Álgebra moderna

Rubén Maguregui

Esta obra está publicada bajo la licencia *Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)*.
https://creativecommons.org/licenses/by-sa/4.0/deed.es

Índice general

Índice general v

Parte I Fundamentos 1

Capítulo I: Teoría de conjuntos 3

1.1 Conjuntos . . . 3
1.2 Subconjuntos . . . 7
1.3 Operaciones de conjuntos . . . 9

Capítulo II: Los números naturales 15

Capítulo III: Los números enteros 17

3.1 Números enteros . . . 17

Parte II Estructuras algebraicas 31

Capítulo IV: Teoría de grupos 33

4.1 Operaciones binarias; semigrupos y monoides . . . 33
4.2 Grupos . . . 38
4.3 Permutaciones . . . 43
4.4 Subgrupos . . . 51
4.5 Homomorfismos . . . 54
4.6 Grupos cíclicos . . . 55
4.7 Clases laterales; el teorema de Lagrange . . . 62
4.8 Subgrupos normales . . . 68
Ejercicios . . . 71
4.9 Grupos cociente . . . 72
4.10 Teoremas de isomorfía . . . 75
Ejercicios . . . 78

4.11 Acciones de grupo 78
Ejercicios 86

BIBLIOGRAFÍA 89

Parte I

Fundamentos

Capítulo I

Teoría de conjuntos

1.1 Conjuntos

En esta sección ofreceremos un estudio breve de las nociones básicas de la teoría de conjuntos, ya que esta materia proporciona los conceptos fundamentales a partir de los cuales podemos definir aquellos que son el objeto de estudio de este libro. Dado que nuestro interés en los fundamentos conjuntistas no va mucho más allá de fijar el lenguaje habitual en el que se expresan o se definen las nociones de prácticamente todas las matemáticas modernas, no tendremos ocasión de desarrollar la teoría de conjuntos con el cuidado y la formalidad que son necesarios para evitar ciertas complicaciones lógicas que surgen al examinar con detalle las ideas presentadas en esta sección (como es el caso, notablemente, del concepto mismo de conjunto), sino que aquí nos conformaremos con exponer la materia en su aspecto informal e intuitivo, enfoque comúnmente conocido como "teoría intuitiva de conjuntos", título que pretende distinguir dicho enfoque del estudio axiomático y formal de esta materia.

Así pues, apelamos a la intuición del lector y definimos informalmente un **conjunto** como una "colección" de objetos cualesquiera a la que concebimos como un todo. Los objetos que conforman a un conjunto se dicen sus **elementos**. Para indicar que un objeto x es un elemento de un conjunto A escribimos

$$x \in A.$$

La situación opuesta, de que x no es un elemento de A, se representa mediante la notación

$$x \notin A$$

Un aspecto esencial de nuestro concepto intuitivo de conjunto es que para todo objeto x y todo conjunto A, o bien tenemos que $x \in A$, o bien que $x \notin A$. También usaremos regularmente expresiones como

$$x, y \in A$$

para indicar el hecho de que $x \in A$ y $y \in A$, y ésta es una abreviación que, desde luego, podemos extender para indicar la pertenencia de cualquier número de elementos a un conjunto dado.

Es intuitivamente claro que, a parte de los elementos que contienen, no hay nada más que debería distinguir a dos conjuntos. Dicho de otro modo, todo conjunto está completamente definido por los elementos que contiene, algo que usualmente se expresa

diciendo que éste está determinado o definido por su "extensión". Esta característica de los conjuntos vistos como conceptos abstractos constituye el postulado que define la relación de igualdad entre conjuntos, conocido como "el principio de extensión":

Principio de extensión. *Dos conjuntos A y B son iguales si éstos consisten de los mismos elementos, lo cual se expresa escribiendo*

$$A = B.$$

Por lo tanto, en términos de la relación de pertenencia, $A = B$ representa el hecho de que $x \in A$ si y sólo si $x \in B$.

Para indicar que dos conjuntos no son iguales, escribiremos $A \neq B$. Por el principio de extensión, esto significa que existe al menos un objeto x tal que está en uno de los conjuntos pero no en el otro.

Las siguientes propiedades de la igualdad de conjuntos son inmediatas.

Proposición 1.1. *Para cualesquiera conjuntos A, B y C, se cumple que*

(a) $A = A$.

(b) $A = B$ *si y sólo si* $B = A$.

(c) *Si* $A = B$ *y* $B = C$, *entonces* $A = C$.

Aceptaremos la existencia de un conjunto sin elementos, que representaremos por $\varnothing$ y que llamaremos **conjunto vacío**. En símbolos, el conjunto vacío está caracterizado por que el enunciado

$$x \in \varnothing$$

es falso para cualquiera que sea el objeto x. Observemos que el principio de extensión implica que sólo puede existir un conjunto vacío, pues, al estar los conjuntos completamente determinados por los elementos que contienen, cualquier otro conjunto sin elementos será igual $\varnothing$, luego en realidad sólo existe un conjunto vacío.

Con la finalidad de proporcionar otros ejemplos concretos de conjuntos que faciliten la comprensión de los conceptos explicados en este capítulo, haremos uso de los conjuntos numéricos de las matemáticas elementales y supondremos conocidas del lector las propiedades básicas de los mismos. Para representar a dichos conjuntos numéricos, utilizaremos la simbología explicada a continuación:

- $\mathbb{N}$ para representar al conjunto de los números naturales[1],

$$0, 1, 2, 3, \ldots$$

- $\mathbb{Z}$ para representar al conjunto de los números enteros,

$$\ldots, -2, -1, 0, 1, 2, \ldots.$$

[1] La inclusión del cero dentro del conjunto de números naturales no es universal, y muchos autores optan por excluirlo en su definición de dicho conjunto. Así, para ellos, el conjunto de números naturales "inicia" en el 1, en cuyo caso "número natural" y "número entero positivo" resultan ser sinónimos.

- $\mathbb{Q}$ para representar al conjunto de los números racionales, es decir, a los números de la forma $\frac{a}{b}$ con a y b enteros.
- $\mathbb{R}$ para representar al conjunto de los números reales, los cuales incluyen tanto a los números racionales como a los números irracionales (o sea, aquellos que no pueden expresarse como un cociente $\frac{a}{b}$ de dos enteros a y b).
- $\mathbb{C}$ para representar al conjunto de los números complejos, que son los números de la forma $a + bi$ donde $a, b \in \mathbb{R}$ e $i = \sqrt{-1}$ es la unidad imaginara.

Es importante reiterar que cualquier mención o uso de dichos conjuntos y sus propiedades algebraicas no tiene otra finalidad que la que acabamos de mencionar, y que, por lo tanto, no intervienen para nada en el desarrollo de la teoría de conjuntos que se proporciona en este capítulo, pues de hecho es mediante la nociones básicas de la teoría de conjuntos estudiadas en este capítulo que podremos dar definiciones (o, mejor dicho, construcciones) de estos conjuntos numéricos y de sus propiedades algebraicas que asumimos conocidas por el lector.

También utilizaremos las notaciones $\mathbb{Z}^*$, $\mathbb{Q}^*$, etc., para representar al conjunto formado por los elementos positivos del conjunto a cuyo símbolo se añade el superíndice "$*$".

Usaremos diversas notaciones para representar conjuntos cuyos elementos son conocidos. La más simple de éstas consiste en listar los elementos de un conjunto dado encerrados entre llaves. Así, por ejemplo, el conjunto de los enteros positivos menores que seis está representado por

$$\{1, 2, 3, 4, 5\}.$$

Esta notación recibe comúnmente el nombre de "notación por extensión". Por supuesto, ella sólo es conveniente cuando el conjunto que se especifica no consiste de muchos elementos, si bien en ocasiones podemos utilizar abreviaciones con puntos suspensivos como en

$$\{1, 2, 3, \dots, 100\} \tag{1.1}$$

que obviamente se entiende como el conjunto de todos los enteros positivos menores o iguales que 100, o como en

$$\{1, 2, 3, \dots\},$$

que especifica al conjunto de todos los enteros positivos, o incluso también como en

$$\{1, 4, 9, 25, \dots\},$$

que inmediatamente reconocemos como el conjunto de los cuadrados perfectos.

Algo que debemos observar en torno a la notación por extensión es que, por ejemplo, las expresiones

$$\{1, 2, 3\}, \qquad \{3, 2, 1\}, \qquad \{1, 2, 2, 2, 3, 3\},$$

representan todas al mismo conjunto según se deduce del principio de extensión, pues todas ellas hablan del conjunto cuyos elementos son exactamente los enteros 1, 2 y 3. En cambio, los conjuntos

$$\{1, 2\} \qquad \text{y} \qquad \{\{1, 2\}\}$$

no son iguales, pues el primero consiste de dos elementos (los enteros 1 y 2) mientras que el segundo consiste de un solo elemento, el conjunto $\{1, 2\}$, o sea, que el segundo de los conjuntos consiste precisamente del primero de ellos, o sea que, en particular,

$$\{1, 2\} \in \{\{1, 2\}\}.$$

Este último ejemplo nos muestra que los objetos contenidos por un conjunto pueden ser a su vez conjuntos. Desde luego, esta situación de tener conjuntos dentro de otros conjuntos puede darse en niveles de profundidad arbitrarios. Para evitar monotonía en el lenguaje, es común hablar de una **colección de conjuntos** en lugar de un conjunto de conjuntos, y utilizar símbolos caligráficos como

$$\mathcal{A}, \quad \mathcal{B}, \quad \mathcal{C}, \ldots$$

para representar a los conjuntos de ese tipo.

Otra notación que se utiliza con frecuencia, y que no tiene la inconveniencia de la notación por extensión al trabajar con conjuntos de gran cantidad de elementos, es la llamada "notación por comprensión", la cual especifica a un conjunto indicando alguna propiedad que cumplen todos sus elementos (y solamente ellos). Con más detalle, en esta notación el conjunto de todos los elementos x para los cuales el enunciado $p(x)$ es cierto se representa por

$$\{x \mid p(x)\},$$

que se lee como "el conjunto de todos los x tales que $p(x)$". Así pues, tenemos que esta notación está caracterizada por la equivalencia

$$a \in \{x \mid p(x)\} \qquad \text{si y sólo si} \qquad p(a),$$

donde $p(a)$ es la proposición que resulta de sustituir x por un objeto específico a. Por ejemplo, el conjunto dado en (1.1) se puede representar también como

$$\{x \mid x \text{ es entero y } 1 \leq x \leq 100\},$$

donde el enunciado $p(x)$ que especifica a este conjunto es, por supuesto,

$$p(x) : \quad x \text{ es entero y } 1 \leq x \leq 100.$$

Notemos que no hay nada especial en la elección de la letra x como "variable" de un enunciado, y que el enunciado $p(x)$ es exactamente el mismo que el enunciado $p(y)$ siempre y cuando la letra y no estuviera ya presente en $p(x)$. Así, por ejemplo, el conjunto de los enteros positivos no mayores a 100 se puede representar también mediante $\{y \mid y \in \mathbb{Z} \text{ y } 1 \leq y \leq 100\}$. Por el contrario, en un enunciado como

$$p(x) : \quad x = 2y \text{ para algún entero } y,$$

que en términos más simples no hace más que afirmar que x es un entero par, no podemos considerar que $p(x)$ y $p(y)$ son lo mismo, pues con esa sustitución estaremos confundiendo el propósito de cada variable y habremos convertido el enunciado en

una proposición que de inmediato podemos juzgar como verdadera o falsa (o sea, que el resultado habrá sido similar a sustituir x por un objeto concreto y no una variable). En efecto, pues $p(y)$ resultaría ser la proposición $y = 2y$ para algún entero y, que es verdadera por que sí existe algún entero y (único en este caso)que es igual a su doble, y es precisamente $y = 0$. Desde luego, en este caso podemos elegir la letra z, o cualquier otra que no sea y, y expresar el mismo enunciado en términos de esa nueva letra:

$$p(z): \quad z = 2y \text{ para algún entero } y.$$

Una variación de la notación por comprensión que se usa con frecuencia consiste en escribir

$$\{x \in U \mid p(x)\} \tag{1.2}$$

para representar al conjunto de los elementos que satisfacen tanto el enunciado $x \in U$ como el enunciado $p(x)$, es decir, al conjunto $\{x \mid x \in U \text{ y } p(x)\}$. Dicha notación puede leerse como "el conjunto de todos los x en U tales que $p(x)$".

Así, por ejemplo, tenemos que el conjunto dado en (1.1) puede especificarse brevemente como

$$\{x \in \mathbb{Z}^* \mid x \leq 100\},$$

recordando que $\mathbb{Z}^*$ representa al conjunto de los enteros positivos.

Otra variación bastante conveniente de la notación por comprensión consiste en representar por

$$\{f(x) \mid p(x)\} \tag{1.3}$$

al conjunto que en la notación original quedaría representado por

$$\{y \mid y = f(x) \text{ para algún } x \text{ que cumple } p(x)\}.$$

La expresión (1.3) puede leerse como "el conjunto de todos los $f(x)$ donde $p(x)$". Por ejemplo,

$$\left\{n^2 \mid n \in \mathbb{Z}^*\right\} = \{1, 4, 9, 25, \ldots\}$$

es el conjunto de todos los n^2 donde n es un entero positivo, o sea, que se trata del conjunto de los cuadrados perfectos.

