Parte III Estructuras algebraicas

Las estructuras algebraicas constituyen una de las herramientas básicas para tratar la mayor parte de los problemas asociados a la matemática discreta. En este libro, hemos pretendido dar las primeras nociones algebraicas para poder tratar, a título de ejemplo, algunos de los problemas más conocidos dentro de este ámbito.

En esta última parte, como se ha hecho en el resto del libro, todos los conjuntos a los cuales nos referiremos serán conjuntos finitos o numerables. El primer capítulo de esta parte introduce los conceptos de relaciones, aplicaciones, operaciones, y se acaba presentando las estructuras algebraicas que se tratarán en los capítulos siguientes. Algunas de las nociones que se consideran corresponden a una formación básica y, por tanto, han sido ya utilizadas a lo largo del libro, pero por razones de coherencia formal se ha considerado conveniente reconsiderarlas y agruparlas ordenadamente en su contexto original. El capítulo siguiente está dedicado al estudio de los grupos como modelo más completo de estructura definida a partir de una operación. El tercer capítulo trata las estructuras algebraicas con dos operaciones: anillos y cuerpos. Además de su interés intrínseco como estructuras discretas, los grupos, anillos y cuerpos ofrecen una variedad considerable de aplicaciones. Por ejemplo, la teoría de enumeración de Pólya se estudia al final del capítulo de grupos y en el último capítulo se presentan algunas aplicaciones que constituyen tradicionalmente temas propios de la matemática discreta: diseños combinatorios, geometrías finitas y cuadrados latinos.

Capítulo 9

Introducción a las estructuras algebraicas

1. Relaciones
2. Aplicaciones
3. Operaciones
4. Estructuras algebraicas

La base que fundamenta esta última parte descansa sobre la noción elemental de correspondencia o relación. Como caso particular, aparece el concepto de aplicación a partir del cual se obtiene la noción de operación que abrirá las puertas que conducen al mundo de las estructuras algebraicas. Éste es, por tanto, un capítulo introductorio que nos permitirá definir las bases que se desarrollarán en los capítulos siguientes, dedicados al estudio de las estructuras algebraicas más relevantes.

9.1 Relaciones

Comenzaremos considerando el conjunto formado por todos los posibles pares ordenados formados a partir de los elementos de dos conjuntos. Así pues, dados dos conjuntos A y B, su *producto cartesiano* se define como

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

El hecho de que se trate de pares ordenados hace que $A \times B \neq B \times A$ si $A \neq B$.

Estos pares ordenados se pueden interpretar como relaciones entre los elementos de un conjunto con los del otro. Esta interpretación conduce al concepto siguiente, básico en toda esta parte.

Dados dos conjuntos A y B, se llama *correspondencia* o *relación* de A a B a cualquier subconjunto R del producto cartesiano $A \times B$.

Como ejemplo ilustrativo de esta definición podemos considerar la siguiente relación entre los conjuntos $A = \{a, b\}$ y $B = \{1, 2, 3\}$:

$$R = \{(a, 1), (a, 2), (b, 2)\}$$

Para visualizar estas relaciones es útil usar el grafo de la relación. Éste es un digrafo bipartito $(A \cup B, R)$, que tiene A y B como partes estables y hay un arco de $a \in A$ hacia $b \in B$ si y sólo si $(a, b) \in R$.

La relación del ejemplo anterior se representaría con el grafo siguiente:

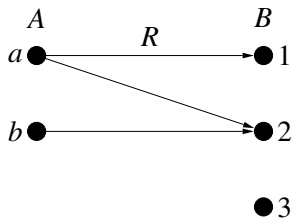


Figura 9.1: Grafo de la relación R

Si $A = B$ diremos que la relación es *binaria* sobre A. Si R es una relación binaria sobre A y $(a, a') \in R$ entonces diremos que a está relacionado con a' y lo denotaremos como aRa'.

En el caso que la relación sea binaria, el grafo que la representa tiene por vértices los elementos del conjunto A y los arcos quedan determinados por las relaciones, es decir, hay un arco de a hacia a' si y sólo si $(a, a') \in R$. Este grafo lo notaremos como,

$$G = (A, R)$$

Como ejemplos ilustrativos podemos considerar los grafos de las relaciones siguientes:

1. La relación $\{(1, 1), (1, 3), (2, 4)\}$ en el conjunto $A = \{1, 2, 3, 4\}$ se puede representar por el grafo de la figura 9.2.

2. El grafo de la relación "ser menor o igual que" en el conjunto $A = \{1, 2, 3, 4\}$ se puede representar como en la figura 9.3.

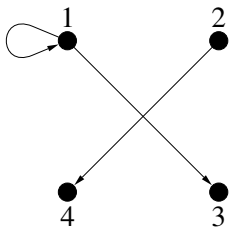


Figura 9.2:

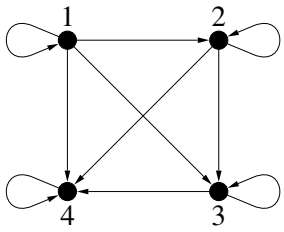


Figura 9.3:

Hay muchas relaciones que tienen en común propiedades con significación especial. Dada una relación R definida sobre un conjunto A, diremos que R es

- *reflexiva* si y sólo si para todo $a \in A$, aRa;
- *simétrica* si y sólo si para todo $a, b \in A$, $aRb \Rightarrow bRa$;
- *antisimétrica* si y sólo si para todo $a, b \in A$, aRb y $bRa \Rightarrow a = b$;
- *transitiva* si y sólo si para todo $a, b, c \in A$, aRb y $bRc \Rightarrow aRc$.

Es fácil construir ejemplos de relaciones que verifiquen algunas de estas propiedades:

1. Si sobre el conjunto de los seres humanos escogemos como relación "ser hermano de", podemos comprobar fácilmente que se verifican las propiedades simétrica y transitiva.
2. Si en el conjunto anterior consideramos la relación "ser estudiante de", ninguna de estas propiedades se cumplen en general.
3. Si la relación que escogemos en el mismo conjunto es "ser más alto que", se verifican sólo las dos últimas propiedades.

4. Si la relación considerada es "ser más alto o igual que", entonces se cumplen todas excepto la segunda de estas propiedades.

La agrupación de algunas de estas propiedades conduce a determinadas clases de relaciones que, por su interés, tienen un nombre propio que las representa.

Diremos que una relación binaria R definida sobre un conjunto A es de *orden* si es reflexiva, antisimétrica y transitiva.

Ejemplos inmediatos de relaciones de orden son los siguientes:

1. "Ser más pequeño" sobre el conjunto de los números naturales.

2. La inclusión no estricta es también una relación de orden sobre el conjunto de las partes de cualquier conjunto. En particular, si $A = \{a, b\}$ podemos representar esta relación con el grafo siguiente,

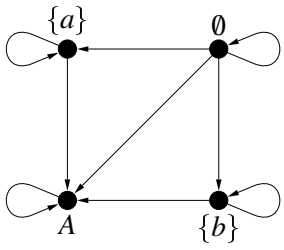


Figura 9.4: Grafo de una relación de orden

Para simplificar el grafismo podemos suprimir los autoenlaces que representan la reflexividad, así como también las aristas que se deducen de la transitividad. Siguiendo este criterio, la representación de la relación anterior es la que figura en 9.5.

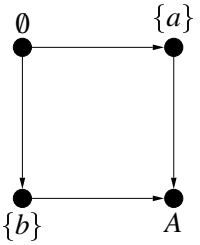


Figura 9.5: Grafo simplificado de una relación de orden

Es útil observar que el grafo de una relación de orden no puede contener ciclos (excepto autoenlaces). Esto quiere decir que hay pares de elementos no relacionados. En el ejemplo anterior, $\{a\}$ no está relacionado con $\{b\}$. Estas situaciones no se presentan si el orden es total.

Una relación de orden R sobre el conjunto A, se dice que es *total* si para todo $a, b \in A$, aRb o bRa. En caso contrario, se dice que el orden es *parcial*.

Así, el grafo que reprenta un orden total tiene que ser una "cadena".

Como ejemplos de relaciones de orden podemos considerar la relación de inclusión sobre las partes de un conjunto como relación de orden parcial. Por ejemplo, si $A = \{a, b\}$, $\{a\}$ y $\{b\}$ no están relacionados, mientras que la relación binaria "ser menor o igual" sobre los números naturales es una relación de orden total.

Otro tipo importante de relación, que conduce a la identificación de objetos equivalentes respecto a alguna propiedad común, es la siguiente.

Se dice que una relación R sobre un conjunto A es de *equivalencia* si es reflexiva, simétrica y transitiva.

Un ejemplo importante de este tipo de relación en el conjunto de los enteros es la llamada *relación congruencia módulo n*. Se dice que dos enteros x, y son congruentes módulo n si y sólo si $x - y$ es un múltiplo de n, es decir, $x = y + kn$ para algún entero k, y se denota normalmente por

$$x \equiv y \pmod{n}$$

Es fácil verificar que la relación de congruencia satisface las propiedades reflexiva, simétrica y transitiva.

Si R es una relación de equivalencia definida sobre A, llamamos *clase de equivalencia* de un elemento $a \in A$ al conjunto de elementos que están relacionados con a según R, y lo denotamos por $[a] = \{x \in A \mid xRa\}$.

Toda relación de equivalencia proporciona una clasificación o partición del conjunto original en subconjuntos que representan las clases de equivalencia originadas por medio de la relación.

Recordemos en primer lugar la definición de partición.

Una colección de subconjuntos propios de un conjunto A, $\{A_i\}_{i \in I}$, es una *partición* de A si y sólo si satisface las dos condiciones siguientes:

1. $\cup_{i \in I} A_i = A$.
2. $A_i \cap A_j = \phi, \quad \forall i, j \in I, \quad i \neq j$.

Proposición 9.1. Si R es una relación de equivalencia sobre un conjunto A, entonces la colección de clases de equivalencia $\{[a], a \in A\}$ es una partición de A.

Demostración.

1. La unión de clases de equivalencia es A. En primer lugar $[a] \subseteq A$, para todo $a \in A$ y, por tanto, $\cup_{a\in A}[a] \subseteq A$. También es cierta la inclusión contraria ya que para todo $a \in A$, $a \in [a]$ (como mínimo $[a]$ contiene a debido a la reflexividad de la relación). De aquí $A \subseteq \cup_{a\in A}[a]$.

2. Todas las clases son disyuntas. Es decir, si $[a] \cap [b] \neq \phi$, entonces es preciso ver que estas clases coinciden. Si suponemos que $x \in [a] \cap [b]$, esto significa que aRx y xRb y, por tanto, aRb. Entonces para todo $y \in [a]$, yRa y aRb implican yRb, de manera que $[a] \subset [b]$. De forma análoga se ve que $[b] \subset [a]$.

□

Observemos que la reflexividad de la relación nos permite demostrar que las clases de equivalencia cubren todo el conjunto A, mientras que la simetría y la transitividad nos garantizan que las clases son disyuntas.

De hecho, también es cierto que toda partición permite definir (de manera formal) una relación de equivalencia sobre el conjunto unión de estas partes. Para ver esto, si $\{A_i\}_{i\in I}$ es una partición del conjunto A, definimos la relación de equivalencia R de la forma siguiente: aRb si y sólo si a y b pertenecen a un mismo conjunto A_i de la partición. Es inmediato comprobar que esta relación verifica las tres propiedades que la hacen de equivalencia.

Hay dos ejemplos extremos (poco interesantes) de relaciones de equivalencia que siempre se pueden definir sobre un conjunto.

1. Uno es la *relación trivial* en la cual cada elemento sólo está relacionado con sí mismo. Con esta relación se obtienen tantas clases como elementos tiene el conjunto de partida y cada clase contiene sólo un elemento.

2. En el extremo opuesto podemos definir la *relación universal* en la cual cada elemento está relacionado con cualquier otro. Esta relación únicamente proporciona una clase de equivalencia que coincide con el propio conjunto de partida.

Un ejemplo no trivial de relación de equivalencia es el de congruencia módulo n en $\mathbb{Z}$. En particular,

1. Si $n = 2$ esta relación permite clasificar los enteros en dos subconjuntos, el de los números pares y el de los números impares, $\mathbb{Z} = [0] \cup [1]$.

2. Si tomamos $n = 3$, $\mathbb{Z}$ queda dividido en tres clases, $\mathbb{Z} = [0] \cup [1] \cup [2]$, donde

$$\begin{aligned} [0] &= \{0, \pm 3, \pm 6, \pm 9, \dots\}, \\ [1] &= \{1, 1 \pm 3, 1 \pm 6, 1 \pm 9, \dots\}, \\ [2] &= \{2, 2 \pm 3, 2 \pm 6, 2 \pm 9, \dots\} \end{aligned}$$

La partición de los elementos de un conjunto en clases de equivalencia permite considerar un nuevo conjunto (desde la perspectiva de la relación de equivalencia) con menos elementos, el constituido por sus clases de equivalencia, que formalmente definimos de la forma siguiente.

Dada una relación de equivalencia R sobre un conjunto A, el *conjunto cociente* de A módulo R es el conjunto que tiene por elementos las clases de equivalencia y lo notaremos como $A/R = \{[a] \mid a \in A\}$.

Sobre el conjunto de los enteros, las relaciones de congruencia de los ejemplos anteriores dan lugar a los siguientes conjuntos cociente:

1. Si R es la relación de congruencia módulo 2, entonces $\mathbb{Z}/R = \{[0], [1]\}$.

2. Si R es la relación de congruencia módulo 3, entonces $\mathbb{Z}/R = \{[0], [1], [2]\}$.

Las relaciones de equivalencia, aunque directamente no dan lugar a ningún tipo especial de construcción algebraica, son imprescindibles para trabajar a un cierto nivel con cualquiera de ellas.

9.2 Aplicaciones

Las aplicaciones o funciones discretas son un caso particular de relación o correspondencia entre dos conjuntos finitos o numerables, en la cual a cada elemento del primer conjunto le hacemos corresponder un único elemento del segundo conjunto. Este tipo de relación es una de las más utilizadas en todo lo referente a la matemática discreta.

De forma precisa, se dice que una relación f sobre el conjunto $X \times Y$ es una *aplicación* o función discreta si y sólo si para todo $x \in X$ existe un único $y \in Y$ tal que xfy. Si xfy o $(x, y) \in f$, se dice que f envía x a y y lo denotamos escribiendo $f(x) = y$. También se dice que y es la imagen de x por f, o bien, que x es una antiimagen de y.

El conjunto imagen de X a través de f es el subconjunto de Y sobre el que se envía algún elemento de X y habitualmente se denota como $f(X)$ o también como $Im\, f$. Es decir,

$$f(X) = Im\, f = \{y \in Y \mid \exists x \in X : f(x) = y\}$$

Se dice que X es el *dominio* de la aplicación f y se denota como $Dom f = X$. Se dice también que el *recorrido* de f es Y. Habitualmente, para expresar el dominio y el recorrido de una aplicación f, se utiliza la notación $f : X \longrightarrow Y$.

Si consideramos los conjuntos de números naturales o enteros, podemos definir las aplicaciones siguientes:

1. $f : \mathbb{N} \longrightarrow \mathbb{N},\ f(n) = n+1$
2. $f : \mathbb{N} \longrightarrow \mathbb{Z},\ f(n) = n-1$
3. $f : \mathbb{N} \longrightarrow \{1\},\ f(n) = 1$
4. $f : \mathbb{Z} \longrightarrow \mathbb{Z},\ f(z) = 3z-17.$

En el grafo de una aplicación $f : X \longrightarrow Y$, de cada vértice de X tiene que salir una única arista hacia algun vértice de Y. Los grafos siguientes representan algunas aplicaciones o funciones discretas.

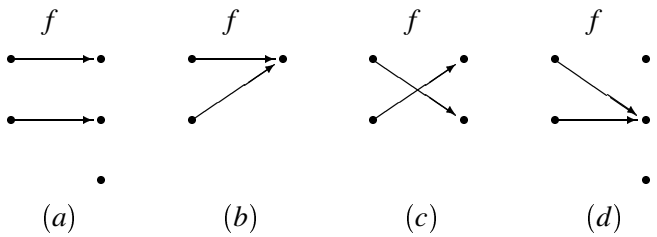


Figura 9.6: Grafos de aplicaciones

A menudo, para definir aplicaciones sobre conjuntos finitos, se especifica el valor que toma la aplicación sobre cada elemento de su dominio.

Tiene interés considerar, como se verá más adelante, la restricción de una aplicación a un subconjunto del dominio y también su relación inversa.

Dada una aplicación $f : X \longrightarrow Y$ y un subconjunto $X' \subset X$, una *restricción* de f sobre X' es una aplicación $f' : X' \longrightarrow Y$ que coincide con f si consideramos f restringida a X'. Lo denotamos como $f_{|X'} = f'$. También se dice que f es una *extensión* de f'.

La *relación inversa* de una aplicación $f : X \longrightarrow Y$ es el conjunto de pares ordenados $\{(y,x) \mid (x,y) \in f\}$ y se denota como f^{-1}.

Como sugiere la definición, el grafo de la inversa de una aplicación se obtiene invertiendo el sentido de los arcos en el grafo de la función original. La inversa de una función $f : X \longrightarrow Y$ es siempre una relación sobre $Y \times X$, pero no necesariamente es una aplicación, como se puede observar en la figura anterior.

Hay ciertos tipos de funciones que por su comportamiento reciben un nombre especial. Entre las más comunes se encuentran las siguientes.

Una aplicación $f : X \longrightarrow Y$ se llama

- *inyectiva* si y sólo si para todo $x, x' \in X$, si $x \neq x'$, entonces $f(x) \neq f(x')$.
- *exhaustiva* si y sólo si para todo $y \in Y$, existe $x \in X$ tal que $f(x) = y$.
- *biyectiva* si y sólo si es inyectiva y exhaustiva.

En la figura 9.6 hay representada en primer lugar una aplicación inyectiva, seguida de una exhaustiva y una biyectiva. La última de las aplicaciones queda fuera de esta clasificación.

Observar también que, si $f : X \longrightarrow Y$ es una biyección, entonces $f^{-1} : Y \longrightarrow X$ es una aplicación y es también biyectiva.

Una interpretación a veces útil de la clasificación anterior es la siguiente. Si $f : X \longrightarrow Y$ es una aplicación y $b \in Y$ es un valor arbitrario, entonces decir que

a) la solución de la ecuación $f(x) = b$, en caso de existir, es única es equivalente a decir que f es inyectiva;

b) la ecuación $f(x) = b$ admite solución en x es equivalente a decir que f es exhaustiva;

c) existe una única solución de la ecuación $f(x) = b$ es equivalente a decir que f es biyectiva.

La proposición siguiente dice que, en algunos casos, estas tres condiciones son equivalentes.

Proposición 9.2. Si X e Y son dos conjuntos finitos con el mismo número de elementos, entonces $f : X \longrightarrow Y$ es inyectiva si y sólo si f es exhaustiva.

