}$. Esto requiere definir sumas y productos apropiados de cortaduras, lo cual no es del todo trivial, pero puede hacerse. Si tenemos entonces una teoría lo suficientemente buena de $(\mathbb{N}, +, \cdot)$ para asegurar la existencia de tal sistema (ninguna teoría axiomática lo hace), tal como en cierta forma lo hacen la teoría ordinal o la cardinal, o si admitimos desde un comienzo que $(\mathbb{N}, +, \cdot)$ nos ha sido dado por Dios (Kröneckner), podemos construir $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$, garantizando así su existencia. Este es un mérito de las teorías constructivas o genéticas, que las teorías axiomáticas no tienen.

*1.37 Sea $(\tilde{\mathbb{R}}, +, \cdot, \tilde{\mathbb{R}}_+)$, un sistema numérico que satisface los mismos axiomas algebraicos de $(\mathbb{R}, +, \cdot, \mathbb{R}_+)$ y los mismos axiomas de orden, incluyendo el axioma (A.C.R). Demuestre que existe una aplicación biyectiva $f: \mathbb{R} \rightarrow \tilde{\mathbb{R}}$ tal que $f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ y que $f(a) \leq f(b)$ si $a \leq b$. (Indicación. Defina $\tilde{\mathbb{N}}$, $\tilde{\mathbb{Z}}$, $\tilde{\mathbb{Q}}$ en $\tilde{\mathbb{R}}$ de la manera obvia, y comience por definir $f: \mathbb{N} \rightarrow \tilde{\mathbb{R}}$ por $f(0) = \tilde{0}$ y $f(n+1) = f(n) + \tilde{1}$, verificando que f aplica biyectivamente $\mathbb{N}$ sobre $\tilde{\mathbb{N}}$. Luego extienda sucesivamente f a $\mathbb{Z}$, y a $\mathbb{Q}$, de la manera obvia, verificando que $f(\mathbb{Z}) = \tilde{\mathbb{Z}}$ y $f(\mathbb{Q}) = \tilde{\mathbb{Q}}$, biyectivamente. Finalmente, para $r \in \mathbb{R}$, defina $f(r) = \sup\{f(x) : x \in \mathbb{Q}, x < r\}$. Demuestre además que f es única con las anteriores propiedades. Demuestre finalmente que no es posible definir una aplicación biyectiva de $\mathbb{R}$ en $\mathbb{Q}$ que satisfaga las propiedades anteriores de f .

1.38 Verifique las relaciones (1.55), (1.56), (1.58), (1.59), (1.60) y (1.61).

1.39 Compruebe las relaciones (1.75), (1.76), (1.77), (1.78), (1.79), (1.80), (1.81), (1.82), (1.83) y (1.84).

1.40 Demuestre que no existe en $\mathbb{C}$ una relación de orden $a < b$ (i.e., $a \leq b$ y $a \neq b$) tal que $0 < a+b$ y $0 < ab$ si $0 < a$ y $0 < b$. (Indicación. Demuestre que no puede ser $0 < i^2$).

1.41 Para $0 \leq k \leq n$, k y n enteros, se definen

$$n! = \begin{cases} 1, & n = 0, \\ (n-1)!n, & n \geq 1. \end{cases}$$

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

Verifique que $\binom{n}{0} = \binom{n}{n} = 1$ y demuestre que para $1 \leq k \leq n$,

$$\binom{n}{k} = \binom{n}{n-k}, \quad \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

Concluya que si $0 \leq k \leq n$, $\binom{n}{k}$ es un número natural (haga inducción sobre n).

1.42 Sean $a, b \in \mathbb{C}$. Use inducción y los resultados del ejercicio 1.41 para demostrar que si $n \in \mathbb{N}$ entonces

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k, \quad 2^n = \sum_{k=0}^n \binom{n}{k}.$$

Demuestre también que si a y b son reales, $a, b \geq 0$, entonces

$$\left(\frac{a+b}{2}\right)^n \leq \frac{a^n + b^n}{2}, \quad n \geq 0.$$

1.43 Para $a \in \mathbb{R}$, $a > 0$, y $r \in \mathbb{Q}$, sea a^r como en la nota 1.27. Demuestre que

$$a) \quad a^r \cdot a^{r'} = a^{r+r'}, \quad r, r' \in \mathbb{Q}.$$

$$b) \quad (a^r)^{r'} = a^{rr'}, \quad r, r' \in \mathbb{Q}.$$

$$c) \quad \text{Si también } b > 0, (ab)^r = a^r b^r, \quad r \in \mathbb{Q}.$$

**1.44 (Para lectores muy pacientes). Para $a \in \mathbb{R}$, $a \geq 1$, y $x \in \mathbb{R}$, $x > 0$, defínase

$$a^x = \sup\{a^r : r \in \mathbb{Q}, 0 < r < x\}.$$

Verifique que a^x está bien definido. Para $0 < a < 1$ y $x \in \mathbb{R}$, $x > 0$, defínase

$$a^x = [(a^{-1})^x]^{-1}.$$

Finalmente, para $a > 0$ y $x \in \mathbb{R}$, $x \leq 0$, defínase

$$a^x = (a^{-1})^{-x}.$$

Verifique que

$$a) \quad a^x \cdot a^y = a^{x+y}, \quad a > 0, \quad x, y \in \mathbb{R}.$$

$$b) \quad (a^x)^y = a^{xy}, \quad a > 0, \quad x, y \in \mathbb{R}.$$

$$c) \quad (ab)^x = a^x b^x, \quad a, b > 0, \quad x \in \mathbb{R}.$$

Demuestre también que si $a > 0$ y $r \in \mathbb{Q}$, la definición de a^r dada en la nota 1.27 coincide con la presente. Es decir, demuestre que

$$a^r = \sup \{a^s : s \in \mathbb{Q}, 0 < s < r\}, \quad a \geq 1, \quad r \in \mathbb{Q}, \quad r > 0.$$

Para otra definición de a^x , $a, x \in \mathbb{R}$, $a > 0$, véase [9], capítulo 5, nota 5.10.

1.45 Verifique que

$$a) \quad \sum_{k=0}^n (-1)^k \binom{2n}{2k} = 2^n \cos \frac{n\pi}{2}.$$

$$b) \quad \sum_{k=0}^n (-1)^{k+1} \binom{2n}{2k-1} = 2^n \sin \frac{n\pi}{2}.$$

$$c) \quad \sum_{k=0}^n (-1)^k \binom{2n+1}{2k+1} = 2^n \sqrt{2} \sin \frac{(2n+1)\pi}{4}.$$

$$d) \quad \sum_{k=0}^n (-1)^k \binom{2n+1}{2k} = 2^n \sqrt{2} \cos \frac{(2n+1)\pi}{4}.$$

$$e) \quad \sum_{k=0}^n (-1)^k \binom{2n+1}{2k} = \sum_{k=0}^n (-1)^{n-k} \binom{2n+1}{2k+1}.$$

1.46 Si $\mathbb{C}_+ = \{z \in \mathbb{C} : \Re(z) \geq 0\}$ y $\mathbb{C}^+ = \{z \in \mathbb{C} : \Im(z) \geq 0\}$ ¿son $(\mathbb{C}_+, +, \cdot)$ y $(\mathbb{C}^+, +, \cdot)$ sistemas numéricos? Demuestre que si $K \subseteq \mathbb{R}$ es un dominio y $K_+ = \{x \in K : x \geq 0\}$, entonces $(K_+, +, \cdot)$ es un sistema numérico.

1.47 Sea $S \subseteq \mathbb{C}$. Demuestre que $-(-S) = S$, y concluya que $S = -S$ si y sólo si $-S \subseteq S$. Verifique igualmente que si $0 \notin S$ entonces $(S^{-1})^{-1} = S$, y demuestre que $S^{-1} = S$ si y sólo si $S^{-1} \subseteq S$.

1.48 Si $(S, +, \cdot)$ es un dominio numérico y $a \in S$ es tal que $a^{-1} \in S$, se dice que a es una *unidad* de S . Demuestre que a es una unidad de S si y sólo si a^{-1} también lo es, y que si a, b son unidades de S , ab es una unidad de S . ¿Cuáles son las unidades de $(\mathbb{Z}, +, \cdot)$? Si $(S, +, \cdot)$ es un campo ¿cuáles son las unidades de S ?

1.49 Si $(S, +, \cdot)$ es un dominio numérico y $a, b \in S$, diremos que $a \mid b$ en S (a divide a b en S) si $a \neq 0$ y existe $c \in S$ tal que $ac = b$. Se dice también que a es un *divisor* o un *factor* de b . Demuestre:

a) Si $a \in S$ y $a \neq 0$, $a \mid a$ en S .

b) Si $a, b, c \in S$ y $a \mid b$, $b \mid c$, entonces $a \mid c$.

c) Si $a, b \in S$, $a \mid b$ y $b \mid a$, existen $u, v \in S$ tales que $av = 1$ y que $b = ua$, $a = vb$, así que u, v son unidades de S . (ejercicio 1.48)

1.50 Si S es un dominio, $a, b \in S$, y existe una unidad $u \in S$ tal que $b = ua$, en cuyo caso $a = vb$, $v = u^{-1}$, se dice que a y b son *asociados en S* , y se escribe $a \sim b \pmod{S}$. Demuestre que si $a, b \in S$, $ab \neq 0$, entonces $a \sim b \pmod{S}$ si y sólo si $a \mid b$ y $b \mid a$ en S . Demuestre también que si $G = \{(a, b) : a, b \in S, a \sim b \pmod{S}\}$, entonces $R = (S, G, S)$ es una relación de equivalencia en S .

1.51 Sea $(S, +, \cdot)$ un dominio. Se dice que $a \in S$ es *irreducible en S* , si a no es una unidad, y si sus únicos divisores son las unidades y los elementos de S de la forma ua donde u es una unidad. Demuestre que si $(S, +, \cdot)$ es un campo, no existen en S elementos irreducibles. ¿Cuáles son los elementos irreducibles de $(\mathbb{Z}, +, \cdot)$? Demuestre que si $(S, +, \cdot)$ y $(S', +, \cdot)$ son dominios tales que $S \subseteq S'$, entonces:

a) Si $a \in S$ es irreducible en S' , a es también irreducible en S .

b) Si $S \neq S'$, pueden existir elementos $a \in S$ que son irreducibles en S pero no en S' . ¿Puede usted dar un ejemplo de esta circunstancia?

c) Toda unidad de S es una unidad de S' .

1.52 Se dice que el sistema numérico $(S, +, \cdot)$ es *estable bajo conjugación* si $\bar{S} = \{\bar{a} : a \in S\} \subseteq S$ (es decir, si $\bar{S} = S$). Demuestre que $\mathbb{Z}[i]$ y $\mathbb{Q}[i]$ son estables bajo conjugación, pero que $\mathbb{N}[i] = \{a + bi : a, b \in \mathbb{N}\}$ no lo es.

1.53 Sea $(K, +, \cdot)$ un campo numérico. Demuestre que las afirmaciones siguientes son equivalentes:

a) K es estable bajo conjugación. (ejercicio 1.52).

b) $\text{Re}(K) = \{\Re(a) : a \in K\}$ es un subcampo de K .

c) Si $a \in K$, entonces $|a|^2 \in K$.

1.54 Demuestre que si $(K, +, \cdot)$ es un campo numérico, $(\bar{K}, +, \cdot)$ también lo es ($\bar{K} := \{\bar{z} : z \in K\}$).

1.55 Si $S \subseteq \mathbb{C}$ es tal que

1. $0 \in S$,
2. $-S \subseteq S$,
3. $S + S \subseteq S$,

se dice que $(S, +)$ es un *grupo numérico aditivo* o, más precisamente, un *subgrupo aditivo* de $(\mathbb{C}, +)$. A su vez, si $S \subseteq \mathbb{C}$ es tal que

1. $0 \notin S$, $1 \in S$,
2. $S^{-1} \subseteq S$,
3. $SS \subseteq S$,

se dice que $(S, \cdot)$ es un *grupo numérico multiplicativo* o, más precisamente, un *subgrupo multiplicativo* de $(\mathbb{C}^*, \cdot)$, donde $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

Demuestre:

- a) Si $(S, +, \cdot)$ es un dominio, $(S, +)$ es un grupo aditivo.
- b) Si $(K, +, \cdot)$ es un campo, $(K^*, \cdot)$, donde $K^* = K \setminus \{0\}$, es un grupo multiplicativo.
- c) Si $(S, +, \cdot)$ es un dominio, el conjunto $U(S)$ de las unidades de S (ejercicio 1.48) es, con la multiplicación, un grupo multiplicativo.

1.56 Verifique que $\mathbb{Q}[\sqrt{2}]$ dado por (1.89) es un campo numérico en el cual $a + b\sqrt{2} = c + d\sqrt{2}$ si y sólo si $a = c$ y $b = d$, y en el cual, si $a + b\sqrt{2} \neq 0$, $(a + b\sqrt{2})^{-1} = (a - b\sqrt{2}) / (a^2 - 2b^2)$. ¿Es posible que $a^2 = 2b^2$, $a, b \in \mathbb{Q}$? Verifique también que $\mathbb{Q}[i]$ dado por (1.90) es un campo en el cual, si $a + bi \neq 0$, entonces $(a + bi)^{-1} = (a - bi) / (a^2 + b^2)$.

1.57 Demuestre que $\mathbb{Q}[\sqrt[3]{2}]$ dado por (1.92) es un campo. (Indicación. Observe que si $a, b, c \in \mathbb{Q}$ entonces $\text{mcd}(x^3 - 2, a + bx + cx^2) = 1$ cuando $a^2 + b^2 + c^2 \neq 0$. Use entonces el teorema 1.30.)

1.58 Verifique que $\tilde{\mathbb{Q}}$ dado por (1.91) no puede ser un campo. De hecho, ni siquiera es un sistema numérico. (Indicación. Tal como en el ejercicio 1.57, observe que si $a^2 + b^2 + c^2 \neq 0$ entonces $\text{mcd}(x^3 - 2, a + bx + cx^2) = 1$, y muestre que esto contradice el que $\sqrt[3]{4} = (\sqrt[3]{2})^2 = a + b\sqrt[3]{2}$, $a, b \in \mathbb{Q}$.)

1.59 Sea $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} : a, b \in \mathbb{Z}\}$. Verifique que $\mathbb{Z}[i\sqrt{5}]$ es un dominio pero no un campo. Demuestre, de hecho, que las únicas unidades de $\mathbb{Z}[i\sqrt{5}]$ son -1 y 1 , y que $a \in \mathbb{Z}[i\sqrt{5}]$ es irreducible si y sólo si $a \neq \pm 1$ y sus únicos divisores son ± 1 y $\pm a$. Diremos que a es un *primo* de $\mathbb{Z}[i\sqrt{5}]$ si a es irreducible y $\Re(a) > 0$ o $\Re(a) = 0$ e $\Im(a) > 0$. Verifique entonces que $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ son primos distintos y que $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, así que $\mathbb{Z}[i\sqrt{5}]$ no es un dominio factorial. Demuestre finalmente que todo irreducible de $\mathbb{Z}[i\sqrt{5}]$ está asociado con un primo.

1.60 Sea $p \geq 2$ un primo y $\mathbb{Q}_p$ el conjunto de los $r \in \mathbb{Q}$ que pueden escribirse en la forma $r = m/n$ con $m, n \in \mathbb{Z}$, $p \nmid n$. Demuestre:

- a) $\mathbb{Q}_p$ es un dominio de integridad.
- b) $u \in \mathbb{Q}_p$ es una unidad si y sólo si $u = a/b$ donde $a, b \in \mathbb{Z}$ y $p \nmid ab$.
- c) Si $r \in \mathbb{Q}_p$, existen $n \in \mathbb{Z}$, $n \geq 0$, y una unidad $u \in \mathbb{Q}_p$, tales que $r = up^n$.
- d) Los únicos elementos irreducibles de $\mathbb{Q}_p$ son los de la forma up donde u es una unidad de $\mathbb{Q}_p$.
- e) $\mathbb{Q}_p$ es un dominio factorial.
- f) $\mathbb{Q}_p$ no es un campo.

1.61 Demuestre que en el dominio $\mathbb{Z}[i]$ de los enteros de Gauss, las únicas unidades son ± 1 y $\pm i$. Si p es irreducible en $\mathbb{Z}[i]$ y $\Re(p) > 0$, $\Im(p) \geq 0$, se dice que p es un *primo* de $\mathbb{Z}[i]$. Demuestre que si q es irreducible en $\mathbb{Z}[i]$, siempre existe un primo p tal que $p \sim q \pmod{\mathbb{Z}[i]}$.

1.62 Verifique que 5 no es un primo de $\mathbb{Z}[i]$, y encuentre una descomposición de 5 en factores primos (Resp. $5 = (-i)(2 + i)(1 + 2i)$). Verifique también que $5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$ son descomposiciones de 5 en factores irreducibles, y describa las relaciones de asociación para estas descomposiciones. (Resp. $2 + i = i(1 - 2i)$, $2 - i = (-i)(1 + 2i)$.)

1.63 Verifique las relaciones (1.115), (1.116) y (1.117).

1.64 Verifique la relación (1.122).

1.65 Demuestre todas las afirmaciones del texto entre el teorema 1.31 y la nota 1.48.

1.66 Verifique que, en $\mathbb{Q}[x]$,

$$\begin{aligned} 1 &= \frac{1}{2}(x^2 + 1) + \frac{1-x}{2}(1+x) \\ &= \frac{2+x}{2}(x^2 + 1) + \frac{(-1)(x^2+x)}{2}(1+x). \end{aligned}$$

Demuestre, sin embargo, que si K es un campo numérico arbitrario, $f(x), g(x) \in K[x]$, $f(x)g(x) \neq 0$, y $d(x) = \text{mcd}(f(x), g(x))$, existen $m(x), n(x)$, únicos, tales que

$$d(x) = m(x)f(x) + n(x)g(x)$$

y que $\text{grad}(m(x)) < \text{grad}(g(x))$ o $\text{grad}(n(x)) < \text{grad}(f(x))$.

1.67 Sean K, L campos numéricos, $K \subseteq L$, $K \neq L$. Sean $f(x), g(x) \in K[x]$. Dé una relación de Bezout para $d(x) = \text{mcd}(f(x), g(x))$, la cual sea válida en $L[x]$ pero no en $K[x]$.

1.68 Sea K un campo numérico, $f(x) \in K[x]$ un polinomio de grado dos o tres. Demuestre que $f(x)$ es irreducible en $K[x]$ si y sólo si $f(x)$ no tiene raíces en K . ¿Es $x^2 - 4x + 2$ irreducible en $\mathbb{Q}[x]$? ¿Es irreducible en $\mathbb{R}[x]$? ¿Son $x^3 + x + 1$ y $x^3 + x^2 + x + 1$ irreducibles en $\mathbb{Q}[x]$?

1.69 Sean $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$, $r = a/b \in \mathbb{Q}$, con $a, b \in \mathbb{Z}$ y $\text{mcd}(a, b) = 1$. Demuestre que si r es raíz de $f(x)$ entonces $b \mid a_n$ y $a \mid a_0$. (Este resultado permite sistematizar la búsqueda de raíces racionales de $f(x) \in \mathbb{Q}[x]$.)

1.70 (Algoritmo euclídeo para el mcd.) Sean K un campo numérico, $f(x), g(x) \in K[x]$, con $g(x) \neq 0$ y $\text{grad}(g(x)) \leq \text{grad}(f(x))$. Escribase $r_0(x) = f(x)$, $r_1(x) = g(x)$, y supóngase que

$$r_k(x) = q_{k+1}(x)r_{k+1}(x) + r_{k+2}(x), \quad 0 \leq k \leq n-1, \quad n \geq 1,$$

donde $\text{grad}(r_{k+2}(x)) < \text{grad}(r_{k+1}(x))$, $0 \leq k \leq n-1$, y $r_{n+1}(x) = 0$ (división consecutiva de residuos hasta obtener un residuo nulo, comenzando con $r_0(x) = f(x)$, $r_1(x) = g(x)$). Demuestre que

$$r_n(x) = \text{mcd}(r_0(x), r_1(x)) = \text{mcd}(f(x), g(x)).$$

(Indicación. Demuestre que $r_n(x) \mid f(x)$, $r_n(x) \mid g(x)$, y que si $r(x) \mid f(x)$, $r(x) \mid g(x)$ entonces $r(x) \mid r_n(x)$). En los casos $n = 1, 2, 3$, encuentre, mediante el algoritmo mismo, $m(x)$ y $n(x)$ tales que (1.137) sea válida.

1.71 Sea K un campo numérico. Determine el mcd en $K[x]$ de las siguientes parejas de polinomios:

a) $3x^3 + 13x^2 + 15x + 9, x^3 + 4x^2 + 45x + 3$. (Resp. $x + 3$).

b) $x^6 + x^5 + x^4 + 2x^2 + 3x + 1, x^3 + x^2 + x + 1$. (Resp. 1)

c) $x^3 - 6x + 7, x + 4$. (Resp. 1)

d) $2x^7 - 4x^5 - 2, x^2 - 2$. (Resp. $x + 1$)

e) $x^7 - x^4 + x^3 - 1, x^3 - 1$. (Resp. $x^3 - 1$)

1.72 Sean $a, b \in \mathbb{Z}$, $d = \text{mcd}(a, b)$, $m, n \in \mathbb{Z}$, $m, n \geq 0$. Demuestre que $d^k = \text{mcd}(a^m, b^n)$, $k = \min(m, n)$. Concluya que $d = \text{mcd}(a, b^n) = \text{mcd}(a^m, b)$. Extienda los anteriores resultados al caso de $d(x) = \text{mcd}(f(x), g(x))$, donde $f(x), g(x) \in K[x]$ y K es un campo.

1.73 Se dice que una expresión decimal de $a \in [0, 1]$ es periódica si es de la forma $0.a_1a_2\dots\overline{b_1b_2\dots b_m}$, donde la barra sobre $b_1b_2\dots b_m$ significa que esta sucesión de dígitos ($0 \leq b_i \leq 9$), denominada el periodo de la expresión, se repite indefinidamente. Así, $1/3 = 0.\overline{3}$, $2/15 = 0,1\overline{3}$, etc. Demuestre que si $a \in [0, 1]$ admite una expresión decimal periódica entonces a es racional. (Indicación. Si $a = 0.a_1a_2\dots\overline{b_1b_2\dots b_m}$, demuestre que $10^n(10^m - 1)a$ es un entero.). Verifique, por ejemplo, que si $a = 0,4\overline{91}$ entonces $a = 487/990$, y que $1 = 0.\overline{9}$. Obsérvese que $0.a_1a_2\dots a_n\overline{9}$ ha sido excluido de los desarrollos decimales. Así, $0.\overline{9}$ no es el desarrollo decimal de 1: su desarrollo es $1 = 1.\overline{0}$.

*1.74 Demuestre que si $a \in [0, 1]$ es racional, su desarrollo decimal es periódico.

1.75 Demuestre que

a) $0.\overline{a} \times 0.\overline{b} = 0.a \times 0.\overline{b}$.

b) $\frac{0.\overline{a}}{0.\overline{b}} = \frac{a}{b}$, $b \neq 0$.

c) $\frac{0.\overline{a}}{a} = 0.\overline{1}$, $a \neq 0$.

d) $\frac{0.\overline{a0}}{0.\overline{b0}} = \frac{a}{b}$, $b \neq 0$.

1.76 Demuestre que si X es un conjunto finito con n elementos (sección 1.11) el número de subconjuntos de X con k elementos, $0 \leq k \leq n$, es $\binom{n}{k}$. Concluya que $\wp(X)$ tiene 2^n elementos, y que 2^n es también el cardinal del conjunto de todas las aplicaciones $f: X \rightarrow \{0, 1\}$.

1.77 Demuestre que si X es un conjunto con n elementos (sección 1.11), el cardinal del conjunto $\mathcal{F}_0(X)$ de todas las aplicaciones biyectivas de X en sí mismo es $n!$.

1.78 (Fracciones Parciales) Sean $f_1(x), \dots, f_n(x)$, $n \geq 2$, polinomios no nulos sobre un campo K , tales que $\text{mcd}(f_i(x), f_j(x)) = 1$ si $i \neq j$, y sean $f(x) = f_1(x) \cdots f_n(x)$ y $g(x) \in K[x]$ con $\text{grad}(g(x)) < \text{grad}(f(x))$. Demuestre que existen $m_i(x) \in K[x]$ con $\text{grad}(m_i(x)) < \text{grad}(f_i(x))$, $i = 1, \dots, n$, tales que

$$\frac{g(x)}{f(x)} = \frac{m_1(x)}{f_1(x)} + \cdots + \frac{m_n(x)}{f_n(x)}.$$

(Indicación. Para cada $i \leq k \leq n$, sea $\hat{f}_k(x) = f(x)/f_k(x)$. Demuestre entonces que $1 = \text{mcd}(\hat{f}_1(x), \dots, \hat{f}_n(x))$, y use una relación de Bezout (1.147) para mcd . Multiplique luego por $g(x)/f(x)$ y recorra finalmente al algoritmo de la división en cada término.) Demuestre también que si $f(x) = (p(x))^n$, $n \geq 1$, $p(x) \in K[x]$, $p(x) \neq 0$ y $g(x) \in K[x]$ con $\text{grad}(g(x)) < \text{grad}(f(x))$, entonces

$$\frac{g(x)}{f(x)} = \frac{m_1(x)}{p(x)} + \frac{m_2(x)}{(p(x))^2} + \cdots + \frac{m_n(x)}{(p(x))^n}, \quad k = 1, 2, \dots, n.$$

1.79 (Fracciones parciales monógenas). Sean K un campo y

$$f(x) = (x - a_1)^{n_1} \cdots (x - a_m)^{n_m},$$

donde $a_k \in K$, $a_k \neq a_j$ si $k \neq j$, $n_k \geq 1$, $k = 1, 2, \dots, m$. Demuestre que si $g(x) \in K[x]$ y $\text{grad}(g(x)) < \text{grad}(f(x))$, entonces

$$\frac{g(x)}{f(x)} = \sum_{k=1}^m \frac{m_k(x)}{(x - a_k)^{n_k}}, \quad m_k(x) \in K[x], \quad \text{grad}(m_k(x)) < n_k.$$

Demuestre además que para $k = 1, 2, \dots, m$,

$$\frac{m_k(x)}{(x - a_k)^{n_k}} = \sum_{i=1}^{n_k} \frac{b_{ki}}{(x - a_k)^i}, \quad b_{ki} \in K, \quad i = 1, 2, \dots, n_k.$$

1.80 (Gauss). Sean $f(x), g(x) \in \mathbb{Z}[x]$ polinomios primitivos (es decir $c(f(x)) = c(g(x)) = 1$). Demuestre que $h(x) = f(x)g(x)$ también es primitivo. (Indicación. Supóngase que $f(x) = a_0 + \cdots + a_n x^n$,

$g(x) = b_0 + \cdots + b_m x^m$, con $a_n b_m \neq 0$. Por hipótesis, $\text{mcd}(a_0, \dots, a_n) = \text{mcd}(b_0, \dots, b_m) = 1$. Supóngase además que $a = c(h(x))$, y que p es un primo tal que $p \mid a$. Evidentemente p no divide a todos los a_i ni a todos los b_j . Sean $k = \min\{i : p \nmid a_i\}$, $h = \min\{j : p \nmid b_j\}$, $l = k + h$. Demuestre que si c_l es el coeficiente de x^l en $h(x)$ entonces $p \nmid c_l$, observando, con $a_{k+i} = 0$ si $k + i > m$, $b_{h+i} = 0$ si $h + i > n$, que

$$c_l - a_k b_h = \sum_{i=1}^h a_{k+i} b_{h-i} + \sum_{i=1}^k a_{k-i} b_{h+i},$$

y que si $p \mid c_l$, p dividiría el miembro de la derecha pero no el de la izquierda de la anterior igualdad.

1.81 Verifique en detalle que $\mathbb{Z}[x]$ es un dominio factorial (nota 1.56). Demuestre también la afirmación de la nota 1.57.

1.82 Sean $R = (X, G, X)$ una relación de equivalencia, $\varphi : X \rightarrow X/R$ la aplicación cociente. Si $Y \subseteq X$ es tal que $\varphi : Y \rightarrow X/R$ es biyectiva, se dice que Y es un sistema de representantes de R .

a) Demuestre que Y es un sistema de representantes de R si y sólo si Y tiene un único elemento en común con cada clase de equivalencia módulo R .

b) Demuestre que el axioma (A.E.), sección 1.11, es equivalente a la afirmación: Toda relación de equivalencia (X, G, X) tiene un sistema de representantes. (Indicación. Si $I \neq \emptyset$, $A_i \neq \emptyset$ para todo $i \in I$ y $A_i \cap A_j = \emptyset$ para $i \neq j$, entonces $G = \bigcup_{i \in I} (A_i \times A_i)$ es la gráfica de una relación de equivalencia sobre $X = \bigcup_{i \in I} A_i$.)

1.83 Sea $(A_i)_{i \in I}$ una familia de conjuntos. El conjunto de todas las aplicaciones $f : I \rightarrow \bigcup_{i \in I} A_i$ tales que $f(i) \in A_i$ para todo $i \in I$ (funciones de elección) se denota con $\prod_{i \in I} A_i$, y se denomina el producto cartesiano generalizado de $(A_i)_{i \in I}$. Demuestre que si $I = \emptyset$ entonces $\bigcup_{i \in I} A_i = \emptyset$ y $\prod_{i \in I} A_i = \{(\emptyset, \emptyset, \emptyset)\}$, mientras que si $I \neq \emptyset$ y $A_i = \emptyset$ para algún $i \in I$ entonces $\prod_{i \in I} A_i = \emptyset$. Demuestre también que si $I \neq \emptyset$ y $A_i \neq \emptyset$ para todo $i \in I$, el axioma (A.E.) es equivalente a afirmar que $\prod_{i \in I} A_i \neq \emptyset$.

1.84 Sean $X_1, \dots, X_n$, $n \geq 2$, conjuntos, $X = \bigcup_{i=1}^n X_i$. Demuestre que $X_1 \times \cdots \times X_n \neq \emptyset$ si y sólo si $X_i \neq \emptyset$, $i = 1, 2, \dots, n$. Demuestre en

este caso, sin recurrir al axioma (A.E.), que existe una aplicación $f : I \longrightarrow X$, $I = \{1, 2, \dots, n\}$, tal que $f(i) \in X_i$, $i = 1, 2, \dots, n$. (Indicación. Demuestre que existe una aplicación biyectiva

$$\psi : \prod_{i \in I} X_i \longrightarrow X_1 \times \dots \times X_n,$$

donde $\prod_{i \in I} X_i$ es el conjunto de las funciones de elección de I en X .)

- 1.85 Sea $(A_i)_{i \in I}$ una familia de subconjuntos no vacíos de $\mathbb{N}$ con $I \neq \emptyset$. Demuestre sin usar el axioma (A.E.) que existe $f : I \longrightarrow \bigcup_{i \in I} A_i$ tal que $f(i) \in A_i$ para todo $i \in I$. Si $\emptyset \neq A_i \subseteq \mathbb{Z}$ para todo $i \in I$, e $I \neq \emptyset$ ¿es posible demostrar, sin usar el axioma (A.E.), que existe $f : I \longrightarrow \bigcup_{i \in I} A_i$ tal que $f(i) \in A_i$ para todo $i \in I$?
- 1.86 Demuestre que si $X \subseteq Y$ entonces $\text{Card}(X) \leq \text{Card}(Y)$, y que si Y es finito entonces $X = Y$ si y sólo si $\text{Card}(X) = \text{Card}(Y)$. ¿Es esto último cierto si X o Y es infinito?
- 1.87 Demuestre que $\text{Card}(X) \leq \text{Card}(\wp(X))$ y que si X es finito entonces $\text{Card}(X) < \text{Card}(\wp(X))$.
- 1.88 Demuestre que X es finito si y sólo si $\text{Card}(X) < \aleph_0$.
- 1.89 Demuestre que si X o Y es finito, $\text{Card}(X) = \text{Card}(Y)$ si y sólo si existe $f : X \longrightarrow Y$, biyectiva.
- 1.90 Se dice que $a \in \mathbb{C}$ es un *número algebraico*, si existe $f(x) \in \mathbb{Q}[x]$, $f(x) \neq 0$, tal que $f(a) = 0$. De igual manera, $a \in \mathbb{R}$ es un *algebraico*, si existe $f(x) \in \mathbb{Z}[x]$, $f(x) \neq 0$, tal que $f(a) = 0$. Sea $\text{Alg}(\mathbb{Q})$ el conjunto de los números algebraicos complejos. Demuestre que $\text{Alg}(\mathbb{Q})$ es enumerable. (Indicación. Use los teoremas 1.27 y 1.39)

Parte II

Teoría elemental de los grupos

Capítulo 2

Grupos

Dado un conjunto G , una aplicación

$$\begin{aligned}(\cdot) : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \cdot b\end{aligned}$$

se denomina una *ley de composición interna sobre G* . *Interna* se refiere al hecho de que dados $a, b \in G$, $a \cdot b$ es también un elemento de G . Otras notaciones usadas frecuentemente para $(\cdot)$ son: $(\circ)$, $(*)$, $(+)$. Se escribe entonces, respectivamente, $a \circ b$, $a * b$, $a + b$, en lugar de $a \cdot b$. La notación $(\cdot)$ se conoce como la *notación multiplicativa*. A su vez, $(+)$ es la *notación aditiva*. La notación multiplicativa $(\cdot)$ es la preferida para el desarrollo de la teoría general, aunque $(\circ)$ y $(*)$ son también comunes. La notación aditiva $(+)$ se reserva generalmente para casos especiales. Cuando se usa la notación multiplicativa, es corriente escribir simplemente ab en lugar de $a \cdot b$.

Definición 2.1. Un *grupo* $(G, \cdot)$ es un sistema formado por un conjunto G y una ley de composición interna $(\cdot)$ sobre G tal que

- (i) $(ab)c = a(bc)$, cualesquiera que sean a, b, c en G .
- (ii) Existe $e \in G$ tal que $ae = ea = a$ para todo $a \in G$.
- (iii) Para todo $a \in G$ existe $a' \in G$ tal que $aa' = a'a = e$.

Si $(G, \cdot)$ es un grupo entonces $G \neq \emptyset$, pues $e \in G$. La propiedad (i) de la definición anterior se conoce como la *propiedad asociativa* o la *asociatividad* de $(\cdot)$. La (ii), como la *propiedad modulativa* de $(\cdot)$, y la (iii), como la

propiedad invertiva de $(\cdot)$ con respecto a e . Como es claro, un grupo $(G, \cdot)$ tiene la siguiente propiedad:

(iv) *Cualesquiera que sean $a, b \in G$, también $ab \in G$.*

La propiedad (iv) se conoce como la *propiedad clausurativa* de $(\cdot)$.

Si un grupo $(G, \cdot)$ satisface la propiedad

(v) *Cualesquiera que sean $a, b \in G$, $ab = ba$,*

se dice que $(G, \cdot)$ es un *grupo conmutativo* o un *grupo abeliano*. La propiedad (v) se conoce como la *propiedad conmutativa* o la *conmutatividad* de $(\cdot)$.

Muchos grupos importantes son conmutativos; otros, igualmente importantes, no lo son.

Antes de dar ejemplos de grupos, estableceremos algunas propiedades de los mismos que se deducen fácilmente de la definición.

Teorema 2.1. *En un grupo $(G, \cdot)$ existe un único $e \in G$ que satisface la propiedad (ii) de la definición 2.1.*

Demostración. Supóngase que $e' \in G$ es también tal que $ae' = e'a = a$ para todo $a \in G$. Entonces, $e' = ee' = e$. $\square$

Definición 2.2. Se dice que e es el *elemento neutro* de $(G, \cdot)$.

Teorema 2.2. *Si $(G, \cdot)$ es un grupo y $a, b \in G$ son tales que $ac = bc$ para algún $c \in G$, entonces $a = b$.*

Demostración. Si $c' \in G$ es tal que $cc' = e$ entonces $(ac)c' = (bc)c'$, de lo cual $a(cc') = b(cc')$, así que $a = ae = be = b$. $\square$

La propiedad establecida en el teorema 2.2 se conoce como la *propiedad cancelativa a derecha* de $(\cdot)$. Análogamente se tiene que:

Si $a, b \in G$ y existe $c \in G$ tal que $ca = cb$, entonces $a = b$. Esta se conoce como la *propiedad cancelativa a izquierda* de $(\cdot)$. La demostración es análoga a la del teorema 2.2, tomando $c' \in G$ tal que $c'c = e$.

Corolario 2.1. *Si $(G, \cdot)$ es un grupo y $e' \in G$ es tal que $e'a = a$ para algún $a \in G$, entonces $e' = e$, el elemento neutro de G .*

Demostración. En efecto, $e'a = ea$, y basta aplicar el teorema 2.2. $\square$

De manera análoga, si $ae' = a$ para algún $a \in G$, necesariamente $e' = e$.

Corolario 2.2. *Si $(G, \cdot)$ es un grupo y $a \in G$, existe un y sólo un $a' \in G$ tal que $aa' = e$.*

Demostración. La existencia de a' resulta de (iii). La unicidad, del teorema 2.2. $\square$

Análogamente, existe un único $a' \in G$, tal que $a'a = e$. En total, existe un y sólo un a' en G tal que $aa' = a'a = e$.

Definición 2.3. Si $(G, \cdot)$ es un grupo y $a \in G$, el único $a' \in G$ tal que $a'a = aa' = e$ se denomina el *inverso* de a y se denota con a^{-1} .

Corolario 2.3. *Si $a \in G$, para que $a' = a^{-1}$ es necesario y suficiente que $aa' = e$ o que $a'a = e$.*

Teorema 2.3. *Si $(G, \cdot)$ es un grupo y $a, b \in G$, la ecuación $ax = b$ tiene la única solución $x = a^{-1}b$.*

Demostración. Como $a(a^{-1}b) = (aa^{-1})b = eb = b$, es claro que $x = a^{-1}b$ es solución. La unicidad resulta del teorema 2.2. $\square$

De igual manera, $x = ba^{-1}$ es la única solución de $xa = b$.

Corolario 2.4. *Sean $(G, \cdot)$ un grupo, e su elemento neutro, $a, b \in G$. Entonces:*

1. $e^{-1} = e$
2. $(a^{-1})^{-1} = a$
3. $(ab)^{-1} = b^{-1}a^{-1}$.

Demostración. (1) En efecto, e^{-1} y e resuelven la ecuación $ex = e$. (2) Tanto a como $(a^{-1})^{-1}$ resuelven $a^{-1}x = e$. (3) Ambos, $(ab)^{-1}$ y $b^{-1}a^{-1}$, resuelven $(ab)x = e$. $\square$

Nota 2.1. En general, $(ab)^{-1} \neq a^{-1}b^{-1}$. Véase el ejemplo 2,11.

Nota 2.2. En un grupo abeliano $(G, \cdot)$ notado multiplicativamente, es usual denotar con 1 (uno) el elemento neutro e de G . A su vez, es corriente denotar con $\frac{b}{a}$ ó b/a la solución única de $ax = b$, que es la misma de $xa = b$. En particular, $a^{-1} = \frac{1}{a} = 1/a$. La notación b/a puede ser causa de confusión si se usa en el caso no conmutativo.

Nota 2.3. Si $(G, +)$ es un grupo abeliano notado aditivamente, es costumbre denotar con 0 (cero) el elemento neutro de G y con $-a$ el inverso de a con respecto a 0. Nótese que entonces $-0 = 0$, $-(-a) = a$ y $-(a+b) = (-a) + (-b)$. A su vez, $x = b - a$ denotará la solución única de $a+x = b$, que es la misma de $x+a = b$. Nótese que $b-a = b+(-a) = (-a)+b$ y que $0-a = -a$.

Ejemplo 2.1. Si X es un conjunto no vacío, denotaremos con $\mathcal{F}_0(X)$ el conjunto de todas las aplicaciones biyectivas de X en sí mismo. Entonces $(\mathcal{F}_0(X), \circ)$, donde $(\circ)$ es la ley de composición de funciones, $(f \circ g)(x) = f(g(x))$, $x \in X$, es un grupo, en el cual la aplicación idéntica I de X , $I(x) = x$ para todo $x \in X$, es el elemento neutro, y en el cual f^{-1} , la aplicación inversa de f ($f^{-1}(x) = y$ si y sólo si $f(y) = x$) es el inverso de f . Si X se reduce a un único elemento a ($X = \{a\}$), $\mathcal{F}_0(X) = \{I\}$, donde I es la aplicación $I(a) = a$. Si X es un conjunto con n elementos, $\mathcal{F}_0(X)$ tiene $n!$ elementos (ejercicio 1.77).

Ejemplo 2.2. Si $X = \{1, 2, \dots, n\}$, $n \geq 1$, y $f \in \mathcal{F}_0(X)$, es costumbre escribir

$$f =: \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix},$$

o, si $f(k) = m_k$, $k = 1, 2, \dots, n$,

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ m_1 & m_2 & \dots & m_n \end{pmatrix}.$$

Nótese que $1 \leq m_k \leq n$, $k = 1, 2, \dots, n$.

Es también corriente, en este caso, considerar como ley de composición en $\mathcal{F}_0(X)$ la ley

$$f \cdot g := g \circ f \quad (2.1)$$

en lugar de la $g \circ f$. Como es natural, escribiremos $fg = f \cdot g$. El producto $(\cdot)$ hace más cómodo el cálculo de $g \circ f(k)$, como lo muestra el siguiente diagrama:

$$fg = \begin{pmatrix} 1 & \dots & k & \dots & n \\ f(1) & \dots & f(k) & \dots & f(n) \end{pmatrix} \begin{pmatrix} 1 & \dots & f(k) & \dots & n \\ g(1) & \dots & g(f(k)) & \dots & g(n) \end{pmatrix}$$

Así,

$$\begin{pmatrix} 1 & 2 & 3 \\ \downarrow & & \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & & \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & & \\ 3 & & \end{pmatrix}.$$

Es usual escribir $S_n = \mathcal{F}_0(\{1, 2, \dots, n\})$ y denominar a $(S_n, \cdot)$ el grupo simétrico de n objetos.

Ejemplo 2.3. Los siguientes son grupos abelianos aditivos (véase capítulo 1):

1. $(\mathbb{C}, +)$: el grupo aditivo de los números complejos,
2. $(\mathbb{R}, +)$: el grupo aditivo de los números reales,
3. $(\mathbb{Q}, +)$: el grupo aditivo de los números racionales,
4. $(\mathbb{Z}, +)$: el grupo aditivo de los números enteros.
5. Si $(S, +, \cdot)$ es un dominio (capítulo 1, sección 1.9.), $(S, +)$ es un grupo aditivo.

En todos ellos, 0 es el elemento neutro y $-a$ es el inverso de a .

Ejemplo 2.4. Los siguientes son grupos abelianos multiplicativos:

1. $(\mathbb{C}^*, \cdot)$: el grupo multiplicativo de los números complejos no nulos,
2. $(\mathbb{R}^*, \cdot)$: el grupo multiplicativo de los números reales no nulos,
3. $(\mathbb{Q}^*, \cdot)$: el grupo multiplicativo de los números racionales no nulos.
4. Si $(K, +, \cdot)$ es un campo numérico (capítulo 1, sección 1.9), $(K^*, \cdot)$ es un grupo multiplicativo.

En el ejemplo 2.4, si $G = \mathbb{C}, \mathbb{R}, \mathbb{Q}, K$, $G^* = G \setminus \{0\}$, para cada uno de estos grupos, 1 es el elemento neutro y $a^{-1} = 1/a$ es el inverso de a .

Ejemplo 2.5. Si $K = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, entonces $M_{m \times n}(K)$, el conjunto de las matrices de orden $m \times n$ sobre K es, con la adición usual de matrices, un grupo abeliano aditivo.

Ejemplo 2.6. Si $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, entonces $GL_n(K)$, el conjunto de las matrices cuadradas de orden $n \times n$ sobre K con determinante no nulo (matrices no singulares), es, con la multiplicación usual de matrices, un grupo multiplicativo. Esto resulta de observar que si $A \in GL_n(K)$ y $A^{-1} := (\text{Det}(A))^{-1} \text{Adj}(A)$, donde $\text{Adj}(A) = [a_{ij}]$ con $a_{ij} = (-1)^{i+j} \text{Det}(A_{ji})$, siendo A_{ji} la matriz obtenida de A suprimiendo la j -ésima fila y la i -ésima columna, entonces $A^{-1}A = AA^{-1} = I$ (la matriz $\text{Adj}(A)$ se conoce como la *matriz adjunta de A*), y además

$$\text{Det}(I) = 1, \text{Det}(AB) = \text{Det}(A) \text{Det}(B), \quad (2.2)$$

donde I es la matriz identidad de orden $n \times n$ y $\text{Det}(A)$ denota el determinante de la matriz A . Nótese que entonces $\text{Det}(A^{-1}) = (\text{Det}(A))^{-1}$. Que tal grupo no es abeliano si $n \geq 2$, se establece en el ejemplo 2.11.

Definición 2.4. Si $(G, \cdot)$ es un grupo con elemento neutro e , $a \in G$ y $m \in \mathbb{N}$, definimos

$$a^m = \begin{cases} e, & \text{si } m = 0, \\ a^n a, & \text{si } m = n + 1, \quad n \in \mathbb{N}. \end{cases} \quad (2.3)$$

Nótese que $a^1 = a$, y un argumento inductivo demuestra fácilmente que $e^m = e$ para todo $m \in \mathbb{N}$. A su vez, $a^{m+1} = a^m a$ para todo $m \in \mathbb{N}$. Por otra parte, $a^{m+1} = aa^m$. En efecto, esto es claro si $m = 0$; y si lo suponemos para m entonces $aa^{m+1} = (aa^m)a = a^{m+1}a = a^{(m+1)+1}$, de lo cual es también válido para $m + 1$ y, por lo tanto, para todo $m \in \mathbb{N}$.

Teorema 2.4. Si $(G, \cdot)$ es un grupo, $a \in G$ y $m, n \in \mathbb{N}$, entonces

$$a^{m+n} = a^m a^n. \quad (2.4)$$

Demostración. Haremos inducción sobre n (manteniendo m fijo, pero arbitrario). La afirmación es clara si $n = 0$. Y si la suponemos para un cierto n entonces $a^{m+(n+1)} = a^{(m+n)+1} = a^{m+n} a = (a^m a^n) a = a^m (a^n a) = a^m a^{n+1}$, de lo cual vale también para $n + 1$ y, así, para todo $n \in \mathbb{N}$. $\square$

Nota 2.4. Como es claro, $a^{m+n} = a^n a^m$, así que, $a^m a^n = a^n a^m$ cualesquiera que sean $a \in G$ y $m, n \in \mathbb{N}$.

Definición 2.5. Si $(G, \cdot)$ es un grupo, $a \in G$ y $n \in \mathbb{N}$, definimos

$$a^{-n} := (a^{-1})^n \quad (2.5)$$

Teorema 2.5. Si $(G, \cdot)$ es un grupo, $a \in G$ y $n \in \mathbb{N}$, entonces

$$a^{-n} = (a^n)^{-1}. \quad (2.6)$$

Demostración. La afirmación es clara si $n = 0$ o $n = 1$. Supongámosla para n . Entonces, $a^{-(n+1)} = (a^{-1})^{n+1} = (a^{-1})^n a^{-1} = a^{-n} a^{-1} = (a^n)^{-1} a^{-1} = (aa^n)^{-1} = (a^{n+1})^{-1}$. Hemos recurrido al hecho de que $(ab)^{-1} = b^{-1}a^{-1}$ y, también, a que $aa^n = a^{n+1}$. Esto demuestra la afirmación para $n + 1$ y, por lo tanto, para todo $n \in \mathbb{N}$. $\square$

Teorema 2.6. Si $(G, \cdot)$ es un grupo, $a \in G$ y $m, n \in \mathbb{N}$, $m \geq n$, entonces

$$a^{m-n} = a^m a^{-n}. \quad (2.7)$$

Demostración. En efecto, $m - n \in \mathbb{N}$, así que $a^{m-n} a^n = a^{(m-n)+n} = a^m$. Entonces, $a^{m-n} = (a^{m-n} a^n) (a^n)^{-1} = a^m a^{-n}$. $\square$

Nota 2.5. Si $m < n$ en el teorema 2.6, entonces $a^{m-n} = a^{-(n-m)} = (a^{n-m})^{-1} = (a^n a^{-m})^{-1} = (a^{-m})^{-1} a^{-n} = [(a^m)^{-1}]^{-1} a^{-n} = a^m a^{-n}$, lo cual demuestra que (2.7) es aún válida si $m, n \in \mathbb{N}$ y $m < n$.

Teorema 2.7. Si $(G, \cdot)$ es un grupo, $a \in G$ y $m, n \in \mathbb{N}$, entonces

$$a^{-m} a^{-n} = a^{-(m+n)}$$

Demostración. En efecto, $a^{-m} a^{-n} = (a^{-1})^m (a^{-1})^n = (a^{-1})^{m+n} = a^{-(m+n)}$. $\square$

Observamos que mediante (2.3) y (2.5), a^m ha sido definido para todo $m \in \mathbb{Z}$. De hecho,

$$a^m = (a^{-1})^{-m} \quad (2.8)$$

para todo $m \in \mathbb{Z}$. Esto es claro si $m = -n$, $n \in \mathbb{N}$, pues entonces $n = -m$ y $a^m = a^{-n} = (a^{-1})^n = (a^{-1})^{-m}$; y si $m \in \mathbb{N}$, entonces $(a^{-1})^{-m} =$

$\left[(a^{-1})^{-1}\right]^m = a^m$. De los teoremas 2.4, 2.6 y 2.7, y de lo observado en la nota 2.5, se deduce entonces que

Teorema 2.8. Si $(G, \cdot)$ es un grupo, $a \in G$ y $m, n \in \mathbb{Z}$, entonces

$$a^{m+n} = a^m a^n. \quad (2.9)$$

En particular, $a^m a^n = a^n a^m$.

Nota 2.6. Si $(G, \cdot)$ es un grupo y $a, b \in G$ son tales que $ab = ba$, se dice que a y b conmutan. Si a y b conmutan, entonces a y b^n conmutan para todo $n \in \mathbb{N}$, como se verifica fácilmente por inducción (ejercicio 2.11). También a^{-1} y b^{-1} conmutan, pues $b^{-1}a^{-1} = (ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1}$. Finalmente, a y b^{-1} conmutan, pues $(ab^{-1})(b^{-1}a)^{-1} = a(b^{-1}a^{-1})b = a(a^{-1}b^{-1})b = e$. En total, si a y b conmutan entonces $ab^m = b^m a$ para todo $m \in \mathbb{Z}$ (ejercicio 2.11). Como es claro a y a^m conmutan para todo $m \in \mathbb{Z}$. Nótese que e , el elemento neutro de G , conmuta con todo $a \in G$.

Teorema 2.9. Si $(G, \cdot)$ es un grupo, $a, b \in G$ y a y b conmutan, entonces

$$(ab)^m = a^m b^m \quad (2.10)$$

para todo $m \in \mathbb{N}$.

Demostración. La afirmación es clara si $m = 0, 1$. Y si la suponemos para m entonces $(ab)^{m+1} = (ab)^m (ab) = (a^m b^m)(ba) = a^m (b^m b) a = a^m (b^{m+1} a) = (a^m a) b^{m+1} = a^{m+1} b^{m+1}$, pues a y b^{m+1} conmutan (nota 2.6). $\square$

Corolario 2.5. Si $(G, \cdot)$ es un grupo, $a, b \in G$ y a y b conmutan, entonces

$$(ab)^m = a^m b^m \quad (2.11)$$

para todo $m \in \mathbb{Z}$.

Demostración. La afirmación fue demostrada arriba para $m \in \mathbb{N}$. Y si $m = -n$, $n \in \mathbb{N}$, entonces $(ab)^m = (ab)^{-n} = \left[(ab)^{-1}\right]^n = (b^{-1}a^{-1})^n = (a^{-1}b^{-1})^n = (a^{-1})^n (b^{-1})^n = a^{-n} b^{-n} = a^m b^m$, pues a^{-1} y b^{-1} conmutan. $\square$

Nota 2.7. Las relaciones (2.10) y (2.11) pueden ser falsas si a y b no conmutan (en particular, puede ser que $(ab)^{-1} \neq a^{-1}b^{-1}$. ejemplo 2.11).

Definición 2.6. Se dice que un conjunto G dotado de una ley de composición interna $(\cdot)$ es un grupo de derecha si

1. $(ab)c = a(bc)$, cualesquiera que sean $a, b, c \in G$.
2. Existe $e \in G$ tal que $ae = a$ para todo $a \in G$.
3. Para todo $a \in G$ existe $a' \in G$ tal que $aa' = e$.

Todo grupo $(G, \cdot)$ es un grupo de derecha. Si $(G, \cdot)$ es un grupo de derecha, $ab \in G$ cualesquiera que sean $a, b \in G$ (pues $(\cdot)$ es una ley de composición interna). Por otra parte, si $a \in G$ y $a^2 = aa = a$, necesariamente $a = e$, pues si $a' \in G$ es tal que $aa' = e$ entonces $a^2 a' = a(aa') = ae = a$, y también $a^2 a' = aa' = e$.

Teorema 2.10. Todo grupo de derecha es, de hecho, un grupo.

Demostración. Si $(G, \cdot)$ es un grupo de derecha y $a, a' \in G$ son tales que $aa' = e$, entonces $(a'a)^2 = a'aa'a = (a'e)a = a'a$, así que también $a'a = e$. Por otra parte, $ea = (aa')a = a(a'a) = ae = a$, lo cual completa la demostración. $\square$

Mediante (1), (2) y (3) de la Definición 2.6, pero cambiando $ae = a$ por $ea = a$ en (2) y $aa' = e$ por $a'a = e$ en (3), se define un grupo de izquierda. Como es claro, un grupo es un grupo de izquierda, y demostrando que en un grupo de izquierda la condición $a^2 = a$ también implica que $a = e$, se demuestra que todo grupo de izquierda es, de hecho, un grupo. Curiosamente, se concluye así que los grupos de izquierda y derecha son los mismos.

Nota 2.8. Por el contrario, pueden existir sistemas $(G, \cdot)$ en los cuales $(\cdot)$ es una ley de composición interna asociativa sobre G tal que

1. existe $e \in G$ tal que $ae = a$ para todo $a \in G$,
2. para todo $a \in G$ existe $a' \in G$ tal que $a'a = e$,

y los cuales no son, sin embargo, grupos. Véase el ejercicio 2.9.

Teorema 2.11. Sea $(G, \cdot)$ un sistema formado por un conjunto G y una ley de composición interna $(\cdot)$ sobre G tal que

1. $(ab)c = a(bc)$ cualesquiera que sean $a, b \in G$.
2. En G son válidas las leyes cancelativas a derecha e izquierda.

Entonces, si G es finito y no vacío, $(G, \cdot)$ es un grupo.

Demostración. Como $G \neq \emptyset$, existe $a \in G$. Sea $f_a : G \rightarrow G$ la aplicación $f_a(x) = ax$. Por (2), f_a es inyectiva y, como G es finito, también sobreyectiva (capítulo 1, sección 1.11). Existirá entonces $e_a \in G$ tal que $f_a(e_a) = ae_a = a$ y, como $a(e_ab) = (ae_a)b = ab$, nuevamente (2) implica que $e_ab = b$ cualquiera que sea $b \in G$. Pero, como $g_b : G \rightarrow G$ dada por $g_b(x) = xb$ es también sobreyectiva, para todo $b \in G$ existirá $b' \in G$ tal que $g_b(b') = b'b = e_a$, lo cual demuestra que $(G, \cdot)$ es un grupo de izquierda con elemento neutro $e_a \in G$. Entonces, G es un grupo. $\square$

Nota 2.9. En un grupo G , finito o infinito, las condiciones (1) y (2) del teorema 2.11 se verifican. Sin embargo, puede ser que para $(G, \cdot)$, con G infinito, tales condiciones se verifiquen, sin que $(G, \cdot)$ sea un grupo. Tal es el caso de los sistemas $(\mathbb{N}, +)$ y $(\mathbb{N}^*, \cdot)$, donde $\mathbb{N}$ es el conjunto de los números naturales, $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ y $(+)$ y $(\cdot)$ son la adición y la multiplicación usuales. Aconsejamos al lector verificar las condiciones (1) y (2) del teorema 2.11 para estos sistemas.

Definición 2.7. Si $G = \{a_1, a_2, \dots, a_n\}$ y $(\cdot)$ es una ley de composición interna sobre G (así que, dados $1 \leq i, j \leq n$, existe $1 \leq k \leq n$ tal que $a_i \cdot a_j = a_k$), la matriz $[a_{ij}]_{n \times n}$, donde $a_{ij} = a_i a_j$, se denomina la *tabla de multiplicación* de $(G, \cdot)$.

Si $G = \{a_1, a_2, \dots, a_n\}$ es un grupo y convenimos en que $a_1 = e$ es el elemento neutro, entonces $a_{1j} = a_1 a_j = a_j$ y $a_{i1} = a_i a_1 = a_i$, $i, j = 1, 2, \dots, n$; es decir, tanto la primera fila como la primera columna de $[a_{ij}]_{n \times n}$ es $(a_1, a_2, \dots, a_n)$. De hecho, cualquier fila de $[a_{ij}]_{n \times n}$ contiene todos los elementos $a_1, a_2, \dots, a_n$ en algún orden. Esto es consecuencia del hecho de que para cada i , fijo, la ecuación $a_i x = a_j$, $j = 1, 2, \dots, n$, siempre tiene solución. Como lo mismo es cierto de la ecuación $x a_j = a_i$, toda columna de $[a_{ij}]_{n \times n}$ contiene también todos los elementos $a_1, a_2, \dots, a_n$ en algún orden. Es decir, si $[a_{ij}]_{n \times n}$ es la tabla de multiplicación de un grupo finito, toda fila y toda columna de $[a_{ij}]_{n \times n}$ contiene todos los elementos de G , y es fácil ver que si una tabla de multiplicación asociativa satisface tal propiedad, ésta es necesariamente la tabla de multiplicación de un grupo (pues las condiciones (1) y (2) del teorema 2.11 deberán satisfacerse, ya que las aplicaciones inyectivas y sobreyectivas de un grupo finito en sí mismo coinciden: capítulo 1, sección 1.11). Las tablas de multiplicación de grupos con n elementos deben entonces buscarse entre las matrices $[a_{ij}]_{n \times n}$ que contienen exactamente los

mismos elementos $a_1, a_2, \dots, a_n$ en cada fila y cada columna (en algún orden). La asociatividad, sin embargo, no se puede deducir fácilmente de la tabla.

Así, para un conjunto con un único elemento e , la única tabla posible es $[e]$, que es la tabla de un grupo. Para uno con dos elementos, $G = \{e, a\}$, la única tabla posible es

$$A = \begin{bmatrix} e & a \\ a & e \end{bmatrix}, \quad (2.12)$$

y es la tabla de un grupo (pues es obviamente asociativa). Para un conjunto con tres elementos, $G = \{e, a, b\}$, es también claro que una sola tabla es posible:

$$A = \begin{bmatrix} e & a & b \\ a & b & e \\ b & e & a \end{bmatrix}, \quad (2.13)$$

la cual es efectivamente la tabla de un grupo. Nótese que la alternativa

$$A' = \begin{bmatrix} e & a & b \\ a & e & \\ b & & \end{bmatrix}, \quad (2.14)$$

es inconducente: necesariamente sería $a_{23} = b$, que es absurdo.