1.2 SUBCONJUNTOS

Una relación más general que la igualdad es la de la **inclusión** de conjuntos: decimos que un conjunto A es **subconjunto** de otro B, lo que en símbolos se expresa

$$A \subset B,$$

si todo elemento de A lo es también de B, o sea, cuando se cumple que

$$x \in A \qquad \text{implica} \qquad x \in B$$

para todo objeto x. Nótese que el hecho de que $A \subset B$ no excluye la posibilidad de que A y B sean iguales. Cuando sí queda descartada esa posibilidad, decimos que A es un **subconjunto propio** de B, cosa que indicaremos con la notación[2]

$$A \subsetneq B.$$

Las siguientes propiedades de la inclusión de conjuntos son evidentes.

Proposición 1.2. *Sean A, B y C conjuntos cualesquiera. Entonces*

(a) $A \subset A$.

(b) $A \subset B$ *y* $B \subset A$ *si y sólo si* $A = B$.

(c) *Si* $A \subset B$ *y* $B \subset C$, *entonces* $A \subset C$.

Otro verdad trivial sobre la inclusión involucra al conjunto vacío, y es que

$$\varnothing \subset A,$$

para cualquiera que sea el conjunto A. Quizá la forma más fácil de convencerse de ese hecho es notar que la única cosa que lo haría falso sería encontrar un elemento x que esté en $\varnothing$ pero no en A y concluir que eso es imposible por que el conjunto vacío no contiene ningún elemento.

En este punto es conveniente comentar sobre una representación gráfica de los conjuntos que ocurren en una situación dada y que en muchas ocasiones facilita la comprensión de las relaciones que existen entre dichos conjuntos. Nos referimos a los llamados **diagramas de Venn**, en los que los conjuntos se dibujan como figuras cerradas cuyo interior representa los elementos contenidos por el conjunto. Así, por ejemplo, el diagrama de la figura 1.1 ilustra adecuadamente la situación de que $A \subset B$.

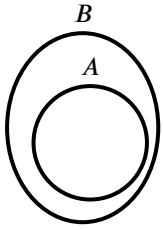


Figura 1.1. Representación de la inclusión $A \subset B$ de un conjunto A en un conjunto B.

Sin embargo, el lector debe tener cierto cuidado y dibujar diagramas de Venn de tal manera que éstos exhiban la suficiente generalidad que requieran los conjuntos que se pretenden representar, o, en su defecto, el lector debe hacer abstracción de estos

[2] En algunos textos, encontrará el lector el uso del símbolo "$\subseteq$" para indicar la inclusión de conjuntos, y reservado el uso del símbolo "$\subset$" para la inclusión propia. Por lo tanto, el lector debe consultar las definiciones relevantes siempre que existan dudas sobre la notación empleada por un autor dado.

diagramas a fin de no deducir de ellos detalles específicos que no tienen los conjuntos considerados. Así, por ejemplo, en ocasiones será necesario imaginar la posibilidad de que, en un diagrama como el de la figura 1.1, los conjuntos A y B sean iguales a pesar de que las representaciones gráficas sugieran otra cosa.

Al conjunto conformado por todos los subconjuntos de un conjunto A lo llamamos **conjunto potencia** de A, y lo representamos por $\mathcal{P}(A)$.

Ejemplo 1.3. Sea $A = \{1, 2, 3\}$. Entonces

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$ ◂

Proposición 1.4. *Si A es un conjunto de n elementos, entonces $|\mathcal{P}(A)| = 2^n$.*

Demostración: Consideremos un subconjunto S de A y, para todo objeto $x \in A$, definamos $p(x) = 1$ si $x \in S$ y $p(x) = 0$ si $x \notin S$. Entonces el conjunto S está completamente determinado por los valores $p(x)$, lo que significa que S puede formarse de tantas maneras distintas como podamos asignar los valores 1 y 0 a $p(x)$ para cada $x \in A$. Puesto que existen 2^n formas de hacer dichas asignaciones (pues para cada $x \in A$ existen dos posibilidades para el valor de $p(x)$, y en total hay $n = |A|$ elementos x en A), tenemos que S puede formarse de 2^n formas distintas. En otras palabras, existen 2^n subconjuntos de A. ■

1.3 OPERACIONES DE CONJUNTOS

Las operaciones con conjuntos nos permiten obtener nuevos conjuntos a partir de otros. Por ejemplo, si A y B son dos conjuntos, la **unión** de A y B es el conjunto formado por todos los elementos de A y todos los elementos de B, y se representa por $A \cup B$. En símbolos,

$$x \in A \cup B \qquad \text{si y sólo si} \qquad x \in A \quad \text{o} \quad x \in B,$$

o sea,

$$A \cup B = \{x \mid x \in A \text{ o } x \in B\}.$$

Observemos que la disyunción "o" de la definición anterior se debe interpretar en el sentido matemático (o lógico) usual, de manera que se satisface (o sea, es verdadera) en los casos en que x es elemento de A, en que x es elemento de B y en que x es elemento de ambos conjuntos.

Por su parte, la **intersección** de dos conjuntos A y B, representada por $A \cap B$, es el conjunto conformado por los elementos que A y B tienen en común, o sea que

$$x \in A \cap B \qquad \text{si y sólo si} \qquad x \in A \quad \text{y} \quad x \in B,$$

o bien,

$$A \cap B = \{x \mid x \in A \text{ y } x \in B\}.$$

Recordando la notación usada en la expresión (1.2), podríamos escribir también $A \cap B = \{x \in A \mid x \in B\}$ (o, desde luego, $A \cap B = \{x \in B \mid x \in A\}$).

En la figura 1.2 se representan las operaciones de unión e intersección de conjuntos mediante regiones sombreadas en un diagrama de Venn.

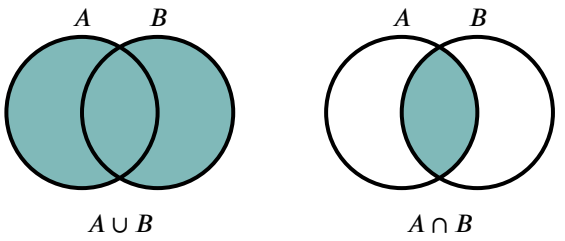


Figura 1.2. Unión e intersección de dos conjuntos A y B representada por el área sombreada.

Ejemplo 1.5. Sean $A = \{1, 2, 3, 4, 5, 6\}$ y $B = \{5, 6, 7, 8, 9\}$. Tenemos

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \qquad \text{y} \qquad A \cap B = \{5, 6\}. \qquad \blacktriangleleft$$

Es claro que la unión resulta en un conjunto mayor que cualquiera de los conjuntos que la forman. Para ser más precisos, es claro que

$$A \subset A \cup B \tag{1.4}$$

para cualesquiera que sean los conjuntos A y B. La igualdad $A = A \cup B$ se da, por supuesto, cuando $B \subset A$, pues en ese caso B no contribuye con ningún elemento adicional a la unión. En particular, $A \cup A = A$. Por su parte, la intersección de dos conjuntos resulta en un conjunto menor que cualquiera de ellos, en el sentido de que

$$A \cap B \subset A \tag{1.5}$$

para cualesquiera que sean los conjuntos A y B. En esta caso la igualdad $A = A \cap B$ se da con la inclusión inversa a la que se necesita para la unión, es decir, con $A \subset B$. Similar a como ocurre para la unión, tenemos el caso particular $A \cap A = A$.

Recogemos éstas y otras propiedades elementales de la unión y la intersección en la proposición siguiente.

Proposición 1.6. *La unión y la intersección de conjuntos verifican las propiedades siguientes:*

(a) *El conjunto vacío es neutro respecto de la unión y absorbente respecto de la intersección. Esto es, para cualquier conjunto A,*

$$A \cup \varnothing = A \quad y \quad A \cap \varnothing = \varnothing$$

(b) *Si U es un conjunto y $A \subset U$, entonces*

$$A \cup U = A \quad y \quad A \cap U = A.$$

(c) *Leyes de idempotencia: para todo conjunto A,*

$$A \cup A = A \quad y \quad A \cap A = A.$$

(d) *Leyes asociativas: para cualesquiera conjuntos A, B y C,*

$$(A \cup B) \cup C = A \cup (B \cup C) \quad y \quad (A \cap B) \cap C = A \cap (B \cap C).$$

(e) *Leyes conmutativas: para cualesquiera conjuntos A y B,*

$$A \cup B = B \cup A \quad y \quad A \cap B = B \cap A.$$

(f) *Leyes distributivas: para cualesquiera conjuntos A, B y C,*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad y \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Demostración: Demostraremos únicamente la distributividad de la unión sobre la intersección enunciada en (f) y dejaremos el resto como ejercicio al lector. Para establecer que

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \tag{1.6}$$

es necesario demostrar que todo elemento del miembro izquierdo lo es también del derecho y que, recíprocamente, todo elemento del miembro derecho lo es del izquierdo. Supongamos pues que $x \in A \cup (B \cap C)$. Se sigue de esto que $x \in A$ o $x \in B \cap C$. Si ocurre lo primero, es decir, si $x \in A$, entonces $x \in A \cup B$ y $x \in A \cup C$, luego $x \in (A \cup B) \cap (A \cup C)$. Pero esto mismo es cierto si ocurre que $x \in B \cap C$, pues en ese caso $x \in B$ y $x \in C$, y así de nuevo $x \in (A \cup B) \cap (A \cup C)$. Esto prueba la inclusión

$$A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C),$$

pero como es evidente que todos los pasos que nos llevaron a esta conclusión son invertibles, resulta que también $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$, luego queda demostrada la igualdad (1.6). ■

Si A y B son dos conjuntos, se define la **diferencia** de A y B (en ese orden) como el conjunto formado por todos los elementos de A que no están en B (véase la figura 1.3). A este conjunto lo representaremos por $A \setminus B$. Así pues,

$$A \setminus B = \{x \mid x \in A \text{ y } x \notin B\}.$$

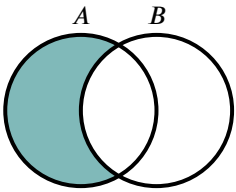
Ejemplo 1.7. Si $A = \{1, 2, 3, 4, 5, 6\}$ y $B = \{5, 6, 7, 8, 9\}$, entonces

$$A \setminus B = \{1, 2, 3, 4\} \qquad \text{y} \qquad B \setminus A = \{7, 8, 9\}. \quad ◂$$

Ejemplo 1.8. Demostrar que $A \setminus B = \varnothing$ si y sólo si $A \subset B$. ◂

Cuando B es un subconjunto de A, la diferencia $A \setminus B$ se dice también **complemento** de B en A (véase la figura 1.4).

En ocasiones es cómodo convenir en que todos los conjuntos considerados en un contexto dado están incluidos en cierto conjunto U al que nos referimos como **conjunto universo**. Desde luego, diferentes contextos tendrán diferentes conjuntos universos y



$A \setminus B$

Figura 1.3. Diferencia de dos conjuntos A y B representada por el área sombreada.

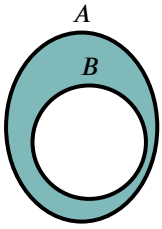


Figura 1.4. Complemento $A \setminus B$ del conjunto B en el conjunto A.

en ocasiones no es relevante aclarar cuál es el conjunto universo específico que se está considerando. Una de las ventajas de suponer que contamos con un conjunto universo es que podemos simplificar algunas notaciones. Por ejemplo, usaremos la notación $\overline{A}$ para representar al complemento de A en su conjunto universo, como lo ilustra el diagrama de Venn siguiente:

▸ **Ejercicio 1.9.** Demostrar que $A \setminus B = A \cup \overline{B}$.

La proposición siguiente nos habla de una relación importante que involucra las tres operaciones de conjuntos que hemos introducido.

Proposición 1.10 (Leyes de De Morgan). *Para cualesquiera conjuntos A, B y C,*

(a) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

(b) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

En particular,

(c) $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

(d) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Demostración: Demostraremos (a) y dejaremos el resto como ejercicio para el lector. Sea $x \in A \setminus (B \cup C)$. Entonces $x \in A$ y $x \notin (B \cup C)$. De la última relación se deduce

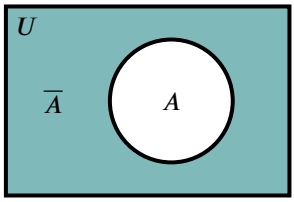


Figura 1.5. Complemento de un conjunto A en su conjunto universo

que $x \notin B$ y $x \notin C$, así que, como $x \in A$, tenemos $x \in A \setminus B$ y $x \in A \setminus C$, luego $x \in (A \setminus B) \cap (A \setminus C)$. Esto prueba que

$$A \setminus (B \cup C) \subset (A \setminus B) \cap (A \setminus C).$$

Invirtiendo el argumento se demuestra la inclusión inversa, lo que establece la igualdad deseada. ■

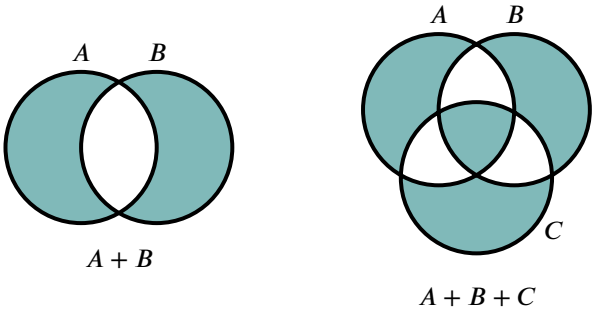


Figura 1.6. Diferencia simétrica de dos y de tres conjuntos.