Demostración. En general, si X e Y son finitos, es fácil ver que f es inyectiva si y sólo si $|X| = |f(X)|$ y f es exhaustiva si y sólo si $|f(X)| = |Y|$. Cuando $|X| = |Y|$, estas dos condiciones son equivalentes. □

Cabe observar que este resultado sólo es cierto si X e Y son finitos. Como ejemplo, si consideramos la aplicación $f : \mathbb{N} \longrightarrow \mathbb{N}$, $f(n) = 2n$, que envía los números naturales a los números pares, ésta es claramente una aplicación inyectiva, pero en cambio no es exhaustiva.

De la demostración de este resultado se deduce el *principio de Dirichlet* o también llamado *principio del palomar*, que ha sido introducido en el capítulo 5 y que, expresado en términos de esta proposición, dice que si $|X| > |Y|$, entonces algún elemento de Y tiene que tener más de una antiimagen.

Uno de los recursos más potentes para la obtención de nuevas funciones a partir de otras ya conocidas se obtiene a partir de la composición de funciones.

Dadas dos funciones $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ se define la *composición* de f con g, que se denota como $g \circ f$, como aquella aplicación $g \circ f : X \longrightarrow Z$ tal que $(g \circ f)(x) = g(f(x))$.

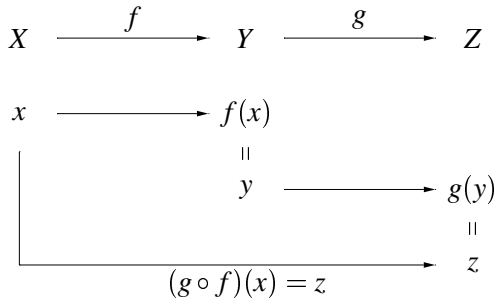


Figura 9.7: Composición de aplicaciones

A título de ejemplo ilustrativo se pueden considerar los grafos que figuran en 9.7, que

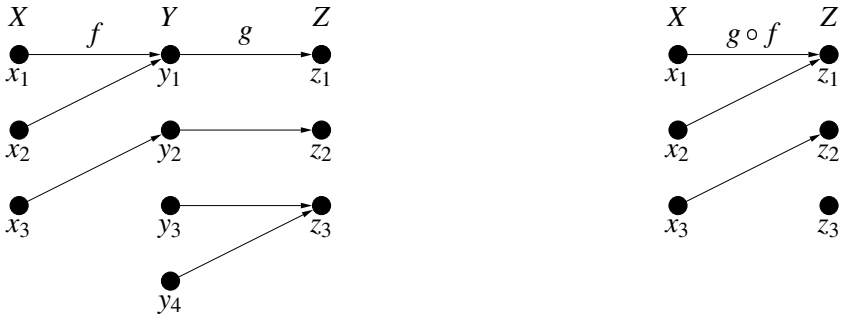


Figura 9.8: Grafo de una composición de aplicaciones

representan el grafo de la composición $g \circ f$ a partir de los grafos de las aplicaciones f y g.

Una cuestión interesante que se plantea constantemente en matemáticas es la de saber cuándo, al combinar dos entidades con propiedades comunes, se obtiene un resultado con la misma propiedad. Para la composición de aplicaciones tenemos el resultado siguiente:

Proposición 9.3. Dadas dos aplicaciones, $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$, se puede afirmar que:

a) si f, g son inyectivas, entonces $g \circ f$ es también inyectiva;

b) si f, g son exhaustivas, entonces $g \circ f$ es también exhaustiva.

Demostración. a) Para demostrar que $g \circ f$ es inyectiva, sean $x, x' \in X$ tales que $(g \circ f)(x) = (g \circ f)(x')$. Entonces, de $g(f(x)) = g(f(x'))$ se deduce que $f(x) = f(x')$ ya que g es inyectiva. Como f es también inyectiva deducimos que $x = x'$, y por tanto obtenemos la inyectividad de $g \circ f$.

b) Dado $z \in Z$, como g es exhaustiva, existe $y \in Y$ tal que $g(y) = z$. Por otra parte, como f es también exhaustiva, existe $x \in X$ tal que $f(x) = y$. Así, $z = g(y) = g(f(x)) = (g \circ f)(x)$ y, por tanto, $Im(g \circ f) = Z$. □

Cabe observar que, de esta proposición, se deduce directamente la biyección de la composición, siempre que las funciones originales sean biyectivas.

9.3 Operaciones

Las operaciones binarias más familiares son las operaciones aritméticas de la suma y el producto. Cada una de estas operaciones es una regla que asocia a cada par de números otro número bien definido. El concepto genérico de operación binaria es una generalización de esta idea.

Una *operación binaria*, a veces llamada también *ley de composición interna*, sobre un conjunto A es una aplicación de $A \times A$ sobre A.

$$\begin{array}{rccc} f: & A \times A & \longrightarrow & A \\ & (a,b) & \longrightarrow & f(a,b) \end{array}$$

Habitualmente, las aplicaciones que representan operaciones binarias se denotan mediante algún símbolo que une los elementos operados, por ejemplo,

$$f(a,b) = a \star b, \quad f(a,b) = a \perp b, \quad f(a,b) = a + b$$

Seguidamente damos los ejemplos de operaciones binarias más utilizadas.

1. Además de las operaciones aritméticas elementales, en el conjunto de los números naturales se pueden definir muchas otras operaciones, como por ejemplo

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ (n,m) & \longrightarrow & n(m+1) \end{array}$$

2. La composición de aplicaciones definidas de un conjunto X en él mismo, que denotamos como $F(X)$, constituye un ejemplo importante de operación no aritmética.

$$\begin{array}{ccc} F(X) \times F(X) & \longrightarrow & F(X) \\ (f,g) & \longrightarrow & f \circ g \end{array}$$

3. Si consideramos $\wp(X)$, el conjunto de las partes del conjunto X, la unión y la intersección son dos ejemplos importantes de operaciones.

$$\begin{array}{rcl} \wp(\mathbf{X}) \times \wp(\mathbf{X}) & \longrightarrow & \wp(\mathbf{X}) \\ (A,B) & \longrightarrow & A \cup B \end{array} \qquad \begin{array}{rcl} \wp(\mathbf{X}) \times \wp(\mathbf{X}) & \longrightarrow & \wp(\mathbf{X}) \\ (A,B) & \longrightarrow & A \cap B \end{array}$$

Una estructura algebraica importante basada en estas operaciones es la llamada *de Boole*, que se define en el problema 7 del penúltimo capítulo.

Otros ejemplos importantes de operaciones aritméticas son la suma y el producto sobre enteros módulo n y constituyen lo que se llama *aritmética modular*. Estas operaciones se definen de manera natural, es decir, asignando a la suma de clases la clase de la suma y como producto de clases la clase del producto.

$$\begin{array}{rcl} \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ ([a],[b]) & \longrightarrow & [a]+[b]=[a+b] \end{array} \qquad \begin{array}{rcl} \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ ([a],[b]) & \longrightarrow & [a]\cdot[b])=[a\cdot b] \end{array}$$

Es preciso comprobar que estas operaciones están bien definidas, es decir, que no dependen de los representantes escogidos en cada clase. Ciertamente, si a, a' son dos representantes cualesquiera de la clase $[a]$ y b, b' dos de la clase $[b]$, entonces podemos escribir $a' = a + hn$ y $b' = b + kn$, y por tanto $a' + b' = a + b + pn$ y $a' \cdot b' = a \cdot b + qn$, $h, k, p, q \in \mathbb{Z}$, de donde

$$[a' + b'] = [a + b] \quad y \quad [a' \cdot b'] = [a \cdot b]$$

La aritmética computacional ofrece muchos ejemplos de operaciones binarias sobre conjuntos finitos. Cada computador tiene un repertorio de operaciones aritméticas sobre los números enteros, que normalmente incluyen sumas, diferencias, multiplicaciones y divisiones. A causa de la propia estructura del computador, sólo un subconjunto finito de enteros pueden ser manipulados. Por tanto, en la práctica, las operaciones aritméticas son modulares.

Se pueden describir otros tipos de operaciones binarias diferentes de las operaciones aritméticas brevemente comentadas. El hecho de que una señal pueda tomar valores sobre el conjunto $\mathbb{Z}_2 = \{0, 1\}$ hace que cualquier dispositivo con dos entradas y una salida represente una operación binaria sobre $\mathbb{Z}_2$.

Una operación binaria se puede describir tabulando los valores de los pares asociados a su dominio. Esta tabulación normalmente se llama *tabla de composición* de la operación. Como ejemplo consideremos la operación definida sobre el conjunto $A = \{a, b, c, d\}$ descrita en la tabla 9.1.

En particular son útiles las tablas de operaciones aritméticas modulares. Como ejemplos, podemos considerar las que figuran en las tablas 9.2 y 9.3.

Estas operaciones se dicen binarias por indicar que cada par ordenado de elementos de A es enviado por la operación a un nuevo elemento de A. Si son ternas ordenadas de elementos

Tabla 9.1: Tabla de una operación binaria

$\star$	a	b	c	d
a	b	c	d	d
b	a	b	c	d
c	c	a	c	d
d	a	b	a	b

Tabla 9.2: Tabla de la suma en $\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

de A las que son enviadas a A por la operación, diremos que la operación es *ternaria*. De forma similar, si la operación nos proporciona las imágenes en A de n-tuplas de A, entonces hablaremos de una operación *n-ária*.

Una manera sencilla de construir operaciones n-árias es la de componer recursivamente operaciones binarias. Por ejemplo, a partir de una operación binaria $f : A \times A \longrightarrow A$, podemos construir la operación ternaria

$$\begin{array}{rccc} f: & A\times A\times A & \longrightarrow & A \\ & (a,b,c) & \longrightarrow & f(f(a,b),c) \end{array}$$

Esta es la manera en que los ordenadores realizan operaciones sobre un conjunto de n

Tabla 9.3: Tabla del producto en $\mathbb{Z}_4$

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

entradas, ya que internamente el ordenador sólo admite operaciones binarias. Por ejemplo, la operación ternaria $f(a,b,c) = a+b+c$ se efectúa haciendo

$$f(a,b,c) = (a+b)+c$$

Las operaciones binarias pueden tener propiedades que resultan imprescindibles para la construcción de estructuras algebraicas. Las que presentan un interés más relevante en este sentido son las siguientes.

Dadas dos operaciones binarias, $\star$ y $\perp$, definidas sobre un conjunto A, diremos que la operación $\star$ es

- *asociativa* si y sólo si, para todo $a,b,c \in A$, $a\star(b\star c) = (a\star b)\star c$;
- *conmutativa* si y sólo si, para todo $a,b \in A$, $a\star b = b\star a$;
- *distributiva* respecto de $\perp$ si y sólo si, para todo $a,b,c \in A$, se satisfacen las igualdades siguientes:

$$\begin{aligned} a\star(b\perp c) &= (a\star b)\perp(a\star c) \\ (b\perp c)\star a &= (b\star a)\perp(c\star a) \end{aligned}$$

Observar que las dos igualdades que se tienen que cumplir (para que $\star$ sea distributiva respecto de $\perp$) coinciden cuando $\star$ es conmutativa.

En los conjuntos de los números naturales, enteros y racionales, tanto la suma como el producto son operaciones asociativas y conmutativas, y el producto es distributivo respecto de la suma, pero la suma no es distributiva respecto del producto.

Cabe observar que, en $\mathbb{Q}$, la diferencia y el cociente no son ni asociativas ni conmutativas, y también que, en $\mathbb{Z}$, el cociente no está definido, ya que hay pares de números (por ejemplo, $(3,2)$) que no tienen una imagen definida. Similarmente, en $\mathbb{N}$ no se puede definir el cociente y, en este caso, tampoco la diferencia.

Ejercicio 9.4. Comprobar que la unión y la intersección sobre el conjunto de las partes de cualquier conjunto son operaciones asociativas y conmutativas y, en este caso, que la unión es distributiva respecto de la intersección y también en sentido contrario.

La composición de aplicaciones constituye un ejemplo importante de operación asociativa y no conmutativa. La asociatividad se comprueba fácilmente y, en cuanto a la conmutatividad, podemos considerar, por ejemplo

$$f,g : \mathbb{N} \longrightarrow \mathbb{N}$$

tales que, $f(n) = 2n$ y $g(m) = m+1$. Entonces, $(g \circ f)(n) = 2n+1$, mientras que $(f \circ g)(m) = 2(m+1)$.

Un conjunto con una operación binaria, independientemente de las propiedades de esta operación, puede admitir ciertos elementos que por su comportamiento respecto de la operación se llaman *singulares*. Así, dado un conjunto A y una operación binaria $\star$, se dice que $e \in A$ es un elemento *neutro* respecto de $\star$ si y sólo si

$$a \star e = e \star a = a \qquad \forall a \in A$$

Lema 9.5. En cada operación binaria existe como máximo un elemento neutro.

Demostración. Supongamos que e y e' fuesen dos elementos neutros respecto de $\star$. Entonces se tendría que verificar que $e' = e \star e' = e' \star e = e$; por tanto, si existe neutro, éste es único. □

Si A tiene elemento neutro e respecto de $\star$, entonces se dice que $a' \in A$ es un elemento *inverso* de $a \in A$ respecto de $\star$ si y sólo si $a \star a' = a' \star a = e$.

Lema 9.6. Si $\star$ es una operación asociativa sobre el conjunto A, y admite un elemento neutro $e \in A$, entonces cada elemento $a \in A$ admite como máximo un elemento inverso $a' \in A$.

Demostración. Si $a', a'' \in A$ fuesen dos inversos de $a \in A$, entonces

$$a' = a' \star e = a' \star (a \star a'') = (a' \star a) \star a'' = a''$$

□

La existencia de neutros e inversos respecto de las operaciones aritméticas elementales puede comprobarse fácilmente en los conjuntos de números con que se trabaja habitualmente. Así, tenemos:

1. En $\mathbb{N}$ no hay elemento neutro respecto de la suma y, por tanto, no tiene sentido hablar de inversos respecto de esta operación. Si consideramos el producto, el 1 es el elemento neutro. Como no existe ningún natural diferente del 1, que multiplicado por otro dé 1, ningún elemento (diferente de 1) tiene inverso.

2. Si consideramos la suma en $\mathbb{Z}$, tenemos el cero como neutro y $-a$ como inverso de $a \in Z$, mientras que con el producto, aunque también exista neutro, el 1, ningún elemento tiene inverso.

3. En el conjunto $\mathbb{Q}$, tanto la suma como el producto admiten elementos neutros e inversos respecto de las dos operaciones.

4. Las operaciones aritméticas elementales sobre $\mathbb{Z}_n$ admiten como neutros las clases del $[0]$ y del $[1]$ respectivamente. El inverso respecto de la suma de una clase $[a]$ es claramente la clase $[-a]$. La existencia de inversos respecto del producto no es tan evidente como en el caso de la suma; en el próximo capítulo veremos que $[a] \in \mathbb{Z}_n$ admite inverso respecto del producto si y sólo si $mcd(a,n) = 1$.

   Como ejemplo, si consideramos en $\mathbb{Z}_9$ los elementos 2, 4, 5, 7 y 8, estos tienen inverso, como es fácil comprobar, $(2 \times 5 \equiv 1 \pmod 9)$, $4 \times 7 \equiv 1 \pmod 9$, $(8 \times 8 \equiv 1 \pmod 9)$, mientras que no hay ningún entero s tal que $3 \times s \equiv 1 \pmod 9$ ni $6 \times s \equiv 1 \pmod 9$.

Ejemplos no numéricos de elementos singulares los encontramos al considerar:

1. El conjunto de las partes de un conjunto, $\wp(X)$, con la unión y la intersección como operaciones admite como neutros respectivos el $\emptyset$ y el propio conjunto X. Es fácil comprobar que ningún subconjunto no trivial de X admite inverso respecto de la unión ni respecto de la intersección.

2. El conjunto de las aplicaciones, $F(X)$, definidas desde un conjunto cualquiera X en él mismo respecto de la composición admite siempre la aplicación identidad como neutro, ya que para todo $x \in X$, y para toda $f \in F(X)$,

$$(f \circ Id)(x) = f(Id(x)) = f(x) = Id(f(x)) = (Id \circ f)(x)$$

   Recordemos que la aplicación inversa de $f \in F(X)$ sólo existe si f es biyectiva, entonces la existencia de aplicaciones inversas queda restringida al subconjunto de aplicaciones biyectivas, que denotamos como $F^*(X)$.

9.4 Estructuras algebraicas

En esta última sección se introduce la noción de estructura algebraica, así como también ciertos aspectos generales, teniendo en cuenta que en los capítulos sucesivos se desarrollarán con más precisión los modelos más importantes de estas estructuras.

La idea básica subyacente en la definición de estructura algebraica es la de un conjunto con una o varias operaciones, aunque puede intervenir más de un conjunto, así como también otros tipos de relaciones. En general, las operaciones definidas pueden ser n-arias, pero si no se especifica lo contrario, aquí consideraremos únicamente operaciones binarias y nos referiremos a ellas directamente como operaciones.

Una *estructura algebraica* es una n-tupla cuyos elementos son conjuntos y relaciones entre estos conjuntos, de las cuales se destacan en particular las operaciones y también, si se

quiere, los elementos singulares que puedan tener estos conjuntos respecto de las operaciones asociadas. Para denotarla podemos escribir

$$(X, Y, \dots, R_1, R_2, \dots, \star, \perp, \dots, e, e', \dots)$$

donde $X, Y, \dots$ son conjuntos, $R_1, R_2, \dots$ relaciones definidas en estos conjuntos, $\star, \perp, \dots$ son operaciones n-arias (en general) sobre estos conjuntos, y $e, e', \dots$ elementos singulares de estas operaciones.

De hecho, al largo de todo este capítulo se han estado utilizando ya ejemplos de estructuras algebraicas, entre las cuales tenemos:

1. $(\mathbb{N}, \leqslant)$. Relación de orden total sobre los naturales.
2. $(\mathbb{N}, =)$. Relación de equivalencia, también sobre los naturales.
3. $(\wp(X), \cup, \emptyset)$. La operación unión que tiene por neutro el conjunto vacío.
4. $(F(X), \circ, Id)$. La composición de aplicaciones con la aplicación identidad como neutro.
5. $(\mathbb{Q}, +, \cdot, 0, 1)$. La suma y el producto sobre los racionales con el 0 como neutro de la suma y el 1 como neutro del producto.

Es preciso mencionar que las estructuras más importantes están definidas sobre un único conjunto en el cual hay definidas una o dos operaciones. Los elementos singulares normalmente no se especifican si son fácilmente deducibles. A continuación daremos una clasificación ordenada de estas estructuras. Primero introduciremos aquellas que están definidas a partir de una única operación.

Dado un conjunto X y una operación $\star$ sobre X, diremos que la estructura algebraica $(X, \star)$ es un:

- *semigrupo* si y sólo si $\star$ es asociativa;
- *monoide* si y sólo si $\star$ es asociativa y X tiene elemento neutro;
- *grupo* si y sólo si $\star$ es asociativa, X tiene elemento neutro y cada elemento de X tiene inverso.