Para cuatro elementos, $G = \{e, a, b, c\}$, las alternativas para la segunda fila son

$$A_1 = \begin{bmatrix} e & a & b & c \\ a & e & c & b \\ b & & & \\ c & & & \end{bmatrix}, A_2 = \begin{bmatrix} e & a & b & c \\ a & c & e & b \\ b & & & \\ c & & & \end{bmatrix}, A_3 = \begin{bmatrix} e & a & b & c \\ a & b & c & e \\ b & & & \\ c & & & \end{bmatrix} \quad (2.15)$$

que, de hecho, determinan completamente sus segundas columnas, en la forma

$$A_1 = \begin{bmatrix} e & a & b & c \\ a & e & c & b \\ b & c & & \\ c & b & & \end{bmatrix}, A_2 = \begin{bmatrix} e & a & b & c \\ a & c & e & b \\ b & e & & \\ c & b & & \end{bmatrix}, A_3 = \begin{bmatrix} e & a & b & c \\ a & b & c & e \\ b & c & & \\ c & e & & \end{bmatrix}. \quad (2.16)$$

Para la tercera fila de A_1 existe la alternativa

$$A_{1,1} = \begin{bmatrix} e & a & b & c \\ a & e & c & b \\ b & c & e & a \\ c & b & & \end{bmatrix}, A_{1,2} = \begin{bmatrix} e & a & b & c \\ a & e & c & b \\ b & c & a & e \\ c & b & & \end{bmatrix}, \quad (2.17)$$

que conduce a las posibles tablas

$$A_{1,1} = \begin{bmatrix} e & a & b & c \\ a & e & c & b \\ b & c & e & a \\ c & b & a & e \end{bmatrix}, \quad A_{1,2} = \begin{bmatrix} e & a & b & c \\ a & e & c & b \\ b & c & a & e \\ c & b & e & a \end{bmatrix}. \quad (2.18)$$

Para la matriz A_2 sólo es posible una tercera fila:

$$A_2 = \begin{bmatrix} e & a & b & c \\ a & c & e & b \\ b & e & c & a \\ c & b & & \end{bmatrix}. \quad (2.19)$$

Esto conduce a la otra posible tabla

$$A_2 = \begin{bmatrix} e & a & b & c \\ a & c & e & b \\ b & e & c & a \\ c & b & a & e \end{bmatrix}. \quad (2.20)$$

Finalmente, para A_3 sólo es posible una tercera fila,

$$A_3 = \begin{bmatrix} e & a & b & c \\ a & b & c & e \\ b & c & e & a \\ c & e & & \end{bmatrix},$$

la cual conduce a la tabla:

$$A_3 = \begin{bmatrix} e & a & b & c \\ a & b & c & e \\ b & c & e & a \\ c & e & a & b \end{bmatrix}. \quad (2.21)$$

Las tablas $A_{1,1}$, $A_{1,2}$, A_2 y A_3 son, de hecho, tablas de grupos, y las únicas posibles.

Para $n \geq 5$, el anterior trabajo es engorroso (al menos sin la ayuda de implementos de cálculo rápido), y es frecuentemente más conveniente recurrir a otros procedimientos para establecer las posibles tablas (entre ellos, el de desarrollar un poco más la teoría de los grupos). Véase, al respecto, el ejemplo 3.4.

Nota 2.10. La tabla de multiplicación de un grupo abeliano finito G es una matriz simétrica, es decir $a_{ij} = a_{ji}$ cualesquiera que sean i, j . Recíprocamente, si la tabla de multiplicación de un grupo finito es simétrica, este grupo es abeliano. Para un grupo conmutativo G , el teorema 2.9 y su corolario son automáticamente válidos. Obsérvese que de lo dicho anteriormente para las tablas de multiplicación se deduce que todo grupo con 1, 2, 3 o 4 elementos es conmutativo.

Nota 2.11. Como lo hemos mencionado, la notación aditiva (+) para la operación de un grupo se usa exclusivamente cuando éste es conmutativo. En tal caso el elemento neutro de G se denota con 0 y el inverso de $a \in G$ con $(-a)$. Es usual también escribir ma en lugar de a^m , $a \in G$, $m \in \mathbb{Z}$, y las relaciones $a^{m+n} = a^m a^n$, $(ab)^m = a^m b^m$, $a, b \in G$, $m, n \in \mathbb{Z}$, toman entonces la forma $(m+n)a = ma + na$, $m(a+b) = ma + mb$. Nótese que $0 \cdot 0 = 0$.

Ejemplo 2.7. Todo grupo G en el cual $a^2 = e$, es decir, $a = a^{-1}$ para todo $a \in G$, es automáticamente conmutativo. En efecto, $(ab)^{-1} = ab$, y también $(ab)^{-1} = b^{-1}a^{-1} = ba$.

Ejemplo 2.8. Si G es un grupo en el cual $(ab)^i = a^i b^i$ para todo $i = 0, 1, 2, \dots$, entonces G es abeliano. De hecho, si $(ab)^i = a^i b^i$ para tres enteros consecutivos $i = n, n+1, n+2$, entonces G es abeliano. En efecto, $a^{n+1}b^{n+1} = (ab)^{n+1} = (ab)(ab)^n = (ab)a^n b^n$, de lo cual $a^n b = ba^n$. De la misma manera se verifica que $a^{n+1}b = ba^{n+1}$. Pero entonces $aa^n b = aba^n = ba^{n+1}$, y así $ab = ba$.

Ejemplo 2.9. Si G es un grupo en el cual $(ab)^3 = a^3 b^3$ y $(ab)^5 = a^5 b^5$ cualesquiera que sean $a, b \in G$, entonces G es abeliano. Para comprobar esto obsérvese en primer lugar que $a(ba)^2 b = (ab)^3 = a^3 b^3$, así que $(ba)^2 = a^2 b^2$. Pero entonces $(ab)^4 = ((ab)^2)^2 = (b^2 a^2)^2 = (a^2)^2 (b^2)^2 = a^4 b^4$, y la afirmación resulta de lo establecido en el ejemplo 2.8.

Ejemplo 2.10. Si $(G, \cdot)$ es un grupo con 5 elementos, necesariamente G es abeliano. Para demostrar esto, supóngase que existen $a, b \in G$ tales que $ab \neq ba$. Claramente $a \neq e, b \neq e$, donde e es el elemento neutro de G (pues e conmuta con todo elemento de G). También $a \neq b$ (pues a conmuta consigo mismo), $a \neq ab, b \neq ab, b \neq ba, a \neq ba, ab \neq e$ (pues a conmuta con a^{-1}) y $ba \neq e$. Entonces $G = \{e, a, b, ab, ba\}$. Teniendo ahora en cuenta que a conmuta con cualquier potencia de a se concluye que $a^2 \neq b, a^2 \neq ab$,

$a^2 \neq ba$, así que $a^2 = e$, o sea que, $a = a^{-1}$. De la misma manera, $b^2 = e$ y $b = b^{-1}$. Ahora, es claro que $aba \neq a, ab, ba$. Tampoco $aba = e$, pues sería $ab = a^{-1} = a$, y entonces $b = e$. Finalmente $aba \neq b$, ya que $ab \neq ba$. Es decir, aba no tiene cabida en G , lo cual es absurdo. Entonces la hipótesis inicial $ab \neq ba$ es contradictoria, y será $ab = ba$ para todos los $a, b \in G$.

Ejemplo 2.11. El grupo $GL_2(K)$, $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, no es abeliano, pues, por ejemplo,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}. \quad (2.22)$$

A partir de

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad (2.23)$$

se pueden construir matrices no conmutativas de cualquier orden $n \geq 2$. Así,

$$\begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} B & 0 \\ 0 & 0 \end{bmatrix} \quad (2.24)$$

no conmutan, y $GL_n(K)$ no será conmutativo para $n \geq 2$.

EJERCICIOS

- 2.1 Sean $(G, \cdot)$ un grupo, $a \in G$. Demuestre que las aplicaciones $f_a, g_a, h_a : G \rightarrow G$ dadas respectivamente por (a) $f_a(x) = ax$, (b) $g_a(x) = xa$, (c) $h_a(x) = axa^{-1}$, $x \in G$, son biyectivas, que si e es el elemento neutro de G entonces $f_e = g_e = h_e$ es la aplicación idéntica de G , y que si $b = a^{-1}$, entonces $f_a^{-1} = f_b$, $g_a^{-1} = g_b$, $h_a^{-1} = h_b$.
- 2.2 Con respecto al ejercicio 2.1, verifique que $h_a(xy) = h_a(x)h_a(y)$ cualesquiera que sean $x, y \in G$, que $h_a(e) = e$, y que $h_a(x^{-1}) = (h_a(x))^{-1}$ para todo $x \in G$.
- 2.3 Con respecto al ejercicio 2.2, verifique que $(h_a(x))^n = h_a(x^n)$ para todo $n \in \mathbb{Z}$ y todo $x \in G$, así que $(axa^{-1})^n = ax^n a^{-1}$ en tales circunstancias. (Indicación. Considere primero el caso de $n \in \mathbb{N}$ y haga inducción.)
- 2.4 Sean $(G, \cdot)$ un grupo, $a \in G$, $m, n \in \mathbb{Z}$. Demuestre que $(a^m)^n = a^{mn}$. (Indicación. Considere primero el caso de $n \in \mathbb{N}$.)

2.5 Sean $(G, +)$ un grupo abeliano aditivo en el cual 0 es el elemento neutro, $-a$ es el inverso de a y $b - a$ es la solución única de $a + x = b$. Demuestre que

- a) $-(b - a) = a - b$,
- b) $a - (b + c) = (a - b) - c$,
- c) $a - (b - c) = (a - b) + c$,
- d) $a + (b - c) = (a + b) - c$,

cualesquiera que sean $a, b, c \in G$.

2.6 Sean $(G, \cdot)$ un grupo abeliano multiplicativo en el cual 1 es el elemento neutro y b/a es la única solución de $ax = b$. Verifique que $a^{-1} = 1/a$ y demuestre que

- a) $1/(b/a) = a/b$,
- b) $a/(bc) = (a/b)/c$,
- c) $a/(b/c) = (ac)/b$,
- d) $a(b/c) = (ab)/c$,
- e) $(a/b)(c/d) = (ac)/(bd)$,
- f) $(a/b)/(c/d) = (ad)/(bc)$,

cualesquiera que sean $a, b, c, d \in G$. Establezca análogos de (e) y (f) para el ejercicio 2.5

- 2.7 Con respecto al ejercicio 2.5, demuestre que $n(b - a) = nb - na$ cualesquiera que sean $a, b \in G$ y $n \in \mathbb{Z}$, y establezca el resultado análogo en el caso del ejercicio 2.6. Demuestre también que $(mn)a = m(na)$ cualesquiera que sean $a \in G$ y $m, n \in \mathbb{Z}$.
- 2.8 Sean G un conjunto, $e \in G$. Considere en G la ley de composición interna $a \cdot b = a$. Verifique que e es elemento neutro a derecha de G para $(\cdot)$ y que para todo $a \in G$ existe $a' \in G$ tal que $a' \cdot a = e$, pero que si G tiene más de un elemento, $(G, \cdot)$ no es un grupo.
- 2.9 Sea G un conjunto no vacío provisto de una ley de composición interna $(\cdot)$ asociativa y en el cual las ecuaciones $ax = b$ y $xa = b$ tienen al menos una solución cualesquiera que sean $a, b \in G$. Demuestre que si G es finito, o si las soluciones de las ecuaciones $ax = b$ y $xa = b$ son además únicas, entonces $(G, \cdot)$ es un grupo, y que este último es el caso si G es finito.

2.10 Sean $(G, \cdot)$ un grupo y $a, b \in G$. Supóngase que a y b conmutan. Demuestre por inducción que $ab^m = b^ma$ para todo $m \in \mathbb{N}$, y concluya luego que esto es válido para todo $m \in \mathbb{Z}$. Demuestre finalmente que $(ab)^2 = a^2b^2$ si y sólo si a y b conmutan.

2.11 Considere el grupo $(S_3, \cdot)$ y sean

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$d = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Verifique que la tabla de multiplicación de $(S_3, \cdot)$ es

$$\begin{bmatrix} e & a & b & c & d & f \\ a & e & d & f & b & c \\ b & f & e & d & c & a \\ c & d & f & e & a & b \\ d & c & a & b & f & e \\ f & b & c & a & e & d \end{bmatrix}$$

¿Es $(S_3, \cdot)$ un grupo conmutativo?

Capítulo 3

Subgrupos

Definición 3.1. Sea $(G, \cdot)$ un grupo cuyo elemento neutro es e . Se dice que un subconjunto H de G es un *subgrupo* de G si H tiene las tres propiedades siguientes:

- (i) $e \in H$.
- (ii) Si $a, b \in H$ entonces $ab \in H$.
- (iii) Si $a \in H$ entonces $a^{-1} \in H$.

Un subgrupo H de un grupo G nunca es vacío (pues $e \in H$), y si $a, b \in H$ entonces $ab^{-1} \in H$ (pues también $b^{-1} \in H$). Recíprocamente:

Teorema 3.1. Si $H \subseteq G$, $H \neq \emptyset$ y H tiene la propiedad

- (iv) Si $a, b \in H$, también $ab^{-1} \in H$, entonces H es un subgrupo de G .

Demostración. Como $H \neq \emptyset$ existe $c \in H$, y, en virtud de (iv), $e = cc^{-1} \in H$. Entonces (i) de la Definición 3.1 se satisface, y si $a \in H$, también en virtud de (iv), $a^{-1} = ea^{-1} \in H$. Finalmente, si $a, b \in H$ entonces $a, b^{-1} \in H$, de lo cual $ab = a(b^{-1})^{-1} \in H$. Esto demuestra que (ii) y (iii) de la definición 3.1 también se satisfacen, y H es así un subgrupo de G . $\square$

Nota 3.1. Un subgrupo H de G tiene la propiedad

- (v) Dados $a, b \in H$, también $ab \in H$.

Si $H \subseteq G$, $H \neq \emptyset$ y H tiene la anterior propiedad, puede suceder que H no sea un subgrupo de G , aún si $e \in H$. Por ejemplo $\mathbb{N} \subseteq \mathbb{Z}$ tiene la anterior propiedad y $0 \in \mathbb{N}$, pero $\mathbb{N}$ no es un subgrupo de $(\mathbb{Z}, +)$. Lo mismo, $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ tiene tal propiedad y $1 \in \mathbb{Z}^*$, pero $\mathbb{Z}^*$ no es un subgrupo de $(\mathbb{Q}^*, \cdot)$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. De hecho, la propiedad (v) no implica que $e \in H$ (aún si $H \neq \emptyset$). Por ejemplo, $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ no es un subgrupo de $(\mathbb{Z}, +)$, y $0 \notin \mathbb{N}^*$, pero satisface (v).

Sin embargo:

Teorema 3.2. Si $(G, \cdot)$ es un grupo y $H \subseteq G$ es finito, no vacío y satisface (v) de la nota 3.1, entonces H es un subgrupo de G .

Demostración. Como $H \neq \emptyset$, existe $c \in H$. Ahora, en virtud de (v), $f_c(x) = cx$, donde $c \in H$, es una aplicación de H en sí mismo, la cual es evidentemente inyectiva (si $cx = cy$, necesariamente $x = y$). Como H es finito, f_c será también sobreyectiva, y deberá existir $e_c \in H$ tal que $f_c(e_c) = c$; es decir, $ce_c = c$. Pero entonces $e_c = e$, el elemento neutro de G , así que $e \in H$. Como $f_a : H \rightarrow H$ es sobreyectiva para todo $a \in H$, para cada $a \in H$ deberá existir $a' \in H$ tal que $f_a(a') = e$, o sea, que $aa' = e$, de lo cual $a' = a^{-1}$. Se concluye que si $a \in H$, también $a^{-1} \in H$. Entonces, H es un subgrupo de G . $\square$

Ejemplo 3.1. Si $(G, \cdot)$ es un grupo y $a \in G$,

$$[a] := \{a^n : n \in \mathbb{Z}\} \quad (3.1)$$

es un subgrupo de G . En efecto, $e = a^0$, $(a^n)^{-1} = a^{-n}$ y $a^m a^n = a^{m+n}$, y todo resulta de observar que $0 \in \mathbb{Z}$, $-n \in \mathbb{Z}$ y $m+n \in \mathbb{Z}$ si $m, n \in \mathbb{Z}$. Se dice que $[a]$ es el *subgrupo cíclico de G generado por a* . Si $(G, +)$ es un grupo abeliano aditivo es corriente escribir ma en lugar de a^m . Entonces $[a] = \{ma : m \in \mathbb{Z}\}$.

Definición 3.2. Se dice que un grupo $(G, \cdot)$ es *cíclico* si $G = [a]$ para algún $a \in G$. Es decir, si G coincide con el subgrupo cíclico generado por alguno de sus elementos.

Ejemplo 3.2. El grupo $(\mathbb{Z}, +)$ es un grupo cíclico aditivo generado por 1, pues $m = m \cdot 1$ para todo $m \in \mathbb{Z}$. Así, $\mathbb{Z} = [1]$.

Nota 3.2. Si $(G, \cdot)$ es un grupo y H es un subgrupo de G , es claro que $(H, \cdot)$ es, efectivamente, un grupo. Si $a \in G$, $([a], \cdot)$ es un grupo abeliano, pues $a^m a^n = a^{m+n} = a^n a^m$ cualesquiera que sean $m, n \in \mathbb{Z}$.

En particular:

Teorema 3.3. Todo grupo cíclico es abeliano.

Definición 3.3. Sean $(G, \cdot)$ un grupo, $a \in G$. Se dice que a tiene *orden finito*, o que a es de *orden finito*, si existe $m \in \mathbb{Z}$, $m \neq 0$, tal que $a^m = e$. En tal caso

$$o(a) := \min\{m > 0 : a^m = e\} \quad (3.2)$$

se denomina el orden de G .

Nota 3.3. Como es claro, si $a \in G$ es de orden finito y $a^m = e$, también $a^{-m} = e$. Esto implica que el conjunto en (3.2) es no vacío, así que $o(a) \in \mathbb{N}$, $o(a) \geq 1$. Obsérvese además que $o(e) = 1$. Si $a \in G$ no tiene orden finito, es decir, si $a^m \neq e$ para todo $m \in \mathbb{Z}$, $m \neq 0$, es corriente decir que a tiene *orden infinito*, y escribir $o(a) = \infty$. Así, todo elemento $n \neq 0$ del grupo aditivo $(\mathbb{Z}, +)$ tiene orden infinito:

$$o(n) = o(1) = \infty, \quad n \in \mathbb{Z}, \quad n \neq 0. \quad (3.3)$$

Por otra parte, $o(0) = 1$.

Nota 3.4. Si G es un grupo, $a \in G$ tiene orden finito m y $a^n = e$, $n \in \mathbb{Z}$, entonces m divide a n , pues en caso contrario $n = mq + r$ donde $q, r \in \mathbb{Z}$ y $0 < r < m$ (capítulo 1, sección 1.4), así que $e = a^n = (a^m)^q a^r = e^q a^r = a^r$, lo cual es absurdo.

Nota 3.5. La notación $|a|$ es usual para el orden de un elemento a de un grupo G , sin embargo puede ser causa de confusión en algunos casos, como en el de los enteros, donde $|a|$, el orden de $a \in \mathbb{Z}$, puede confundirse con el valor absoluto $|a|$ de a . Así $|1| = \infty$ si $|1|$ es el orden de 1 como elemento del grupo $(\mathbb{Z}, +)$, mientras que $|1| = 1$ si $|1|$ denota el valor absoluto de 1.

Teorema 3.4. Un elemento a de un grupo $(G, \cdot)$ tiene orden finito si y sólo si

$$[a] = \{a^n : n \in \mathbb{N}\}. \quad (3.4)$$

Si además $m = o(a)$, entonces

$$[a] = \{a^n : 0 \leq n < m\}, \quad (3.5)$$

y para todo $n \in \mathbb{Z}$,

$$a^n = a^{r(n,m)} \quad (3.6)$$

donde $r(n, m)$ es el resto de dividir n por m (capítulo 1, sección 1.4).

Demostración. Si $[a] = \{a^n : n \in \mathbb{N}\}$, para todo $m \in \mathbb{Z}$, $m < 0$, deberá existir $n \in \mathbb{N}$ tal que $a^m = a^n$. Entonces $a^{n-m} = e$ y, como $n - m \neq 0$, a tendrá orden finito. Supóngase recíprocamente que a tiene orden finito m . Si $n \in \mathbb{Z}$ entonces $n = mq + r(n, m)$ donde $q \in \mathbb{Z}$, así que $a^n = (a^m)^q a^{r(n, m)} = e^q a^{r(n, m)} = a^{r(n, m)}$. Como $0 \leq r(n, m) < m$, esto demuestra el teorema, pues implica que $\{a^n : 0 \leq n < m\} \subseteq \{a^n : n \in \mathbb{N}\} \subseteq \{a^n : n \in \mathbb{Z}\} \subseteq \{a^n : 0 \leq n < m\}$. $\square$

Definición 3.4. Si G es un grupo finito, el orden $o(G)$ de G es el número de sus elementos. Si H es un subgrupo finito de G , $o(H)$, el orden de H , es también el número de sus elementos.

Nota 3.6. Si G no es finito, es corriente escribir $o(G) = \infty$. También $o(H) = \infty$ si H es un subgrupo infinito de G . Es claro entonces que

$$o([a]) = o(a) \quad (3.7)$$

para todo $a \in G$

Si $(G, \cdot)$ es un grupo, H es un subgrupo de G y $a \in G$, escribiremos

$$aH = \{ax : x \in H\} \quad (3.8)$$

y

$$Ha = \{xa : x \in H\}. \quad (3.9)$$

Se dice que aH es una clase lateral izquierda de H , una coclase a izquierda de H , o un cogrupo a izquierda de H . Respectivamente, Ha es una clase lateral, una coclase o un cogrupo a derecha de H . Nótese que $eH = He = H$ y que $a \in aH \cap Ha$.

En general aH no es un subgrupo de G . De hecho, aH es un subgrupo de G si y sólo si $a \in H$, en cuyo caso $aH = H$. Esto es un corolario del siguiente teorema.

Teorema 3.5. Si H es un subgrupo de G y $a, b \in G$, $aH = bH$ si y sólo si $aH \cap bH \neq \emptyset$.

Demostración. Como $a \in aH$, es claro que si $aH = bH$ entonces $aH \cap bH = aH \neq \emptyset$. Supóngase recíprocamente que $z \in aH \cap bH$ y sean $x, y \in H$

tales que $z = ax = by$. Demostraremos que $aH \subseteq bH$. Sea $c \in aH$, así que $c = ah$ con $h \in H$. Como $a = byx^{-1}$, $yx^{-1} \in H$, y también $(yx^{-1})h \in H$, entonces $c = bh'$ con $h' = (yx^{-1})h \in H$, así que $c \in bH$. Que $bH \subseteq aH$ se demuestra de la misma manera. $\square$

Corolario 3.1. Bajo la hipótesis del teorema, $aH = bH$ si y sólo si $aH \subseteq bH$.

Demostración. Si $aH = bH$, es claro que $aH \subseteq bH$. Recíprocamente, si $aH \subseteq bH$ entonces $aH \cap bH = aH \neq \emptyset$, así que $aH = bH$. $\square$

Corolario 3.2. Bajo las hipótesis del teorema, $aH = bH$ si y sólo si $b^{-1}a \in H$.

Demostración. Si $aH = bH$ entonces $a \in bH$, de lo cual $a = bh$, $h \in H$. Pero entonces $b^{-1}a = h \in H$. Recíprocamente, si $b^{-1}a \in H$ entonces $a = b(b^{-1}a) \in bH$, así que $aH \cap bH \neq \emptyset$. $\square$

Corolario 3.3. Si H es un subgrupo de G y $a \in G$, $aH = H$ si y sólo si $a \in H$.

Demostración. En efecto, $aH = eH$ si y sólo si $a = ea = e^{-1}a \in H$. $\square$

Corolario 3.4. Si a y H son como en el corolario anterior, aH es un subgrupo de G si y sólo si $a \in H$.

Demostración. Si $a \in H$ entonces $aH = H$ y aH es un subgrupo de G . Recíprocamente, si aH es un subgrupo de G entonces $e \in aH$, así que $e = ah$, $h \in H$. Como necesariamente $h = a^{-1}$ entonces $a^{-1} \in H$, de lo cual $a = (a^{-1})^{-1} \in H$. $\square$

Obsérvese ahora que $\varphi : aH \rightarrow G$ dada por $\varphi(x) = (ba^{-1})x$ es una aplicación inyectiva tal que $\varphi(aH) = bH$. En efecto, φ es claramente inyectiva, y si $c \in aH$, así que $c = ah$, $h \in H$, entonces $\varphi(c) = ba^{-1}ah = bh \in bH$, lo cual demuestra que $\varphi(aH) \subseteq bH$. Finalmente, si $d = bh' \in bH$ entonces $(ab^{-1})d = ah' \in aH$ y $\varphi((ab^{-1})d) = d$, lo cual establece que $\varphi(aH) = bH$. Se deduce que aH y bH tienen, cualesquiera que sean $a, b \in G$, el mismo número de elementos. En particular, aH y H tienen el mismo número de elementos:

$$\#(aH) = o(H) \quad (3.10)$$

para todo $a \in G$. Aquí $\#(aH)$ es el número de elementos de aH , con $\#(aH) = \infty$ si H es infinito.

Supóngase entonces que G es un grupo y que H es un subgrupo de G . El conjunto

$$G/H = \{aH : a \in G\} \quad (3.11)$$

de las clases laterales izquierdas de H es una *partición* de G , es decir, $aH \neq \emptyset$ para todo $a \in G$, $aH \cap bH = \emptyset$ si $aH \neq bH$, y

$$G = \bigcup_{a \in G} aH. \quad (3.12)$$

Además, todos los conjuntos aH tienen el mismo número de elementos. Esto y la relación (3.12) implican que si G es finito y C es un subconjunto de G que tiene con cada coclase aH un único elemento en común, entonces

$$o(G) = \sum_{a \in C} \#(aH) = \#(C) \cdot o(H). \quad (3.13)$$

Como es claro, $\#(C) = \#(G/H)$, así que

$$\#(G/H) = o(G)/o(H). \quad (3.14)$$

Como $\#(G/H)$, $o(H)$ y $o(G)$ son enteros positivos, se tiene entonces el siguiente teorema, uno de los más importantes de la teoría de los grupos.

Teorema 3.6 (Lagrange). Si G es un grupo finito y H es un subgrupo de G , entonces $o(H)$ divide $o(G)$.

Corolario 3.5 (Lagrange). Si G es un grupo finito y $a \in G$, entonces $o(a)$ es finito y divide $o(G)$.

Demostración. En efecto, $o(a) = o([a])$ y $[a]$ es un subgrupo de G . $\square$

Corolario 3.6. Si G es un grupo finito con $m = o(G)$, entonces $a^m = e$ para todo $a \in G$.

Demostración. En efecto, $m = o(a)n$ para algún $n \in \mathbb{N}$, y, como $a^{o(a)} = e$, también $a^m = (a^{o(a)})^n = e^n = e$. $\square$

Nota 3.7. Si $(G, \cdot)$ es un grupo, H es un subgrupo de G y $a \in H$, $[a] = \{a^n : n \in \mathbb{Z}\} \subseteq H$; es decir, $[a]$ es un subgrupo de todo subgrupo

H de G tal que $a \in H$. En otros términos, $[a]$ es el más pequeño subgrupo K de G tal que $a \in K$. Es por esta razón que se dice que $[a]$ es el subgrupo generado por a .

Nota 3.8. Resultados análogos a los establecidos para las clases laterales a izquierda de un subgrupo H de G valen para las clases a derecha. Así, $Ha = Hb$ si y sólo si $Ha \cap Hb \neq \emptyset$, lo cual ocurre si y sólo si $ab^{-1} \in H$. Entonces

$$G \setminus H = \{Ha : a \in G\}, \quad (3.15)$$

el conjunto de las clases laterales derechas de H , es también una partición de G , o sea, $Ha \neq \emptyset$ para todo $a \in G$ (nótese que $a \in Ha$), $Ha \cap Hb = \emptyset$ si $Ha \neq Hb$, y

$$G = \bigcup_{a \in G} Ha. \quad (3.16)$$

Además $\#(Ha) = o(H)$ para todo $a \in G$. De hecho, $x \mapsto xa$ es una correspondencia biyectiva de H sobre Ha y $x \mapsto x(a^{-1}b)$, una de Ha sobre Hb . Más aún, $x \mapsto bxa^{-1}$ es una correspondencia biyectiva de Ha sobre bH (y $x \mapsto axa^{-1}$, una de Ha sobre aH). Evidentemente, $He = eH = H$.

Nota 3.9. Si $(G, \cdot)$ es un grupo, $a \in G$ y $n \in \mathbb{Z}$, es claro que $[a^n] \subseteq [a]$, pero puede suceder que $[a^n] \neq [a]$. En notación aditiva $[a] = \{ma : m \in \mathbb{Z}\}$, así que $[na] \subseteq [a]$ para todo $n \in \mathbb{Z}$, pero, en general, $[na] \neq [a]$. Nótese, sin embargo, que $[a^{-1}] = [a]$, pues también $[a] \subseteq [a^{-1}]$, ya que $a = (a^{-1})^{-1}$. Por lo tanto, en notación aditiva, $[-a] = [a]$.

Ejemplo 3.3. Si $a \in \mathbb{Z}$, $[a] = \{ma : m \in \mathbb{Z}\} = \mathbb{Z}a$, el conjunto de los múltiplos de a . Como es claro, $[-a] = \mathbb{Z}(-a) = \mathbb{Z}a = [a]$. Evidentemente $\mathbb{Z}0 = \{0\}$, pero si $a \neq 0$, $\mathbb{Z}a$ es infinito. Obsérvese que $\mathbb{Z}a = a\mathbb{Z}$ para todo $a \in \mathbb{Z}$. Si $n \in \mathbb{Z}$ y $a \neq 0$, es claro que $\mathbb{Z}(na) \subseteq \mathbb{Z}a$, pero si $n \neq \pm 1$, $\mathbb{Z}(na) \neq \mathbb{Z}a$, ya que $a \notin \mathbb{Z}(na)$ (si $a \in \mathbb{Z}(na)$, sería $a = m(na) = (mn)a$ para algún $m \in \mathbb{Z}$, de lo cual $mn = 1$, así que $n = \pm 1$). Obsérvese finalmente que las clases laterales de $a\mathbb{Z}$ en $\mathbb{Z}$ son los conjuntos de la forma $b + a\mathbb{Z} = b + \mathbb{Z}a = \mathbb{Z}a + b = a\mathbb{Z} + b$. De hecho, $b + a\mathbb{Z} = r(b, a) + a\mathbb{Z}$, pues $b - r(b, a) = aq$, $q \in \mathbb{Z}$, así que $b - r(b, a) \in a\mathbb{Z}$. Si $a > 0$,

$$\mathbb{Z}/a\mathbb{Z} = \{a\mathbb{Z}, 1 + a\mathbb{Z}, 2 + a\mathbb{Z}, \dots, (a-1) + a\mathbb{Z}\} \quad (3.17)$$

es un conjunto finito con a elementos. Si $a < 0$,

$$\mathbb{Z}/a\mathbb{Z} = \{k + a\mathbb{Z} : 0 \leq k \leq |a| - 1 = -a - 1\} = \mathbb{Z}/(-a)\mathbb{Z}. \quad (3.18)$$

Si $a = 0$,

$$\mathbb{Z}/a\mathbb{Z} = \mathbb{Z}/\{0\} = \{\{k\} : k \in \mathbb{Z}\} \quad (3.19)$$

es infinito.

Definición 3.5. Si $(G, \cdot)$ es un grupo, $a \in G$ y $n \in \mathbb{Z}$ es tal que $[a^n] = [a]$, se dice que n es un *exponente primitivo* de a y que a^n es una *potencia primitiva* de a .

Como $[a^n] = [a^{-n}]$, n es primitivo si y sólo si $(-n)$ también lo es.

Teorema 3.7. Si $(G, \cdot)$ es un grupo, $a \in G$ y $[a]$ es infinito, a^n es una potencia primitiva de a si y sólo si $n = \pm 1$.

Demostración. Como $[a] = [a^{-1}]$, es claro que 1 y -1 son primitivos. Recíprocamente, si $[a^n] = [a]$ entonces $a = (a^n)^k$ para algún $k \in \mathbb{Z}$, así que $a^{nk-1} = e$, y, como $[a]$ es infinito, necesariamente $nk - 1 = 0$. Entonces $n = \pm 1$. $\square$

Nota 3.10. Observamos que si $[a]$ es finito, de modo que $[a] = \{a^k : 0 \leq k < m - 1\}$ donde $m = o(a)$, entonces n es primitivo si y sólo si $r(n, m)$, el resto de dividir n por m , también lo es. Esto resulta de que $a^n = a^{r(n, m)}$ para todo $n \in \mathbb{Z}$.

Teorema 3.8. Si $[a]$ es finito y $o(a) = m$, a^n es primitiva, o sea, n es primitivo, si y sólo si $\text{mcd}(n, m) = 1$ (capítulo 1, sección 1.4).

Demostración. Si $\text{mcd}(n, m) = 1$, existen $p, q \in \mathbb{Z}$ tales que $pm + qn = 1$ (capítulo 1, teorema 1.11), así que $(a^m)^p (a^n)^q = a$. Como $(a^m)^p = e^p = e$ entonces $(a^n)^q = a$, lo cual asegura que $a \in [a^n]$. Entonces $[a^n] = [a]$, y n es así primitivo. Supóngase recíprocamente que $[a^n] = [a]$, es decir, que $a^{nl} = a$ para algún $l \in \mathbb{Z}$. Pero entonces $nl - 1 = km$, $k \in \mathbb{Z}$, de lo cual $1 = ln + (-k)m$ y $1 = \text{mcd}(n, m)$. $\square$

Ejemplo 3.4. Si $n \in \mathbb{N}$, $n \geq 1$, el conjunto $T_n = \{z \in \mathbb{C} : z^n = 1\}$ de las raíces n -ésimas de la unidad (capítulo 1, sección 1.8) es un subgrupo cíclico de $(\mathbb{C}^*, \cdot)$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. En efecto, T_n es un subgrupo, pues $1 \in T_n$; si $z \in T_n$ también $z^{-1} \in T_n$, pues $(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1$; y si $z_1, z_2 \in T_n$ entonces $z_1 z_2 \in T_n$, pues $(z_1 z_2)^n = z_1^n z_2^n = 1 \cdot 1 = 1$. Además, como se establece en el capítulo 1, sección 1.8, teorema 1.23, si $w_n = e^{2\pi i/n}$, entonces $T_n = \{w_n^l : l = 0, 1, \dots, n-1\}$. Se concluye que T_n es el grupo cíclico generado

por w_n (con $o(w_n) = n$). Además, $l \in \mathbb{Z}$, w_n^l es una potencia primitiva de w_n si y sólo si w_n^l es una raíz primitiva n -ésima de la unidad (véase el capítulo 1, sección 1.8, nota 1.30), lo cual ocurre si y sólo si $\text{mcd}(l, n) = 1$.

Los dos teoremas siguientes, no del todo triviales, son característicos del tipo de resultados que se busca en la teoría de los grupos finitos. Si G es un grupo y H es un subgrupo de G tal que $\{e\} \neq H \neq G$, se dice que H es un subgrupo propio de G . El primer teorema caracteriza los grupos sin subgrupos propios. El segundo establece una propiedad importante de los grupos de orden primo.

Teorema 3.9. Si un grupo G no tiene subgrupos propios, entonces G es un grupo cíclico finito; y si $o(G) = p > 1$, entonces p es un número primo.

Demostración. Claramente $G = \{e\}$ no tiene subgrupos propios y es finito, cíclico y $o(G) = 1$. Supongamos entonces $o(G) > 1$, y sea $a \in G$, $a \neq e$. Entonces $[a] = G$. Si no, $[a]$ sería un subgrupo propio de G . Ahora, si $o(a) = \infty$, $[a^2]$ sería un subgrupo propio de $[a] = G$. Entonces $o(a) = p < \infty$. Pero, si p no es primo y q es un primo que divide a p , entonces $\text{mcd}(p, q) = q > 1$, así que, según el teorema 3.8, $[a^q] \subseteq [a]$ y $[a^q] \neq [a]$, de lo cual $[a^q]$ es un subgrupo propio de G . Esto es absurdo. Entonces p es primo, y como $G = [a]$ y $o(G) = p$, G es cíclico de orden primo. $\square$

Teorema 3.10. Si G es un grupo finito y $o(G) = p$ es un primo, G es necesariamente cíclico, está generado por cualquier elemento $a \in G$, $a \neq e$ y no tiene subgrupos propios.

Demostración. Sean $a \in G$, $a \neq e$, y $H = [a]$. Si fuera $H \neq G$, entonces $m = o(H)$ dividiría $o(G)$ y $m \neq o(G)$, lo cual aseguraría que $m = 1$. Esto es absurdo pues $a \in H$, así que $H \neq \{e\}$. Entonces $G = [a]$, y es cíclico. $\square$

Nota 3.11. Obsérvese que en el teorema anterior, $G = [b]$ para todo $b \in G$, $b \neq e$. Es decir, si $o(G) = p$ es primo y $G = [a]$, entonces $G = [a^n]$ para todo n , $1 \leq n < p$. Esto es obvio, y resulta también de observar que, necesariamente, $\text{mcd}(n, p) = 1$.

Ejemplo 3.5. Como consecuencia del teorema anterior, es fácil describir las posibles tablas de multiplicación de un grupo $G = \{e, a, b, c, d\}$ con 5 elementos. Podemos suponer, en efecto, que $b = a^2$, $c = a^3$, $d = a^4$ (ó,

$d = a^2, b = a^3, c = a^4$, etc.), así que una de tales tablas es

$$\begin{bmatrix} e & a & b & c & d \\ a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \end{bmatrix}$$

Las otras tablas posibles se elaboran de la misma manera. Este es un ejemplo simple de como la teoría de los grupos puede ser de ayuda en la elaboración de las tablas de multiplicación de un grupo. Obsérvese que la teoría permite también concluir que todo grupo de orden primo (y en particular de orden 5) es necesariamente abeliano (y lo mismo es cierto de todo grupo G de orden $n \leq 5$).

Tenemos finalmente el siguiente teorema.

Teorema 3.11. Si G es un grupo cíclico, todo subgrupo H de G también lo es.

Demostración. Si $G = [a]$ y $a^n \in H$, también $a^{-n} \in H$. Ahora, si $H = \{e\}$, es claro que H es cíclico. Si $H \neq \{e\}$, existe, en virtud de lo anterior, $n \in \mathbb{N}$, $n > 0$, tal que $a^n \in H$. Sea entonces $m = \min\{n \in \mathbb{N} : n > 0 \text{ y } a^n \in H\}$. Si $a^n \in H$ entonces m divide a n , pues en caso contrario $n = mq + r$, $q, r \in \mathbb{Z}$, $0 < r < m$, de lo cual $a^n = (a^m)^q a^r$, así que $a^r = a^n (a^m)^{-1} \in H$, que es absurdo (pues m es mínimo tal que $m > 0$ y $a^m \in H$). Entonces $a^n = (a^m)^k$, $k \in \mathbb{Z}$, así que $H = [a^m]$. $\square$

Nota 3.12. Si $G = \{e, a, \dots, a^{m-1}\}$ es cíclico de orden $m < \infty$ y $0 \leq k < m$, entonces a^k genera un subgrupo propio de G si y sólo si $\text{mcd}(m, k) = d > 1$. Por consiguiente $o(a^k) = m/d$. En efecto, si $n = o(a^k)$ entonces $n \mid \frac{m}{d}$, pues $(a^k)^{m/d} = (a^m)^{k/d} = e$. Por otra parte $m \mid kn$, pues $a^{kn} = e$. Entonces $m/d \mid k/d \cdot n$, y como $\text{mcd}(m/d, k/d) = 1$, entonces $m/d \mid n$.

EJERCICIOS

- 3.1 ¿Son $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ subgrupos de $(\mathbb{C}, +)$? ¿Son $\mathbb{Z}$ y $\mathbb{Q}$ subgrupos de $(\mathbb{R}, +)$? ¿Es $\mathbb{Z}$ un subgrupo de $\mathbb{Q}$? ¿Es $\mathbb{N}$ un subgrupo de $(\mathbb{Z}, +)$?

EJERCICIOS

- 3.2 Recuerdese que si $K \subseteq \mathbb{C}$, $K^* = K \setminus \{0\}$. ¿Son $\mathbb{Q}^*$ y $\mathbb{R}^*$ subgrupos de $(\mathbb{C}^*, \cdot)$? ¿Es $\mathbb{Q}^*$ un subgrupos de $(\mathbb{R}, \cdot)$? ¿Es $\mathbb{Z}^*$ un subgrupo de $(\mathbb{Q}^*, \cdot)$?
- 3.3 Sea $T = \{z \in \mathbb{C} : |z| = 1\}$, ¿Es T un subgrupos de $(\mathbb{C}^*, \cdot)$? ¿Es $(T_n, \cdot)$, $n \geq 1$, el grupo de las raíces n -ésimas de la unidad un subgrupode $(T, \cdot)$?
- 3.4 Mediante la tabla de multiplicar del ejercicio 2.12, encuentre todos los subgrupos de $(S_3, \cdot)$. (Indicación. Tales subgrupos tienen ordenes 1, 2, 3 o 6).
- 3.5 Sean $K = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, y $H_K = \{A \in GL_n(\mathbb{C}) : \text{Det}(A) \in K\}$. ¿Es H_K un subgrupo de $GL_n(\mathbb{C})$? Sea $H = \{A \in GL_n(\mathbb{C}) : \text{Det}(A) \in \mathbb{R} \text{ y } \text{Det}(A) > 0\}$. ¿Es H un subgrupo de $GL_n(\mathbb{C})$? Si $H' = \{A \in GL_n(\mathbb{C}) : \text{Det}(A) \leq 0\}$. ¿Es H' un subgrupo de $GL_n(\mathbb{R})$?
- 3.6 Demuestre que H es un subgrupo de $(\mathbb{Z}, +)$ si y sólo si existe $m \in \mathbb{N}$ tal que $H = m\mathbb{Z}$ y que $H \neq \{0\}$ si y sólo si $m \neq 0$. Demuestre igualmente que si H es un subgrupo de $(\mathbb{Q}, +)$, existe $m \in \mathbb{N}$ tal que $m\mathbb{Z} \subseteq H$ y que si $H \neq \{0\}$, m puede tomarse diferente de 0. ¿Es esto último cierto de todo subgrupo H de $(\mathbb{C}, +)$?
- 3.7 Demuestre que si H es un subgrupo de $(G, \cdot)$ y $a \in G$, $aHa^{-1} = \{axa^{-1} : x \in H\}$ es también un subgrupo de G .
- 3.8 Demuestre que si $(H_i)_{i \in I}$ es una familia de subgrupos de $(G, \cdot)$, $H = \bigcap_{i \in I} H_i$ es también un subgrupo de G . Concluya que:
- Si $A \subseteq G$, existe un subgrupo H de G tal que
 - $A \subseteq H$
 - Si H' es un subgrupo de G tal que $A \subseteq H'$, entonces $H \subseteq H'$.
 Se dice que H es el subgrupo generado por A y se denota con $[A]$. (Indicación. Considere la familia $(H_i)_{i \in I}$ de todos los subgrupos de G que contienen a A . Hay al menos uno: G .)
 - $[a]$ es el subgrupo generado por $A = \{a\}$.
 - $[\emptyset] = \{e\}$, donde e es el elemento neutro de G .
- 3.9 Sea $(G, \cdot)$ un grupo abeliano. Demuestre que $F(G) := \{a \in G : o(a) < \infty\}$ es un subgrupo de G . ¿Qué es $F(G)$ si G es finito?

3.10 Sea $(G, \cdot)$ un grupo abeliano y $n \in \mathbb{Z}$. Demuestre que tanto $G^n = \{a^n : a \in G\}$ como $G_n = \{a \in G : a^n = e\}$ son subgrupos de G . Verifique que si $G = S_3$ entonces G^2 es un subgrupo de G pero G_2 no lo es, mientras que G_3 es un subgrupo pero G^3 no lo es.

3.11 Sea $(G, \cdot)$ un grupo. Demuestre:

- La aplicación $\varphi : G \rightarrow G$ definida por $\varphi(x) = x^{-1}$ es biyectiva con $\varphi(e) = e$ y $\varphi(ab) = \varphi(b)\varphi(a)$ cualesquiera que sean $a, b \in G$.
- Sea $(G, \cdot)$ es abeliano, $\varphi(ab) = \varphi(a)\varphi(b)$ cualesquiera que sean $a, b \in G$ y $\varphi(a)^n = \varphi(a^n)$ para todo $a \in G$ y todo $n \in \mathbb{Z}$.
- Si $(G, \cdot)$ es abeliano, $o(G) = n \geq 1$, $G = \{a_1, a_2, \dots, a_n\}$ y $x = a_1 a_2 \cdots a_n$ entonces $\varphi(x) = x$, así que $x^2 = e$.
- Si G y x son como en (c) y existe un único $b \in G$, $b \neq e$, tal que $b^2 = e$, entonces $x = b$.
- Si G y x son como en (c) y existe más de un $b \in G$, $b \neq e$, tal que $b^2 = e$, entonces $x = b$.
- Si G y x son como en (c) y n es impar, entonces $x = e$.

3.12 Sean $(G, \cdot)$ un grupo, H un subgrupo de G , G/H el conjunto de las clases laterales izquierdas de H , $G \setminus H$ el conjunto de las clases laterales derechas. Demuestre que la aplicación $\psi : G/H \rightarrow G \setminus H$ dada por $\psi(aH) = Ha^{-1}$ está bien definida y es biyectiva. ¿Está bien definida la aplicación $\varphi(aH) = Ha$? Si lo está, demuéstrela. Si no, dé un contraejemplo. (Indicación. Considere el grupo $G = S_3$ del ejercicio 2.12 y sea $H = \{e, a\}$. Calcule bH , fH , Hb , Hf .)

Capítulo 4

Subgrupos Normales

Definición 4.1. Se dice que un subgrupo H de $(G, \cdot)$ es un *subgrupo normal* de G si $aH = Ha$ para todo $a \in G$.

Es decir, H es normal si y sólo si toda clase lateral izquierda de H es igual a la correspondiente clase lateral derecha. Evidentemente G es un subgrupo normal de sí mismo. También $H = \{e\}$ es un subgrupo normal de G . Existen grupos G cuyos únicos subgrupos normales son $\{e\}$ y G (véase el capítulo 8).

Si $(G, \cdot)$ es abeliano, todo subgrupo H de G es normal. Si $n \geq 2$, el subgrupo $GL_n(\mathbb{R})$ de $GL_n(\mathbb{C})$ no es normal (ejercicio 4.1). Tampoco $GL_n(\mathbb{Q})$ es un subgrupo normal de $GL_n(\mathbb{R})$. Si $G = S_3$ (ejercicio 2.12) es el grupo simétrico de 3 objetos, $H = \{e, d, f\}$ es un subgrupo normal de G , pero $H_1 = \{e, a\}$, $H_2 = \{e, b\}$ y $H_3 = \{e, c\}$ no lo son (ejercicio 4.2).

El siguiente teorema contiene algunas de las propiedades más importantes de los subgrupos normales. Definimos

$$aHa^{-1} := \{aha^{-1} | h \in H\}.$$

Teorema 4.1. Sean $(G, \cdot)$ un grupo, H un subgrupo de G . Las afirmaciones siguientes son equivalentes:

- H es un subgrupo normal de G .
- $aH \subseteq Ha$ cualquiera que sea $a \in G$.

3. $aHa^{-1} \subseteq H$ para todo $a \in G$.
4. $H \subseteq aHa^{-1}$ cualquiera que sea $a \in G$.
5. $Ha \subseteq aH$ para todo $a \in G$.

Demostración. Es claro que (1) $\Rightarrow$ (2). Para ver que (2) $\Rightarrow$ (3), obsérvese que (2) implica que para todo $a \in G$ y todo $h \in H$ existe $h' \in H$ tal que $ah = h'a$. Pero entonces $aha^{-1} = h' \in H$, o sea, $aha^{-1} \in H$ para todo $h \in H$, así que $aHa^{-1} \subseteq H$. Ahora, si $aHa^{-1} \subseteq H$ para todo $a \in G$, y $h \in H$, entonces $aha^{-1} = h'$ para algún $h' \in H$, de lo cual $h = a^{-1}h'a$, o sea, $h \in a^{-1}Ha$; entonces $H \subseteq a^{-1}Ha$ para todo $a \in G$, en particular $H \subseteq (a^{-1})^{-1}Ha^{-1} = aHa^{-1}$ para todo $a \in G$, y de esto (3) $\Rightarrow$ (4). Para ver que (4) $\Rightarrow$ (5) obsérvese que, de (4), si $a \in G$ y $h \in H$ entonces $h = ah'a^{-1}$ para algún $h' \in H$, de lo cual $ha = ah'$, $h' \in H$; entonces, $Ha \subseteq aH$, lo cual demuestra (5). Demostraremos finalmente que (5) $\Rightarrow$ (1). Basta demostrar que si (5) se satisface, también $aH \subseteq Ha$ para todo $a \in G$. Sean entonces $a \in G$, $h \in H$ y $x = ah$; entonces $x^{-1} = h^{-1}a^{-1} \in Ha^{-1}$, y como $Ha^{-1} \subseteq a^{-1}H$, se tiene que $h^{-1}a^{-1} = a^{-1}h'$, $h' \in H$; pero entonces $x = (h')^{-1}a \in Ha$, y así $aH \subseteq Ha$. $\square$

Corolario 4.1. Sea H un subgrupo de $(G, \cdot)$. Entonces H es normal si y sólo si para todo $a \in G$, $aH = Hb$ para algún $b \in G$.

Demostración. Si H es normal, $aH = Ha$ para todo $a \in G$, así que la condición se satisface. Por otra parte, si $aH = Hb$ entonces $a \in Hb \cap Ha$, o sea $Hb \cap Ha \neq \emptyset$. Esto implica que $Hb = Ha$. Entonces $aH = Ha$, y H es así normal. $\square$

Nota 4.1. Como es claro del teorema 4.1, H es normal en G si y sólo si $H = aHa^{-1} = a^{-1}Ha$ para todo $a \in G$ (pues si H es normal, de (3), $aHa^{-1} \subseteq H$, y, de (4), $H \subseteq aHa^{-1}$. Lo recíproco es trivial).

Definición 4.2. Si $(G, \cdot)$ es un grupo y H es un subgrupo de G , denotaremos con $[G : H]$, y lo denominaremos el *índice de H en G* , el número de clases laterales izquierdas de H en G :

$$[G : H] := \#(G/H).$$

$[G : H] = \infty$ si G/H es infinito.

Si G es un grupo y $A, B \subseteq G$, definimos

$$AB = A \cdot B := \{ab : a \in A, b \in B\}$$

El siguiente teorema es fundamental.

Teorema 4.2. Si H es un subgrupo normal de $(G, \cdot)$, la ley de composición $(aH)(bH) = \{ahbh' : h, h' \in H\}$, es una ley de composición interna en G/H que hace de este conjunto un grupo, en el cual $H = eH$ es el elemento neutro y $a^{-1}H$ es el inverso de aH . Más aún,

$$(aH)(bH) = (ab)H.$$

Demostración. Demostraremos primero que $(aH)(bH) = (ab)H$, lo cual asegurará que la ley de composición dada en G/H es clausurativa (o sea, una ley de composición interna). Sean entonces $x = ah$, $y = bh'$, donde $h, h' \in H$. Demostraremos que $xy \in (ab)H$. Pero, como H es normal, $Hb = bH$, así que existe $h'' \in H$ tal que $hb = bh''$, y entonces $xy = (ah)(bh') = a(hb)h' = a(bh'')h' = (ab)(h''h')$. Como $h''h' \in H$, la afirmación queda demostrada. Sea, recíprocamente, $z = (ab)h$, $h \in H$, un elemento de $(ab)H$. Como $z = (ae)(bh)$, entonces $z \in (aH)(bH)$. Así, $(aH)(bH) = abH$. Ahora, la anterior ley de composición en G/H es asociativa. En efecto, $[(aH)(bH)](cH) = [(ab)H](cH) = (ab)cH = a(bc)H = (aH)[bcH] = (aH)[(bH)(cH)]$. Como además $(aH)H = (aH)(eH) = (ae)H = aH$, $H = eH$ es el elemento neutro de G/H para esta ley. Como finalmente $(aH)(a^{-1}H) = aa^{-1}H = eH = H$, es claro que $(aH)^{-1} = a^{-1}H$, y el teorema queda demostrado. $\square$

Corolario 4.2. Si G es abeliano y H es un subgrupo de G , H es normal en G y G/H es abeliano.

Demostración. Es claro que H es normal, y como $(aH)(bH) = (ab)H = (ba)H = (bH)(aH)$, G/H es abeliano. $\square$

Nota 4.2. Si H es un subgrupo normal de G , la ley de composición en G/H está dada por

$$(aH)(bH) = \{(ax)(by) : x, y \in H\},$$

y como

$$(aH)(bH) = (ab)H,$$

resulta ser una ley de composición interna en G/H . Es natural preguntarse si cuando H no es normal, la relación anterior, permite aún definir, directamente, una operación en G/H . Esto es falso, pues puede suceder que

$aH = a'H$ y $bH = b'H$ y que $(ab)H \neq (a'b')H$. En efecto $(ab)H = (a'b')H$ vale si y sólo si $(ab)^{-1}(a'b') = b^{-1}(a^{-1}a')b' \in H$, y esto no se deduce de $a^{-1}a' \in H$, $b^{-1}b' \in H$ si H no es normal. Obsérvese, sin embargo, que si H es normal, $(ab)^{-1}(a'b') = (b^{-1}(a^{-1}a')b)b^{-1}b'$ y, como en tal caso $b^{-1}(a^{-1}a')b \in H$, entonces $(ab)^{-1}(a'b') \in HH = H$, como era de esperarse.

Definición 4.3. El conjunto G/H de las clases laterales izquierdas de un subgrupo normal H de G con la ley de composición interna

$$(aH)(bH) = (ab)H$$

se denomina el grupo cociente de G por H .

Nota 4.3. Obsérvese que cuando H es normal en G , el orden $o(G/H)$ de G/H es

$$o(G/H) = [G : H],$$

el índice de H en G .

Nota 4.4. Es conveniente observar que cuando se considera como elemento de G/H , aH es un objeto, y en muchas ocasiones (aunque no en todas), es poco importante tener presente que aH es un subconjunto de G . Para enfatizar este hecho es frecuente denotar a aH simplemente con $\bar{a}$, especialmente cuando no hay riesgo de confusión, así que

$$\overline{ab} = \overline{a}\overline{b}, (\overline{a})^{-1} = \overline{a^{-1}},$$

pero debe recordarse que $\overline{a} = \overline{b}$ no implica que $a = b$: sólo que $b^{-1}a \in H$.

Obsérvese que $o(\overline{a})$ es ∞ o el mínimo $m \in \mathbb{N}$, $m > 0$, tal que $(\overline{a})^m = \overline{a^m} = \overline{e}$ (o sea, tal que $a^m \in H$). En este contexto $o(aH) = o(\overline{a})$ no tiene nada que ver con el número de elementos de aH . En particular, $o(H) = o(\overline{e}) = 1$, aunque H tenga más de un elemento. Esperamos que el contexto permita evitar posibles confusiones.

Ejemplo 4.1. Si $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, el conjunto

$$H = \{A \in GL_n(K) : \text{Det}(A) \in \mathbb{R}, \text{Det}(A) > 0\}$$

es un subgrupo de $GL_n(K)$. Como además $\text{Det}(XAX^{-1}) = \text{Det}(XX^{-1}A) = \text{Det}(A) > 0$ para $A \in H$ y $X \in GL_n(K)$, H es un subgrupo normal de $GL_n(K)$. También

$$SL_n(K) := \{A \in GL_n(K) : \text{Det}(A) = 1\}$$

es un subgrupo normal de G , y lo mismo es cierto de

$$|SL_n|(K) := \{A \in GL_n(K) : |\text{Det}(A)| = 1\}.$$

Como una aplicación del hecho de que G/H es un grupo si H es normal en G , demostraremos el siguiente teorema, un recíproco parcial del teorema de Lagrange.

Teorema 4.3 (Cauchy). Si G es un grupo abeliano finito y p es un primo que divide $o(G)$, existe $a \in G$ tal que $o(a) = p$, y G tendrá así un subgrupo de orden p .

Demostración. Razonaremos por inducción sobre $o(G)$. Sea $b \in G$, $b \neq e$. Si $o(b) = o(G)$ (lo cual ocurre en particular si $o(G) = p$) y $m = o(G)/p$, entonces $o(b^m) = p$, y la afirmación queda demostrada con $a = b^m$. Podemos suponer entonces que $H = [b] \neq G$. Si $o(H) = p$, la afirmación resulta con $a = b$. Si $o(H) \neq p$, pero $p \mid o(H)$, podemos concluir por inducción (puesto que $o(H) < o(G)$) que también existe $a \in H$ con $o(a) = p$. Supongamos entonces que p no divide a $o(H)$, así que p divide a $[G : H]$. Como G es abeliano, H es normal y G/H es un grupo, obviamente abeliano. Como además $H \neq \{e\}$, $o(G/H) = o(G)/o(H) < o(G)$, y como $p \mid o(G/H)$, podemos suponer por inducción que existe $c \in G$ tal que cH tiene orden p en G/H . Entonces $(cH)^p = c^pH = H$, o sea $c^p \in H$, y si $k = o(H)$, $(c^k)^p = (c^p)^k = e$. Pero $c^k \neq e$ (en caso contrario $(cH)^k = H$, y se tendría que $p \mid k$ (nota 3.10)), así que si $a = c^k$ entonces $o(a) = p$. $\square$

Las siguientes observaciones se refieren a resultados que serán útiles en los capítulos siguientes.

Nota 4.5. Si N es un subgrupo normal de G y M es un subgrupo de G tal que $N \subseteq M$, es claro que N es un subgrupo normal de M . Como todo subgrupo de G es un subgrupo normal de sí mismo, es falso en general que si N es un subgrupo normal de un subgrupo M de G entonces N es un subgrupo normal de G (esto puede suceder aún si M es normal en G . Véase el ejercicio 8.11).

Nota 4.6. Si M y N son subgrupos de G y $MN = \{xy : x \in M, y \in N\}$, no necesariamente MN es un subgrupo de G (véase el ejercicio 4.3). Esto es cierto, sin embargo, si $MN = NM$. En efecto, es claro que $e \in MN$, y si $a = xy$, $x \in M, y \in N$, entonces $a^{-1} = y^{-1}x^{-1} \in NM = MN$. Por otra parte, si $a = xy$ y $b = x'y'$ donde $x, x' \in M$ y $y, y' \in N$, entonces

$ab = x(yx')y'$, y como $yx' \in NM = MN$, existirán $x'' \in M$, $y'' \in N$ tales que $yx' = x''y''$, de lo cual $ab = (xx'')(y''y') \in MN$. Finalmente, es fácil verificar que si MN es un subgrupo de G entonces $MN = NM$. De todo esto se deduce el siguiente teorema.

Teorema 4.4. Si M, N son subgrupos de G y N es normal en G entonces MN es un subgrupo de G y N es un subgrupo normal de MN . Además $M \cap N$ es un subgrupo de N y un subgrupo normal de M .