Otra operación con conjuntos que nos va a interesar es la **diferencia simétrica**. Si A y B son dos conjuntos, la diferencia simétrica de A y B es el conjunto

$$A + B = (A \setminus B) \cup (B \setminus A).$$

La figura 1.6 nos permite apreciar fácilmente que $A + B = (A \cup B) \setminus (A \cap B)$. Demostrar este hecho formalmente se deja como ejercicio al lector.

Vamos ahora a generalizar las operaciones de unión e intersección para que éstas apliquen a una colección arbitraria de conjuntos. Si $\mathcal{C}$ es una colección de conjuntos, definimos la **unión de los conjuntos** de $\mathcal{C}$, representada por $\bigcup \mathcal{C}$, como el conjunto

$$\bigcup \mathcal{C} = \{x \mid x \in A \text{ para algún } A \in \mathcal{C}\},$$

o sea que $x \in \bigcup \mathcal{C}$ si y sólo si x es un elemento de al menos uno de los conjuntos contenidos en $\mathcal{C}$. Por su parte, la **intersección de los conjuntos** de $\mathcal{C}$, representada por

$\bigcap \mathcal{C}$, es el conjunto

$$\bigcap \mathcal{C} = \{x \mid x \in A \text{ para todo } A \in \mathcal{C}\},$$

es decir, $x \in \bigcap \mathcal{C}$ si y sólo si x es un elemento de cada uno de los conjuntos contenidos en $\mathcal{C}$.

Ejemplo 1.11. Si A y B son conjuntos, entonces está claro que la unión de los conjuntos de la colección $\{A, B\}$ se reducen a las operaciones ya conocidas,

$$\bigcup\{A, B\} = A \cup B \qquad \text{y} \qquad \bigcap\{A, B\} = A \cap B. \qquad \blacktriangleleft$$

Ejemplo 1.12. Para cada número natural n, definamos el conjunto $I_n = \{0, \dots, n\}$, de tal modo que, por ejemplo,

$$I_0 = \{0\}, \qquad I_1 = \{0, 1\}, \qquad I_2 = \{0, 1, 2\}, \qquad I_3 = \{0, 1, 2, 3\}, \dots$$

Entonces

$$\bigcup\{I_n \mid n \in \mathbb{N}\} = \{0, 1, 2, 3, \dots\} = \mathbb{N},$$

pues todo número natural k está en al menos un I_n (concretamente, $k \in I_k$, y más en general, $k \in I_n$ si $n \geq k$). Por otra parte,

$$\bigcap\{I_n \mid n \in \mathbb{N}\} = \{0\},$$

pues $0 \in I_n$ para todo n y no hay otro número natural que cumpla esto, pues $k \notin I_n$ si $k > n$. $\blacktriangleleft$

Ejemplo 1.13. Sea A un conjunto cualquiera y sea $\mathcal{C}$ el conjuntos de todos los subconjuntos de A, es decir, el conjunto potencia $\mathcal{P}(A)$. Entonces $\bigcup \mathcal{C} = A$ y $\bigcap \mathcal{C} = \varnothing$. $\blacktriangleleft$

Proposición 1.14. *Sea $\mathcal{C}$ una colección no vacía de conjuntos y S un conjunto cualquiera. Se verifican las leyes distributivas*

$$S \cap \bigcup_{A \in \mathcal{C}} A = \bigcup_{A \in \mathcal{C}} (S \cap A) \qquad y \qquad S \cup \bigcap_{A \in \mathcal{C}} A = \bigcap_{A \in \mathcal{C}} (S \cup A).$$

Capítulo II

Los números naturales

Capítulo III

Los números enteros

3.1 Números enteros

Teorema 3.1 (Algoritmo de la división). *Para cualesquiera enteros x y y con $y > 0$, existen enteros únicos q y r tales que*

$$x = qy + r \qquad con\ 0 \leq r < y. x = qy + r \qquad con\ 0 \leq r < y.$$

Demostración: Consideremos el conjunto $S = \{x - ky \geq 0 \mid k \in \mathbb{Z}\}$. Este conjunto es no vacío, pues por ejemplo $x - ky \geq 0$ para $k = -|x|$, así que el principio de buen ordenamiento de $\mathbb{N}$ nos dice que $S \subset \mathbb{N}$ tiene un mínimo, digamos $r = x - qy$. Entonces $x = qy - r$ con $0 \leq r < y$, pues si no fuese así tendríamos $0 \leq r - y = (x - qy) - y = x - (q + 1)y$ y por tanto $r - y \in S$, en contradicción con la elección de r como el mínimo de S.

Para demostrar la unicidad de q y r, supongamos que q' y $'r$ son enteros que cumplen lo mismo. Entonces $q'y + r' = qy + r$ y por tanto $(q' - q)y = r - r'$. Pesto que $y > 0$, esto implica que $|q' - q|\ y = |r - r'|$, de donde se sigue que $|q' - q| = 0$, pues de otro modo $|r - r'|$ sería mayor que y, lo que no puede ser por que $0 \leq r, r' < y$. Concluimos entonces que $q' = q$, y de aquí que $r' = r$. Esto demuestra que q y r son los únicos enteros con las propiedades indicadas en el teorema. ■

Definición 3.2. A los elementos q y r del teorema anterior los llamamos **cociente** y **residuo** de la división de x por y, respectivamente.

Ejemplo 3.3. Consideremos los enteros 26 y 7. Tenemos que

$$26 = 3 \cdot 7 + 5$$

con $5 < 7$, así que el cociente y el residuo de dividir 26 por 7 son 3 y 5, respectivamente. Por otra parte, el cociente y el residuo de dividir 7 por 26 son 0 y 7, pues

$$7 = 0 \cdot 26 + 7$$

con $7 \leq 26$. En general, es claro que si $0 \leq x < y$, entonces el cociente y el residuo de dividir x por y son 0 y x. ¿Qué podemos decir del caso en que $x < 0 < y$? ◂

Observemos que si r es el residuo de dividir x por y, entonces el algoritmo de la división nos dice que

$$r \in \{1, 2, 3, \ldots, y-1\}.$$

Ejemplo 3.4. Todo cuadrado perfecto deja residuo de 0 o 1 al ser dividido entre 4. En efecto, pues si $n \in \mathbb{Z}$ entonces $n = q \cdot 2 + r$ con $r = \{0, 1\}$, y por tanto

$$n^2 = 4q^2 + 4qr + r = 4(q^2 + qr) + r^2$$

con $r^2 = 0$ o $r^2 = 1$, luego $r^2 < 4$ es el residuo de dividir n^2 entre 4. ◂

Vamos ahora a extender el teorema 3.1 para incorporar el caso $y < 0$.

Corolario 3.5. *Para cualesquiera entero x y y con $y \neq 0$, existen enteros únicos q y r tales que*

$$x = qy + r \qquad \text{con } 0 \leq r < |y|\,.$$

Demostración: Lo sabemos para $y > 0$. Supongamos entonces que $y < 0$, de manera que $-y > 0$. Por el teorema 3.1, existen enteros únicos $\overline{q}$ y r tales que $x = \overline{q}(-y) + r$ con $0 \leq r < (-y) = |y|$, luego $q = -\overline{q}$ y r son los números buscados. ■

Vamos a introducir una notación que resulta conveniente para expresar los cocientes de las divisiones de enteros. Si α es un número real cualquiera, la expresión $\lfloor \alpha \rfloor$ representa al mayor de los enteros menores que α. Por ejemplo,

$$\lfloor 4.6 \rfloor = 4, \qquad \left\lfloor \sqrt{2} \right\rfloor = 1, \qquad \lfloor \pi \rfloor = 3, \qquad \lfloor -2.3 \rfloor = -3.$$

El último de estos ejemplos nos muestra que $\lfloor \alpha \rfloor$ nos da la parte entera de α únicamente cuando $\alpha \geq 0$. Por otra parte, si α mismo es entero entonces obviamente $\lfloor \alpha \rfloor = \alpha$.

Similarmente, tenemos la notación $\lceil \alpha \rceil$, que representa al menor de los enteros mayores que α. Así,

$$\lceil 4.6 \rceil = 5, \qquad \left\lceil \sqrt{2} \right\rceil = 2, \qquad \lceil \pi \rceil = 4, \qquad \lceil -2.3 \rceil = -2.$$

De nuevo, es claro que si α es entero entonces $\lceil \alpha \rceil = \alpha$. Por otra parte, en general se cumple que

$$\lfloor -\alpha \rfloor = -\lceil \alpha \rceil \qquad \text{y} \qquad \lceil -\alpha \rceil = -\lfloor \alpha \rfloor\,.$$

Proposición 3.6. *Si x y $y \neq 0$ son enteros cualesquiera, entonces el cociente de dividir x por y es $\left\lfloor \frac{x}{y} \right\rfloor$ si $y > 0$ y es $\left\lceil \frac{x}{y} \right\rceil$ si $y < 0$.*

Demostración: Si q y r son el cociente y el residuo de dividir x por $y > 0$, entonces

$$\frac{x}{y} = q + \frac{r}{y}, \qquad \text{con } 0 \leq \frac{r}{y} < 1,$$

luego $q = \lfloor q + r/y \rfloor = \lfloor x/y \rfloor$. Si $y < 0$ y $\overline{q}$ es el cociente de dividir x por $-y$, entonces $q = -\overline{q}$ es el residuo de dividir x por y, de modo que $q = -\lfloor -x/y \rfloor = \lceil x/y \rceil$. ■

Ejemplo 3.7.

- El cociente de dividir 26 por 7 es $\left\lfloor \frac{26}{7} \right\rfloor = \left\lfloor 3.\overline{714285} \right\rfloor = 3$ y el residuo es $26 - 3 \cdot 7 = 5$.
- El cociente de dividir 26 por -7 es $\left\lceil \frac{26}{-7} \right\rceil = \left\lceil -3.\overline{714285} \right\rceil = -3$, y el residuo es de nuevo $r = 26 - (-3)(-7) = 5$.
- El cociente de dividir -26 entre 7 es $\left\lfloor -\frac{26}{7} \right\rfloor = -4$, con residuo $r = -26 - (-4)(7) = 2$.
- El cociente de dividir -26 por -7 es $\left\lceil \frac{-26}{-7} \right\rceil = 4$, con residuo $r = -26 - 4(-7) = 2$.

◀

Definición 3.8. Si x y y son dos enteros, decimos que x **divide** a y, en símbolos

$$x \mid y,$$

si existe un entero q tal que $y = qx$. Otra forma de indicar que x divide a y es decir que x es un **factor** (o **divisor**) de y, o también que y es un **múltiplo** de x.

Otros hechos elementales sobre la divisibilidad de enteros se enuncian en la proposición siguiente.

Proposición 3.9. *Si $x, y, x', y' \in \mathbb{Z}$, se verifican las afirmaciones siguientes:*

(a) *si $x \mid y$ y $x' \mid y'$, entonces $xx' \mid yy'$;*

(b) *si $k \neq 0$, entonces $x \mid y$ si y sólo si $kx \mid ky$.*

(c) *si $x \mid y$ y $y \neq 0$, entonces $|x| \leq |y|$.*

(d) *$x \mid y$ y $y \mid x$ si y sólo si $x = \pm y$.*

Demostración: Demostraremos (4) y dejaremos el resto como ejercicio al lector. Si $x = \pm y$ entonces $y = \pm x$ y por lo tanto $x \mid y$ y $y \mid x$. Recíprocamente, si $x \mid y$ y $y \mid x$, entonces $x, y \neq 0$ y por lo tanto $|x| \leq |y|$ y $|y| \leq |x|$ de acuerdo con el apartado (3), o sea que $|x| = |y|$, luego $x = \pm y$. ■

Definición 3.10. Si x y y son dos enteros no nulos, el **máximo común divisor** de éstos es el mayor de los enteros que dividen tanto a x como a y. A dicho número lo representaremos por $\text{mcd}\,(x, y)$. Cuando $\text{mcd}\,(x, y) = 1$, se dice que x y y son **primos relativos**.

El siguiente teorema describe un procedimiento eficiente de calcular el máximo común divisor.