Si $\star$ es conmutativa diremos que la estructura correspondiente es abeliana o conmutativa.

Entre los ejemplos que se han tratado al largo del capítulo es rutinario comprobar la estructura algebraica que corresponde a algunos de ellos.

Ejercicio 9.7. Comprobar las siguientes afirmaciones.

1. $(\mathbb{Z}, \times)$ es un monoide abeliano.

2. $(\mathbb{Z}, +)$ es un grupo abeliano.
3. $(\wp(X), \cup)$ es también un monoide abeliano.
4. $(F(X), \circ)$ es un monoide no abeliano.
5. $(F^*(X), \circ)$ es un grupo no abeliano.

Dado un conjunto X y dos operaciones, $\star$ y $\perp$ sobre X, diremos que $(X, \star, \perp)$ es un:

- *anillo* si y sólo si $(X, \star)$ es un grupo abeliano, $\perp$ es asociativa y distributiva respecto de $\star$,
- *anillo unitario* si y sólo si es un anillo y $(X, \perp)$ tiene elemento neutro,
- *anillo unitario abeliano* si y sólo si es un anillo y $(X, \perp)$ tiene elemento neutro y $(X, \perp)$ es conmutativa,
- *cuerpo* si y sólo si es un anillo unitario abeliano y $(X, \perp)$ tiene elementos inversos.

De forma similar a como hemos hecho con los ejemplos sobre estructuras algebraicas con una única operación, podemos aprovechar aquí también ejemplos ya tratados con dos operaciones.

Ejercicio 9.8. Comprobar las afirmaciones siguientes.

1. $(\mathbb{Z}, +, \times)$ es un anillo unitario abeliano.
2. $(\mathbb{Z}_n, +, \times)$ es también un anillo unitario abeliano.
3. $(\mathbb{Q}, +, \times)$ es un cuerpo abeliano.
4. $(\mathbb{Z}_p, +, \times)$ es un cuerpo abeliano si y sólo si $p \in Z$ es un número primo.

Ejercicio 9.9. Comprobar que el conjunto de las aplicaciones entre números racionales, respecto de la suma y el producto, definidas a continuación, $(F(\mathbb{Q}), +, \times)$, tiene estructura de anillo unitario abeliano.

Para toda $f, g \in F(\mathbb{Q})$, y para todo $q \in \mathbb{Q}$, definimos:

$$\begin{array}{rcl} F(\mathbb{Q}) \times F(\mathbb{Q}) & \longrightarrow & F(\mathbb{Q}) \\ (f,g)(q) & \longrightarrow & (f+g)(q) = f(q) + g(q) \end{array}$$

$$\begin{array}{rcl} F(\mathbb{Q}) \times F(\mathbb{Q}) & \longrightarrow & F(\mathbb{Q}) \\ (f,g)(q) & \longrightarrow & (f \times g)(q) = f(q) \times g(q) \end{array}$$

Observar que la unicidad en la suma y el producto de números racionales se transmite a la suma y el producto de aplicaciones racionales. Es decir, estas operaciones están bien definidas.

Una vez sabemos lo que significa que un conjunto X tenga una determinada estructura algebraica, es natural plantearse la cuestión siguiente: al considerar un subconjunto $Y \subset X$, ¿es posible que esta estructura se mantenga al restringirla a Y? Esta cuestión da lugar a un concepto muy utilizado en este ámbito, el de subestructura.

Dada una estructura algebraica $(X, \star)$ y un subconjunto $X' \subset X$, se dice que $(X', \star)$ es una *subestructura* de la anterior si y sólo si la operación $\star$ es cerrada en X', es decir,

$$x' \star y' = z' \in X' \qquad \forall x', y' \in X'$$

y además mantiene las propiedades y los elementos singulares que definen la estructura original.

Observar que la asociatividad y la conmutatividad de una operación se mantienen en cualquier subconjunto del conjunto de partida.

De forma general, dada una estructura algebraica,

$$(X, Y, \dots, R_1, R_2, \dots, \star, \perp, \dots, e, e', \dots)$$

y una familia de subconjuntos $X' \subset X$, $Y' \subset Y$, ..., se dice que la estructura algebraica

$$(X', Y', \dots, R_1, R_2, \dots, \star, \perp, \dots, e, e', \dots)$$

es una subestructura de la estructura original si y sólo si las relaciones, las operaciones y los elementos singulares originales se mantienen con las mismas propiedades al considerar la estructura original restringida a la familia de subconjuntos.

Entre los ejemplos anteriores podemos observar que algunas de las estructuras algebraicas son subestructuras de otras.

1. $(\mathbb{N}, \times)$ es un submonoide abeliano del monoide abeliano $(\mathbb{Z}, \times)$. Pero, si consideramos como operación la suma, la estructura de grupo que hay en $\mathbb{Z}$ se pierde en $\mathbb{N}$, ya que este último conjunto no contiene los elementos inversos.

2. $(\mathbb{Z}, +)$ es un subgrupo abeliano del grupo abeliano $(\mathbb{Q}, +)$. Pero no es cierto que el anillo unitario abeliano $(\mathbb{Z}, +, \times)$ sea una subestructura del cuerpo abeliano $(\mathbb{Q}, +, \times)$, ya que los elementos inversos respecto del producto en $\mathbb{Q}$ no están en $\mathbb{Z}$.

Dos estructuras algebraicas diferentes pueden compartir características similares. Si una estructura está definida sobre un conjunto X y una estructura similar lo está sobre un conjunto

Y, la similitud de estas estructuras se pone de manifiesto por medio de una aplicación entre los conjuntos X e Y que conserva las características de la estructura.

Dadas dos estructuras algebraicas $(X,\star)$ e $(Y,\perp)$, la aplicación $f : X \longrightarrow Y$ es un *morfismo* de $(X,\star)$ en $(Y,\perp)$ si y sólo si

$$f(x)\perp f(x') = f(x\star x') \qquad \forall x,x' \in X$$

La definición dice que la imagen de la composición de dos elementos coincide con la composición de las imágenes de cada uno de ellos.

Si $f : X \longrightarrow Y$ es un morfismo de $(X,\star)$ en $(Y,\perp)$, se dice que $(f(X),\perp)$ es la *imagen homomórfica* de X por f.

Observar que la operación $\perp$ será siempre cerrada en $f(X)$.

Por ejemplo, $(\mathbb{Z},\times)$ y $(\mathbb{N}\cup\{0\},\times)$ son homomórficos, ya que la aplicación

$$|\,| : \mathbb{Z} \longrightarrow \mathbb{N}\cup\{0\}$$

que envía cada entero z a su módulo $|z|$, satisface la condición de morfismo, es decir,

$$|z\times z'| = |z|\times|z'| \qquad \forall z,z' \in \mathbb{Z}$$

Como los morfismos son aplicaciones, éstas pueden ser inyectivas, exhaustivas y biyectivas. En cada caso reciben también nombres especiales.

Si f es un morfismo de $(X,\star)$ en $(Y,\perp)$, entonces diremos que f es un:

- *monomorfismo* si y sólo si f es inyectiva,
- *epimorfismo* si y sólo si f es exhaustiva,
- *isomorfismo* si y sólo si f es biyectiva.

Como ejemplos de esta clasificación podemos considerar los siguientes:

1. La aplicación identidad $Id : (\mathbb{N},\times) \longrightarrow (\mathbb{Z},\times)$, que envía cada número natural a él mismo, es un monomorfismo.
2. La aplicación $|\,| : (\mathbb{Z},\times) \longrightarrow (\mathbb{N}\cup\{0\},\times)$, que envía cada número entero z a su módulo $|z|$, es un epimorfismo.
3. La congruencia módulo n, $[\,] : (\mathbb{Z},+) \longrightarrow (\mathbb{Z}_n,+)$, que envía cada entero z a su clase $[z]$, es un ejemplo importante de epimorfismo.

Como una congruencia módulo n es una relación de equivalencia, ésta induce una partición del conjunto en clases y da lugar al conjunto cociente, que permite introducir la noción de *estructura cociente*. Más concretamente y en general:

Una relación de equivalencia R sobre una estructura $(X,\star)$ se dice que es *compatible* respecto de una operación $\star$ si y sólo si

$$xRx',\ yRy' \quad \Rightarrow \quad (x\star y)R(x'\star y')$$

Es decir, si la operación no depende de los representantes elegidos.

Si R es compatible con $\star$, entonces se dice que R induce una *estructura cociente*, $(X/R,\star_R)$ donde X/R es el conjunto de las clases de equivalencia de X módulo R y $\star_R$ es la operación inducida por R, es decir,

$$[x\star y] = [x]\star_R[y] \qquad \forall x,y\in X$$

Observar que no hay ambigüedad en la definición de $\star_R$, ya que no depende de los representantes escogidos en cada clase. Es por ello que se ha introducido la noción de compatibilidad. Ya hemos visto que la relación de congruencia módulo n en los enteros es compatible con la suma y con el producto. Justamente, $(\mathbb{Z}_n,+_n,\times_n)$ es la estructura cociente del anillo unitario $(\mathbb{Z},+,\times)$ por la relación de congruencia módulo n.

La compatibilidad de una relación respecto de una operación es una propiedad muy restrictiva. Es fácil encontrar ejemplos de particiones no compatibles con ciertas operaciones. Así, en $\mathbb{Z}$, la partición $A_1=\{1,2\}$ y $A_2=\mathbb{Z}\setminus A_1$ no es compatible con la suma, ya que al operar dos elementos de la clase A_1 podemos obtener un nuevo elemento de la misma clase $[1+1]=[2]=A_1$, o bien un elemento de la otra clase $[1+2]=[3]=A_2$.

Es interesante observar que la estructura algebraica $(X/R,\star_R)$ es una imagen homomórfica de la estructura $(X,\star)$ considerando el epimorfismo

$$f: X \longrightarrow X/R$$

que envía cada $x\in X$ a su clase $[x]$. Habitualmente, éste se llama *epimorfismo natural* de X sobre X/R.

A todo morfismo de una estructura algebraica sobre ella misma se le llama *endomorfismo*. Si el morfismo es biyectivo entonces se llama *automorfismo*.

La noción de morfismo se extiende a todas las estructuras algebraicas. Por ejemplo, un morfismo de la estructura $(X,\star,\perp)$ en la estructura $(Y,\star',\perp')$ es una aplicación $f: X\longrightarrow Y$ que satisface para todo $x,y\in X$,

$$f(x\star y)=f(x)\star' f(y) \quad y \quad f(x\perp y)=f(x)\perp' f(y)$$

es decir, respeta todas las operaciones y consiguientemente todas las propiedades que involucren a estas operaciones.

En general, la imagen homomórfica de una estructura algebraica es otra estructura con conjuntos, relaciones, operaciones y elementos singulares que se corresponden uno a uno con cada elemento de la estructura inicial. Además, las propiedades especiales de la estructura original se mantienen en la estructura imagen. Así, si $\star$ es asociativa en $(X, \star, \perp, e)$, $\star'$ lo es también en la imagen homomórfica $(f(X) \subset X', \star', \perp', e')$, como se puede comprobar fácilmente. En particular, el elemento neutro de la estructura original va a parar al elemento neutro de la estructura imagen, como se demuestra a continuación.

Lema 9.10. Dadas dos estructuras algebraicas $(X, \star, e)$ e $(Y, \perp, e')$ con elementos neutros respectivos e y e' y un morfismo $f : X \longrightarrow Y$, se cumple siempre que $e' = f(e)$.

Demostración. Para todo $x \in X$, la imagen homomórfica de $x \star e = x$ es

$$f(x) \perp f(e) = f(x)$$

y, por tanto, $f(e) = e'$. □

Capítulo 10

Grupos

1. Definiciones y propiedades
2. Grupos abelianos finitos
3. Grupos de permutaciones
4. Digrafos de Cayley
5. Teoría de enumeración de Pólya

La estructura de grupo es la más simple de las que se considerarán y también una de las que tiene una incidencia más extensa en sus aplicaciones.

En la sección 1 de este capítulo se revisa la definición de grupo que ya se ha enunciado en el capítulo anterior, se introduce la terminología básica y se ven las primeras propiedades. La sección 2 está dedicada al estudio de los grupos abelianos finitos, de los cuales se describe la estructura. Los grupos de permutaciones, y en particular los grupos simétrico y alternado, merecen una atención especial y en la sección 3 se consideran algunos aspectos algebraicos y combinatorios de estos grupos. Los grafos de Cayley proporcionan una manera de visualizar la estructura de un grupo. La interrelación entre la teoría de grupos y la teoría de grafos por medio de los grafos de Cayley es muy enriquecedora para ambas teorías y está relacionada con la descripción de un grupo mediante lo que se llaman *presentaciones*. Estas cuestiones se tratan en la sección 4. El capítulo se acaba con una aplicación de la teoría de grupos a un problema de enumeración que se conoce como teoría de Pólya. El objetivo es enumerar configuraciones diferentes sobre un conjunto que goza de ciertas simetrías.

10.1 Definiciones y propiedades

Tal como se ha introducido en la última sección del capítulo anterior, la estructura de grupo viene dada por la definición siguiente.

Un *grupo* es un par $(G,\cdot)$ formado por un conjunto y una operación binaria que cumple:

G0 La operación es cerrada, es decir, $a\cdot b\in G$, para todo $a,b\in G$.

G1 La operación es asociativa, es decir, $(a\cdot b)\cdot c=a\cdot(b\cdot c)$, para todo $a,b,c\in G$.

G2 El conjunto G tiene elemento neutro, que se denotará por e, respecto de la operación.

G3 Cada elemento de G tiene inverso respecto de la operación. El inverso del elemento $a\in G$ se denotará por a^{-1}.

Si además la operación es conmutativa, se dice que el grupo es *abeliano*.

Las propiedades descritas en los axiomas $G1$, $G2$ y $G3$ son una abstracción de las propiedades que satisfacen las operaciones elementales en los conjuntos de números. Así, los conjuntos de números enteros o racionales con la suma, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, son ejemplos de grupos abelianos. De la misma manera, el conjunto de números racionales con el producto, $(\mathbb{Q}^*,\cdot)$, tiene también estructura de grupo abeliano.

Por abuso de notación nos referiremos a menudo a un grupo indicando sólo su conjunto base, dejando de lado la referencia a la operación. Así pues, hablaremos del grupo G en lugar de hablar del grupo $(G,\cdot)$, de manera que debe quedar sobreentendido a qué operación se hace referencia. Siguiendo los modelos aritméticos de los conjuntos de números, la notación genérica de la operación es '$\cdot$' (notación multiplicativa) y entonces el elemento neutro se denota por 'e' o por '1'. A menudo se escribe 'ab' en lugar de '$a\cdot b$'. Cuando el grupo es abeliano, la operación se denota por '$+$' (notación aditiva), el elemento neutro se denota por '0' y el inverso de x por '$-x$'.

Algunas de las propiedades elementales que se derivan de los axiomas de grupo son las siguientes:

Proposición 10.1. En un grupo $(G,\cdot)$ se cumple:

1. El elemento neutro es único.
2. El elemento inverso de cada elemento es único.
3. El inverso de a^{-1} es a, es decir, $(a^{-1})^{-1}=a$.
4. El inverso de $a\cdot b$ es $b^{-1}\cdot a^{-1}$, es decir, $(a\cdot b)^{-1}=b^{-1}\cdot a^{-1}$.
5. La ecuación $a\cdot x=b$ tiene una solución única $x=a^{-1}\cdot b\in G$.

Ejercicio 10.2. Demostrar las propiedades enunciadas en la proposición anterior e indicar cuáles de los axiomas de grupo se usan.

La última de las propiedades, que asegura que en un grupo una ecuación del tipo $ax = b$ tiene siempre una solución única en x, es característica de la estructura de grupo. Este punto de vista es importante ya que, históricamente, los objetivos iniciales del álgebra estaban ligados a la resolución de ecuaciones.

Es preciso observar también el cambio de orden en la escritura de los elementos en la propiedad 3 de la proposición. Si G es un grupo abeliano, se puede escribir $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$. Esta relación aparentemente más natural puede dejar de cumplirse si el grupo no es abeliano.

En este capítulo nos centraremos sobre todo en grupos finitos, es decir, en los que el conjunto de base del grupo es finito.

Una de las maneras de representar la estructura de un grupo finito es dando la tabla de la operación. Por ejemplo, la tabla siguiente corresponde a la de un grupo de cuatro elementos, $G = \{e, a, b, c\}$.

Tabla 10.1: Tabla de un grupo de cuatro elementos

·	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

En la tabla de un grupo se pueden visualizar fácilmente los dos últimos axiomas de la estructura: la fila y la columna que corresponden al elemento neutro son idénticas a la fila y la columna cero respectivamente. Además, en cada fila y en cada columna aparece una única vez este elemento neutro al operar cada elemento con su único inverso. Otra propiedad característica más de la tabla de un grupo es que en cada una de las filas y de las columnas aparece una única vez cada uno de los elementos del grupo. Esto es porque si $x \cdot y = x \cdot z$, multiplicando los dos lados de la igualdad por x^{-1} obtenemos $y = z$. La tabla muestra también si el grupo es abeliano, caso en el que hay una simetría respecto de la diagonal principal como en la tabla anterior. La propiedad asociativa es la que no queda reflejada en la tabla y se tiene que verificar de manera exhaustiva (y a menudo tediosa).

Ejercicio 10.3. Usando las propiedades que se han mencionado de la tabla de un grupo, demostrar que hay un único grupo de dos elementos y un único grupo de tres elementos.

Subgrupos

De acuerdo con la noción genérica de subestructura, se dice que un subconjunto $H \subset G$ es un *subgrupo* de G si con la operación '$\cdot$' restringida a los elementos de H se satisfacen los axiomas de grupo. Por ejemplo, el subconjunto formado por los elementos $H = \{e, b\}$ en el grupo de la tabla anterior (10.1) es un subgrupo, ya que la operación restringida a este subconjunto es cerrada, tiene elemento neutro e y el elemento b tiene como inverso el mismo b. La tabla de este subgrupo está representada en 10.2.

Tabla 10.2: Subgrupo del grupo de la tabla 10.1

$\cdot$	e	b
e	e	b
b	b	e

De hecho, 10.2 corresponde a la tabla del único grupo de dos elementos. En realidad no es preciso comprobar los cuatro axiomas de grupo para determinar si un subconjunto es o no un subgrupo.

Proposición 10.4. Sea $(G, \cdot)$ un grupo y $H \subset G$. Entonces, $(H, \cdot)$ es un subgrupo de $(G, \cdot)$ si y sólo si se satisface la relación

$$a \cdot b^{-1} \in H \qquad \forall a, b \in H$$

Si G es finito, $(H, \cdot)$ es un subgrupo si y sólo si la operación es cerrada en H.