Demostración. Como $MN = \bigcup_{a \in N} aN = \bigcup_{a \in N} Na = NM$, se deduce que MN es un subgrupo de G , y es obvio que N es un subgrupo normal de MN . Es además claro que $M \cap N$ es un subgrupo de M y de N , y si $a \in M$ y $b \in M \cap N$ entonces $aba^{-1} \in N$ (pues N es normal) y $aba^{-1} \in M$ (pues $ab \in M$ y $a^{-1} \in M$), así que $aba^{-1} \in M \cap N$. $\square$

Corolario 4.2. Si G es abeliano y M, N son subgrupos de G , MN es un subgrupo de G .

EJERCICIOS

4.1 Demuestre que si $n \geq 2$, $GL_n(\mathbb{Q})$ y $GL_n(\mathbb{R})$ no son subgrupos normales en $GL_n(\mathbb{C})$, y que tampoco $GL_n(\mathbb{Q})$ es normal en $GL_n(\mathbb{R})$.

4.2 Con respecto al ejercicio 2.12, verifique que $H = \{e, d, f\}$ es un subgrupo normal de $G = S_3$, pero que $H_1 = \{e, a\}$, $H_2 = \{e, b\}$, $H_3 = \{e, c\}$ no lo son.

4.3 Sean G , H_1 y H_2 como en el ejercicio 4.2. Verifique que:

- a) $(dH_1)(fH_1) = \{e, a, b, f\} \neq (df)H_1 = \{e, a\}$.
- b) $H_1H_2 = \{e, a, b, d\} \neq H_2H_1 = \{e, a, b, f\}$.
- c) H_1H_2 y H_2H_1 no son subgrupos de G .

Verifique además que $dH_1 \neq H_1x$ para todo $x \in G$.

4.4 Demuestre que si $n \geq 2$, $\{A \in GL_n(\mathbb{R}) : \text{Det}(A) = 1\} = SL_n(\mathbb{R})$ es un subgrupo normal de $GL_n(\mathbb{C})$.

4.5 Sean $(G, \cdot)$ un grupo, H un subgrupo de G . Demuestre que $H' = \bigcap_{a \in G} aHa^{-1}$ es un subgrupo normal de G contenido en H y que $H' = H$ si y sólo si H es normal en G .

4.6 Demuestre que si M y N son subgrupos de G y $H = MN$ es un subgrupo de G , entonces $MN = NM$. Demuestre además que si M y N son normales en G entonces H es un subgrupo normal de G y que si $M \cap N = \{e\}$ entonces $ab = ba$ cualesquiera que sean $a \in M$, $b \in N$. (Indicación. ¿Donde está $aba^{-1}b^{-1}$?)

4.7 Sea $(G, \cdot)$ un grupo y para cada $a \in G$ sea $C(a) = \{x \in G : xa = ax\} = \{x \in G : xax^{-1} = a\}$. Demuestre que $C(a)$ es un subgrupo de G y que $Z(G) = \bigcap_{a \in G} C(a)$, el conjunto de los $x \in G$ que conmutan con todo $a \in G$, es un subgrupo normal de G . Demuestre además que $(Z(G), \cdot)$ es un grupo abeliano, que todo subgrupo H de $Z(G)$ es un subgrupo normal de G y que $C(a) = G$ si y sólo si $a \in Z(G)$. Se dice que $Z(G)$ es el *centro* de G .

4.8 Sean $(G, \cdot)$ un grupo, H un subgrupo de G . Demuestre que si $aH = bH$ implica que $Ha = Hb$ cualesquiera que sean $a, b \in G$, entonces H es un subgrupo normal de G .

4.9 Sean $(G, \cdot)$ un grupo, H un subgrupo normal de G . Demuestre que si $o(a)$ es finito, $a \in G$, el orden $o(aH)$ de aH en G/H divide a $o(a)$.

4.10 Sean $(G, \cdot)$ un grupo, H un subgrupo de G tal que $H \subseteq Z(G)$ (ejercicio 4.7). Demuestre que H es normal en G y que si G/H es cíclico entonces $(G, \cdot)$ es abeliano.

4.11 Sea $(G, \cdot)$ un grupo y supóngase que existen $a, b \in G$ con $ab = ba$ y $o(a) = m$, $o(b) = n$, donde $\text{mcd}(m, n) = 1$. Demuestre que $o(ab) = mn$. Concluya que si $o(G) = mn$ entonces G es cíclico, y que este es siempre el caso si G es abeliano y $o(G) = pq$ donde p y q son primos distintos.

4.12 Sea $(G, \cdot)$ un grupo abeliano y supóngase que $o(G) = mn$, donde $\text{mcd}(m, n) = 1$. Sea G_m como en el ejercicio 3.10 y considere el grupo G/G_m . Demuestre que si $(xG_m)^m = G_m$ en G/G_m , entonces $x \in G_m$ (es decir, $o(x) \mid m$).

4.13 Sean G un grupo, $a, b \in G$ con $ab = ba$ y $o(a) = m$, $o(b) = n$. Demuestre que si $[a] \cap [b] = \{e\}$ entonces $o(ab) = \text{lcm}(m, n)$.

Capítulo 5

Homomorfía e isomorfía

Definición 5.1. Sean $(G, \cdot)$ y $(G', \cdot)$ grupos. Una aplicación $f : G \rightarrow G'$ tal que

$$f(ab) = f(a)f(b)$$

se denomina un *homomorfismo de G en G'* . Si f es inyectiva, se dice que f es un *monomorfismo de G en G'* . Si es sobreyectiva, que es un *epimorfismo de G sobre G'* . Si es biyectiva, que es un *isomorfismo de G sobre G'* .

Un isomorfismo es entonces, al mismo tiempo, un monomorfismo y un epimorfismo.

Ejemplo 5.1. Si $m \in \mathbb{Z}$ y $m \neq 0$, la aplicación $f(a) = ma$ es un homomorfismo de $(\mathbb{Z}, +)$ en $(\mathbb{Z}, +)$, es decir, de $(\mathbb{Z}, +)$ en sí mismo. Evidentemente, f es un monomorfismo. De hecho, f puede considerarse como un isomorfismo de $(\mathbb{Z}, +)$ sobre $(m\mathbb{Z}, +)$, el cual es un subgrupo de $(\mathbb{Z}, +)$.

Ejemplo 5.2. Si $(\mathbb{R}^*, \cdot)$, donde $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, es el grupo multiplicativo de los números reales no nulos, $f(x) = |x|$ es un homomorfismo de $(\mathbb{R}^*, \cdot)$ en $(\mathbb{R}_+, \cdot)$, el grupo multiplicativo de los números reales estrictamente positivos. También $g(x) = \log x$ es un homomorfismo de $(\mathbb{R}_+, \cdot)$ en $(\mathbb{R}, +)$, y $h(x) = \log |x|$, uno de $(\mathbb{R}^*, \cdot)$ en $(\mathbb{R}, +)$. Es fácil ver que g es un isomorfismo y que f y h son epimorfismos pero no isomorfismos. Nótese que $g^{-1}(x) = e^x$ es también un isomorfismo de $(\mathbb{R}, +)$ sobre $(\mathbb{R}_+, \cdot)$.

Ejemplo 5.3. Sea $(T, \cdot)$ el grupo multiplicativo de los números complejos z tales que $|z| = 1$. Entonces $f : \mathbb{R} \rightarrow T$ dado por $f(x) = e^{2\pi i x}$ es un epimorfismo de $(\mathbb{R}, +)$ sobre $(T, \cdot)$. Claramente, f no es un isomorfismo.

Ejemplo 5.4. La aplicación $f : \mathbb{C} \rightarrow \mathbb{R}_+^*$ dada por $f(z) = |z|$ es un epimorfismo de $(\mathbb{C}^*, \cdot)$, el grupo multiplicativo de los números complejos no nulos, sobre $(\mathbb{R}_+^*, \cdot)$. A su vez, la aplicación $g(z) = e^{2\pi iz}$ de $(\mathbb{C}, +)$ en $(\mathbb{C}^*, \cdot)$ es un epimorfismo. Ni f ni g son isomorfismos.

Ejemplo 5.5. Si $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, la aplicación $f : GL_n(K) \rightarrow K^* = K \setminus \{0\}$ dada por $f(A) = \text{Det}(A)$ es un epimorfismo de $(GL_n(K), \cdot)$ sobre $(K^*, \cdot)$.

Ejemplo 5.6. Si H es un subgrupo normal de $(G, \cdot)$, $\varphi : G \rightarrow G/H$ dada por $\varphi(a) = aH$ es un epimorfismo de $(G, \cdot)$ sobre $(G/H, \cdot)$, el cual es un isomorfismo si y sólo si $H = \{e\}$. Se dice que φ es el epimorfismo canónico de G sobre G/H .

Teorema 5.1. Si f es un homomorfismo de $(G, \cdot)$ en $(G', \cdot)$ y e es el elemento neutro de G , $f(e)$ es el elemento neutro e' de G' y $f(a^{-1}) = (f(a))^{-1}$ para todo $a \in G$.

Demostración. Como $f(a) = f(ae) = f(a)f(e)$, es claro que $f(e) = e'$. Como entonces $e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$, también $f(a^{-1}) = (f(a))^{-1}$. $\square$

Nota 5.1. Como se verifica fácilmente, si $f : G \rightarrow G'$ y $g : G' \rightarrow G''$ son homomorfismos, $g \circ f$ también lo es (pues $g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = g \circ f(a)g \circ f(b)$; y si $f : G \rightarrow G'$ es un isomorfismo, f^{-1} es un isomorfismo (obsérvese que $f(f^{-1}(a')f^{-1}(b')) = f(f^{-1}(a'))f(f^{-1}(b')) = a'b'$, de lo cual $f^{-1}(a')f^{-1}(b') = f^{-1}(a'b')$, cualesquiera que sean $a', b' \in G'$).

Nota 5.2 (Importante). Si G y G' son grupos y H es un subgrupo normal de G , para definir una aplicación f de G/H en G' no es suficiente en general asignar un elemento a^* a cada elemento $a \in G$ y luego tomar $f(aH) = a^*$, pues puede suceder que $aH = bH$ con $a \neq b$ y que $a^* \neq b^*$. Para que f quede bien definida es necesario asegurarse de que $a^* = b^*$ si $b^{-1}a \in H$. Así, si $g : G \rightarrow G'$ es una aplicación, para que $f : G/H \rightarrow G'$ dada por $f(aH) = g(a)$ quede bien definida es necesario y suficiente que $g(a) = g(b)$ si $b^{-1}a \in H$ (véanse los ejercicios 5.11 y 5.12).

Si $(G, \cdot)$ y $(G', \cdot)$ son grupos y $f : G \rightarrow G'$ es un isomorfismo de G sobre G' , en cuyo caso se dice que $(G, \cdot)$ y $(G', \cdot)$ son isomorfos, $(G, \cdot)$ y $(G', \cdot)$ son esencialmente el mismo grupo (se dice usualmente que, salvo por diferencias de notación, son el mismo grupo: x y $f(x)$ se consideran entonces, salvo por

la forma como se denotan, iguales). Dicho de otra manera, desde el punto de vista de sus propiedades como grupos, y no teniendo en cuenta su origen, ni la manera como se escriban, es imposible distinguir entre grupos isomorfos. Así, $(\mathbb{R}_+^*, \cdot)$ y $(\mathbb{R}, +)$ son iguales si se identifican x y $\log x$ (o, x y e^x), pero $(\mathbb{Q}, +)$ y $(\mathbb{R}, +)$ son muy diferentes (capítulo 1, sección 1.11). Si G y G' son isomorfos, es usual escribir $G \approx G'$. Nótese que $G \approx G$ (pues la identidad de G es un isomorfismo de G sobre sí mismo). Es claro además que si $G \approx G'$ entonces $G' \approx G$ y que si $G \approx G'$ y $G' \approx G''$ entonces $G \approx G''$. Esto resulta de observar que si f es un isomorfismo también f^{-1} lo es, y que si f y g son isomorfismos y $g \circ f$ está definida, $g \circ f$ es un isomorfismo.

Es claro, por ejemplo, que dos grupos de orden n , con $n = 1, 2, 3$, son necesariamente isomorfos (téngase en cuenta que para cada uno de estos órdenes solo una tabla de multiplicación es posible). Es también fácil verificar que los grupos de orden 4 cuyas tablas de multiplicación son A_{12} , A_2 o A_3 (capítulo 2) son isomorfos ($e \rightarrow e, a \rightarrow c, b \rightarrow b, c \rightarrow a$ es un isomorfismo de A_{12} sobre A_2 ; $e \rightarrow e, a \rightarrow b, b \rightarrow a, c \rightarrow c$, uno de A_{12} sobre A_3). En cuanto a A_{11} , un grupo con esta tabla no puede ser isomorfo a ninguno de los otros tres. Como dos grupos isomorfos a un tercero son isomorfos entre sí, todo grupo de orden 4 es isomorfo sea a uno cuya tabla es A_{11} o a uno cuya tabla es A_{12} , lo cual se expresa diciendo que sólo existen esencialmente dos grupos de orden 4.

Ejemplo 5.7. Todo grupo cíclico infinito $(G, \cdot)$ es isomorfo a $(\mathbb{Z}, +)$. En efecto, $G = [a]$ donde $[a] = \{a^n : n \in \mathbb{Z}\}$ para algún $a \in G$, y $f : \mathbb{Z} \rightarrow G$ dada por $f(n) = a^n$ para todo $n \in \mathbb{Z}$ es un isomorfismo.

Nota 5.3. Dos grupos isomorfos tienen necesariamente el mismo orden. Dos grupos de un mismo orden primo son necesariamente isomorfos. Es decir, para cada número primo p existe esencialmente un único grupo de orden p : el grupo cíclico $(\mathbb{Z}_p, +)$. Para un orden finito no primo n , esto no es siempre cierto (tal es el caso de $n = 4$). Sin embargo, es claro que dos grupos cíclicos de orden n son isomorfos.

Nota 5.4 (Importante). Los grupos hicieron su aparición en matemáticas esencialmente como grupos de transformaciones (permutaciones): conjuntos de aplicaciones biyectivas de un conjunto X en sí mismo con la ley de composición de funciones como operación, con la identidad I de X como elemento neutro, y con la aplicación inversa T^{-1} como inversa de T . Como es claro, un conjunto $\mathcal{G}$ de transformaciones de X en sí mismo tal que $I \in \mathcal{G}$,

que $S \circ T \in \mathcal{G}$ si $S, T \in \mathcal{G}$, y que $S^{-1} \in \mathcal{G}$ cuando $S \in \mathcal{G}$, es, en efecto, un grupo para la ley de composición de funciones como ley de grupo. De hecho, todo grupo G es en esencia un grupo de transformaciones. En efecto, si para cada $a \in G$, $T_a : G \rightarrow G$ es la aplicación $T_a(x) = ax$, es claro que T_a es biyectiva, y, como $I = T_e$, $T_a^{-1} = T_{a^{-1}}$ y $T_a \circ T_b = T_{ab}$, el conjunto $\mathcal{G} = \{T_a : a \in G\}$ de tales transformaciones es un grupo en el sentido anterior. Como la aplicación $T : G \rightarrow \mathcal{G}$ dada por $T(a) = T_a$ es obviamente biyectiva (si $T_a = T_b$ entonces $a = b$) y además $T(ab) = T_{ab} = T_a \circ T_b = T(a) \circ T(b)$, T es un isomorfismo. El hecho de que *todo grupo G pueda realizarse, o representarse, como un grupo de transformaciones, es decir, que sea isomorfo a un tal grupo, se conoce como el teorema de Cayley*. La identificación explícita de G con una representación G como subgrupo de $(\mathfrak{F}_0(G), \cdot)$ no es, sin embargo, una tarea fácil. Este problema será considerado, en algún detalle, en el capítulo 11.

La noción de isomorfía permite, en cierta forma, reducir el número de grupos por considerar, al menos dentro de una clase dada de grupos. Así, de todos los grupos cíclicos infinitos, basta considerar a $(\mathbb{Z}, +)$, y como prototipo de los grupos cíclicos de orden n puede tomarse $(T_n, \cdot)$, el grupo de las raíces n -ésimas de la unidad, o, más naturalmente, el grupo $\mathbb{Z}_n$ de las clases izquierdas de $\mathbb{Z}$ para $n\mathbb{Z}$:

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}, \bar{a} = a + n\mathbb{Z}.$$

Recordamos ahora que si $f : X \rightarrow Y$, $A \subseteq X$ y $B \subseteq Y$, entonces

$$f(A) = \{f(x) : x \in A\}, \quad f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

Por lo tanto, $y \in f(A)$ si y sólo si existe $x \in A$ tal que $y = f(x)$ y $x \in f^{-1}(B)$ si y sólo si $f(x) \in B$.

Teorema 5.2. Sean $(G, \cdot)$ y $(G', \cdot)$ grupos, $f : G \rightarrow G'$ un homomorfismo, H un subgrupo de G y H' un subgrupo de G' . Entonces:

1. $f(H)$ es un subgrupo de G' .
2. $f^{-1}(H')$ es un subgrupo de G .
3. Si H' es un subgrupo normal de G' , entonces $f^{-1}(H')$ es un subgrupo normal de G .

Demostración. (1) Como $f(e) = e'$, donde e' es el elemento neutro de G' , es claro que $f(H) \neq \emptyset$. Sean $a', b' \in f(H)$ y $a, b \in H$ tales que $f(a) = a'$, $f(b) = b'$. Como $a'(b')^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$, entonces $a'(b')^{-1} \in f(H)$, y $f(H)$ es así un subgrupo de G' .

(2) Como $f(e) = e' \in H'$ (pues H' es un subgrupo de G'), es claro que $e \in f^{-1}(H')$, así que $f^{-1}(H') \neq \emptyset$. Ahora, si $a, b \in f^{-1}(H')$ entonces $f(a), f(b) \in H'$, de lo cual $f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \in H'$, así que $ab^{-1} \in f^{-1}(H')$.

(3) Para ver que $f^{-1}(H')$ es normal si H' lo es, sean $x \in G$ y $h \in f^{-1}(H')$, de modo que $f(h) \in H'$. Como H' es normal, $f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)f(h)f(x)^{-1} \in H'$, de lo cual $xhx^{-1} \in f^{-1}(H')$. Entonces, $f^{-1}(H')$ es normal. $\square$

Nota 5.5. Por el contrario, puede suceder que H sea normal en G sin que $f(H)$ sea normal en G' . Por ejemplo, $H = SL_n(\mathbb{R})$ es un subgrupo normal de $G = GL_n(\mathbb{R})$ (ejercicio 4.4). Sean $G' = GL_n(\mathbb{C})$ y $f : G \rightarrow G'$ la aplicación $f(x) = x$, la cual es obviamente un homomorfismo. Como se deduce del mismo ejercicio 4.4, $f(H) = H$ no es un subgrupo normal de G' . El teorema 5.3, abajo, da una condición sobre f bajo la cual $f(H)$ es normal si H lo es.

El siguiente corolario del anterior teorema resulta de observar que $\{e'\}$ es un subgrupo normal de G' .

Corolario 5.1. Si $f : G \rightarrow G'$ es un homomorfismo, $f^{-1}(\{e'\})$ es un subgrupo normal de G .

El subgrupo $f^{-1}(\{e'\})$ (el cual se escribe a veces en la forma más simple $f^{-1}(e')$) es particularmente importante, como podremos comprobarlo. Se denomina el núcleo de f y se denota con $\ker(f)$ o, simplemente, con $\ker f$:

$$\ker f := f^{-1}(\{e'\}).$$

Teorema 5.3. Si $f : G \rightarrow G'$ es un epimorfismo y H es un subgrupo normal de G , $f(H)$ es un subgrupo normal de G' .

Demostración. Sean $a' \in G$ y $h' \in f(H)$. Dado que $f(G) = G'$, existen $a \in G$ y $h \in H$ tales que $f(a) = a'$ y $f(h) = h'$, así que $a'h'(a')^{-1} = f(a)f(h)(f(a))^{-1} = f(a)f(h)f(a^{-1}) = f(aha^{-1})$. Pero entonces, como $aha^{-1} \in H$, también $a'h'(a')^{-1} = f(aha^{-1}) \in f(H)$. $\square$

Teorema 5.4. Si $f : G \rightarrow G'$ es un homomorfismo, f es un monomorfismo si y sólo si $\ker f = \{e\}$.

Demostración. Si $\ker f = \{e\}$ y $f(a) = f(b)$ entonces $f(b)^{-1}f(a) = f(b^{-1}a) = f(b^{-1}a) = e'$, así que $b^{-1}a \in \ker f$, o sea, $b^{-1}a = e$, de lo cual $a = b$. Entonces f es inyectiva. Recíprocamente, si f es inyectiva y $a \in \ker f$ entonces $f(a) = e' = f(e)$, así que $a = e$. Entonces, $\ker f = \{e\}$. $\square$

Nota 5.6. Ligados a los grupos $(\mathbb{Z}_p, +)$ existen otros grupos abelianos que no dejan de tener su importancia en diversas circunstancias (véase, por ejemplo, el capítulo 11). En verdad son, junto con otros sistemas relacionados, de gran importancia en la llamada teoría de los números. Estos son los grupos multiplicativos $(\mathbb{Z}_p^*, \cdot)$, donde $\mathbb{Z}_p^* = \mathbb{Z} \setminus \{0\}$ donde $p \geq 2$ es un número primo. De hecho, aún si $p \geq 2$ no es primo, podemos definir en $\mathbb{Z}_p$ una ley de composición por

$$(a + p\mathbb{Z})(b + p\mathbb{Z}) = ab + p\mathbb{Z},$$

o, en forma más concisa, por

$$\overline{ab} = \overline{a}\overline{b}, \text{ donde } \overline{a} = a + p\mathbb{Z}, \overline{b} = b + p\mathbb{Z}$$

Tal ley está en efecto bien definida, pues si $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$ entonces

$$\overline{ab} - \overline{a'b'} = \overline{ab - a'b' + a'b' - a'b'} = \overline{a(b - b')} + \overline{(a - a')b'} = \overline{0},$$

ya que $p \mid a(b - b')$ y $p \mid (a - a')b'$, de lo cual $\overline{ab} = \overline{a'b'}$. Es además fácil comprobar que tal ley es asociativa, conmutativa y tiene a $\overline{1}$ como elemento neutro. Puede suceder, sin embargo, que esta ley no sea clausurativa en $\mathbb{Z}_p^*$. De hecho, lo es si y sólo si p es primo. En efecto, si p no es primo y $a, b \in \mathbb{Z}$, $1 < a < p$, $1 < b < p$, son tales que $ab = p$, obviamente $\overline{ab} = \overline{0}$, pero $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$. Recíprocamente, si p es primo y $\overline{ab} = \overline{0}$, así que $p \mid ab$, necesariamente $p \mid a$ o $p \mid b$, de lo cual $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$. Es fácil ver ahora (ejercicio 5.7) que si p es primo (y sólo en tal caso), $(\mathbb{Z}_p^*, \cdot)$ es un grupo abeliano. Es posible demostrar además que $(\mathbb{Z}_p^*, \cdot)$ y $(\mathbb{Z}_{p-1}, +)$ son isomorfos (ejercicio 6.16).

Nota 5.7. Como es obvio, si $p \geq 2$ es un entero, la ley de composición (5.5), o, lo que es lo mismo, la (5.6), tiene en $\mathbb{Z}_p$ la propiedad adicional

$$\overline{a}(\overline{b} + \overline{c}) = \overline{ab} + \overline{ac}.$$

Esto permite concluir que cuando $p \geq 2$ es un primo, el sistema $(\mathbb{Z}_p, +, \cdot)$ tiene, salvo por el hecho de que $\mathbb{Z}_p \not\subseteq \mathbb{C}$, todas las propiedades de un campo numérico (capítulo 1, sección 1.9). Esto permite definir, tal como en sección 1.10 del mismo capítulo, el sistema $\mathbb{Z}_p[x]$ de los polinomios en x con coeficientes en $\mathbb{Z}_p$ y, tal como allí, se verifica, para este sistema, la validez de los teoremas 1.26 y 1.27 y de los corolarios 1.7 y 1.8. Esto implica que para todo $n \geq 1$ en $\mathbb{Z}$, la ecuación $x^n = \overline{1}$ tiene a lo sumo n soluciones en $\mathbb{Z}_p^*$. Este hecho será importante en el capítulo 11.

Nota 5.8. Si $a, b \in \mathbb{Z}$ y $b - a \in p\mathbb{Z}$ (o sea, si $p \mid b - a$), es corriente escribir

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

y decir que a es congruente con b módulo p . Es obvio que la relación $R_p = (\mathbb{Z}, G_p, \mathbb{Z})$, donde $G_p = \{(a, b) : a \in \mathbb{Z}, b \in \mathbb{Z} \text{ y } a \equiv b \pmod{p}\}$ es una relación de equivalencia en $\mathbb{Z}$ (ejercicio 1.9) y que $\mathbb{Z}/R_p = \mathbb{Z}_p$.

EJERCICIOS

5.1 Verifique que si $f : G \rightarrow G'$ y $g : G' \rightarrow G''$ son isomorfismos, también $g \circ f$ lo es, y concluya que, en una clase dada de grupos, la relación de isomorfía $G \approx G'$ si G y G' son isomorfos tiene las tres propiedades siguientes:

1. $G \approx G$.
2. Si $G \approx G'$ entonces $G' \approx G$.
3. Si $G \approx G'$ y $G' \approx G''$ entonces $G \approx G''$.

Es, por lo tanto, una relación de equivalencia (ejercicio 1.9).

5.2 Sean $(G, \cdot)$ un grupo, H un subgrupo de G , $\mathfrak{F}_0(G/H)$ el grupo de todas las aplicaciones biyectivas de G/H en sí mismo.

- a) Demuestre que si para cada $a \in G$, $T_a : G/H \rightarrow G/H$ es la aplicación $T_a(bH) = abH$, $b \in G$, entonces T_a está bien definida y $T_a \in \mathfrak{F}_0(G/H)$ (es decir, $abH = ab'H$ si y sólo si $bH = b'H$).
- b) Verifique que $T_e = I$ es la identidad de G/H , que $T_a \circ T_b = T_{ab}$ cualesquiera que sean $a, b \in G$, y que $T_a^{-1} = T_{a^{-1}}$ para todo $a \in G$.

c) Sea $T : G \rightarrow \mathfrak{F}_0(G/H)$ la aplicación $T(a) = T_a$, $a \in G$. Demuestre que T es un homomorfismo (así que $T(ab) = T(a) \circ T(b)$) y que $\ker T \subseteq H$. Más precisamente, demuestre que $\ker T = \bigcap_{a \in G} aHa^{-1}$, y que H es normal en G si y sólo si $\ker T = H$.

5.3 Sea $(G, \cdot)$ un grupo. Demuestre que para todo $a \in G$, la aplicación $\delta_a : G \rightarrow G$, dada por $\delta_a(x) = axa^{-1}$, es un isomorfismo de G sobre sí mismo, que δ_e es la aplicación idéntica de G , que $\delta_a^{-1} = \delta_{a^{-1}}$ y que $\delta_a \circ \delta_b = \delta_{ab}$. Demuestre además que un subgrupo H de G es normal si y sólo si $H = \bigcap_{a \in G} \delta_a(H) = \bigcap_{a \in G} aHa^{-1}$.

5.4 Sean $(G, \cdot)$ y δ_a , para $a \in G$, como en el ejercicio 5.3. Sea $\mathfrak{F}_0(G)$ el grupo de las aplicaciones biyectivas de G en sí mismo. Sea $\delta : G \rightarrow \mathfrak{F}_0(G)$ definida por $\delta(a) = \delta_a$. Demuestre que δ es un homomorfismo de G en $\mathfrak{F}_0(G)$ y que $\ker \delta = Z(G)$, el centro de G (ejercicio 4.7).

5.5 Sean $(G, \cdot)$ un grupo, $n \in \mathbb{Z}$, $G^n = \{a^n | a \in G\}$, $G_n = \{a \in G | a^n = e\}$. Demuestre que si $f_n(x) = x^n$ es un homomorfismo de G en sí mismo entonces G^n y G_n son subgrupos de G . De hecho, $G^n = f_n(G)$, $G_n = \ker f_n$. Demuestre además que:

- Si G es abeliano, f_n es un homomorfismo de G en sí mismo para todo $n \in \mathbb{Z}$.
- Si f_2 es un homomorfismo de G en sí mismo, G es abeliano. Lo mismo es cierto si f_{-1} lo es.
- Si f_m es un homomorfismo de G en sí mismo para $m = n, n+1, n+2$, donde $n \in \mathbb{Z}$ está fijo, entonces G es abeliano.
- Si f_3 y f_5 son homomorfismos de G en sí mismo, G es abeliano.

5.6 Sea $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, y considere en K la operación $a * b = a + b + ab$ (llamada la "adiplicación"). Demuestre que $(*)$ es clausurativa, asociativa, admite un elemento neutro, 0, pero no es invertiva con respecto a 0. Demuestre, sin embargo, que $(K^0, *)$, $K^0 = K \setminus \{-1\}$, es un grupo, y que $f : K^* \rightarrow K^0$ dada por $f(x) = x - 1$ es un isomorfismo de $(K^*, \cdot)$ sobre $(K^0, *)$. (Indicación. Observe que $a * b = (a+1)(b+1) - 1$.)

5.7 Sean p un número primo y $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$. Demuestre que la ley de composición $(a + p\mathbb{Z})(b + p\mathbb{Z}) = ab + p\mathbb{Z}$, o sea, $\overline{a}\overline{b} = \overline{ab}$, donde $\overline{a} =$

$a + p\mathbb{Z}$, tiene las propiedades cancelativas tanto a izquierda como a derecha en $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\overline{0}\}$, y concluya que $(\mathbb{Z}_p^*, \cdot)$ es un grupo abeliano cuyo elemento neutro es $\overline{1}$. (Indicación. Véase el teorema 2.11.)

5.8 Demuestre que cuando p es primo, la ley de composición $(\cdot)$ en $\mathbb{Z}_p^*$ (ejercicio 5.7) satisface

$$\overline{a}\overline{b} = \overline{r(ab, p)},$$

donde $r(ab, p)$ es el resto de dividir ab por p . Demuestre además que

$$(\overline{a})^{p-1} = \overline{a^{p-1}} = \overline{1}$$

para todo $a \in \mathbb{Z}$ tal que $\overline{a} \neq \overline{0}$, y concluya que $\overline{a^{p-2}}$ es, para todo $a \in \mathbb{Z}$ tal que $\overline{a} \neq \overline{0}$, el inverso de $\overline{a}$ en $(\mathbb{Z}_p^*, \cdot)$. (Nota. La relación $\overline{a^{p-1}} = \overline{1}$, válida para todo $a \in \mathbb{Z}$ con $\overline{a} \neq \overline{0}$, se puede expresar diciendo (véase la nota 5.8) que si a no es divisible por p entonces $a^{p-1} \equiv 1 \pmod{p}$, lo cual se conoce como el Pequeño teorema de Fermat). Como es claro entonces, $a^p \equiv a \pmod{p}$, aún si $p \mid a$.

5.9 Para cada $m \in \mathbb{Z}$, sea $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$. Demuestre que $(\mathbb{Z}_m^*, \cdot)$, donde $(\cdot)$ está dada por $(a + m\mathbb{Z})(b + m\mathbb{Z}) = ab + m\mathbb{Z}$, o sea, por $\overline{a}\overline{b} = \overline{ab}$, es un grupo si y sólo si m es un número primo.

5.10 Sean p un primo y $a \in \mathbb{N}$ tal que p no divide a a y p no divide a $(a^m - 1)$ para $m = 1, 2, 3, \dots, p-2$. Tal es el caso, por ejemplo, de $p = 5$ y $a = 2$. Demuestre que entonces $f(n) = \overline{a}^n$ es un epimorfismo de $(\mathbb{Z}, +)$ sobre $(\mathbb{Z}_p^*, \cdot)$ tal que $\ker f = (p-1)\mathbb{Z}$. En particular, $f(n) = \overline{2}^n$ es un epimorfismo de $(\mathbb{Z}, +)$ sobre $(\mathbb{Z}_5^*, \cdot)$ tal que $\ker f = 4\mathbb{Z}$.

5.11 Sean $G = S_3$ el grupo simétrico de tres objetos (ejercicio 2.12), $g : G \rightarrow G$ la aplicación $g(x) = x$, $x \in G$, $H = \{e, d, f\}$. Demuestre que H es un subgrupo normal de G y que $aH = bH$. Concluya que no es posible definir una aplicación $\overline{g} : G/H \rightarrow G$ tal que $\overline{g}(xH) = g(x)$ para todo $x \in G$.

5.12 Sean $n \geq 2$ y $\mathbb{H}$ el subgrupo de $GL_n(\mathbb{R})$ de las matrices A con $\text{Det}(A) > 0$. Demuestre que $\mathbb{H}$ es un subgrupo normal de $GL_n(\mathbb{R})$ y que si $f : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ es la aplicación $f(A) = \text{Det}(A)$, no es posible definir una aplicación $\overline{f} : GL_n(\mathbb{R})/\mathbb{H} \rightarrow \mathbb{R}^*$ tal que $\overline{f}(AH) = f(A)$ para todo $A \in GL_n(\mathbb{R})$. ¿Es esto posible si $\mathbb{H} = SL_n(\mathbb{R})$? Si lo es, ¿es la aplicación $\overline{f}$ resultante un homomorfismo? ¿Es un isomorfismo?

Capítulo 6

Los teoremas de isomorfía

Sean $f : G \rightarrow G'$ un homomorfismo y H un subgrupo normal de G . Sea $\varphi : G \rightarrow G/H$ el epimorfismo canónico $\varphi(a) = aH$. No siempre es posible determinar una aplicación $\bar{f} : G/H \rightarrow G'$ por $\bar{f}(aH) = f(a)$ para todo $a \in G$, pues puede suceder que $aH = bH$ y que $f(a) \neq f(b)$ (ejercicios 5.11 y 5.12), con lo cual $\bar{f}$ no quedaría bien definida. Para que tal definición de $\bar{f}$ sea posible es necesario que si $aH = bH$, o sea, si $b^{-1}a \in H$, entonces $b^{-1}a \in \ker(f)$, o sea, $f(b)^{-1}f(a) = f(b^{-1}a) = e'$, pues esto último implica que $f(a) = f(b)$. Pero, para que todo esto se dé, basta evidentemente que $H \subseteq \ker(f)$. En tal situación se tiene además que $\bar{f}$ es automáticamente un homomorfismo, pues $\bar{f}((aH)(bH)) = \bar{f}((ab)H) = f(ab) = f(a)f(b) = \bar{f}(aH)\bar{f}(bH)$.

Supongamos recíprocamente que existe un homomorfismo $\bar{f} : G/H \rightarrow G'$ tal que $\bar{f}(aH) = f(a)$ para todo $a \in G$. Si $x \in H$ entonces $\bar{f}(xH) = \bar{f}(eH) = f(e) = e'$, lo cual implica que $f(x) = e'$, o sea, que $x \in \ker(f)$. Entonces, $H \subseteq \ker(f)$. Es decir, $\bar{f}$ existe si y sólo si $H \subseteq \ker(f)$.

Nótese finalmente que $\bar{f}(aH) = \bar{f}(\varphi(a)) = \bar{f} \circ \varphi(a)$. Por lo tanto, decir que $\bar{f}(aH) = f(a)$, sea, que $\bar{f} \circ \varphi(a) = f(a)$, para todo $a \in G$, equivale a decir que $\bar{f} \circ \varphi = f$. Hemos demostrado por lo tanto el siguiente teorema.

Teorema 6.1. Sean G y G' grupos, $f : G \rightarrow G'$ un homomorfismo, H un subgrupo normal de G , G/H el grupo cociente de G por H , y $\varphi : G \rightarrow G/H$ el epimorfismo canónico. Para que exista un homomorfismo $\bar{f} : G/H \rightarrow G'$ tal que $\bar{f} \circ \varphi = f$, o sea, tal que el diagrama

$$\begin{array}{ccc}
 & G/H & \\
 \varphi \nearrow & & \searrow \bar{f} \\
 G & \xrightarrow{f} & G'
 \end{array} \quad (6.1)$$

sea conmutativo, es necesario y suficiente que $H \subseteq \ker(f)$.

Supóngase ya que $H \subseteq \ker f$, así que $\bar{f}$ existe. Si $H = \ker(f)$ entonces $\bar{f}$ es un monomorfismo, pues si $\bar{f}(aH) = \bar{f}(bH)$ entonces $f(a) = f(b)$, o sea $b^{-1}a \in \ker(f)$, de lo cual $b^{-1}a \in H$, y así $aH = bH$. Recíprocamente, si f es un monomorfismo y $a \in \ker(f)$ entonces $\bar{f}(aH) = f(a) = e'$, o sea, $\bar{f}(aH) = \bar{f}(eH)$, así que $aH = eH = H$ (pues $\bar{f}$ es inyectiva). Esto implica que $a \in H$, es decir que $\ker(f) \subseteq H$, de lo cual $\ker(f) = H$ (pues ya sabemos que $H \subseteq \ker(f)$). Se tiene entonces el siguiente teorema.

Teorema 6.2. (Primer teorema de isomorfía). Si $f : G \rightarrow G'$ es un epimorfismo y $K = \ker(f)$, existe un isomorfismo $\bar{f}$ de G/K sobre G' tal que $\bar{f}(aK) = f(a)$ para todo $a \in G$.

Si $\varphi : G \rightarrow G/K$ es el epimorfismo canónico, se tiene entonces el diagrama conmutativo

$$\begin{array}{ccc}
 & G/K & \\
 \varphi \nearrow & & \searrow \bar{f} \\
 G & \xrightarrow{f} & G'
 \end{array} \quad (6.2)$$

en el cual $\bar{f}$ es un isomorfismo de G/K sobre G' . Si f no es sobreyectivo, $\bar{f}$ es aún un isomorfismo de G/K sobre $f(G)$.

El primer teorema de isomorfía se expresa usualmente diciendo que un grupo G' es la imagen homomorfa de otro, G , si y sólo si G' es un grupo cociente de G .

Ejemplo 6.1. Si $(\mathbb{R}^*, \cdot)$ es el grupo multiplicativo de los números reales no nulos y $(\mathbb{R}_+^*, \cdot)$ el de los números reales estrictamente positivos, $K = \{-1, 1\}$

es un subgrupo (normal) de $\mathbb{R}^*$ y $\mathbb{R}^*/K \approx \mathbb{R}_+^*$. En efecto, $f(x) = |x|$ es un epimorfismo de $\mathbb{R}^*$ sobre $\mathbb{R}_+^*$ (pues $f(|x|) = |x|$ y $\ker(f) = K = \{-1, 1\}$). Esto expresa, de otra manera, el hecho de que todo número real x se escribe en la forma $x = \pm|x|$. También $f(z) = |z|$ es un epimorfismo de $(\mathbb{C}^*, \cdot)$ sobre $(\mathbb{R}_+^*, \cdot)$ y, como $\ker(f) = T = \{z \in \mathbb{C} : |z| = 1\}$, entonces $\mathbb{C}^*/T \approx \mathbb{R}_+^*$, que es otra manera de decir que todo número complejo z se escribe en la forma $z = rw$ donde $r > 0$ y $w \in T$. A su vez, $f(x) = e^{2\pi ix}$ es un epimorfismo de $(\mathbb{R}, +)$ sobre $(T, \cdot)$, y como $K = \ker(f) = \{x \in \mathbb{R} : e^{2\pi ix} = 1\} = \mathbb{Z}$, entonces $\mathbb{R}/\mathbb{Z} \approx T$. Como además $f(z) = e^{2\pi iz}$ es un epimorfismo de $(\mathbb{C}, +)$ sobre $(\mathbb{C}^*, \cdot)$ (nótese al respecto que si $z \in \mathbb{C}^*$ y $z = |z|e^{i\theta}$, $\theta \in \mathbb{R}$, entonces $f(\xi) = z$, donde $\xi = \frac{1}{2\pi i}(\log |z| + i\theta)$), y como $\ker(f) = \mathbb{Z}$, entonces $\mathbb{C}/\mathbb{Z} \approx \mathbb{C}^*$. Obsérvese finalmente que $f(x) = e^{\frac{2\pi i}{n}x}$, donde $n > 0$ es un entero, es un epimorfismo de $(\mathbb{Z}, +)$ sobre $(T_n, \cdot)$, el grupo de las raíces n -ésimas de la unidad, y que $\ker(f) = n\mathbb{Z}$, así que $\mathbb{Z}/n\mathbb{Z} \rightarrow T_n$ es un isomorfismo, como es natural.

Ejemplo 6.2. Sea $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Como $f(A) = \det(A)$ es un epimorfismo de $(GL_n(K), \cdot)$ sobre $(K^*, \cdot)$ y $\ker(f) = SL_n(K)$ (ejemplo 4.1), entonces $GL_n(K)/SL_n(K) \approx K^*$. De la misma manera se verifica que para $K = \mathbb{Q}, \mathbb{R}, GL_n(K)/|SL_n|(K) \approx K_+^* = K_+ \setminus \{0\}$.

Ejemplo 6.3. Si H es un subgrupo normal de G y $\varphi : G \rightarrow G/H$ es el epimorfismo canónico entonces $\ker \varphi = H$, y si $\bar{\varphi}$ es el isomorfismo de G/H en G/H tal que $\bar{\varphi} \circ \varphi = \varphi$, es decir, que hace conmutativo el diagrama

$$\begin{array}{ccc}
 & G/H & \\
 \varphi \nearrow & & \searrow \bar{\varphi} \\
 G & \xrightarrow{\varphi} & G/H
 \end{array} \quad (6.3)$$

entonces $\bar{\varphi}$ es la identidad de G/H .

El siguiente corolario del teorema 6.1 es frecuentemente útil.

Corolario 6.1 (Segundo teorema de isomorfía). Sean $f : G \rightarrow G'$ un epimorfismo, $K = \ker(f)$, H' un subgrupo de G' y $H = f^{-1}(H')$. Entonces K es un subgrupo normal de H y $H/K \approx H'$.

Demostración. Si $f' : H \rightarrow H'$, es la aplicación $f'(x) = f(x)$, f' está bien definida, pues si $x \in f^{-1}(H')$ entonces $f(x) \in H'$, y es obviamente un homomorfismo. Es también un epimorfismo, pues como f lo es, dado $y \in H'$, existe $x \in G$ tal que $y = f(x)$, y es claro entonces que $x \in f^{-1}(H') = H$, así que $f'(x) = y$. Es claro además que $\ker(f') \subseteq \ker(f)$. Por otra parte, si $x \in \ker(f)$, entonces $x \in f^{-1}(H')$, pues $f^{-1}\{e'\} \subseteq f^{-1}(H')$, y como entonces $f'(x) = f(x) = e'$, también $x \in \ker(f')$, así que $\ker(f') = \ker(f)$. Entonces $H/\ker(f') \approx f'(H) = H'$. $\square$

Nota 6.1. Se deduce que si $f : G \rightarrow G'$ es un epimorfismo, existe una correspondencia biyectiva entre los subgrupos de G' y los subgrupos de G que contienen a $K = \ker f$. Esta correspondencia asocia al subgrupo H' de G' el subgrupo $H = f^{-1}(H')$ de G . Tal correspondencia asigna a subgrupos normales de G' , subgrupos normales de G que contienen a K . Nótese además que $f^{-1}(H')/K \approx H'$, como resulta del corolario 6.1.

Cuando se aplica al epimorfismo canónico $\varphi : G \rightarrow G/N$, donde N es normal en G , tal correspondencia asigna al subgrupo $\overline{M}$ de G/N el subgrupo $M = \varphi^{-1}(\overline{M})$ de G , el cual contiene a N , y el cual es normal en G si $\overline{M}$ es normal en G/N . Además, $M/N \approx \overline{M}$. Todo esto resulta de observar que $N = \ker \varphi$. Los resultados discutidos en esta nota se conocen a veces como el *teorema de correspondencia*.

Nota 6.2. Si $f : G \rightarrow G'$ es un epimorfismo con $K = \ker f$, H es un subgrupo de G y $H' = f(H)$, entonces $H \subseteq f^{-1}(H')$ (ejercicio 1.6), pero, en general, $H \neq f^{-1}(H')$. De hecho, $H = f^{-1}(H')$ si y sólo si $K \subseteq H$. En efecto, si $K \subseteq H$ y $x \in f^{-1}(H')$ entonces $f(x) \in H'$, así que $f(x) = f^{-1}(y)$ para algún $y \in H$; esto implica que $f(y^{-1}x) = e'$, o sea, que $y^{-1}x \in K$, de lo cual $y^{-1}x \in H$, y entonces $x \in yH = H$. Esto demuestra que $f^{-1}(H') \subseteq H$, lo cual asegura que $H = f^{-1}(H')$. Por otra parte, como $K = f^{-1}\{e'\} \subseteq f^{-1}(H')$, es claro que $K \subseteq H$ si $H = f^{-1}(H')$. Si $K \not\subseteq H$ de todas maneras KH es un subgrupo de G que contiene a K y obviamente $KH \subseteq f^{-1}(H')$ (pues $H, K \subseteq f^{-1}(H')$). Como además se verifica obviamente que $f(KH) = f(H) = H'$, lo dicho anteriormente asegura que $KH = f^{-1}(H')$. Es decir, si $K \not\subseteq H$, $f^{-1}(f(H)) \neq H$, pero $f^{-1}(f(H)) = KH$. Nótese que entonces $KH/H \approx f(H) = H'$. Evidentemente $KH = H$ si y sólo si $K \subseteq H$. Cuando lo observado arriba se aplica al epimorfismo $\varphi : G \rightarrow G/N$, se concluye que si H es un subgrupo de G y $H' = \varphi(H)$, entonces $\varphi^{-1}(H') = NH = H$ y $NH/N \approx H'$, con $\varphi^{-1}(H') = H$ si y sólo si $N \subseteq H$.

Como una aplicación del anterior corolario tenemos el siguiente teorema,

que, como el de Cauchy, es también un recíproco parcial del teorema de Lagrange.

Teorema 6.3. Si p es un primo y G es un grupo abeliano de orden mp^n donde $n \geq 0$ y $p \nmid m$, G tiene, para cada $0 \leq k \leq n$ un subgrupo de orden p^k .

Demostración. El grupo G tiene un elemento a de orden p (teorema 4.3) y $[a]$ es un subgrupo normal de G de orden p . Sea $G' = G/[a]$. Entonces G' tiene orden mp^{n-1} , y, por inducción, podemos suponer que para cada $0 \leq k \leq n-1$, G' tiene un subgrupo H' de orden p^k . Sean $\varphi : G \rightarrow G/[a]$ el epimorfismo canónico y $H = \varphi^{-1}(H')$. Como $H/\ker \varphi \approx H'$ y $\ker \varphi = [a]$, entonces H tiene orden p^{k+1} , y es un subgrupo de G . Esto demuestra que G tiene subgrupos de orden p^k para todo $0 \leq k \leq n$. $\square$

El anterior teorema se conoce como el *primer teorema de Sylow para los grupos abelianos*. Puede enunciarse también diciendo que si G es un grupo abeliano finito, p es un primo y p^n , $n \geq 0$, es la máxima potencia de p que divide a $o(G)$, entonces G tiene subgrupos de orden p^k para todo $0 \leq k \leq n$, o, aún, diciendo que G tiene subgrupos de orden p^k para todo $k \geq 0$ tal que $p^k \mid o(G)$. Posteriormente demostraremos que el teorema 6.3 es aún cierto si G no es abeliano.

Teorema 6.4. (Tercer teorema de isomorfía)). Sean G un grupo, M y N subgrupos de G . Supóngase que N es un subgrupo normal de G . Entonces MN es un subgrupo de G y N es normal en MN . Además $M \cap N$ es un subgrupo normal de M y

$$MN/N \approx M/M \cap N. \quad (6.4)$$

Se deduce que si M y N son finitos entonces MN es finito y $o(MN) = (o(M)o(N))/o(M \cap N)$.

Demostración. Ya sabemos (teorema 4.4) que MN , es un subgrupo de G y que N , es un subgrupo normal de MN . Sea $\varphi : M \rightarrow MN/N$, dada por $\varphi(a) = aN$. Es claro que φ es un homomorfismo. De hecho, φ es un epimorfismo, pues una clase lateral izquierda de N en MN , es de la forma $(ab)N$ donde $a \in M$ y $b \in N$ y, como $b \in N$, entonces $(ab)N = a(bN) = aN = \varphi(a)$. Veamos, finalmente, que $\ker(\varphi) = M \cap N$. Si $a \in \ker(\varphi)$, o sea, si $\varphi(a) = aN = N$, donde $a \in M$, entonces $a \in N$, así que $a \in M \cap N$. Recíprocamente, si $a \in M \cap N$ entonces $aN = N$, así que $\varphi(a) = N$, y entonces

$a \in \ker(\varphi)$. Esto demuestra la última afirmación, y completa (en virtud del teorema 6.2) la demostración del teorema. $\square$

Nota 6.3. Si el grupo G es un grupo abeliano aditivo, es corriente escribir $M + N$ en lugar de MN , y el teorema anterior toma la forma

$$M/M \cap N \approx (M + N)/N. \quad (6.5)$$

Como corolarios del anterior teorema tenemos:

Corolario 6.2. Si M, N son subgrupos finitos de un grupo G , $M \cap N = \{e\}$ y N es normal en G , entonces MN es un subgrupo finito de G y $o(MN) = o(M)o(N)$.

Corolario 6.3. Si M y N son subgrupos finitos de un grupo G , N es normal en G y $\text{mcd}(o(M), o(N)) = 1$, entonces MN es un subgrupo de G y $o(MN) = o(M)o(N)$.

Demostración. Como $o(M \cap N)$ divide a $o(M)$ y a $o(N)$, necesariamente $o(M \cap N) = 1$ (o sea, $M \cap N = \{e\}$), así que $o(MN) = o(M)o(N)$. $\square$

Corolario 6.4. Si $(G, \cdot)$ es un grupo abeliano finito, para cada divisor m de $o(G)$ existe un subgrupo M , de G con $o(M) = m$.

Demostración. Supóngase que $o(G) = p_1^{m_1} \cdots p_l^{m_l}$, donde los $p_i, i = 1, 2, \dots, l$, son primos distintos, y supóngase que $m = p_1^{k_1} \cdots p_l^{k_l}$, donde $0 \leq k_i \leq m_i, i = 1, 2, \dots, l$. Para cada $i = 1, 2, \dots, l$, existe un subgrupo M_i de G con $(M_i) = p_i^{k_i}$ (teorema 6.3). Como $\text{mcd}(o(M_1), o(M_2)) = 1$, $M_1 M_2$ es un subgrupo de G de orden $p_1^{k_1} p_2^{k_2}$. Como a su vez, $\text{mcd}(o(M_1 M_2), o(M_3)) = 1$, también $M_1 M_2 M_3$ es un subgrupo de G con $o(M_1 M_2 M_3) = p_1^{k_1} p_2^{k_2} p_3^{k_3}$. Continuando de esta manera se llega a que $M = M_1 M_2 \cdots M_l$ es un subgrupo de G con $o(M) = m$. $\square$

Corolario 6.5. Si G es un grupo abeliano finito con $o(G) = p_1^{m_1} \cdots p_l^{m_l}$, donde los $p_i, i = 1, 2, \dots, l$, son primos distintos, y $m_i \geq 0$, entonces $G = M_1 M_2 \cdots M_l$, donde M_i es un subgrupo de G con $o(M_i) = p_i^{m_i}, i = 1, 2, \dots, l$.

Relacionado con el corolario anterior, tenemos el siguiente.

Corolario 6.6. Si G es un grupo abeliano con $o(G) = p_1 \cdots p_l$, donde $p_1, \dots, p_l$ son primos distintos, entonces $G = M_1 M_2 \cdots M_l$, donde el subgrupo

M_i , de orden p_i , es cíclico para todo $i = 1, 2, \dots, l$. Además, G mismo es cíclico.

Demostración. Si M_i es un subgrupo de G de orden $p_i, i = 1, 2, \dots, l$, M_i es cíclico (teorema 3.10), digamos, $M_i = [a_i]$, $o(a_i) = p_i$. Pero entonces, $a = a_1 a_2 \cdots a_l$ tiene orden $p_1 \cdots p_l$. En efecto, si no, deberá existir $1 \leq i \leq l$ tal que $p_i \nmid o(a)$, y si $m = o(G)/p_i$ entonces $o(a) \mid m$, así que $e = a^m = a_1^m a_2^m \cdots a_l^m = a_i^m$ (ya que $o(a_j) = p_j$ divide a m si $j \neq i$), lo cual es absurdo (pues p_i no divide a m). $\square$

Si G es un grupo abeliano finito, p es un primo y H es un subgrupo de G de orden $p^n, n \geq 0$, se dice que H es un p -subgrupo de G . Si p^n es la máxima potencia de p que divide a $o(G)$ (en cuyo caso $o(G) = mp^n, p \nmid m$), se dice entonces que H es un p -subgrupo de Sylow de G . Los subgrupos M_i de G en el corolario 6.4 anterior son p_i -subgrupos de G , y aquellos en el corolario 6.5 son p_i -subgrupos de Sylow. Los resultados siguientes son consecuencia de los anteriores.

Corolario 6.7. Si $(G, \cdot)$ es un grupo abeliano finito, p es un primo, P es un p -subgrupo de Sylow de G y $a \in G$ es tal que $o(a)$ es una potencia de p , entonces $a \in P$.

Demostración. Podemos suponer que $o(G)$ es como en el corolario 6.5, que $p = p_1$ y que $P = M_1$. Como $G = M_1 \cdots M_l$, existirán $x_i \in M_i, i = 1, \dots, l$, tales que $a = x_1 \cdots x_l$, de lo cual $x_1^{-1} a = x, x = x_2 \cdots x_l$. Pero evidentemente $\text{mcd}(o(x), p) = 1$, y como $o(x_1^{-1} a)$ deberá ser una potencia de p , sólo queda que $o(x_1^{-1} a) = 1$, de lo cual $x_1^{-1} a = e$, y así, $a = x_1 \in P$. $\square$

Corolario 6.8. Sean $(G, \cdot)$ un grupo abeliano finito, p un primo, P un p -subgrupo de Sylow de G , H un p -subgrupo de G . Entonces $H \subseteq P$, y P es el único p -subgrupo de Sylow de G .

Demostración. Si $a \in H$, $o(a)$ es una potencia de p , así que $a \in P$. Entonces $H \subseteq P$, y es claro que si H es también un p -subgrupo de Sylow de G , necesariamente $H = P$. $\square$

El teorema 6.3 así como los corolarios 6.7 y 6.8 son casos especiales de los teoremas de Sylow que se consideran en el capítulo 10.

Definición 6.1. Sean $M_1, \dots, M_l$ subgrupos normales de un grupo G , tales que $G = M_1 \cdots M_l$. Para cada $1 \leq i \leq l$, sea $\widehat{M}_i$ el producto de los subgrupos

M_j para $j \neq i$. Si

$$M_i \cap \widehat{M}_i = \{e\}, i = 1, 2, \dots, l, \quad (6.6)$$

se dice que G es el producto directo interno de los subgrupos M_i y que cada M_i es un factor directo interno de G .

Como $M_j \subseteq \widehat{M}_i$ si $i \neq j$, se deduce que si G es el producto directo interno de sus subgrupos M_i $i = 1, 2, \dots, l$, entonces

$$M_i \cap M_j = \{e\}, i \neq j; \quad (6.7)$$

pero esta última condición no garantiza, como veremos en el capítulo 7, que (6.6) sea válida (ejercicio 7.8. Véase también el ejercicio 8.19).

Es claro, por ejemplo, que G en los corolarios 6.5 y 6.6 es el producto directo interno de los subgrupos M_i , pues evidentemente $\text{mcd}(o(M_i), o(\widehat{M}_j)) = 1$ si $i \neq j$. Este hecho es particularmente interesante en el caso del corolario 6.6, pues los subgrupos M_i son cíclicos. Como veremos posteriormente, todo grupo abeliano finito es el producto directo interno de subgrupos cíclicos. Esto, si obvio cuando $o(G) = p_1 \cdots p_l$, donde los p_i son primos distintos, está lejos de ser evidente si $o(G)$ incluye potencias superiores de uno o más primos, y se conoce como el teorema estructural de los grupos abelianos finitos (véase el capítulo 7).

El teorema 6.5 siguiente es útil dentro del contexto de los productos directos internos. Necesitaremos en su demostración el siguiente lema.

Lema 6.1. Si M y N son subgrupos normales de un grupo $(G, \cdot)$ y $M \cap N = \{e\}$, entonces $ab = ba$ cualesquiera que sean $a \in M$ y $b \in N$.

Demostración. Si $a \in M$ y $b \in N$, también $a^{-1} \in M$ y $b^{-1} \in N$, y de $(ab)(ba)^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1}$ y de la normalidad de M y N se deduce que $(ab)(ba)^{-1} \in M \cap N$. Entonces $(ab)(ba)^{-1} = e$, y así $ab = ba$. $\square$

Nota 6.4. Si un subgrupo M de G es el producto directo interno de los subgrupos normales M_i de G , tanto los subgrupos $\widehat{M}_i$ como M son subgrupos normales de G . Esto resulta inmediatamente de la relación

$$a(x_1x_2 \dots x_n)a^{-1} = (ax_1a^{-1})(ax_2a^{-1}) \dots (ax_na^{-1}), \quad (6.8)$$

válida para $a, x_1, x_2, \dots, x_n \in G$.

Teorema 6.5. Sean G un grupo, $M_1, \dots, M_n$ subgrupos de G . Las afirmaciones siguientes son equivalentes:

1. El grupo G es el producto directo interno de los subgrupos M_i , $i = 1, 2, \dots, n$.
2. Los subgrupos $M_1, \dots, M_n$ son normales en G con $M_i \cap M_j = \{e\}$ si $i \neq j$, y todo elemento $x \in G$ se escribe de una y sólo una manera en la forma $x = a_1a_2 \dots a_n$, donde $a_i \in M_i$, $i = 1, 2, \dots, n$.

Demostración. Si 1. se satisface, los M_i , $i = 1, 2, \dots, n$, son normales en G , $M_i \cap M_j = \{e\}$ si $i \neq j$, y $G = M_1M_2 \dots M_n$, así que todo $x \in G$ se escribe al menos de una manera en la forma requerida. Ahora, si $x = a_1a_2 \dots a_n = b_1b_2 \dots b_n$ donde $a_i, b_i \in M_i$ es claro que $b_1^{-1}a_1 = (b_2 \dots b_n)(a_2 \dots a_n)^{-1} \in \widehat{M}_1$, así que $b_1^{-1}a_1 = e$. Entonces $a_1 = b_1$ y $a_2 \dots a_n = b_2 \dots b_n$, y continuando de esta manera se llega a que $b_2^{-1}a_2 \in \widehat{M}_2, \dots, b_{n-1}^{-1}a_{n-1} \in \widehat{M}_{n-1}$ y $a_n = b_n$, o sea, a que $a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$. Esto demuestra 2.

Para ver que $2. \Rightarrow 1.$, obsérvese que 2. implica que $G = M_1M_2 \dots M_n$, y si $x \in M_i \cap \widehat{M}_i$, se tendría que $x = a_1a_2 \dots a_{i-1}a_{i+1} \dots a_n$, $a_j \in M_j$, $j \neq i$. Pero si $y \in M_i$ entonces $ya_j = a_jy$ para todo $j \neq i$ (lema 6.1), de lo cual $e = a_1 \dots a_{i-1}x^{-1}a_{i+1} \dots a_n$, $x \in M_i$. Entonces $x^{-1} = a_j = e$ para todo $j \neq i$, así que $x = e$. $\square$

Nota 6.5. Es fácil verificar, usando como guía la demostración del corolario 6.6, que si G es el producto directo interno de los subgrupos cíclicos M_i , $i = 1, 2, \dots, n$, y si $\text{mcd}(o(M_i), o(M_j)) = 1$, $i \neq j$, entonces G mismo es cíclico. No se pide que $o(M_i)$ sea primo.