Teorema 3.11 (Algoritmo de Euclides). *Sean x y y enteros no nulos y sean $(r_k)_k$ y $(q_k)_k$ las sucesiones de residuos y de cocientes, respectivamente, definidas por las relaciones recursivas siguientes:*

$$\begin{aligned} x &= q_1 y + r_1, & 0 \leq r_1 < y, \\ y &= q_2 r_1 + r_2, & 0 \leq r_2 < r_1, \\ r_{k-2} &= q_k r_{k-1} + r_k, & 0 \leq r_k < r_{k-1} \text{ o } r_k = 0. \end{aligned}$$

Entonces $\operatorname{mcd}(x, y) = r_m$ *con m el menor número natural tal que* $r_{m+1} = 0$.

Demostración: Puesto que $\operatorname{mcd}(x, y) = \operatorname{mcd}(\pm x, \pm y)$, basta enfocarnos únicamente en el caso $x, y > 0$. Por el algoritmo de la división, las sucesiones $(q_k)_k$ y $(r_k))_k$ definidas de esta manera existen. Puesto que $r_{k-1} > r_k$ o $r_k = 0$, la sucesión de residuos es monótona decreciente, o sea que $r_k = 0$ para cierto entero k, por lo que existe el menor entero positivo m tal que $r_{m+1} = 0$, es decir,

$$\begin{aligned} x &= q_1 y + r_1, & 0 \leq r_1 < y, \\ y &= q_2 r_1 + r_2, & 0 \leq r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, & 0 \leq r_3 < r_2, \\ &\vdots & \\ r_{m-2} &= q_m r_{m-1} + r_m, & 0 \leq r_m < r_{m-1} \\ r_{m-1} &= q_{m+1} r_m, & r_{m+1} = 0. \end{aligned}$$

Observamos que r_m, el menor de los términos no nulos de $(r_k)_k$, divide a r_{m-1}, luego también divide a r_{m-2}, y continuando de esta manera concluimos que r_m es un divisor común de x y y. Si $d = \text{máx}(x, y)$, entonces $r_m \leq d$, pero las ecuaciones de arriba muestran que d divide a r_1, luego también a r_2, y así sucesivamente hasta encontrar que divide a r_m, así que $d \leq r_m$. Concluimos entonces que $r = d$, como lo afirma el teorema. ■

Ejemplo 3.12. Encontraremos $\operatorname{mcd}(2352, 350)$. Para dicho par de números, el algoritmos de Euclides se desarrolla así:

$$\begin{aligned} 2352 &= 6(350) + 252 \\ 350 &= 1(252) + 98 \\ 252 &= 2(98) + 56 \\ 98 &= 1(56) + 42 \\ 56 &= 1(42) + 14 \\ 42 &= 3(14). \end{aligned}$$

Por lo tanto, $\operatorname{mcd}(2352, 350) = 14$. ◂

El teorema siguiente establece una caracterización importante del máximo común divisor.

Teorema 3.13 (Identidad de Bézout). *Para cualesquiera enteros no nulos x y y existen enteros s y t tales que $sx + ty = \mcd(x, y)$. Con más detalle,* $\mcd(x, y)$ *es el menor de los enteros positivos de la forma $sx + ty$ con $s, t \in \mathbb{Z}$.*

Demostración: Sea $S = \{kx + ly \mid k, l \in \mathbb{Z}, kx + ly > 0\}$. Este conjunto es no vacío, pues, por ejemplo, $xx + yy = x^2 + y^2 > 0$. Por lo tanto, el principio de buen ordenamiento de $\mathbb{N}$ nos dice que S tienen un mínimo, sigamos $d = sx + ty$. Vamos a comprobar que $d = \mcd(x, y)$. Por el algoritmo de la división, $x = qd + r$ con $0 \leq r < d$. Puesto que

$$r = x - qd = x - q(sx + ty) = x - qsx - qty = (1 - qs)x + (-qt)y,$$

no puede ser $r > 0$, pues de otro modo r estaría en S, en contradicción con la minimalidad de d en S. Por lo tanto, debemos tener $r = 0$, así que d divide a x. De manera similar se comprueba que $d \mid r$, por lo que d es un divisor común de x y y. Si d' es otro divisor común de x y y, existen $a, b \in \mathbb{Z}$ tales que $d = sx + ty = sad' + tbd'$, lo que muestra que d' divide a d y por tanto $d' \leq d$, así que d es el máximo común divisor de x y y.■

Definición 3.14. Si $x_1, \ldots, x_n$, son enteros, a los enteros de la forma

$$s_1x_1 + \cdots s_nx_n,$$

con $s_1, \ldots, s_n \in \mathbb{Z}$, los llamamos **combinaciones lineales** de $x_1, \ldots, x_n$.

Proposición 3.15. *Si $x \in \mathbb{Z}$ divide a cada uno de los enteros $y_1, \ldots, y_n$, entonces x divide a toda combinación lineal de éstos.*

La proposición anterior, cuya demostración es inmediata y se deja como ejercicio al lector, nos dice en particular que toda combinación lineal de x y y es un múltiplo de su máximo común divisor. Por otra parte, de la identidad de Bézout se deduce que, recíprocamente, todo múltiplo de $\mcd(x, y)$ es una combinación lineal de x y y.

Corolario 3.16. *Si x y y son enteros no nulos, la ecuación $sx + ty = n$ tiene soluciones enteras s y t si y sólo si n es un múltiplo de* $\mcd(x, y)$. *En particular, $sx+ty = n$ siempre tiene soluciones cuando x y y son primos relativos.*

Ejemplo 3.17. Encontraremos las soluciones enteras a la ecuación $280s + 231t = 21$. Aplicando el algoritmo de Euclides, obtenemos

$$\begin{aligned} 280 &= 1(231) + 49, \\ 231 &= 4(49) + 35, \\ 49 &= 1(35) + 14, \\ 35 &= 2(14) + 7, \\ 14 &= 2(7), \end{aligned}$$

o sea que $\mcd(280, 231) = 7$. Puesto que 7 divide a 21, la ecuación planteada sí tiene soluciones enteras por el corolario 3.16. Resolviendo para cada residuo en las ecuaciones

de arriba y sustituyendo de abajo hacia arriba, obtenemos

$$\begin{aligned} 7 &= 35 - 2(14) \\ &= [231 - 4(49)] - 2[49 - (231 - 4(49))] \\ &= 3(231) - 14(49) \\ &= 3(231) - 14(280 - 231) \\ &= -14(280) + 17(231). \end{aligned}$$

Por lo tanto, $21 = -42(280) + 51(231)$, así que las soluciones a la ecuación del problema son $s = -42$, $t = 51$. ◀

Ejemplo 3.18. Encontraremos enteros x y y tales que $91x + 221y = 1053$. Mediante el algoritmo de Euclides, obtenemos

$$\begin{aligned} 221 &= 2(91) + 39, \\ 91 &= 2(39) + 13, \\ 39 &= 3(13), \end{aligned}$$

por lo que $\text{mcd}\,(91, 221) = 13$, el cual divide a 1053 y así sabemos que la ecuación $91x + 221y = 1053$ sí tiene soluciones enteras. Trabajando con este desarrollo del algoritmo de Euclides de abajo hacia arriba, encontramos que

$$\begin{aligned} 13 &= 91 - 2(39) \\ &= 91 - 2(221 - 2(91)) \\ &= 5(91) - 2(221). \end{aligned}$$

Multiplicando ambos miembros por 81, obtenemos

$$91(405) - 221(162) = 1053,$$

así que las soluciones de la ecuación son $x = 405$ y $y = -162$. ◀

Las soluciones encontradas con el procedimiento de los ejemplos anteriores no son únicas.

▸ **Ejercicio 3.19.** Encontrar enteros $x \neq 405$ y $y \neq -162$ tales que $91x + 221y = 1053$.

Solución: Ya que contamos con las soluciones $x = 405$ y $y = -162$, podemos investigar valores enteros a y b tales que

$$91(405 + a) + 221(-162 + b) = 1053.$$

Despejando a, observamos que dichos números deben satisfacer $b = -7a/17$, luego basta elegir a como cualquier múltiplo de 17. Por ejemplo, para $a = 17$ tenemos $b = -7$, y en efecto

$$91(405 + 17) + 221(-162 - 7) = 91(422) + 221(-169) = 1053,$$

así que $x = 422$ y $y = -169$ constituyen otro par de soluciones enteras a la ecuación $91x + 221y = 1053$.

Recordemos que dos enteros x y y se dicen primos relativos cuando no tienen más divisor común que la unidad, o sea que $\mathrm{mcd}\,(x, y) = 1$. La identidad de Bézout nos da una forma alternativa de caracterizar esta situación:

Corolario 3.20. *Dos enteros x y y son primos relativos si y sólo si existen enteros s y t tales que $sx + ty = 1$.*

Corolario 3.21. *Para cualesquiera $x, y \in \mathbb{Z}$, $d = \mathrm{mcd}\,(x, y)$ si y sólo si x/d y y/d son primos relativos.*

Corolario 3.22. *Sean $a, x, y \in \mathbb{Z}$. Si $a \mid xy$ y $\mathrm{mcd}\,(a, x) = 1$, entonces $a \mid y$.*

Demostración: Puesto que $\mathrm{mcd}\,(a, x) = 1$, el corolario 3.20 nos dice que existen $s, t \in \mathbb{Z}$ tales que $sa + tx = 1$, o sea que $y = say + txy$, donde cada término es divisible entre a, luego $a \mid y$. ∎

Definición 3.23. Un entero $p > 1$ se dice **primo** si no tiene más divisores positivos que él mismo y la unidad. Un entero positivo $x > 1$ que no es primo, y que por tanto es de la forma ab con $1 < a, b < x$, se dice que es **compuesto**.

Es inmediato que todo entero $x > 1$ tiene al menos un divisor primo. En efecto, pues si x es primo, entonces éste es su propio divisor primo, y si es compuesto, entonces el menor de los divisores $p > 1$ de x ha de ser primo, pues de lo contrario existiría un $d > 1$ que divide a p y por tanto a x, lo que no puede ser pues $d < p$ y hemos supuesto que p es el menor de los divisores de x mayores a la unidad. Observemos que este divisor primo verifica $p \leq \sqrt{x}$, pues $x = py$ y $1 < p \leq y$, así que $p^2 \leq x$.

El hecho siguiente se conocía desde la antigüedad y aparece como la Proposición 20 del Libro IX de los *Elementos* de Euclides.

Teorema 3.24 (Euclides). *Existen infinitos números primos.*

Demostración: Veamos una demostración distinta a la que nos dejó Euclides. Sea f la aplicación en $\mathbb{Z}$ dada por $f(x) = x(x + 1)$, y sea a cualquier entero mayor a la unidad. Puesto que todo entero tiene al menos un divisor primo, y puesto que a y $a + 1$ son siempre primos relativos, su producto $f(a) = a(a + 1)$ tiene más divisores primos distintos de los que tiene a. Por lo tanto, el número de factores primos de $f^n(a)$ (con f^n la composición de f consigo misma n veces) es estrictamente creciente respecto de $n \in \mathbb{N}$, así que hay infinitos números primos. ∎

A la fecha en la que se escriben estas letras, el mayor número primo conocido es

$$2^{82,589,933} - 1,$$

consistente de 24, 862, 048 dígitos y encontrado en diciembre de 2018.

Como observábamos más arriba, todo número entero x mayor a la unidad tiene al menos un divisor primo. Se deduce entonces por inducción que x puede descomponerse como un producto de números primos. Esto incluye, por supuesto, el caso en que x es él mismo un número primo, pues ahí lo que tenemos es un producto de primos con x como su único factor. Más aún, podemos definir el producto vacío de enteros (un producto sin ningún factor) como la unidad, y así afirmar que

Proposición 3.25. *Todo entero positivo es un producto de números primos.*

Demostración: Sea x un entero positivo, y razonemos por inducción sobre x. Si $x = 1$, el teorema es cierto, pues se trata del producto vacío de primos. Supongamos el teorema cierto para todos los enteros menores o iguales a x. Si $x + 1$ es primo, no hay nada más que decir. Si no lo es, entonces es un producto ab de enteros tales que $a, b > 1$, o sea que $a, b < x + 1$ y por lo tanto $a, b \leq x$, luego la hipótesis de inducción nos dice que a y b son primos o producto de primos, por lo que $x + 1 = ab$ es un producto de primos. ■

Como el lector pudo haberlo supuesto ya, la factorización de un entero positivo en producto de números primos es única salvo el orden de los factores, y la razón esencial está en la siguiente propiedad de los números primos:

Proposición 3.26 (Lema de Euclides). *Si x y y son enteros y p es un número primo tal que $p \mid xy$, entonces $p \mid x$ o $p \mid y$.*

Demostración: Supongamos que $p \mid xy$ y que $p \nmid x$. Entonces $\operatorname{mcd}(p, x) = 1$ pues p es primo, así que $p \mid y$ por el corolario 3.22. ■

Observemos que el recíproco del lema de Euclides también es cierto: si un entero p satisface la propiedad enunciada en el lema para cualesquiera enteros x y y, entonces p ha de ser un número primo. En efecto, pues si en tales condiciones tuviésemos $p = xy$ con $x > 1$, entonces $p \mid x$ pero también $x \mid p$, o sea que $x = p$ y $y = 1$, y por lo tanto p es primo.