Demostración. Supongamos que se satisface la relación. Si $a \in H$, tomando $b = a$ obtenemos $a \cdot a^{-1} = e \in H$ de manera que H contiene el elemento neutro. Entonces, tomando $a = e$, para cualquier elemento $b \in H$, $e \cdot b^{-1} = b^{-1} \in H$, de manera que cualquier elemento de H tiene inverso en H. Dados dos elementos $a, b \in H$, tenemos que $a \cdot (b^{-1})^{-1} = ab \in H$, de manera que la operación es cerrada. Finalmente, la propiedad asociativa se hereda directamente de la misma propiedad en G. Recíprocamente, si $(H, \cdot)$ es un subgrupo de $(G, \cdot)$, está claro que se satisface la relación, es decir, si $a, b \in H$ entonces $a, b^{-1} \in H$ y por tanto $a \cdot b^{-1} \in H$. Finalmente, en caso que G sea finito, basta que la operación sea cerrada en H. La demostración se deja como ejercicio. □

Ejercicio 10.5. Demostrar que en el enunciado de la proposición anterior se puede substituir la relación $a \cdot b^{-1} \in H$ para todo $a, b \in H$ por

$$a^{-1} \cdot b \in H \qquad \forall a, b \in H$$

De manera simplificada se escribe $H < G$ para denotar que $(H, \cdot)$ es un subgrupo de $(G, \cdot)$. Está claro que el subconjunto formado sólo por el elemento neutro es un subgrupo de G. Todo el grupo G es también un subgrupo de él mismo. Estos dos se llaman subgrupos *triviales* de G, mientras que los subgrupos no triviales se llaman también subgrupos *propios*.

Ejercicio 10.6. Demostrar que $(\mathbb{Z}, +) < (\mathbb{Q}, +)$.

Ejercicio 10.7. Demostrar que $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$, el conjunto de múltiplos de un número entero n, es un subgrupo de $(\mathbb{Z}, +)$.

Un subgrupo propio H de G induce en G una relación de equivalencia R_H definida por

$$aR_Hb \Leftrightarrow a^{-1} \cdot b \in H, \qquad \forall a, b \in G$$

Ejercicio 10.8. Demostrar que R_H es efectivamente una relación de equivalencia.

De acuerdo con la última proposición (y el ejercicio que sigue), si $a, b \in H$, entonces $a^{-1} \cdot b \in H$, de manera que aR_Hb. Recíprocamente, si aR_Hb y $a \in H$, entonces $b = a \cdot (a^{-1}b) \in H$. Esto quiere decir que los elementos de H forman una de las clases de equivalencia. De manera similar se puede ver que la clase de un elemento $a \in G$ es justamente el conjunto de los elementos $aH = \{ax, x \in H\}$ y que todas ellas se pueden describir de esta manera.

Ejercicio 10.9. Demostrar esta última afirmación: Si H es un subgrupo de G, las clases de equivalencia de la relación R_H son los conjuntos de la forma $aH = \{ax, x \in H\}$ para cada $a \in G$.

Por ejemplo, si G es el grupo de cuatro elementos de la tabla 10.1 y H el subgrupo de dos elementos de la tabla 10.2, $H = b + H = \{e, b\}$ y $a + H = \{a, c\}$ son las clases de equivalencia de la relación R_H (usamos la notación aditiva).

A causa de su forma, las clases de equivalencia por la relación R_H se llaman *clases laterales por la izquierda* de G módulo H. Está claro que todas las clases tienen el mismo cardinal (si aH, bH son dos clases, la aplicación $f : aH \longrightarrow bH$ dada por $f(ax) = bx$ es una biyección). Si G es un grupo finito, el número de clases se llama *índice* de H en G y se denota por $|G : H|$. Así pues,

$$|G : H| = \frac{|G|}{|H|}$$

Esto lleva a uno de los primeros resultados que se obtuvieron en la teoría de grupos.

Teorema 10.10 (Teorema de Lagrange). Sea G un grupo finito y H un subgrupo propio de G. Entonces $|H|$ es un divisor de $|G|$.

El teorema de Lagrange limita el número de subgrupos que puede tener un grupo. Por ejemplo, un grupo de orden primo no puede tener ningún subgrupo propio. El recíproco del teorema de Lagrange no es necesariamente cierto: el hecho que k sea un divisor de $|G|$ no quiere decir que G tenga que tener un subgrupo de orden k (o que no pueda tener más de uno).

Si $H < G$, habríamos podido definir también la relación de equivalencia ${}_HR$ dada por

$$a\,{}_HR\,b \Leftrightarrow a \cdot b^{-1} \in H$$

En este caso, las clases de equivalencia son Ha, $a \in G$ y se llaman *clases laterales por la derecha* de G módulo H. Si G es un grupo abeliano, entonces $aH = Ha$, para todo $a \in G$; en este caso, las clases laterales por la derecha coinciden con las clases por la izquierda. Si G no es abeliano, las clases por la derecha no coinciden necesariamente con las clases por la izquierda y las dos relaciones dan lugar a particiones diferentes.

Si $xH = Hx$ para todo $x \in G$, se dice que H es un subgrupo *normal* de G y se indica escribiendo $H \triangleleft G$. En este caso, la operación '$\cdot$' del grupo G induce una operación en el conjunto de G/H de clases de equivalencia definida como

$$(xH) \cdot (yH) = (x \cdot y)H$$

Ejercicio 10.11. Comprobar que, si H es un subgrupo normal de G, la operación está bien definida, es decir, el resultado no depende del representante que se escoge en cada clase. Más concretamente, si $xH = x'H$ e $yH = y'H$, entonces $(x \cdot y)H = (x' \cdot y')H$. Esto no es necesariamente cierto si H no es un subgrupo normal.

No es difícil comprobar que el conjunto G/H con esta operación vuelve a tener estructura de grupo. De hecho, la clase eH es su elemento neutro y el elemento inverso de xH es $x^{-1}H$. Este grupo se llama *grupo cociente* de G módulo H.

Ejercicio 10.12. Demostrar que, efectivamente, si $H \triangleleft G$, entonces G/H con la operación $(aH) \cdot (bH) = abH$ tiene estructura de grupo.

En el capítulo anterior hemos visto un ejemplo importante de grupo cociente. Recordemos que la relación de congruencia módulo n en el conjunto $\mathbb{Z}$ de los números enteros está definida como

$$x \equiv y \pmod{n} \Leftrightarrow n|(x-y)$$

Si llamamos $n\mathbb{Z}$ al subgrupo de los múltiplos de n introducido en el ejercicio 10.7, vemos que la relación de congruencia es una relación de equivalencia módulo este subgrupo. Como $(\mathbb{Z},+)$ es un grupo abeliano, $n\mathbb{Z}$ es un subgrupo normal, de manera que se puede definir el grupo cociente $\mathbb{Z}/n\mathbb{Z}$, que habitualmente se denota por $\mathbb{Z}_n$, con la operación

$$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (a+b) + n\mathbb{Z}$$

Tanto $\mathbb{Z}$ como $n\mathbb{Z}$ son grupos infinitos, pero $\mathbb{Z}_n$ es un grupo finito de orden n.

Morfismos de grupos

Particularizaremos ahora al caso de la estructura de grupo otra de las definiciones generales que se han dado en el capítulo anterior. Una aplicación

$$f : G \longrightarrow H$$

entre dos grupos $(G,\cdot)$, $(H,\circ)$ es un *morfismo* de grupos si

$$f(a\cdot b) = f(a)\circ f(b) \qquad \forall a,b \in G$$

es decir, es lo mismo operar dos elementos en G y aplicar la función f que aplicar la función f a los dos elementos y operar las imágenes en H.

Ejercicio 10.13. Sea $f : G \longrightarrow H$ un morfismo de grupos.

1. Demostrar que $f(e_G) = e_H$.
2. Demostrar que $f(a^{-1}) = (f(a))^{-1}$.

Si la función f es biyectiva, se dice que es un *isomorfismo* de grupos y también que los dos grupos $(G,\cdot)$ y $(H,\circ)$ son *isomorfos*. Dos grupos isomorfos tienen las mismas propiedades algebraicas y, desde el punto de vista de la estructura, difieren sólo en la denominación de sus elementos. Por ejemplo, el conjunto $H = \{0,1\}$ con la operación 'o exclusiva' que tiene por tabla:

$\oplus$	0	1
0	0	1
1	1	0

es isomorfo al grupo representado en la tabla 10.2, donde el isomorfismo viene dado por $f(e) = 0$ y $f(b) = 1$. Desde el punto de vista de la estructura, los dos grupos son entonces idénticos.

Ejercicio 10.14. Sea $f : G \longrightarrow H$ un morfismo del grupo $(G,\cdot)$ en el grupo $(H,\circ)$.

1. Demostrar que el subconjunto $G_0 = \{x \in G \mid f(x) = e_H\}$ es un subgrupo de G. Demostrar además que se trata de un subgrupo normal.
2. Demostrar que el subconjunto $Im\, f$ es un subgrupo de H.
3. Demostrar que f es un morfismo inyectivo si y sólo si G_0 es el subgrupo trivial $G_0 = \{e_G\}$.
4. Demostrar que la aplicación $\hat{f} : G/G_0 \longrightarrow Im\, f$ dada por $\hat{f}(x\cdot G_0) = f(x)$ está bien definida y es un isomorfismo de grupos.

Producto cartesiano de grupos

El producto cartesiano de grupos proporciona una manera de generar nuevos grupos a partir de otros conocidos.

Dados dos grupos $(G_1, \star_1, e_1)$ y $(G_2, \star_2, e_2)$, podemos definir una operación $\star$ sobre $G_1 \times G_2$ de forma natural:

$$(g_1, g_2) \star (h_1, h_2) = (g_1 \star_1 h_1, g_1 \star_2 h_2)$$

Se puede comprobar fácilmente que este producto es asociativo, como consecuencia de la asociatividad en los grupos originales. Está claro que (e_1, e_2) es el elemento neutro de esta nueva operación y que, para cada $(g_1, g_2) \in G_1 \times G_2$, $(g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$ es su inverso. Así,

$$(G_1 \times G_2, \star)$$

es un grupo que se llama *producto cartesiano* de los grupos G_1 por G_2.

Ejercicio 10.15. Demostrar que $G_1 \times G_2$ es abeliano si y sólo si lo son G_1 y G_2.

Ejercicio 10.16. Comprobar que $\mathbb{Z}_2 \times \mathbb{Z}_2$ es un grupo no isomorfo a $\mathbb{Z}_4$.

De forma similar se puede definir el producto cartesiano de n grupos, $G_1, G_2, \ldots, G_n$,

$$G_1 \times G_2 \times \cdots \times G_n$$

Ejercicio 10.17. Comprobar que $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ es un grupo isomorfo a $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3$.

De los subgrupos propios de G_1 y G_2 podemos obtener también de manera natural subgrupos propios de $G_1 \times G_2$.

Ejercicio 10.18. Si H_1 y H_2 son subgrupos propios de G_1 y G_2 respectivamente, entonces $H_1 \times H_2$ es un subgrupo propio de $G_1 \times G_2$.

En particular, G_1 y G_2 se pueden considerar subgrupos de $G_1 \times G_2$ por medio de las identificaciones siguientes:

$$\begin{aligned} G_1 &\leftrightarrow G_1' = G_1 \times \{e_2\} \\ G_2 &\leftrightarrow G_2' = \{e_1\} \times G_2 \end{aligned}$$

Es inmediato ver que estas identificaciones representan isomorfismos que identifican cada $g_1 \in G_1$ con $(g_1, e_2) \in G_1'$ y, similarmente, cada $g_2 \in G_2$ con $(e_1, g_2) \in G_2'$. Así, cada elemento $(g_1, g_2) \in G_1 \times G_2$ se identifica de manera única con $((g_1, e_2), (e_1, g_2)) \in G_1' \times G_2'$. Es preciso observar que, $G_1' \cap G_2' = (e_1, e_2)$ y además se cumple que $(g_1, e_2) \star (e_1, g_2) = (e_1, g_2) \star (g_1, e_2)$ para todo $g_1 \in G_1$ y $g_2 \in G_2$.

Recíprocamente, nos podemos plantear la cuestión siguiente: ¿es posible expresar un grupo G como producto cartesiano de otros grupos de órdenes (evidentemente) más pequeños (y por tanto más manejables)?

Esta cuestión sugiere la definición siguiente. Se dice que un grupo G es *producto directo* de sus subgrupos H y H' si

1. $G = \{hh' \mid h \in H, h' \in H'\}$;

2. $H \cap H' = \{e\}$, e es el elemento neutro de G;

3. H y H' son subgrupos normales en G.

En particular, el producto cartesiano $G = G_1 \times G_2$ es también el producto directo de los subgrupos G'_1 y G'_2 de G,

$$G = G_1 \times G_2 \simeq G'_1 \times G'_2$$

de manera que las nociones de producto cartesiano y producto directo de grupos son equivalentes.

Observar que, si G es abeliano, la tercera condición la cumple cualquiera de sus subgrupos. Así, para obtener una descomposición de G como producto directo de otros grupos, será preciso buscar entre los subgrupos que tengan intersección trivial. En este caso, se usa a veces $G = H \oplus H'$ para denotar que el producto directo de H y H' es abeliano, siguiendo la costumbre de utilizar la notación aditiva en el caso de grupos abelianos.

Así, por ejemplo, $(\mathbb{Z}_6, +)$ tiene dos subgrupos propios,

$$\begin{aligned} H &= \{0,3\} \simeq \mathbb{Z}_2 \\ H' &= \{0,2,4\} \simeq \mathbb{Z}_3 \end{aligned}$$

cuya intersección es el elemento neutro de $(\mathbb{Z}_6, +)$. Podemos obtener los elementos de $\mathbb{Z}_6$ a partir de los elementos de $\mathbb{Z}_2 \times \mathbb{Z}_3$, mediante la identificación que figura a continuación:

$\mathbb{Z}_6$	$\leftrightarrow$	$\mathbb{Z}_2 \times \mathbb{Z}_3$
0	$\leftrightarrow$	(0,0)
1	$\leftrightarrow$	(1,1)
2	$\leftrightarrow$	(0,2)
3	$\leftrightarrow$	(1,0)
4	$\leftrightarrow$	(0,1)
5	$\leftrightarrow$	(1,2)

Tabla 10.3: Tabla de $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$

+	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(0,0)	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(1,1)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)	(0,0)
(0,2)	(0,2)	(1,0)	(0,1)	(1,2)	(0,0)	(1,1)
(1,0)	(1,0)	(0,1)	(1,2)	(0,0)	(1,1)	(0,2)
(0,1)	(0,1)	(1,2)	(0,0)	(1,1)	(0,2)	(1,0)
(1,2)	(1,2)	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)

Con esta identificación es fácil comprobar que la tabla 10.3 correspondiente a

$$(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$$

coincide con la tabla de $(\mathbb{Z}_6, +)$.

Por tanto, podemos afirmar que $\mathbb{Z}_6 = H_1 \oplus H_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$.

Ejercicio 10.19. Comprobar que $\mathbb{Z}_{12} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_3$. Comprobar también que $\mathbb{Z}_{12}$ no es producto directo de $\mathbb{Z}_2$ y $\mathbb{Z}_6$. ¿Por qué?

En la sección siguiente se usarán descomposiciones en productos directos para obtener la clasificación de los grupos abelianos.

10.2 Grupos abelianos finitos

En esta sección se describe una clase importante de grupos finitos: los grupos abelianos. Los grupos abelianos más simples son los grupos *cíclicos*, que se verán en primer lugar. A continuación se verá que todos los grupos abelianos se pueden expresar como productos directos de grupos cíclicos.

Grupos cíclicos

Los grupos cíclicos proporcionan el ejemplo más sencillo de grupo finito. Para introducirlos se considera primero el concepto de orden de un elemento en un grupo. Sea G un grupo finito y g un elemento de G. Indicaremos por

$$g^k = \underbrace{gg\ldots g}_{k}$$

Consideremos la sucesión de elementos $g, g^2, g^3, \ldots, g^k, \ldots$. Como el grupo es finito, en esta sucesión no todos los elementos pueden ser diferentes, de manera que para algunos índices m, n tendremos $g^m = g^n$. Supongamos que $m < n$. Multiplicando ambos lados de la igualdad por $(g^m)^{-1} = g^{-m}$, obtenemos $g^{n-m} = e$. Así pues, tenemos:

Proposición 10.20. Si G es un conjunto finito y $g \in G$, existe un entero k tal que $g^k = e$.

La proposición anterior justifica la definición siguiente.

Sea G un grupo finito y $g \in G$. Se llama *orden* de g, y se indica por $|g|$, al menor número natural k para el cual $g^k = e$.

Si g tiene orden k, entonces los elementos $g, g^2, \ldots, g^{k-1}, g^k = e$ son todos diferentes. Efectivamente, si hubiese dos iguales, $g^p = g^q, p < q < k$, entonces $g^{q-p} = e$, contrariamente al hecho que k es el menor natural con esta propiedad. Además, $g^m = g^{m+k}$ para todo $m \in \mathbb{N}$, de manera que la secuencia infinita de potencias de g tiene período k, es decir, los elementos de la secuencia se repiten cada k posiciones. Está claro que el producto de dos potencias de g es otra potencia de g, de manera que la operación del grupo es cerrada en el subconjunto $H = \{g, g^2, \ldots, g^{k-1}, g^k = e\}$. Según la proposición 10.4, tenemos el resultado siguiente.

Proposición 10.21. Sea G un grupo finito y $g \in G$ un elemento de orden k. Entonces

$$H = \{g, g^2, \ldots, g^{k-1}, g^k = e\}$$

es un subgrupo de G de orden $k = |g|$.

En particular, según el teorema de Lagrange, tenemos:

Corolario 10.22. Sea G un grupo finito y $g \in G$. Entonces $|g|$ es un divisor de $|G|$.

Al subgrupo H de las potencias de un elemento $g \in G$ se lo llama subgrupo *generado* por g, y también se dice que g *genera* H. La estructura cíclica de este grupo sugiere la definición siguiente.

Un grupo finito G es *cíclico* si contiene un elemento g que genera todo el grupo, es decir, todos los elementos de G se expresan como potencia de g.

Ejercicio 10.23. Demostrar que un grupo cíclico es abeliano.

Ejercicio 10.24. Sean G y H dos grupos cíclicos del mismo orden k, generados por los elementos $g \in G$ y $h \in H$ respectivamente. Demostrar que la aplicación $f : G \longrightarrow H$ definida por $f(g^n) = h^n, n = 1, 2, \ldots, k$ es un isomorfismo de grupos.

Según el enunciado de este último ejercicio, vemos que, salvo isomorfismo, hay como mucho un único grupo cíclico para cada orden k. Vamos a ver que hay efectivamente uno para cada orden.

Proposición 10.25. El grupo $\mathbb{Z}_n$ es un grupo cíclico de orden n.