Supóngase ahora que M y N son subgrupos normales de G y que $M \subseteq N$. Entonces es posible definir una aplicación $f: G/M \rightarrow G/N$ tal que $f(aM) = aN$. En efecto, si $aM = bM$ entonces $b^{-1}a \in M$, de lo cual $b^{-1}a \in N$, y así $aN = bN$. Tal aplicación resulta ser un homomorfismo, pues $f((aM)(bM)) = f((ab)M) = abN = (aN)(bN) = f(aM)f(bM)$. Además, $\ker(f) = N/M = \{aM | a \in N\}$. En efecto, si $aM \in \ker(f)$, o sea, si $f(aM) = aN = N$, entonces $a \in N$, así que $aM \in N/M$. Por otra parte, si $aM \in N/M$, es decir, si $aM = bM$ con $b \in N$, entonces $b^{-1}a \in M$, de lo cual $b^{-1}a \in N$, así que $aN = bN = N$, o sea, $f(aM) = N$, y entonces $aM \in \ker(f)$. Como f es un epimorfismo, el teorema 6.2 implica entonces el teorema siguiente.

Teorema 6.6. (Cuarto teorema de isomorfía). Si M y N son subgrupos normales de G tales que $M \subseteq N$, entonces

$$(G/M)/(N/M) \approx G/N. \quad (6.9)$$

Demostración. Sea $f : G/M \rightarrow G/N$ el epimorfismo dado por $f(aM) = aN$, como arriba, y sea $\tilde{f}$ para f dado como en el teorema 6.2. Entonces $\tilde{f} : (G/M)/\ker(f) \rightarrow G/N$ es un isomorfismo. Como $\ker(f) = N/M$, el teorema queda demostrado. $\square$

A manera de apéndice, observamos que las ideas que conducen al anterior resultado pueden generalizarse, ligeramente, para establecer el siguiente teorema, cuya verificación dejamos al lector interesado.

Teorema 6.7. (Quinto teorema de isomorfía). Sean G y G' grupos, $f : G \rightarrow G'$ un homomorfismo, M un subgrupo normal de G y N un subgrupo normal de G' . Para que exista un homomorfismo $\tilde{f} : G/M \rightarrow G'/N$ tal que $\tilde{f}(aM) = f(a)N$ para todo $a \in G$, es necesario y suficiente que $f(M) \subseteq N$, o, lo que es lo mismo, que $M \subseteq f^{-1}(N)$. En tales circunstancias $\ker(\tilde{f}) = f^{-1}(N)/M$ y si f es un epimorfismo entonces $\tilde{f}$ también lo es, y

$$G/M/f^{-1}(N)/M \approx G'/N \quad (6.10)$$

mediante el isomorfismo $\tilde{\tilde{f}}$ obtenido de $\tilde{f}$ por aplicación del teorema 6.2.

Definición 6.2. Se dice que el homomorfismo $\tilde{f}$ en el anterior teorema se obtiene de f por paso a los cocientes.

Nota 6.6. Si G, G', M, N y f son como en el teorema anterior, y si $\varphi : G \rightarrow G/M$ y $\psi : G' \rightarrow G'/N$ son los epimorfismos canónicos, el homomorfismo $\tilde{f}$ obtenido de f por paso a los cocientes es aquél que hace conmutativo el diagrama

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \varphi \uparrow & & \downarrow \psi \\ G/M & \xleftarrow{\tilde{f}} & G'/N \end{array} \quad (6.11)$$

EJERCICIOS

- 6.1 Demuestre que el teorema 6.1 es válido para un subgrupo normal H de G si y sólo si $f(H) = \{e'\}$. Demuestre entonces que $\tilde{f}$, como en el teorema 6.1, es el único homomorfismo $g : G/H \rightarrow G'$ que hacen conmutativo el diagrama en el enunciado del teorema. Sean $N \subseteq M$ subgrupos de un grupo G . Demuestre que aún si M y N no son normales en G , $[G : N]/[G : M] = [M : N]$, así que $[G : M][G : N]$ y $[M : N][G : N]$.
- 6.2 Sean $(G, \cdot)$ un grupo abeliano, $m \in \mathbb{Z}$. Demuestre que si G_m y G^m son como en el ejercicio 3.10, entonces $G/G_m \approx G^m$. Véase el ejercicio 5.5 (e). ¿Es cierto lo anterior si G no es abeliano pero $f(a) = a^m$ es un homomorfismo de G en sí mismo?
- 6.3 Verifique los siguientes isomorfismos de grupos: $\mathbb{Z}_3^* \approx \mathbb{Z}_2$, $\mathbb{Z}_5^* \approx \mathbb{Z}_4$, $\mathbb{Z}_7^* \approx \mathbb{Z}_6$ (véanse, al respecto, los ejercicios 5.7, 5.8 y 5.9).
- 6.4 Sean $(G, \cdot)$ un grupo, $\mathcal{F}_0(G)$ el grupo de las aplicaciones biyectivas de G en sí mismo. Demuestre que $G/Z(G)$ es isomorfo al subgrupo $\mathcal{F} = \{\delta_a | a \in G\}$ de $\mathcal{F}_0(G)$, donde $\delta_a : G \rightarrow G$ es, para cada $a \in G$, el isomorfismo $\delta_a(x) = axa^{-1}$ de G sobre sí mismo (véanse los ejercicios 5.3 y 5.4). Concluya que si $o(G) = n < \infty$ entonces $n > o(\mathcal{F})$ si y sólo si $o(Z(G)) > 1$. Más aún, demuestre que $o(Z(G)) = n/o(\mathcal{F})$.
- 6.5 Sean $(G, \cdot)$ un grupo finito y H un subgrupo de G . Sea $n = [G : H]$ el índice de H en G . Demuestre que si $o(G) \nmid n!$, existe un subgrupo normal N de G , $N \neq \{e\}$, tal que $N \subseteq H$. Demuestre, de hecho, que $N = \bigcap_{a \in G} aHa^{-1} \neq \{e\}$ y es normal. (Indicación. Véase el ejercicio 5.2.)
- 6.6 Sean $(G, \cdot)$ un grupo infinito, H un subgrupo de G tal que $[G : H] < \infty$. Demuestre que existe un subgrupo normal infinito M de G , $M \subseteq H$, tal que $[G : M] < \infty$. Demuestre, de hecho, que si $M = \bigcap_{a \in G} aHa^{-1}$ entonces $M \subseteq H$, M es normal en G y $[G : M] < \infty$, y concluya que M es infinito.
- 6.7 Sean G un grupo, H un subgrupo normal de G , f un isomorfismo de G sobre un grupo G' . ¿Es siempre posible definir una aplicación $\tilde{f} : G/H \rightarrow G'$ tal que $\tilde{f}(aH) = f(a)$ para todo $a \in G$? Si no es siempre posible ¿bajo qué circunstancias sí lo es?

- 6.8 Considere el grupo aditivo $(\mathbb{Z}, +)$ de los enteros y sea f un homomorfismo de $\mathbb{Z}$ en sí mismo. Escribiremos $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{Z}$.
- Demuestre que existe $k \in \mathbb{Z}$ tal que $f(x) = kx$ para todo $x \in \mathbb{Z}$. ¿Qué es $f(1)$? ¿Qué es $\ker(f)$? ¿Qué es $f(\mathbb{Z})$?
 - Sean $m, n \in \mathbb{Z}$. Demuestre que para que exista $\tilde{f}: \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ tal que $\tilde{f}(a + m\mathbb{Z}) = f(a) + n\mathbb{Z}$ para todo $a \in \mathbb{Z}$, es necesario y suficiente que $n|km$, donde $k = f(1)$, y que para que exista $\tilde{f}$ tal que $\tilde{f}(a + m\mathbb{Z}) = a + m\mathbb{Z}$ para todo $a \in \mathbb{Z}$, es necesario y suficiente que $n|m$.
 - Si $f(1) = k$ y $n|k$, demuestre que cualquiera que sea $m \in \mathbb{Z}$, existe $\tilde{f}: \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ tal que $\tilde{f}(a + m\mathbb{Z}) = f(a) + n\mathbb{Z}$ para todo $a \in \mathbb{Z}$. De hecho, $\tilde{f}(a + m\mathbb{Z}) = n\mathbb{Z}$ cualquiera que sea $a \in \mathbb{Z}$.
 - Si $k = f(1)$ y $\text{mcd}(n, k) = 1$, demuestre que para que exista $\tilde{f}: \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ tal que $\tilde{f}(a + m\mathbb{Z}) = f(a) + n\mathbb{Z}$ para todo $a \in \mathbb{Z}$, es necesario y suficiente que $n|m$, y que $\tilde{f}$ es un isomorfismo si y sólo si $m = \pm n$ y $k = \pm 1$.
- 6.9 Sean $(G, \cdot)$ un grupo, N un subgrupo normal de G . Demuestre que G/N es abeliano si y sólo si $aba^{-1}b^{-1} \in N$ cualesquiera que sean $a, b \in G$. Demuestre, de hecho, que si M es el subgrupo generado por $A = \{aba^{-1}b^{-1} | a, b \in G\}$ (ejercicio 3.8), entonces M es normal en G , G/M es abeliano, y si N es normal en G , G/N es abeliano si y sólo si $M \subseteq N$. Demuestre finalmente que si existe un homomorfismo $f: G \rightarrow \mathbb{Z}$ y M es como antes, entonces $M \subseteq \ker f$.
- 6.10 Sean M, N subgrupos de un grupo finito G y supóngase que N es normal en G y que $o(M) > \sqrt{o(G)}$, $o(N) \geq \sqrt{o(G)}$. Demuestre que $M \cap N \neq \{e\}$.
- 6.11 Sean G y G' grupos, H' un subgrupo normal de G' , $\varphi: G \rightarrow G'/H'$ un epimorfismo. Demuestre que $G/\varphi^{-1}(\{H'\}) \approx G'/H'$. Demuestre también que si $f: G \rightarrow G'$ es un epimorfismo y H' es como arriba, entonces $G/f^{-1}(H') \approx G'/H'$. Describa explícitamente los anteriores isomorfismos.
- 6.12 Sea G un grupo y sean M el conjunto de los elementos de orden finito de G y N el conjunto formado por e , el elemento neutro de G , y por los elementos de orden infinito de G .

- Demuestre que si $ab \in M$ cualesquiera que sean $a, b \in M$, entonces M es un subgrupo normal de G , y que si $M \neq G$ (o sea $N \neq \{e\}$) entonces G y G/M son grupos infinitos y todo elemento de G/M , salvo M , tiene orden infinito.
 - Demuestre que si $ab \in N$ cualesquiera que sean $a, b \in N$, entonces N es un subgrupo normal de G y todo elemento de G/N tiene orden finito.
 - Demuestre que si G es abeliano entonces M es un subgrupo de G . Demuestre además que si también N es un subgrupo de G entonces $G/M \approx N$ y $G/N \approx M$.
 - Sean $G = GL_2(\mathbb{R})$, $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$. Demuestre que $o(A) = 4$ y $o(B) = 3$, pero $o(AB) = \infty$. (Indicación. Demuestre que $(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, $n \in \mathbb{Z}$.)
 - Sea G como en (d). Encuentre $A, B \in G$ con $o(A) = o(B) = \infty$, pero $o(AB) < \infty$. Procure hacer esto con $B \neq A^{-1}$.
- 6.13 Sean G un grupo abeliano finito y n un divisor de $o(G)$. Demuestre que el número de soluciones de la ecuación $x^n = e$ es un múltiplo de n . (Indicación. Verifique que el conjunto G_n de tales soluciones es un subgrupo de G . Por otra parte, existe un subgrupo H de G con $o(H) = n$. Demuestre que $H \subseteq G_n$.)
- 6.14 Sea G un grupo abeliano finito tal que para todo $n \in \mathbb{N}$, $n \geq 1$, $G_n = \{x \in G : x^n = e\}$ tiene a lo sumo n elementos. Demuestre que para todo divisor n de $o(G)$, G_n tiene exactamente n elementos, y concluya que G es cíclico. (Indicación. Demuestre, por ejemplo, que para todo primo p , todo p -subgrupo de Sylow de G es cíclico, y recurra a lo observado en la nota 6.5.)
- 6.15 Demuestre que si G es un grupo cíclico finito, $G_n = \{x \in G : x^n = e\}$ tiene a lo sumo n elementos para todo $n \in \mathbb{N}$, $n \geq 1$, y que si $n | o(G)$ entonces $o(G_n) = n$. (Indicación. Recuerdese que todo subgrupo de G es cíclico.)
- *6.16 Use los resultados mencionados en la nota 5.6 y los ejercicios 6.13, 6.14 y 6.15 anteriores para demostrar que si q es un primo, $(\mathbb{Z}_q^*, \cdot)$ es un grupo cíclico. Demuestre además que $\mathbb{Z}_q^* \approx \mathbb{Z}_{q-1}$, y que si $p | q - 1$, la ecuación $x^p = \bar{1}$ tiene exactamente p soluciones. Concluya que si $p | q - 1$, $\mathbb{Z}_q^*$ tiene un único subgrupo de orden p .

Capítulo 7

Productos finitos de grupos

Sean $(G_1, \cdot), \dots, (G_n, \cdot)$ grupos, $G = G_1 \times \dots \times G_n$ el producto cartesiano de los conjuntos G_i . Con la ley de composición $(\cdot) : G \times G \longrightarrow G$ dada por

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n). \quad (7.1)$$

G es evidentemente un grupo, en el cual el elemento neutro es $e = (e_1, \dots, e_n)$, donde $e_i \in G_i$ es el elemento neutro de G_i , y en el cual el inverso $(x_1, \dots, x_n)^{-1}$ de $(x_1, \dots, x_n)$ es $(x_1^{-1}, \dots, x_n^{-1})$. Se dice que G es el *grupo producto* de los grupos G_i , $i = 1, 2, \dots, n$, y que cada G_i es un *factor* de G .

Si para cada i , H_i es un subgrupo de G_i , es evidente que $H_1 \times \dots \times H_n$ es un subgrupo de G . En particular, para todo $k = 1, 2, \dots, n$,

$$\tilde{H}_k = \{e_1\} \times \dots \times \{e_{k-1}\} \times H_k \times \{e_{k+1}\} \times \dots \times \{e_n\} \quad (7.2)$$

es un subgrupo de G . Si para cada $x_k \in H_k$ escribimos

$$\tilde{x}_k = (e_1, \dots, e_{k-1}, x_k, e_{k+1}, \dots, e_n), \quad (7.3)$$

se tiene que $\tilde{H}_k = \{\tilde{x}_k : x_k \in H_k\}$. Como se verifica inmediatamente, si cada H_i es un subgrupo normal de G_i , $H = H_1 \times \dots \times H_n$ es un subgrupo normal de G (véase al respecto (7.8), más adelante); en particular, si H_k es normal en G_k , $\tilde{H}_k$ es normal en G . Si para cada $i = 1, 2, \dots, n$, $f_i : G \longrightarrow G_i$, la aplicación $f : G \longrightarrow G_1 \times \dots \times G_n$ dada por $f(x) = (f_1(x), \dots, f_n(x))$ se denota con

$$f = (f_1, f_2, \dots, f_n), \quad (7.4)$$

y es claro que $f_i = p_i \circ f$, $i = 1, 2, \dots, n$, donde $p_i(x_1, \dots, x_n) = x_i$ es la proyección i -ésima de $G_1 \times \dots \times G_n$ en G_i (la cual es un homomorfismo, si

los G_i son grupos). No existe un nombre especial para f dada por (7.4), aunque las f_i se denominan a veces *las coordenadas de f* . Es claro que f es un homomorfismo de grupos si y sólo si cada f_i lo es.

Si G_i y G'_i , $i = 1, 2, \dots, n$, son grupos, y para cada i , $f_i : G_i \rightarrow G'_i$ es una aplicación, podemos también definir una aplicación $f : G_1 \times \dots \times G_n \rightarrow G'_1 \times \dots \times G'_n$ por

$$f(x_1, \dots, x_n) = (f_1(x_1), \dots, f_n(x_n)). \quad (7.5)$$

Es también fácil verificar que

$$f_i = p_i \circ f \circ q_i, \quad i = 1, 2, \dots, n \quad (7.6)$$

donde $p_i : G_1 \times \dots \times G_n \rightarrow G_i$ y $q_i : G'_1 \times \dots \times G'_n \rightarrow G'_i$ son las proyecciones i -ésimas, y que f es un homomorfismo si y sólo si cada f_i lo es. Es usual escribir

$$f = f_1 \times \dots \times f_n \quad (7.7)$$

y denominar a f el *homomorfismo producto de los homomorfismos f_i* . Es claro además que cada f_i es un isomorfismo, si y sólo si f es un isomorfismo. Si para cada $i = 1, 2, \dots, n$, H_i es un subgrupo normal de G_i , si $\varphi_i : G_i \rightarrow G_i/H_i$ es el homomorfismo canónico, si $\varphi = \varphi_1 \times \dots \times \varphi_n$, es claro que

$$\ker \varphi = H_1 \times \dots \times H_n, \quad (7.8)$$

así que φ induce un isomorfismo

$$\bar{\varphi} : G_1 \times \dots \times G_n / H_1 \times \dots \times H_n \rightarrow G_1/H_1 \times \dots \times G_n/H_n$$

(teorema 6.2) el cual está dado por

$$\bar{\varphi}((x_1, \dots, x_n) H_1 \times \dots \times H_n) = (\varphi_1(x_1), \dots, \varphi_n(x_n)) = (x_1 H_1, \dots, x_n H_n). \quad (7.9)$$

De este isomorfismo se deducen, en particular, los isomorfismos

$$\frac{G_1 \times \dots \times G_n}{\tilde{H}_k} \approx G_1 \times \dots \times G_{k-1} \times \frac{G_k}{H_k} \times G_{k+1} \times \dots \times G_n, \quad (7.10)$$

$$\frac{G_1 \times \dots \times G_k \times \dots \times G_n}{G_1 \times \dots \times G_{k-1} \times \{e_k\} \times G_{k+1} \times \dots \times G_n} \approx \tilde{G}_k \approx G_k, \quad (7.11)$$

y

$$\frac{G_1 \times \dots \times G_k \times \dots \times G_n}{G_1 \times \dots \times G_{k-1} \times H_k \times G_{k+1} \times \dots \times G_n} \approx (G_k / H_k) \approx G_k / H_k. \quad (7.12)$$

Naturalmente, hemos supuesto que $G/\{e\} = G$ y que $G/G = \{e\}$.

Definición 7.1. Si $H_1, \dots, H_n$ son subgrupos de un grupo G , y si la aplicación $\psi : H_1 \times \dots \times H_n \rightarrow G$ dada por

$$\psi(x_1, x_2, \dots, x_n) = x_1 x_2 \dots x_n \quad (7.13)$$

es un isomorfismo, se dice que G es el *producto directo externo de los subgrupos H_i , $i = 1, 2, \dots, n$* , y que cada H_i es un *factor directo de G* .

Ejemplo 7.1. Si $G_1, G_2, \dots, G_n$ son grupos, $G = G_1 \times \dots \times G_n$, y para cada $i = 1, 2, \dots, n$, $\tilde{G}_i$ y $\tilde{x}_i$ son como en (7.2) y (7.3), la aplicación

$$\psi : \tilde{G}_1 \times \dots \times \tilde{G}_n \rightarrow G$$

definida por $\psi(\tilde{x}_1, \dots, \tilde{x}_n) = \tilde{x}_1 \dots \tilde{x}_n$ es evidentemente un homomorfismo, y es un isomorfismo, pues $\psi(\tilde{x}_1, \dots, \tilde{x}_n) = (x_1, \dots, x_n)$. Por lo tanto, el grupo producto $G = G_1 \times \dots \times G_n$ es el *producto directo externo* de los subgrupos $\tilde{G}_1, \dots, \tilde{G}_n$.

Recordando ahora la noción de *producto directo interno de subgrupos de un grupo G* , capítulo 6, nota 6.4, se tiene el siguiente teorema.

Teorema 7.1. Sean G un grupo, $H_1, \dots, H_n$ subgrupos de G . Si G es el producto directo externo de $H_1, \dots, H_n$, entonces:

1. H_i es un subgrupo normal de G para todo $i = 1, 2, \dots, n$.
2. $H_i \cap H_j = \{e\}$ si $i \neq j$.
3. Si $x \in G$, existen $x_1 \in H_1, \dots, x_n \in H_n$, unívocamente determinados por x , tales que $x = x_1 x_2 \dots x_n$.

Además, G es el producto directo interno de los subgrupos H_i , $i = 1, 2, \dots, n$.

Demostración. Como $\psi : H_1 \times \dots \times H_n \rightarrow G$, dada por (7.13), es un isomorfismo, $\tilde{H}_i$ es un subgrupo normal de $H_1 \times \dots \times H_n$ y $H_i = \psi(\tilde{H}_i)$, se deduce que H_i es normal en G . Esto demuestra (1). Como $H_i \cap H_j =$

$\psi(\tilde{H}_i) \cap \psi(\tilde{H}_j) = \psi(\tilde{H}_i \cap \tilde{H}_j) = \{\psi(e)\} = \{e\}$ si $i \neq j$ (pues evidentemente $\tilde{H}_i \cap \tilde{H}_j = \{e\}$ si $i \neq j$), también (2) queda demostrado. Como ψ es sobreyectiva, dado $x \in G$ existen $x_1, \dots, x_n \in G$, $x_i \in H_i$, tales que $\psi(x_1, x_2, \dots, x_n) = x_1 x_2 \cdots x_n = x$, y la unicidad de $x_1 x_2 \cdots x_n$ resulta de la inyectividad de ψ . Esto demuestra (3) y completa, en virtud del teorema 6.5, la demostración del teorema. $\square$

Recíprocamente,

Teorema 7.2. Sean $H_1, \dots, H_n$ subgrupos de G y supóngase que G es el producto directo interno de los subgrupos $H_1, \dots, H_n$, así que:

1. H_i es normal en G para todo $i = 1, 2, \dots, n$.
2. $H_i \cap H_j = \{e\}$ si $i \neq j$.
3. Si $x \in G$, existen $x_1, \dots, x_n \in G$, $x_i \in H_i$, tales que $x = x_1 x_2 \cdots x_n$, estando los x_i determinados unívocamente por x .

Entonces, G es el producto directo externo de $H_1, \dots, H_n$.

Demostración. El hecho de que los H_i sean normales en G y de que $H_i \cap H_j = \{e\}$ si $i \neq j$ implica que $x_i x_j = x_j x_i$ si $x_i \in H_i$, $x_j \in H_j$ e $i \neq j$ (lema 6.1). Por lo tanto, si $x_i, y_i \in H_i$, $i = 1, 2, \dots, n$, entonces

$$(x_1 y_1)(x_2 y_2) \cdots (x_n y_n) = (x_1 \cdots x_n)(y_1 \cdots y_n), \quad (7.14)$$

así que la aplicación $\psi(x_1, \dots, x_n) = x_1 \cdots x_n$ de $H_1 \times \cdots \times H_n$ en G es un homomorfismo y, por 3., necesariamente un isomorfismo. El teorema está demostrado. $\square$

Nota 7.1. Se deduce que sobre un grupo G las nociones de producto directo interno y de producto directo externo de un número finito de subgrupos coinciden. Por tal razón, de ahora en adelante sólo hablaremos de producto directo de subgrupos. Salvo isomorfismo, esta última noción coincide además con la de grupo producto de tales subgrupos.

Nota 7.2. Si un grupo G es el producto directo de dos subgrupos M y N , es claro que $G/M \approx N$. Sin embargo, si M es un subgrupo normal arbitrario de G , no necesariamente G/M es isomorfo a un subgrupo de G ni, mucho menos, $G \approx G/M \times M$. Por ejemplo, si $n \in \mathbb{N}$, $n \neq 0, 1$, $\mathbb{Z}n = \mathbb{Z}/n\mathbb{Z}$ no es

isomorfo a ningún grupo de $(\mathbb{Z}, +)$. De hecho, el único subgrupo finito de $(\mathbb{Z}, +)$ es $\{0\}$.

Nota 7.3. Pueden existir, sin embargo, grupos G y subgrupos normales H_i de G , $i = 1, 2, \dots, n$, tales que $H_i \cap H_j = \{e\}$ si $i \neq j$, que $G = H_1 \cdots H_n$ y que G no sea el producto directo de los H_i . Para un ejemplo, véase el ejercicio 7.8. Obsérvese que debe ser $n \geq 3$. Véase, sin embargo, el ejercicio 7.9.

Recordamos ahora que si un grupo abeliano finito G tiene orden $p_1 \cdots p_m$, donde los p_i son primos distintos, entonces G es el producto directo de subgrupos cíclicos. Por otra parte, si $o(G) = p_1^{n_1} \cdots p_m^{n_m}$, entonces G es el producto directo de los subgrupos M_i , $i = 1, 2, \dots, m$, donde $o(M_i) = p_i^{n_i}$ (corolarios 6.5 y 6.6).

Demostraremos ahora el siguiente teorema, que generaliza a todo grupo abeliano finito la primera de las afirmaciones anteriores.

Teorema 7.3. Si G es un grupo abeliano finito, entonces G es cíclico o es el producto directo de subgrupos cíclicos.

Necesitaremos el siguiente lema que constituye el resultado más engorroso de todo el curso. El lector puede aceptar este resultado y omitir su demostración, aunque puede ser un buen ejercicio comprender los detalles de la misma. Esta ha sido tomada de [15]. Es posible dar demostraciones más elegantes si se tienen mejores conocimientos de álgebra (véase [17]).

Lema 7.1. Sean G un grupo abeliano de orden p^n , donde p es un primo, $m = \max\{o(c) : c \in G\}$ el máximo orden posible de los elementos de G , $a \in G$ con $o(a) = m$, y $H = \langle a \rangle$. Entonces $G = H$, en cuyo caso G es cíclico, o existe un subgrupo cíclico M de G , $M \neq \{e\}$, tal que $M \cap H = \{e\}$ y que $G = HM$, así que G es el producto directo de H y M .

Demostración. La afirmación es cierta si $n = 0, 1$, pues G sería cíclico, de lo cual, $m = p^n$ y $G = H$. Supongamos primero que existe $b \in G$, $b \notin H$, tal que $b^p = e$, y sean $N = \langle b \rangle$ y $\bar{G} = G/N$. Como es claro, $H \cap N = \{e\}$ (pues si $b^k \in H$, $1 \leq k \leq p-1$, también $o(b^k) = p$, de lo cual sería $N \subseteq H$ y $b \in H$). Escribamos $\bar{c} = cN$, para todo $c \in G$, y sea a como en el enunciado del lema. Veamos que $o(\bar{a}) = o(a) = m$. Escribamos $l = o(\bar{a})$. Como $(\bar{a})^m = \bar{a}^m = \bar{e}$, es claro que $l \mid m$. Por otra parte $(\bar{a})^l = \bar{e}$, así que $a^l \in N \cap H$, de lo cual $a^l = e$. Entonces $m \mid l$. Se deduce que $l = m$ y

que $\bar{a}$ es un elemento de $\bar{G}$ de orden máximo posible. Como $o(\bar{G}) < o(G)$, podemos suponer inductivamente que $\bar{G}$ es cíclico y generado por $\bar{a}$, de lo cual $G = HN$ (pues si $c \in G$ entonces $cN = a^k N$ para algún $k \in \mathbb{N}$, así que $ca^{-k} \in N$, o sea, $c = a^k b^j$, $j \in \mathbb{N}$), o que $\bar{G} = [\bar{a}] \bar{M}$, donde $\bar{M} \cap [\bar{a}] = \{e\}$. Ahora, por el corolario 6.1, existe un subgrupo M' de G tal que $M' \supseteq N$ y que $M'/N \approx \bar{M}$, y evidentemente $H \cap M' = \{e\}$ (si no, y $c \in H \cap M'$, $c \neq e$, entonces $\bar{c} \in \bar{M} \cap [\bar{a}]$ y $\bar{c} \neq \bar{e}$, pues $H \approx [\bar{a}]$ mediante el isomorfismo $c \rightarrow \bar{c}$). Además $G = HM'$ (pues si $c \in G$ entonces $\bar{c} = \bar{a}^i \bar{d}^j$, $i, j \in \mathbb{N}$ y $d \in M'$, así que $ca^{-i}d^{-j} = b^k$ para algún $k \in \mathbb{N}$, de lo cual $c = a^i (d^j b^k) \in HM'$). El lema resulta entonces con $M = N$ cuando $\bar{G}$ es cíclico y generado por $\bar{a}$, o con $M = M'$, en caso contrario. Supongamos ahora que no existe $b \in G \setminus H$ con $o(b) = p$. Veamos que entonces $G = H$. Supóngase que $G \neq H$, y sean $l = \min \{o(c) : c \in G \setminus H\}$ y $x \in G \setminus H$ con $o(x) = l$. Como $o(x^p) \leq l/p < l$, necesariamente $x^p \in H$, así que $x^p = a^i$, $i \in \mathbb{N}$. Afirmamos que $p \mid i$. Supongamos lo contrario y que $m = p^k$, $k \in \mathbb{N}$. Como m es el máximo orden posible de los elementos de G , si $c \in G$ entonces $o(c) = p^j$ con $j \leq k$, de lo cual $o(c) \mid m$. Ahora, como $p \nmid i$, así que $m \nmid im/p$, entonces $a^{im/p} \neq e$. Pero esto implica que $x^m = (x^p)^{m/p} = (a^i)^{m/p} = a^{im/p} \neq e$, lo cual es absurdo, pues $o(x) \mid m$. Se deduce que $p \mid i$, así que $i = pj$, $j \in \mathbb{N}$, y si $b = a^{-j}x$ entonces $b^p = a^{-i}x^p = e$, lo cual es absurdo, pues, como $a^{-j} \in H$ mientras que $x \notin H$, entonces $b \notin H$ y $o(b) = p$. Se concluye que $G = H$, y el lema queda demostrado. $\square$

Nota 7.4. El lema 7.1 se expresa también diciendo que si G es un grupo abeliano de orden p^n , $n \geq 0$, donde p es un primo y H es un subgrupo cíclico de G de máximo orden posible, entonces $H = G$, en cuyo caso G es cíclico, o H es un factor directo propio de G , así que existe un subgrupo propio K de G tal que $G \approx H \times K$.

Nota 7.5. Observamos que si un grupo abeliano es el producto directo de los subgrupos $H_1, \dots, H_n$, y cada H_i es a su vez el producto directo de los subgrupos $H_{i1}, \dots, H_{in_i}$, entonces G es el producto directo de los subgrupos H_{ik} , $k = 1, 2, \dots, n_i$, $i = 1, 2, \dots, n$. La demostración es obvia. En vista de esto se tiene el siguiente corolario del lema 7.1.

Corolario 7.1. Si G es un grupo abeliano de orden p^n , donde p es un primo y $n \geq 0$, entonces G es cíclico o el producto directo de subgrupos cíclicos.

Demostración. Según el lema 7.1, G es cíclico (que es el caso si $n = 0, 1$) o existen un subgrupo cíclico $H \neq \{e\}$ y un subgrupo M de G tales que G es

el producto directo de H y M . Como $G/H \approx M$ entonces $o(M) < o(G)$, así que $o(M) = p^k$, $0 \leq k < n$. Razonando por inducción podemos suponer que M es cíclico o el producto directo de subgrupos cíclicos. En vista de lo observado en la nota 7.4, G mismo es cíclico o el producto directo de subgrupos cíclicos. $\square$

Podemos ahora demostrar el teorema 7.3.

Demostración del teorema 7.3. Se tiene que $o(G) = p_1^{n_1} \dots p_m^{n_m}$, donde $m \geq 1$ y $p_1, \dots, p_m$ son primos distintos. Ahora, si $m = 1$, la afirmación resulta inmediatamente del corolario 7.1. Si $m > 1$ el corolario 6.5 garantiza que G es el producto directo de subgrupos $M_1, \dots, M_m$, donde $o(M_k) = p_k^{n_k}$, $k = 1, 2, \dots, m$. Como cada M_k es a su vez cíclico o el producto directo de subgrupos cíclicos, lo observado anteriormente también garantiza que G lo es. $\square$

Nota 7.6. Como lo muestra el corolario 6.6, G puede ser al mismo tiempo cíclico y el producto directo de subgrupos cíclicos propios.

El teorema 7.3 se conoce como el *teorema estructural de los grupos abelianos finitos*. Según el lema 7.1, si G es un grupo abeliano de orden p^n , donde p es un primo y $n \geq 1$ es un entero, se tiene que

$$G \approx \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \dots \times \mathbb{Z}_{p^{n_m}}, \quad m \geq 1 \quad (7.15)$$

donde $1 \leq n_1 \leq n_2 \leq \dots \leq n_m$ son enteros y

$$p^n = o(G) = o(\mathbb{Z}_{p^{n_1}}) \dots o(\mathbb{Z}_{p^{n_m}}) = p^{n_1} \dots p^{n_m} = p^{n_1 + \dots + n_m},$$

así que $n = n_1 + n_2 + \dots + n_m$. Si $n \geq 1$ y $1 \leq n_1 \leq n_2 \leq \dots \leq n_m$ son enteros tales que $n = n_1 + n_2 + \dots + n_m$, $m \geq 1$, se dice que la m -pla $(n_1, n_2, \dots, n_m)$ es una *partición* de n . Por lo tanto, para un $n \geq 1$ dado, habrá a lo sumo tantos grupos no isomorfos de orden p^n como particiones distintas de n sean posibles. Así, si $n = 3$, las posibles particiones de n son (3), (1, 2), (1, 1, 1), y los grupos posiblemente no isomorfos de orden p^3 serán

$$\mathbb{Z}_{p^3}, \quad \mathbb{Z}_p \times \mathbb{Z}_{p^2}, \quad \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p.$$

Si $o(G) = p^4$, los posibles grupos no isomorfos serán

$$\mathbb{Z}_{p^4}, \quad \mathbb{Z}_p \times \mathbb{Z}_{p^3}, \quad \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}, \quad \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2} \quad \text{y} \quad \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p.$$

Si ahora

$$G \approx G_1 \times \cdots \times G_n \quad (7.16)$$

donde $o(G_i) = p_i^{m_i}$ (corolario 6.5), y si $\bar{m}_i$ es el número de particiones posibles de m_i , habrá a lo sumo $\bar{m}_1 \bar{m}_2 \cdots \bar{m}_n$ grupos abelianos no isomorfos de orden $o(G)$. Así, puesto que (2) y (1,1) son las particiones de 2, y (3), (1,2), (1,1,1) son las de 3, habrá a lo sumo $2 \cdot 3 = 6$ grupos no isomorfos de orden $p_1^2 \cdot p_2^3$, $p_1 \neq p_2$, los cuales son:

$$\begin{aligned} &\mathbb{Z}_{p_1^2} \times \mathbb{Z}_{p_2^3}, \\ &\mathbb{Z}_{p_1^2} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2^2}, \\ &\mathbb{Z}_{p_1^2} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2}, \\ &\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2^3}, \\ &\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2^2}, \\ &\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2}. \end{aligned}$$

Teniendo ahora en cuenta que $\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$ si y sólo si $\text{mcd}(m, n) = 1$ (pues evidentemente $(\bar{a}, \bar{b})$ tiene orden a lo sumo $\text{mcm}(m, n)$ en $\mathbb{Z}_m \times \mathbb{Z}_n$), éstos se pueden dar, en su orden, en la forma

$$\begin{aligned} &\mathbb{Z}_{p_1^2 p_2^3}, \\ &\mathbb{Z}_{p_1^2 p_2} \times \mathbb{Z}_{p_2^2}, \\ &\mathbb{Z}_{p_1^2 p_2} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2}, \\ &\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_1 p_2^3}, \\ &\mathbb{Z}_{p_1 p_2} \times \mathbb{Z}_{p_1 p_2^2} \quad \text{y} \\ &\mathbb{Z}_{p_1 p_2} \times \mathbb{Z}_{p_1 p_2} \times \mathbb{Z}_{p_2}. \end{aligned}$$

Nótese que $\mathbb{Z}_{p_1^2 p_2} \times \mathbb{Z}_{p_2^2} \approx \mathbb{Z}_{p_1^2 p_2^2} \times \mathbb{Z}_{p_2}$: ambos son, de hecho, isomorfos a $\mathbb{Z}_{p_1^2} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2^2}$; a su vez,

$$\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_1 p_2^2} \times \mathbb{Z}_{p_2} \approx \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_1 p_2} \times \mathbb{Z}_{p_2^2} \approx \mathbb{Z}_{p_1 p_2} \times \mathbb{Z}_{p_1 p_2^2} \approx \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2^2};$$

$$\mathbb{Z}_{p_1 p_2} \times \mathbb{Z}_{p_1 p_2} \times \mathbb{Z}_{p_2} \approx \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2}.$$

Nota 7.7. Es posible demostrar que si $(n_1, n_2, \dots, n_m)$ y $(n'_1, n'_2, \dots, n'_l)$ son particiones distintas de n , los grupos $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_m}}$ y $\mathbb{Z}_{p^{n'_1}} \times \mathbb{Z}_{p^{n'_2}} \times \cdots \times \mathbb{Z}_{p^{n'_l}}$ no son isomorfos, así que el proceso anteriormente

descrito da *exactamente* los grupos abelianos no isomorfos de orden $m = p^n$ (y, de hecho, de orden m para todo m). No demostraremos esto. El lector interesado puede encontrar la demostración en [16].

Nota 7.8. Una última observación es pertinente. Si $(G, +)$ es un grupo abeliano notado aditivamente y $H_1, \dots, H_n$ son subgrupos de G , es natural escribir $H_1 + H_2 + \cdots + H_n$ en lugar de $H_1 H_2 \cdots H_n$. Y si G es el producto directo de $H_1, H_2, \dots, H_n$, es también usual decir que G es la *suma directa* de $H_1, H_2, \dots, H_n$.

EJERCICIOS

- 7.1 Si $G = G_1 \times \cdots \times G_n$, demuestre que $(G, \cdot)$, donde $(\cdot)$ está definido por (7.1), es en efecto un grupo, en el cual $e = (e_1, \dots, e_n)$ es el elemento neutro y $(x_1, \dots, x_n)^{-1} = (x_1^{-1}, \dots, x_n^{-1})$. Demuestre además que G es abeliano si y sólo si cada G_i , $i = 1, 2, \dots, n$, es abeliano.
- 7.2 Demuestre que si H_i es un subgrupo de G_i , $i = 1, 2, \dots, n$, entonces $H = H_1 \times \cdots \times H_n$ es un subgrupo de $G = G_1 \times \cdots \times G_n$, y que H es normal en G si y sólo si cada H_i es normal en G_i , $i = 1, 2, \dots, n$. Demuestre a su vez que $\tilde{H}_k$ definido por (7.2) es un subgrupo de G y que $\tilde{H}_k$ es normal en G si y sólo si H_k es normal en G_k .
- 7.3 Demuestre que $p_i : G_1 \times \cdots \times G_n \rightarrow G_i$, $i = 1, 2, \dots, n$, es un epimorfismo, y que si G' es un grupo y $f : G' \rightarrow G_1 \times \cdots \times G_n$, f es un homomorfismo si y sólo si $f_i = f \circ p_i$ es un homomorfismo para todo $i = 1, 2, \dots, n$. Verifique además que $f = (f_1, \dots, f_n)$ como en (7.4).
- 7.4 Para cada $k = 1, 2, \dots, n$, sea $q_k : G_k \rightarrow G = G_1 \times \cdots \times G_n$ dada por $q_k(x_k) = \tilde{x}_k$, donde $x_k \in G_k$ y $\tilde{x}_k$ es como en (7.3). Demuestre que q_k es un monomorfismo de G_k en G y que $q_k(G_k) = \tilde{G}_k$, donde $\tilde{G}_k$ es como en (7.2). Demuestre además que si $G' = G'_1 \times G'_2 \times \cdots \times G'_n$ y $f : G \rightarrow G'$ es la aplicación $f = f_1 \times \cdots \times f_n$ dada por (7.5) y (7.7) donde $f_i : G_i \rightarrow G'_i$, entonces f es un homomorfismo si y sólo si cada f_i lo es, y un isomorfismo si y sólo si cada f_i es un isomorfismo.
- 7.5 Sean $G_1, \dots, G_n$ grupos y sean $1 < i_1 < i_2 < \cdots < i_m < n$ tales que $G_{i_k} \neq \{e\}$ si y sólo si $i = i_k$, $k = 1, 2, \dots, m$. Demuestre que $\tilde{G}_k \cap \tilde{G}_j = \{e\}$ si $k \neq j$ y que $G = G_1 \times \cdots \times G_n = \tilde{G}_{i_1} \cdot \tilde{G}_{i_2} \cdots \tilde{G}_{i_m}$, y concluya que $G_1 \times \cdots \times G_n \approx G_{i_1} \times G_{i_2} \times \cdots \times G_{i_m}$.

7.6 Sean $G_1, \dots, G_n$ grupos y sea $\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ biyectiva. Demuestre que $\tilde{G}_{\sigma(i)} \cap \tilde{G}_{\sigma(j)} = \{e\}$ si $i \neq j$ y que $G_1 \times \dots \times G_n = \tilde{G}_{\sigma(1)} \cdot \tilde{G}_{\sigma(2)} \cdots \tilde{G}_{\sigma(n)}$, y concluya que $G_1 \times \dots \times G_n \approx G_{\sigma(1)} \times G_{\sigma(2)} \times \dots \times G_{\sigma(n)}$.

7.7 Establezca las relaciones (7.10), (7.11) y (7.12).

7.8 Sean $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, $H_1 = \{(1, 0), (0, 0)\}$, $H_2 = \{(0, 1), (0, 0)\}$, $H_3 = \{(1, 1), (0, 0)\}$. Verifique que $H_i \cap H_j = \{(0, 0)\}$ si $i \neq j$ y que $H_1 + H_2 + H_3 = G$ (nota 7.8), pero que G no es la suma directa de H_1 , H_2 y H_3 . Verifique, en particular, que $H_1 \cap (H_2 + H_3) \neq \{(0, 0)\}$. Para una versión multiplicativa de este ejercicio, véase el ejercicio 8.19.

7.9 Sean $(G, \cdot)$ un grupo finito, $M_1, M_2, \dots, M_n$ subgrupos normales de G tales que $G = M_1 M_2 \dots M_n$ y que $o(G) = o(M_1) o(M_2) \cdots o(M_n)$. Demuestre que G es el producto directo de $M_1, M_2, \dots, M_n$. ¿Es $o(G) = o(H_1) o(H_2) o(H_3)$ en el ejercicio 7.8?

7.10 Sean G un grupo y M un subgrupo normal de G . Demuestre que si $\bar{G} = G/M$ es cíclico y generado por $\bar{a} = aM$, $a \in G$, entonces $G = HM$, donde $H = [a]$. Concluya que si $M \cap H = \{e\}$ y H es normal en G entonces G es el producto directo de H y M , y que éste es el caso si $a \in Z(G)$ (ejercicio 4.7) y M es de orden primo y generado por $b \notin H$.

7.11 Sean G un grupo y N un subgrupo normal de G . Supóngase que $\bar{G} = G/N$ es el producto directo de $\bar{H}$ y $\bar{M}$ y que $\bar{H}$ está generado por $\bar{a} = aN$ donde $a \in G$. Sean $H = [a]$ y M un subgrupo de G tal que $M \supseteq N$ y que $M/N = \bar{M}$. Demuestre que M es normal en G y que $G = HM$. Demuestre además que si $o(H) = o(\bar{H})$ y $a \in Z(G)$ (ejercicio 4.7), entonces G es el producto directo de H y M .

7.12 Sean H_1 y H_2 grupos, $G = H_1 \times H_2$.

- Demuestre que si H_1 y H_2 son cíclicos finitos de órdenes respectivos m y n , entonces G es cíclico si y sólo si $\text{mcd}(m, n) = 1$.
- Supóngase que $H_1 = H_2 = H$ y sea $\Delta = \{(x, x) : x \in H\}$. Demuestre que Δ es un subgrupo de G y que $\Delta \approx H$. Demuestre además que Δ es un subgrupo normal de G si y sólo si H es abeliano.

7.13 Supóngase que H_1 y H_2 son subgrupos de un grupo cíclico finito G y que $G = H_1 H_2$. Demuestre que G es el producto directo de H_1 y H_2 si y sólo si $\text{mcd}(o(H_1), o(H_2)) = 1$.

7.14 Sea G un grupo abeliano finito con $o(G) = mn$ donde $\text{mcd}(m, n) = 1$. Sean $M = \{x \in G : x^m = e\}$, $N = \{x \in G : x^n = e\}$. Demuestre que M y N son subgrupos de G y que G es el producto directo de M y N . Demuestre además que $o(M) = m$, $o(N) = n$.

7.15 Sean G un grupo abeliano, H y K subgrupos de G tales que $o(H) = m$, $o(K) = n$ son finitos. Demuestre que $M = HK$ es un subgrupo de G el cual contiene un subgrupo N con $o(N) = \text{mcm}(m, n)$. ¿Es esto mismo posible si G no es abeliano pero $H = [a]$, $K = [b]$, $ab = ba$ y $o(a) = m$, $o(b) = n$? ¿Lo será aún si G no es abeliano pero H y K son subgrupos abelianos de G , normales en G y tales que $H \cap K = \{e\}$, $o(H) = m$ y $o(K) = n$?

7.16 Sean G un grupo infinito, M y N subgrupos normales de G tales que $[G : M] < \infty$ y $[G : N] < \infty$. Demuestre que $[G : M \cap N] < \infty$. (Indicación. Sea $\varphi : G \rightarrow G/M \times G/N$ el homomorfismo $\varphi(x) = (xM, xN)$. Verifique que $\ker \varphi = M \cap N$.)

Capítulo 8

El grupo simétrico

El *grupo simétrico* $((S_n, \cdot), n \geq 1)$, es el grupo obtenido al dotar el conjunto S_n de las aplicaciones biyectivas de $\{1, 2, \dots, n\}$ en sí mismo (las llamadas *permutaciones de n objetos*) de la ley de composición $(\cdot)$ dada por

$$\sigma \cdot \rho = \rho \circ \sigma \quad (8.1)$$

donde $(\circ)$ es la composición usual de funciones. Generalmente escribiremos $\sigma\rho$ en lugar de $\sigma \cdot \rho$. Nótese que el elemento neutro de $(S_n, \cdot)$ es aún la aplicación idéntica e de $\{1, 2, \dots, n\}$, y si $\sigma \in S_n$, σ^{-1} es simplemente la aplicación inversa de σ .

Nota 8.1. Para muchos autores, el grupo simétrico es $(S_n, \circ)$, es decir, prefieren la ley de composición de funciones a la (8.1). Como veremos, sin embargo, la ley $(\cdot)$ tiene ligeras ventajas sobre la $(\circ)$. Obsérvese que

$$\sigma_1 \sigma_2 \cdots \sigma_n = \sigma_n \circ \sigma_{n-1} \circ \cdots \circ \sigma_1. \quad (8.2)$$

Si $\sigma \in S_n$ y $\sigma(k) = i_k$, $1 \leq k \leq n$, es usual escribir

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}. \quad (8.3)$$

También,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}. \quad (8.4)$$

Una de las ventajas del producto $(\cdot)$ es la siguiente, que ilustramos en el caso $n = 4$. Si

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix},$$

para calcular $\sigma\rho(3)$, por ejemplo, es suficiente seguir el camino directo esquematizado abajo:

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

Entonces $\sigma\rho(3) = 1$. A su vez, $\sigma\rho(4)$ se obtiene de

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

o sea, $\sigma\rho(4) = 2$. En total,

$$\sigma\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Para calcular $\sigma \circ \rho$ sería necesario seguir caminos inversos. Así, $\sigma \circ \rho(3) = 4$ resulta de

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & & & \\ 4 & 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & \downarrow & \\ 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & \downarrow & \\ & & & 4 \end{pmatrix}.$$

En total,

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

Los caminos inversos pueden ser incómodos cuando se desea considerar el producto de muchas permutaciones (y, en especial, el producto de muchos ciclos, como veremos más adelante).

Definición 8.1. Si $\sigma \in S_n$ e $1 \leq i \leq n$ es tal que $\sigma(i) \neq i$, se dice que σ *mueve* a i . El conjunto de los $1 \leq i \leq n$ que son movidos por σ se denomina el *orbital* de σ .

Por ejemplo, si

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix},$$

el orbital de σ es $\{1, 4, 5\}$. Como es claro, *dos permutaciones distintas pueden tener el mismo orbital*. Así, si σ es como arriba, entonces $\sigma^2 \neq \sigma$, pero el

orbital de σ^2 es aún $\{1, 4, 5\}$. Obsérvese que si $e \in S_n$ es la permutación idéntica, su orbital es vacío. Como es claro, e es la única permutación con esta propiedad.

Definición 8.2. Se dice que una permutación σ de S_n es una *permutación cíclica* o, simplemente, un *ciclo*, si existen $i_1, i_2, \dots, i_p$ en $\{1, 2, \dots, n\}$, $1 < p \leq n$, todos distintos, tales que

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \dots, \sigma(i_{p-1}) = i_p, \quad \sigma(i_p) = i_1 \quad (8.5)$$

y que $\sigma(i) = i$ para $i \notin \{i_1, i_2, \dots, i_p\}$. Se dice también, en forma más precisa, que σ es un p -ciclo cuyo orbital es $\{i_1, i_2, \dots, i_p\}$. Escribiremos

$$\sigma = (i_1, i_2, \dots, i_p). \quad (8.6)$$

Un 2-ciclo se denomina una *trasposición*.

Así,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 1 & 6 \end{pmatrix} = (1, 3, 4, 5)$$

y

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2, 4)$$

son ciclos (respectivamente, un 4-ciclo y un 2-ciclo), con orbitales respectivos $\{1, 2, 4, 5\}$ y $\{2, 4\}$.

La notación (8.6) para los ciclos abre la posibilidad de confundir éstos con las p -plas. Esto es particularmente cierto de los 2-ciclos (trasposiciones) y las parejas ordenadas. Sólo podemos esperar que el contexto evite cualquier confusión.

Como es claro,

$$(i_1, i_2, \dots, i_p) = (i_2, i_3, \dots, i_p, i_1) = \dots = (i_p, i_1, \dots, i_{p-1}). \quad (8.7)$$

Es también claro que *dos ciclos distintos pueden tener el mismo orbital*. Si $\sigma = (i_1, i_2, \dots, i_p)$, entonces

$$\sigma = (i_1, \sigma(i_1), \dots, \sigma^{p-1}(i_1)) = (i_k, \sigma(i_k), \dots, \sigma^{p-1}(i_k)) \quad (8.8)$$

para todo $1 \leq k \leq p$, y también

$$\sigma = (\sigma(i_1), \sigma^2(i_1), \dots, \sigma^p(i_1)) = (\sigma(i_k), \sigma^2(i_k), \dots, \sigma^p(i_k)). \quad (8.9)$$

Las fórmulas (8.8) y (8.9) muestran que en la descripción de un ciclo $\sigma = (i_1, \dots, i_p)$, la escogencia de i_1 es en realidad poco importante (cualquiera de los i_k serviría igual). Sin embargo, una vez escogida i_1 , se tiene que

$$\sigma^{k-1}(i_1) = i_k, \quad 1 \leq k \leq p; \quad \sigma^p(i_1) = i_1. \quad (8.10)$$

Esto implica que si $\sigma = (i_1, \dots, i_p)$, $p \geq 2$, entonces

$$p = \min\{m > 1 : \sigma^m(i_1) = i_1\} = \min\{m > 1 : \sigma^m(i_k) = i_k\} \quad (8.11)$$

para todo $1 \leq k \leq p$.

Definición 8.3. Si $\sigma = (i_1, \dots, i_p)$ es un p -ciclo, se dice que p es la *longitud* de σ : $p = l(\sigma)$. Si $i = \min\{i_1, \dots, i_p\}$, se dice que σ es un *ciclo basado en i* o *con base i* .

Nota 8.2. Nótese que si σ es un ciclo, $l(\sigma) \geq 2$. Si τ es una transposición, es claro que $l(\tau) = 2$ y que $\tau^2 = e$, así que $\tau^{-1} = \tau$. Nótese, más generalmente, que si $\sigma = (i_1, \dots, i_p)$ es un ciclo de longitud p , σ^{-1} es también un ciclo de longitud p . De hecho, $\sigma^{-1} = (i_p, i_{p-1}, \dots, i_1)$. Así, $(1, 2, 3)^{-1} = (3, 2, 1) = (1, 3, 2) = (2, 1, 3)$.

Observar que

$$(i_1, \dots, i_p) = (i_k, \dots, i_p, i_1, \dots, i_{k-1}), \quad 1 \leq k \leq p, \quad (8.12)$$

es conveniente al multiplicar ciclos, pues permite seguir caminos directos. Así, si $\sigma = (1, 3)(3, 5, 4)(1, 3, 2)$ en S_6 , entonces

$$\begin{aligned} (1, 3)(3, 5, 4)(1, 3, 2), \sigma(1) &= 5 \\ (1, 3)(3, 5, 4)(2, 1, 3), \sigma(2) &= 1 \\ (3, 1)(3, 5, 4)(1, 3, 2), \sigma(3) &= 3 \\ (1, 3)(4, 3, 5)(3, 2, 1), \sigma(4) &= 4 \\ (1, 3)(5, 4, 3)(3, 2, 1), \sigma(5) &= 5 \end{aligned}$$

Como $\sigma \in S_6$, también $\sigma(6) = 6$. Es decir,

$$(1, 3)(3, 5, 4)(1, 3, 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 2 & 4 & 6 \end{pmatrix}.$$

Nota 8.3. Nótese que si $\sigma = (i_1, i_2, \dots, i_p)$, σ puede considerarse como un *ciclo de S_n para todo $n \geq \max\{i_1, \dots, i_p\}$* .

Definición 8.4. Se dice que los ciclos $\sigma = (i_1, \dots, i_p)$ y $\rho = (j_1, \dots, j_q)$ son *disyuntos* si sus orbitales son *disyuntos*, es decir, si $\{i_1, \dots, i_p\} \cap \{j_1, \dots, j_q\} = \emptyset$.

Así, $(1, 2, 4, 5)$ y $(3, 6, 7)$ son ciclos disyuntos, mientras que $(1, 2, 4, 5)$ y $(2, 6, 7)$ no lo son. Como es claro, si $\sigma_1, \dots, \sigma_m$ son ciclos disyuntos, el orbital O de $\sigma = \sigma_1 \cdots \sigma_m$ es $O_1 \cup \dots \cup O_m$, donde O_i es el orbital de σ_i . Nótese que $O_i \cap O_j = \emptyset$ si $i \neq j$, y para cualquier permutación ρ , decir que $\rho = \sigma$ es equivalente a decir que el orbital O' de ρ es O y que $\rho(i) = \sigma_k(i)$ si $i \in O_k$, $1 \leq k \leq m$.

Nota 8.4. Sean $\sigma \in S_n$, $n \geq 1$ y $1 \leq i \leq n$. Si $\sigma(i) = i$, se dice usualmente que σ *inmoviliza o estabiliza a i* .

Nota 8.5. Si σ y ρ en S_n son tales que $\sigma\rho = \rho\sigma$, entonces $(\sigma\rho)^n = \sigma^n\rho^n$ para todo $n \in \mathbb{Z}$ (teorema 2.9 y corolario 2.5). Obsérvese también que si σ es una permutación y $n \in \mathbb{Z}$, $\sigma(i) = i$ implica $\sigma^n(i) = i$. Es decir, si $\sigma^n(i) \neq i$, necesariamente $\sigma(i) \neq i$.

Nota 8.6. Es claro que si σ y ρ son ciclos disyuntos entonces $\sigma\rho = \rho\sigma$. Es decir, si $\sigma_1, \dots, \sigma_p$ son ciclos disyuntos, $\sigma = \sigma_1 \cdots \sigma_p$ es independiente del orden en que se multiplican dichos ciclos. En particular, $\sigma = \sigma_2\sigma_3 \cdots \sigma_p\sigma_1 = \sigma_p\sigma_{p-1} \cdots \sigma_1$, etc. Entonces, como se deduce de lo dicho en la nota 8.5,

$$\sigma^n = \sigma_1^n \sigma_2^n \cdots \sigma_p^n, \quad n \in \mathbb{Z}. \quad (8.13)$$

El lector no deberá creer, sin embargo, que toda potencia de un ciclo es a su vez un ciclo. Por ejemplo, $(1, 2, 3, 4)^2 = (1, 3)(2, 4)$. Nótese, sin embargo, que $(1, 2, 3, 4)^3 = (1, 4, 3, 2)$.

En lo que sigue, *convendremos en que e , la identidad de S_n , es también un ciclo, el cual denotaremos con (1):*

$$e = (1). \quad (8.14)$$

Diremos que $e = (1)$ es un *ciclo de longitud 1*: $l(e) = 1$. Cualquier otro ciclo σ tiene longitud $l(\sigma) > 1$. Diremos también que (1) es el *ciclo trivial* o el *ciclo degenerado*. Cualquier otro ciclo será *no trivial*. Es frecuente encontrar en la literatura que $(1) = (2) = (3) = \dots = (n)$. Nosotros evitaremos hacer uso de estas notaciones.

El siguiente es el teorema fundamental de la teoría de los grupos simétricos. Guardando las proporciones, es un análogo del lema 1.1 y de los teoremas 1.16 y 1.35 del capítulo 1, y juega un papel similar.

Teorema 8.1. Si $\sigma \in S_n$ y $\sigma \neq e$, existen ciclos disyuntos no triviales $\sigma_1, \dots, \sigma_p$, $p \geq 1$, tales que

$$\sigma = \sigma_1 \cdots \sigma_p. \quad (8.15)$$

En otras palabras, si $\sigma \in S_n$ y $\sigma \neq e$, σ es un ciclo no trivial o un producto de ciclos disyuntos no triviales.