Teorema 3.27 (Teorema Fundamental de la Artimética). *Todo entero positivo x admite una factorización en un producto de números primos. Además, esta factorización es única salvo el orden de los factores.*

Demostración: Por la proposición 3.25, x puede escribirse como un producto $p_1 \cdots p_n$ de $n \geq 0$ números primos. Supongamos que $q_1 \cdots q_m$ es otra factorización prima de x de m factores. Sin pérdida de generalidad, podemos asumir que $n \geq m$. Demostraremos por inducción sobre n que $m = n$ y que ambas factorizaciones consisten de los mismos factores. Para $n = 0$, $x = 1$ y la afirmación es trivialmente cierta. Supongamos ahora el teorema cierto para todo entero que sea producto de $n \geq 1$ primos. Si $p_1 \cdots p_{n+1} = q_1 \cdots q_m$ son factorizaciones primas de x, entonces el lema de Euclides nos dice que p_{n+1} divide a alguno de los primos $q_1, \ldots, q_m$, lo que sólo puede ocurrir si p_{n+1} es uno de estos primos, digamos $p_{n+1} = q_i$. Dividiendo ambas factorizaciones de x entre este número, tenemos que

$$p_1 \cdots p_n = q_1 \cdots q_{i-1} q_{i+1} \cdots q_{m-1},$$

y por hipótesis de inducción, ambos miembros consisten exactamente de los mismos factores. Por lo tanto, $p_1 \cdots p_{n+1}$ y $q_1 \cdots q_m$ son factorizaciones de x que difieren, cuando mucho, en el orden de los factores. ■

Se sigue entonces que todo entero x es de forma única un producto

$$p_1^{k_1} \cdots p_n^{k_n}, \quad i = 1, \ldots, n,$$

de potencias de números primos distintos. A esta forma de representar a x la llamamos la **factorización prima** de x. Si admitimos factores $p^{k_i} = 1$ de exponentes nulos, la

factorización deja de ser única, pues obviamente factores así pueden insertarse arbitrariamente en la factorización. No obstante, la inclusión de estos factores permite que en las factorizaciones primas de dos o más enteros intervengan los mismos números primos.

Proposición 3.28. *Si $x = p_1^{k_1} \cdots p_n^{k_n}$ es una factorización prima de x, entonces los divisores de x son precisamente los productos $p_1^{l_1} \cdots p_n^{l_n}$ tales que $0 \leq l_i \leq k_i$ para todo $i = 1, \ldots, n$.*

Demostración: Es claro que todo producto de esta forma es un divisor de x. Recíprocamente, si d es un divisor de x, entonces $x = dq$ para cierto $q \in \mathbb{Z}$. Considerando la factorización prima de cada entero en esa igualdad, el lema de Euclides nos dice que que los únicos primos que pueden aparecer en la factorización prima de d son $p_1, \ldots, p_n$, y esto mismo aplica para q. Puesto que el exponente de p_i en la factorización prima de x es la suma de los exponentes (posiblemente nulos) que p_i tiene en las factorizaciones primas de d y q, concluimos que $d = p_1^{l_1} \cdots p_n^{l_n}$ con $l_i \leq k_i$ para todo $i = 1, \ldots, n$. ■

Insertando primos con exponentes nulos en caso de ser necesario, podemos hacer que en las factorizaciones primas de dos enteros aparezcan los mismos números primos. Esto nos permite enunciar una caracterización útil del máximo común divisor de enteros.

Proposición 3.29. *Si $x, y > 0$ son enteros con factorizaciones primas $p_1^{k_1} \cdots p_n^{k_n}$ y $p_1^{l_1} \cdots p_n^{l_n}$, respectivamente, entonces*

$$\operatorname{mcd}(x, y) = p_1^{\min(k_1, l_1)} \cdots p_n^{\min(k_n, l_n)}.$$

Demostración: Sea $d = p_1^{\min(k_1, l_1)} \cdots p_n^{\min(k_n, l_n)}$. Claramente d es un divisor común de x y y. Si d' es otro divisor común de x y y, entonces, por la proposición anterior, d' es de la forma $p_1^{t_1} \cdots p_n^{t_n}$ con $t_i \leq k_i, l_i$, por lo que d' divide a d, lo que nos dice que d es el máximo común divisor de x y y. ■

Definición 3.30. Si x y y son dos enteros positivos, el **mínimo común múltiplo** de x y y es el menor de los enteros que son múltiplos tanto de x como de y.

Proposición 3.31. *Si x y y son enteros positivos y $p_1^{k_1} \cdots p_n^{k_n}$ y $p_1^{l_1} \cdots p_n^{l_n}$ son, respectivamente, sus factorizaciones primas, entonces*

$$\operatorname{mcm}(x, y) = p_1^{\max(k_1, l_1)} \cdots p_n^{\max(k_n, l_n)}.$$

La demostración de la proposición anterior se deja como ejercicio al lector.

Corolario 3.32. *Los múltiplos comunes de dos enteros no nulos x y y son los múltiplos de* $\operatorname{mcm}(x, y)$.

De las proposiciones 3.29 y 3.31 se de duce la siguiente relación entre el máximo común divisor y el mínimo común múltiplo.

Proposición 3.33. *Para cualesquiera enteros positivos x y y,*

$$xy = \operatorname{mcd}(x, y) \cdot \operatorname{mcm}(x, y).$$

Demostración: El resultado se sigue de las proposiciones 3.29 y 3.31 y de que $k + l = \text{mín}(k, l) + \text{máx}(k, l)$. ■

En particular, tenemos que $\operatorname{mcd}(x, y) = 1$ si y sólo si $\operatorname{mcm}(x, y) = xy$. De esto se deducen hechos como el siguiente:

Proposición 3.34. *Si $x, y, n \in \mathbb{Z}$ con $\operatorname{mcd}(x, y) = 1$, entonces $x \mid n$ y $y \mid n$ si y sólo si $xy \mid n$.*

Demostración: La suficiencia es evidente. Para el recíproco se sigue de que $xy = \operatorname{mcm}(x, y)$, y como n es un múltiplo común de x y y, éste ha de ser divisible entre xy por el corolario 3.32. ■

Definición 3.35. Sea n un entero positivo. Decimos que dos enteros x y y son **congruentes módulo *n*** si x y y dejan el mismo residuo al ser divididos por n. Para indicar esto, escribimos

$$x \equiv y \,(\text{mód}\, n).$$

La definición anterior motiva el uso de la notación $x \text{ mód } n$ para referirnos al residuo que deja x al ser divido por n. Así, tenemos que

$$x \equiv y \,(\text{mód}\, n) \qquad \text{si y sólo si} \qquad x \text{ mód } n = y \text{ mód } n.$$

El hecho siguiente es inmediato.

Proposición 3.36. *La relación de congruencia módulo un entero positivo n es de equivalencia.*

Ejemplo 3.37. Tenemos que $15 \text{ mód } 12 = 3$ y que $39 \text{ mód } 12 = 3$, o sea que $15 \equiv 39 \,(\text{mód } 12)$. ◂

La proposición siguiente nos da una caracterización alternativa de la relación de congruencia.

Proposición 3.38. *Sea n un entero positivo. Dos enteros x y y son congruentes módulo n si y sólo si su diferencia es divisible entre n.*

Demostración: Sean $x \equiv y \,(\text{mód}\, n)$. Entonces $x = qn + r$ y $y = q'n + r$, así que $x - y = (q - q')n$ y por lo tanto $n \mid (x - y)$. Recíprocamente, sea $x - y$ divisible entre n. Sean q, q', r, r' los enteros tales que $x = qn + r$ y $y = q'$ con $0 \leq r, r' < n$. Supongamos, sin pérdida de generalidad, que $r \leq r'$. Puesto que

$$x - y = (q - q')n + (r - r'), \qquad 0 \leq r - r' < r < n,$$

las diferencias $q - q'$ y $r - r'$ han de ser el cociente y el residuo de dividir $x - y$ entre n, respectivamente. Pero como $n \mid (x - y)$, tenemos $r - r' = 0$, luego $r = r'$ y por lo tanto $x \equiv y \,(\text{mód}\, n)$. ■

Proposición 3.39. *Si* $x \equiv x' \pmod{n}$ *y* $y \equiv y' \pmod{n}$*, entonces*

(a) $x + y \equiv x' + y' \pmod{n}$*;*

(b) $xy \equiv x'y' \pmod{n}$*.*

(c) $x^k \equiv x'^k \pmod{n}$ *para todo entero* $k \geq 0$*.*

Demostración: Sean $x \equiv x' \pmod{n}$ y $y \equiv y' \pmod{n}$, o sea que $x - x'$ y $y - y'$ son divisibles entre n. (1) Puesto que

$$(x + y) - (x' + y') = (x - x') + (y - y'),$$

la diferencia del miembro izquierdo es divisible entre n y por lo tanto $x + y \equiv x' + y' \pmod{n}$.

(2) Tenemos

$$xy - x'y' = xy - xy' + xy' - x'y' = x(y - y') + y'(x - x'),$$

lo que muestra que $xy - x'y'$ ha de ser divisible entre n, y así $xy \equiv x'y' \pmod{n}$.

(3) Se deduce de (2) y el principio de inducción matemática. ■

Como caso particular de la proposición anterior, tenemos que si $x \equiv y \pmod{n}$, entonces $a + x \equiv y + a \pmod{n}$ y $ax \equiv ay \pmod{n}$ para cualquier entero $a \in \mathbb{Z}$.

▸ **Ejercicio 3.40.** ¿Cuál es el último dígito de $8569451217^{26357296}$?

Solución: El último dígito de dicho número es el residuo que éste deja al ser divido entre 10,

$$r = 8569451217^{26357296} \bmod 10.$$

Es fácil ver que, en general, $x^n \bmod 10 = d^n \bmod 10$, donde d es el último dígito de x^n (leyendo de izquierda a derecha), es decir, el dígito de las unidades de x. Por lo tanto, nosotros tenemos que

$$r \equiv 7^{26357296} \pmod{10}.$$

Observemos que $7^4 = 2401 \equiv 1 \pmod{10}$ y que $26357296 = 4(6589324)$, de manera que, por la proposición 3.39,

$$\begin{aligned} d &= 7^{26357296} \bmod 10 \\ &= 7^{4(6589324)} \bmod 10 \\ &= 1^{6589324} \bmod 10 \\ &= 1 \bmod 10 \\ &= 1. \end{aligned}$$

Así pues, el último dígito de $8569451217^{26357296}$ es 1.

La proposición siguiente es una formulación del corolario 3.20 en términos de congruencias:

Proposición 3.41. *La congruencia* $ax \equiv 1 \pmod{n}$ *tiene solución* x *si y sólo si* a *y* n *son primos relativos.*

Demostración: $ax \equiv 1 \pmod{n}$ si y sólo si existe un entero k tal que $ax - 1 = kn$, o sea, tal que $ax + (-kn) = 1$, así que la proposición se sigue del corolario 3.20. ■

Si x es tal que $ax \equiv 1 \pmod{n}$, decimos que x es el "recíproco", o "inverso", de a módulo n, y podemos expresar la afirmación de la proposición anterior diciendo que un entero a tiene "recíprocos" módulo n, o que es "invertible" módulo n, si y sólo si a es primo relativo de n.

Pasemos ahora a un resultado de suma importancia en la teoría de números y sus aplicaciones.

Teorema 3.42 (Teorema Chino del Residuo). *Si $n_1, \ldots, n_k$ son números enteros primos relativos dos a dos y $a_1, \ldots, a_k$ son enteros cualesquiera, entonces existe un solución x al sistema de congruencias*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ &\vdots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

Más aún, x' es otra solución al sistema si y sólo si $x' \equiv x \pmod{N}$, donde $N = \prod_{i=1}^{n} n_i$.

Demostración: Sea $N = \prod_{i=1}^{n} n_i$ y definamos $N_i = N/n_i$. Que los enteros n_i son todos primos relativos dos a dos significa que $\operatorname{mcd}(n_i, n_j) = 1$ cuando $i \neq j$, lo que implica $\operatorname{mcd}(n_i, N_i) = 1$, luego existe un s_i tal que $s_i N_i \equiv 1 \pmod{n_i}$. Por otra parte, $n_i \mid N_j$ cuando $i \neq j$, o sea que $s_i N_j \equiv 0 \pmod{n_i}$. Con esto tenemos que, para todo $j = 1, \ldots, k$,

$$x = \left(\sum_{i=1}^{k} (s_i N_i) a_i \right) \bmod n_j = \sum_{i=1}^{k} ((s_i N_i) a_i \bmod n_j) = a_j \bmod n_j.$$

Así, x es una solución al sistema de congruencias planteado.