Demostración. Cualquier elemento $k+n\mathbb{Z} \in \mathbb{Z}_n$ se puede escribir como $k+n\mathbb{Z} = k(1+n\mathbb{Z})$, de manera que la clase del 1 genera todo el grupo. □

Los grupos cíclicos aparecen en muchas y diversas aplicaciones, de modo que resulta útil adquirir una cierta habilidad para operar en estos grupos (lo que se llama *aritmética modular*). La manera habitual de trabajar en estos grupos consiste en tomar como representantes de las n clases los enteros de 0 a $n-1$ y efectuar la suma ordinaria entre estos elementos, buscando después el representante correspondiente. Así, por ejemplo, los grupos cíclicos de órdenes 4 y 5 tienen las tablas siguientes:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Así pues, hay un y sólo un grupo cíclico de orden n para cada entero positivo, el grupo $\mathbb{Z}_n$. Este es el único grupo de orden n cuando n es un número primo.

Proposición 10.26. Si p es un número primo, hay un único grupo de orden p y este es cíclico.

Demostración. Sea G un grupo de orden p y g un elemento cualquiera de G diferente de e. Según el corolario 10.22, el orden de g es un divisor de $|G| = p$. Como p es primo, tiene que ser $|g| = p$, de manera que el subgrupo generado por g es todo G. □

Los grupos cíclicos tienen otra particularidad en relación al teorema de Lagrange: para cada divisor k de n, existe un único subgrupo de $\mathbb{Z}_n$ de orden k. Esto se puede ver a partir de las proposiciones siguientes.

Proposición 10.27. Cualquier subgrupo de un grupo cíclico es cíclico.

Proposición 10.28. Sea k un divisor de n y $h = n/k$. El conjunto de múltiplos de h en $\mathbb{Z}_n$ forma un subgrupo de orden k.

Ejercicio 10.29. Demostrar las proposiciones anteriores y deducir que para cada divisor k de n hay un único subgrupo de orden k de $\mathbb{Z}_n$.

Proposición 10.30. Si n y m son enteros primos entre sí, entonces

$$\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$$

Este resultado es consecuencia de la proposición 10.33 que veremos más adelante. En general, $\mathbb{Z}_n$ es isomorfo al producto directo de los subgrupos cíclicos que tienen órdenes divisores de n y estos órdenes son primos entre sí.

Teorema 10.31. Sea $\mathbb{Z}_n$ un grupo cíclico de orden $n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$, donde p_i son números primos diferentes. Entonces,

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_s^{n_s}}$$

Así, por ejemplo, sabemos ya que $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$. Si observamos la tabla 10.3, podemos comprobar que $(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ genera todo $\mathbb{Z}_2 \times \mathbb{Z}_3$ y por tanto deducimos que $\mathbb{Z}_2 \times \mathbb{Z}_3$ es cíclico. Esta es otra manera de comprobar que $\mathbb{Z}_2 \times \mathbb{Z}_3$ es isomorfo a $\mathbb{Z}_6$.

El ejercicio siguiente muestra, en cambio, que no siempre se puede descomponer $\mathbb{Z}_n$ en producto de grupos cíclicos de órdenes divisores de n.

Ejercicio 10.32. Comprobar que el grupo cíclico de cuatro elementos, $\mathbb{Z}_4$, no es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. ¿Por qué?

Grupos abelianos

Conocer la estructura interna de un grupo es en general un problema difícil. Si el grupo es abeliano, este problema tiene solución, como veremos a continuación.

En el apartado anterior hemos estudiado el modelo más sencillo de grupo abeliano, aquel que está generado por un único elemento. Si consideramos ahora un grupo G generado por un conjunto de elementos $S = \{g_1, g_2, \ldots, g_r\} \subset G$ (es decir, cualquier elemento de G se puede obtener como 'producto' de elementos de S) tales que conmuten entre ellos, $g_i g_j = g_j g_i$, para todo i, j, entonces cualquier elemento g de G se puede expresar como producto de potencias de estos generadores:

$$g = g_1^{x_1} g_2^{x_2} \cdots g_r^{x_r}$$

Como consecuencia, G es un *grupo abeliano*.

La relación entre los órdenes de dos elementos y el orden del producto de estos elementos es importante para conocer cuál es la estructura interna del grupo que generan. El resultado siguiente es útil en este sentido.

Proposición 10.33. Sean g y h dos elementos de un grupo abeliano G con órdenes respectivos n y m tales que $\text{mcd}(n,m) = 1$. Entonces el orden de gh es nm.

Demostración. Si $k = nm$, podemos decir que $(gh)^k = g^k h^k = 1$ y, por tanto, el orden de gh tiene que ser un divisor de k. Supongamos ahora que este orden fuese $k' < k$. En este caso tendríamos

que $(gh)^{k'} = g^{k'}h^{k'} = 1$, y de aquí que $g^{k'} = (h^{-1})^{k'}$. Ahora bien, el orden de este elemento $|g^{k'}|$ tiene que dividir al orden de g, $|g| = n$ y el orden de h, $|h| = m$. Como $\mathrm{mcd}(n,m) = 1$, el orden de $g^{k'}$ y de $(h^{-1})^{k'}$ tiene que ser 1. Por otra parte, $1 = (hh^{-1})^{k'} = h^{k'}(h^{-1})^{k'} = h^{k'}$, de donde se deduce que k' tiene que ser un múltiplo de n, de m y del mínimo común múltiplo. Como $\mathrm{mcd}(n,m) = 1$, tiene que ser $k' = \mathrm{mcm}(n,m) = nm$. □

Ejercicio 10.34. Demostrar la proposición 10.30 usando la proposición anterior.

Para caracterizar los órdenes de los elementos de un grupo abeliano finito, es útil considerar el orden máximo de sus elementos, llamado *exponente del grupo*.

Proposición 10.35. El orden de cualquier elemento de un grupo finito abeliano divide al exponente del grupo.

Demostración. Sea n el exponente de un grupo abeliano G y sea $g \in G$ tal que $|g| = n$. Supongamos que existiese un elemento $g' \in G$ de orden $|g'| = n'$ tal que n' no dividiese a n. Si $d = \mathrm{mcd}(n,n')$, entonces $|g^d| = n/d$ es relativamente primo con n', $\mathrm{mcd}(n/d,n') = 1$, y, por tanto, la proposición anterior nos dice que $|g'g^d| = n'n/d$. Pero como hemos supuesto que n' no divide a n, $n' > d$ y el orden de $|g'g^d| > n$ en contradicción con el hecho que n es el exponente del grupo. □

En particular, si el orden de un grupo abeliano es su exponente, entonces el grupo es cíclico. Si el grupo está generado por más de un elemento, $G = \langle g_1, g_2, \ldots, g_r \rangle$, y los órdenes de sus generadores son primos entre sí, entonces el orden de $g_1 g_2 \cdots g_r$ es producto de los órdenes de todos los generadores, que es justamente el orden de G y por tanto en este caso el grupo es también cíclico. Como consecuencia, si un grupo finito abeliano no es cíclico, debe tener como mínimo dos generadores con órdenes no primos entre sí.

A continuación describiremos la estructura general de los grupos abelianos. Las demostraciones de los resultados que siguen no se incluirán en este texto a causa de su nivel de dificultad. El lector interesado las puede encontrar, por ejemplo, en [3].

El primer paso para determinar la estructura de un grupo abeliano es un resultado similar al de la proposición 10.30. Para cada primo p, llamamos $G(p)$ al conjunto de todos elementos de G que tienen orden una potencia de p.

Ejercicio 10.36. Demostrar que si $G(p) \neq \emptyset$, entonces $G(p)$ es un subgrupo de G. Demostrar que si p divide a n, entonces $G(p)$ tiene orden una potencia de p.

Recordemos que el orden de cualquier elemento divide al orden del grupo. El siguiente teorema asegura que la afirmación recíproca también es cierta para divisores primos de $|G|$ y constituye la clave para la clasificación de los grupos abelianos.

Teorema 10.37 (Cauchy). Si p es un primo que divide a $|G|$, entonces hay algún elemento $g \in G$ que tiene orden p.

Este teorema asegura que $G(p) \neq \emptyset$ si y sólo si p divide a n. Como, para dos primos diferentes p, q, $G(p) \cap G(q) = \emptyset$, se obtiene en particular:

Proposición 10.38. Si G es un grupo abeliano de orden $n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$, entonces

$$G \simeq G(p_1) \times \cdots \times G(p_s)$$

Según la proposición anterior, sólo es preciso determinar la estructura de cada uno de los grupos abelianos $G(p)$ de orden una potencia de p. Si cada uno de ellos es cíclico, de acuerdo con los comentarios anteriores, G también es cíclico. Si $G(p)$ no es cíclico, se puede expresar también como producto de grupos cíclicos.

Proposición 10.39. Si G es un grupo abeliano de orden p^k, p primo, entonces

$$G \simeq \mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_t}}$$

para algunos $r_1, \ldots, r_t$ tales que $k = r_1 + \cdots + r_t$.

Según la proposición anterior, cada descomposición de k en suma de enteros $r_1 + \cdots + r_t$ proporciona un grupo abeliano de orden p^k y todos se pueden obtener así. Por ejemplo, los únicos grupos abelianos de orden $n = 3^3$ son $\mathbb{Z}_{27}$, $\mathbb{Z}_9 \times \mathbb{Z}_3$ y $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, que son diferentes entre sí.

Las proposiciones 10.38 y 10.39 proporcionan una caracterización completa de la estructura general de cualquier grupo abeliano finito.

Teorema 10.40. Si G es un grupo abeliano finito de orden $n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$, entonces

$$G \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$$

donde cada n_i es una potencia de alguno de los primos de la descomposición de n y $n_1 \cdots n_t = n$.

Ejercicio 10.41. Encontrar todos los grupos abelianos de orden $n = 24$.

10.3 Grupos de permutaciones

Como ya se ha mencionado en el capítulo anterior, el conjunto de aplicaciones biyectivas de un conjunto en él mismo forma un grupo con la composición de aplicaciones. El elemento neutro

del grupo es la aplicación identidad, y la aplicación inversa de una aplicación f está definida como $f^{-1}(y) = x \Leftrightarrow f(x) = y$.

Cuando X es un conjunto finito, estas aplicaciones se llaman *permutaciones*. Cualquier conjunto de permutaciones que forme grupo, se llama *grupo de permutaciones* y el conjunto de todas las permutaciones de n elementos es lo que se llama *grupo simétrico* de n símbolos que se denota por S_n y tiene $n!$ elementos.

Los grupos de permutaciones constituyeron uno de los estímulos principales para el estudio de los grupos finitos. De hecho, todo grupo finito se puede interpretar como un grupo de permutaciones. Este resultado, conocido como el teorema de Cayley, así como un estudio detallado de esta clase de grupos se verá más adelante en esta sección. Antes, sin embargo, discutiremos un ejemplo importante de grupos de permutaciones: los grupos de simetrías.

Grupos de simetrías

La estructura de grupo aparece de forma natural en el estudio de simetrías. En términos generales, una simetría sobre un conjunto es una biyección entre sus elementos que respeta su estructura. Las simetrías, por tanto, se pueden componer y el conjunto de todas ellas tiene estructura de grupo con la composición. En esta sección ilustramos este hecho a partir de un grupo de simetrías particular, el de los movimientos rígidos de un polígono regular que dejan su forma invariante.

Consideremos un triángulo equilátero de vértices ABC. Una rotación de $\pi/3$ radianes con centro el baricentro del triángulo lleva el vértice A al B, el B al C, el C al A y deja el triángulo invariante. Este es entonces un movimento rígido del triángulo que deja su forma invariante (véase la figura 10.1).

Llamamos g a este movimento. Si lo aplicamos dos veces (es decir, g^2), tenemos otro movimiento que también deja el triángulo invariante. Si lo aplicamos tres veces tenemos los vértices del triángulo en la posición inicial.

Los dos movimientos, g y g^2, no dejan ningún vértice fijo y son los únicos con esta propiedad. El triángulo admite, sin embargo, otros movimientos que lo dejan también invariante. El movimiento de rotación de π radianes sobre el eje dado por cada una de las alturas deja también el triángulo invariante. Los hay tres de estos movimientos, uno para cada una de las alturas. Llamamos a a la rotación que deja fijo el vértice A y, de manera similar, b y c a las que dejan fijos los vértices B y C respectivamente (véase la figura 10.1). Cada uno de estos movimientos queda identificado por su acción sobre los vértices A, B y C del triángulo, de manera que se puede ver el grupo de simetrías como un grupo de permutaciones de tres elementos. Los cinco movimientos que hemos visto y la identidad constituyen, por tanto, todas las simetrías del triángulo, ya que sólo hay seis permutaciones de tres elementos. En 10.4 está la tabla del grupo que forman. De la tabla se desprende que el grupo de simetrías de un triángulo es no abeliano.

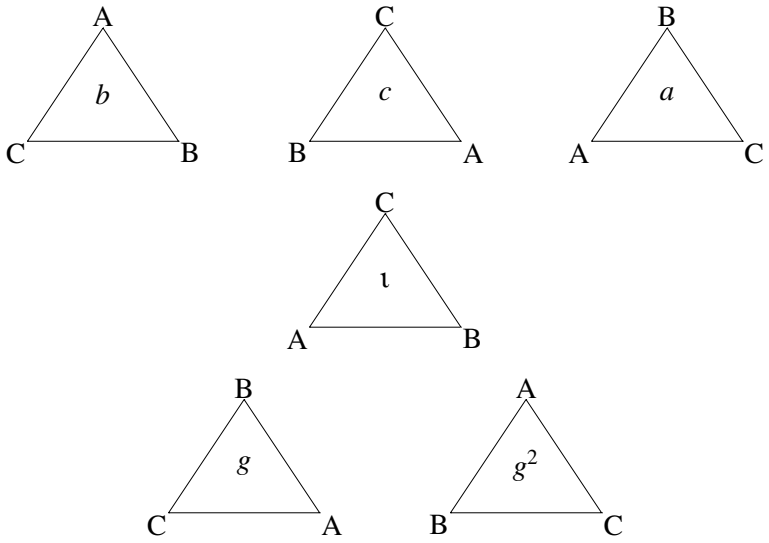


Figura 10.1: Simetrías del triángulo

Este es el grupo no abeliano más pequeño y forma parte de la familia de los llamados *grupos diédricos*, que se denotan por D_n y de los que hay uno para cada entero positivo n. La característica de todos estos grupos no abelianos es que tienen tamaño $2n$ y contienen un subgrupo cíclico de tamaño n que, además, es un subgrupo normal. En la tabla 10.4 se puede comprobar esta afirmación para $n = 3$. Para cada n, el grupo de simetrías de un polígono regular de n vértices es precisamente el grupo diédrico D_{2n}. Todas las simetrías se obtienen por una rotación de $2\pi/n$ radianes que, aplicada reiteradamente, proporciona las n simetrías que son giros y que dan lugar al subgrupo cíclico de D_{2n}. Los otros movimientos son rotaciones de π radianes en torno a un eje que pasa por un vértice y por el centro del polígono. En la figura 10.2 se ilustra

Tabla 10.4: Tabla de composición de las simetrías del triángulo

$\cdot$	e	g	g^2	a	b	c
e	e	g	g^2	a	b	c
g	g	g^2	e	c	a	b
g^2	g^2	e	g	b	c	a
a	a	b	c	e	g	g^2
b	b	c	a	g^2	e	g
c	c	a	b	g	g^2	e

la situación para el caso del pentágono.

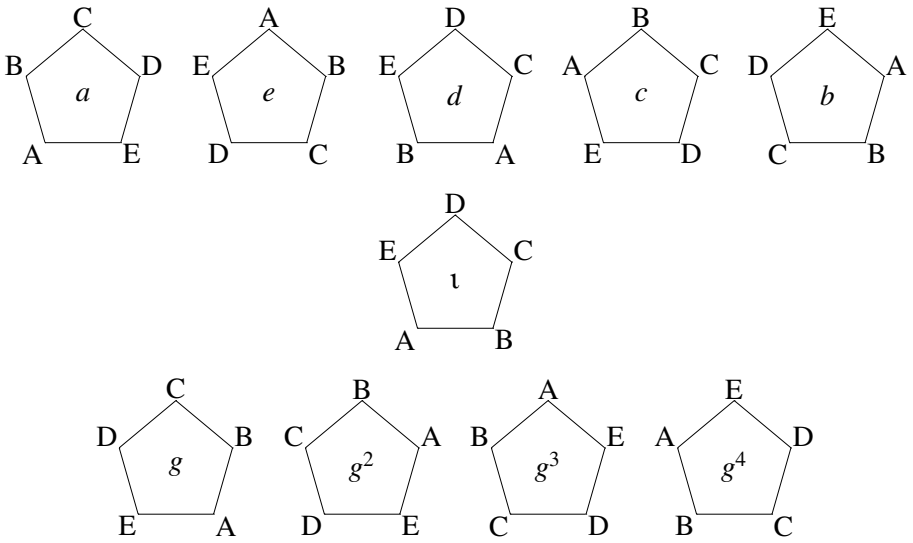


Figura 10.2: Simetrías del pentágono regular

El conjunto de automorfismos de un grafo (véase el problema 5.12) proporciona otro ejemplo importante de grupo de simetrías. En este caso, una simetría de un grafo es una biyección entre sus vértices que conserva las adyacencias. Por ejemplo, el grupo de automorfismos de un grafo completo de n vértices es el grupo simétrico de n símbolos, ya que cada biyección entre los vértices es un automorfismo del grafo.

Ejercicio 10.42. Demostrar que el grupo de automorfismos de un ciclo de orden n es el grupo diédrico D_n.

Notación cíclica de las permutaciones

Volvamos ahora al estudio general de los grupos de permutaciones. Para estudiarlos, el nombre que se da a los elementos del conjunto X donde se aplican resulta irrelevante, de manera que consideraremos $X = \{1, 2, \ldots, n\}$.

Para hacer más manejable el estudio de las permutaciones, conviene desarrollar una cierta notación. En primer lugar, si σ, τ son dos permutaciones de n elementos, su producto $\sigma\tau$ representa la composición leída de derecha a izquierda, es decir, aplicando τ en primer lugar y σ después (los algebristas suelen preferir la lectura inversa). Denotaremos la permutación identidad con la letra ι.

Para representar una permutación de n elementos, Lagrange usaba una notación matricial en la que colocaba los elementos de 1 a n en la primera fila y la lista de sus imágenes en la

segunda:

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

Esta es la notación *tabular*. Observar que la segunda fila es siempre una permutación de la primera, de donde viene la denominación de *permutaciones*.