Demostración. Si $n = 1$, $S_n = \{(1)\}$. Si $n = 2$, $S_n = \{(1), (1, 2)\}$. Si $n = 3$, $S_n = \{(1), (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$. Por lo tanto, la afirmación del teorema es evidente si $n = 1, 2, 3$. Supongamos entonces $n \geq 1$ arbitrario y sea $\sigma \in S_n$, $\sigma \neq e$. Sean O el orbital de σ e $i_1 = \min O$. Debe existir $k > 1$ tal que $\sigma^k(i_1) = i_1$ (por ejemplo, $k = o(\sigma)$). Sea $m_1 = \min\{k > 1 : \sigma^k(i_1) = i_1\}$, y considérese el ciclo $\sigma_1 = (i_1, \sigma(i_1), \dots, \sigma^{m_1-1}(i_1))$. Es claro que σ_1 es un ciclo basado en i_1 . Se dice que σ_1 es el ciclo con base i_1 determinado por σ . Sea O_1 el orbital de σ_1 . Es claro que si $O \setminus O_1 = \emptyset$ entonces $\sigma = \sigma_1$. En caso contrario, sean $i_2 = \min(O \setminus O_1)$, $m_2 = \min\{k > 1 : \sigma^k(i_2) = i_2\}$, σ_2 el ciclo basado en i_2 y de longitud m_2 determinado por σ , y O_2 su orbital. Continuando de esta manera, sean $i_p = \min(O \setminus (O_1 \cup O_2 \cup \dots \cup O_{p-1}))$, σ_p el ciclo basado en i_p y de longitud $m_p = \min\{k > 1 : \sigma^k(i_p) = i_p\}$ determinado por σ , y O_p su orbital. Como O es un conjunto finito, este proceso debe agotarlo en algún momento. Digamos $O = O_1 \cup \dots \cup O_p$, con $O_i \neq \emptyset$, $i = 1, 2, \dots, p$. Nótese que los conjuntos O_i , $i = 1, 2, \dots, p$, son dos a dos disyuntos, así que los ciclos σ_i , $i = 1, 2, \dots, p$, son disyuntos. Como además $\sigma(j) = \sigma_k(j)$ si $j \in O_k$, es claro que

$$\sigma = \sigma_1 \cdots \sigma_p \quad (8.16)$$

es una descomposición de σ como producto de ciclos disyuntos. $\square$

El proceso descrito en la demostración del teorema 8.1 es algorítmico y puede usarse para descomponer en ciclos disyuntos una permutación dada. Así,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 1 & 7 & 2 & 6 \end{pmatrix} = (1, 3, 4)(2, 5, 7, 6). \quad (8.17)$$

En este caso $p = 2$, $i_1 = 1$, $i_2 = 2$, $m_1 = 3$, $m_2 = 4$. En efecto, obsérvese en primer lugar que $\sigma(1) = 3$, $\sigma^2(1) = \sigma(3) = 4$, $\sigma^3(1) = \sigma^2(3) = \sigma(4) = 1$, así que σ_1 en la demostración del teorema 8.1 es $\sigma_1 = (1, 3, 4)$, $m_1 = 3$

y $O_1 = \{1, 3, 4\}$. En este caso $O \setminus O_1 = \{1, 2, 3, 4, 5, 6, 7\} \setminus \{1, 3, 4\} = \{2, 5, 6, 7\}$, y como $\sigma(2) = 5$, $\sigma^2(2) = \sigma(5) = 7$, $\sigma^3(2) = \sigma^2(5) = \sigma(7) = 6$, $\sigma^4(2) = \sigma(6) = 2$, se tendrá que $\sigma_2 = (2, 5, 7, 6)$, $m_2 = 4$, $O_2 = \{2, 5, 6, 7\}$. Como $O \setminus O_1 \cup O_2 = \emptyset$, el proceso terminará aquí y será $\sigma = \sigma_1 \sigma_2$. De manera análoga,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 7 & 4 & 5 & 6 & 9 & 8 \end{pmatrix} = (1, 3, 2)(4, 7, 6, 5)(8, 9) \quad (8.18)$$

y

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 5 & 6 & 1 & 3 & 2 \end{pmatrix} = (1, 7, 2, 4, 6, 3, 5) \quad (8.19)$$

Nota 8.7. De hecho, la descomposición (8.16) de σ en producto de ciclos disyuntos es, salvo tal vez por el orden de los factores, la única posible. En efecto, si σ está dada por (8.16) con σ_k como en la demostración del teorema 8.1, y también $\sigma = \rho_1 \dots \rho_q$, donde los ρ_k son ciclos disyuntos con ρ_k basado en j_k , dado que el orden de los ciclos en el producto es irrelevante, podemos suponer que $j_1 < \dots < j_q$, así que $j_1 = i_1$, y, como $\sigma^k(i_1) = \sigma_1^k(i_1) = \rho_1^k(i_1)$ para todo k , entonces $\sigma_1 = \rho_1 = (i_1, \sigma(i_1), \dots, \sigma^{m_1-1}(i_1))$, con m_1 como en la demostración del teorema. Esto implica que $\rho = \sigma_2 \dots \sigma_p = \rho_2 \dots \rho_q$, y un argumento inductivo permite concluir que $p = q$ y que $\sigma_i = \rho_i$, $i = 2, \dots, p$.

Si $\sigma \neq e$ es una permutación en S_n y $\sigma = \sigma_1 \dots \sigma_m$, $m \geq 1$, donde los σ_i son ciclos disyuntos no triviales, no hay obstáculo alguno para suponer que $l(\sigma_1) \leq l(\sigma_2) \leq \dots \leq l(\sigma_m)$. Como la descomposición $\sigma = \sigma_1 \dots \sigma_m$ es única, la m -pla $(l(\sigma_1), \dots, l(\sigma_m))$ es un invariante (una característica inmutable) de σ , denominado la estructura cíclica de σ . Por ejemplo, las permutaciones en (8.17), (8.18) y (8.19) tienen, respectivamente, las estructuras cíclicas (3,4), (2,3,4) y (7). Convendremos en que la estructura cíclica de e es (1).

Teorema 8.2. Si σ es un ciclo de S_n , el orden $o(\sigma)$ de σ como elemento de S_n es precisamente $l(\sigma)$, la longitud de σ . Así,

$$o((i_1, \dots, i_p)) = p. \quad (8.20)$$

Demostración. En efecto, si $\sigma = (i_1, \dots, i_p)$ entonces $\sigma = (i_1, \sigma(i_1), \dots, \sigma^{p-1}(i_1))$, así que $\sigma^{k-1}(i_1) = i_k \neq i_1$, $1 < k \leq p$, y $\sigma^p(i_1) = i_1$. Más generalmente, $\sigma = (i_j, \sigma(i_j), \dots, \sigma^{p-1}(i_j))$, $i \leq j \leq p$, también $\sigma^{k-1}(i_j) \neq i_j$, $1 < k \leq p$, y $\sigma^p(i_j) = i_j$, $j = 1, 2, \dots, p$. Se deduce que σ^p estabiliza a $i_1, \dots, i_p$, y como σ^p también estabiliza a $i \notin \{i_1, \dots, i_p\}$, entonces $\sigma^p = e$. Finalmente, como p es mínimo tal que $\sigma^p(i_1) = i_1$, necesariamente $p = o(\sigma)$. $\square$

Teorema 8.3. Si $\sigma \in S_n$ y $\sigma = \sigma_1 \cdots \sigma_p$, donde los σ_i son ciclos disyuntos no triviales, entonces

$$o(\sigma) = \text{mcm}(o(\sigma_1), \dots, o(\sigma_p)) = \text{mcm}(l(\sigma_1), \dots, l(\sigma_p)), \quad (8.21)$$

donde $\text{mcm}(a_1, \dots, a_p)$, $a_i \in \mathbb{Z}$, $a_i \neq 0$, es el mínimo común múltiplo de $a_1, \dots, a_p$ (capítulo 1, secciones 1.4 y 1.10).

Demostración. Sean $m_i = o(\sigma_i)$ y $m = \text{mcm}(m_1, \dots, m_p)$. Nótese que $m_i > 1$, $i = 1, 2, \dots, p$. Como $m_i \mid m$ para todo $i = 1, 2, \dots, p$, entonces $\sigma_i^m = e$ para todo $i = 1, 2, \dots, p$, y como $\sigma^m = \sigma_1^m \cdots \sigma_p^m$ (pues $\sigma_i \sigma_j = \sigma_j \sigma_i$, donde $1 \leq i, j \leq p$), entonces $\sigma^m = e$. Se concluye que $o(\sigma) \mid m$. Por otra parte, si $l = o(\sigma)$, entonces $\sigma^l = \sigma_1^l \cdots \sigma_p^l = e$. Esto implica que $\sigma_i^l = e$, $i = 1, 2, \dots, p$. En efecto, si fuera $\sigma_i^l \neq e$ para algún i , y $\sigma_i^l(k) \neq k$, necesariamente $\sigma_i(k) \neq k$, de lo cual $\sigma_j(k) = k$ y también $\sigma_j^l(k) = k$ para $j \neq i$. Pero entonces $\sigma^l(k) = \sigma_i^l(\rho(k))$ donde ρ es el producto de las σ_j^l , $j \neq i$, así que $\sigma^l(k) = \sigma_i^l(k) \neq k$ (ya que, evidentemente, $\rho(k) = k$). Esto es absurdo, pues $\sigma^l = e$, e implica que $m_i \mid l$, $i = 1, 2, \dots, p$. Entonces $m \mid l$, y así $m = l = o(\sigma)$. $\square$

El teorema 8.3 suministra entonces una aplicación útil de la descomposición en ciclos disyuntos para determinar el orden de una permutación.

Ejemplo 8.1. Las permutaciones en (8.17), (8.18) y (8.19) tienen órdenes respectivos 12, 12, 7. Además,

$$o\left(\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix}\right) = 2.$$

Definición 8.6. Si $(G, \cdot)$ es un grupo, H es un subgrupo de G y A es un subconjunto no vacío de H tal que todo elemento de H es el producto de un número finito de elementos de $A \cup A^{-1}$, donde $A^{-1} = \{a^{-1} : a \in A\}$, se dice que A es un *sistema de generadores* de H y que H es el *subgrupo de G generado por A* . Se escribe $H = [A]$. Si $H = G$, se dice que A es un *sistema de generadores* de G y que G está *generado por A* : $G = [A]$.

Nota 8.8. Como se verifica inmediatamente, $[A]$ es simplemente la intersección de todos los subgrupos de G que contienen a A .

Como toda permutación de S_n es un ciclo o un producto de ciclos, y los inversos de ciclos son a su vez ciclos, se tiene del teorema 8.1 que el conjunto

de los ciclos de S_n es un sistema de generadores de S_n . Aunque muy útil, el conjunto de los ciclos de S_n es un sistema muy grande de generadores. En lo que sigue, daremos sistemas de generadores más pequeños.

Teorema 8.4. El conjunto de todas las trasposiciones (i, j) , $1 \leq i < j \leq n$, es un sistema de generadores de S_n con $\binom{n}{2} = \frac{n(n-1)}{2}$ elementos.

Demostración. Es suficiente demostrar que todo ciclo $(i_1, \dots, i_p)$ es un producto de trasposiciones. Esto es fácil, pues evidentemente

$$(i_1, \dots, i_p) = (i_1, i_2)(i_1, i_3) \dots (i_1, i_p). \quad (8.22)$$

Como en S_n hay tantas trasposiciones como subconjuntos de dos elementos en $\{1, 2, \dots, n\}$, este número es $\binom{n}{2}$ (ejercicio 1.76). $\square$

Nota 8.9. El conjunto de todas las trasposiciones de S_n , aunque frecuentemente conveniente, es aún un sistema muy grande de generadores de S_n . Conviene en que $(i, j) = e$ si $i = j$, la relación

$$(i_1, \dots, i_p) = (1, i_1)(1, i_2) \dots (1, i_p)(1, i_1) \quad (8.23)$$

muestra que el conjunto $\{(1, j) : 1 < j \leq n\}$ es un sistema de generadores de S_n con sólo $n-1$ elementos. De hecho, para todo $i = 1, 2, \dots, n$, $\{(i, j) : 1 \leq i \leq n\}$ es un sistema de generadores de S_n con $n-1$ elementos, y 8.23 vale con i en lugar de 1.

La observación anterior da una descomposición en trasposiciones la cual es, en general, distinta de la descomposición (8.22). Es decir, la factorización en trasposiciones no es necesariamente única. Así, en S_4 , $(2, 3, 4) = (3, 4, 2) = (4, 2, 3)$, de lo cual $(2, 3, 4) = (2, 3)(2, 4) = (1, 2)(1, 3)(1, 4)(1, 2) = (3, 4)(2, 3) = (2, 4)(3, 4)$, etc. Más aún, se tiene el resultado siguiente, también frecuentemente útil.

Teorema 8.5. El conjunto $\{(1, 2), (2, 3), (3, 4), \dots, (n-1, n)\}$ es también un sistema de generadores de S_n con $n-1$ elementos.

Demostración. Es suficiente observar que si $1 < m \leq n$ entonces

$$(1, m) = (1, 2)(2, 3) \dots (m-1, m)(m-2, m-1) \dots (2, 3)(1, 2), \quad (8.24)$$

y usar la relación (8.23). $\square$

Nota 8.10. La descomposición de una permutación σ obtenida a partir de (8.24) involucra en general un gran número de permutaciones. Es, por lo tanto, de más valor teórico que práctico. De acuerdo con todo lo anterior, para obtener una descomposición en trasposiciones de una permutación lo más conveniente es obtener primero su descomposición en ciclos disyuntos y luego recurrir a una cualquiera de las relaciones (8.22), (8.23) u (8.24), según lo que se quiera o sea más conveniente. Así,

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 1 & 7 & 2 & 6 \end{pmatrix} &= (1, 3, 4) (2, 5, 7, 6) \\ &= (1, 3) (1, 4) (2, 5) (2, 7) (2, 6) \\ &= (1, 3) (1, 4) (1, 2) (1, 5) (1, 7) (1, 6) (1, 2). \end{aligned}$$

Nótese que también que $(1, 3, 4) = (4, 1, 3) = (4, 1)(4, 3)$ y $(2, 5, 7, 6) = (5, 7)(5, 6)(5, 2)$, etc. A su vez,

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

La descomposición en trasposiciones no es, en general, una descomposición en ciclos disyuntos. Observamos también que si $\sigma = (i, j)$ es una trasposición, considerada como una función de $\{1, \dots, n\}$ en sí mismo, σ está caracterizada por $\sigma(k) = (i, j)(k) = k$ si $k \neq i, j$, mientras que $\sigma(i) = (i, j)(i) = j$ y $\sigma(j) = (i, j)(j) = i$. Esta observación es importante en la demostración del siguiente teorema.

Teorema 8.6. Si (i, j) es una trasposición, entonces

$$(\sigma(i), \sigma(j)) = \sigma \circ (i, j) \circ \sigma^{-1} = \sigma^{-1}(i, j)\sigma \quad (8.25)$$

cualquiera que sea la permutación σ .

Demostración. Verifiquemos que $(i, j) = \sigma^{-1} \circ (\sigma(i), \sigma(j)) \circ \sigma$. Ahora, si $k \neq i, j$, entonces $(\sigma(i), \sigma(j))(\sigma(k)) = \sigma(k)$, pues $\sigma(k) \neq \sigma(i), \sigma(j)$. Entonces $\sigma^{-1}(\sigma(i), \sigma(j))(\sigma(k)) = \sigma^{-1}(\sigma(k)) = k$ y, como es claro, también $(i, j)(k) = k$. Por otra parte, si $k = i$ entonces $\sigma^{-1}((\sigma(i), \sigma(j))(\sigma(i))) = \sigma^{-1}(\sigma(j)) = j$, y también $(i, j)(i) = j$. La verificación para $k = j$ es semejante. $\square$

Corolario 8.1. Si $(i_1, i_2, \dots, i_p)$ es un ciclo, entonces

$$\sigma \circ (i_1, \dots, i_p) \circ \sigma^{-1} = (\sigma(i_1), \dots, \sigma(i_p)) = \sigma^{-1}(i_1, \dots, i_p)\sigma \quad (8.26)$$

cualquiera que sea la permutación σ .

Demostración. En efecto, $\sigma^{-1}(i_1, \dots, i_p)\sigma = \sigma^{-1}((i_1, i_2)(i_1, i_3)\dots(i_1, i_p)\sigma = (\sigma^{-1}(i_1, i_2)\sigma)(\sigma^{-1}(i_1, i_3)\sigma)\dots(\sigma^{-1}(i_1, i_p)\sigma) = (\sigma(i_1), \sigma(i_2))(\sigma(i_1), \sigma(i_3))\dots(\sigma(i_1), \sigma(i_p)) = (\sigma(i_1), \sigma(i_2), \dots, \sigma(i_p))$. $\square$

Nota 8.11. Las relaciones (8.25) y (8.26) son de gran importancia en la teoría del grupo $(S_n, \cdot)$. Se deduce que dados dos ciclos $(i_1, \dots, i_p)$ y $(j_1, \dots, j_p)$ de la misma longitud, existe una permutación σ tal que

$$(j_1, \dots, j_p) = \sigma^{-1}(i_1, \dots, i_p)\sigma. \quad (8.27)$$

De hecho, (8.27) es válida para cualquier permutación σ tal que $\sigma(i_1) = j_1$, $\sigma(i_2) = j_2, \dots, \sigma(i_p) = j_p$. Nótese que, como $(j_1, \dots, j_p) = (j_2, \dots, j_p, j_1) = (j_3, \dots, j_p, j_1, j_2) = \dots = (j_p, j_1, \dots, j_{p-1})$, esto da lugar, al menos, a p permutaciones distintas. Lo anterior se expresa diciendo que, en S_n , dos ciclos de la misma longitud son siempre conjugados. Más aún:

Teorema 8.7. En S_n , dos permutaciones σ y ρ con la misma estructura cíclica son conjugadas. Es decir, existe $\tau \in S_n$ tal que

$$\rho = \tau^{-1}\sigma\tau. \quad (8.28)$$

Demostración. Si σ es un ciclo, también lo es ρ , y de la misma longitud. La afirmación resulta entonces de lo dicho en la nota 10.11. Supóngase entonces que $\sigma = \sigma_1\sigma_2 \dots \sigma_m$, $\rho = \rho_1\rho_2 \dots \rho_m$, donde $m > 1$ y $\sigma_1, \dots, \sigma_m$ y $\rho_1, \dots, \rho_m$ son ciclos disyuntos, $\sigma_k = (i_{k1}, \dots, i_{kp_k})$, $\rho_k = (j_{k1}, \dots, j_{kp_k})$. La disyunción de los ciclos asegura la existencia de $\tau \in S_n$ tal que $\tau(i_{kh}) = j_{kh}$, $k = 1, 2, \dots, m$, $1 \leq h \leq p_k$, así que $\rho_k = \tau^{-1}\sigma_k\tau$, $k = 1, 2, \dots, m$. Entonces, $\rho = \tau^{-1}\sigma_1\sigma_2 \dots \sigma_m\tau = (\tau^{-1}\sigma_1\tau) \dots (\tau^{-1}\sigma_m\tau) = \rho_1 \dots \rho_m$, y la afirmación queda demostrada. $\square$

El teorema 8.7 anterior es de vital importancia en la teoría del grupo simétrico.

Ejemplo 8.2. Las siguientes permutaciones $\rho = (3, 5, 7)(8, 9)(2, 4, 10, 12)$ y $\tau = (2, 4, 8)(6, 7)(3, 5, 9, 11)$ de S_{12} tienen la misma estructura cíclica. Si, por ejemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 3 & 2 & 5 & 4 & 10 & 8 & 6 & 7 & 9 & 12 & 11 \end{pmatrix},$$

entonces $\sigma^{-1}\rho\sigma = \tau$.

Nota 8.12. Si σ y ρ son permutaciones conjugadas en S_n entonces σ y ρ tienen la misma estructura cíclica. En efecto, si $\rho = \tau^{-1}\sigma\tau$, la afirmación es clara si $\sigma = (i_1, \dots, i_p)$ es un p -ciclo, pues será $\rho = (\tau(i_1), \dots, \tau(i_p))$, el cual es también un p -ciclo; y si $\sigma = \sigma_1 \cdots \sigma_n$, $n \geq 2$, donde los σ_i son ciclos disyuntos no triviales, entonces $\rho = \rho_1 \cdots \rho_n$ donde $\rho_i = \tau^{-1}\sigma_i\tau$, $i = 1, 2, \dots, n$, ρ_i es un ciclo de la misma longitud de σ_i , y los σ_i son disyuntos. Por otra parte, si τ y σ tienen la misma estructura cíclica $(l_1, \dots, l_m)$, de lo dicho en la nota 8.11 se deduce que habrá al menos $l = l_1 l_2 \cdots l_m$ permutaciones τ tales que $\tau^{-1}\sigma\tau = \rho$. Por ejemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 9 & 8 & 11 & 2 & 10 & 4 & 7 & 6 & 3 & 1 & 5 \end{pmatrix}$$

también hará el trabajo del ejemplo 8.2.

Para terminar la discusión sobre los generadores de S_n , daremos un resultado que suministra un sistema minimal de generadores.

Teorema 8.8. Si $\tau = (1, 2)$ y $\sigma = (1, 2, \dots, n)$, $\{\tau, \sigma\}$ es un sistema de generadores de S_n , $n \geq 2$.

Demostración. Sea $\sigma = (1, 2, \dots, n)$. Como es claro, si $0 \leq k \leq n-2$, $\sigma^k(1) = k+1$, $\sigma^k(2) = k+2$, así que

$$(k+1, k+2) = \sigma^{-k}(1, 2)\sigma^k = (\sigma^k(1), \sigma^k(2)), \quad (8.29)$$

donde $\sigma^{-k} = (\sigma^k)^{-1} = (\sigma^{-1})^k$. Como $\{(1, 2), \dots, (n-1, n)\}$ es un sistema de generadores de S_n , toda permutación de S_n es también un producto apropiado de las permutaciones τ , σ y σ^{-1} . $\square$

Nota 8.13. Obsérvese, por ejemplo, que, en S_4 , y con $\sigma = (1, 2, 3, 4)$, se tiene que

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

lo cual da una expresión de $(1, 4)$ en términos de $(1, 2)$, $(1, 2, 3, 4)$ y $(1, 2, 3, 4)^{-1} = (4, 3, 2, 1)$. Obsérvese también que $(2, 3) = (1, 4, 3, 2)(1, 2)$

$$(1, 2, 3, 4); (3, 4) = (1, 4, 3, 2)^2(1, 2)(1, 2, 3, 4)^2 = (1, 3)(2, 4)(1, 2)(1, 3)(2, 4);$$

$$(1, 3) = (1, 2)(2, 3)(1, 2) = (1, 2)(1, 4, 3, 2)(1, 2)(1, 2, 3, 4)(1, 2), \text{ etc.}$$

El siguiente resultado será útil en lo que sigue.

Teorema 8.9. Si $n \geq 3$, el centro $Z(S_n)$ de S_n se reduce a $\{e\}$, donde $e \in S_n$ es la permutación idéntica.

Demostración. Sea $\sigma \in Z(S_n)$, así que $\sigma^{-1}\rho\sigma = \rho$ cualquiera que sea $\rho \in S_n$. Si fuera $\sigma \neq e$, existiría $1 \leq i \leq n$ tal que $j = \sigma(i) \neq i$ y, como $n \geq 3$, también existiría $k \neq i, j$. Pero entonces $\sigma^{-1}(i, k)\sigma = (\sigma(i), \sigma(k)) = (j, \sigma(k)) \neq (i, k)$, lo cual es absurdo. $\square$

Nota 8.14. Para $n = 1, 2$, $Z(S_n) = S_n$.

Nota 8.15. Obsérvese que para que $\sigma \in Z(S_n)$ es necesario y suficiente que $\sigma^{-1}\tau\sigma = \tau$ para toda transposición τ . En efecto, si $\rho \in S_n$ entonces $\rho = \tau_1 \cdots \tau_m$ donde las τ_i son trasposiciones, y entonces $\sigma^{-1}\rho\sigma = (\sigma^{-1}\tau_1\sigma)(\sigma^{-1}\tau_2\sigma) \cdots (\sigma^{-1}\tau_m\sigma) = \tau_1 \cdots \tau_m = \rho$.

Definición 8.7. Para una permutación $\sigma \in S_n$, definimos

$$\mathcal{E}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \quad (8.30)$$

El número $\mathcal{E}(\sigma)$ se denomina el signo de σ en S_n .

Para el significado de la notación en (8.30), véase la sección 1.6 del capítulo 1.

Como $\sigma(i) = 1, 2, \dots, n$ si $i = 1, 2, \dots, n$ y $\sigma(i) \neq \sigma(j)$ si $i < j$, entonces

$$\mathcal{E}(\sigma) = \frac{\prod_{i < j} (\sigma(i) - \sigma(j))}{\prod_{i < j} (i - j)} = \pm 1,$$

ya que el producto en el numerador incluye, salvo tal vez por el signo, los mismos $\binom{n}{2}$ factores que el del denominador (puede ser que $\sigma(i) > \sigma(j)$ para $i < j$). Así, es evidente que $\mathcal{E}(e) = 1$, mientras que si $\sigma = (1, 2)$ entonces $\mathcal{E}(\sigma) = -1$. Esto último resulta simplemente de observar que las posibles parejas (i, j) con $i < j$ son $(1, 2)$, para la cual $(\sigma(i) - \sigma(j)) / (i - j) = (2 - 1) / (1 - 2) = -1$; las $(1, j)$ con $2 < j \leq n$, para las cuales

$$\frac{\sigma(i) - \sigma(j)}{i - j} = \frac{\sigma(1) - \sigma(j)}{1 - j} = \frac{2 - j}{1 - j} > 0;$$

las $(2, j)$ con $2 < j \leq n$, en cuyo caso

$$\frac{\sigma(i) - \sigma(j)}{i - j} = \frac{\sigma(2) - \sigma(j)}{2 - j} = \frac{1 - j}{2 - j} > 0;$$

y las (i, j) con $i > 2$, para las que $(\sigma(i) - \sigma(j)) / (i - j) = (i - j) / (i - j) = 1$. Así, sólo $(\sigma(1) - \sigma(2)) / (1 - 2) = -1 < 0$. Nótese que $\mathcal{E}(e)$ y $\mathcal{E}(1, 2)$ son independientes de n .

Teorema 8.10. La aplicación $\mathcal{E} : S_n \mapsto \{-1, 1\}$, con $\mathcal{E}(\sigma)$ dado por (8.30), es un homomorfismo de S_n en el grupo multiplicativo $\{-1, 1\}$, y un epimorfismo si $n \geq 2$.

Demostración. En efecto, si $\sigma, \rho \in S_n$ y $\tau = \sigma\rho$, entonces

$$\begin{aligned} \mathcal{E}(\tau) &= \prod_{i < j} \frac{\tau(i) - \tau(j)}{i - j} = \prod_{i < j} \frac{\rho(\sigma(i)) - \rho(\sigma(j))}{i - j} \\ &= \prod_{i < j} \frac{\rho(\sigma(i)) - \rho(\sigma(j))}{\sigma(i) - \sigma(j)} \cdot \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= \prod_{i < j} \frac{\rho(\sigma(i)) - \rho(\sigma(j))}{\sigma(i) - \sigma(j)} \cdot \prod_{i < j} \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= \prod_{i < j} \frac{\rho(i) - \rho(j)}{i - j} \cdot \prod_{i < j} \frac{\sigma(i) - \sigma(j)}{i - j}. \end{aligned}$$

La última igualdad resulta de observar que $\sigma(i) \neq \sigma(j)$ si $i < j$, y de

$$\frac{\rho(\sigma(i)) - \rho(\sigma(j))}{\sigma(i) - \sigma(j)} = \frac{\rho(\sigma(j)) - \rho(\sigma(i))}{\sigma(j) - \sigma(i)}.$$

Entonces $\mathcal{E}(\tau) = \mathcal{E}(\rho)\mathcal{E}(\sigma) = \mathcal{E}(\sigma)\mathcal{E}(\rho)$ y $\mathcal{E}$ es así un homomorfismo. Como $\mathcal{E}(e) = 1$ mientras que $\mathcal{E}(1, 2) = -1$ si $n \geq 2$, $\mathcal{E}$ es un epimorfismo en este caso. $\square$

Corolario 8.2. Si $\rho \in S_n$, $n \geq 2$, es cualquier transposición, entonces $\mathcal{E}(\rho) = -1$.

Demostración. Hemos visto que $\mathcal{E}(\tau) = -1$ si $\tau = (1, 2)$. Sean $\rho = (i, j)$ y σ una permutación de S_n tal que $\sigma(1) = i$, $\sigma(2) = j$. Entonces $\sigma^{-1}\tau\sigma = \rho$, de lo cual $\mathcal{E}(\rho) = \mathcal{E}(\sigma^{-1})\mathcal{E}(\tau)\mathcal{E}(\sigma) = \mathcal{E}(\sigma^{-1})\mathcal{E}(\sigma)\mathcal{E}(\tau) = \mathcal{E}(\sigma^{-1}\sigma)\mathcal{E}(\tau) = \mathcal{E}(e)(-1) = -1$. $\square$

Como hemos visto, una permutación puede admitir muchas factorizaciones distintas como producto de trasposiciones. Sin embargo:

Corolario 8.3. En cualquier factorización en trasposiciones de una permutación dada σ de S_n , el número de éstas es siempre par o siempre impar. Este número es par si $\mathcal{E}(\sigma) = 1$, e impar si $\mathcal{E}(\sigma) = -1$.

Demostración. Si $\sigma = \sigma_1 \cdots \sigma_m$, donde las σ_i son trasposiciones, entonces $\mathcal{E}(\sigma) = \mathcal{E}(\sigma_1)\mathcal{E}(\sigma_2) \cdots \mathcal{E}(\sigma_m) = (-1)^m$. Como $\mathcal{E}(\sigma) = 1$ o $\mathcal{E}(\sigma) = -1$, pero no ambos, m será siempre par o siempre impar. $\square$

Corolario 8.4. Si σ es un ciclo de S_n de longitud p ,

$$\mathcal{E}(\sigma) = (-1)^{p-1} \quad (8.31)$$

Por lo tanto, $\mathcal{E}(\sigma) = 1$ si y sólo si p es impar.

Demostración. Si $\sigma = (i_1, \dots, i_p)$, entonces, de (8.22), σ es el producto de las $(p-1)$ transposiciones (i_1, i_k) , $k = 2, \dots, p$. $\square$

Nota 8.16. Obsérvese que si σ es un ciclo, $\mathcal{E}(\sigma)$ es independiente de n en tanto $\sigma \in S_n$. A través de su descomposición en ciclos, podemos considerar que una permutación $\sigma \in S_m$ también pertenece a S_n para todo $n \geq m$. De hecho, σ se identifica con la permutación $\hat{\sigma}$ de S_n dada por $\hat{\sigma}(i) = \sigma(i)$, $1 \leq i \leq m$, y por $\hat{\sigma}(i) = i$, si $m < i \leq n$. Como es claro σ y $\hat{\sigma}$ tienen la misma descomposición en ciclos disyuntos, así que $\mathcal{E}(\sigma) = \mathcal{E}(\hat{\sigma})$. Es decir, $\mathcal{E}(\sigma)$ es también independiente de n en tanto $\sigma \in S_n$.

Definición 8.8. El núcleo $\ker(\mathcal{E})$ del homomorfismo $\mathcal{E} : S_n \mapsto \{-1, 1\}$ se denomina el grupo alternante de n objetos y se denota con $\mathcal{A}_n$.

Entonces $\mathcal{A}_n = \{\sigma \in S_n : \mathcal{E}(\sigma) = 1\}$, así que $\sigma \in \mathcal{A}_n$ si y sólo si es el producto de un número par de transposiciones. Como además $\mathcal{A}_1 = S_1 = \{(1)\}$, mientras que (teorema 6.2) $S_n/\mathcal{A}_n \approx \{-1, 1\}$ para $n \geq 2$, se deduce que

$$o(\mathcal{A}_n) = \frac{1}{2}n!, \quad n \geq 2. \quad (8.32)$$

Nótese que si $n \geq 3$, todo 3-ciclo (ciclo de longitud 3) $(i, j, k) = (i, j)(i, k)$ pertenece a $\mathcal{A}_n$ (si $n = 1, 2$, no hay, de hecho, 3-ciclos). Más aún:

Teorema 8.11. Los 3-ciclos forman, para $n \geq 3$, un sistema de generadores de $\mathcal{A}_n$.

Demostración. Es suficiente demostrar que el producto de dos transposiciones es, a su vez, un 3-ciclo o un producto de 3-ciclos. Ahora, si i, j, h, k son todos distintos, entonces

$$(i, j)(h, k) = (i, j, h)(h, i, k), \quad (8.33)$$

y si i, j, k son distintos

$$(i, j)(i, k) = (i, j, k). \quad (8.34)$$

Finalmente

$$(i, j)^2 = (1, 2, 3)^3.$$

Esto demuestra el teorema. $\square$

Como consecuencia de lo dicho en la nota 8.11 o de lo establecido en el teorema 8.7, se deduce que dos 3-ciclos de S_n son siempre conjugados. Por lo tanto:

Corolario 8.5. Si un subgrupo normal H de S_n contiene un 3-ciclo entonces H contiene a todo 3-ciclo y $A_n \subseteq H$. Si H es un subgrupo propio de S_n , necesariamente $H = A_n$.

Demostración. Si ρ es un 3-ciclo en H , cualquier otro 3-ciclo σ se escribe en la forma $\sigma = \tau^{-1}\rho\tau$ donde $\tau \in S_n$. Como H es normal, también $\sigma \in H$. Como A_n está generado por los 3-ciclos, $A_n \subseteq H$. Finalmente, si $H \neq S_n$ entonces $[S_n : H] \geq 2$. Pero $A_n \subseteq H$. Entonces $[S_n : H] \leq [S_n : A_n] = 2$. Se concluye que $[S_n : H] = 2$, de lo cual, $H = A_n$. $\square$

De hecho, si $n \geq 5$, se puede decir mucho más.

Teorema 8.12. Si $n \geq 5$ y H es un subgrupo normal propio de S_n , necesariamente $H = A_n$.

Demostración. Es suficiente demostrar que H contiene un 3-ciclo. Sea $\sigma \in H, \sigma \neq e$. Como $Z(S_n) = \{e\}$ entonces $\sigma \notin Z(S_n)$, y deberá existir una transposición $\tau \in S_n$ tal que $\sigma^{-1}\tau\sigma \neq \tau$ (nota 8.15). Sea $\tau_1 = \sigma^{-1}\tau\sigma$. También τ_1 es una transposición y $\tau_1\tau = \sigma^{-1}(\tau\sigma\tau) = \sigma^{-1}(\tau^{-1}\sigma\tau) \in H$, ya que $\sigma^{-1} \in H$ y $\tau^{-1}\sigma\tau \in H$, pues $\sigma \in H$ y H es normal.

Ahora, si $\tau_1 = (i, j)$ y $\tau = (i, k)$, donde i, j, k son distintos, entonces $(i, j, k) = \tau_1\tau \in H$, y la afirmación queda demostrada en este caso. Supon-

gamos entonces $\tau_1 = (i, j)$, $\tau = (h, k)$, donde i, j, h, k son distintos, y sea $1 \leq l \leq n$, l distinto de i, j, h, k (el cual existe pues $n \geq 5$). Claramente $(i, l)\tau_1\tau(i, l)^{-1} = (i, l)(i, j)(h, k)(i, l) = (l, j)(h, k) \in H$ y, como $(i, j)(h, k)(l, j)(h, k) = (i, l, j)$, también $(i, l, j) \in H$. En virtud del corolario 8.5, esto demuestra el teorema. $\square$

Para $n \geq 5$ se tiene el siguiente resultado.

Teorema 8.13. Si $n \geq 5$ y σ, ρ son 3-ciclos en S_n , existe $\tau \in A_n$ tal que $\rho = \tau^{-1}\sigma\tau$. Es decir, σ y ρ , que son conjugados en S_n , son aún conjugados en A_n .

Demostración. Supóngase que $\sigma = (i_1, i_2, i_3)$ y sean $i_4 \neq i_5$ y distintos de i_1, i_2, i_3 . Como es claro, $(i_4, i_5)(i_1, i_2, i_3)(i_4, i_5) = (i_1, i_2, i_3)$. Sea $\tau_0 \in S_n$ tal que $\rho = \tau_0^{-1}\sigma\tau_0$. Si $\tau_0 \in A_n$, no hay nada que demostrar. Si $\tau_0 \notin A_n$, sea $\tau = (i_4, i_5)\tau_0$. Entonces $\tau \in A_n$ y $\tau^{-1}\sigma\tau = \tau_0^{-1}(i_4, i_5)\sigma(i_4, i_5)\tau_0 = \tau_0^{-1}\sigma\tau_0 = \rho$, y la afirmación es válida también en este caso. $\square$

Nota 8.17. Sean $n = 3, 4$ y $\sigma \in S_n$. Como $(1, 3, 2) = \sigma^{-1}(1, 2, 3)\sigma = (\sigma(1), \sigma(2), \sigma(3))$ implica que σ es una de las transposiciones $(1, 2)$, $(2, 3)$ ó $(1, 3)$, se deduce que $(1, 2, 3)$ y $(1, 3, 2)$ no son conjugados en A_n , $n = 3, 4$.

Corolario 8.6. Si un subgrupo normal H de A_n , $n \geq 5$, contiene un 3-ciclo, necesariamente $H = A_n$.

Demostración. En efecto, el teorema 8.13 asegura que H contiene a todo 3-ciclo, de lo cual $A_n \subseteq H$. $\square$

Definición 8.9. Si un grupo G no tiene subgrupos normales propios, se dice que G es un grupo simple.

Así, todo grupo de orden primo es necesariamente simple. Como $A_1 = A_2 = \{(1)\}$ y A_3 tiene orden 3, A_n es simple para $n = 1, 2, 3$. El grupo A_4 no es simple. En efecto $o(A_4) = 12$ y, como se verifica inmediatamente,

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

es un subgrupo de A_4 (hágase una tabla), el cual es normal en S_4 , y por ende en A_4 , pues si $1 \leq i_1, i_2, i_3, i_4 \leq 4$ son todos distintos, y $\sigma \in S_4$, entonces $\sigma(i_1), \sigma(i_2), \sigma(i_3)$ y $\sigma(i_4)$ también son distintos y $\sigma^{-1}(i_1, i_2)(i_3, i_4)\sigma = (\sigma^{-1}(i_1, i_2)\sigma)(\sigma^{-1}(i_3, i_4)\sigma) = (\sigma(i_1), \sigma(i_2))(\sigma(i_3), \sigma(i_4))$, así que $\sigma^{-1}V\sigma = V$.

V. El grupo V se conoce como el 4 grupo de Klein. Como se verifica fácilmente, $V \approx \mathbb{Z}_2 \times \mathbb{Z}_2$.

En lo que sigue, demostraremos que A_n es simple para $n \geq 5$. La demostración, aunque no es difícil, es algo larga y delicada. Obsérvese antes que si G es un grupo y H es un subgrupo de G ,

$$N(H) = \{a \in G : aHa^{-1} = H\} \quad (8.35)$$

es evidentemente un subgrupo de G , denominado el *normalizador* de H (véase, al respecto, el capítulo 9). Como es claro, H es un subgrupo normal de $N(H)$. Más aún, si H' es un subgrupo de G y H es un subgrupo normal de H' , entonces H' es un subgrupo de $N(H)$. Así, H es normal en G si y sólo si $N(H) = G$.

Lema 8.1. Si $n \geq 5$ y $n!/2$ no es un cuadrado perfecto, A_n es simple.

Demostración. Supóngase que A_n no es simple y que M sea un subgrupo normal propio de A_n con el mínimo orden posible. Si fuera $N(M) = S_n$, M sería normal en S_n , y el teorema 8.12 aseguraría que $M = A_n$, lo cual es absurdo. Como $A_n \subseteq N(M)$ (pues M es normal en A_n), necesariamente $[S_n : N(M)] = 2$, y entonces $N(M) = A_n$. Ahora, si $\sigma = (1, 2)$ entonces $\sigma \notin A_n = N(M)$, de lo cual, $N = \sigma M \sigma^{-1} \neq M$. Sin embargo, como $\sigma^{-1} A_n \sigma = A_n$, N es aún un subgrupo de A_n , evidentemente normal, con $o(N) = o(M)$. Se deduce que MN y $M \cap N$ son subgrupos normales de A_n . Como $N \neq M$, necesariamente $M \cap N \neq M$, y como el orden de M como subgrupo normal de A_n es mínimo posible, serán $M \cap N = \{e\}$ y $o(MN) = o(M)^2$. Pero si $H = MN$ entonces $A_n \subseteq N(H)$, y como $(1, 2) \in N(H)$, deberá ser $N(H) = S_n$, lo cual, según el teorema 8.12, implica que $H = A_n$ y $o(A_n) = o(M)^2$. Esto es absurdo, y garantiza que A_n es simple. $\square$

Como $n!/2$ no es un cuadrado perfecto si $n = 5, 6, 7$ ($5!/2 = 60$, $6!/2 = 360$, $7!/2 = 2520$), se deduce que si A_n no es simple, $n \neq 4$, necesariamente $n > 7$.

Nota 8.18. De hecho, si $n > 2$, $n!/2$ nunca es un cuadrado perfecto, pero esto no es fácil de demostrar, y no podremos hacer uso de este resultado. Entonces, deberemos demostrar aún que:

Teorema 8.14 Si $n > 7$, A_n es un grupo simple.

La demostración requiere el siguiente lema.

Lema 8.2 Si $n \geq 4$, $Z(A_n) = \{e\}$.

Demostración. Sean $\sigma \in A_n$, $\sigma \neq e$, e i, j tales que $j = \sigma(i) \neq i$. Si $\sigma(j) = i$ y $h \neq i, j$, entonces $\sigma^{-1}(i, j, h)\sigma = (\sigma(i), \sigma(j), \sigma(h)) = (j, i, \sigma(h)) \neq (i, j, h)$, y $\sigma \notin Z(A_n)$. Si $\sigma(j) \neq i$, sean h, k tales que i, j, h, k sean distintos. Entonces $\sigma^{-1}(i, j)(h, k)\sigma = (\sigma(i), \sigma(j))(\sigma(h), \sigma(k)) = (j, \sigma(j))(\sigma(h), \sigma(k)) \neq (i, j)(h, k)$, pues los ciclos que aparecen en los productos son disyuntos y $(j, \sigma(j)) \neq (j, i)$. Entonces, tampoco $\sigma \in Z(A_n)$ en este caso. $\square$

Demostración del teorema 8.14. Supóngase que A_n no es simple, y sea H un subgrupo normal propio de A_n . Sea $\sigma \in H$, $\sigma \neq e$. Como $Z(A_n) = \{e\}$, debe existir un 3-ciclo $\tau \in A_n$ tal que $\sigma^{-1}\tau\sigma \neq \tau$. Claramente $e \neq \rho = \sigma^{-1}(\tau\sigma\tau^{-1}) \in H$ (pues $\sigma^{-1}, \tau\sigma\tau^{-1} \in H$). Pero $\rho = (\sigma^{-1}\tau\sigma)\tau^{-1}$, y tanto $\sigma^{-1}\tau\sigma$ como τ^{-1} son 3-ciclos (no necesariamente disyuntos). Digamos $\sigma^{-1}\tau\sigma = (i_1, i_2, i_3)$ y $\tau^{-1} = (i_4, i_5, i_6)$. Nótese que si $p = \#\{i_1, \dots, i_6\}$ entonces $p \geq 4$ (de otra manera $p = 3$, y el producto de (i_1, i_2, i_3) por (i_4, i_5, i_6) sería la identidad o un 3-ciclo, lo cual, en virtud del corolario 8.6, es absurdo, pues $e \neq \rho \in H$). Sean $i_7 \neq i_1, \dots, i_6$, el cual existe pues $n > 7$, y N el subgrupo de A_n de las permutaciones pares que dejan fijo a todo $i \neq i_1, \dots, i_7$. Como $5 \leq m = p + 1 \leq 7$ y N es isomorfo a A_m , N es un subgrupo simple de A_n , y como $e \neq \rho \in H \cap N$, entonces $H \cap N = N$ y $N \subseteq H$. Pero, como $(i_1, i_2, i_3) \in N$, necesariamente (corolario 8.6) $H = A_n$, lo cual es absurdo. Entonces, A_n es simple. $\square$

Los grupos A_n , $n \neq 4$, son entonces una familia infinita de grupos finitos simples. Existen algunas otras familias infinitas de grupos finitos simples (entre ellas, los grupos de orden primo) y 26 grupos finitos simples no ubicables dentro de ninguna de tales familias. Los grupos finitos simples son, en cierta forma, los pilares sobre los cuales se construyen todos los grupos finitos, de lo cual su importancia, que justifica el enorme esfuerzo realizado para su clasificación, la cual se completó en la década de 1970 a 1980: un trabajo descomunal que comprende más de diez mil páginas impresas y que representa uno de los grandes logros de la matemática del Siglo XX. La simplicidad de A_n para $n \geq 5$ está también relacionada con la resolubilidad de las ecuaciones polinómicas de grado ≥ 5 , y es por lo tanto importante en la teoría de los campos y, en especial, en la teoría de Galois.

EJERCICIOS

8.1 En cada uno de los casos siguientes calcule la factorización en ciclos disyuntos de σ , su estructura cíclica, su orden y $\mathcal{E}(\sigma)$.

a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$

b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}$

c) $(1, 2, 3, 5, 7)(2, 4, 7, 6)$

d) $(1, 2, 3)^{-1}(3, 5, 7, 9)(1, 2, 3)$

e) $(1, 2)(1, 3)(1, 4)$

f) Demuestre que si $\sigma \in S_n$ y $(l_1, \dots, l_m)$ es su estructura cíclica, entonces $\mathcal{E}(\sigma) = (-1)^{l_1+l_2+\dots+l_m-m}$.

8.2 Exprese cada una de las siguientes permutaciones, si es posible, como producto de 3-ciclos.

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix}$

c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix}$

d) $(1, 3)(1, 5)(2, 4)(6, 7)$

8.3 Verifique que no es posible que exista $\sigma \in S_n$, $n \geq 7$, tal que $\sigma^{-1}(1, 2, 3)\sigma = (1, 2, 4)(5, 6, 7)$. Demuestre, más generalmente, que si ρ es un ciclo de S_n , no es posible que existan dos ciclos disyuntos no triviales τ_1, τ_2 y $\sigma \in S_n$, tales que $\sigma^{-1}\rho\sigma = \tau_1\tau_2$.

8.4 Sea $p \leq q$ un número primo. Demuestre que los únicos elementos de orden p de S_n son los p -ciclos o los productos finitos de p -ciclos disyuntos.

8.5 Demuestre que si $1 \leq k \leq n$, el número de k -ciclos de S_n es $\frac{n!}{k(n-k)!}$.

8.6 Explique por qué si $n \geq 4$ y $\sigma, \sigma \neq e$, debe existir un 3-ciclo τ tal que $\sigma^{-1}\tau\sigma \neq \tau$.

8.7 Demuestre que si p es primo, $p \nmid k$ y σ es un p -ciclo, entonces $\sigma(\sigma^k) = p$ y σ^k es un p -ciclo. Concluya que si $1 \leq k < p$ entonces σ^k es un p -ciclo.

8.8 Demuestre que si n es impar, A_n está generado por los n -ciclos. (Indicación. Demuestre que si H es el subgrupo de A_n generado por los n -ciclos, $H \neq \{e\}$ y es normal en S_n .)

8.9 Demuestre, más generalmente, que si $3 \leq p \leq n$ y p es impar, los p -ciclos generan A_n .

8.10 Sea $n \geq 3$. Demuestre que cualesquiera que sean $1 \leq i_1, \dots, i_n \leq n$, el n -ciclo $(i_1, i_2, \dots, i_n)$ y la transposición (i_1, i_2) generan a S_n . Demuestre además que si n es primo, cualquier n -ciclo y cualquier transposición generan a S_n . (Indicación. Si n es primo y σ es un n -ciclo, dados $1 \leq i \neq j \leq n$, existe $1 \leq k \leq n$ tal que $\sigma^k(i) = j$ y σ^k es aún un n -ciclo). ¿Es esto último cierto si n es arbitrario?

8.11 Demuestre que si un subgrupo H de S_n contiene una permutación impar entonces $o(H)$ es par y la mitad de los elementos de H son permutaciones impares. (Indicación. Demuestre que $H/H \cap A_n \approx H A_n / A_n = S_n / A_n$).

8.12 Demuestre que si $m < n$, S_m y A_m son respectivamente isomorfos a subgrupos de S_n y A_n . Demuestre además que $V = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ es un subgrupo de A_n para todo $n \geq 4$, el cual es normal en A_n si y sólo si $n = 4$.

8.13 Sean $\sigma \in S_n$ un n -ciclo, $1 \leq k < n$, $m = \text{mcd}(n, k)$. Demuestre que σ^k tiene orden n/m . Supóngase que $\sigma^k = \rho_1 \cdots \rho_p$, $p \geq 1$, donde los ρ_i son ciclos disyuntos no triviales. Demuestre que $o(\rho_i) = n/m = l(\rho_i)$, y concluya que $p = m$. Es decir, σ^k es el producto de m -ciclos de longitud n/m (cada uno).

8.14 Sea σ una permutación de S_n . Demuestre que

$$C(\sigma) := \{\rho : \rho^{-1}\sigma\rho = \sigma\}$$

es un subgrupo de S_n y que la aplicación

$$\psi_\sigma : S_n / C(\sigma) \longrightarrow CL(\sigma) := \{\tau^{-1}\sigma\tau : \tau \in S_n\}$$

dada por $\psi_\sigma(\tau C(\sigma)) = \tau^{-1}\sigma\tau$ es biyectiva. Concluya que $o(C(\sigma)) \cdot \#(CL(\sigma)) = n!$. Se dice que $C(\sigma)$ es el centralizador de σ y que $CL(\sigma)$ es la clase de los conjugados de σ .

- 8.15 Sea σ un n -ciclo de S_n . Demuestre que $C(\sigma)$ (ejercicio 8.14) es el subgrupo generado por σ y que $\#(CL(\sigma)) = (n-1)!$. (Indicación. Verifique primero las afirmaciones para $n=3$, por cálculo directo.)
- 8.16 Sea σ un ciclo de longitud m de S_n , donde $m \leq n$. Demuestre que (ejercicio 8.14) o $C(\sigma) = m(n-m)!$ y que $\#(CL(\sigma)) = (m-1)!\binom{n}{m}$.
- 8.17 Sea $\sigma \in S_n$ cuya estructura cíclica es $(l_1, \dots, l_m)$ con $l_1 < l_2 < \dots < l_m$ y $l_1 + l_2 + \dots + l_m = n$. Demuestre que si $\rho \in S_n$ tiene la misma estructura cíclica de σ , existen $l = l_1 l_2 \dots l_m$ permutaciones τ en S_n tales que $\tau^{-1} \sigma \tau = \rho$. Concluya que $o(C(\sigma)) = l$. ¿Qué se puede decir si $l < n$?
- 8.18 Considere el grupo cuatro de Klein V y sean $H_1 = \{(1), (1, 2)(3, 4)\}$, $H_2 = \{(1), (1, 3)(2, 4)\}$, $H_3 = \{(1), (1, 4)(2, 3)\}$. Verifique que H_1, H_2 y H_3 son subgrupos normales de V , el cual es a su vez normal en A_4 , pero que ninguno de H_1, H_2 o H_3 es normal en A_4 .
- 8.19 Sean V y H_1, H_2 y H_3 como en el ejercicio 8.18. Verifique que $H_i \cap H_j = \{(1)\}$ si $i \neq j$ y que $V = H_1 \cdot H_2 \cdot H_3$, pero que V no es el producto directo de H_1, H_2 y H_3 . Compruebe, en particular, que $H_1 \cap (H_2 H_3) \neq \{(1)\}$.
- *8.20 Supóngase que $\sigma \in S_n$ tiene la estructura cíclica $(l_1, \dots, l_m)$ donde $l_1 = l_2 = \dots = l_m = l$ y $ml = n$. Demuestre que $o(C(\sigma)) = l^m m!$.

Parte III

Grupos y resultados especiales

Capítulo 9

Grupos de operadores

Como lo mencionamos en el capítulo 5, nota 5.4 (teorema de Cayley), todo grupo es en esencia un grupo $\mathcal{G}$ de transformaciones (permutaciones) de un conjunto X , es decir, de funciones biyectivas de X en sí mismo, las cuales se pueden interpretar como “operadores” sobre X : se puede considerar en efecto que tales aplicaciones “actúan naturalmente” sobre los elementos de X mediante la “operación” $\mathcal{G} \times X \longrightarrow X$ dada por $(f, x) \longmapsto f(x)$, para producir nuevos elementos de X . Esta noción de “operatividad” se puede generalizar a cualquier grupo G , lo cual tiene, como veremos, ciertas ventajas e importantes consecuencias. La presentación que sigue está inspirada en [8].

Definición 9.1. Se dice que un grupo $(G, \cdot)$ *opera o actúa sobre un conjunto* X , si existe una aplicación $(*)$,

$$\begin{aligned} (*) : G \times X &\longrightarrow X \\ (a, x) &\longmapsto a * x, \end{aligned}$$

tal que:

- (i) Si e es el elemento neutro de G , $e * x = x$ para todo $x \in X$.
- (ii) Cualesquiera que sean $a, b \in G$ y $x \in X$, $a * (b * x) = (ab) * x$.

Se dice entonces que $(*)$ es la *operación* o la *acción de G sobre X* y que G y sus elementos *operan o actúan sobre X mediante $(*)$* . Se dice también que G es un *grupo de operadores sobre X* y que $(*)$ es una *ley de composición externa sobre X con operadores en G* .

Nota 9.1. La acción sobre X de un grupo G de transformaciones de X mediante $(f, x) \mapsto f(x)$ es una acción en el sentido de la Definición 9.1. De hecho, toda acción es en cierta forma de este tipo, pues si G opera sobre X y para cada $a \in G$, $\Psi_a : X \rightarrow X$ es la aplicación $\Psi_a(x) = a * x$, entonces Ψ_a es biyectiva con $\Psi_a^{-1} = \Psi_{a^{-1}}$ y $\Psi_a \circ \Psi_b = \Psi_{ab}$, así que $\mathcal{G} = \{\Psi_a : a \in G\}$ es un grupo de transformaciones de X cuyo elemento neutro, la aplicación idéntica de X , es Ψ_e , y el cual replica, mediante su "acción natural" sobre X , la acción de G sobre este conjunto. Sin embargo, puede suceder que la aplicación $\Psi : G \rightarrow \mathcal{G}$ dada por $\Psi(a) = \Psi_a$, la cual es un epimorfismo de G sobre $\mathcal{G}$, no sea un isomorfismo (ejemplo 9.4 con G abeliano o con $Z(G) \neq \{e\}$), de tal manera que no se puede considerar que G y $\mathcal{G}$ sean grupos idénticos. Esta es una de las razones para definir directamente la acción de G sobre X .

Definición 9.2. Si G opera sobre X mediante $(*)$, el conjunto

$$\mathcal{O}(x) = \{a * x : a \in G\}, \quad x \in X, \quad (9.1)$$

se denomina la *órbita de x* . A su vez, el conjunto

$$E(x) = \{a \in G : a * x = x\}, \quad x \in X, \quad (9.2)$$

se conoce como el *estabilizador de x* . Cuando $\mathcal{O}(x) = X$ para todo $x \in X$, se dice que G opera transitivamente sobre X . (Si $X \neq \emptyset$, esto es equivalente a decir que $\mathcal{O}(x) = X$ para algún $x \in X$.)

Nota 9.2. Como es claro $\mathcal{O}(x) \subseteq X$, y es el recorrido que efectúa x en X cuando los diferentes elementos de G operan o actúan sobre él. A su vez, $E(x)$ es el subconjunto de G de los elementos que al actuar sobre x lo dejan invariante. Como es claro,

$$\mathcal{O}(x) = \{\Psi_a(x) : a \in G\}, \quad (9.3)$$

donde $\Psi_a(x) = a * x$ (nota 9.1), mientras que

$$E(x) = \{a \in G : \Psi_a(x) = x\}, \quad (9.4)$$

así que $E(x)$ es el conjunto de los $a \in G$ para los cuales x es "punto fijo" de Ψ_a . Es evidente que G opera transitivamente sobre cada órbita $\mathcal{O}(x)$, por esta razón es frecuente referirse a las órbitas como las *clases de transitividad* (o aún como las *clases de intransitividad*).

Teorema 9.1. Si G actúa sobre X , $E(x)$ es, para todo $x \in X$, un subgrupo de G . Además, la aplicación

$$\Psi_x : G/E(x) \rightarrow \mathcal{O}(x)$$

dada por

$$\Psi_x(aE(x)) = a * x$$

está bien definida y es biyectiva.

Demostración. Como $e * x = x$, es claro que $e \in E(x)$ para todo $x \in X$. Por otra parte, si $a, b \in E(x)$ entonces $(ab) * x = a * (b * x) = a * x = x$, y también $ab \in E(x)$. Finalmente, si $a \in E(x)$ entonces $x = e * x = a^{-1} * (a * x) = a^{-1} * x$, así que $a^{-1} \in E(x)$. Para establecer la última afirmación hay que demostrar que si $a, b \in G$ entonces $aE(x) = bE(x)$ si y sólo si $a * x = b * x$, pero esto es obvio, pues ambas afirmaciones son equivalentes a $b^{-1}a \in E(x)$. $\square$

Ahora, como $e * x = x$ para todo $x \in X$, se tiene que $x \in \mathcal{O}(x)$, así que $\mathcal{O}(x) \neq \emptyset$ y

$$X = \bigcup_{x \in X} \mathcal{O}(x). \quad (9.5)$$

Demostraremos que $\{\mathcal{O}(x) : x \in X\}$ es una *partición de X* , o sea, que $\mathcal{O}(x) \cap \mathcal{O}(y) = \emptyset$ si $\mathcal{O}(x) \neq \mathcal{O}(y)$. Esto es parte del siguiente teorema.

Teorema 9.2. Si G opera sobre X , las afirmaciones siguientes son equivalentes para $x, y \in X$:

1. $x \in \mathcal{O}(y)$.
2. $y \in \mathcal{O}(x)$.
3. $\mathcal{O}(x) = \mathcal{O}(y)$.
4. $\mathcal{O}(x) \cap \mathcal{O}(y) \neq \emptyset$.

Demostración. Decir que $x \in \mathcal{O}(y)$ es equivalente a decir que $x = a * y$ para algún $a \in G$, lo cual equivale a que $y = a^{-1} * x$, o sea, a que $y \in \mathcal{O}(x)$. Esto demuestra que (1) y (2) son equivalentes. Demostremos que (2) implica (3). En primer lugar $\mathcal{O}(x) \subseteq \mathcal{O}(y)$, pues si $z \in \mathcal{O}(x)$ entonces $z = b * x$, $b \in G$, y, como $x = a * y$, para algún $a \in G$, entonces $z = (ba) * y$, así que $z \in \mathcal{O}(y)$.

Teniendo ahora en cuenta que $y = a^{-1} * x$, se demuestra, de la misma manera, que $\mathcal{O}(y) \subseteq \mathcal{O}(x)$. Para ver que (3) implica (4), obsérvese simplemente que si $\mathcal{O}(x) = \mathcal{O}(y)$ entonces $x \in \mathcal{O}(y)$, así que $x \in \mathcal{O}(x) \cap \mathcal{O}(y)$. Veamos finalmente que (4) implica (1). Pero esto es obvio, pues si $z \in \mathcal{O}(x) \cap \mathcal{O}(y)$ entonces $z = a * x = b * y$, $a, b \in G$, de lo cual $x = (a^{-1}b) * y \in \mathcal{O}(y)$. $\square$

Se deduce que $\mathcal{O}(x) = \mathcal{O}(y)$ si y sólo si $\mathcal{O}(x) \subseteq \mathcal{O}(y)$. Además:

Corolario 9.1. Si X es finito y $C \subseteq X$ tiene con cada órbita un único elemento en común, entonces C es finito, $[G : E(x)]$ es finito para todo $x \in X$, y

$$\#(X) = \sum_{x \in C} \#(\mathcal{O}(x)) = \sum_{x \in C} [G : E(x)], \quad (9.6)$$

donde $\#(A)$ denota el número de elementos del conjunto A .

Demostración. Que $[G : E(x)]$ es finito resulta del teorema 9.1, del cual resulta además que $\#(\mathcal{O}(x)) = [G : E(x)]$. $\square$

Definición 9.3. La relación (9.6) se conoce como la *ecuación orbital* o la *ecuación de clases de la acción de G sobre X* .