Puesto que los enteros n_i son primos relativos dos a dos, la generalización de la proposición 3.34 a k factores nos dice que $n_i \mid (x - a_i)$ si y sólo si $N \mid (x - a_i)$ para todo $i = 1, \ldots, k$. En otras palabras, $x \equiv a_i \pmod{n_i}$ si y sólo si $x \equiv a \pmod{N}$, así que x' es una solución al sistema de congruencias si y sólo si $x' \equiv x \equiv a_i \pmod{N}$. ■

Pasemos ahora a estudiar congruencias de potencias primas de enteros. Necesitaremos los hechos siguientes.

Proposición 3.43. *Si p es un número primo, entonces $p \mid \binom{p}{k}$ para $0 < k < p$.*

Demostración: Tenemos que $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, o sea,

$$p! = k!(p-k)!\binom{p}{k}.$$

Vemos entonces que p divide al miembro derecho, pero como los factores de $k!(p-k)!$ son todos menores que p, debemos concluir que p divide a $\binom{p}{k}$. ■

Más en general, tenemos que

Proposición 3.44. *Si p es un número primo y n un entero positivo, entonces $p \mid \binom{p^n}{k}$ para $0 < k < p^n$.*

Demostración: Observemos primero lo siguiente: si $p^n \mid ab$ pero $p^n \nmid a$, entonces $p \mid b$, pues en ese caso a es de la forma $a = p^m x$ con $0 \leq m < n$ y por tanto $p^{n-m} \mid (a/p^m)b$, y como p divide a p^{n-m} pero no divide a a, debe ser $p \mid a$. De esta manera, como

$$p^n! = \binom{p^n}{k} k!(p^n - k)!,$$

tenemos que p^n divide al miembro derecho pero no a $k!(p^n - k)!$ por que consiste de factores menores que p^n al ser $0 < k < p^n$, así que p debe dividir a $\binom{p^n}{k}$. ■

Teorema 3.45. *Si p es primo y x, y enteros cualesquiera, entonces*

$$(x + y)^{p^n} \equiv x^{p^n} + y^{p^n} \pmod{p}$$

para cualquier entero $n \geq 0$. En particular,

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

Demostración: Por el teorema binomial,

$$(x + y)^{p^n} = x^{p^n} + \binom{p^n}{1} x^{p^n-1} y + \binom{p^n}{2} x^{p^n-2} y^2 + \cdots + y^{p^n},$$

y por la proposición anterior p divide a cada término entre x^{p^n} y y^{p^n}, o sea que el residuo de dividir $(x + y)^{p^n}$ entre p es $x^{p^n} + y^{p^n}$. ■

Teorema 3.46. *Si x es entero y p es un número primo, entonces*

$$x^{p^n} \equiv x \pmod{p}$$

para todo entero $n \geq 0$.

Demostración: Por la proposición 3.39, basta probarlo por inducción sobre $x \geq 0$, el caso base $x = 0$ siendo obvio. Supongamos la congruencia cierta para un entero $x \geq 0$. Entonces $x^{p^n} + 1 \equiv x + 1 \pmod{p}$, pero $x^{p^n} + 1 \equiv (x + 1)^{p^n}$ por la proposición anterior. ■

Corolario 3.47 (Pequeño Teorema de Fermat). *Si x es entero y p es primo, entonces*

$$x^p \equiv x \pmod{p}.$$

Parte II

Estructuras algebraicas

Capítulo IV

Teoría de grupos

4.1 Operaciones binarias; semigrupos y monoides

Definición 4.1. Una **operación binaria** (o simplemente **operación**) en un conjunto X es una aplicación $* : X \times X \to X$ que envía a cada par (x, y) de elementos de X a otro elemento de X representado por $x * y$.

Observemos que, como una operación binaria en X es una aplicación de dominio $X \times X$, ésta debe estar definida para todo $(x, y) \in X \times X$. Así, por ejemplo, mientras que la suma $(x, y) \mapsto x + y$ y la multiplicación $(x, y) \mapsto xy$ ordinarias en los conjuntos numéricos elementales ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$) son operaciones binarias, la resta lo es en todos estos conjuntos excepto $\mathbb{N}$, pues $x - y$ no es un número natural para todos los casos en que x y y lo sean. Una situación similar la encontramos con la división ordinaria, que no es una operación binaria en ninguno de los conjuntos numéricos anteriores (por no estar definida la división entre cero), aunque sí lo es, por ejemplo, en $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

Para simplificar la notación, por lo regular emplearemos los símbolos $+$ y $\cdot$ para representar operaciones binarias aunque no se traten de la suma o de la multiplicación de siempre. Del uso de uno u otro símbolo se desprenden las dos notaciones que se describen a continuación:

La notación aditiva. En esta notación una operación en un conjunto X se representa por $+$ y se llama **suma** a la imagen $x + y$ de $(x, y) \in X \times X$ por $+$. En $x + y$, decimos que x y y son los **términos** de la suma.

La notación multiplicativa. En esta notación una operación en un conjunto X se denota por $\cdot$ y a la imagen de (x, y) se le representa por $x \cdot y$ o simplemente por xy, y se denomina **producto** de x y y (en ese orden), los cuales a su vez se dicen los **factores** del producto.

El lector debe acostumbrarse a leer ambas notaciones sin atribuirle a las operaciones, por mera familiaridad con los símbolos y términos utilizados, propiedades que no hayan sido probadas o asumidas de forma explícita, pues aquí trataremos con varias operaciones que, si bien las llamaremos sumas o productos, sólo desde un punto de vista suficientemente abstracto se asemejan a las operaciones elementales a las que estos términos suelen hacer referencia. De hecho, en lo sucesivo nos vamos a adherir principalmente a la notación multiplicativa para seguir introduciendo algunos conceptos y resultados en torno a las operaciones binarias en general.

Al trabajar con una operación binaria $\cdot$ en un conjunto X, debemos tomar en cuenta que las expresiones como

$$xyz,$$

donde $x, y, z \in X$, no están definidas de antemano, ya que, como el nombre lo indica, la operación *binaria* sólo puede actuar sobre dos elementos de X, de manera que la expresión anterior sólo puede entenderse tras indicar la forma en que ha de calcularse el resultado operando únicamente con dos factores a la vez. La forma usual de hacer esto es, desde luego, insertando paréntesis y acordar que $(xy)z$ hacer referencia al resultado de calcular primero xy y después multiplicar lo obtenido por z, mientras que $x(yz)$ representa el producto de x por el resultado de calcular yz. Por supuesto, una operación es mucho más amena si ambos procesos nos llevan al mismo resultado para cualesquiera que sean los elementos $x, y, z \in X$.

Definición 4.2. Una operación binaria $\cdot$ en un conjunto X es **asociativa** si para cualesquiera $x, y, z \in X$, tenemos

$$x(yz) = (xy)z.$$

Definición 4.3. Un **semigrupo** es un par $(G, \cdot)$ con G un conjunto no vacío y $\cdot : G \times G \to G$ una operación asociativa en G.

Por lo regular hablaremos de un semigrupo G para referirnos al semigrupo $(G, \cdot)$ cuando no haya posibilidad de confusión sobre cuál es la operación del semigrupo.

La suma y la multiplicación en $\mathbb{R}$ (o en cualquier otro de los conjuntos numéricos elementales) son ejemplos inmediatos de operaciones asociativas, por lo que $(\mathbb{R}, +)$ y $(\mathbb{R}, \cdot)$ son ambos semigrupos, mientras que la resta y la división (en $\mathbb{R}$ y en $\mathbb{R} \setminus \{0\}$, respectivamente) son ejemplos elementales de operaciones *no* asociativas. Por ejemplo, tenemos que

$$5 - (2 - 1) = 4 \qquad \text{y} \qquad (5 - 2) - 1 = 2.$$

Cuando tratamos con una operación asociativa, los productos de tres elementos ya no resultan ambiguos, pues da igual si pensamos en xyz como $x(yz)$ o como $(xy)z$, y por tanto podemos prescindir de los paréntesis. Un razonamiento inductivo nos dice que esto mismo ocurre para el caso de productos con cualquier número de factores. Para probar esto con formalidad, vamos a convenir que, de inicio, la forma correcta de efectuar la multiplicación de varios factores es calculando de izquierda a derecha, como se precisa a continuación.

Definición 4.4. Sea $\cdot$ una operación binaria en un conjunto X, n un entero positivo y $x_1, \ldots, x_n$ elementos de X. El **producto** de $x_1, \ldots, x_n$ (en ese orden) se representa por $\prod_{i=1}^{n} x_i = x_1 \cdots x_n$ y se define inductivamente por la fórmula

$$\prod_{i=1}^{n} x_i = x_1 \cdots x_n = \begin{cases} x_1 & \text{si } n = 1; \\ (x_1 \cdots x_{n-1})x_n & \text{si } n > 1. \end{cases}$$

En la notación aditiva, la operación sobre los elementos $x_1, \ldots, x_n$ se denota por $x_1 + \cdots + x_n$ o por $\sum_{i=1}^{n} x_i$.

Nota: Cuando una operación se lee como lo especifica la definición anterior, decimos que ésta es **asociativa por la izquierda**, pues en tal caso un producto se calcula agrupando factores desde la izquierda. Por ejemplo,

$$x_1x_2x_3x_4x_5 = (((x_1x_2)x_3)x_4)x_5.$$

La asociatividad por la izquierda constituye la forma convencional de hacer cálculos con las operaciones matemáticas elementales, y es así como las calculadoras numéricas evalúan (o deberían evaluar) operaciones con más de dos factores o términos. Esta cuestión debe tenerse presente para entender resultados con operaciones que no son asociativas si decidimos omitir paréntesis. Por ejemplo, de acuerdo con esta convención tenemos que

$$5 - 3 - 1 = (5 - 3) - 1 = 1.$$

Probaremos pues que, cuando una operación es asociativa, podemos insertar paréntesis de manera arbitraria en productos de cualquier número de factores sin cambiar el resultado.

Teorema 4.5 (Ley asociativa general). *Si G es un semigrupo y $x_1, \ldots, x_n$ elementos de G con $n > 1$, entonces, para cualesquiera enteros r y s tales que $r + s = n$, tenemos*

$$\prod_{i=1}^{n} x_i = \left(\prod_{i=1}^{r} x_i\right)\left(\prod_{i=1}^{s} x_{i+r}\right).$$

Demostración: Por inducción sobre $n = r+s$. El caso base $n = 2$ es obvio. Supongamos el teorema cierto para productos de $n > 1$ factores o menos. Si $r + s = n + 1$, entonces

$$\begin{aligned}
\prod_{i=1}^{r+s} x_i &= \left(\prod_{i=1}^{r+s-1} x_i\right) x_{r+s} \\
&= \left[\left(\prod_{i=1}^{r} x_i\right)\left(\prod_{i=1}^{s-1} x_{i+r}\right)\right] x_{r+s} && \text{(por hip. de inducción)} \\
&= \left(\prod_{i=1}^{r} x_i\right)\left[\left(\prod_{i=1}^{s-1} x_{i+r}\right) x_{r+s}\right] && \text{(por hip. de inducción)} \\
&= \left(\prod_{i=1}^{r} x_i\right)\left(\prod_{i=1}^{s} x_{i+r}\right). && \blacksquare
\end{aligned}$$

Definición 4.6. Si X es un semigrupo, $x \in X$ y n un entero positivo, definimos

$$x^n = \prod_{i=1}^{n} x.$$

En la notación aditiva, escribimos $nx = \sum_{i=1}^{n} x$.

Corolario 4.7 (Leyes de los exponentes). *Para todo elemento x de un semigrupo G y cualesquiera enteros positivos m y n, se cumplen*

(a) $x^m x^n = x^{m+n}$;

(b) $(x^m)^n = x^{mn}$.

Demostración: (a) es un caso particular de la ley asociativa general (teorema 4.5). (b) Se deduce de (a) y de una inducción sobre n, pues $(x^m)^{n+1} = (x^m)^n x^m = x^{mn} x^m = x^{mn+m} = x^{m(n+1)}$. ∎

Notemos que, en la notación aditiva, las conclusiones del corolario anterior se expresan así:

$$nx + mx = (n + m)x \qquad \text{y} \qquad n(mx) = (nm)x.$$

Hay otra propiedad que poseen algunas operaciones con la cual el lector está sin duda familiarizado:

Definición 4.8. Una operación $\cdot$ en un conjunto X se dice **conmutativa** si

$$xy = yx$$

para cualesquiera $x, y \in X$. Diremos que un semigrupo es **conmutativo** si su operación es conmutativa.

▸ **Ejercicio 4.9.** Sea $\star$ la operación "promedio" en el conjunto de los números racionales, o sea que $x \star y = (x + y)/2$ para cualesquiera $x, y \in \mathbb{Q}$. Demostrar que esta operación es conmutativa pero no asociativa.

Probaremos ahora que en un semigrupo conmutativo, similar a como ocurre con la asociatividad (teorema 4.5), la conmutatividad puede extenderse a cualquier número de factores.

Teorema 4.10 (Ley conmutativa general). *Sea G un semigrupo conmutativo y supongamos que $x_1, \ldots, x_n$ son $n \geq 1$ elementos de X. Entonces*

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{n} x_{\sigma(i)}$$

para cualquier biyección $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$.