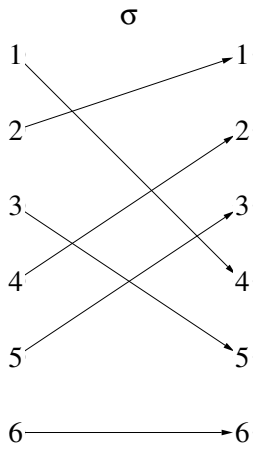
Hay otra notación que a menudo es útil, la notación *cíclica* introducida por Cauchy. Partiendo de un elemento $x_0 \in X$, consideremos la imagen de x_0, $\sigma(x_0)$, la imagen de éste, $\sigma(\sigma(x_0)) = \sigma^2(x_0)$, y así sucesivamente hasta que vuelve a aparecer $x_0 = \sigma^{j_0}(x_0)$. Si $j_0 = n$, escribimos

$$\sigma = (x_0, \sigma(x_0), \sigma^2(x_0), \ldots, \sigma^{n-1}(x_0))$$

mientras que, si $j_0 < n$, tomamos cualquier elemento que aún no haya aparecido, x_1, y consideramos las imágenes $\sigma(x_1), \sigma^2(x_1), \ldots$ hasta que vuelve a aparecer x_1. Iterando este procedimiento hasta que han aparecido todos los elementos, obtenemos una representación de la permutación como

$$\sigma = (x_0, \sigma(x_0), \ldots, \sigma^{j_0-1}(x_0))(x_1, \sigma(x_1), \ldots, \sigma^{j_1-1}(x_1)) \cdots (x_k, \sigma(x_k), \ldots, \sigma^{j_k-1}(x_k))$$

Por ejemplo, la permutación de 6 elementos



se escribe en notación tabular y en la notación cíclica como

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 3 & 6 \end{pmatrix} = (142)(35)(6)$$

Cada uno de los paréntesis en la última notación se llama *ciclo* de la permutación y la longitud de cada ciclo es el número de elementos que tiene. En el ejemplo, la permutación σ se escribe

como un ciclo de longitud 3, uno de longitud 2 y uno de longitud 1. Para simplificar la notación, a veces se dejan de lado los ciclos de longitud 1. Dos ciclos son *disyuntos* si no tienen ningún elemento en común. Una manera de expresar lo que hemos obtenido es la siguiente:

Proposición 10.43. Cada permutación $\sigma \in S_n$ se puede expresar de manera única como producto de ciclos disyuntos.

Ejercicio 10.44. Escribir en notación cíclica la permutación $\sigma\tau$, donde

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 3 & 6 \end{pmatrix} \quad \text{y} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 4 & 5 \end{pmatrix}$$

Ejercicio 10.45. Escribir en notación tabular la permutación $\sigma\tau$, donde $\sigma = (154)(236)$ y $\tau = (136)(25)(3)$.

La estructura cíclica de una permutación define en cierta manera su estructura algebraica.

Lema 10.46. El orden de una permutación $\sigma \in S_n$ es el mínimo común múltiplo de las longitudes de los ciclos de su descomposición cíclica.

Demostración. Consideremos primero el caso en que σ se escribe como un único ciclo de longitud k, $\sigma = (x_1 x_2 \cdots x_k)$ (sin contar los ciclos de longitud 1). Entonces, σ^i envía x_1 a x_{1+i}, x_2 a x_{2+i} y, en general, x_m al símbolo con subíndice $m+i \pmod k$. En particular, σ^i es la permutación identidad si y sólo si i es un múltiplo de n. Si σ se escribe como el producto de ciclos disyuntos $c_1 c_2 \cdots c_r$, de longitudes $l_1, l_2, \ldots, l_r$, entonces $\sigma^i = c_1^i c_2^i \cdots c_r^i$, y este producto es la identidad si y sólo si cada c_j^i es la identidad, de manera que i tiene que ser múltiplo de cada una de las longitudes. Recíprocamente, si i es múltiplo de todas las longitudes l_i, entonces $\sigma^i = \iota$. □

Así, por ejemplo, el orden de la permutación $(14)(25)(36)$ es 2, y el de la permutación $(135)(24)$ es 6.

Teorema de Cayley

Hay muchos subconjuntos de permutaciones que forman grupo respecto de la composición, es decir, que son subgrupos del grupo simétrico. Por ejemplo, el subgrupo generado por una permutación que consta de un único ciclo,

$$c_n = (12 \cdots n)$$

es un grupo cíclico de orden n, es decir, $\langle c_n \rangle \simeq \mathbb{Z}_n$.

El teorema de Cayley proporciona un resultado que justifica el interés de los grupos de permutaciones para el estudio de los grupos finitos.

Teorema 10.47 (Cayley). Cualquier grupo G de n elementos es isomorfo a un grupo de permutaciones de n símbolos.

Demostración. Como hemos hecho en el ejemplo anterior, identificamos cada elemento $g \in G$ con la permutación σ_g de n símbolos definida por $\sigma_g(x) = gx$. Esta identificación proporciona una biyección f entre los elementos de G y n permutaciones de S_n. Para ver que es un morfismo, es preciso comprobar que $f(gh) = f(g)f(h)$. Pero $f(gh)$ es la permutación dada por $f(gh)(x) = ghx$ y $f(g)f(h)(x) = f(g)(hx) = ghx$, de manera que f es efectivamente un isomorfismo. □

Tabla 10.5: La tabla de D_3

$\cdot$	e	g	g^2	a	b	c
e	e	g	g^2	a	b	c
g	g	g^2	e	c	a	b
g^2	g^2	e	g	b	c	a
a	a	b	c	e	g	g^2
b	b	c	a	g^2	e	g
c	c	a	b	g	g^2	e

Para ilustrar este resultado utilizaremos el grupo diédrico de 6 elementos. Podemos identificar cada elemento del grupo con una permutación de seis elementos, de la manera siguiente,

$$\begin{array}{ccc} e & \longrightarrow & (1)(2)(3)(4)(5)(6) \\ g & \longrightarrow & (123)(465) \\ g^2 & \longrightarrow & (132)(456) \\ a & \longrightarrow & (14)(25)(36) \\ b & \longrightarrow & (15)(26)(34) \\ c & \longrightarrow & (16)(24)(35) \end{array}$$

donde hemos cambiado e, g, g^2, a, b, c por $1, 2, 3, 4, 5, 6$. Es fácil comprobar que esta identificación es en realidad un isomorfismo, es decir, que resulta lo mismo operar con los elementos del grupo diédrico que componer las correspondientes permutaciones. Esto es lo que dice el teorema de Cayley, que proporciona un contexto general para todos los grupos finitos.

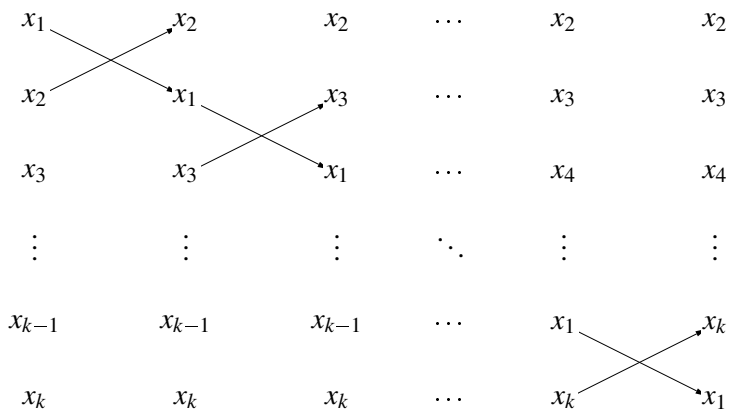
Transposiciones. El grupo alternado.

Una permutación que se escribe como un único ciclo de longitud 2 se llama *transposición*. Escribiremos $\tau_{ij} = (ij)$. El conjunto de transposiciones es interesante por el hecho que cual-

quier permutación se puede expresar como producto de transposiciones (no necesariamente disyuntas). Podemos expresar este resultado de la forma siguiente:

Proposición 10.48. El conjunto de todas las transposiciones de n símbolos genera todo S_n.

Demostración. Un ciclo $(x_1x_2\dots x_k)$ se puede expresar en términos de las transposiciones según el esquema siguiente:



o sea, que

$$(x_1x_2\dots x_k) = (x_1x_k)(x_1x_{k-1})\cdots(x_1x_3)(x_1x_2)$$

Ahora, cualquier permutación se puede expresar como producto de ciclos disyuntos, y cada uno de ellos se puede expresar como producto de transposiciones. □

Ejercicio 10.49. Escribir la permutación $(125)(346)$ como producto de transposiciones.

Ejercicio 10.50. Dar una cota superior del número de transposiciones que aparecen en la expresión de una permutación de S_n como producto de transposiciones.

En realidad no son precisas todas las transposiciones para generar todo el grupo simétrico.

Proposición 10.51. Las n transposiciones de la forma $(1i)$, $i = 2,3,\dots,n$ generan el grupo simétrico.

Demostración. Observemos simplemente que cualquier transposición (ij) se puede escribir como $(1i)(1j)(1i)$. □

Ejercicio 10.52. Demostrar que se puede generar todo el grupo S_n a partir de

1. las transposiciones $(12),(23),\dots,((n-1)n)$;

2. la transposición (12) y el ciclo $(23\dots n)$.

Según la proposición y el ejercicio anteriores, está claro que una permutación admite en general diversas expresiones diferentes como producto de transposiciones. Sin embargo, todas estas expresiones tienen una cosa en común.

Proposición 10.53. Si $\sigma = \tau_1\tau_2\cdots\tau_k = \tau'_1\tau'_2\cdots\tau'_{k'}$ son dos expresiones de la permutación σ como producto de transposiciones, entonces k y k' tienen la misma paridad.

Demostración. Sea π una permutación cualquiera y c el número de ciclos en su expresión cíclica (que es única). Sea $\tau = (ij)$ una transposición. Si i, j pertenecen al mismo ciclo $(ix_2\cdots x_{k-1}jx_{k+1}\cdots x_m)$ de la expresión cíclica de π, entonces

$$(ij)(ix_2\cdots x_{k-1}jx_{k+1}\cdots x_m) = (ix_2\cdots x_{k-1})(jx_{k+1}\cdots x_m)$$

(véase la figura 10.3), mientras que el resto de ciclos quedan inalterados por la acción de τ. Si, en cambio, i, j pertenecen a ciclos diferentes, $(ix_2\cdots x_m)$ y $(jy_2\cdots y_{m'})$, entonces $(ij)(ix_2\cdots x_m)$ $(jy_2\cdots y_{m'}) = (ix_2\cdots x_m jy_2\cdots y_{m'})$ y el resto de ciclos quedan inalterados por la acción de τ. En el primer caso, el número de ciclos de $\tau\pi$ es $c+1$ y en el segundo es $c-1$.

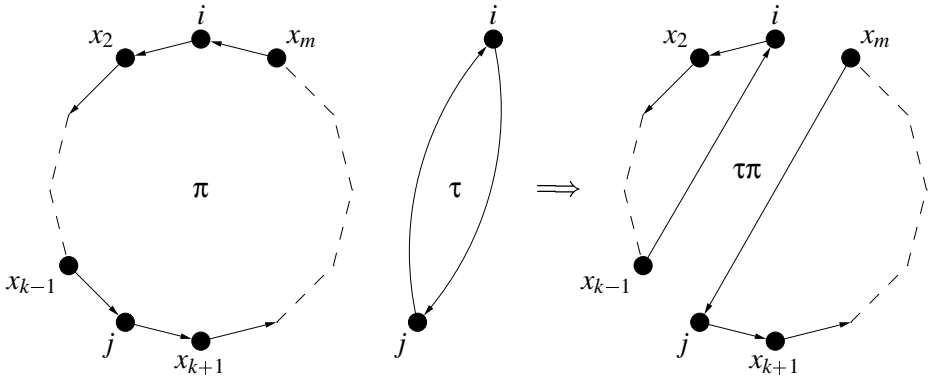


Figura 10.3: Composición de un ciclo y una transposición

Supongamos entonces que el número de ciclos en la expresión cíclica de $\sigma = \tau_1\tau_2\cdots\tau_k$ es c. El número de ciclos de τ_k es $(n-1)$ (contamos también los ciclos de longitud 1). Aplicando iteradamente el resultado anterior, cada vez que se aplica una transposición el número de ciclos del producto aumenta o disminuye en una unidad, y el resultado final tiene que ser c, de manera que $c = (n-1) - a + b$, siendo a el número de veces que disminuye y b el número de veces que aumenta, con $a + b = k$. Así pues, $c = (n-1) + k - 2a$. Haciendo lo mismo con la segunda descomposición obtendremos $c = (n-1) + k' - 2a'$ para un cierto a'. Restando las

dos igualdades, se ve que $k-k' = 2(a-a')$. Por tanto, o bien k y k' son ambos pares, o bien son ambos impares. □

Las permutaciones que se escriben como producto par de transposiciones se llaman permutaciones *pares* y las que no, se llaman *impares*. La *signatura* de una permutación es $sgn(\sigma) = 1$ si σ es par y $sgn(\sigma) = -1$ si es impar.

Ejercicio 10.54. Estudiar la paridad de un ciclo de orden k.

Ejercicio 10.55. Considerar el polinomio de n variables

$$P(x_1, x_2, \ldots, x_n) = \prod_{i<j} (x_i - x_j)$$

Demostrar que

$$P(x_1, x_2, \ldots, x_n) = (-1)^{sgn(\sigma)} P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

Si τ es una transposición cualquiera, la aplicación $f_\tau : S_n \longrightarrow S_n$ definida como $f_\tau(\sigma) = \tau\sigma$ es una biyección que envía las permutaciones pares a las impares y viceversa, de manera que S_n contiene $n!/2$ permutaciones pares y un número igual de impares. Otra particularidad de esta clasificación de las permutaciones de S_n es la siguiente.

Proposición 10.56. El conjunto de permutaciones pares es un subgrupo de S_n.

Demostración. Sólo es preciso ver que el conjunto de permutaciones pares es cerrado por la composición. Esto es evidente, ya que si $\sigma = \tau_1\tau_2\cdots\tau_k$ y $\sigma' = \tau'_1\tau'_2\cdots\tau'_{k'}$, entonces su producto se puede escribir como producto de transposiciones $\sigma\sigma' = \tau_1\tau_2\cdots\tau_k\tau'_1\tau'_2\cdots\tau'_{k'}$ de longitud $(k+k')$, que es par si k y k' son pares. □

El subgrupo de permutaciones pares se llama subgrupo *alternado*, se denota por $Alt(n)$ y tiene $n!/2$ elementos. Como la relación de equivalencia inducida en S_n por este subgrupo sólo tiene dos clases, A_n es obviamente un subgrupo normal de S_n. Este subgrupo tiene una importancia singular por la conexión que establecieron Galois y Abel entre la posibilidad de resolver una ecuación de grado n $a_0x^n + a_{n-1}x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ con una cantidad finita de operaciones elementales, con la existencia de subgrupos normales de A_n. Se puede demostrar que A_n no tiene subgrupos normales para $n \geqslant 5$, cosa que proporciona el argumento para asegurar que las ecuaciones de grado mayor que cuatro no se pueden resolver, en general, por radicales.

Grupos de matrices

Una manera de representar una permutación σ de n elementos consiste en considerar una matriz cuadrada $P_\sigma = (p_{ij})$ de orden n en la que

$$p_{ij} = \begin{cases} 1 & \text{si } \sigma(i) = j \\ 0 & \text{de otro modo} \end{cases}$$

Así, por ejemplo, a la permutación $\sigma = (142)(35)(6)$ le corresponde la matriz

$$P_\sigma = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Observemos que en cada fila y en cada columna hay exactamente un 1 y el resto de elementos son ceros. Este tipo de matrices se llaman justamente *matrices de permutaciones*. Observar que el determinante de cualquiera de estas matrices es ± 1. Diremos P_n al conjunto de las matrices de permutaciones de orden n.

El interés de esta representación proviene del hecho que la composición de permutaciones se traduce justamente en el producto de matrices.

Lema 10.57. Sean σ, τ dos permutaciones de S_n y P_σ, P_τ sus representaciones matriciales. Entonces:

1. $P_{\tau\sigma} = P_\sigma P_\tau$, es decir, la composición de permutaciones se traduce en producto de matrices.

2. $P_{\sigma^{-1}}$ es la matriz transpuesta ${P_\sigma}^T$.

Demostración. Sean $P_\sigma = (p_{ij})$ y $Q_\tau = (q_{ij})$. Entonces, su producto es $R = P_\sigma Q_\tau = (r_{ij})$ donde $r_{ij} = \sum_{k=1}^{n} p_{ik} q_{kj}$. El término r_{ij} vale 1 si y sólo si existe algún valor de k tal que $p_{ik} = q_{kj} = 1$ y en cualquier otro caso $r_{ij} = 0$. Como para cada fila (i) y para cada columna (j) existe un y sólo un valor de k tal que $p_{ik} = 1$ y $q_{kj} = 1$, $R = (r_{ij})$ es una matriz de permutaciones. Además, si π es la permutación asociada a R, $\pi(i) = j \Leftrightarrow r_{ij} = 1 \Leftrightarrow p_{ik} = q_{kj} = 1$ para un único k y $\tau\sigma(i) = \tau(k) = j$, de manera que $\pi = \tau\sigma$.

Por otra parte, $(p_{ji}) = P_{\sigma^{-1}}$, ya que $\sigma(i) = j$ si y sólo si $i = \sigma^{-1}(j)$. Por tanto, $P_{\sigma^{-1}}$ es la matriz transpuesta de P_σ. □

Como consecuencia directa del lema anterior, el conjunto P_n de todas las matrices de permutaciones de orden n tiene estructura de grupo con el producto de matrices, y este grupo es isomorfo a S_n.

Se pueden definir grupos de matrices más generales que los grupos de matrices de permutaciones. Por ejemplo, el conjunto de matrices cuadradas invertibles con coeficientes en $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ tienen estructura de grupo con el producto. Estos son ejemplos de grupos infinitos que, en general, no son abelianos.

El producto de matrices se puede definir también cuando los términos son los elementos de $\mathbb{Z}_n$ y las operaciones de suma y producto se hacen módulo n. Cualquier subconjunto de matrices invertibles donde la operación producto sea cerrada proporciona un nuevo ejemplo de grupo de matrices que, en este caso, es finito (y, en general, no abeliano). Los grupos de matrices proporcionan entonces una fuente importante de ejemplos de grupos finitos.

Por ejemplo, el conjunto de todas las matrices cuadradas 2×2 invertibles con términos de $\mathbb{Z}_2$ forma un grupo de 6 elementos:

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

Ejercicio 10.58. Demostrar que el grupo anterior es isomorfo al grupo diédrico de 6 elementos.

Ejercicio 10.59. Considerar el grupo de las matrices invertibles de la forma

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

que tienen sus términos en $\mathbb{Z}_3$. ¿Es isomorfo al grupo del ejercicio anterior?

10.4 Digrafos de Cayley

Una buena manera de estudiar los grupos finitos consiste en describirlos a través de lo que se llaman *presentaciones*. Recordemos que, dado un grupo G, se dice que $S \subset G$ es un conjunto de generadores de G si cada elemento de G se puede expresar como producto de elementos de S, y se escribe

$$G = \langle S \rangle$$

Por ejemplo, si G es un grupo cíclico, hay un elemento $g \in G$ tal que cualquier elemento $x \in G$ se expresa como $x = g^k$ para una cierta potencia k de g, es decir, $G = \langle \{g\} \rangle$. El grupo diédrico de seis elementos introducido en la sección anterior no es cíclico. Esto quiere decir que se

precisa más de un elemento para conseguir un conjunto de generadores. Se puede comprobar fácilmente que el subconjunto $S = \{g, a\}$ es un conjunto de generadores de D_6.