Definición 9.4. Si G opera sobre X , el conjunto de los elementos de G que dejan estable a todo elemento de X se denomina el *estabilizador de X* y se denota con $E(X)$. Así,

$$E(X) = \bigcap_{x \in X} E(x). \quad (9.7)$$

A su vez,

$$Z(X) = \{x \in X : a * x = x \text{ para todo } a \in G\} \quad (9.8)$$

se denomina el *subconjunto estable de X* y, a veces, el *centro de X* .

Nota 9.3. Evidentemente $E(X)$ es un subgrupo normal de G , núcleo del epimorfismo $\Psi : G \rightarrow \mathcal{G}$ descrito en la nota 9.1. Entonces $G/E(X) \approx \mathcal{G}$, y Ψ es un isomorfismo si y sólo si $E(X) = \{e\}$, en cuyo caso la acción de G puede reemplazarse por la de $\mathcal{G}$.

Definición 9.5. Si G opera sobre X de tal manera que $E(X) = \{e\}$, se dice que G opera *fielmente* sobre X .

Teorema 9.3. Si G actúa sobre X , las afirmaciones siguientes para $x \in X$ son equivalentes:

1. $x \in Z(X)$.
2. $\mathcal{O}(x) = \{x\}$.
3. $E(x) = G$.

Si además C es un subconjunto de X que tiene en común con cada órbita de X un único elemento, entonces $Z(X) \subseteq C$.

Demostración. Resulta inmediatamente de (9.8). $\square$

Corolario 9.2. Si G opera sobre X y X es finito, la ecuación (9.6) puede escribirse en la forma

$$\#(X) = \#(Z(X)) + \sum_{x \in C'} [G : E(x)], \quad (9.9)$$

donde $C' = C \setminus Z(X)$ y C tiene con cada órbita un único elemento en común.

Nota 9.4. Si G opera sobre X por $(a, x) \rightarrow a * x$, $a \in G$, $x \in X$, y H es un subgrupo de G , también H opera de manera natural sobre X por $(a, x) \rightarrow a * x$, $a \in H$, $x \in X$, acción que se conoce como la *acción de H sobre X inducida por la acción de G* . Si $\mathcal{O}_H(x)$ y $E_H(x)$ denotan respectivamente la órbita y el estabilizador de $x \in X$ bajo la acción de H inducida por la acción de G , es claro que $\mathcal{O}_H(x) \subseteq \mathcal{O}(x)$ y que $E_H(x) = E(x) \cap H$. Por otra parte, $H/E_H(x) = H/E(x) \cap H$ se corresponde biyectivamente con $\mathcal{O}_H(x)$ mediante la aplicación $\Psi_x : H/E_H(x) \rightarrow \mathcal{O}_H(x)$ dada por $\Psi_x(aE_H(x)) = a * x$, $a \in H$. Nótese también que $Z_H(X)$, el centro de X para la acción inducida de H sobre X , contiene a $Z(X)$: $Z(X) \subseteq Z_H(X)$. Sin embargo, en general, $Z_H(X) \neq Z(X)$. Así, si $H = \{e\}$, $Z_H(X) = X$, pero sólo raramente $Z(X) = X$ cuando $G \neq \{e\}$ (véase, al respecto, el ejemplo 9.1, más adelante). Para la acción de H sobre X , la ecuación de clases toma, cuando X es finito, la forma

$$\#(X) = \sum_{x \in C_H} [H : E(x) \cap H] = \#(Z_H(X)) + \sum_{x \in C'_H} [H : E(x) \cap H], \quad (9.10)$$

donde $C_H \subseteq X$ tiene con cada órbita $\mathcal{O}_H(x)$ un único elemento en común y donde $C'_H = C_H \setminus Z_H(X)$.

Examinaremos ahora varios ejemplos notables de grupos de operadores.

Ejemplo 9.1. Si $(G, \cdot)$ es un grupo y H es un subgrupo de G , H opera sobre $X = G$ mediante la ley

$$(*) : H \times G \longrightarrow G \\ (a, x) \longmapsto a * x = ax$$

En este caso $\mathcal{O}(x) = Hx = \{ax : a \in H\}$, es la clase lateral derecha de H en x , y $E(x) = \{e\}$, pues si $ax = x$ para algún $x \in G$, necesariamente $a = e$. La ecuación de clases toma, cuando G es finito, la forma obvia

$$\#(G) = [G : H] \cdot o(H), \quad (9.11)$$

pues si C tiene con cada órbita un único elemento en común entonces $\#(C) = [G : H]$, y $\#(\mathcal{O}(x)) = \#(Hx) = o(H)$ para todo $x \in G$. Para esta acción $Z(X) = G$ si $H = \{e\}$ y $Z(X) = \emptyset$ si $H \neq \{e\}$, mientras que $E(X) = \{e\}$, así que H opera fielmente sobre G (Definición 9.5)

Ejemplo 9.2. Sean G un grupo y S el conjunto de los subgrupos de G . Entonces G opera sobre S por conjugación, es decir, mediante la acción

$$(*) : G \times S \longrightarrow S \\ (a, H) \longmapsto a * H = aHa^{-1}.$$

En este caso $E(H)$ se denota con $N(H)$ y se denomina el *normalizador* de H en G . Nótese que $N(H) = \{a \in G : aHa^{-1} = H\}$ es un subgrupo de G , y es claro que H es un subgrupo normal de $N(H)$ (pues $aHa^{-1} = H$ para todo $a \in N(H)$). Evidentemente H es normal en G si y sólo si $N(H) = G$. Si H es un subgrupo de G y $a \in G$, se dice que aHa^{-1} es un *conjugado* de H , y entonces $\mathcal{O}(H)$ es la *clase de conjugación* de H en G y se denota con $CL(H)$. Como es claro $CL(H) = \{H\}$ si y sólo si H es normal en G , así que $Z(S)$ es la clase de los subgrupos normales de G . Si G es finito entonces

$$\#(S) = \sum_{H \in C} \#(CL(H)) \quad (9.12)$$

donde C tiene con cada clase $CL(H)$ un único elemento en común, y, como $\#(CL(H)) = [G : N(H)]$, entonces

$$\#(S) = \sum_{H \in C} [G : N(H)] = \#(Z(S)) + \sum_{H \in C'} [G : N(H)] \quad (9.13)$$

donde $C' = C \setminus Z(S)$.

Ejemplo 9.3. Más frecuentemente que sobre la clase S de todos los subgrupos de G , se considera la acción de G sobre subclases propias S_0 de S . Las clases deben ser tales que $aHa^{-1} \in S_0$ si $H \in S_0$ y $a \in G$ (por ejemplo, subgrupos de un orden dado). En este caso $Z(S_0) = Z(S) \cap S_0$ es la clase de los subgrupos normales de G en S_0 , y si G es finito, C es como en el ejemplo 9.2, y $C_0 = C \cap S_0$, entonces

$$\#(S_0) = \sum_{H \in C_0} [G : N(H)] = \#(Z(S_0)) + \sum_{H \in C'_0} [G : N(H)] \quad (9.14)$$

donde $C'_0 = C_0 \setminus Z(S_0)$. Si K es un subgrupo de G , también K opera sobre S_0 mediante la acción inducida por la acción de G , y es evidente que $E_K(H) = N_K(H) = K \cap N(H)$ para todo $H \in S_0$. La ecuación (9.14) es aún válida sustituyendo en todas partes a G por K , a $N(H)$ por $N(H) \cap K$, a C_0 por una clase que tenga con cada órbita $CL_K(H) = \{aHa^{-1} : a \in K\}$ un único elemento en común, y a $Z(S_0)$ por $Z_K(S_0) = \{H \in S_0 : aHa^{-1} = H \text{ para todo } a \in K\}$. Como es claro $Z(S_0) \subseteq Z_K(S_0)$, pero en general, son diferentes.

Ejemplo 9.4. Si $(G, \cdot)$ es un grupo, G opera sobre sí mismo por conjugación, es decir, por medio de la acción

$$(*) : G \times G \longrightarrow G \\ (a, x) \longmapsto a * x = axa^{-1}.$$

En este caso $E(x)$ se denota con $C(x)$ y se denomina el *centralizador* de x en G . Como es claro, $C(x)$ es un subgrupo de G . A su vez, $\mathcal{O}(x)$ se denota con $CL(x)$ y se denomina la *clase de conjugación* de x o la *clase de los conjugados* de x en G (si $a, x \in G$, se dice que axa^{-1} es un *conjugado* de x en G): $CL(x) = \{axa^{-1} : a \in G\}$. Como es claro, $\#(CL(x)) = [G : C(x)]$. Además, en este caso

$$E(G) = Z(G) = \bigcap_{x \in G} C(x), \quad (9.15)$$

y el centro $Z(G)$ de G es así un subgrupo normal de G . Además, $(Z(G), \cdot)$ es obviamente un grupo abeliano y G es abeliano si y sólo si $G = Z(G)$. Si C tiene un único elemento en común con cada clase de conjugación $CL(x)$, $x \in G$, y G es finito, entonces

$$o(G) = \sum_{x \in C} [G : C(x)] = o(Z(G)) + \sum_{x \in C'} [G : C(x)] \quad (9.16)$$

donde $C' = C \setminus Z(G)$. Nótese que, dado que $CL(x) = \{x\}$ para todo $x \in Z(G)$, se tiene que $Z(G) \subseteq C$. Por otra parte, si H es un subgrupo de G y H opera sobre G por conjugación, es decir, por medio de la acción inducida por la anterior acción de G , entonces $E_H(x)$ se denota con $C_H(x)$, y es claro que $C_H(x) = C(x) \cap H$. Si G es finito se tiene entonces que

$$o(G) = \sum_{x \in C_H} [H : H \cap C(x)] = o(Z_H(G)) + \sum_{x \in C'_H} [H : H \cap C(x)] \quad (9.17)$$

donde $Z_H(G) = \{x \in G : axa^{-1} = x \text{ para todo } a \in H\}$ es el centro de G para tal acción, C_H tiene con cada clase de conjugación

$$O_H(x) = CL_H(x) = \{axa^{-1} : a \in H\}, \quad x \in G,$$

un único elemento en común, y $C'_H = C_H \setminus Z_H(G)$. Obsérvese además que $O_H(x) \subseteq O(x)$ para todo $x \in G$ y que $Z(G) \subseteq Z_H(G)$, pero, en general, $Z_H(G) \neq H \cap Z(G)$.

Ejemplo 9.5. Si $(G, \cdot)$ es un grupo y H es un subgrupo de G , G opera sobre el conjunto G/H de las clases laterales izquierdas de H mediante

$$(*) : G \times G/H \longrightarrow G/H \\ (a, bH) \longmapsto a * (bH) = (ab)H.$$

En este caso

$$E(bH) = bHb^{-1} \quad (9.18)$$

y

$$O(bH) = G/H, \quad (9.19)$$

para todo $b \in G$, pues dado $c \in G$ siempre existe $a \in G$ tal que $ab = c$, así que G opera transitivamente sobre G/H (definición 9.2). Como es claro, G/bHb^{-1} está en correspondencia biyectiva con G/H mediante la aplicación $\varphi(a(bHb^{-1})) = (ab)H$. Además

$$E(G/H) = \bigcap_{b \in G} bHb^{-1} \quad (9.20)$$

es un subgrupo normal de G contenido en H , $Z(G/H) = \{G\}$ si $H = G$, y

$$Z(G/H) = \emptyset \quad (9.21)$$

si $H \neq G$. La correspondiente ecuación orbital se reduce a

$$\#(G/H) = [G : H]. \quad (9.22)$$

La teoría de los grupos de operadores es útil en diversos campos, incluyendo temas tan diversos como las *ecuaciones diferenciales no lineales* y los *sistemas dinámicos*. Los *espacios homogéneos de un grupo*, conjuntos sobre los que éste actúa fiel y transitivamente, son importantes en la teoría de los *grupos topológicos* y, en especial, en la de los *grupos de Lie*; y los *espacios afines*, espacios homogéneos del grupo aditivo de un espacio vectorial, constituyen el marco natural de muchas ideas geométricas. En el próximo capítulo examinaremos algunas aplicaciones de los grupos de operadores a la teoría misma de los grupos.

EJERCICIOS

- 9.1 Con respecto al ejemplo 9.1, verifique en detalle que $a * x = ax$ define bien una acción de H sobre G , que $O(x) = Hx$ y que $E(x) = \{e\}$.
- 9.2 Con respecto a la nota 9.4, demuestre que en efecto $E_H(x) = E(x) \cap H$ y que φ_x es biyectiva para todo $x \in X$. Dé ejemplos en los cuales $O_H(x) \neq O(x)$ para algún $x \in X$ y $Z_H(X) \neq Z(X) \cap H$.
- 9.3 Verifique, en el ejemplo 9.2, que $a * H = aHa^{-1}$ es en efecto una acción de G sobre S , que H es un subgrupo normal de $N(H)$ y que $N(H) = G$ si y sólo si H es normal en G . Demuestre también que $O(H) = \{H\}$ es equivalente a afirmar que H es normal en G . Verifique finalmente que si S_n es la clase de los subgrupos de G de orden n , G actúa sobre S_n por conjugación (ejemplo 9.3) y que $E(H)$ para esta acción es aún $N(H)$ para todo $H \in S_n$.
- 9.4 Sean $(G, \cdot)$ un grupo que opera sobre un conjunto X mediante $(*)$ y $\psi : G \longrightarrow \mathcal{F}_0(X)$ definida por $\psi(a) = \psi_a$, donde $\psi_a(x) = a * x$ para todo $x \in X$. Demuestre que ψ está bien definida (o sea que $\psi_a \in \mathcal{F}_0(X)$), es un homomorfismo (es decir, $\psi_a \circ \psi_b = \psi_{ab}$, $a, b \in G$) y $\ker \psi = E(X)$. Concluya que si X es finito con n elementos, $o(G/E(X))$ divide a $n!$. Dé un ejemplo en el cual $E(X) \neq \{e\}$, así que ψ no es un monomorfismo y G no es isomorfo a $\psi(G) = \{\psi_a : a \in G\} = \mathcal{G}$ (nota 9.1).
- 9.5 Demuestre que si H es un subgrupo de G y G opera sobre G/H como en el ejemplo 9.5, las afirmaciones siguientes son equivalentes:

- a) H es un subgrupo normal de G .
- b) $E(bH) = H$ para todo $b \in G$.

$$c) \quad E(G/H) = H.$$

9.6 Supóngase que $(G, \cdot)$ es un grupo, que H es un subgrupo de G con $n = [G : H] < \infty$, y que G es infinito o que G es finito pero $o(G) \nmid n!$. Demuestre que existe un subgrupo normal N de G tal que $N \subseteq H$, que $N \neq \{e\}$ y que $[G : N] < \infty$. Demuestre además que $[G : H]$ divide a $[G : N]$, y concluya que si $n = 2$ entonces H es normal en G . (Indicación. Considere la acción de G sobre G/H del ejemplo 9.5 y use el ejercicio 9.4).

9.7 Demuestre que si $(G, \cdot)$ opera sobre un conjunto X de tal manera que dados $x, y \in X$ siempre existe $a \in G$ tal que $a * x = y$, entonces G opera transitivamente sobre X (definición 9.2).

- Demuestre que si $X \neq \emptyset$, G opera transitivamente sobre X si y sólo si $O(x) = X$ para algún $x \in X$, en cuyo caso $O(x) = X$ para todo $x \in X$.
- Demuestre que si H es un subgrupo de G y G opera sobre $X = G/H$ como en el ejemplo 9.5, entonces G opera transitivamente sobre X .
- Demuestre que si G opera transitivamente sobre $X \neq \emptyset$, existen $x_0 \in X$ y un subgrupo H de G tales que la aplicación $\varphi(aH) = a * x_0$ está bien definida y aplica biyectivamente G/H sobre X . ¿Qué es H ?
- Si G, X, H son como en (c) y $x \in X$, demuestre que $E(x) = bHb^{-1}$ para algún $b \in G$.
- Supóngase que G, X, H y φ son como en (c) y que G opera sobre G/H como en el ejemplo 9.5. Demuestre que si $\psi : G \times G/H \rightarrow G \times X$ es la aplicación $\psi(a, bH) = (a, \varphi(bH))$, entonces ψ es biyectiva y el diagrama

$$\begin{array}{ccc} (*) : G \times G/H & \longrightarrow & G/H \\ \downarrow \psi & & \downarrow \varphi \\ (*) : G \times X & \longrightarrow & X \end{array}$$

es conmutativo, así que $\varphi(a * (bH)) = a * \varphi(bH)$. Concluya que toda acción transitiva sobre un conjunto no vacío X es, en esencia, la acción de G sobre G/H descrita en el ejemplo 9.5. Es decir, X puede identificarse con G/H para un subgrupo apropiado H de G , de tal manera que la acción sobre X se identifique con la acción sobre G/H dada en el ejemplo 9.5.

9.8 Sean M y N subgrupos de G . Demuestre que aún si ninguno de M ó N es un subgrupo normal de G , la aplicación $\psi : M/M \cap N \rightarrow MN/N$ dada por $\psi(x(M \cap N)) = xN, x \in M$, está bien definida y es biyectiva.

9.9 Se dice que un grupo G opera fielmente sobre un conjunto X (Definición 9.5) si G opera sobre X y $E(X) = \{e\}$. Demuestre que si G opera sobre X y ψ es como en el ejercicio 9.4, G opera fielmente sobre X si y sólo si ψ es un monomorfismo, es decir, un isomorfismo de G sobre $\psi(G)$. Concluya que si G opera fielmente sobre X y X es finito con n elementos, también G es finito y $o(G)$ divide a $n!$. Dé un ejemplo en el cual X tenga n elementos, $o(G) = n!$ y G opere fielmente sobre X .

9.10 Demuestre que todo subgrupo G del grupo $\mathcal{F}_0(X)$ de las aplicaciones biyectivas de X en sí mismo, opera fielmente sobre X mediante la operación $(f, x) \rightarrow f(x), f \in G, x \in X$, y que $\mathcal{F}_0(X)$ opera fiel y transitivamente sobre X , así que X es un espacio homogéneo de $(\mathcal{F}_0(X), \circ)$.

9.11 Demuestre que si G opera sobre G/H como en el ejemplo 9.5 y H no contiene ningún subgrupo normal N de $G, N \neq \{e\}$, entonces G opera fiel y transitivamente sobre G/H .

9.12 Demuestre que si $(G, \cdot)$ es un grupo y H es un subgrupo de G , H opera fielmente sobre G mediante $(a, x) \rightarrow ax, a \in H, x \in G$. Concluya que H es isomorfo a un subgrupo del grupo $(\mathcal{F}_0(G), \circ)$, y que esto es cierto, en particular, si $H = G$ (teorema de Cayley). Demuestre además que H opera transitivamente sobre G si y sólo si $H = G$. Suponga ahora que G es finito y que $p = [G : H]$ es el primo más pequeño que divide a $o(G)$. Demuestre que H es normal en G . (Indicación. Considere la acción de G sobre G/H del ejemplo 9.5.)

9.13 Sea $\mathcal{G} = GL_n(K)$ el grupo multiplicativo de las matrices no singulares de orden $n \times n$ sobre $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$; $E = K_n$, el conjunto de matrices $n \times 1$ sobre K (vectores columna de orden n). Demuestre que $\mathcal{G}$ opera fiel y transitivamente sobre E mediante la ley $M * x = Mx, M \in \mathcal{G}, x \in E$. Para $x \in E$, describa $E(x)$ para esta acción.

*9.14 Sean $(E, +)$ el grupo aditivo de un espacio vectorial sobre $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, X un conjunto. Si $(E, +)$ opera sobre X de tal manera que dados $x, y \in X$ siempre existe un único $a \in E$ tal que $a * x = y$, se dice que X es un espacio afín sobre E . Demuestre que si X es un espacio afín

sobre $(E, +)$ entonces X es un espacio homogéneo del grupo $(E, +)$. (nota. Si $x, y \in X$, es usual denotar con $\overrightarrow{xy}$ al único $a \in E$ tal que $a * x = y$. Se dice que $\overrightarrow{xy}$ es el *vector libre de origen x y extremo y* .)

- *9.15 Sea $X = K^n = \{(x_1, \dots, x_n) : x_i \in K, i = 1, 2, \dots, n\}$, donde $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, y sea K_n como en el ejercicio 9.13. Defina $K_n \times X \rightarrow X$, $(a, x) \rightarrow a * x$, por

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} * (x_1, \dots, x_n) = (a_1 + x_1, \dots, a_n + x_n).$$

Demuestre que X es un espacio afín (ejercicio 9.14) del grupo aditivo $(K_n, +)$, y que si $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ entonces

$$\overrightarrow{xy} = \begin{bmatrix} y_1 - x_1 \\ \vdots \\ y_n - x_n \end{bmatrix}.$$

- 9.16 Sea $(E, +)$ el grupo aditivo de un espacio vectorial sobre $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Demuestre que $(E, +)$ opera sobre $X = E$ mediante la acción $a * x = a + x$, y que para esta acción, X es un espacio afín (ejercicio 9.14) de $(E, +)$. Verifique que para esta acción, $\overrightarrow{xy} = y - x$.

Capítulo 10

La teoría de Sylow

Consideraremos en este capítulo algunas aplicaciones de los resultados del capítulo 9. Estas aplicaciones, que conforman la llamada *teoría de Sylow*, se resumen en cuatro teoremas, los célebres *teoremas de Sylow*, que representan esfuerzos por encontrar recíprocos parciales del teorema de Lagrange en el caso no conmutativo y están en los orígenes del gran caudal de investigaciones que, como lo mencionamos en el capítulo 8, condujeron, en la década de los años setenta del pasado siglo, a la clasificación completa de los denominados grupos finitos simples, los pilares sobre los que se construyen todos los grupos. La exposición que sigue, basada en la teoría de los grupos de operadores, toma ideas de [8], [10], [15], [16], [17] y [22].

Definición 10.1. Si $(P, \cdot)$ es un grupo, p es un primo y $o(P) = p^n$, $n \geq 0$ un entero, se dice que P es un p -grupo.

Definición 10.2. Sean $(G, \cdot)$ un grupo finito y p un número primo. Si H es un subgrupo de G de orden p^n , $n \geq 0$ un entero, se dice que H es un p -subgrupo de G . Si p^n es la máxima potencia de p que divide a $o(G)$, se dice que H es un p -subgrupo de Sylow de G .

Si $p \nmid o(G)$, el único p -subgrupo de G es $\{e\}$, su orden es $1 = p^0$, y es el único p -subgrupo de Sylow de G . Si $p \mid o(G)$ y $o(G) = mp^n$, donde $n \geq 1$ y $p \nmid m$, los subgrupos de Sylow de G , si los hay, tendrán orden p^n , y cualquier otro p -subgrupo de G tendrá orden p^k , $0 \leq k < n$. Como es evidente, si H es un p -grupo y N es un subgrupo de H , también N es un p -grupo.

Nota 10.1 Obsérvese que si p es un primo y P es un p -subgrupo de Sylow de G , entonces $p \nmid [G : P]$. Si $a \in G$ y $o(a) = p^k$, $k \geq 1$, se dice que a es un

p -elemento de G . Si G es un p -grupo, todo elemento $a \in G$, $a \neq e$, es un p -elemento. Lo recíproco es también cierto y será consecuencia del teorema siguiente.

Teorema 10.1 (Primer teorema de Sylow). Sean $(G, \cdot)$ un grupo finito, p un primo, p^n , $n \geq 0$, la máxima potencia de p que divide a $o(G)$. Entonces G tiene, para todo $0 \leq k \leq n$, un subgrupo H de orden p^k .

Demostración. Haremos inducción sobre $o(G)$. La afirmación es clara si $o(G) = p^m$, $m = 0, 1$, los mínimos valores posibles de $o(G)$. Supongamos entonces que la afirmación es válida para todo grupo G' con $o(G') < o(G)$, y demostrémosla para G . Escribamos la ecuación (9.16) en la forma

$$o(G) = o(Z(G)) + \sum_{a \in C'} [G : C(a)] \quad (10.1)$$

donde $C' = C \setminus Z(G)$ y C tiene con cada clase de conjugación $CL(x)$, $x \in G$, un único elemento en común. Como es claro, $o(C(a)) < o(G)$ para todo $a \in C'$, así que si $p \nmid [G : C(a)]$, en cuyo caso $p^n \mid o(C(a))$, $C(a)$ tendrá, para cada $0 \leq k \leq n$, un subgrupo H de orden p^k . Como H es un subgrupo de G , el teorema quedará demostrado en este caso. Supongamos entonces que $p \mid [G : C(a)]$ para todo $a \in C'$. Como entonces $p \mid o(G)$, se tendrá que $p \mid o(Z(G))$, y como $Z(G)$ es abeliano, el teorema de Cauchy (teorema 4.3) garantiza la existencia de $a \in Z(G)$ con $o(a) = p$. Sea $N = \langle a \rangle$. Como $N \subseteq Z(G)$, N es un subgrupo normal de G , y si $G' = G/N$ entonces $o(G') < o(G)$, y la máxima potencia de p que divide a G' será p^{n-1} . Por la hipótesis de inducción, G' tendrá, para todo $0 \leq k \leq n-1$, un subgrupo H' de orden p^k . Pero, por lo dicho en la nota 6.1, existe un subgrupo H de G tal que $N \subseteq H$ y que $H/N \approx H'$, así que $o(H) = p^{k+1}$. Entonces, G tendrá subgrupos de orden p^k para todo $1 \leq k \leq n$. Esto demuestra el teorema. $\square$

Nota 10.2. Si $o(G) = mp^n$ donde $p \nmid m$, puede ser que no existan subgrupos H de G con $o(H) = m$.

De la demostración del teorema 10.1 se deduce el siguiente corolario.

Corolario 10.1. Si p es un primo, $(G, \cdot)$ es un p -grupo y $o(G) > 1$, entonces $Z(G) \neq \{e\}$.

Demostración. Considérese para G la ecuación (10.1). Como $o(C(a)) < o(G)$ para todo $a \in C'$, entonces $p \mid \sum_{a \in C'} [G : C(a)]$. Como $p \mid o(G)$, entonces $p \mid o(Z(G))$. $\square$

El corolario siguiente es el segundo teorema de Sylow.

Corolario 10.2. (Segundo teorema de Sylow) Si p es un primo y $o(G) = p^n$, $n \geq 0$, entonces G tiene, para todo $0 \leq k \leq n$, un subgrupo normal de orden p^k .

Demostración. Que G tiene subgrupos de orden p^k , para todo $0 \leq k \leq n$, es consecuencia del teorema 10.1. Aquí demostraremos que tales subgrupos pueden tomarse normales (cuando G es un p -grupo). Procederemos por inducción sobre n . La afirmación es clara si $n = 0, 1$. Supóngase entonces que $n > 1$ y que $o(Z(G)) = p^m$. Entonces, por el corolario 10.1, $m \geq 1$, y como $Z(G)$ es normal en G , $G' = G/Z(G)$ es un grupo de orden p^{n-m} . Como $n-m < n$, G' tendrá, para todo $0 \leq k \leq n-m$, un subgrupo normal H' de orden p^k . Pero por el corolario 6.1 y la nota 6.1, existe un subgrupo H de G tal que $Z(G) \subseteq H$ y que $H/Z(G) \approx H'$, y como H' es normal, también H puede tomarse normal en G . Esto demuestra que para todo $m \leq k \leq n$, existe un subgrupo normal H de G con $o(H) = p^k$. Pero, como $Z(G)$ es abeliano, $Z(G)$ tendrá, para todo $0 \leq k \leq m$, un subgrupo H de orden p^k , (corolario 6.4) y, como $H \subseteq Z(G)$, H será un subgrupo normal de G de orden p^k , $0 \leq k \leq m$. $\square$

Corolario 10.3. Si p es un primo y todo elemento $a \neq e$ de un grupo finito G es un p -elemento, entonces G es un p -grupo.

Demostración. Si existiera un primo q , $q \neq p$, tal que $q \mid o(G)$, G tendría un q -elemento. $\square$

Para establecer el siguiente teorema de Sylow, necesitaremos algunas observaciones que, por fáciles de demostrar, no dejan de ser curiosas, inteligentes e importantes.

Lema 10.1. Sean G un grupo finito, p un primo, P un p -subgrupo de Sylow de G , $N(P) = \{a \in G : aPa^{-1} = P\}$, su normalizador. Si H es un p -subgrupo de G y $H \subseteq N(P)$, entonces $H \subseteq P$.

Demostración. Como P es evidentemente un subgrupo normal de $N(P)$, HP es un subgrupo de $N(P)$ (y, de G), y $HP/P \approx H/H \cap P$, de lo cual $o(HP) = o(P) \cdot [H : H \cap P]$. Pero evidentemente $[H : H \cap P]$ es una potencia de p , así que HP es un p -grupo. Como $P \subseteq HP$, necesariamente $HP = P$, y $[H : H \cap P] = 1$. Entonces $H \cap P = H$, de lo cual $H \subseteq P$. $\square$

Corolario 10.4. Sean G un grupo finito, p un primo, H un p -subgrupo de G , P un p -subgrupo de Sylow de G . Entonces,

$$N(P) \cap H = P \cap H. \quad (10.2)$$

Demostración. Si $H' = N(P) \cap H$ entonces H' es un subgrupo de H y, por lo tanto, un p -subgrupo de G . Como $H' \subseteq N(P)$ entonces $H' \subseteq P$, de lo cual $H' = P \cap H' = P \cap N(P) \cap H = P \cap H$. $\square$

Nota 10.3. Obsérvese que si P es un p -subgrupo de Sylow de G , todo conjugado aPa^{-1} de P también lo es. Del lema 10.1 se deduce que si P es un p -subgrupo de Sylow de G , los únicos p -elementos a de G que normalizan a P , es decir, que $aPa^{-1} = P$, son los propios elementos de P .

Sea $CL(P)$ el conjunto de los conjugados de P en G , $CL(P) = \{aPa^{-1} : a \in G\}$, así que $\#CL(P) = [G : N(P)]$ (ejemplo 9.3). Sea H un subgrupo de G y considérese la acción de H sobre $CL(P)$ por medio de $H \times C(P) \rightarrow C(P)$ dada por $(a, Q) \rightarrow aQa^{-1}$, $a \in H$, $Q \in CL(P)$. Sean $E(Q) = N_H(Q)$ y $CL_H(Q) = \{aQa^{-1} : a \in H\}$ el estabilizador y la órbita de $Q \in CL(P)$ para esta acción. Sean $CL_H(Q_1), \dots, CL_H(Q_l)$, $Q_1 = P$, las diferentes órbitas posibles. Como evidentemente $N_H(Q) = N(Q) \cap H$, se tiene que

$$[G : N(P)] = \#(CL(P)) = \sum_{k=1}^l [H : H \cap N(Q_k)]. \quad (10.3)$$

Esto es consecuencia de la ecuación (9.6). El siguiente es el tercer teorema de Sylow.

Teorema 10.2 (Tercer teorema de Sylow). Sean $(G, \cdot)$ un grupo finito, p un número primo. Entonces

1. Todo p -subgrupo de G está contenido en algún p -subgrupo de Sylow de G .
2. Todos los p -subgrupos de Sylow de G son conjugados.

Demostración. 1) Supóngase que P es un p -subgrupo de Sylow de G y que H en (10.3) es un p -subgrupo de G . Claramente $p \nmid [G : N(P)]$, pues $N(P) \supseteq P$ y $p \nmid [G : P]$. Por otra parte $p \mid [H : H \cap N(Q_k)]$, donde los Q_k son como en (10.3), a no ser que $[H : H \cap N(Q_k)] = 1$. Pero, en virtud

de lo anterior, esto último debe ocurrir para algún $1 \leq k \leq l$, de lo cual $H \cap N(Q_k) = H$, o sea, $H \subseteq N(Q_k)$, así que $H \subseteq Q_k$ (lema 10.1). Como Q_k , siendo un conjugado de P , es un p -subgrupo de Sylow de G , (1) queda demostrado.

2) Sean P y Q p -subgrupos de Sylow. Como Q es un p -subgrupo de G , existe, en virtud de la demostración de (1) con $H = Q$, un conjugado P' de P tal que $Q \subseteq P'$, de lo cual $Q = P'$. Entonces, Q es un conjugado de P . $\square$

Nota 10.4. Obsérvese que el teorema 10.2 asegura que si $S(p)$ es la clase de los p -subgrupos de Sylow de G entonces

$$S(p) = CL(P) \quad (10.4)$$

cualquiera que sea $P \in S(p)$. En otras palabras, G opera transitivamente sobre $S(p)$ por conjugación (definición 9.2). Nótese de paso que el estabilizador $E(S(p))$ de la acción de G sobre $S(p)$ es

$$E(S(p)) = \bigcap_{Q \in S(p)} N(Q) = \bigcap_{x \in G} xN(P)x^{-1} \quad (10.5)$$

cualquiera que sea $P \in S(p)$, y es un subgrupo normal de G . La última igualdad en (10.5) resulta de observar que $xN(P)x^{-1} = N(xPx^{-1})$ para todo $x \in G$. Como es claro entonces, $E(S(p)) = G$ si y sólo si algún $P \in S(p)$ es normal en G , lo cual ocurre si y sólo si $CL(P) = \{P\} = S(p)$.

De la conjugación de los p -subgrupo de Sylow o de la observación anterior se deducen entonces los siguientes corolarios del teorema 10.2.

Corolario 10.5. Si $(G, \cdot)$ es un grupo finito y p es un primo, las afirmaciones siguientes son equivalentes:

1. G tiene un único p -subgrupo de Sylow.
2. G tiene un p -subgrupo de Sylow normal.

Corolario 10.6. Si $(G, \cdot)$ es un grupo abeliano finito, G tiene, para cada primo p , un único p -subgrupo de Sylow.

Corolario 10.7. Sea $(G, \cdot)$ un grupo de orden $p_1^{n_1} \cdots p_m^{n_m}$, donde los p_i son primos distintos, $i = 1, 2, \dots, m$. Supóngase además que para cada primo p ,

G tiene un único p -subgrupo de Sylow, y sean $P_1, \dots, P_m$ los p -subgrupos de Sylow de G correspondientes en su orden a los primos $p_1, \dots, p_m$. Entonces G es el producto directo de los grupos P_i , $i = 1, 2, \dots, m$.

Demostración. Los P_i son normales en G y si $\hat{P}_i$ es el producto de los P_j , $j \neq i$, es claro que $P_i \cap \hat{P}_i = \{e\}$. Como además $o(P_1) o(P_2) \cdots o(P_m) = o(G)$, la afirmación es clara. $\square$

Nota 10.5. Más aún, bajo las hipótesis del corolario 10.7, si $1 \leq i_1 \leq i_2 \leq \dots \leq i_l \leq m$, G tiene un subgrupo normal H de orden $p_{i_1}^{n_{i_1}} \cdots p_{i_l}^{n_{i_l}}$, i.e., $H = P_{i_1} P_{i_2} \cdots P_{i_l}$. Es posible demostrar, de hecho, que G tiene subgrupos normales de orden m , para todo $m \mid o(G)$ (véase el capítulo 12).

Finalmente tenemos

Corolario 10.7. Si $(G, \cdot)$ es un grupo de orden p^2 , donde p es un primo, entonces G es abeliano.

La demostración resulta inmediatamente del siguiente lema, del corolario 10.1 (o sea, de $[G : Z(G)] = 1, p$), y del hecho de que todo grupo de orden primo es cíclico.

Lema 10.2. Si $(G, \cdot)$ es un grupo y H es un subgrupo de G tal que $H \subseteq Z(G)$ y que G/H es cíclico, entonces G es abeliano.

Demostración. Como es claro, H es normal en G . Supóngase que $G/H = [\bar{a}]$, donde $\bar{a} = aH$, $a \in G$. Si $b, c \in G$ entonces $b = a^m h$, $c = a^n h'$, donde $m, n \in \mathbb{Z}$ y $h, h' \in H$. Entonces $ab = a^{m+n} h h' = ba$, pues $h, h' \in Z(G)$, así que a^m y a^n conmutan con h y h' , los cuales, a su vez, conmutan entre sí. $\square$

Consideremos ahora el cuarto y último teorema de Sylow.

Teorema 10.3 (Cuarto teorema de Sylow). Sean $(G, \cdot)$ un grupo finito, p un número primo, $n(p)$ el número de p -subgrupos de Sylow de G . Entonces $n(p)$ es un divisor de $o(G)$ y

$$n(p) \equiv 1 \pmod{p}. \quad (10.6)$$

Demostración. Sea $P \in \mathcal{S}(p)$, un p -subgrupo de Sylow de G . Como según (10.4), $\mathcal{S}(p) = CL(P)$, se tiene que $n(p) = \#\mathcal{S}(p) = [G : N(P)]$, así que

$n(p) \mid o(G)$. Por otra parte, si en (10.3) tomamos $H = P$, obtenemos

$$[G : N(P)] = \sum_{k=1}^l [P : P \cap N(Q_k)] \quad (10.7)$$

donde los Q_k , $k = 1, 2, \dots, l$, $Q_1 = P$, generan las distintas órbitas de $CL(P)$ bajo la acción de P . Obsérvese que los Q_k son p -grupos de Sylow. Como $p \nmid [P : P \cap N(Q_k)]$ si y sólo si $[P : P \cap N(Q_k)] = 1$, es decir, si y sólo si $P \cap N(Q_k) = P = P \cap Q_k = Q_k$, o sea, si y sólo si $k = 1$, la última afirmación resulta entonces de

$$n(p) = 1 + \sum_{k=2}^l [P : P \cap N(Q_k)], \quad (10.8)$$

la cual resulta, a su vez, de (10.7), y completa la demostración. $\square$

Si resulta ser $l = 1$, la sumatoria en (10.7) deberá tomarse igual a 1 y la de (10.8) deberá tomarse nula.

Como una consecuencia importante del anterior teorema, tenemos el siguiente corolario.

Corolario 10.9. Si $(G, \cdot)$ es un grupo finito de orden pq , donde $p < q$ son primos tales que $p \nmid (q-1)$, entonces G es cíclico.

Demostración. Como $n(p) \mid o(G)$, las únicas posibilidades para $n(p)$ son $n(p) = 1, p, q, pq$. Sea entonces P un p -subgrupo de Sylow de G . Claramente no puede ser $n(p) = pq$, pues $p \nmid pq-1$. Tampoco puede ser $n(p) = p$, pues $p \nmid (p-1)$. Finalmente, como $p \nmid (q-1)$, $n(p) \neq q$. Entonces $n(p) = 1$, y P es el único p -subgrupo de Sylow de G , de lo cual es normal en G . Por otra parte, si $n(q)$ es el número de q -subgrupos de Sylow y Q es uno de ellos, $n(q) = [G : N(Q)] = 1, p$. Si $n(q) = 1$ entonces $N(Q) = G$ y Q es normal en G . Por otra parte, no puede ser $n(q) = p$, pues debería tenerse que $q \mid (p-1)$, lo cual es absurdo. Entonces P y Q son normales en G , de lo cual resulta que si $P = [a]$ y $Q = [b]$ entonces $ab = ba$, y de esto se deduce fácilmente que $o(ab) = pq$. Entonces, G es cíclico. $\square$

Se deduce, por ejemplo, que sólo hay esencialmente un grupo de orden 15: el grupo cíclico $\mathbb{Z}_{15}$. Lo mismo es cierto de los grupos de orden 35: sólo $\mathbb{Z}_{35}$. Esto no vale, sin embargo, para los grupos de orden 6, pues $2 \mid (3-1)$, y, como sabemos, hay al menos dos de tales grupos: el cíclico, $\mathbb{Z}_6$, y el grupo

simétrico S_3 , el cual no es abeliano. Nótese que S_3 tiene, en efecto, tres subgrupos de Sylow de orden 2.

Veamos algunas aplicaciones de la teoría de Sylow en la clasificación de los grupos. En lo que sigue debe tenerse en cuenta que si $mn \neq 0$, $\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$ si y sólo si $\text{mcd}(m, n) = 1$, pues si $s = \text{mcm}(m, n)$, el orden de $(\bar{1}, \bar{1})$ como elemento de $\mathbb{Z}_m \times \mathbb{Z}_n$ es $s : o(\bar{1}, \bar{1}) = s$.

Ejemplo 10.1 Si p es un primo, sólo hay esencialmente dos grupos G de orden p^2 : $\mathbb{Z}_{p^2}$ y $\mathbb{Z}_p \times \mathbb{Z}_p$. En efecto, G es abeliano (corolario 10.5), y basta aplicar los resultados obtenidos en el capítulo 8. Nótese que $\mathbb{Z}_p \times \mathbb{Z}_p$ no es cíclico, pues todo elemento de $\mathbb{Z}_p \times \mathbb{Z}_p$, distinto del elemento neutro, tiene orden p . En particular, $\mathbb{Z}_9$ y $\mathbb{Z}_3 \times \mathbb{Z}_3$ son esencialmente los únicos grupos de orden 9.

Ejemplo 10.2. Sólo hay esencialmente dos grupos G de orden 45: $\mathbb{Z}_9 \times \mathbb{Z}_5 \approx \mathbb{Z}_{45}$ y $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \approx \mathbb{Z}_3 \times \mathbb{Z}_{15}$, ambos abelianos. En efecto, si $o(G) = 45$, G tiene, dado que $3 \nmid 4$, un único subgrupo $H(9)$ de orden 9. También, puesto que $5 \nmid 8$ y $5 \nmid 2$, G tiene un único subgrupo $H(5)$ de orden 5. Como $H(9)$ y $H(5)$ son entonces normales en G , G es el producto directo de $H(9)$ y $H(5)$, y la afirmación resulta de lo dicho en el ejemplo 10.1. Es también cierto que sólo existen esencialmente dos grupos de orden 99: $\mathbb{Z}_9 \times \mathbb{Z}_{11} \approx \mathbb{Z}_{99}$ y $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11} \approx \mathbb{Z}_3 \times \mathbb{Z}_{33}$, ambos abelianos.

Ejemplo 10.3. Sólo existen esencialmente dos grupos de orden 126 que tengan un subgrupo normal de orden 2. Estos son $\mathbb{Z}_9 \times \mathbb{Z}_7 \times \mathbb{Z}_2$ y $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_2 \approx \mathbb{Z}_3 \times \mathbb{Z}_{42}$, ambos abelianos. Nótese, al respecto, que $\mathbb{Z}_6 \times \mathbb{Z}_{21} \approx \mathbb{Z}_3 \times \mathbb{Z}_{42}$. Como $2 \mid 62$, $2 \mid 20$, $2 \mid 8$ y $2 \mid 6$, hay varias posibilidades para grupos no abelianos de orden 126.

Para terminar este capítulo, tenemos el siguiente teorema, frecuentemente útil.

Teorema 10.4. Si $(G, \cdot)$ es un grupo finito y H es un subgrupo de G tal que $p = [G : H]$ es el mínimo primo que divide a $o(G)$, entonces H es normal en G .

Demostración. Considérese la acción de G sobre G/H descrita en el ejemplo 9.5 y sea $N = \bigcap_{b \in G} bHb^{-1}$. Como se establece en el ejemplo 9.5, N es el estabilizador de G/H para esta acción. Claramente N es normal en G y $N \subseteq$

H , así que $[G : N] \geq p$, y si $[G : N] = p$, entonces $N = H$ y H será normal en G . Sea $\psi : G \rightarrow \mathcal{F}_0(G/H)$ dada por $\psi(a) = \psi_a$, donde $\psi_a(bH) = (ab)H$ para todo $b \in G$. Claramente ψ está bien definida (es decir, $\psi_a \in \mathcal{F}_0(G/H)$) y es un homomorfismo de G en $\mathcal{F}_0(G/H)$ (o sea, $\psi(ab) = \psi_{ab} = \psi_a \circ \psi_b = \psi(a)\psi(b)$). Además $\ker(\psi) = N$, y G/N será isomorfo a un subgrupo de $\mathcal{F}_0(G/H)$, así que $[G : N] \mid p!$. Pero, si fuera $[G : N] > p$, existiría un primo q , $q \mid (p-1)!$, tal que $q \mid [G : N]$, de lo cual $q \mid o(G)$. Como sería $q < p$, esto es absurdo. Entonces, $[G : N] = p$. $\square$

EJERCICIOS

- 10.1 ¿Cuántos grupos no isomorfos de órdenes 35 y 65 existen?
- 10.2 ¿Cuántos grupos posibles no isomorfos de órdenes 10 y 14 tienen subgrupos normales de orden 2?
- 10.3 Verifique que sólo existen dos grupos esencialmente distintos (no isomorfos) de orden 6: S_3 y $\mathbb{Z}_6$.
- 10.4 Sea $(G, \cdot)$ un grupo de orden p^2q donde $p > q$ son primos tales que $q \nmid p^2 - 1$. Demuestre que G es abeliano. ¿Qué se puede decir si $o(G) = p^2q^2$, $p > q + 1$ y $q \nmid p^2 - 1$?
- 10.5 Sean G un grupo finito, H un subgrupo normal de G , p un primo y P un p -subgrupo de Sylow de G . Demuestre que $H \cap P$ es un p -subgrupo de Sylow de H y que HP/H es un p -subgrupo de Sylow de G/H .
- *10.6 Sea G un grupo finito tal que, para todo primo p , todo p -subgrupo de G es normal en G . Demuestre que para cada divisor m de $o(G)$ existe un subgrupo normal H de G con $o(H) = m$. ¿Será esto aún cierto si sólo se supone que los p -subgrupos de Sylow de G son normales? (Resp: Sí.)
- *10.7 Sean G un grupo finito, p un primo y P un p -subgrupo de Sylow de G . Demuestre que $N(N(P)) = N(P)$. Más generalmente, demuestre que si H es un subgrupo de G tal que $N(P) \subseteq H$, entonces $N(H) = H$.
- 10.8 ¿Puede dar usted ejemplo de un grupo infinito en el cual todo elemento, salvo el elemento neutro, tenga orden p , p un primo?
- *10.9 Sean p un primo, G un p -grupo no cíclico. Demuestre que existe un subgrupo normal H de G tal que $G/H \approx \mathbb{Z}_p \times \mathbb{Z}_p$.

- 10.10 Sea G un p -grupo de orden p^n , $n \geq 1$ (p , primo). Demuestre que todo subgrupo de G de orden p^{n-1} es normal en G .
- 10.11 Sean G un grupo finito, p un primo y P un p -subgrupo de Sylow de G . Demuestre que si P es normal en G , existe un subgrupo H de G tal que $G = PH$. Dé un ejemplo que muestre que no necesariamente $G \approx P \times H$, aún si $H \cap P = \{e\}$. Demuestre, sin embargo, que esto último es cierto si $P \subseteq Z(G)$.
- 10.12 Sean G un p -grupo (p , primo), P un subgrupo normal de G . Demuestre, que existe un subgrupo normal H de G tal que $G = PH$, pero que no necesariamente $G \approx P \times H$. (Indicación. Considere $\mathbb{Z}_{p^2}$, p un primo.)
- *10.13 Sea G un grupo finito y supóngase que $o(G) = p_1 p_2 p_3$ donde $p_1 < p_2 < p_3$ son primos. Demuestre que si G tiene un subgrupo normal de orden p_2 entonces tiene también un subgrupo normal de orden p_3 .
- *10.14 Sean G un grupo finito, p un primo tal que $p \mid o(G)$ y que $\varphi(a) = a^p$ es un homomorfismo de G en sí mismo. Demuestre que:
- G tiene un único p -subgrupo de Sylow.
 - Si P es el p -subgrupo de Sylow de G entonces P es normal en G y existe un subgrupo normal H de G tal que G es el producto directo de P y H .
 - $Z(G) \neq \{e\}$.
- *10.15 Sea G un grupo de orden pqr , donde $p < q < r$ son primos. Demuestre
- G tiene un único r -subgrupo de Sylow.
 - G tiene un subgrupo normal de orden qr .
 - Si $q \nmid (r-1)$, el q -subgrupo de Sylow de G es normal en G .
- 10.16 Sean p un primo, G un grupo de orden p^n , $n \geq 1$. Demuestre que G es abeliano si y sólo si $o(Z(G)) \geq p^{n-1}$, y que si $o(Z(G)) \geq p^{n-2}$ entonces $G/Z(G)$ es abeliano.
- 10.17 Demuestre que todo grupo de orden 30 tiene un y sólo un subgrupo normal de orden 15 y que $\mathbb{Z}_{30}$ es esencialmente el único grupo de orden 30 con un subgrupo normal de orden 2. Verifique, en particular, que $S_3 \times \mathbb{Z}_5$ no tiene subgrupos normales de orden 2.

- 10.18 Demuestre que si un grupo de orden 36 no tiene subgrupos normales de orden 3 entonces tiene subgrupos normales de órdenes 9 y 18. (Indicación. ejercicio 9.6.)
- 10.19 Demuestre que si un grupo de orden 108 no tiene subgrupos normales de orden 9 entonces tiene subgrupos normales de órdenes 27 y 54. Demuestre también que si un grupo de orden 54 no tiene subgrupos normales de orden 9 entonces tiene subgrupos normales de orden 6.
- *10.20 Sean p un primo, G un p -grupo finito. Demuestre que si $N \neq \{e\}$ es un subgrupo normal de G , entonces $N \cap Z(G) \neq \{e\}$.

Capítulo 11

Grupos del tipo (p, q) y grupos diedros

Haremos en este capítulo una breve excursión en el problema de la existencia y clasificación de los grupos finitos no conmutativos: la búsqueda de ejemplos concretos con los cuales comparar un grupo abstracto dado, colocándolo dentro de su clase de isomorfía. Teniendo que ver con el problema de la existencia de tales ejemplos, esto mostraría, de paso, que muchos resultados de la teoría de los grupos no son afirmaciones sobre objetos inexistentes. Desafortunadamente, éstos no son problemas fáciles, y sólo podremos analizar casos sencillos (y no completamente), con el propósito de ilustrar al lector sobre la naturaleza del problema. Nos limitaremos así a los llamados grupos del tipo (p, q) y, en particular, a los grupos diedros. Sólo para estos últimos, y para los primeros cuando $p < q$ son primos, daremos resultados completos de existencia e isomorfía análogos a los dados para los grupos cíclicos (capítulos 2 - 6) y para los grupos abelianos finitos (capítulo 7).

El problema de la existencia de grupos con propiedades específicas se aborda usualmente mediante la teoría de los llamados grupos libres (y de los subgrupos y grupos cocientes de éstos determinados mediante generadores y relaciones). Esta teoría, bastante abstracta, conduce generalmente, para su concreción, a la llamada teoría de la representación de los grupos, un tema relativamente avanzado de la matemática, que hace buen uso del álgebra lineal y especialmente de la teoría de matrices, y que por tal razón no podemos considerar aquí (véanse, sin embargo, los ejercicios 11.14 y 11.17, para una muestra de su carácter).

En lugar de lo anterior, nosotros estableceremos dos teoremas de existencia de grupos, identificándolos como subgrupos de un grupo $(S_n, \cdot)$ apropiado. Para establecer ciertas relaciones necesarias recurriremos a algunos resultados elementales sobre los grupos multiplicativos $(\mathbb{Z}_n^*, \cdot)$, donde n es un primo y $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$, estando dado el producto por la relación

$$\bar{a} \cdot \bar{b} = \overline{ab}, \quad a, b \in \mathbb{Z}, \quad (11.1)$$

donde $\bar{a} = a + n\mathbb{Z}$. Como $\bar{a} = r(a, n) + n\mathbb{Z}$, siendo $r(a, n)$ el resto de dividir a por n , se tiene que $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ y $\mathbb{Z}_n^* = \{\bar{1}, \bar{2}, \dots, \overline{n-1}\}$. Recordamos (capítulo 5) que si $a, b \in \mathbb{Z}$, la relación $a \equiv b \pmod{n}$ significa que $\bar{a} = \bar{b}$ en $\mathbb{Z}_n$, es decir, que $n \mid a - b$. Por ejemplo, $a \equiv r(a, n) \pmod{n}$ para todo $a \in \mathbb{Z}$, y $a \equiv 0 \pmod{n}$ si y sólo si $n \mid a$.

Mostrar que la ley de composición (11.1) está bien definida y es una ley de composición interna en $\mathbb{Z}_n$ que cuando n es primo hace del conjunto $\mathbb{Z}_n^*$ un grupo abeliano, fue establecido en el capítulo 5, nota 5.6. También es claro que si p y q son primos distintos y existe $1 < r < q$ tal que $\bar{r}^p = \bar{1}$ en $\mathbb{Z}_q^*$, necesariamente $p \mid q - 1$. En efecto, el orden $o(\bar{r})$ de $\bar{r}$ en $\mathbb{Z}_q^*$ será > 1 (pues $\bar{r} \neq \bar{1}$, ya que $q \nmid r - 1$), y dividirá a p y a $q - 1$, pues $\mathbb{Z}_q^*$ es un grupo y $o(\mathbb{Z}_q^*) = q - 1$. Esto implica que $o(\bar{r}) = p$, de lo cual $p \mid q - 1$. Menos trivial es demostrar que si $p \mid q - 1$, tal r existe, pero esto es consecuencia del teorema de Cauchy (teorema 4.3). Además, el subgrupo $\langle \bar{r} \rangle$ generado por $\bar{r}$ en $\mathbb{Z}_q^*$ es $\{\bar{r}^k : 0 \leq k < p\}$ y tiene orden p , así que las $\bar{r}^k$, $0 \leq k < p$, son todas distintas y $o(\bar{r}^k) = p$. Hemos demostrado entonces el siguiente resultado.

Lema 11.1. Si $p < q$ son primos, $p \mid q - 1$ si y sólo si existe $1 < r < q$ tal que $o(\bar{r}^k) = p$ en $\mathbb{Z}_q^*$, así que $r^k \not\equiv 1 \pmod{q} = r^k q = r^k q$ para $k = 1, \dots, p - 1$, pero $r^p \equiv 1 \pmod{q}$.

Nota 11.1. Obsérvese que, bajo las hipótesis del lema anterior, la ecuación $x^p = \bar{1}$ tiene un conjunto completo de soluciones distintas en $\mathbb{Z}_q^*$ (es decir, p soluciones distintas, las únicas posibles. Véanse, al respecto, los resultados mencionados en la nota 5.7 y en los ejercicios 6.13 - 6.16). De esta observación se deduce sin más el siguiente corolario del lema 11.1, el cual será importante en la demostración del teorema 11.9.

Corolario 11.1. Si $p < q$ son primos, $p \mid q - 1$ y $1 < r, s < q$ son tales que $r^p \equiv 1 \pmod{q}$ y $s^p \equiv 1 \pmod{q}$, existe $1 \leq k < p$ tal que

$$s \equiv r^k \pmod{q}. \quad (11.2)$$

Demostración. Si H es el subgrupo de $(\mathbb{Z}_q^*, \cdot)$ generado por $\bar{r}$, $o(H) = p$. Como en $\mathbb{Z}_q^*$ sólo hay p soluciones de $x^p = \bar{1}$, necesariamente $\bar{s} \in H$, así que $\bar{s} = \bar{r}^k$ para algún $1 \leq k < p$. Está demostrado (11.2). $\square$

Definición 11.1. Sean p, q enteros, $p \geq 1, q \geq 1$. Se dice que un grupo $(G, \cdot)$ es del tipo (p, q) , si existen $a, b \in G$ y $1 < r < q$ tales que:

- (i) $o(a) = p, \quad o(b) = q.$
- (ii) $ab = b^r a.$
- (iii) Todo elemento $x \in G$ se escribe de manera única en la forma $x = a^i b^j$, donde $i, j \in \mathbb{Z}, 0 \leq i < p, 0 \leq j < q.$

Obsérvese que $q \geq 3$ y que G es no conmutativo, así que $p \geq 2$. De (iii) se deduce además que G es finito con

$$o(G) = pq. \quad (11.3)$$

Si $(G, \cdot)$ es como en la definición 11.1, se dice, más precisamente, que $(G, \cdot)$ es del tipo (p, q) y generado por (a, b) .

De la definición 11.1 se deduce fácilmente que

$$(iv) \quad ab^{r^n} = b^{r^{n+1}} a, \quad n = 0, 1, 2, \dots$$

$$(v) \quad a^n b = b^{r^n} a^n, \quad n = 0, 1, 2, \dots$$

$$(vi) \quad a^n b^s = b^{sr^n} a^n, \quad n \geq 0, s \in \mathbb{Z}.$$

En efecto, la afirmación (iv) es cierta si $n = 0$, y para $n > 0$ resulta de que $ab^{r^n} a^{-1} = (aba^{-1})^{r^n} = (b^r)^{r^n} = b^{r^{n+1}}$. La demostración de (v) resulta de un sencillo argumento por inducción basado en (iv), y la de (vi), de observar que $a^n b^s a^{-n} = (a^n b a^{-n})^s = (b^{r^n})^s = b^{sr^n}$.

Además,

$$r^p \equiv 1 \pmod{q}, \quad \text{mcd}(r, q) = 1. \quad (11.4)$$

En efecto, de (v), $a^p b = b^{r^p} a^p$, o sea, $b = b^{r^p}$. Entonces $b^{r^p-1} = e$, de lo cual $q \mid r^p - 1$. Por otra parte, si fuera $\text{mcd}(r, q) = d \neq 1$, sería $o(b^r) = q/d$, lo cual es absurdo, pues de $b^r = aba^{-1}$ se deduce que $o(b^r) = o(b) = q$.

Como evidentemente $a^{-1} = a^{p-1}$, (11.4) y la validez de (vi) para $n \geq 0$ implican su validez para todo $n \in \mathbb{Z}$, así que

(vii) $a^n b^s = b^{sr^n} a^n$, $b^s a^n = a^n b^{sr^n}$, $n, s \in \mathbb{Z}$.

Teorema 11.1. Sea $(G, \cdot)$ del tipo (p, q) y generado por (a, b) . Sean $M = [a]$ y $N = [b]$. Entonces $G = MN$ y N es un subgrupo normal de G . Además, $M \cap N = \{e\}$.

Demostración. Que $G = MN$ resulta inmediatamente de (iii). Por otra parte, de (ii) existe $1 < r < q$ tal que $aba^{-1} = b^r$, y de (vii) resulta que $a^n b^s a^{-n} = b^{sr^n} \in N$ cualesquiera que sean $s, n \in \mathbb{Z}$. Sean entonces $0 \leq i < p$, $0 \leq j < q$ y $x = a^i b^j \in G$. Entonces $xb^s x^{-1} = a^i (b^j b^s b^{-j}) a^{-i} = a^i b^s a^{-i} \in N$ cualquiera que sea $s \in \mathbb{Z}$, lo cual demuestra que N es normal. Finalmente, de $o(M/M \cap N) = o(MN/N) = o(G/N) = p$ se deduce que $o(M \cap N) = 1$, lo cual completa la demostración. $\square$

Nota 11.2. Obsérvese que en el anterior teorema, la aplicación

$$\varphi: M \times N \longrightarrow G, \quad \varphi(x, y) = xy,$$

resulta ser biyectiva. Sin embargo, no puede ser un isomorfismo de grupos. En efecto, M no puede ser normal en G (pues sería $ab = ba$ y (ii) no podría ser válida), así que G no puede ser el producto directo de M y N .

Nota 11.3. Es claro que si $(G, \cdot)$ es finito y no conmutativo, y si $G = MN$ donde M y N son subgrupos cíclicos de G tales que $M \cap N = \{e\}$ y que N es normal en G , entonces G es del tipo (p, q) donde $p = o(M)$ y $q = o(N)$, y si $M = [a]$ y $N = [b]$, entonces (a, b) genera a G . En efecto, es claro que (i) y (iii) se satisfacen para (a, b) y que $aba^{-1} = b^r$, $0 \leq r < q$. Obviamente no puede ser $r = 0$, pues $b \neq e$, y tampoco puede ser $r = 1$, pues $(G, \cdot)$ no es conmutativo. Obsérvese que, bajo las hipótesis, $p \geq 2$ y $q \geq 3$.