Demostración: Por inducción sobre n. Para $n = 1$ el teorema se verifica trivialmente. Supongámoslo cierto para todo entero menor o igual que cierto entero n y sea $j = \sigma^{-1}(n + 1)$. Entonces

$$\begin{aligned}\prod_{i=1}^{n+1} x_{\sigma(i)} &= \left(\prod_{i=1}^{j-1} x_{\sigma(i)}\right) \cdot x_{n+1} \cdot \left(\prod_{i=1}^{n+1-j} x_{\sigma(j+i)}\right) \\ &= \left(\prod_{i=1}^{j-1} x_{\sigma(i)}\right)\left(\prod_{i=1}^{n+1-j} x_{\sigma(j+i)}\right) \cdot x_{n+1},\end{aligned}$$

donde la posibilidad de reordenar de los productos de la última igualdad se sigue de la hipótesis de inducción. Sea ψ la biyección de $\{1, \dots, n\}$ en sí mismo dada por

$$\psi(i) = \begin{cases} \sigma(i) & i < j \\ \sigma(i+1) & i \geq j. \end{cases}$$

Entonces

$$\begin{aligned} \prod_{i=1}^{n+1} x_{\sigma(i)} &= \left(\prod_{i=1}^{j-1} x_{\psi(i)} \right) \left(\prod_{i=1}^{n+1-j} x_{\psi(j+i)} \right) \cdot x_{n+1} \\ &= \left(\prod_{i=1}^{n} x_{\psi(i)} \right) \cdot x_{n+1} \\ &= \left(\prod_{i=1}^{n} x_i \right) \cdot x_{n+1} \\ &= \prod_{i=1}^{n+1} x_i. \end{aligned}$$

■

Definición 4.11. Sea X un conjunto y $\cdot$ una operación binaria en X. Un elemento $e \in X$ se dice una **identidad** (o **elemento neutro**) de X (respecto de la operación $\cdot$) si para todo $x \in X$,

$$xe = ex = x.$$

Existe un término para referirnos a los sistemas algebraicos en los que contamos con una identidad:

Definición 4.12. Un semigrupo es un **monoide** si cuenta con identidad respecto de su operación.

Es inmediato que un monoide G no puede tener más de una identidad: si e y e' son identidades en G, entonces $e' = e' \cdot e = e$, luego estamos hablando del mismo elemento.

Usaremos los símbolos 1 y 0 para representar a la identidad de un monoide según se esté utilizando la notación multiplicativa o la aditiva, respectivamente. Además, usaremos un subíndice, como en "1_G", cuando resulte necesario aclarar el monoide al que pertenece una identidad dada.

Ejemplo 4.13. El ejemplo más elemental e inmediato de monoide es posiblemente el conjunto $\mathbb{N}$ de los números naturales con su suma usual, para la cual el cero es la identidad. Por supuesto, $\mathbb{N}$ es también un monoide multiplicativo con identidad 1, como también lo es el conjunto $\mathbb{N} \setminus \{0\} = \mathbb{Z}^+$ de enteros positivos. ◂

Ejemplo 4.14. El conjunto $\{2n + 1 \mid n \in \mathbb{Z}\}$ de los enteros impares es un monoide respecto de la multiplicación ordinaria. ◂

Ejemplo 4.15. El conjunto de las matrices cuadradas de $n \times n$ con componentes en $\mathbb{R}$ forma un monoide respecto de la suma o la multiplicación usual de matrices. ◀

Ejemplo 4.16. Si S es un conjunto cualquiera, el conjunto S^S de todas las aplicaciones de S en sí mismo es un monoide respecto de la composición de aplicaciones. Aquí la identidad es la aplicación identidad, $\mathrm{id}_S : S \to S$ dada por $\mathrm{id}_S(x) = x$ para todo $x \in S$. ◀

Cuando G es un monoide, podemos extender la definición de las potencias de elementos de G (definición 4.6) para incluir exponentes nulos, estableciendo que

$$x^0 = 1$$

para todo $x \in G$. Es inmediato que esta definición es consistente con las leyes de los exponentes (corolario 4.7).

4.2 GRUPOS

Definición 4.17. Sea G un monoide y $x \in G$. Si $y \in G$ es tal que $xy = yx = 1$, entonces decimos que y es un **inverso** de x.

Es fácil verificar que si el inverso de un elemento dado existe, entonces es único: si y, y' son inversos de x, entonces $y' = y' \cdot 1 = y'(xy) = (y'x)y = 1 \cdot y = y$. El inverso de $x \in G$, si éste existe, se representa por x^{-1} en la notación multiplicativa y por $-x$ en la notación aditiva. Desde luego, tenemos que

$$(x^{-1})^{-1} = x.$$

Definición 4.18. Un **grupo** es un monoide G cuyos elementos son todos invertibles. Si la operación de G es además conmutativa, decimos que G es un grupo **abeliano**.

Puesto que nuestro principal interés son los grupos y no los semigrupos ni los monoides, quizá sea conveniente desglosar lo que significa la definición anterior, que nos dice que el par $(G, \cdot)$ es un grupo si cumplen las propiedades siguientes:

(a) Para cualesquiera $x, y, z \in G$, $(xy)z = x(yz)$.

(b) Existe un elemento $1 \in G$, llamado identidad (o elemento neutro) de G, tal que $1 \cdot x = x \cdot 1 = x$ para todo $x \in G$.

(c) Para todo $x \in G$ existe un $x^{-1} \in G$, llamado inverso de x, tal que $xx^{-1} = x^{-1}x = 1$.

Como ya vimos, la identidad de un grupo (más en general, de un monoide) es única, como también lo es el inverso de cualquier elemento del grupo.

Por ejemplo, el conjunto $\mathbb{N}$ de los números naturales (que para nosotros incluye al cero) es un monoide pero no un grupo respecto de la suma ordinaria de dichos números, pues el único elemento invertible es el cero (que es su propio inverso, como ocurre para

la identidad de cualquier monoide). En contraste, el conjunto de los números enteros enteros $\mathbb{Z}$ sí es un grupo abeliano respecto de la suma ordinaria de números enteros, con 0 como la identidad del grupo y con $-x$ el inverso de $x \in \mathbb{Z}$. Siempre que hablemos del grupo $\mathbb{Z}$, se entenderá que nos referimos a $\mathbb{Z}$ con dicha estructura. Por otra parte, observemos que, respecto de la multiplicación, $\mathbb{Z}$ es un monoide pero no un grupo, pues ningún entero distinto de la unidad tiene inverso multiplicativo.

Veamos algunos otros ejemplos de grupos.

Ejemplo 4.19. Desde luego, son también grupos respecto de la suma los conjuntos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$. Respecto de la multiplicación, son grupos los conjuntos $\mathbb{Q}^*$, $\mathbb{R}^*$ y $\mathbb{C}^*$. También son grupos multiplicativos los conjuntos formados por los elementos positivos de los tres conjuntos anteriores. ◂

Ejemplo 4.20 (Enteros módulo *n*). La relación de congruencia módulo un entero n es de equivalencia, y por tanto induce una partición de $\mathbb{Z}$ en clases de equivalencia, a las que llamamos **clases residuales** módulo n. A la clase de un entero k la representamos por $[k]$, o sea que

$$[k] = \{x \in \mathbb{Z} \mid x \equiv k \,(\text{mód}\, n)\}.$$

Al conjunto de todas las clases residuales módulo n lo representamos por $\mathbb{Z}_n$. Del algoritmo de la división se deduce que $\mathbb{Z}_n$ consiste exactamente de las clases

$$[0], \quad [1], \quad [2], \quad \ldots, \quad [n-1],$$

todas ellas distintas entre sí. Sobre este conjunto definimos la operación de **suma módulo *n*** por la fórmula

$$[x] + [y] = [x + y].$$

Puesto que esta operación se especifica en términos de representantes de las clases residuales, es necesario verificar que está bien definida comprobando que el resultado de aplicar la fórmula no cambia al tomar otros representantes de las clases, o sea, que si $[x] = [x']$ y $[y] = [y']$, entonces $[x + y] = [x' + y']$. Pero esto es consecuencia directa del apartado (a) de la proposición 3.39.

Se verifica de inmediato que $\mathbb{Z}_n$ es un grupo respecto de la operación de suma módulo n. Su elemento neutro es $[0]$, y el inverso de $[x]$ es $[-x] = [n - x]$. Cuando hablemos del grupo $\mathbb{Z}_n$, se entenderá que nos estamos refiriendo a este grupo. ◂

Ejemplo 4.21 (Unidades de $\mathbb{Z}_n$). En $\mathbb{Z}_n$ podemos definir también la **multiplicación módulo *n***, en este caso por la fórmula

$$[x][y] = [xy].$$

Por el apartado (b) de la proposición 3.39, esta operación está bien definida, si bien tal operación da a $\mathbb{Z}_n$ estructura de monoide con identidad $[1]$ pero no de un grupo en el caso general, ya que es posible que una clase residual no tenga inverso multiplicativo. Sin embargo, es claro que el subconjunto de $\mathbb{Z}_n$ formado por las clases residuales que sí cuentan con inverso multiplicativo será un grupo respecto de la multiplicación de clases, al que llamamos **grupo de las unidades** de $\mathbb{Z}_n$ y que representamos por $U(\mathbb{Z}_n)$.

En particular, es claro que $[0] \notin U(\mathbb{Z}_n)$, y en general $[x] \in U(\mathbb{Z}_n)$ si y sólo si existe $y \in \mathbb{Z}$ tal que $xy \equiv 1 \pmod{n}$. Puesto que

$$\begin{aligned} xy \equiv 1 \pmod{n} \quad &\Leftrightarrow \quad \text{existe } k \in \mathbb{Z} \text{ tal que } xy - 1 = kn \\ &\Leftrightarrow \quad \text{existe } k \in \mathbb{Z} \text{ tal que } xy + kn = 1 \\ &\Leftrightarrow \quad \operatorname{mcd}(x, n) = 1, \end{aligned}$$

tenemos

$$U(\mathbb{Z}_n) = \{[x] \in \mathbb{Z}_n \mid \operatorname{mcd}(x, n) = 1\},$$

luego $\left|U(\mathbb{Z}_n)\right| = \phi(n)$, donde ϕ es la aplicación ϕ de Euler. En el caso particular en que p es primo, tenemos

$$U(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\} = \{[1], \ldots, [p-1]\}. \qquad \blacktriangleleft$$

Ejemplo 4.22 (Racionales módulo uno). La relación $\sim$ en el grupo aditivo de los números racionales $\mathbb{Q}$ dada por $x \sim y$ si y sólo si $x - y \in \mathbb{Z}$ es claramente de equivalencia. Al conjunto de las clases de equivalencia inducidas por esta relación lo representaremos por $\mathbb{Q}/\mathbb{Z}$, y sobre éste definimos la operación de suma dada por $[x] + [y] = [x + y]$. Se deja al lector verificar que esta operación está bien definida y que con ella $\mathbb{Q}/\mathbb{Z}$ forma un grupo aditivo, mismo que llamaremos grupo de los **racionales módulo uno**. $\blacktriangleleft$

Ejemplo 4.23. El subconjunto $\{-1, 1, i, -i\}$ de $\mathbb{C}$, donde $i^2 = -1$, es un grupo respecto de la multiplicación ordinaria de números complejos. $\blacktriangleleft$

Ejemplo 4.24 (Raíces *n*-ésimas de la unidad). Generalizando el ejemplo anterior, tomemos el número complejo $\zeta = e^{2\pi/n}$ con $n \in \mathbb{Z}^+$, de manera que

$$\zeta, \quad \zeta^2, \quad \zeta^3, \ldots \quad , \zeta^{n-1}, \quad \zeta^n = 1,$$

son las n raíces n-ésimas de la unidad. Puesto que $\zeta^j = \zeta^{j \bmod n}$ y $\zeta^j \zeta^k = \zeta^{j+k}$, éstas forman un grupo respecto de la multiplicación ordinaria de números complejos, al cual representaremos por μ_n. Su elemento neutro es el 1 y el inverso de cada ζ^s es ζ^{n-s}. Siempre que hablemos del grupo de las raíces n-ésimas de la unidad nos estaremos refiriendo a esta estructura. $\blacktriangleleft$

Ejemplo 4.25 (Grupo de Klein). Sea $\mathbf{V} = \{1, a, b, c\}$ y defínase el producto en $\mathbf{V}$ por la siguiente tabla de multiplicar:

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Tenemos entonces que 1 es la identidad y que todo elemento de **V** es su propio inverso. Verificar que se trata también de una operación asociativa es fácil si observamos que si x, y y z son los tres elementos de **V** que no son la identidad, entonces $xy = z$, $xz = y$ y $yz = x$, luego para dichos elementos tenemos que $(xy)z = 1 = x(yz)$, $(xy)y = zy = x = x(yy)$ y que $(xx)y = y = xz = x(xy)$. La asociatividad en el caso en que alguno de estos tres elementos es la identidad es obvia. A **V** se le conoce como **grupo de Klein**. ◀

Ejemplo 4.26 (Producto directo de grupos). Sean G y H dos grupos cualesquiera, y defínase sobre su producto cartesiano $G \times H$ la operación dada por

$$(g, h)(g', h') = (gg', hh').$$

Es inmediato que $G \times H$ forma un grupo respecto de esta operación. A este grupo lo llamamos **producto directo** de G y H. Esta construcción nos da una forma más concreta de obtener el grupo de Klein, pues el lector podrá comprobar que no existe ninguna distinción formal entre la tabla de multiplicar de **V** y la de $\mathbb{Z}_2 \times \mathbb{Z}_2$ más allá del nombre de los elementos. Más adelante introduciremos las nociones que nos permitirán precisar lo que queremos decir con que no exista una diferencia esencial entre dos grupos. ◀

▸ **Ejercicio 4.27.** Demostrar que $G \times H$ es abeliano si y sólo si G y H son ambos abelianos.