Ejercicio 10.60. Expresar todos los elementos de D_6 como productos de elementos de $S = \{g, a\}$. ¿Son generadores los subconjuntos $S' = \{g, b\}$ y $S'' = \{a, b\}$? ¿Cuántos subconjuntos de dos generadores tiene el grupo?

Una lista de generadores de un grupo no es suficiente para determinar (salvo isomorfismos) de qué grupo se trata. Por ello es preciso indicar cuando dos expresiones diferentes corresponden al mismo elemento del grupo. Por ejemplo, en el caso del grupo cíclico de n elementos tenemos $g = g^{n+1}$ o $g^2 = g^{2n+2}$. En el caso del grupo diédrico generado por $\{g, a\}$, tenemos $g = ag^2a$. Todas estas igualdades se pueden expresar poniendo la identidad a un lado de la igualdad. Por ejemplo, las dos igualdades anteriores para el caso del grupo cíclico se expresarían como $g^n = e$ y $g^{2n} = e$, mientras que la identidad anterior del grupo diédrico se podría expresar como $gaga = e$. En este contexto, cada una de estas expresiones igualadas al elemento neutro se llama una *relación*.

El objetivo de presentar un grupo a través de generadores y relaciones consiste en encontrar un conjunto mínimo de relaciones a partir de las cuales se puedan obtener todos los elementos del grupo. Un conjunto de relaciones con esta propiedad se llama conjunto de relaciones *definidor* del grupo. Por ejemplo, en el caso del grupo cíclico de orden n, basta con la relación $g^n = e$ para deducir todas las demás. El par formado por un conjunto S de generadores y un conjunto R de relaciones definidoras se llama una *presentación* del grupo, y se denota por

$$G = \langle S | R \rangle$$

En el caso del grupo cíclico, entonces, tenemos la presentación

$$G = \langle g | g^n = e \rangle$$

y esta expresión determina el grupo. Como norma general, cuando se escribe $g^n = e$ en una presentación se sobreentiende que n es la potencia más pequeña de g que da e. De la misma manera, cuando hay varios generadores, se sobreentiende que ninguna subexpresión de una relación da el elemento neutro. Habitualmente, las relaciones se escriben simplemente como g^n en lugar de $g^n = e$.

Encontrar una presentación no es fácil en general, especialmente en lo que respecta a encontrar un conjunto reducido de relaciones definidoras. En general, una de las relaciones que se incluye es la que da el orden de los elementos. Una presentación de D_6 con los generadores g, a incluiría entonces las relaciones $g^3 = e$ y $a^2 = e$. Pero éstas no son definidoras del grupo. Por ejemplo, no se puede deducir que $gaga = e$. Con ésta se obtiene ya un conjunto de relaciones definidoras del grupo:

$$D_6 = \langle g, a | g^3, a^2, gaga \rangle$$

Determinar cuál es la tabla del grupo a partir de una presentación, o si un conjunto de relaciones es definidor de un grupo del cual tenemos la tabla, puede ser una tarea penosa, pero una presentación suele ser una manera económica y precisa de identificar un grupo. Los digrafos de Cayley proporcionan una visualización de un grupo expresado en términos de generadores que resulta muy útil.

Dado un grupo G y un conjunto de generadores S, el *digrafo de Cayley* de G respecto de S es el digrafo $Cay(G,S)$ que tiene por conjunto de vértices los elementos del grupo y por conjunto de arcos $\{(x,xs), x \in G, s \in S\}$. Si $S = S^{-1}$ e identificamos cada arco del digrafo con una arista, obtenemos el *grafo de Cayley* de G respecto de S. En las figuras 10.4 y 10.5 hay dibujados los digrafos de Cayley $Cay(\mathbb{Z}_6, \{2,3\})$ y $Cay(D_6, \{g,a\})$ y los grafos de Cayley $Cay(\mathbb{Z}_5, \{1,-1\})$ y $Cay(S_3\{(12),(13)\}$.

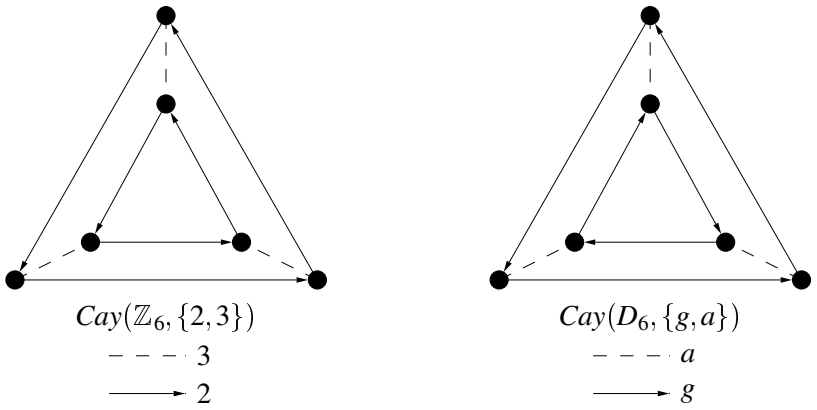


Figura 10.4: Ejemplos de digrafos de Cayley

El digrafo de Cayley del grupo cíclico de n elementos (con un único generador) es un ciclo de n vértices. Cada ciclo de un digrafo de Cayley corresponde a una relación, y un conjunto de relaciones es definidora del grupo si y sólo si todos los ciclos del digrafo se pueden descomponer en ciclos correspondientes a las relaciones definidoras.

Ejercicio 10.61. El *grupo de los cuaternones* es un grupo de ocho elementos que se define a través de la presentación siguiente:

$$Q_8 = \langle a,b | a^4, b^4, abab^{-1}, a^2b^2 \rangle$$

Dibujar el digrafo de Cayley $Cay(Q_8, \{a,b\})$.

El interés de los digrafos de Cayley está en la interrelación entre propiedades combinatorias del digrafo y propiedades algebraicas del grupo. No es difícil ver las siguientes interrelaciones.

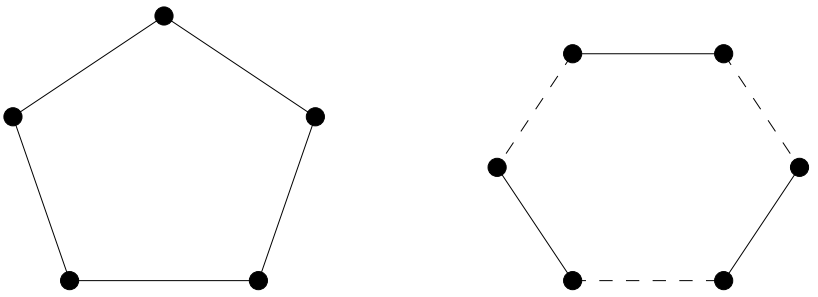


Figura 10.5: Ejemplos de grafos de Cayley

Proposición 10.62. Sea G un grupo y S un conjunto de generadores de G. Entonces $Cay(G,S)$ es un digrafo regular de grado $|S|$ fuertemente conexo.

Una característica especial de los digrafos de Cayley es la siguiente (véase el problema 5.13).

Proposición 10.63. Los digrafos de Cayley son vértice-simétricos.

Demostración. Dado un digrafo de Cayley, $Cay(G,S)$, y dos vértices $g,h \in G$ del digrafo, la aplicación $f_{gh} : G \longrightarrow G$ definida como $f_{gh}(x) = (hg^{-1})x$ satisface:

1. es una biyección, ya que $(hg^{-1})x = (hg^{-1})y$ implica $x = y$;
2. $f_{gh}(g) = h$;
3. es un automorfismo del digrafo, ya que (x, xs) es un arco si y sólo si $((hg^{-1})x, (hg^{-1})xs)$ lo es.

Por tanto, para cada par de vértices hay un automorfismo del digrafo que envía uno al otro. □

Desde el punto de vista de la teoría de grafos, los digrafos de Cayley suministran ejemplos numerosos y variados de digrafos vértice-simétricos. No todos los digrafos vértice-simétricos son, sin embargo, digrafos de Cayley. El ejemplo más pequeño en número de vértices de digrafo vértice-simétrico que no es de Cayley es el digrafo de Petersen, obtenido a partir del grafo del mismo nombre reemplazando cada arista por un arco. En cambio, el ciclo de n vértices es el digrafo de Cayley de un grupo cíclico de orden n respecto de un generador, y el digrafo completo de n vértices es el digrafo de Cayley de cualquier grupo G de orden n

respecto del conjunto de generadores $S = G \setminus \{e\}$. Los llamados digrafos de doble enlace, donde cada nodo $i \in \{0, 1, \ldots, n-1\}$ es adyacente a $i \pm a \pmod n$ y a $i \pm b \pmod n$ con $a, b \in \{0, 1, \ldots, n-1\}$, y que son utilizados en el diseño de redes de interconexión, son los grafos de Cayley $Cay(\mathbb{Z}_n, \{a, b, -a, -b\})$.

10.5 Enumeración de Pólya

La teoría de enumeración de Pólya tiene origen en el intento de enumerar diferentes compuestos químicos orgánicos. La diferencia entre compuestos se establece por la naturaleza y posición de los átomos en la estructura de una molécula, pero no entre aquellos que sólo difieren por ciertas simetrías. Por ejemplo, los dos primeros compuestos de la figura 10.6 son el mismo, mientras que el primero y el último no son químicamente iguales.

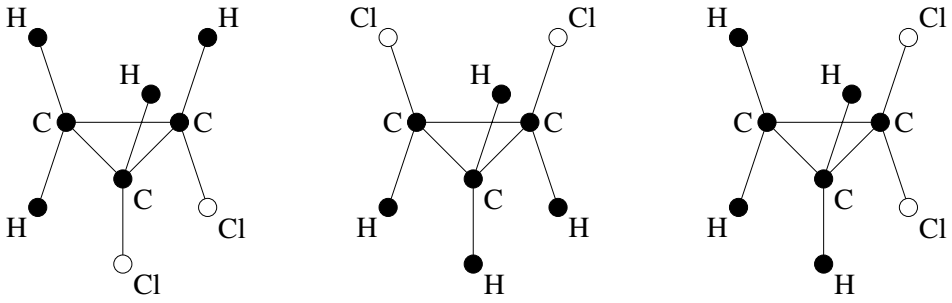


Figura 10.6: Simetría de compuestos químicos

El resultado que permite resolver este tipo de problemas de enumeración se conoce como el teorema de Pólya. Su objetivo es enumerar clases diferentes de configuraciones construidas sobre un objeto que tiene una cierta simetría. Para la exposición de la teoría de Pólya, substituiremos átomos por etiquetas o *colores*, que se asignan a diferentes elementos de un conjunto. Este conjunto gozará de ciertas simetrías que harán que diferentes maneras de colorear los vértices resulten equivalentes. El objetivo será contar cuántas clases de maneras equivalentes de hacer la coloración hay.

Supongamos, por ejemplo, que queremos asignar uno de los dos colores $\{\bullet, \circ\}$ a los vértices del grafo de la figura 10.7. De las $PR_4^2 = 16$ posibles maneras de hacer esta asignación, no consideraremos, sin embargo, diferentes aquellas que no se pueden distinguir sin enumerar explícitamente los vértices, es decir, las configuraciones encuadradas en la figura 10.8.

Con este criterio de diferenciación se obtienen, pues, 9 maneras diferentes en lugar de las 16 originales.

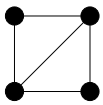


Figura 10.7:

La situación es, en general, la siguiente. Tenemos un conjunto $X = \{1, 2, \ldots, n\}$ y un grupo de permutaciones G de los elementos de X. En el ejemplo, X es el conjunto de vértices del grafo, y G es el grupo de automorfismos del grafo (si numeramos los vértices de 1 a 4 en sentido horario, $G = \{\iota, (13), (24), (13)(24)\}$). Finalmente tenemos un conjunto $C = \{c_1, \ldots, c_k\}$ de etiquetas o colores (en el ejemplo $C = \{\bullet, \circ\}$). Cada aplicación

$$f : X \longrightarrow C$$

proporciona una manera de asignar colores a los elementos de X. Diremos que es una *coloración* de los elementos de X. Llamamos C^X al conjunto de estas coloraciones, que tiene k^n elementos. Lo que decide el criterio de diferenciación de dos coloraciones es la acción del grupo G. Diremos que dos coloraciones $f, f' \in C^X$ son *G-equivalentes* si existe alguna permutación $\sigma \in G$ de manera que $f' = f\sigma$. En el ejemplo anterior, las coloraciones de la figura 10.9 son equivalentes, ya que, numerando los vértices en sentido horario y tomando la permutación $\sigma = (24) \in G$, tenemos que $f' = f\sigma$.

De forma similar, diremos que dos coloraciones son G-diferentes si no son G-equivalentes. El teorema de Pólya proporciona una manera de obtener este número de configuraciones diferentes en términos del tamaño n de X, del número k de colores y de la estructura del grupo G de permutaciones. El resultado se basa en la enumeración de lo que se llaman *órbitas* de un grupo de permutaciones. La *órbita* de un elemento $x \in X$, que denotaremos por O_x, es el conjunto de elementos $y \in X$ para los cuales hay alguna permutación en G que envía x a y, es decir:

$$O_x = G(x) = \{g(x), g \in G\} \subset X$$

En el grupo de automorfismos $G = \{\iota, (13), (24), (13)(24)\}$ del grafo del ejemplo anterior, la órbita del 1 es $\{1, 3\}$ y la del 2 es $\{2, 4\}$. En general, el número de órbitas de un grupo de permutaciones está relacionado con el número de puntos que deja fijos cada una de las permutaciones: como más puntos fijos dejen los elementos de G, más órbitas tiene el grupo. Para hacer precisa esta afirmación necesitamos otra definición. Dado un elemento $x \in X$, el *estabilizador* de x en G es el conjunto G_x de permutaciones que dejan x fijo,

$$G_x = \{g \in G \mid g(x) = x\} \subset G$$

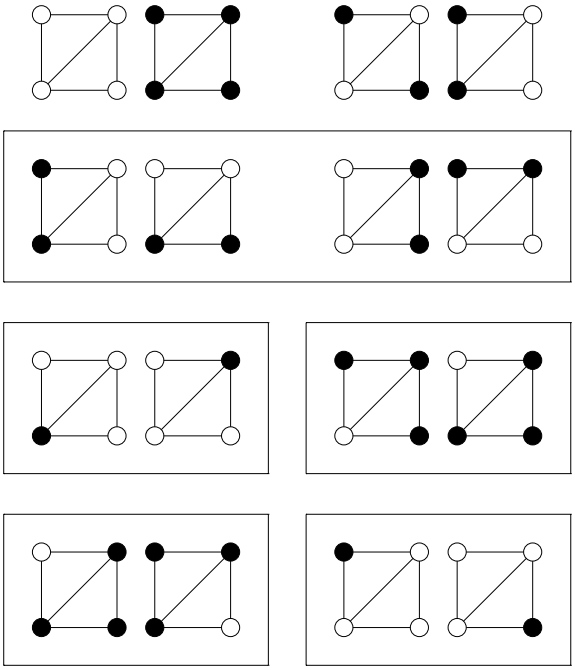


Figura 10.8: Coloraciones equivalentes

Ejercicio 10.64. Demostrar que G_x es un subgrupo de G. Demostrar que todas las permutaciones de una clase lateral hG_x envían x al mismo elemento $y = h(x)$ (si $h_1, h_2 \in hG_x$, entonces $h_1(x) = h_2(x) = y$).

Finalmente, para cada $g \in G$, diremos $fix(g) = \{x \in X \mid g(x) = x\} \subset X$ al conjunto de puntos de X que quedan fijos por g.

Lema 10.65 (Lema de Burnside). El número de órbitas de un grupo de permutaciones G que actúa sobre el conjunto X es

$$\frac{1}{|G|} \sum_{g \in G} fix(g)$$

Demostración. De acuerdo con lo que dice el ejercicio 10.64, si y está en la órbita de x, hay tantas permutaciones que envían x a y como el número de elementos de G_x. Por tanto, $|G| = |G_x| \cdot |O_x|$. Por otra parte, está claro que $1 = \sum_{y \in O_x} (1/|O_x|)$, de manera que el número de órbitas

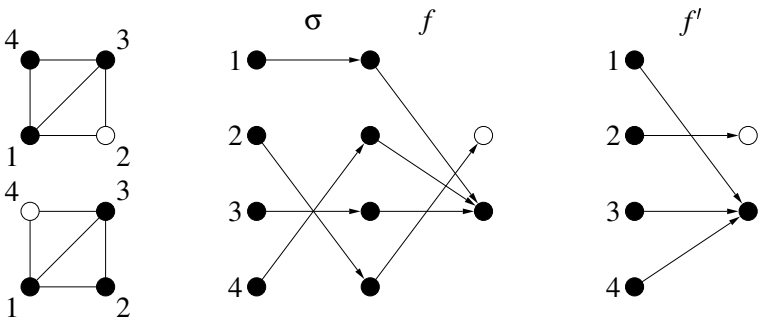


Figura 10.9: Dos coloraciones G-equivalentes

es

$$\sum_{x\in G}\frac{1}{|O_x|}=\frac{1}{|G|}\sum_{x\in G}|G_x|$$

Consideremos ahora los pares $\{(g,x)\in G\times X \mid g(x)=x\}$. Hay dos maneras de contar estos pares: para cada $x\in X$ el número de pares es G_x, mientras que para cada $g\in G$, el número de pares es $fix(g)$. Por tanto, $\sum_{x\in G}|G_x|=\sum_{g\in G}fix(g)$, de donde se deduce el enunciado del lema. □

El lema anterior se puede interpretar diciendo que el número de órbitas coincide con el número medio de puntos fijos de cada permutación de G.

El problema de enumeración que nos ocupa se puede formular en términos del número de órbitas de un cierto grupo de permutaciones. Recordemos que dos coloraciones $f,f'\in C^X$ son G-equivalentes si hay alguna permutación $\sigma\in G$ tal que $f=f'\sigma$, y nuestro objetivo es contar cuántas clases de equivalencia hay.

Podemos interpretar G como un grupo de permutaciones sobre C^X si definimos, para cada $f\in C^X$, $\overline{\sigma}(f)=f\sigma$. Si dos de estas coloraciones f,f' son diferentes, entonces $f\sigma, f'\sigma$ también lo son, de manera que la aplicación $\overline{\sigma}$ es inyectiva. Como C^X es finito, también es biyectiva, es decir, $\overline{G}=\{\overline{\sigma},\sigma\in G\}$ es un grupo de permutaciones de C^X. Observemos finalmente que dos coloraciones son G-equivalentes si y sólo si pertenecen a la misma órbita de $\overline{G}$.