Nota 11.4. Demostrar la existencia de grupos de un tipo (p, q) dado no es, en general, una tarea fácil. Nosotros no haremos esto sino en dos casos muy especiales, aunque algunos de los resultados, incluyendo el lema 11.1, pueden extenderse para incluir circunstancias algo más generales (véase [2]).

Definición 11.2. Se dice que un grupo G del tipo $(2, q)$ es *diedro*, si está generado por un par (a, b) tal que $o(a) = 2$, $o(b) = q$ y

$$aba^{-1} = b^{-1}. \quad (11.5)$$

Se escribe $G = D_q(a, b)$.

Nota 11.5. Obsérvese que $b^{-1} = b^{q-1}$.

Teorema 11.2. Si $(G, \cdot)$ es un grupo de orden $2q$ con $q \geq 3$, $a \in G$ es tal que $o(a) = 2$, y existe $b \in G$ con $o(b) = q$ y $aba^{-1} = b^{-1}$, entonces G es diedro y generado por (a, b) , así que $G = D_q(a, b)$.

Es necesario demostrar G es del tipo $(2, q)$, o sea, que (iii) de la Definición 11.1 se verifica. Esto será consecuencia del resultado más general siguiente.

Teorema 11.3. Sea $(G, \cdot)$ un grupo de orden pq , donde p es primo. Si para algún $a \in G$ tal que $o(a) = p$ existe $b \in G$ tal que $o(b) = q$ y que

$$aba^{-1} = b^r, \quad 1 < r < q, \quad (11.6)$$

entonces G es del tipo (p, q) y generado por (a, b) .

Demostración. Sean $M = [a]$ y $N = [b]$. Entonces $M \cap N = \{e\}$, ya que si $a^s \in N$, $1 \leq s < p$, entonces $M = [a^s] \subseteq N$, lo cual es absurdo, pues como N es conmutativo, (11.6) no podría tenerse con $r \neq 1$. Entonces $\#(MN) = pq$ y $G = MN$. Como (11.6) garantiza también que N es normal en G , el teorema resulta de lo dicho en la nota 11.3. $\square$

Demostraremos ahora la existencia de grupos diedros.

Teorema 11.4. Para todo $q \geq 3$ existen grupos diedros de orden $2q$. Uno de ellos es el subgrupo $D_q(\sigma, \rho)$ de S_q generado por el q -ciclo $\rho = (1, 2, \dots, q)$ y la permutación σ dada por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & \frac{q+1}{2} & \frac{q+3}{2} & \dots & q \\ 1 & q & q-1 & \dots & \frac{q+3}{2} & \frac{q+1}{2} & \dots & 2 \end{pmatrix} \quad (11.7)$$

si q es impar y por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & \frac{q}{2} & \frac{q+2}{2} & \frac{q+4}{2} & \dots & q \\ 1 & q & q-1 & \dots & \frac{q+4}{2} & \frac{q+2}{2} & \frac{q}{2} & \dots & 2 \end{pmatrix} \quad (11.8)$$

si q es par.

Demostración. Nótese que σ es simplemente la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & q-1 & q \\ 1 & q & q-1 & \dots & 3 & 2 \end{pmatrix}.$$

Evidentemente $\sigma \neq e$ y, como se deduce de (11,7) y (11,8),

$$\sigma = (2, q)(3, q-1) \cdots \left(\frac{q+1}{2}, \frac{q+3}{2} \right), \quad q \text{ impar}, \quad (11.9)$$

y

$$\sigma = (2, q)(3, q-1) \cdots \left(\frac{q}{2}, \frac{q+4}{2} \right), \quad q \text{ par}. \quad (11.10)$$

Siendo producto de transposiciones disyuntas, $\sigma^2 = e$. Además, $\sigma\rho\sigma^{-1} = \sigma^{-1}\rho\sigma = (\sigma(1), \sigma(2), \dots, \sigma(q)) = (1, q, q-1, \dots, 2) = \rho^{-1}$, y se tiene que $o(\rho) = l(\rho) = q$. Por lo tanto, si G es el subgrupo de S_q generado por $\{\sigma, \rho\}$, el teorema 11.3 garantiza que $G = D_q(\sigma, \rho)$. $\square$

Nota 11.6. Si σ es una permutación de S_q tal que $\sigma^{-1}\rho\sigma = \rho$, donde $\rho = (1, 2, \dots, q)$, entonces $(\sigma(1), \sigma(2), \dots, \sigma(q))$ es $(k+1, k+2, \dots, q, 1, 2, \dots, k)$ para algún $1 \leq k \leq q$, así que

$$\sigma(j) = \begin{cases} k+j, & 1 \leq j \leq q-k \\ q-k+j, & q-k < j \leq q. \end{cases} \quad (11.11)$$

Entonces $\sigma = \rho^k$, $1 \leq k \leq q$. Se deduce que si σ, τ son tales que $\sigma\rho\sigma^{-1} = \rho^{-1}$ y $\tau\rho\tau^{-1} = \rho^{-1}$, en cuyo caso $\tau^{-1}(\sigma\rho\sigma^{-1})\tau = \rho$, necesariamente $\sigma^{-1}\tau = \rho^k$ para algún $0 \leq k < q$, de lo cual $\tau = \sigma\rho^k \in D_q(\sigma, \rho)$. Es decir, todas las permutaciones τ tales que $\tau\rho\tau^{-1} = \rho^{-1}$ están en el grupo $D_q(\sigma, \rho)$ del teorema 11.4, y como además $(\sigma\rho^k)^2 = \sigma\rho^k\sigma\rho^k = \rho^{-k}\rho^k$ para σ en tal teorema, necesariamente $\tau^2 = e$. Entonces $D_q(\sigma, \rho) = D_q(\tau, \rho)$, así que $D_q(\sigma, \rho)$ no depende de σ en tanto $\sigma\rho\sigma^{-1} = \rho^{-1}$. Tampoco depende de ρ en tanto ρ sea una potencia k -ésima de $(1, 2, \dots, q)$ con $\text{mcd}(q, k) = 1$, pero, en general, ρ no puede sustituirse por un q -ciclo arbitrario. Obsérvese finalmente que

$$D_q(\sigma, \rho) = \{e, \sigma\} \cup \{\rho^k : 1 \leq k < q\} \cup \{\sigma\rho^k : 1 \leq k < q\} \quad (11.12)$$

y que la reunión es disyunta.

Nota 11.7. Si $(G, \cdot)$ es un grupo no conmutativo de orden $2q$ y N es un subgrupo de orden q de G , N es necesariamente normal en G . En efecto, si $a \in G$ y $a \notin N$ entonces $aN \cap N = N \cap Na = \emptyset$. Como $[G : N] = 2$ entonces $G = aN \cup N = N \cup Na$, lo cual implica que $aN = Na$. En virtud de lo dicho en la nota 11.3, si existe $b \in N$ tal que $o(b) = q$ (lo cual ocurre, por ejemplo, si q es primo), y $o(a) = 2$, G es del tipo $(2, q)$ y generado por (a, b) . Esto no garantiza que G sea diedro. Este es sin embargo el caso si $q \geq 3$ es

primo, pues si $aba^{-1} = b^r$, $1 < r \leq q-1$, de $r^2 \equiv 1 \pmod{q}$ (relación (11,4)) se deduce que $q \mid (r-1)(r+1)$, así que $q = r+1$ y $r = q-1$. Entonces:

Teorema 11.5. Si G es no conmutativo y de orden $2q$, donde $q \geq 3$ es primo, entonces G es diedro, y si $a, b \in G$ son tales que $o(a) = 2$, $o(b) = q$, G está generado por (a, b) , y $aba^{-1} = b^{-1}$.

Nota 11.8. Obsérvese que obviamente $2 \mid q-1$ en el teorema anterior.

Caracterizaremos ahora como grupos del tipo (p, q) a los grupos no conmutativos de orden pq donde $p < q$ son primos. Necesitaremos el siguiente lema.

Lema 11.2. Si $(G, \cdot)$ es un grupo no conmutativo de orden pq , donde $p < q$ son primos, entonces $p \mid q-1$, y si $b \in G$ es tal que $o(b) = q$, $N = [b]$ es un subgrupo normal de G .

Demostración. Sean $a, b \in G$ tales que $o(a) = p$ y $o(b) = q$, y sean $M = [a]$ y $N = [b]$. Como $M \cap N = \{e\}$ entonces $\#(MN) = pq$, así que $G = MN$ y todo elemento x de G se escribe de manera única en la forma $x = b^i a^j$, $0 \leq i \leq q-1$, $0 \leq j \leq p-1$. Obsérvese que si H_1 y H_2 son subgrupos distintos de G de orden q , necesariamente $H_1 \cap H_2 = \{e\}$. Supóngase entonces que N no es normal en G (así que $p > 2$) pero que $a^i N a^{-i} = N$, donde $1 \leq i < p$. Entonces $a^i b a^{-i} = b^r$, $1 \leq r \leq q-1$, lo cual es absurdo, pues G sería conmutativo o del tipo (p, q) y generado por (a^i, b) (teorema 11.3), lo cual garantizaría la normalidad de N . Entonces, los conjugados $a^i N a^{-i}$ de N , $0 \leq i < p$, son todos distintos, lo cual implica que sólo se intersectan en $\{e\}$ y que G tiene al menos $p(q-1)$ elementos de orden q (el número de elementos distintos en la reunión de los $a^i N a^{-i}$, $0 \leq i < p$). Esto deja lugar a sólo $p-1$ elementos de orden p (pues $p(q-1) + 1 + (p-1) = p(q-1) + p = pq$), así que $M = [a]$ es necesariamente normal en G y G es del tipo (q, p) y generado por (b, a) (nota 11.3). Sea $1 < r < p$ tal que $b a b^{-1} = a^r$. Ahora, como $(\mathbb{Z}_p, \cdot)$ es un grupo de orden $p-1$, si $\bar{r}$ denota la clase módulo p de r y $\bar{r}^k = \bar{1}$, o sea, si $r^k \equiv 1 \pmod{p}$, entonces $\text{mcd}(k, p-1) \neq 1$, y como, según (11.4), $r^q \equiv 1 \pmod{p}$, entonces $\text{mcd}(q, p-1) \neq 1$, lo cual es absurdo. Entonces N es normal en G y, por lo observado en la nota 11.3, G es del tipo (p, q) y generado por (a, b) . Supongamos entonces que $aba^{-1} = b^r$, $1 < r < q$. Como $r^p \equiv 1 \pmod{q}$ (relación (11.4)), entonces $p \mid q-1$ (lema 11.1). $\square$

Nota 11.9. De hecho, N es el único subgrupo normal de orden q . En efecto, M no puede ser normal en G , pues si tal fuera el caso se tendría que $ab = ba$,

lo cual implicaría que G es abeliano. Entonces, tal como al comienzo de la demostración del lema 11.2, se concluye que G tiene $q(p-1)$ elementos de orden p , lo cual sólo deja campo para $q-1$ elementos de orden q . Obsérvese finalmente que si $p \nmid q-1$, G deberá ser irremediabilmente abeliano.

Nota 11.10. Los resultados del anterior lema y de la nota 11.9 son consecuencia inmediata de la teoría de Sylow (teoremas 10.3 y 10.4). La demostración que dimos no recurre a esta teoría, para preservar la independencia del capítulo. De la demostración del lema 11.2 se deduce sin más que:

Teorema 11.6. Si $(G, \cdot)$ es no conmutativo y de orden pq , donde $p < q$ son primos, entonces $p \mid q-1$, y si $a, b \in G$ son tales que $o(a) = p$ y $o(b) = q$, G está generado por (a, b) .

Demostraremos ahora la existencia de grupos del tipo (p, q) , cuando $p < q$ son primos y $p \mid q-1$.

Teorema 11.7. Si $p < q$ son primos tales que $p \mid q-1$, existe un grupo $D[p, q]$ del tipo (p, q) .

Demostración. Podemos suponer que $p > 2$ (teorema 11.5). Sea $1 < r < q$, mínimo, tal que $\bar{r}$ sea solución de la ecuación $x^p = \bar{1}$ en $\mathbb{Z}_q^*$ (lema 11.1). Sean $\rho = (1, 2, \dots, q)$ y σ una permutación de S_q tales que $\sigma\rho\sigma^{-1} = \rho^r$ y que $\sigma(1) = 1$. Tal permutación existe pues ρ^r es también un q -ciclo, y la condición $\sigma(1) = 1$ la determina unívocamente. Sea $D[p, q]$ el subgrupo de S_q generado por $\{\sigma, \rho\}$. Claramente $o(\rho) = q$. Demostraremos que $\sigma^p = e$, lo cual, dado que $\sigma \neq e$ (pues $\rho^r = (\sigma^{-1}(1), \dots, \sigma^{-1}(q)) \neq \rho$), asegurará que $o(\sigma) = p$, y completará, en virtud del teorema 11.6, la demostración. Pero, tal como en la demostración de (v), se deduce, a partir de $\sigma\rho = \rho^r\sigma$, que $\sigma^p\rho = \rho^{r^p}\sigma^p$. Entonces $\sigma^p\rho = \rho\sigma^p$, pues $r^p \equiv 1 \pmod{q}$. En virtud de lo dicho en la nota 11.6, esto implica que $\sigma^p = \rho^k$, $0 \leq k < q$. Pero, como $\sigma^p(1) = 1$ y ρ^k es un q -ciclo si $1 \leq k < q$, necesariamente $k = 0$ y $\sigma^p = e$. $\square$

Nota 11.11. Si G tiene orden pq , donde $p < q$ son primos, y M y N son subgrupos respectivos de órdenes p y q de G , entonces G es cíclico si y sólo si M y N son normales en G (que es el caso si $p \nmid q-1$). En efecto, si $M = [a]$, $N = [b]$ y son normales, $ab = ba$, lo cual implica que $o(ab) = o(a)o(b) = pq$. En tales circunstancias $G \approx \mathbb{Z}_{pq}$ (lo cual es aún posible si $p \mid q-1$).

Estudiaremos ahora el problema de la isomorfía de los grupos del tipo (p, q) y de los grupos diedros.

Teorema 11.8. Sean $(G_1, \cdot)$ y $(G_2, \cdot)$ grupos del tipo (p, q) , con generadores respectivos (a_1, b_1) y (a_2, b_2) . Si $a_i b_i a_i^{-1} = b_i^r$, $1 < r < q$, $i = 1, 2$, entonces $G_1 \approx G_2$.

Demostración. Sean $a = a_i$, $b = b_i$, $i = 1, 2$. Entonces $(a^i b^j) (a^h b^k) = a^i (b^j a^h) b^k$, donde $0 \leq i, h < p$, $0 \leq j, k < q$, de lo cual, mediante (vii), $(a^i b^j) (a^h b^k) = a^{i+h} b^{jr^h+k}$. Por lo tanto, si $f : G_1 \mapsto G_2$ está dada por $f(a_1^i b_1^j) = a_2^i b_2^j$, $i, j \in \mathbb{Z}$ (que f está bien definida resulta de (iii)), entonces

$$\begin{aligned} f((a_1^i b_1^j) (a_1^h b_1^k)) &= f(a_1^{i+h} b_1^{jr^h+k}) = a_2^{i+h} b_2^{jr^h+k} = (a_2^i b_2^j) (a_2^h b_2^k) \\ &= f(a_1^i b_1^j) f(a_1^h b_1^k), \end{aligned}$$

así que f es un homomorfismo; de hecho, un epimorfismo. Que f es inyectiva resulta de observar que si $f(a_1^i b_1^j) = a_2^i b_2^j = e$, donde $0 \leq i < p$, $0 \leq j < q$, necesariamente $i = j = 0$, de lo cual $a_1^i b_1^j = e$. Esto demuestra el teorema. $\square$

Corolario 11.2. Todo grupo diedro G de orden $2q$ es isomorfo al grupo $D_q(\sigma, \rho)$.

Necesitaremos ahora el siguiente lema.

Lema 11.3. Si G es del tipo (p, q) y está generado por (a, b) con $aba^{-1} = b^r$, $1 < r < q$, y si $1 \leq l < p$ es tal que $\text{mcd}(r^l, q) = 1$, entonces G está también generado por a y por $b_1 = b^{r^l}$. Además, $ab_1 a^{-1} = b_1^r$.

Demostración. Como $\text{mcd}(r^l, q) = 1$ entonces $o(b_1) = q$, y la relación $ab_1 a^{-1} = b_1^r$ resulta fácilmente de (vii). Ahora, si $M = [a]$ y $N = [b]$ entonces $G = MN$ y $M \cap N = \{e\}$, y como $N = [b_1]$, (iii) es también válida para (a, b_1) (nota 11.3). $\square$

Teorema 11.9. Si G_1 y G_2 son del tipo (p, q) , donde $p < q$ son primos, entonces $G_1 \approx G_2$.

Demostración. Supóngase que G_1 está generado por a_1 y b_1 con $a_1 b_1 a_1^{-1} = b_1^r$, $1 < r < q$, y que G_2 lo está a su vez por a_2 y b_2 con $a_2 b_2 a_2^{-1} = b_2^s$, $1 < s < q$. De (11.4), $r^p \equiv 1 \pmod{q}$ y $s^p \equiv 1 \pmod{q}$. En virtud del corolario 11.1, esto implica que $s \equiv r^k \pmod{q}$, $0 \leq k < p$. De hecho $k > 0$, pues $q \nmid s-1$, y $q \nmid r^k$, ya que $q \nmid s$. Entonces $\text{mcd}(r^k, q) = 1$. Del lema 11.3 se

deduce entonces, reemplazando a b_2 por $b_2^{r^k}$, si es necesario, que podemos suponer $s = r$. En virtud de lo establecido en el teorema 11.8, esto implica que $G_1 \approx G_2$. $\square$

Nota 11.12. Se deduce que si G es del tipo (p, q) , donde $p < q$ son primos, G está generado por (a, b) y (c, d) , y $aba^{-1} = b^r$, $cdc^{-1} = d^s$, $1 < r, s < q$, entonces existe $0 < k < p$ tal que $s \equiv r^k \pmod{q}$.

Corolario 11.3. Si G_1 y G_2 son grupos no conmutativos de orden pq , donde $p < q$ son primos, entonces $G_1 \approx G_2$.

Invocando los teoremas 11.6 y 11.7, se tiene el resultado más preciso siguiente.

Corolario 11.4. Si G es un grupo no conmutativo de orden pq donde $p < q$ son primos, entonces $p \mid q - 1$, y G es, de hecho, isomorfo al grupo $D[p, q]$.

Nota 11.13. Se concluye que si G es un grupo de orden pq , donde $p < q$ son primos, se tiene la alternativa

1. $G \approx \mathbb{Z}_{pq}$
2. $G \approx D[p, q]$

La primera posibilidad ocurre si y sólo si G es abeliano, lo cual se da automáticamente si $p \nmid q - 1$. La segunda posibilidad ocurre si y sólo si G es no abeliano, lo cual sólo es posible si $p \mid q - 1$.

Nota 11.14. El grupo diedro $D_q(\sigma, \rho)$ admite una interpretación simple y sugestiva que no deja de ser útil para calcular explícitamente tal grupo en casos especiales: como el grupo de las simetrías de un polígono regular de q lados.

Considérese el conjunto $S(q)$ de las simetrías de un polígono regular de q lados con respecto a sus "elementos de simetría". Estos últimos son:

1. Las bisectrices de los ángulos en los vértices, es decir, las rectas del plano que bisecan cada uno de estos ángulos.
2. El centro del polígono: punto de intersección de las bisectrices.
3. Las mediatrices, es decir, las rectas del plano que unen los puntos medios de lados opuestos.

Las mediatrices son elementos de simetría sólo cuando q es par, y son $\frac{q}{2}$ en número. Las correspondientes simetrías son:

- a. Las reflexiones sobre una bisectriz.
- b. Las rotaciones en un ángulo $\frac{2\pi}{q}k$, $k = 1, 2, \dots, q$, alrededor del centro.
- c. Las reflexiones sobre una mediatriz, cuando q es par.

Nótese que las bisectrices son q si q es impar y sólo $\frac{q}{2}$ si q es par, pues en este último caso cada una de ellas biseca simultáneamente dos ángulos.

Esto determina el número de posibles simetrías con respecto a cada uno de los elementos: $\frac{q}{2}$ reflexiones sobre las bisectrices si q es par; q , si q es impar; el número de rotaciones alrededor del centro es siempre q ; cuando q es par habrá además $\frac{q}{2}$ reflexiones sobre las mediatrices. Esto da un total de $2q$ simetrías en cada caso. Así, $\#(S(q)) = 2q$. La ley de composición que hace de $S(q)$ un grupo se obtiene dando un sentido dinámico a las simetrías: reflejar sobre una recta, rotar en un cierto ángulo. La composición se obtiene entonces efectuando una de tales acciones, α , y seguidamente la otra, β . El resultado se escribe $\beta \circ \alpha$ o $\alpha\beta$, según el gusto. Nosotros preferiremos la segunda notación. Como es claro, cualquier sucesión de tales acciones deja invariante el polígono y debe ser por lo tanto una de las simetrías mencionadas. Es además claro que si α es una reflexión entonces $o(\alpha) = 2$, y que si β es una rotación en un ángulo $\frac{2\pi}{q}$ entonces $o(\beta) = q$.

Para interpretar $S(q)$ en términos de $D_q(\sigma, \rho)$, enumérense los vértices del polígono de 1 a q en el sentido positivo (el opuesto al del movimiento de las manecillas del reloj). Luego escójase un sistema de coordenadas $x-y$ en el plano de tal manera que el eje y sea la bisectriz al primer vértice del polígono, así que el centro de éste está también sobre el eje y . Colóquese finalmente el centro del polígono en el punto $(0, 0)$ del sistema $x-y$, y efectuando una rotación del polígono en un ángulo π , si es necesario, colóquese su primer vértice en el semiplano superior del sistema de coordenadas. Diremos en este caso que el polígono está en posición inicial canónica. Sea β la rotación en el sentido positivo en un ángulo $\frac{2\pi}{q}$. Los vértices se permutarán en el orden $1 \rightarrow 2 \rightarrow 3 \rightarrow \dots \rightarrow q-1 \rightarrow q \rightarrow 1$, y es natural describirla mediante el ciclo $(1, 2, 3, \dots, q-1, q) = \rho$. A su vez, la reflexión α sobre el eje y (la bisectriz al primer vértice) permutará los vértices en la forma $1 \rightarrow 1, 2 \rightarrow q, 3 \rightarrow q-1, \dots, q-1 \rightarrow 3, q \rightarrow 2$, y puede entonces describirse mediante la

permutación σ dada por (11.7) o (11.8) en el teorema 11.4. Como es obvio, con estas identificaciones $\alpha\beta$ se identifica con $\sigma\rho$, y más generalmente, $\alpha^i\beta^j$, $i = 1, 2$, $j = 1, 2, \dots, q$, con $\sigma^i\rho^j$. Podemos entonces considerar que $S(q)$ es un subgrupo de $D_q(\sigma, \rho)$, así que $S(q) = D_q(\sigma, \rho)$. Como es claro, $\alpha^2 = e$ (todo queda quieto) y β^k , $1 \leq k \leq q$, es la rotación en un ángulo $\frac{2\pi}{q}k$, con $\beta^q = e$, así que si α_i denota la reflexión sobre la bisectriz al i -ésimo vértice ($\alpha_1 = \alpha$) y γ_j es la reflexión sobre la mediatriz por el punto medio del lado $[j, j+1]$, entonces

$$S(q) = \{\beta^k : 1 \leq k \leq q\} \cup \{\alpha_i : 1 \leq i \leq q\}, q \text{ impar} \quad (11.13)$$

y

$$S(q) = \{\beta^k : 1 \leq k \leq q\} \cup \{\alpha_i : 1 \leq i \leq \frac{q}{2}\} \cup \{\gamma_j : 1 \leq j \leq \frac{q}{2}\}, q \text{ par.} \quad (11.14)$$

La identificación de $S(q)$ con $D_q(\sigma, \rho)$ permite calcular rápidamente este último grupo en casos particulares. En cierta forma $S(q)$ establece, de manera intuitiva, la existencia de grupos diedros, suministrando un recurso adicional nada despreciable en la teoría de los grupos.

EJERCICIOS

- 11.1 Demuestre que el producto (11.1) es clausurativo en $\mathbb{Z}_n^*$ si y sólo si n es un número primo.
- 11.2 Demuestre que $(\mathbb{Z}_n^*, \cdot)$ es un grupo si y sólo si n es un número primo.
- 11.3 Sean $n > 1$ un número entero, $U(\mathbb{Z}_n)$ el subconjunto de $\mathbb{Z}_n^*$ de las clases $k + n\mathbb{Z}$ tales que $1 \leq k < n$ y que $\text{mcd}(k, n) = 1$. Demuestre que $(U(\mathbb{Z}_n), \cdot)$, con $(\cdot)$ definido por (11.1), es aún un grupo, y que $U(\mathbb{Z}_n) = \mathbb{Z}_n^*$ si y sólo si n es un número primo. Verifique que $U(\mathbb{Z}_8) \approx \mathbb{Z}_2 \times \mathbb{Z}_2$ y que $U(\mathbb{Z}_9) \approx \mathbb{Z}_6$.
- 11.4 Demuestre en detalle la relación (v) para un grupo del tipo (p, q) . Haga lo mismo con la relación (vii).
- 11.5 Demuestre en detalle que (11.4), el hecho de que $a^{p-1} = a^{-1}$, y la validez de (vi) para $n \geq 0$, implican la validez de esta última relación para todo $n \in \mathbb{Z}$.

- 11.6 Demuestre que en todo grupo G del tipo (p, q) debe tenerse que $p \geq 2$ y $q \geq 3$, así que $o(G) \geq 6$.
- 11.7 Demuestre que si $(G, \cdot)$ es un grupo y $a, b \in G$ son tales que $ab = b^r a$, $r \neq 1$, entonces $(ab)^n = b^{rm_r(n)} a^n$, $(ba)^n = b^{m_r(n)} a^n$, $(ab)^n = b^{(r-1)m_r(n)} (ba)^n$, $n = 0, 1, \dots$, donde $m_r(n) = 1 + r + \dots + r^{n-1} = \frac{r^n - 1}{r - 1}$, $n \geq 0$. Extienda las anteriores igualdades al caso $n \in \mathbb{Z}$, $n < 0$. (Indicación. Defina $m_r(n) = \frac{r^n - 1}{r - 1}$ para todo $n \in \mathbb{Z}$, y observe que $m_r(-n) = -m_r(n)r^{-n}$, $n \in \mathbb{Z}$).
- 11.8 Verifique en detalle que $D_4(\sigma, \rho)$ se identifica con el grupo $S(4)$ de las simetrías de un cuadrado cuyo centro está en el punto $(0, 0)$ del plano cartesiano, en el cual el eje x y el eje y son bisectrices, y en el cual los vértices se enumeran de 1 a 4 en sentido positivo, comenzando con aquel sobre el eje y positivo. Verifique entonces que $(1, 3, 4, 2)$ no pertenece a $S(4)$ (ni, a $D_4(\sigma, \rho)$). Haga lo mismo con $D_5(\sigma, \rho)$ y el grupo $S(5)$ de las simetrías de un pentágono regular.
- 11.9 Calcule todos los subgrupos de $D_q(\sigma, \rho)$ para $q = 3, 4, 5$. ¿Es el grupo cuatro de Klein un subgrupo de $D_4(\sigma, \rho)$?
- 11.10 Demuestre que $(S_3, \cdot)$ es diedro y generado por $\sigma = (2, 3)$ y $\rho = (1, 2, 3)$. Compruebe además que es el grupo de las simetrías de un triángulo equilátero.
- 11.11 ¿Cuántos grupos no isomorfos de orden 6 existen? ¿cuántos de orden 15? ¿cuántos de orden 21? Demuestre que A_4 , el grupo alternante de 4 elementos, no tiene subgrupos de orden 6.
- 11.12 Sean $(G, \cdot)$ un grupo finito y q un divisor primo de $o(G)$. Demuestre que si H_1 y H_2 son subgrupos distintos de orden q de G entonces $H_1 \cap H_2 = \{e\}$.
- 11.13 Sean $(G, \cdot)$ un grupo finito y q un divisor primo de $o(G)$. Demuestre que si H es un q -subgrupo de G y $\mathcal{H}$ es la reunión de los conjugados de H entonces $\#(\mathcal{H}) = n(q)(q - 1) + 1$, donde $n(q)$ es el número de conjugados de H distintos entre sí. Demuestre también que si $p = o(G) - n(q)(q - 1)$ es tal que $\text{mcd}(p, q) = 1$, y si hay un subgrupo P de G de orden p , necesariamente P es normal en G y en G hay exactamente $n(q)(q - 1)$ elementos de orden q .

11.14 Demuestre que si $q \geq 3$, el subgrupo G de $GL_2(\mathbb{C})$ generado por

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ y } B = \begin{pmatrix} e^{2\pi i/q} & 0 \\ 0 & e^{-2\pi i/q} \end{pmatrix}$$

es isomorfo a $D_q(\sigma, \rho)$.

(Indicación. Verifique que $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$, $n = 0, 1, 2, \dots$)

11.15 Demuestre que el centro de $D_q(\sigma, \rho)$ se reduce a $\{e\}$ si q es impar y es el subgrupo $\{e, \rho^{q/2}\}$ si q es par.

11.16 Demuestre que los únicos subgrupos normales propios de $D_q(\sigma, \rho)$ son:

- a) El generado por ρ^i , $i > 0$, donde $i \mid q$.
- b) El generado por $\{\sigma, \rho^2\}$, cuando q es par.
- c) El generado por $\{\sigma\rho, \rho^2\}$, cuando q es par.

(Indicación. Demuestre que si H es normal y $\sigma\rho^i \in H$, $i > 0$, entonces $\rho^2 \in H$ y $\sigma \in H$ si i es par, mientras que $\rho^2 \in H$ y $\sigma\rho \in H$ si i es impar.)

11.17 Sea G el subgrupo de $GL_2(\mathbb{R})$ generado por las matrices

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \text{ y } B = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix},$$

donde $\theta = \frac{2\pi}{q}$, $q \geq 3$. Demuestre que G es isomorfo al grupo diedro $D_q(\sigma, \rho)$, mediante un isomorfismo que a A hace corresponder σ y a B , ρ . Para hacer esto, demuestre que G se identifica de manera natural con el grupo $S(q)$ de las simetrías de un polígono regular $\mathcal{P}$ de q lados (en posición inicial canónica), identificando la matriz $C \in G$ con la aplicación $f_C : \mathcal{P} \mapsto \mathcal{P}$ dada por $f_C(x, y) = (x, y)C$. Compruebe entonces que f_A es la reflexión sobre el eje y , y que f_B es la rotación positiva en un ángulo $\frac{2\pi}{q}$. Verifique además que si se definen $\langle (x, y), (u, v) \rangle = ux + vy$ y $\|(x, y)\| = \sqrt{x^2 + y^2}$ entonces $\langle f_C(x, y), f_C(u, v) \rangle = \langle (x, y), (u, v) \rangle$ y $\|f_C(x, y)\| = \|(x, y)\|$ para todo $C \in G$, y concluya que f_C preserva ángulos y distancias, así que transforma vértices adyacentes (vértices de un mismo lado del polígono) en vértices adyacentes.

Capítulo 12

Nilpotencia y resolubilidad

En este último capítulo dedicado a la teoría de los grupos, estudiaremos dos clases de éstos que son generalizaciones próximas de los grupos abelianos y que tienen por esta razón propiedades análogas: *los grupos nilpotentes y los grupos resolubles*. Los primeros son los más cercanos a los grupos abelianos. Los segundos son quizá los más importantes, dada su relación con la llamada *teoría de Galois* y con la resolubilidad de las ecuaciones polinómicas de grado superior.

Desde el punto de vista de la teoría de los grupos, ambos son importantes, por su conexión con la teoría de las series de composición, teoría ésta que muestra el papel que juegan los grupos simples en la descripción de los grupos no abelianos.

Sólo presentaremos algunas de las propiedades más elementales de estos grupos, con el fin de promover una cierta familiaridad con ellos y con las técnicas para manejarlos. En particular, sólo tocaremos superficialmente sus conexiones con la teoría de las series de composición, y omitiremos por completo (al menos por el momento) sus relaciones con la teoría de Galois. La presentación que haremos está basada en ideas de [16], [17], [22], pero algunas demostraciones son nuestras.

Comenzaremos por revisar algunas nociones y resultados considerados previamente, con el fin de dar una cierta autonomía al presente capítulo.

Si $(G, \cdot)$ es un grupo finito y p es un número primo, G es un p -grupo si $o(G) = p^n$, $n \geq 0$. Si $(G, \cdot)$ es un grupo finito y H es un subgrupo de $(G, \cdot)$,

el cual es un p -grupo, se dice que H es un p -subgrupo de G ; si además $o(H)$ es la máxima potencia de p que divide a $o(G)$, se dice que H es un p -subgrupo de Sylow de G .

Si $(G, \cdot)$ es un grupo, $a, b \in G$ y existe $x \in G$ tal que $b = xax^{-1}$, se dice que b es un *conjugado* de a . En tal caso a es también un conjugado de b , pues $a = x^{-1}bx$. El conjunto

$$CL(a) = \{xax^{-1} : x \in G\} \quad (12.1)$$

se denomina la *clase de conjugación* de a . Es claro que $a \in CL(a)$ y que $b \in CL(a)$ si y sólo si $a \in CL(b)$, lo que obviamente equivale a decir que $CL(a) = CL(b)$. Por lo tanto, $CL(a) \cap CL(b) \neq \emptyset$ si y sólo si $CL(a) = CL(b)$, así que $\{CL(a) : a \in G\}$ es una partición de G , es decir, $CL(a) \neq \emptyset$ para todo $a \in G$, $CL(a) \cap CL(b) = \emptyset$ si $CL(a) \neq CL(b)$ y

$$G = \bigcup_{a \in G} CL(a). \quad (12.2)$$

Supóngase ahora que G es finito y que C es un subconjunto de G que tiene un único elemento en común con cada clase de conjugación. Entonces

$$o(G) = \sum_{a \in C} \#(CL(a)) \quad (12.3)$$

donde $\#(CL(a))$ es el número de elementos de $CL(a)$. Como es evidente, si e es el elemento neutro de G entonces $CL(e) = \{e\}$, así que (12.3) se escribe

$$o(G) = 1 + \sum_{a \in C'} \#(CL(a)) \quad (12.4)$$

donde $C' = C \setminus \{e\}$. Por otra parte, si $a \in G$, $C(a) = \{x \in G : xax^{-1} = a\}$ es evidentemente un subgrupo de G , denominado el *centralizador* de a (capítulo 10), y

$$Z(G) = \bigcap_{a \in G} C(a) \quad (12.5)$$

es un subgrupo de G , el cual es obviamente normal y abeliano. El subgrupo $Z(G)$ de G ha aparecido varias veces en capítulos previos y juega un papel importante en la teoría de los grupos (véase el ejercicio 4.7). Se denomina el *centro* de G . Como es claro, $a \in Z(G)$ si y sólo si $C(a) = G$. Además, para todo $a \in G$, la aplicación $\varphi_a : G/C(a) \rightarrow CL(a)$ dada por $\varphi_a(xC(a)) = xax^{-1}$ está bien definida y es biyectiva (es decir, $xC(a) = yC(a)$ si y sólo si

$xax^{-1} = yay^{-1}$, lo cual es obvio, pues ambas afirmaciones equivalen a que $y^{-1}x \in C(a)$). Esto implica que si G es finito entonces $\#(CL(a)) = [G : C(a)]$. Se tiene entonces que:

Teorema 12.1. Si $(G, \cdot)$ es un p -grupo finito y $G \neq \{e\}$, entonces $Z(G) \neq \{e\}$.

Demostración. Supóngase que $o(G) = p^n$, $n \geq 1$, que $Z(G) = \{e\}$ y que C' es como en (12.4). Como $p \mid [G : C(a)]$, para todo $a \in C'$, pues $C(a) \neq G$, entonces $p \mid \sum_{a \in C'} \#(CL(a))$, así que $p \mid p^n - 1$. Esto es absurdo. Entonces, $Z(G) \neq \{e\}$. $\square$

El teorema 12.1 fue demostrado en el capítulo 10 dentro del marco general de la teoría de Sylow. Para preservar la independencia del capítulo, hemos incluido aquí la demostración anterior, algo más directa.

Si H es un subgrupo de G , definimos

$$N(H) = \{a \in G : aHa^{-1} = H\}. \quad (12.6)$$

Se dice que $N(H)$ es el *normalizador* de H en G . Es claro que $N(H)$ es un subgrupo de G y que H es un subgrupo normal de $N(H)$. Más generalmente, si H' es un subgrupo de G y $H \subseteq H'$, H es un subgrupo normal de H' si y sólo si $H' \subseteq N(H)$. Por lo tanto, H es normal en G si y sólo si $N(H) = G$.

Si G es un grupo y A es un subconjunto no vacío de G , el *subgrupo* $[A]$ de G generado por A es el conjunto de los productos finitos de elementos de $A \cup A^{-1}$, donde $A^{-1} = \{a^{-1} : a \in A\}$. Por lo tanto, si H es un subgrupo de G y $A \subseteq H$, también $[A] \subseteq H$. Si $a, b \in G$,

$$[a, b] = aba^{-1}b^{-1} \quad (12.7)$$

se denomina el *conmutador* de a y b . Claramente $[a, e] = e$, $[a, b]^{-1} = [b, a]$, y $[a, b] = e$ si y sólo si $ab = ba$. Más generalmente, $ab = [a, b]ba$, así que $[a, b]$ mide en cierta forma el grado de no conmutatividad de a y b . Si H, K son subgrupos de G , $[H, K]$ denotará el subgrupo de G generado por $\{[a, b] : a \in H, b \in K\}$. Entonces $[H, K] = [K, H]$.

Además:

Teorema 12.2. Si H y K son subgrupos de G , $H \subseteq N(K)$ si y sólo si $[H, K] \subseteq K$.

Demostración. Si $H \subseteq N(K)$ y $a \in H, b \in K$, entonces $aba^{-1} \in K$, así que $[a, b] \in K$. Recíprocamente, si $a \in H$ y cualquiera que sea $b \in K$ se tiene que $[a, b] \in K$, entonces $aba^{-1} = [a, b]b \in K$ para todo $b \in K$, así que $aKa^{-1} \subseteq K$; es decir, $a \in N(K)$. $\square$

Corolario 12.1. Un subgrupo H de G es normal si y sólo si $[G, H] \subseteq H$.

Nota 12.1. Obsérvese que un subgrupo H de G es tal que $H \subseteq Z(G)$ si y sólo si $[H, G] = \{e\}$. Más generalmente, si K es un subgrupo de G y definimos

$$C(K) = \{a \in G : [a, x] = e, x \in K\}, \quad (12.8)$$

entonces $H \subseteq C(K)$ si y sólo si $[H, K] = \{e\}$. Nótese que

$$C(K) = \bigcap_{x \in K} C(x). \quad (12.9)$$

Se dice que $C(K)$ es el *centralizador* de K en G . Claramente $C(K) \subseteq N(K)$ y $C(G) = Z(G)$.

Definición 12.1. Si $(G, \cdot)$ es un grupo, definimos inductivamente $G^{(0)} = G$, $G^{(1)} = [G, G]$, $G^{(2)} = [G, G^{(1)}]$, ..., $G^{(n+1)} = [G, G^{(n)}]$, $n = 2, 3, \dots$. El subgrupo $G^{(n)}$ se denomina la *n-ésima potencia* de G .

Es claro que $G^{(2)} \subseteq G^{(1)} \subseteq G^{(0)}$, e inductivamente se deduce que $G^{(n+1)} \subseteq G^{(n)}$.

Teorema 12.3. Para todo $n \geq 0$, $G^{(n)}$ es un subgrupo normal de G .

Demostración. Es claro que si $A \neq \emptyset$ y $xAx^{-1} \subseteq A$ para todo $x \in G$, entonces A es normal en G . Evidentemente $G^{(0)}$ y $G^{(1)}$ son normales en G (esto último resulta de observar que si $a, b \in G$ entonces $x[a, b]x^{-1} = [xax^{-1}, xbx^{-1}]$). Suponiendo entonces, por inducción, que $G^{(n)}$ es normal en G , donde $n \geq 1$, se deduce que si $a \in G$ y $b \in G^{(n)}$ entonces $x[a, b]x^{-1} = [xax^{-1}, xbx^{-1}] \in [G, G^{(n)}] = G^{(n+1)}$, así que $G^{(n+1)}$ es también normal en G . $\square$

Definición 12.2. Se dice que un grupo $(G, \cdot)$ es *nilpotente* si existe $n \geq 0$ tal que $G^{(n)} = \{e\}$.

Evidentemente todo grupo abeliano G es nilpotente, pues $G^{(1)} = \{e\}$. De hecho, G es abeliano si y sólo si $G^{(1)} = \{e\}$. Es en este sentido en el cual los grupos nilpotentes generalizan naturalmente los grupos abelianos. Como $G^{(n)}$ se conoce usualmente como la *n-ésima potencia* de G , un grupo es nilpotente si y sólo si alguna de sus potencias se anula (es decir, se reduce a $\{e\}$).

Teorema 12.4. Si un grupo $(G, \cdot)$ es nilpotente, todo subgrupo H de G también lo es.

Demostración. Como $(H, \cdot)$ es un grupo, $H^{(n)}$ está definido para todo n ($H^{(0)} = H$, $H^{(1)} = [H, H]$, $H^{(2)} = [H, H^{(1)}]$, ..., $H^{(n+1)} = [H, H^{(n)}]$, $n \geq 1$), y suponiendo que $H^{(n)} \subseteq G^{(n)}$ para un $n \geq 1$ dado, se concluye que también $H^{(n+1)} = [H, H^{(n)}] \subseteq [G, G^{(n)}] = G^{(n+1)}$. Se deduce que $H^{(n)} \subseteq G^{(n)}$ para todo $n \geq 0$, así que $H^{(n)} = \{e\}$ si $G^{(n)} = \{e\}$. $\square$

Lema 12.1. Si $(G, \cdot)$ es un grupo y H es un subgrupo normal de G ,

$$(G/H)^{(n)} = G^{(n)}H/H, \quad n \geq 0. \quad (12.10)$$

Demostración. La afirmación es evidente si $n = 0$. Suponiéndola para un $n > 0$ dado, se observa que si $bH \in (G/H)^{(n)}$ entonces $bH = cH$, $c \in G^{(n)}$, así que $[aH, bH] = [aH, cH] = [a, c]H \in G^{(n+1)}H/H$ para todo $a \in G$. Esto implica que $(G/H)^{(n+1)} = [G/H, (G/H)^{(n)}] \subseteq G^{(n+1)}H/H$. Para demostrar la afirmación recíproca, es decir, que $G^{(n+1)}H/H \subseteq (G/H)^{(n+1)}$, basta evidentemente demostrar que si $a \in G$ y $b \in G^{(n)}$ entonces $[a, b]H \in (G/H)^{(n+1)}$, lo cual es obvio, pues $[a, b]H = [aH, bH]$, y, por la hipótesis de inducción, $bH \in (G/H)^{(n)}$. Se concluye que (12.10) es válida para todo $n \geq 0$. $\square$

Teorema 12.5. Si G es nilpotente y H es un subgrupo normal de G , G/H es nilpotente.

Demostración. Si $G^{(n)} = \{e\}$ entonces $G^{(n)}H/H = \{H\}$, así que $(G/H)^{(n)} = \{H\}$. $\square$

Los dos teoremas siguientes suministran ejemplos de grupos nilpotentes no necesariamente abelianos.

Lema 12.2. Si H es un subgrupo de G , $H \subseteq Z(G)$ y G/H es nilpotente, también G es nilpotente.

Demostración. En efecto, existe $n \geq 0$ tal que $(G/H)^{(n)} = G^{(n)}H/H = \{H\}$, así que $G^{(n)} \subseteq H$. Entonces $G^{(n)} \subseteq Z(G)$, de lo cual $G^{(n+1)} = [G, G^{(n)}] = \{e\}$. $\square$

Corolario 12.2. Un grupo G es nilpotente si y sólo si $G/Z(G)$ también lo es.

Teorema 12.6. Si p es un primo, todo p -grupo finito G es nilpotente.

Demostración. Haremos inducción sobre $o(G)$. La afirmación es clara si $o(G) = 1$ u $o(G) = p$, pues G es abeliano. Supongamos entonces que $o(G) > p$ y que la afirmación es cierta para todo p -grupo G' con $o(G') < o(G)$, y demostrémosla para G . Pero esto es obvio, pues como $Z(G) \neq \{e\}$ (teorema 12.1) y $G' = G/Z(G)$ es un p -grupo con $o(G') < o(G)$, entonces G' es nilpotente. $\square$

Teorema 12.7. Un grupo finito G en el cual todos sus subgrupos de Sylow son normales es necesariamente nilpotente.

Demostración. Sean $p_1, \dots, p_m$ los divisores primos de $o(G)$ y $P_1, \dots, P_m$ subgrupos de Sylow de G , siendo P_i un p_i -grupo. Entonces $G = P_1 P_2 \dots P_m$, y el producto es directo, como se verifica inmediatamente (pues si para cada $1 \leq i \leq m$, $\hat{P}_i$ es el producto de los P_j , $j \neq i$, entonces, $\hat{P}_i$ es un subgrupo normal de G tal que $P_i \cap \hat{P}_i = \{e\}$. Véase el capítulo 6). Entonces, todo elemento $x \in G$ se escribe (de manera única) en la forma $x = a_1 a_2 \dots a_n$, donde $a_i \in P_i$. Sea $a \in Z(P_1)$. Evidentemente a conmuta con todos los a_i , $i = 1, 2, \dots, m$, así que a conmuta con x . Entonces $a \in Z(G)$; es decir, $Z(P_1) \subseteq Z(G)$. Haremos ahora inducción sobre $o(G)$. La afirmación es clara si $o(G) = 1$, o, de hecho, si G es un p -grupo. Sean $a \in Z(P_1)$, $H = [a]$, $G' = G/H$ y $\varphi : G \rightarrow G'$ el epimorfismo canónico. Si $P'_i = \varphi(P_i)$, los subgrupos P'_i son subgrupos de Sylow de G' (y, con la posible excepción de P'_1 , no triviales), los cuales son normales en G' (pues φ es un epimorfismo). Si suponemos entonces que la afirmación es cierta para todo grupo finito con $o(G') < o(G)$, ésta resulta inmediatamente para G , como consecuencia del lema 12.2. $\square$

De hecho, la propiedad de que todos sus subgrupos de Sylow son normales caracteriza completamente los grupos nilpotentes finitos, como resultará del siguiente teorema.

Lema 12.3. Si $G \neq \{e\}$ es nilpotente, entonces $Z(G) \neq \{e\}$.

Demostración. En efecto, si n es mínimo tal que $G^{(n)} = \{e\}$, entonces $G^{(n-1)} \neq \{e\}$, y como $[G : G^{(n-1)}] = \{e\}$, necesariamente $G^{(n-1)} \subseteq Z(G)$. $\square$

Teorema 12.8. En un grupo finito nilpotente, todos los subgrupos de Sylow son normales.

Demostración. Sean G un grupo finito nilpotente, y sean $p_1, \dots, p_m$ los divisores primos de $o(G)$. Para cada $i = 1, \dots, m$, sea P_i un p_i -subgrupo de Sylow de G . Sin pérdida de generalidad podemos suponer que $p_1 \mid o(Z(G))$, y sean $a \in Z(G)$ con $o(a) = p_1$, y $H = [a]$, así que H es normal en G . Haremos inducción sobre $o(G)$. La afirmación del teorema es clara si $o(G) = 1$ o, de hecho, si $o(G)$ es un primo. Supongámosla entonces válida para todo grupo G' con $o(G') < o(G)$, y sean $G' = G/H$ y $\varphi : G \rightarrow G'$ el epimorfismo canónico. Para cada $i = 1, \dots, m$, un p_i -subgrupo de Sylow de G' es $P'_i = \varphi(P_i)$ y, como G' es nilpotente (teorema 12.5) y $o(G') < o(G)$, podemos suponer que P'_i es normal en G' . Como es claro, $\varphi^{-1}(P'_i) = P_i H$, y es entonces un subgrupo normal de G . Por otra parte, como H es normal en G , $P_1 H$ es un p -grupo, así que $P_1 H = P_1$ (de lo cual $a \in P_1$), y P_1 es así normal en G . Nos queda por demostrar que P_i es normal en G para $i = 2, 3, \dots, m$. Sean entonces $b \in G$, $c \in P_i$. Como $P_i H$ es normal en G entonces $b(ca)b^{-1} = (bcb^{-1})a \in P_i H$, así que $(bcb^{-1})a = da^k$, $d \in P_i$, $0 \leq k < p_1$. Pero entonces $o(bcb^{-1}) = o(d)o(a^{k-1})$, lo cual implica que $o(a^{k-1}) = p_1^j$, $j \geq 0$. Esto sólo es posible si $j = 0$ y $k = 1$, de lo cual $bcb^{-1} = d \in P_i$. Esto demuestra el teorema. $\square$

El siguiente resultado es también característico de los grupos nilpotentes finitos. (Véase al respecto el ejercicio 12.21, el cual contiene otra demostración del anterior teorema, la cual depende, sin embargo, de resultados en el capítulo X.).

Teorema 12.9. Si $(G, \cdot)$ es nilpotente y H es un subgrupo propio de G , $H \neq N(H)$.

Demostración. En efecto, como $G^{(0)} = G$ mientras que $G^{(n)} = \{e\}$ para algún $n \geq 1$, habrá un mínimo $0 < m \leq n$ tal que $G^{(m)} \subseteq H$. Entonces, $G^{(m-1)} \not\subseteq H$. Sin embargo, puesto que $G^{(m)} = [G, G^{(m-1)}] \subseteq H$, necesariamente $G^{(m-1)} \subseteq N(H)$ (teorema 12.2). $\square$

Nota 12.2. Existen grupos nilpotentes infinitos, no abelianos, pero los ejemplos son más difíciles de conseguir. Por ejemplo, existen p -grupos

infinitos (grupos en los cuales todo elemento tiene como orden una potencia de p) cuyo centro se reduce a $\{e\}$, con lo cual, contrariamente a los p -grupos finitos, no suministran ejemplos de grupos nilpotentes.

Mostraremos sin embargo un resultado sobre los grupos finitos nilpotentes que refuerza aún más la analogía de éstos con los grupos abelianos finitos.

Teorema 12.10. Si G es un grupo nilpotente finito y m es un divisor de $o(G)$, existe un subgrupo normal H de G con $o(H) = m$.

Demostración. Haremos inducción sobre $o(G)$, siendo clara la afirmación si $o(G)$ es 1 o un primo p . Sea $m \mid o(G)$. Podemos suponer que existe un primo p tal que $p \mid o(G)$ y $p \mid m$. Sean P el correspondiente p -subgrupo de Sylow de G , $Z(P)$ el centro de P . Como es claro, $p \mid o(Z(P))$. Sean entonces $a \in Z(P)$ con $|a| = p$ y $N = \langle a \rangle$. Como $Z(P) \subseteq Z(G)$ (véase la demostración del teorema 12.7), N es un subgrupo normal de G , y si $m = p$, N es el subgrupo H buscado. Supongamos entonces que $m > p$ y que la afirmación es cierta si G' es nilpotente y $o(G') < o(G)$. El grupo $G' = G/N$ es nilpotente y $o(G') < o(G)$. Por lo tanto si $m' = m/p$, G' tiene un subgrupo normal M con $o(M) = m'$, y, en virtud de lo afirmado en la nota 6.1, existe un subgrupo normal H de G con $H/N \approx M$. Como $o(H) = m$, H es el subgrupo normal buscado. $\square$

Finalmente demostraremos el siguiente teorema, frecuentemente útil.

Teorema 12.11. Si G es un grupo finito nilpotente y p es un divisor primo de $o(G)$, todo subgrupo H de G con $[G : H] = p$ es necesariamente normal.

Demostración. Como $p = [G : H] = [G : N(H)] \cdot [N(H) : H]$ y $[N(H) : H] \neq 1$ (teorema 12.9), deberá tenerse que $[G : N(H)] = 1$, o sea, que $N(H) = G$. Entonces, H es normal en G . $\square$

Para grupos no nilpotentes, el anterior teorema sólo es válido, en general, para el mínimo primo que divide $o(G)$. Véase, al respecto, el ejemplo 12.1.

Ejemplo 12.1. Daremos ahora ejemplo de una clase importante de grupos que no son nilpotentes. Recordamos (capítulo 11) que si $p < q$, se dice que un grupo G es del tipo (p, q) si existen $a, b \in G$ con $o(a) = p$ y $o(b) = q$ tales

que todo elemento x de G se escriba de manera única en la forma $x = a^i b^j$, donde $0 \leq i < p$, $0 \leq j < q$, y que $aba^{-1} = b^r$, donde $1 < r < q$. Esto implica que G es no abeliano y que si $H = \langle a \rangle$ y $K = \langle b \rangle$ entonces K es normal en G , $G = HK$ y $H \cap K = \{e\}$. Entonces $G/K \approx H$, así que K y G/K , siendo ambos cíclicos, son nilpotentes. Por otra parte, H no es normal en G (pues G no es abeliano), así que si p es primo y $p \nmid q$, G no puede ser nilpotente (teorema 12.8), y tampoco lo será si q es primo (teorema 12.11). Este ejemplo muestra también, cuando q es primo, o cuando p lo es y $p \nmid q$, que el hecho de que haya un subgrupo normal K de G tal que K y G/K sean ambos nilpotentes no asegura que G sea nilpotente. Lo anterior garantiza también que un grupo diedro D_q con q impar, y en particular S_3 , no es nilpotente (y que tampoco lo es un grupo no abeliano de orden pq donde $p < q$ son primos, pues G resulta ser del tipo (p, q)).

Definición 12.3. Para un grupo $(G, \cdot)$, definimos inductivamente $G_{(0)} = G$, $G_{(1)} = [G, G]$, $G_{(2)} = [G_{(1)}, G_{(1)}]$, ..., $G_{(n+1)} = [G_{(n)}, G_{(n)}]$, $n \geq 2$. Se dice que $G_{(n)}$ es el n -ésimo subgrupo derivado de G .

Por definición $G_{(0)} = G^{(0)} = G$, $G_{(1)} = G^{(1)}$. Por otra parte, $G_{(2)} = [G_{(1)}, G_{(1)}] \subseteq [G, G^{(1)}]$, y si suponemos inductivamente que $G_{(n)} \subseteq G^{(n)}$ entonces $G_{(n+1)} = [G_{(n)}, G_{(n)}] \subseteq [G, G^{(n)}] = G^{(n+1)}$, así que $G_{(n)} \subseteq G^{(n)}$ para todo $n \geq 0$. En lugar de $G_{(n)}$ se escribe a veces $D^n(G)$ (con $D^0(G) = G$ y $D^1(G) = D(G) = [G, G]$). Como es evidente, si H es un subgrupo normal de G , G/H es abeliano si y sólo si $D(G) \subseteq H$, y G mismo es abeliano si y sólo si $D(G) = \{e\}$.

Definición 12.4. Se dice que un grupo $(G, \cdot)$ es resoluble si $G_{(n)} = \{e\}$ para algún $n \geq 0$.

Entonces:

Teorema 12.12. Todo grupo nilpotente G es resoluble.

Demostración. En efecto, si $G^{(n)} = \{e\}$, también $G_{(n)} = \{e\}$. $\square$

En particular, todo grupo abeliano es resoluble (esto es obvio, pues $G_{(1)} = \{e\}$). Lo mismo es cierto de todo grupo finito cuyos subgrupos de Sylow sean todos normales (y, en particular, de todo p -grupo finito).

Lema 12.4. Para todo $n \geq 0$, $G_{(n)}$ es un subgrupo normal de G y $G_{(n)}/G_{(n+1)}$ es abeliano.

Demostración. Como ya se estableció anteriormente, $G_{(0)}$ y $G_{(1)}$ son normales. Suponiendo ahora que $G_{(n)}$ es normal, para demostrar que $G_{(n+1)}$ también lo es basta demostrar que si $a, b \in G_{(n)}$ entonces $x[a, b]x^{-1} \in G_{(n+1)}$ para todo $x \in G$. Pero esto es obvio, pues $x[a, b]x^{-1} = [xax^{-1}, xbx^{-1}]$ y $xax^{-1}, xbx^{-1} \in G_{(n)}$. Como además $G_{(n+1)} = D(G_{(n)})$, $n \geq 0$, es claro que $G_{(n)}/G_{(n+1)}$ es abeliano. $\square$

Corolario 12.5. Si G es resoluble y $G \neq \{e\}$, existe un subgrupo normal H de G , $H \neq \{e\}$, el cual es abeliano.

Demostración. Si n es mínimo tal que $G_{(n)} = \{e\}$, entonces $n \geq 1$ y $G_{(n-1)} \neq \{e\}$. Como $D(G_{(n-1)}) = \{e\}$, necesariamente $H = G_{(n-1)}$ es un subgrupo normal abeliano de G . $\square$

Nota 12.3. Sin embargo, puede suceder, en el corolario 12.5, que $H \not\subseteq Z(G)$. De hecho, puede suceder que $Z(G) = \{e\}$ (véase más adelante).

Si H es un subgrupo de G es claro que $H_{(n)} \subseteq G_{(n)}$ para todo $n \geq 0$. Por lo tanto:

Teorema 12.13. Todo subgrupo de un grupo resoluble es a su vez resoluble.

Tal como se demostró el lema 12.1, se demuestra también que:

Lema 12.5. Si G es un grupo y H es un subgrupo normal de G ,

$$(G/H)_{(n)} = G_{(n)}H/H \quad (12.11)$$

para todo $n \geq 0$.

Entonces:

Teorema 12.14. Si G es resoluble y H es un subgrupo normal de G , G/H es resoluble.

Demostración. Si $G_{(n)} = \{e\}$, entonces $(G/H)_{(n)} = \{H\}$. $\square$

El siguiente teorema marca, sin embargo, una diferencia notable entre los grupos resolubles y los nilpotentes.

Teorema 12.15. Si G es un grupo para el cual existe un subgrupo normal resoluble H tal que G/H es también resoluble, entonces G es resoluble.

Demostración. Por hipótesis existen m y n tales que $H_{(m)} = \{e\}$ y que $(G/H)_{(n)} = \{H\}$. Como entonces $G_{(n)} \subseteq H$, se concluye que $G_{(m+n)} = \{e\}$. $\square$

Corolario 12.6. Para que un grupo G sea resoluble es necesario y suficiente que $G/Z(G)$ sea resoluble.

Corolario 12.7. Todo grupo G de tipo (p, q) y, en particular, todo grupo diedro, es resoluble.

Demostración. Si G está generado por (a, b) y $H = \langle b \rangle$, H es resoluble y normal en G . Como además $G/H \approx \langle a \rangle$ es cíclico y, por lo tanto, abeliano, entonces G/H es resoluble. Se concluye que G es resoluble. $\square$

Nota 12.4. Como hemos visto, si G es del tipo (p, q) y q es primo, G no es nilpotente. Nótese además que si q es impar y G es diedro del tipo $(2, q)$, entonces $Z(G) = \{e\}$ (ejercicio 11.15).

Nota 12.5. Se deduce también que todo grupo no abeliano de orden pq , donde $p < q$ son primos, es resoluble (pues, capítulo 11, G es del tipo (p, q)).

Observamos ahora que si $n \geq 5$, S_n no es resoluble. En efecto, si lo fuera, también lo sería A_n . Pero:

Teorema 12.16. Si G es un grupo simple no conmutativo, G no es resoluble.

Demostración. En caso contrario G tendría un subgrupo normal abeliano H , $H \neq \{e\}$, lo cual es absurdo, pues sería $H \neq G$. $\square$

Nota 12.6. Contrario a lo que sucede con los grupos finitos nilpotentes, es falso en general que si G es un grupo finito resoluble y m es un divisor de $o(G)$, exista un subgrupo H de G con $o(H) = m$. Por ejemplo, A_4 es resoluble (si V es el grupo cuatro de Klein (capítulo 8), dado que V es normal en A_4 , que $o(V) = 4$, y que $o(A_4/V) = 3$, tanto V como A_4/V son abelianos, de lo cual, resolubles). Sin embargo, A_4 no tiene subgrupos de orden 6 (en efecto, si H fuera un tal subgrupo, existiría un 3-ciclo $\sigma \in A_4$, $\sigma \notin H$, así que si $K = \langle \sigma \rangle$ entonces $K \cap H = \{e\}$, de lo cual, siendo H normal en A_4 , HK sería un subgrupo de A_4 de orden 18. Esto es absurdo, pues $o(A_4) = 12$). Sin embargo si m es un divisor de $o(G)$ tal que $o(G) = mn$ con $\text{mcd}(m, n) = 1$, un famoso teorema de P. Hall (véanse [13], [17], [22])

asegura la existencia de subgrupos de orden m de G (y por lo tanto, también de orden n). Más aún, dos de tales subgrupos son siempre conjugados, y si $k \mid m$ y H es un subgrupo de orden k de G , éste queda contenido en uno de tales conjugados. En particular, si $o(G) = mp^n$ donde $n \geq 1$, p es primo y $p \nmid m$, existen subgrupos de orden m de G (denominados p -complementos), los cuales son todos conjugados. El teorema de Hall es uno de los primeros resultados sobre la existencia de p -complementos. Resultados muy profundos en esta dirección fueron posteriormente obtenidos por J. G. Thompson, a comienzos de la década de 1960 (véase [25]).

Examinaremos ahora, brevemente, la conexión entre los grupos nilpotentes y resolubles y las series asociadas a un grupo. Para mucho más detalle, el lector puede consultar [2], [17], [22].

Definición 12.5. Una *serie* para un grupo $(G, \cdot)$ es una sucesión (H_n) , $n \geq 0$, de subgrupos de G con $G = H_0$ y $H_{n+1} \subseteq H_n$ para todo $n \geq 0$. Si para todo $n \geq 0$, H_{n+1} es un subgrupo normal de H_n , se dice que tal serie es *subnormal*. Si H_n es normal en G para todo $n \geq 0$, se dice que (H_n) es *normal*.

Si (H_n) es subnormal (o normal), los grupos H_n/H_{n+1} se denominan los *grupos factores* de la serie (H_n/H_{n+1} es el $(n+1)$ -ésimo factor). Como es claro, toda serie normal es subnormal (lo recíproco es falso, en general).

Si (H_n) es subnormal y los grupos H_n/H_{n+1} son simples, se dice que (H_n) es una *serie composicional*. Si los H_n/H_{n+1} son abelianos, se dice que (H_n) es una *serie resolvente*.

Las series $(G^{(n)})$ y $(G_{(n)})$ son subnormales (de hecho, normales). Ambas son series resolventes del grupo G .

Una serie (H_n) tal que $H_n = \{e\}$ para algún n (con lo cual $H_m = \{e\}$ para todo $m \geq n$) se denomina una *serie terminal*. Si $H_n = \{e\}$, es costumbre presentar (H_n) en la forma

$$G = H_0 \supseteq H_1 \supseteq \dots \supseteq H_{n-1} \supseteq H_n = \{e\},$$

olvidando los términos H_m , $m > n$. Una serie composicional terminal se denomina una *serie de composición* y el número de sus grupos factores no triviales es su *longitud*. Una serie resolvente terminal se denomina una *resolución*. No es difícil demostrar que *toda grupo finito admite una serie de composición*. Un poco más difícil es establecer que *cualquier otra*

tiene la misma longitud y esencialmente los mismos grupos factores (grupos factores correspondientes, una vez desechados los triviales, son iguales salvo isomorfismo). Estos resultados constituyen el denominado *teorema de Jordan-Hölder*, uno de los más importantes de la teoría de los grupos. Un grupo finito arbitrario determina entonces unívocamente, mediante una serie de composición, una cadena de grupos simples: *sus grupos simples componentes*. Es en este sentido en el cual los grupos simples constituyen los pilares sobre los cuales se construyen todos los grupos finitos (véase, al respecto, [12] y [24]), y explica por qué una clasificación completa de ellos conduce al conocimiento de éstos.

Un grupo resoluble admite una resolución. Recíprocamente:

Teorema 12.17. Si un grupo G admite una resolución

$$G = H_0 \supseteq H_1 \supseteq \dots \supseteq H_n = \{e\}$$

entonces G es resoluble.

Demostración. Como $G/H_1 = H_0/H_1$ es abeliano, se deduce que $G_{(1)} \subseteq H_1$. Esto implica de manera análoga que $G_{(i)} \subseteq H_i$ para todo i , así que $G_{(n)} = \{e\}$. $\square$

Nota 12.7. Una resolución no es necesariamente una serie de composición. Sin embargo, es posible demostrar (fácilmente, ejercicio 12.22) que todo grupo resoluble finito, no trivial, admite una serie de composición cuyos grupos factores son todos grupos cíclicos de orden primo. Tal serie de composición es evidentemente una resolución.

Nota 12.8. Como es claro, puede suceder que, para un grupo dado G , la serie $(G_{(n)})$ sea una resolución sin que $(G^{(n)})$ lo sea.

EJERCICIOS

- 12.1 Verifique que S_3 no tiene subgrupos normales de orden 2 y demuestre así, de otra manera, que S_3 , siendo resoluble, no es nilpotente.

12.2 Verifique en detalle que $(G^{(n)})$ es una serie resolvente del grupo G . Es decir, establezca que $D(G^{(n)}) \subseteq G^{(n+1)}$. Concluya que G es nilpotente si y sólo si $(G^{(n)})$ es una resolución de G .

12.3 Sea $(G, \cdot)$ un grupo.

- Demuestre que si existe un subgrupo H de G , $H \neq \{e\}$, tal que $H = D(H)$, G no es resoluble.
- Demuestre que si $(G, \cdot)$ es finito y no resoluble, existe un subgrupo normal H de G , $H \neq \{e\}$, tal que $H = D(H)$.

12.4 Demuestre que un grupo $G \neq \{e\}$ es nilpotente si y sólo si existe $n \geq 0$ tal que $G^{(n)} \subseteq Z(G)$ y $G^{(n)} \neq \{e\}$.

12.5 Demuestre que si G es del tipo (p, q) , donde $p < q$ son primos, entonces $Z(G) = \{e\}$, y concluya así, de otra manera, que G no es nilpotente.

12.6 Demuestre que si G es un grupo diedro generado por a, b con $o(a) = 2$ y $o(b) = q$, entonces $Z(G) \neq \{e\}$ si y sólo si q es par, y que en tal caso $Z(G) = \{e, b^{q/2}\}$. Concluya que si q es impar entonces G no es nilpotente. Demuestre además que si q es par entonces $G/Z(G) \approx G'$ donde G' es el subgrupo de G generado por a y b^2 , y que si $q > 4$ entonces G' es diedro. Concluya de esto que G es nilpotente si y sólo si $q = 2^n$ para algún $n \geq 2$.

12.7 Sean G un grupo, H un subgrupo normal de G , M y N subgrupos de G . Demuestre que

$$[MH, NH] = [M, N]H. \quad (12.12)$$

(Indicación. Recuerde que $MH = HM$, $NH = HN$.)

12.8 Sean G un grupo, H un subgrupo normal de G , M y N subgrupos de G tales que $H \subseteq M$ y $H \subseteq N$. Demuestre que

$$[M/H, N/H] = [M, N]H/H \quad (12.13)$$

y que $M/H \subseteq C(N/H)$ si y sólo si $[M : N] \subseteq H$. Concluya que $M/H \subseteq Z(G/H)$ si y sólo si $[G, M] \subseteq H$.

12.9 Use la relación (12.13) del ejercicio anterior y la (12.12) del ejercicio 12.7 para demostrar inductivamente las relaciones (12.10) y (12.11).

*12.10 Sean G un grupo nilpotente, H un subgrupo normal propio de G . Demuestre que existe $a \in G$ tal que $a \notin H$ y que $[a, x] \in H$ para todo $x \in G$, y que si n es mínimo tal que $G^{(n)} = \{e\}$ entonces $G^{(k)} \cap H \neq \{e\}$ para todo $0 \leq k \leq n-1$. Concluya que $H \cap Z(G) \neq \{e\}$. (Indicación: Use el hecho de que si $H \neq G$ entonces $Z(G/H) \neq \{H\}$).

*12.11 Sean p un primo, G un p -grupo no trivial, H un subgrupo normal de G , $H \neq \{e\}$. Demuestre que $H \cap Z(G) \neq \{e\}$. Demuestre que la misma afirmación es válida en todo grupo finito G cuyos subgrupos de Sylow sean todos normales.

12.12 Demuestre que un grupo simple es resoluble si y sólo si es cíclico de orden primo.

12.13 Sean G y G' grupos, $f : G \rightarrow G'$ un homomorfismo. Demuestre:

- Si $A \subseteq G$, $f([A]) = [f(A)]$, y si f es un epimorfismo y $[A]$ es normal en G entonces $[f(A)]$ es normal en G' . ($[A]$ es el subgrupo generado por A .)
- Si $a, b \in G$, $f([a, b]) = [f(a), f(b)]$.
- Si M, N son subgrupos de G , $f([M, N]) = [f(M), f(N)]$.
- $f(G_{(n)}) = f(G)_{(n)}$ para todo n .
- $f(G^{(n)}) \subseteq f(G)^{(n)}$ para todo n , y si f es un epimorfismo, $f(G^{(n)}) = f(G)^{(n)}$ para todo n .

12.14 Sean G y G' grupos, $f : G \rightarrow G'$ un homomorfismo. Demuestre:

- Si G es resoluble, $f(G)$ también lo es. Si f es un monomorfismo y G' es resoluble, también G es resoluble.
- Si G' es nilpotente y f es un monomorfismo, G es nilpotente. Si f es un epimorfismo y G es nilpotente, G' es nilpotente.
- Si $G \approx G'$, G es nilpotente (respectivamente, resoluble) si y sólo si G' es nilpotente (respectivamente, resoluble).

12.15 Sean G y G' grupos, $f : G \rightarrow G'$ un homomorfismo. Demuestre que $f(Z(G)) \subseteq Z(f(G))$ y que si f es un monomorfismo entonces $f(Z(G)) = Z(f(G))$. Concluya que si f es un epimorfismo, $f(Z(G)) \subseteq Z(G')$, y que si f es un isomorfismo, $f(Z(G)) = Z(G')$.

- 12.16 Demuestre que si H es un subgrupo nilpotente de G y $K \subseteq Z(G)$, entonces $H \cap K$ y HK son subgrupos nilpotentes de G .
- 12.17 Demuestre que si H y K son subgrupos resolubles de G , K normal en G , $H \cap K$ y HK son subgrupos resolubles de G .
- 12.18 Sean G_1 y G_2 grupos, $G_1 \times G_2$ el grupo producto. Verifique que si $(a, b), (c, d) \in G_1 \times G_2$ entonces $[(a, b), (c, d)] = ([a, c], [b, d])$, concluya que $(G_1 \times G_2)^{(n)} = G_1^{(n)} \times G_2^{(n)}$, y demuestre que $G_1 \times G_2$ es nilpotente si y sólo si G_1 y G_2 lo son. Demuestre también que $D^n(G_1 \times G_2) = D^n(G_1) \times D^n(G_2)$ y que $G_1 \times G_2$ es resoluble si y sólo si G_1 y G_2 lo son. ¿Se pueden extender los anteriores resultados al producto de un número finito $G_1 \times G_2 \times \dots \times G_n$ de grupos?
- 12.19 Demuestre que si H y K son subgrupos normales de G tales que $H \cap K = \{e\}$ y que H y K son nilpotentes (resolubles), entonces HK es un subgrupo nilpotente (resoluble) de G .
- 12.20 Sea G un grupo finito cuyo centro $Z(G)$ es diferente de $\{e\}$. Sean p un divisor primo de $o(Z(G))$, $a \in Z(G)$ con $o(a) = p$, $H = [a]$, P un p -subgrupo de Sylow de G . Demuestre que $a \in P$. (Indicación. Sean $G' = G/H$, $\varphi: G \rightarrow G'$ el epimorfismo canónico. Verifique que si $P' = \varphi(P)$ entonces $\varphi^{-1}(P') = PH$ y que $P' \approx PH/H \approx P/H \cap P$. Concluya que no es posible que $P' \approx P$.)
- *12.21 Use el lema 10.1 y el corolario 10.4 (capítulo 10) para demostrar que si G es un grupo finito y P es un subgrupo de Sylow de G entonces $N(N(P)) = N(P)$. Concluya entonces que un grupo finito G es nilpotente si y sólo si $N(H) \neq H$ cualquiera que sea el subgrupo propio H de G .
- 12.22 Sean G un grupo finito, H un subgrupo normal de G tal que G/H es abeliano. Demuestre que existen subgrupos $G = H_0 \supseteq H_1 \supseteq \dots \supseteq H_n = H$ de G tales que H_i es normal en H_{i-1} , $i = 1, 2, \dots, n$, y que H_{i-1}/H_i es cíclico. Concluya que un grupo finito resoluble admite una serie de composición cuyos subgrupos factores son todos cíclicos (y, por tanto, aquellos grupos factores no triviales son de orden primo). De hecho, demuestre que si G es no trivial, los grupos factores de tal serie pueden tomarse todos cíclicos de orden primo.
- 12.23 Demuestre directamente (sin recurrir a la noción de nilpotencia) que todo p -grupo finito (p un primo) es resoluble y que todo grupo finito cuyos subgrupos de Sylow sean todos normales también lo es.

EJERCICIOS SUPLEMENTARIOS

En los siguientes ejercicios se introducen conceptos y se dan resultados adicionales que pueden ser de interés e importancia en la teoría de los grupos. Sus soluciones pueden necesitar recursos de cualquiera de los capítulos 2 a 12 y constituyen entonces un buen repaso de todo el material y un buen entrenamiento para estudios más avanzados en la teoría de los grupos.

- S.1 Sea $(G, \cdot)$ un grupo. Un homomorfismo f de G en sí mismo se denomina un *endomorfismo* de G . Si f es además biyectivo, es decir, un isomorfismo, se dice que f es un *automorfismo* de G .
- Sea G un grupo finito. Demuestre que todo endomorfismo inyectivo de G es automáticamente un automorfismo y que lo mismo es cierto de todo endomorfismo sobreyectivo.
 - Demuestre que si G es un grupo, el conjunto $\text{Aut}(G)$ de todos los automorfismos de G es, con la ley ($\circ$) de composición de funciones, un grupo, en el cual el elemento neutro es la aplicación idéntica de G y en el cual el inverso de f es su aplicación inversa. Demuestre que si G es finito y $o(G) = n$, $\text{Aut}(G)$ es finito y $o(\text{Aut}(G)) \mid n!$.
 - Sean G un grupo, $a \in G$. Demuestre que la aplicación $\delta_a: G \rightarrow G$ dada por $\delta_a(x) = axa^{-1}$ es un automorfismo de G y que $\delta: G \rightarrow \text{Aut}(G)$ dada por $\delta(a) = \delta_a$ es un homomorfismo de G en $\text{Aut}(G)$ cuyo núcleo es el centro $Z(G)$ de G .
 - Sean G y δ como en (c). Demuestre que $\text{Aut}_o(G) := \delta(G)$ es un subgrupo normal de $\text{Aut}(G)$, denominado el *grupo de los automorfismos interiores* de G . Demuestre, más precisamente, que $f \circ \delta_a \circ f^{-1} = \delta_{f(a)}$ para todo $a \in G$ y todo $f \in \text{Aut}(G)$.
 - Sean G y δ como en (c) y (d). Demuestre que $G/Z(G) \approx \text{Aut}_o(G)$ mediante el isomorfismo $\bar{\delta}$ obtenido de δ por paso al cociente (teorema 6.2). Concluya que $\text{Aut}_o(G)$ se reduce a la identidad si y sólo si G es abeliano.

- S.2 Demuestre que si G es un grupo cíclico finito y $n \in \mathbb{Z}$, $f(x) = x^n$ es un endomorfismo de G (ejercicio S.1), el cual es un automorfismo (ejercicio S.1) si y sólo si $\text{mcd}(n, o(G)) = 1$. Más aún, demuestre que $f(x) = x^r$, donde r es el resto de dividir n por $o(G)$, y que todo automorfismo de G es de esta forma con $\text{mcd}(r, o(G)) = 1$.

S.3 Si $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, la aplicación $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}$ definida por

$$\varphi(n) = \#\{k \in \mathbb{N} : 1 \leq k \leq n, \text{mcd}(k, n) = 1\}, \quad n \geq 1, \quad (\text{S.1})$$

se denomina la *función de Euler*. Demuestre que si G es un grupo cíclico de orden n entonces $o(\text{Aut}(G)) = \varphi(n)$.

S.4 Sea G un grupo cíclico infinito. Demuestre que todo endomorfismo (ejercicio S.1) de G es inyectivo y que los únicos automorfismos de G (ejercicio S.1) son la identidad y $f(x) = x^{-1}$.

S.5 Sean $m \in \mathbb{N}$, $m > 1$, y $\mathbb{Z}_m$ el conjunto $\mathbb{Z}/m\mathbb{Z}$ de las clases residuales módulo m . Escribese $\bar{a} = a + m\mathbb{Z}$. Demuestre que $\bar{a} \cdot \bar{b} = \overline{ab + m\mathbb{Z}}$ define una ley de composición interna sobre $\mathbb{Z}_m$, denominada la *multiplicación módulo m* , y que $\bar{a} \cdot \bar{b} \neq 0$ si y sólo si $m \nmid ab$. Obsérvese que $\bar{a} = \overline{r(a, m)}$, donde $r(a, m)$ es el resto de dividir a por m , y concluya que $U_m(\mathbb{Z}) = \{\bar{a} \in \mathbb{Z}_m : 1 \leq a < m, \text{mcd}(a, m) = 1\}$ dotado de la multiplicación $(\cdot)$ módulo m es un grupo en el cual el elemento neutro es $\bar{1}$. Si $\bar{a} \in U_m(\mathbb{Z})$, ¿cómo se determina el inverso $(\bar{a})^{-1}$ de $\bar{a}$? Demuestre que m es primo si y sólo si $U_m(\mathbb{Z}) = \mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{\bar{0}\}$.

S.6 Sea $(U_m(\mathbb{Z}), \cdot)$ como en el ejercicio S.5. Demuestre que $o(U_m(\mathbb{Z})) = \varphi(m)$, donde φ es la función de Euler (ejercicio S.3), y concluya que si $\text{mcd}(a, m) = 1$ entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$ (es decir, $m \mid (a^{\varphi(m)} - 1)$). Verifique que si m es primo, $o(U_m(\mathbb{Z})) = m - 1$ y $a^{m-1} \equiv 1 \pmod{m}$ para todo $a \in \mathbb{Z}$ tal que $m \nmid a$.

S.7 Sean $m \in \mathbb{N}$, $m > 1$, y sea $(T_m, \cdot)$ el grupo multiplicativo de las raíces m -ésimas de la unidad:

$$T_m = \{w_m^k : k = 0, 1, 2, \dots, m-1\}, \quad w_m = e^{2\pi i/m}.$$

Sea U_m el conjunto de las raíces primitivas m -ésimas de la unidad ($U_m = \{w_m^k : 1 \leq k < m, |w_m^k| = m\}$). Demuestre que $w_m^k \in U_m$ si y sólo si $\text{mcd}(k, m) = 1$, y concluya que $\#(U_m) = \varphi(m)$, donde φ es la función de Euler (ejercicio 5.3). ¿Es U_m un subgrupo de T_m ?

S.8 Sean $G = \{a_1, \dots, a_n\}$ un grupo abeliano finito y $x = a_1 a_2 \cdots a_n$. Demuestre que $x^2 = e$ y que si n es impar entonces $x = e$.

S.9 Sean p un número primo y $x \in \mathbb{Z}$ tal que $x^2 \equiv 1 \pmod{p}$ (es decir, $p \mid (x^2 - 1)$). Demuestre que $x \equiv 1 \pmod{p}$ o $x \equiv -1 \pmod{p}$.

S.10 Sea p un número primo impar y considere el grupo $U_p(\mathbb{Z})$ (ejercicio S.5). Verifique que $o(U_p(\mathbb{Z})) = p - 1$ y que si $x = \bar{1} \cdot \bar{2} \cdots \overline{(p-1)}$ entonces $x^2 = \bar{1}$. Demuestre que entonces $x = \overline{-1} = \overline{(p-1)!}$, y concluya que $(p-1)! \equiv -1 \pmod{p}$ y que $(p-2)! \equiv 1 \pmod{p}$. ¿Valen estas relaciones si $p = 2$? (La relación $(p-1)! \equiv -1 \pmod{p}$, válida para todo primo p , se conoce como el *teorema de Wilson*).

S.11 Demuestre que todo grupo finito G de orden > 2 tiene al menos un automorfismo (ejercicio S.1) distinto del automorfismo idéntico.

S.12 Demuestre que un grupo abeliano es simple (capítulo 8) si y sólo si es cíclico de orden primo.

S.13 Demuestre que si G es un grupo simple no conmutativo entonces $G \approx \text{Aut}_o(G)$ (ejercicio S.1).

S.14 Sean G un grupo finito y $\varphi \in \text{Aut}(G)$ tal que $\varphi \circ \varphi$ es la identidad de G . Supóngase además que $\varphi(x) = x$ implica que $x = e$. Demuestre que G es abeliano y que $\varphi(a) = a^{-1}$ para todo $a \in G$. (Indicación. Demuestre primero que la aplicación $\psi : G \rightarrow G$ dada por $\psi(x) = x^{-1}\varphi(x)$ es inyectiva, y concluya que para todo $a \in G$ existe $x \in G$ tal que $a = \psi(x)$).

S.15 Sean G un grupo y p un número primo. Demuestre que un subgrupo finito H de G es un p -subgrupo de G (capítulo 10) si y sólo si todo elemento de H tiene orden p^k para algún $k \geq 0$.

S.16 Sean G y G' grupos, H un subgrupo de G , p un número primo, f un homomorfismo de G en G' . Demuestre que si H es un p -subgrupo de G (capítulo 10), también $f(H)$ es un p -subgrupo de G' .

S.17 Si G es un grupo finito y H es un p -subgrupo de Sylow de G (capítulo 10), demuestre que H es el único p -subgrupo de Sylow de $N(H)$, el normalizador de H (capítulo 9).

S.18 Si H es un p -subgrupo de Sylow del grupo finito G (capítulo 10) y $a \in G$ es un elemento de G de orden p^k , $k \geq 0$, demuestre que $aHa^{-1} = H$ si y sólo si $a \in H$.

S.19 Si H es un p -subgrupo de Sylow de G (capítulo 10) y $a, b \in Z(H)$ son tales que $b = xax^{-1}$ para algún $x \in G$, existe también $y \in N(H)$ tal que $b = yay^{-1}$. (Para la definición de $N(H)$, véase el capítulo 9.)

- S.20 Sean G un grupo finito, p un primo, H un p -subgrupo de Sylow de G (capítulo 10), el cual es normal en G . Demuestre que G/H es un grupo, ninguno de cuyos elementos tiene orden p^k , $k \geq 1$.
- S.21 Sean G y G' grupos finitos, p un número primo, P' un p -subgrupo de G' (capítulo 10), f un monomorfismo de G en G' . Demuestre que $f^{-1}(P')$ es un p -subgrupo de G y que si P' es un p -subgrupo de Sylow de G' (capítulo 10), el cual es normal en G' , también $f^{-1}(P')$ es un p -subgrupo de Sylow de G , normal en G . ¿Qué se puede decir si P' no es normal en G' ?
- S.22 Sean G un grupo finito, p un primo, P un p -subgrupo de Sylow de G (capítulo 10) tal que $P \subseteq Z(G)$. Demuestre que existe un subgrupo normal H de G tal que $H \cap P = \{e\}$ y que $G = HP$.
- S.23 Sean G un grupo finito, H un subgrupo normal de G , p un primo, P un p -subgrupo de Sylow de G (capítulo 10). Demuestre que $H \cap P$ es un p -subgrupo de Sylow de H y que HP/H es un p -subgrupo de Sylow de G/H .
- S.24 ¿Es cíclico un grupo infinito en el cual $\{x : x^n = e\}$ tiene a lo sumo n elementos para todo $n \in \mathbb{N}$, $n \geq 1$. (Indicación. Considere $(\mathbb{Z} \times \mathbb{Z}, +)$, capítulo 7.)
- S.25 Demuestre que si H es un subgrupo normal de G y $C(H) = \bigcap_{a \in H} C(a)$, donde $C(a)$ es el centralizador de a en G (capítulo 9), entonces $C(H)$ es un subgrupo normal de G .
- S.26 Considere el grupo simétrico S_n , $n \geq 1$ (capítulo 8), y sea σ un p -ciclo, $1 \leq p \leq n$. ¿Cuántos conjugados tiene σ en S_n ? ¿Cuál es el orden del centralizador $C(\sigma)$ de σ en S_n . (Respuestas. $n!/p(n-p)!$, $p(n-p)!$). Describa explícitamente $CL(\sigma)$ y $C(\sigma)$ cuando $p = 1$ y cuando $p = n$. (Respuestas. $\{e\}$, S_n si $p = 1$; $\{(1, i_2, \dots, i_n) : 1 < i_k \leq n, k = 2, \dots, n, i_k \neq i_h \text{ si } k \neq h\}$, $\{\sigma^k : 1 \leq k \leq n\}$ si $p = n$).
- S.27 ¿Cuántos conjugados tiene la permutación $\sigma = (1, 2)(3, 4)$ en S_4 ? ¿Cuál es el orden de $C(\sigma)$? ¿Qué son $CL(\sigma)$ y $C(\sigma)$? (Respuestas. 3, 8, $CL(\sigma) = \{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$, $C(\sigma) = \{e, (1, 2)(3, 4), (1, 2), (3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 3, 2, 4), (1, 4, 2, 3)\}$

- S.28 Sea G un grupo. Se dice que un subgrupo M de G es *maximal* si no existe ningún subgrupo propio N de G tal que $M \subseteq N \subseteq G$ y $N \neq M$. Se dice que M es *normal - maximal* si M es normal y no existe ningún subgrupo normal propio N de G tal que $M \subseteq N \subseteq G$ y $N \neq M$.
- Demuestre que si G es finito, dado un subgrupo H de G , $H \neq G$, siempre existe un subgrupo maximal M de G , $M \neq G$, tal que $H \subseteq M$.
 - Demuestre que si H en (a) es normal, M puede tomarse normal - maximal.
 - Demuestre que en todo grupo finito no trivial existen subgrupos maximales y subgrupos normales - maximales distintos de todo el grupo.
 - Demuestre que si M es un subgrupo normal de G , M es normal maximal si y sólo si G/M es un grupo simple.
 - Demuestre que si G es un grupo simple no trivial $G \supseteq \{e\}$ es una serie de composición de G , y la única posible con factores no triviales.
 - Demuestre que si G es un grupo finito, G admite una serie de composición $G = M_0 \supseteq M_1 \supseteq \dots \supseteq M_n = \{e\}$.
- S.29 Sean G un grupo, H un subgrupo de G . Se dice que H es un *subgrupo invariante* o un *subgrupo característico* de G si $f(H) = H$ cualquiera que sea el automorfismo f de G .
- Demuestre que si H es un subgrupo invariante de G , G es un subgrupo normal de G . (Lo recíproco es falso, pero no es fácil de verificar.)
 - Demuestre que si G es finito, p es primo y H es un p -subgrupo de Sylow de G (capítulo 10), H es invariante si y sólo si H es normal en G .
 - Demuestre que H es característico si y sólo si $f(H) \subseteq H$ o $f(H) \supseteq H$ para todo automorfismo f de G .
 - Demuestre que si M y N son subgrupos característicos de G , $M \cap N$ y MN son ambos subgrupos característicos de G .
 - Sean G un grupo, M un subgrupo característico de G , N un subgrupo característico de M . Demuestre que N es un subgrupo característico de G . Demuestre además que si sólo se supone que

M es normal en G , se puede aún concluir que N es normal en G .
¿Es cierto que si M es normal en G y N es normal en M entonces N es normal en G ? (Véase el ejercicio 8.18.)

f) Demuestre que $Z(G)$ es un subgrupo característico de G .

S.30 Sean G un grupo, $a \in G$, H un subgrupo de G , $C(a)$ el centralizador de a , $N(H)$ el normalizador de H (capítulo 9). Demuestre que:

a) $C(xax^{-1}) = xC(a)x^{-1}$ para todo $x \in G$.

b) $N(xHx^{-1}) = xN(H)x^{-1}$ para todo $x \in G$.

c) $C(\varphi(a)) = \varphi C(a)$ para todo $\varphi \in \text{Aut}(G)$.

d) $N(\varphi(H)) = \varphi N(H)$ para todo $\varphi \in \text{Aut}(G)$.

e) Si H es característico, $N(H) = G$.

S.31 Sean G un grupo, $Z_0(G) = \{e\}$, $Z_1(G) = Z(G)$ su centro. Sea $\varphi_1 : G \rightarrow G/Z_1(G)$ el epimorfismo canónico. Definimos $Z_2(G) = \varphi_1^{-1}(Z(G/Z_1(G)))$, e inductivamente $Z_{n+1}(G) = \varphi_n^{-1}(Z(G/Z_n(G)))$, $n \geq 1$. Se obtiene así una sucesión $(Z_n(G))$, $n \geq 0$, de subgrupos normales de G tales que $Z_n(G) \subseteq Z_{n+1}(G)$, $n \geq 0$. Demuestre que

$$Z_{n+1}(G)/Z_n(G) \approx Z(G/Z_n(G)), \quad n \geq 0 \quad (\text{S.2})$$

(La sucesión ascendente $(Z_n(G))$ se denomina la *serie central* de G .)

S.32 Demuestre que si G y G' son grupos y $f : G \rightarrow G'$ es un isomorfismo, entonces f induce un isomorfismo $f_1 : Z(G) \rightarrow Z(G')$. Demuestre a su vez que f_1 induce un isomorfismo $f_1 : G/Z(G) \rightarrow G'/Z(G')$, e isomorfismos $f_2 : Z(G/Z(G)) \rightarrow Z(G'/Z(G'))$ y $f_2 : Z_2(G) \rightarrow Z_2(G')$. Continuando de esta manera, establezca la existencia de isomorfismos $f_n : Z(G/Z_{n-1}(G)) \rightarrow Z(G'/Z_{n-1}(G'))$ y $f_n : Z_n(G) \rightarrow Z_n(G')$ para todo $n \geq 1$. Es decir, si $G \approx G'$, entonces $Z_n(G) \approx Z_n(G')$ y $Z(G/Z_n(G)) \approx Z(G/Z_n(G'))$ para todo $n \geq 0$.

S.33 Demuestre inductivamente que si G es un grupo entonces

$$Z_{n+1}(G)/Z(G) \approx Z_n(G/Z(G)), \quad n \geq 0, \quad (\text{S.3})$$

y concluya (con $Z = Z(G)$) que

$$Z_{n+1}(G)/Z_n(G) \approx Z_n(G/Z)/Z_{n-1}(G/Z), \quad n \geq 1. \quad (\text{S.4})$$

(Use los resultados de los ejercicios S.31 y S.32.)

S.34 Use los resultados del ejercicio S.33 para demostrar que un grupo finito G es nilpotente si y sólo si existe $m \geq 1$ tal que $Z_n(G) = G$ para todo $n \geq m$ (haga inducción sobre $o(G)$). Concluya que $(Z_n(G))$ es una resolución de G si y sólo si G es nilpotente.

Bibliografía

- [1] P. B. Acosta, *Grupos diedros y del tipo (p, q)* , Trabajo de Grado, Universidad Sergio Arboleda, Bogotá, 2002.
- [2] V. S. Albis. *Curso de álgebra*, Departamento de Matemáticas, Universidad Nacional de Colombia, Bogotá, 2002.
- [3] C. B. Allendoerfer and C. O. Oakley, *Principles of Mathematics*, McGraw-Hill, New York, 1965.
- [4] C. B. Allendoerfer and C. O. Oakley, *Fundamentals of Mathematics*, McGraw-Hill, New York, 1965.
- [5] N. Bourbaki, Livre I, *Théorie des ensembles*, Hermann, Paris, 1963.
- [6] J. F. Caycedo, *Teoría de los grupos*, Departamento de Matemáticas, Universidad Nacional de Colombia, Bogotá, 1987.
- [7] J. A. Charris, R. de Castro y J. Varela, *Fundamentos del análisis complejo de una variable*, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Colección Julio Carrizosa Valenzuela N° 8, Bogotá, 2000.
- [8] P. Dubreil et M. L. Dubreil-Jacotin, *Leçons d'algèbre moderne*, Dunod, Paris, 1961.
- [9] J. Dugundji, *Topology*, Allyn and Bacon, Boston, 1966.
- [10] J. B. Fraleigh, *A First Course in Abstract Algebra*, 2nd Edition, Addison Wesley, Reading, Mass, 1977.
- [11] R. Godement, *Cours d'algèbre*, Hermann, Paris, 1963.
- [12] D. Gorenstein, *Finite Groups*, Harper and Row, New York, 1968.
- [13] M. Hall, *The Theory of Groups*, Mcmillan, New York, 1959.

- [14] P. Halmos, *Naive Set Theory*, Van Nostrand, Princeton, 1960.
- [15] I. N. Herstein, *Algebra abstracta*, Grupo Editorial Iberoamérica, México, 1988.
- [16] I. N. Herstein, *Topics in Algebra*, 2nd Edition, Wiley, New York, 1975.
- [17] T. W. Hungerford, *Algebra*, Graduate Text in Mathematics 73, Springer, New York, 1974.
- [18] B. W. Jones, *An Introduction to Modern Algebra*, Macmillan, New York, 1974.
- [19] J. L. Kelley, *Topología general*, EUDEBA, Buenos Aires, 1962.
- [20] S. Lang, *Algebra*, Addison-Wesley, Reading, 1975.
- [21] S. MacLane and G. Birkhoff, *Algebra*, Macmillan, New York, 1967.
- [22] J. Rotman, *The Theory of Groups*, 2nd Edition, Allyn and Bacon, Boston, 1973.
- [23] W. Rudin, *Real and Complex Analysis*, 2nd Edition, McGraw-Hill, New York, 1974.
- [24] P. Suppes, *Axiomatic Set Theory*, van Nostrand, Princeton, 1960.
- [25] J. G. Thompson, *Normal p -complements for finite groups*, J. of Algebra vol 1 (1964), 43-46.
- [26] B. van der Waerden, *Algebra, Vol. I*, 7th Edition, Ungar, New York, 1970.

Índice alfabético

- Algoritmo
 - euclídeo de la división, 54
- Aplicación, 7
 - canónica, 80
 - cociente, 80
- Argumento, 40
- Arquímedes
 - teorema de, 19
- Axioma
 - de elección, 70
- Axioma (s)
 - algebraicos de los reales, 13
 - algebraicos del orden, 13
 - de caracterización de los reales, 17
 - de completez, 17
 - de los conjuntos, 10
- Bezout
 - relación de, 60
 - Teorema de, 60
 - teorema de, 23
- Cailey
 - teorema de, 138
- Campo, 45
 - algebráicamente cerrado, 57
 - de cocientes, 46
 - extensión de un, 45
 - numérico, 45
- Cauchy
 - teorema de, 131
- Centralizador, 201
- Centro, 201
- Ciclo, 173
 - longitud de un, 174
- Clase, 4
 - de conjugación, 234
 - de conjuntos, 11
 - de equivalencia, 79
 - lateral, 118
- Clases
 - de transitividad, 196
- Coclase, 118
- Cogruppo, 118
- Conjunto (s), 3
 - de los números enteros, 21
 - acotado, 15
 - cardinal de un, 4
 - cardinal un, 74
 - clase de, 4, 11
 - cociente, 80
 - complemento de, 5
 - de los números naturales, 18
 - de los números reales, 12
 - diagonal de un, 9
 - diferencia de, 5
 - disyuntos, 5
 - enumerable, 74
 - equinumerosos, 76, 77
 - equipotentes, 77
 - familia de, 11
 - finito, 70

inductivo, 18
 infinito, 70
 intersección de, 5
 partes de un, 11
 unión de, 5
 vacío, 4
 Conmutador, 235
 Cortadura de Dedekind, 85
 Cota
 inferior, 15
 superior, 15
 De Moivre
 fórmulas de, 42
 De Morgan
 leyes de, 11
 Dedekind
 cortadura de, 85
 Descomposición
 prima, 28
 primaria, 27
 Divisor, 22, 52
 Dominio, 45
 de los enteros de Gauss, 45
 de saldos, 46
 factorial, 68
 multiplicativamente simétrico,
 45
 numérico, 45
 unidad de un, 52
 Ecuación
 orbital, 198
 Eisenstein
 criterio de, 68
 Elemento neutro, 12, 100
 Endomorfismo, 249
 Epimorfismo, 135
 Espacio afín, 205
 Estabilizador, 196, 198

Euclides

teorema de, 21, 29, 53

Euler

fórmula de, 41
 función de, 250

Exponente

primitivo, 122

Extremo

inferior, 17
 superior, 17

Factor, 22, 52

directo, 161
 primario, 27

Fermat

pequeño de, 143

Fracciones Parciales, 94

Fracciones parciales
monógenas, 94

Función, 7

biyectiva, 9
 compuesta, 8
 de elección, 70, 95
 idéntica, 9
 inversa, 9
 inyectiva, 8
 recorrido de una, 8
 sobreyectiva, 8

Gauss

enteros de, 45
 teorema de, 58

Gráfica, 6

compuesta, 8
 funcional, 7
 inversa, 8

Grupo, 99

abeliano, 100
 acción de un, 195
 alternante, 185

cíclico, 116

centro de un, 234
 cociente, 130
 conmutativo, 100
 de derecha, 106
 de izquierda, 107
 de Klein, 188
 del tipo (p, q) , 221
 diedro, 222
 n -ésima potencia de un, 236
 nilpotente, 236
 normalizador de un, 188
 numérico aditivo, 90
 numérico multiplicativo, 90
 orden de un, 117, 118
 partición de un, 234
 resoluble, 241
 serie para un, 244
 simétrico, 103
 simétrico, 171
 simple, 187

Homomorfismo, 135

Imagen, 8

directa, 8
 recíproca, 8

Índice, 128

Inverso, 12, 101

Isomorfía

cuarto teorema de, 153
 primer teorema de, 146
 quinto teorema de, 154
 segundo teorema de, 147
 tercer teorema de, 149

Isomorfismo, 135

Klein

grupo de, 188

Lagrange

corolario de, 120

teorema de, 120

Ley de composición interna, 99

Leyes de De Morgan, 11

Máximo, 15

común divisor, 23, 59, 83

Mínimo, 15

común múltiplo, 28, 83

Múltiplo, 22

Matriz

adjunta, 104

Mayor entero, 30

Monomorfismo, 135

Número (s)

imaginario, 36

algebraico, 96

complejos, 35

argumento de un, 40

conjugado, 35

forma polar de un, 40

parte imaginaria, 35

parte real, 35

raíces n -ésimas de, 43

enteros, 21

naturales, 18

primo, 26

primos relativos, 24

racionales, 29

reales, 12

Normalizador, 188

Operador, 195

Orbita, 196

Orbital, 172

Orden

de un grupo, 118

p -elemento, 208

p -grupo, 207

p-subgrupo, 207
 de Sylow, 207
 Pareja ordenada, 6
 Parte entera, 30
 Partición, 79, 120
 Permutación, 171
 cíclica, 173
 orbital de una, 172
 signo de una, 183
 Polinomio (s), 47
 mónico, 59
 asociados, 53
 contenido de un, 66
 descomposición prima de un,
 65
 descomposición primaria de un,
 65
 divisor de un, 52
 factor de un, 52
 grado de un, 51
 irreducible, 62
 primitivo, 66
 primo, 62
 primos relativos, 61
 Potencia
 primitiva, 122
 Principio
 de buena ordenación, 19
 de inducción, 20
 Producto
 cartesiano generalizado, 95
 directo externo, 161
 directo interno, 152
 Producto cartesiano, 6
 Raíz
 n -ésima positiva, 34
 n -ésima primitiva, 44
 de un polinomio, 56
 multiplicidad de una, 58

Relación, 7
 colectivizante, 4
 codominio de una, 7
 de Bezout, 23, 60
 de equivalencia, 79
 de orden, 14
 de orden lineal, 14
 de orden total, 14
 dominio de una, 7
 funcional, 7
 gráfica de una, 7
 Resolución, 244
 Serie, 244
 composicional, 244
 de composición, 244
 longitud de, 244
 normal, 244
 resolvente, 244
 subnormal, 244
 terminal, 244
 Sistema
 de generadores, 178
 de los números complejos, 35
 de los números racionales, 29
 de los números reales, 12
 de los polinomios, 47
 numérico, 45
 Sistma
 aditivamente simétrico, 45
 Subcampo, 45
 Subconjunto, 3
 Subgrupo, 115
 índice de un, 128
 cíclico, 116
 generado, 121
 n -ésimo derivado, 241
 normal, 127
 Sylow
 cuarto teorema de, 212

p-subgrupo de, 151, 207
 primer teorema de, 149
 primer teorema de, 208
 segundo teorema de, 209
 tercer teorema de, 210
 Tabla de multiplicación, 108
 Teorema
 de Euclides, 29
 de Arquímedes, 19
 de Bezout, 23, 60
 de Cailey, 138
 de Cauchy, 131
 de correspondencia, 148
 de Euclides, 21, 53
 de Gauss, 58
 de isomorfía, 146, 147, 149, 153,
 154
 de Lagrange, 120
 de Sylow, 149
 de Wilson, 251
 estructural de los grupos abelianos
 finitos, 165
 fundamental de la aritmética,
 27
 fundamental del álgebra, 58
 Trasposición, 173
 Unidad
 imaginaria, 36
 Valor absoluto, 15, 36
 Wilson
 teorema de, 251

**PUBLICACIONES DE LA
ACADEMIA COLOMBIANA DE CIENCIAS EXACTAS,
FÍSICAS Y NATURALES**

COLECCIÓN JORGE ÁLVAREZ LLERAS

- Volumen 1 - **Mora-Osejo, L.E.** 1987. Estudios morfológicos, autoecológicos y sistemáticos en Angiospermas. 1/16. 196 pp, 75 figs.
- Volumen 2 - **Murillo, M.T. & M.A. Harker.** 1990. Helechos y plantas afines de Colombia. 1/16. 326 pp, 145 figs.
- Volumen 3 - **Lozano-Contreras, G.** 1994. Las Magnoliaceae del Neotrópico 1/16, 148 pp, 46 figs.
- Volumen 4 - **Eslava Ramírez, J.A.** 1994. Aspectos relacionados con la erupción del volcán Nevado del Ruiz. 1/16, 174 pp, 46 figs.
- Volumen 5 - **Rocha de Campos, M.** 1994. Diversidad en Colombia de los cangrejos del género *Neostrengeria*. 1/16 iv + 144 pp, 47 figs.
- Volumen 6 - **Mora-Osejo, L. E. & H. Sturm.** 1994. Estudios ecológicos del páramo y del bosque altoandino, cordillera Oriental de Colombia. Tomos 1 y 2, 1/16, 716 pp, 190 figs.
- Volumen 7 - **Díaz, J.M., J. Garzón-Ferreira & S. Zea.** 1995. Los arrecifes coralinos de la isla de San Andrés, Colombia, estado actual y perspectivas para su conservación. 1/16, 152 pp, 15 figs, 14 tablas, 9 fotografías.
- Volumen 8 - **Eslava Ramírez, J.A.** 1995. Régimen de la presión atmosférica en Colombia. 1/16, 152 pp, 94 figs, 59 tablas.
- Volumen 9 - **Donato, J.Ch., L. E. González & C. L. Rodríguez.** 1996. Ecología de dos sistemas acuáticos de páramo. 1/16, 168 pp, 53 figs, 14 tablas, 9 fotografías.
- Volumen 10 - **Andrade-C. M., G. Amat & F. Fernández. (eds.)** 1996. Insectos de Colombia - Estudios escogidos. 1/16, 544 pp, 145 figs, tablas y mapas.
- Volumen 11 - **González, F.** 1998. Inventario preliminar de gases de efecto invernadero en Colombia, 1990, Fuentes y sumideros. 1/16, xiv + 174 pp, 108 figs, tablas y gráficas.
- Volumen 12 - **Díaz-Piedrahita, S. & J. Cuatrecasas.** 1999. Asteráceas de la flora de Colombia, Senecioneae I, géneros *Dendrophorbium* y *Pentacalia*. 1/16, 392 pp, 110 figs, 24 mapas.
- Volumen 13 - **Amat, G., M. C. Andrade, M. G. & F. Fernández (eds.)** 1999. Insectos de Colombia. 1/16, 438 pp. + tablas, figuras y mapas.
- Volumen 14 - **Rodríguez, H. & F. González.** Opciones para la reducción de emisiones de gases de efecto invernadero (GEI) en Colombia. 1/16, 262 pp.
- Volumen 15 - **Rodríguez, H. & González, F.** 2000. Portafolio colombiano de proyectos para el MDL -sector en energía-. 1/16, 164 pp.
- Volumen 16 - **Espinosa, Baquero A.** 2000. Erupciones históricas de los volcanes colombianos, 1/16, 292 pp.
- Volumen 17- **Mora Osejo, L. E.** 2001. Contribuciones al estudio comparativo de la conductancia y de la transpiración foliar de especies de plantas del páramo. 1/16. xii + 282.

- Volumen 18- **Roldán, G., J. A. Posada & J. C. Gutiérrez.** 2001. Estudio Limnológico de los Recursos Hídricos del Parque de Piedras Blancas. 1/16. x + 146.
- Volumen 19- **Donato-Rondón, J. Ch.** 2001. Fitoplancton de los Lagos Andinos del Norte de Sudamérica (Colombia). 1/16, xii+222.
- Volumen 20- **Aristizábal García, H.** 2002. Los hemípteros de la película superficial del agua en Colombia. 1/16. xv+242, 331 figs.
- Volumen 21- **Pinto, M.** 2002. Estudio sistémico del género *Cavia*. 1/16. 216 pp. 38 figs. 31 láminas, 59 tablas.
- Volumen 22- **Orozco Pardo, C. I.** 2003. Evolutionary biology of *Brunellia* Ruiz & Pavón (Brunelliaceae, Oxalidales). 1/16, 198 pp. + tablas, figuras y mapas.
- Volumen 23- **Vargas Jiménez, C.A.** 2004. Propagación de ondas sísmicas y atenuación de ondas de Coda en el territorio colombiano. 1/16, 240 pp. + anexos. Tablas, figuras y mapas.
- Volumen 24- **Campos, M.R.** 2005. Fresh water crabs from Colombia: a taxonomic and distributional study. 1/16, 364 pp. + tablas, figuras.
- Volumen 25- **Forero, E. & Romero C.** 2005. Estudio en leguminosas colombianas. 1/16, 414 pp. + anexos, tablas y figuras.

COLECCIÓN ENRIQUE PÉREZ ARBELÁEZ

- Volumen 1 - **Memorias del seminario en conmemoración del centenario de Erwin Schrödinger.** 1987, 1/16, 221 pp.
- Volumen 2 - **Díaz-Piedrahita, S. & A. Lourteig.** 1989. Génesis de una flora. 1/16, vii. + 362 pp, 35 figs.
- Volumen 3 - **Cubillos, G., F.M. Poveda & J.L. Villavices.** 1989. Historia epistemológica de la Química. 1/16, 128 pp.
- Volumen 4 - **Hernández de Alba, G. & A. Espinosa.** 1991. Tratados de minería y estudios geológicos de la época colonial, 1616-1803, 1/16 xii + 92 pp, 1 fig.
- Volumen 5 - **Díaz-Piedrahita, S. (ed.)** 1991. José Triana, su vida, su obra y su época. 1/16, viii + 188 pp, 73 figs.
- Volumen 6 - **Díaz-Piedrahita, S.** 1991. La Botánica en Colombia, hechos notables en su desarrollo. 1/16, x + 126 pp. 30 figs, (reimpreso 1997).
- Volumen 7 - **Mantilla, L.C. & S. Díaz-Piedrahita.** 1992. Fray Diego García, su vida y su obra científica en la Expedición Botánica. 1/16, xv + 284, 14 figs. (reimpreso 1995).
- Volumen 8 - **Arias de Greiff, J.** 1993. Historia de la Astronomía en Colombia. 1/16, 200 pp, 32 figs.
- Volumen 9 - **Lértora Mendoza, C.** 1995. Fuentes para el estudio de las ciencias exactas en Colombia. 1/16, 316 pp.
- Volumen 10 - **Gauss, C. F.** 1995. Disquisitiones Arithmeticae. Traductores: H. Barrantes, M. Josephy & A. Ruiz Zúñiga. 1/16, 540 pp.
- Volumen 11- **Murillo Quinche, L.M.** 1997. Obra selecta. 1/16, x + 188 pp, 29 figs, 4 mapas.
- Volumen 12 - **Romero Beltrán, A.** 1997. La investigación de las dolencias infecciosas en la historia. 1/16, xiv + 540 pp.
- Volumen 13 - **Barrantes, H. & A. Ruiz.** 1998. La historia del Comité Interamericano de Educación Matemática. 1/16, x + 198 pp. (español e inglés). Edición electrónica paralela.
- Volumen 14 - **Díaz-Piedrahita, S.** 2000. Matís y los dos Mutis, 1/16, x 346 pp, 41 figs.

COLECCIÓN JULIO CARRIZOSA VALENZUELA

- Volumen 1 - **Castillo, G.** 1992. Física Cuántica, teoría y aplicaciones. Tomo I, 1/16, xxxii + 410, 77 figs.
- Volumen 2 - **Bernal de Ramírez, I.** 1993. Análisis de alimentos. 1/16, xviii + 314 pp, 28 figs. (reimpreso 1998).
- Volumen 3 - **Castillo, G.** 1994. Física Cuántica, teoría y aplicaciones. Tomo II. 1/16, xx + 406 pp., 49 figs.
- Volumen 4 - **Cáceres, D. (ed.).** 1995. Creando ciencia crean docencia. 1/16, 140 pp, 38 figs.
- Volumen 5 - **Romero, C.M. & L.H. Blanco.** 1996. Tópicos de Química Básica. 1/16, 240 pp, 56 figs.
- Volumen 6 - **Peña, G. & M. Pinto.** 1996. Mamíferos más comunes en sitios precerámicos de la sabana de Bogotá. 1/16, 98 pp, 1 mapa, 6 dibujos a color, 18 láminas y 48 gráficos.
- Volumen 7 - **López, C.** 1998. Mecánica Newtoniana. 1/16, 280 pp, 69 figs.
- Volumen 8 - **Charris, C. J., De Castro K. & J. Varela B.** 2000. Fundamentos del análisis complejo de una variable. 1/16, 384 pp.
- Volumen 9 - **Varela, J. de D.** 2000. Principios de Cristalografía. 1/16, xx + 250 pp., 141 figs.
- Volumen 10 - **Kairuz de Civetta, A.** 2002. Introducción al estudio de la composición de los alimentos. 1/16. xx + 166 pp. 16 figs., 30 tablas.
- Volumen 11 - **Muñoz Quevedo, José M.** 2003. Topología Básica. 1/16, VIII +236 pp.
- Volumen 12 - **Romero de Pérez, G.** 2003. Microscopia electrónica. 1/16, XX + 290 pp. 105 figs.
- Volumen 13 - **Charris, J. A., Aldana, B. & P. Acosta,** 2005. Álgebra I. Fundamentos y teoría de los grupos 1/16, x + 264 pp.

COLECCIÓN MEMORIAS

- Volumen 1 - (1994) **Memorias del Seminario Nacional "El quehacer teórico y las perspectivas holista y reduccionista.** 1/16, viii + 184 pp.
- Volumen 2 - (1994) **Memorias del Seminario Konrad Lorenz sobre Etología.** 1/16, iv + 38 pp.
- Volumen 3 - (1995) **Memorias del Seminario-taller sobre Alta Montaña Colombiana.** 1/16, 116 pp.
- Volumen 4 - (1996) **Memorias del Primer Congreso Nacional de Neurocomputación.** 1/16, xiv + 184 pp.
- Volumen 5 - (1996) **Memorias del Primer Congreso Nacional de sobre Cambio Climático.** 1/16, 138 pp, 9 figs.
- Volumen 6 - (1996) **Memorias del Coloquio "Ciencia, tecnología y cultura".** 1/16, xii + 198 pp.
- Volumen 7 - (1996) **Memorias de la III Escuela de verano en Geometría Diferencial, ecuaciones diferenciales parciales y análisis numérico.** 1/16, xiv + 174 pp.
- Volumen 8 - (1996) **Memorias del Seminario de Ciencia Teórica.** 1/16, xv + 170 pp.
- Volumen 9 - (1997) **Memorias del Seminario en conmemoración de los 440 años del nacimiento de René Descartes.** 1/16, xii + 174 pp.
- Volumen 10 - (2001) **Memorias del Simposio Pueblos y Ambientes del pasado precolombino** 1/16, viii + 312 pp.
- Volumen 11 - (2001) **Reflexiones sobre la ciencia y la tecnología: Colombia al iniciarse el siglo XXI,** 1/16, x+166 pp.

COLECCIÓN LUIS DUQUE GÓMEZ

Volumen 1 - **Bueno Hernández, A. & J. Llorente Bousquets.** 2003. El pensamiento biogeográfico en Alfred Russel Wallace. 14x21, 196 pp, 29 figs.

EDICIONES ESPECIALES

- Francisco José de Caldas, su vida, su personalidad, su obra y el descubrimiento de la hipsometría. 1958. 1/16 refilado. 94 pp.
- Alexander von Humboldt en Colombia. Extractos de sus diarios. 1982. Arias de Greiff, J. (ed.). 1/8 refilado. 286 pp., 20 figs.
- Status and problems of Science in Latin America and the Caribbean. 1990. Guardiola, M.L., J.L. Villaveces & G. Violini (eds.). 1/16, 542 pp.
- Science in Latin America and the Caribbean and its role in regional development. 1992. Hamende, A., M.H. Hassan, J.L. Villaveces & G. Violini (eds.) 1/16, 2 vols. 824 pp.
- El cambio global, ciencia para entender el mañana. 1998. Lozano, J. (ed.), carta, 322 pp. Figs., mapas y gráficos.
- Tradición Académica. Diccionario Biográfico y Bibliográfico de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales, 1/16, x + 434 pp.
- **Díaz Piedrahita, S. & L.C. Mantilla R.** 2001. La terapéutica en el Nuevo Reino de Granada. Un recetario franciscano del siglo XVIII. Publicación especial No. 7 208 pp. 502 figs.

EDICIONES ELECTRÓNICAS

- Memorias del VII Encuentro Nacional de Óptica. (Edición en CD-ROM). 2004
- Historia Sísmica de Colombia (1550-1830). (Edición en CD-ROM). 2004

1997

- V. S. Albis, J. Charum, C. H. Sánchez & G. Serrano (Eds.). *Memorias del Seminario en conmemoración de los 400 años del nacimiento de René Descartes.* 1/16, xii + 222 págs., 5 figs., 1 fotografía, 1997. ISBN: 958-9205-26-7; 958-9205-21-6 (Obra completa). US\$ 40.

1998

- Fabio González et al.. *Inventario de gases de efecto invernadero. Fuentes y sumideros: Colombia 1990 / GHG Preliminary Inventory* xiv + 171 págs. Santafé de Bogotá, 1998. ISBN 958-9205-33-X.
- Hugo Barrantes & Ángel Ruiz. *Historia del Comité Interamericano de Educación Matemática / History of the Inter American Committee in Mathematical Education* 1998.

2000

- John D. Lynch, *Enciclopedia de las ranas de Colombia / Encyclopedia of Colombian Frogs.*
- Clóvis Pereira da Silva. *A matemática no Brasil. Uma História de seu Desenvolvimento.* Segunda Edição.
- Lina Rocío Medina Muñoz. *Tradición académica. Diccionario biográfico y bibliográfico de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales.* x + 434 págs. Santafé de Bogotá, 2000. ISBN 958- 9205-34-8.

- Humberto Rodríguez & Fabio González. *Portafolio colombiano de proyectos para el MDL. / Colombian Project Portfolio in the Energy Sector under CDM.* 162 págs. Santafé de Bogotá, 2000. ISBN 958-9205-38-0.
- Humberto Rodríguez & Fabio González. *Opciones para la reducción de emisiones de gases de efecto invernadero en Colombia / Options for Reducing GHG Emissions 1998-2010* . 258 págs. Santafé de Bogotá, 2000. ISBN 958-9205-37-2.

2002

- Luis E. Mora-Osejo & Orlando Fals-Borda. *La superación del eurocentrismo. Enriquecimiento del saber sistémico y endógeno sobre nuestro contexto tropical.* 2002. 16 págs. Acceso libre en la red:
- Armando Espinosa Baquero. *Historia sísmica de Colombia. 1580-1830.* CD-ROM. Se puede acceder a información sobre sismos históricos en Colombia contenida en dos fondos: 1. Banco de datos de la historia sísmica de Colombia BHSC, de 1550 hasta 1830. 2. Estudios y documentos: a. Aspectos generales y metodológicos. b. Estudios generales. c. Estudios específicos. Los interesados en obtener el CD-ROM (Col \$ 25.000 + portes.) deben contactar a: revista@accefn.org.co

2004

- Joaquín Acosta. *Lecciones de geología.* 1850 (2004). 30 págs. Reproducción facsimilar del libro publicado en 1850, por el Coronel Joaquín Acosta, considerado como el primer tratado de geología elemental publicado en Colombia. Acceso libre en la red.
- *Memorias del VII Encuentro Nacional de Óptica (2000).* 2004. El evento se realizó en la Universidad del Quindío (Armenia) del 25 al 29 de septiembre de 2000. CD-ROM. Contiene los resúmenes de las conferencias y contribuciones hechas en el evento, además de los textos completos de algunas de ellas. Acceso libre en la red. Los interesados en obtener el CD-ROM (Col \$ 25.000 + portes.) deben contactar a: revista@accefn.org.co

Las publicaciones de la Academia pueden ser solicitadas directamente al Apartado 44763, Bogotá, D.C., Fax (571) 2443186 Tel. (571) 3414805 Trans. 27 No. 39A - 63/67 - Correo electrónico: accefn@org.co Se ofrecen en venta o mediante intercambio por publicaciones similares. Mayor información a través de Internet: URL: <http://www.accefn.org.co>



EDITORES E IMPRESORES

Edición terminada
en diciembre de 2005.
Bogotá, D.C.- Colombia

ISBN 958-9205-64-X



9 789589 205648



UNIVERSIDAD
SERGIO ARBOLEDA