Ejercicio 10.66. Demostrar que, si C tiene más de un color, $\overline{\sigma}=\overline{\sigma}'$ si y sólo si $\sigma=\sigma'$.

La versión más simple del teorema de Pólya es el resultado de aplicar el lema de Burnside al grupo $\overline{G}$. Llamamos $c(\sigma)$ al número de ciclos en la descomposición de σ. Por ejemplo, si $\sigma=(12)(3)(456)$, entonces $c(\sigma)=3$.

Teorema 10.67. Sea G un grupo de permutaciones de $X = \{1, 2, \ldots, n\}$. El número de coloraciones G–diferentes de X con los colores de $C = \{c_1, c_2, \ldots, c_k\}$ es

$$|G(C^X)| = \frac{1}{|G|} \sum_{\sigma \in G} k^{c(g)}$$

Demostración. Como ya hemos mencionado, el número de coloraciones G-diferentes coincide con el número de órbitas de $\overline{G}$. Según el lema de Burnside, este número de órbitas es

$$\frac{1}{|\overline{G}|} \sum_{\overline{\sigma} \in \overline{G}} fix(\sigma)$$

Si $\sigma = (x_{11}x_{12}\ldots x_{1j_1})\cdots(x_{r1}x_{r2}\ldots x_{rj_r})$ es la descomposición de σ en ciclos disyuntos, $\overline{\sigma}(f) = f\sigma = f$ si y sólo si f es constante en cada uno de los ciclos de σ. Si $c(\sigma) = r$ es el número de ciclos de σ, hay $k^{c(\sigma)}$ posibles coloraciones con esta propiedad. Así pues, $|fix(\sigma)| = k^{c(\sigma)}$. El teorema se obtiene entonces observando que $|G| = |\overline{G}|$ (véase el ejercicio 10.66). □

En el ejemplo que hemos tratado antes, $G = \{\iota, (12), (34), (12)(34)\}$ tiene una permutación de cuatro ciclos (la identidad), dos de tres ciclos y una de dos ciclos. Por tanto, el número de coloraciones diferentes con dos colores del grafo del ejemplo es

$$|G(X)^C| = \frac{1}{4}(2^4 + 2^3 + 2^3 + 2^2) = 9$$

Observar que en la aplicación del teorema es preciso considerar también los ciclos de longitud 1. En particular, en el sumatorio aparece siempre el término $|C|^{|X|}$ que corresponde a la contribución de la permutación identidad.

Es preciso notar también que la aplicación de este resultado exige conocer el número y longitud de los ciclos en la descomposición cíclica de cada permutación de G. Esta información se conoce para algunos de los grupos más comunes, pero puede ser difícil de obtener en general. Una manera de condensar esta información sobre la estructura de los ciclos de las permutaciones de G es lo que se llama el *índice de ciclos* del grupo, que se define de la manera siguiente. Si una permutación $\sigma \in G$ tiene λ_1 ciclos de longitud 1, λ_2 ciclos de longitud 2, ..., λ_n ciclos de longitud n, se dice que σ es del tipo $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$. Por ejemplo, la permutación $(12)(3)(456)$ de un grupo de permutaciones de seis elementos es del tipo $(1,1,1,0,0,0)$. Si llamamos $h(\lambda)$ al número de permutaciones de G de tipo λ, el índice de ciclos de G se define como

$$P_G(x_1, x_2, \ldots, x_n) = \frac{1}{|G|} \sum h(\lambda) x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$$

donde el sumatorio se extiende a todos los λ posibles, es decir, a todos aquellos que satisfacen $1 \cdot \lambda_1 + 2 \cdot \lambda_2 + \cdots + n \cdot \lambda_n = n$. El índice de ciclos del grupo de automorfismos del grafo de nuestro ejemplo es

$$P_G(x_1, x_2, x_3, x_4) = x_1^4 + 2x_1^2 x_2 + x_2^2 \tag{10.1}$$

El teorema 10.67 se puede expresar en términos del índice de ciclos de G como:

Teorema 10.68. El número de coloraciones G-diferentes de X con los colores de $C = \{c_1, \ldots, c_k\}$ es

$$|G(C^X)| = P_G(k, \ldots, k)$$

Así pues, el conocimiento del polinomio de ciclos de un grupo de permutaciones permite resolver el problema de enumeración que nos hemos planteado.

Ejercicio 10.69. Encontrar el polinomio enumerador de ciclos de un grupo cíclico de orden p donde p es un número primo. Calcular cuántas secuencias de ceros y unos de longitud 7 se pueden formar si consideramos iguales dos secuencias que sólo difieren en una traslación cíclica de los dígitos (por ejemplo, las secuencias 1000000 y 0100000 se consideran iguales).

El teorema de enumeración de Pólya va un poco más allá de los enunciados de los teoremas 10.70 y 10.68, y permite calcular el número de configuraciones diferentes en las cuales aparecen un determinado número de colores. Para ello asociamos a cada coloración f un *peso* en términos de los colores de C de la manera siguiente. Si la coloración f asigna el color c_i a α_i de los elementos de X, $1 \leqslant i \leqslant k$, el peso de f es

$$p(f) = c_1^{\alpha_1} \cdot c_2^{\alpha_2} \cdots c_k^{\alpha_k}$$

Por ejemplo, la coloración de la figura 10.10 tiene peso $p(f) = \bullet^3 \circ^1$.

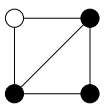


Figura 10.10: Una coloración de peso $p(f) = \bullet^3 \circ^1$

Teorema 10.70 (Pólya, 1935). El número de coloraciones G-diferentes de X con los colores de C que usan α_i veces el color i, $1 \leqslant i \leqslant n$, es el coeficiente de $c_1^{\alpha_1} \cdot c_2^{\alpha_2} \cdots c_k^{\alpha_k}$ en la expresión

$$P_G((c_1 + \cdots + c_k), (c_1^2 + \cdots + c_k^2), \ldots, (c_1^n + \cdots + c_k^n))$$

donde $P_G(x_1, \ldots, x_n)$ es el índice de ciclos de G.

Demostración. El objetivo es ahora contar el número de coloraciones G-diferentes con el mismo peso. Daremos una idea de la demostración sin entrar en los detalles.

Denotamos por $\alpha = (\alpha_1, \ldots, \alpha_k)$ el peso de de la coloración f y denotamos por $(C^X)_\alpha$ las coloraciones de peso α. La aplicación $\tilde{\sigma}(f) = f\sigma$ es una permutación en $(C^X)_\alpha$, de manera que el conjunto $\tilde{G}$ de estas permutaciones es un grupo de permutaciones de $(C^X)_\alpha$. El lema de Burnside nos dice ahora que el número de coloraciones $\tilde{G}$-diferentes de $(C^X)_\alpha$ es

$$\frac{1}{\tilde{G}} \sum_{\tilde{\sigma} \in \tilde{G}} fix(\tilde{\sigma})$$

Las coloraciones fijadas por $\tilde{\sigma}$ son las que toman un valor constante sobre cada ciclo de la permutación σ. Por tanto, el número de coloraciones de peso α que quedan fijadas por una permutación σ de tipo $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ es el coeficiente de $c_1^{\alpha_1} \cdot c_2^{\alpha_2} \cdots c_k^{\alpha_k}$ en el desarrollo de

$$(c_1 + \cdots + c_k)^{\lambda_1} (c_2^2 + \cdots + c_k^2)^{\lambda_2} \cdots (c_1. + \cdots + c_k^n)^{\lambda_n}$$

de donde se obtiene el resultado. □

Veamos cómo se aplicaría este teorema en nuestro ejemplo. Recordando el índice de ciclos de G en la ecuación 10.1, tenemos

$$\begin{aligned} & P_G((\circ + \bullet), (\circ^2 + \bullet^2), (\circ^3 + \bullet^3), (\circ^4 + \bullet^4)) \\ &= \frac{1}{4}(\circ + \bullet)^4 + 2(\circ + \bullet)^2(\circ^2 + \bullet^2) + (\circ^2 + \bullet^2)^2 \\ &= \frac{1}{4}(4\circ^4 + 8\circ^3\bullet + 12\circ^2\bullet^2 + 8\circ\bullet^3 + 4\bullet^4) \end{aligned}$$

En la expresión se puede leer el número de coloraciones G-diferentes para cada distribución de colores. Por ejemplo, el coeficiente de $\circ\bullet^3$ nos dice que hay dos coloraciones G-diferentes que usan tres veces el color '$\bullet$' y una vez el color '$\circ$'.

Notas bibliográficas

La teoría de grupos es una disciplina que ha alcanzado una extensión enorme, especialmente en este siglo, y hay por tanto una bibliografía muy extensa. Como ejemplo de monografías

especializadas en el tema (para las cuales este capítulo podría ser una introducción), se puede mencionar el libro de Robinson [3], mientras que el de Wielandt [5] es una referencia clásica de los grupos de permutaciones. A un nivel más accesible y orientado a las aplicaciones, el libro de Stone [4] es una buena referencia. El texto original en el que Pólya introduce su teoría de enumeración se puede encontrar en una traducción inglesa [2]. Finalmente, el libro de Budden [1], de lectura amena e instructiva, hace una revisión bastante exhaustiva de todos los conceptos de la teoría de grupos y presenta algunas aplicaciones insólitas.

Bibliografía

[1] F. J. Budden. *The Fascination of Groups*. Cambridge University Press, 1972.

[2] G. Pólya, R. C. Read. *Combinatorial Enumeration of Groups, Graphs and Chemical Compounds*. Springer-Verlag, 1987.

[3] D. J. S. Robinson. *A Course in The Theory of Groups*. Springer-Verlag, 1982.

[4] H. S. Stone. *Discrete Mathematical Structures and their Applications*. Science Research Asociates, 1973.

[5] H. Wielandt. *Finite Permutation Groups*. Academic Press, 1964.

Problemas

1. Demostrar que un subgrupo de índice dos es siempre normal.

2. Demostrar que en un grupo de orden par siempre existe un elemento diferente del neutro de orden dos.

3. Demostrar que en cualquier grupo G se cumple para todo $a, b \in G$ que

   (a) $|ab| = |ba|$

   (b) $|aba^{-1}| = |b|$

   donde $|g|$ denota el orden de un elemento.

4. Demostrar que si H_1 y H_2 son subgrupos propios de un grupo finito G, entonces H_1H_2 es subgrupo de G si y sólo si $H_1H_2 = H_2H_1$. Demostrar también que

$$|H_1H_2| = |H_1| \cdot |H_2| / |H_1 \cap H_2|$$

5. Demostrar que $\mathbb{Z} \times \mathbb{Z}$ no tiene subgrupos de la forma $\mathbb{Z}_n \times \mathbb{Z}_m$.

6. Demostrar que si H_1 y H_2 son subgrupos normales de los grupos G_1 y G_2 respectivamente, entonces $H_1 \times H_2$ es subgrupo normal de $G_1 \times G_2$ y

$$(G_1 \times G_2)/(H_1 \times H_2) \simeq (G_1/H_1) \times (G_2/H_2)$$

7. Demostrar que si en un grupo finito G se cumple que para cualquier par de subgrupos F y H, $F \subset H$ o bien $H \subset F$, entonces G es cíclico y tiene orden potencia de un primo.

8. Demostrar que todo grupo cociente de un grupo cíclico es cíclico.

9. Demostrar que un grupo de orden $2p$, donde p es un número primo, o bien es cíclico, o bien es isomorfo al grupo diédrico D_p.

10. Demostrar que un grupo G es abeliano si y sólo si la aplicación $\phi : G \longrightarrow G$ dada por $\phi(g) = g^2$ es un endomorfismo de G.

11. Determinar el número de homomorfismos diferentes entre $\mathbb{Z}_2$ y $\mathbb{Z}_3$. Determinar este número, en general para $\mathbb{Z}_n$ y $\mathbb{Z}_m$ en función de n y de m.

12. Demostrar que la signatura de una permutación coincide con la de su inversa.

13. ¿Cuántos ciclos diferentes de longitud n hay en S_n?

14. Demostrar que, en un grupo de permutaciones, o bien la signatura de todas las permutaciones es par, o bien la mitad tiene signatura par y la otra mitad impar. ¿Cuál es la signatura de un grupo de permutaciones de orden impar?

15. Observar que la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 3 & 4 \end{pmatrix}$$

se puede expresar como producto de ciclos de longitud 3 como $(642)(531)(432)$. Demostrar que cualquier permutación de signatura par se puede expresar como producto de ciclos de longitud 3 (en general con intersecciones no vacías).

16. Demostrar que el número de permutaciones de S_n que se expresan en notación cíclica como un producto de k_1 1-ciclos, k_2 2-ciclos, en general k_j j-ciclos, $j = 1, \ldots, n$, es

$$\frac{1}{1^{k_1} 2^{k_2} \cdots n^{k_n}} \begin{pmatrix} n \\ k_1, \ldots, k_n \end{pmatrix}$$

siempre que $k_1 + 2k_2 + \cdots + nk_n = n$. ¿Cuántos n-ciclos hay en S_n?

17. Recordar que los números de Stirling de segundo tipo $\left\{ {n \atop k} \right\}$ cuentan el número de subconjuntos de tamaño k de un conjunto de n elementos. Sea ahora $s(n,k)$ el número de maneras de poner n elementos en k-ciclos. Por ejemplo, los elementos de $\{1,2,3,4\}$ se pueden poner en 2-ciclos como

$$\begin{array}{cccc} (123)(4) & (124)(3) & (134)(2) & (234)(1) \\ (132)(4) & (142)(3) & (143)(2) & (243)(1) \\ (12)(34) & (13)(24) & (14)(23) & \end{array}$$

de manera que $s(4,2) = 11$. Demostrar que $s(n,k)$ satisface la ecuación de recurrencia

$$s(n,k) = (n-1)s(n-1,k) + s(n-1,k-1)$$

Usando los resultados de la última sección del capítulo de funciones generadoras, deducir que $s(n,k) = \left[{n \atop k} \right]$, el número de Stirling de primer tipo.

18. Dibujar el grafo de Cayley del grupo alternado de 4 símbolos, A_4 respecto de los generadores $\sigma = (123)$ y $\tau = (12)(34)$.

19. Demostrar que todas las relaciones de un grupo finito G se pueden expresar a partir de las relaciones correspondientes a un conjunto de circuitos fundamentales del digrafo de Cayley $Cay(G,S)$.

20. Considerar el grafo que tiene por vértices los subconjuntos de $X = \{1,2,\ldots,n\}$, y en el que dos vértices son adyacentes cuando los correspondientes subconjuntos difieren en exactamente un elemento. Demostrar que el grafo que se obtiene es isomorfo al grafo de Cayley $Cay(\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2, \{e_1,\ldots,e_n\})$, donde $e_i = (0,\ldots,0,\overset{i)}{1},0,\ldots,0)$ (este grafo se llama *hipercubo de dimensión n*; ¿pueden imaginar por qué?).

21. Dado el digrafo de Cayley $Cay(G,S)$ dibujado en la figura 10.11, dar una presentación del grupo G.

22. Demostrar que el índice de ciclos de $\mathbb{Z}_6$ es

$$P_{\mathbb{Z}_6}(x_1,x_2,x_3,x_4,x_5,x_6) = \frac{1}{6}(x_1^6 + x_2^3 + 2x_3^2 + 2x_6)$$

Demostrar que, en general, el índice de ciclos de un grupo cíclico $\mathbb{Z}_n$ es

$$P_{\mathbb{Z}_n}(x_1,\ldots,x_n) = \frac{1}{n}\sum_{d|n} \phi(d) x_d^{n/d}$$

donde ϕ es la función de Euler.

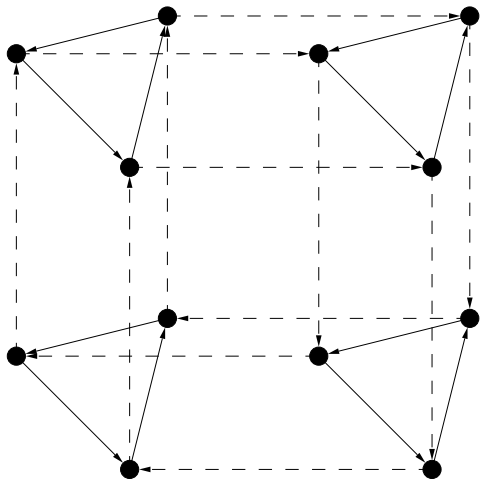


Figura 10.11: $Cay(G,S)$

23. Dos secuencias $(x_1x_2\ldots x_n)$, $(y_1y_2\ldots y_n)$ se dice que son cíclicamente iguales si sólo difieren en una rotación módulo n, es decir, $x_i = y_{i+k \bmod n}$ para $1 \leqslant i \leqslant n$. Por ejemplo, las secuencias 10011 y 00111 son cíclicamente iguales. Esta simetría circular aparece muy frecuentemente. ¿Cuántas secuencias de ceros y unos de longitud n circularmente diferentes hay? ¿Cuántas de estas secuencias de longitud 6 tienen exactamente tres unos?

24. Demostrar que el índice de ciclos del grupo D_3 de simetrías de un triángulo es

$$P_{D_3}(x_1,x_2,x_3) = \frac{1}{6}(x_1^3 + 3x_1x_2^2 + 2x_3^6)$$

En general, demostrar que el índice de ciclos del grupo D_n de simetrías de un polígono regular de n lados es

$$P_{D_n}(x_1,\ldots,x_n) = \frac{1}{2}P_{\mathbb{Z}_n}(x_1,\ldots,x_n) + \frac{1}{4}x_2^{n/2} + \frac{1}{4}x_1^2x_2^{(n/2)-1}$$

si n es par, y

$$P_{D_n}(x_1,\ldots,x_n) = \frac{1}{2}P_{\mathbb{Z}_n}(x_1,\ldots,x_n) + \frac{1}{2}x_1x_2^{(n-1)/2}$$

si n es impar.

25. ¿De cuántas maneras se pueden etiquetar con tres colores los vértices de un polígono regular de n lados si no distinguimos dos maneras que sólo difieren por una simetría del polígono?

26. Demostrar que el índice de ciclos del grupo simétrico S_n es

$$P(S_n;x_1,\ldots,x_n)=\sum_{\lambda}\frac{1}{\lambda_1!2^{\lambda_2}!\cdots n^{\lambda_n}\lambda_n!}x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}$$

donde el sumatorio se extiende a $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_n)$ tales que $\lambda_1+2\lambda_2+\cdots+n\lambda_n=n$. (Recordar la fórmula de Cauchy.)

27. Demostrar que el índice de ciclos del grupo alternado A_n es

$$P(A_n;x_1,\ldots,x_n)=\sum_{\lambda}\frac{1+(-1)^{\lambda_2+\lambda_4+\cdots}}{\lambda_1!2^{\lambda_2}!\cdots n^{\lambda_n}\lambda_n!}x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}$$

donde el sumatorio se extiende a $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_n)$ tales que $\lambda_1+2\lambda_2+\cdots+n\lambda_n=n$.