Ejemplo 4.28. El conjunto de todas las matrices no singulares de $n \times n$ con componentes en $\mathbb{R}$ forman un grupo respecto de la multiplicación de matrices. A este grupo lo llamamos **grupo lineal general**, y lo representamos por $\mathrm{GL}(n, \mathbb{R})$. ◀

Ahora vamos a establecer algunos resultado básicos en relación a los inversos de los elementos de un grupo G. Por ejemplo, tenemos que si $x, y \in G$, entonces

$$(xy)^{-1} = y^{-1}x^{-1}, \tag{4.1}$$

donde no debe pasar inadvertido el orden en que aparecen los factores del miembro derecho. Para comprobar esta igualdad simplemente verificamos que $y^{-1}x^{-1}$ es el inverso de xy. En efecto, pues $xy(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1$. Un sencillo argumento inductivo extiende la fórmula (4.1) a inversos de productos con cualquier número de factores:

Proposición 4.29. *Si $x_1, \ldots, x_n$ son elementos de un grupo G, entonces*

$$(x_1 \cdots x_n)^{-1} = x_n^{-1} \cdots x_1^{-1}.$$

Una consecuencia inmediata de la existencia de inversos en un grupo es que en éste se cumple la ley de cancelación:

Proposición 4.30 (Leyes de cancelación). *Si x, y y z son elementos cualesquiera de un grupo G, entonces cualquiera de las igualdades $xy = xz$ o $yx = zx$ implica $y = z$. En particular, $xx = x$ implica que $x = 1$.*

Demostración: Supongamos que $xy = xz$. Entonces $y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = z$. El caso en que $yx = zx$ se demuestra de forma similar. ■

En un grupo G, la existencia de inversos permite definir potencias negativas: si $x \in G$, definimos

$$x^{-n} = (x^{-1})^n$$

para todo entero $n > 0$. En la notación aditiva, tenemos $-nx = n(-x)$. Desde luego, esta definición es compatible con las leyes de los exponentes que ya conocíamos para potencias no negativas:

Proposición 4.31 (Leyes de los exponentes). *Sean m y n enteros cualesquiera y x un elemento de un grupo G. Se verifican las relaciones siguientes:*

(a) $x^m x^n = x^{m+n}$;

(b) $(x^n)^{-1} = x^{-n}$;

(c) $(x^m)^n = x^{mn}$.

Demostración: (a) Para $m \geq 0$ y $n \geq 0$ ya lo sabemos. Si $m < 0$ y $n \geq 0$ entonces $-m > 0$ y el caso anterior nos dice que $x^{-m}x^{m+n} = x^n$, de donde se sigue la igualdad buscada. Desde luego, el caso $m \geq 0$ y $n < 0$ puede razonarse manera similar. Finalmente, si $n < 0$ y $m < 0$, entonces $x^{-n}x^{-m} = x^{-n+(-m)}$, y al invertir la ecuación obtenemos $x^{m+n} = x^m x^n$. Esto cubre todos los casos posibles para $m, n \in \mathbb{Z}$.

(b) Se sigue inmediatamente de (a), pues $x^n x^{-n} = x^0 = 1$, luego x^{-n} es en efecto el inverso de x^n.

(c) Si $n \geq 0$ entonces $(x^m)^n = x^{mn}$ se sigue de (a) y el principio de inducción matemática sobre n. Probado ese caso, tenemos que si $n < 0$ entonces, por (b), $(x^m)^n = ((x^m)^{-n})^{-1} = (x^{-nm})^{-1} = x^{nm}$. ■

Terminamos la sección mostrando que los axiomas de la definición 4.18 pueden debilitarse y dar lugar al mismo concepto.

Teorema 4.32. *Un semigrupo G es un grupo si y sólo si*

(a) *G cuenta con "identidad derecha": existe un $e \in G$ tal que para todo $x \in G$, $xe = x$;*

(b) *todo elemento de G es "invertible por la derecha": para todo $x \in G$ existe un $x^{-1} \in G$ tal que $xx^{-1} = e$.*

▸ **Ejercicio 4.33.** Dar un ejemplo que demuestre que, en un semigrupo G, la existencia de una identidad derecha y de inversos izquierdos no basta para afirmar que G es un grupo.

Solución: Sea G un conjunto de más de un elemento y defínase el producto en G por la fórmula $xy = x$. Es rutina verificar que G es un semigrupo en el que cualquier elemento de G es una identidad derecha. Sin embargo, ningún elemento $e \in G$ puede ser "la " identidad de G, pues de otro modo el hecho de que $ex = e$ para todo $x \in G$ implicaría que e es inverso izquierdo de todo elemento de G, lo que no puede ser a menos que G consista de un único elemento.

Se deja al lector demostrar la proposición siguiente, que nos da una forma alternativa de caracterizar la estructura de grupo.

Proposición 4.34. *Un semigrupo G es un grupo si y sólo si las ecuaciones $ax = b$ y $ya = b$ tienen soluciones únicas en G.*

▸ **Ejercicio 4.35.** Demostrar la proposición 4.34.

Solución: Sea e la solución de $ax = a$. Entonces e es una identidad derecha para todo elemento $b \in G$, existe un $y \in G$ tal que $ya = b$ y por tanto $be = (ya)e = y(ae) = ya = b$. Por otra parte, $ax = e$ también tiene solución para todo $a \in G$, por lo que todo elemento de G es invertible por la derecha. La conclusión deseada se sigue del teorema 4.32.

4.3 PERMUTACIONES

Antes de continuar, es conveniente contar con un concepto que nos permitirá dar ejemplos concretos de muchos de los conceptos que vienen a continuación.

En matemáticas elementales, una permutación de una lista de n objetos se entiende como un reordenamiento de los elementos de la lista. Por ejemplo, para la lista $(1, 2, 3, 4)$ tenemos los $4! = 24$ ordenamientos siguientes:

$(1,2,3,4)$	$(1,2,4,3)$	$(1,3,2,4)$	$(1,3,4,2)$	$(1,4,2,3)$	$(1,4,3,2)$
$(2,1,3,4)$	$(2,1,4,3)$	$(2,3,1,4)$	$(2,3,4,1)$	$(2,4,1,3)$	$(2,4,3,1)$
$(3,1,2,4)$	$(3,1,4,2)$	$(3,2,1,4)$	$(3,2,4,1)$	$(3,4,1,2)$	$(3,4,2,1)$
$(4,1,2,3)$	$(4,1,3,2)$	$(4,2,1,3)$	$(4,2,3,1)$	$(4,3,1,2)$	$(4,3,2,1)$

Observemos que cualquiera de estos reordenamientos de $(1, 2, 3, 4)$ puede entenderse como una biyección del conjunto $X = \{1, 2, 3, 4\}$ en sí mismo. Por ejemplo, el reordenamiento $(4, 3, 1, 2)$ de $(1, 2, 3, 4)$ es la aplicación $\sigma : X \to X$ que envía el 1 al 3, el 2 al 4, el 3 al 2 y el 4 al 1. En general, y puesto que ningún reordenamiento introduce repeticiones ni omisiones de los elementos de X, deducimos que, en efecto, todo reordenamiento queda caracterizado por una biyección de X en sí mismo.

Definición 4.36. Una **permutación** de $X = \{1, \dots, n\}$ es una biyección de X sobre sí mismo. Representaremos por Σ_n al conjunto de todas las permutaciones de $\{1, \dots, n\}$.

Notemos que la definición anterior es en esencia la misma si en lugar del conjunto $X = \{1, \dots, n\}$ consideremos cualquier otro conjunto Y de n elementos. Teniendo Y el mismo cardinal que X, podemos pensar que Y no es más que X con sus elementos "renombrados". Para expresar esta situación con más detalle, supongamos que Σ_Y es el conjunto de las permutaciones de elementos de Y, es decir, el conjunto de biyecciones $\sigma : Y \to Y$. Al ser $|X| = |Y|$, existe una biyección $f : X \to Y$ que "traduce" los elementos de X a elementos de Y, y con ella podemos traducir toda permutación $\sigma \in \Sigma_Y$ en

$$f^{-1} \circ \sigma \circ f,$$

una permutación de elementos de X (la composición de biyecciones es una biyección). Está claro que σ queda unívocamente determinada por σ y f, o sea, que la aplicación dada

por $\sigma \mapsto f^{-1} \circ \sigma \circ f$ es una biyección entre las permutaciones de Y y las permutaciones de X, luego los conjuntos Σ_n y Σ_Y son en efecto intercambiables. Por lo tanto, cuando en algún punto hablemos del conjunto Σ_Y de las permutaciones en un conjunto Y de n elementos, el lector tendrá claro que no se trata de ningún concepto nuevo y que todo lo dicho para Σ_n vale igual para este conjunto.

Como posiblemente el lector ya los sepa, existen $n!$ formas distintas de ordenar un conjunto de n elementos, o sea que

Proposición 4.37. $\left|\Sigma_n\right| = n!$.

Puesto que hemos definido a las permutaciones compo biyecciones de un conjunto en si mismo, ahora podemos entender el proceso de reordenar dos veces un conjunto de objetos simplemente como la composición de dos permutaciones: si $\tau, \sigma \in \Sigma_n$, $\tau \circ \sigma$ es la permutación que resulta de aplicar σ seguida de τ, pues ya sabemos (proposición **??**) que la composición de biyecciones es de nuevo una biyección, o sea, que dicha composición es una operación binaria en Σ_n, a la cual nos referiremos como **producto** de permutaciones. Se deja al lector verificar que esta operación verifica las propiedades de la definición de grupo (definición 4.18).

Definición 4.38. Llamaremos **grupo simétrico sobre *n* símbolos** a Σ_n equipado con la operación del producto de permutaciones.

Por lo regular representaremos el producto de dos permutaciones τ y σ (en ese orden) con la notación $\tau\sigma$ en lugar de $\tau \circ \sigma$.

A continuación estudiaremos algunas propiedades básicas de las permutaciones que nos permitirán trabajar con ellas de manera más eficiente.

Una notación común para especificar una permutación $\sigma \in \Sigma_n$ consiste en un arreglo de dos filas como

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix},$$

formada por n columnas en las que se coloca cada $i \in \{1, \dots, n\}$ encima del valor al que éste es enviado por σ. Por ejemplo, si σ es la permutación de Σ_5 dada por

$$\sigma(1) = 4, \quad \sigma(2) = 3, \quad \sigma(3) = 5, \quad \sigma(4) = 1, \quad \sigma(5) = 2,$$

entonces

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}.$$

Aunque esta notación es un tanto tediosa, tiene la ventaja de facilitar el cálculo de productos de permutaciones. Por ejemplo, si σ es como arriba y

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix},$$

tenemos que

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix},$$

donde el cálculo se realiza siguiendo los números de derecha izquierda (en la notación $\tau\sigma$, τ actúa después de σ), como lo ilustran las flechas del diagrama siguiente:

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}.$$

No obstante, vamos a introducir otra notación que no sólo representa permutaciones de forma más concisa, sino que además hace mas manifiestas algunas propiedades importantes de una permutación dada. Esta notación se apoya en algunos conceptos adicionales que introducimos a continuación.

Definición 4.39. Decimos que dos permutaciones σ y τ son **disjuntas** si éstas no mueven los mismos números. Con más precisión, lo son si

$$\sigma(i) \neq i \qquad \text{implica} \qquad \tau(i) = i$$

y

$$\tau(j) \neq j \qquad \text{implica} \qquad \sigma(j) = j.$$

Aunque la composición de aplicaciones no es conmutativo, sí lo es entre permutaciones disjuntas.

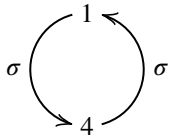
Proposición 4.40. *Si $\sigma, \tau \in \Sigma_n$ son disjuntas, entonces $\sigma\tau = \tau\sigma$.*

Demostración: Sean $\sigma, \tau \in \Sigma_n$ permutaciones disjuntas. Se debe probar que $\tau\sigma(i) = \sigma\tau(i)$ para todo $i \in \{1, \ldots, n\}$. Para esto, observamos que si τ mueve a i, con $\tau(i) = j \neq i$, entonces τ también ha de mover a j por la inyectividad de τ, luego σ fija tanto a i como a j, lo que implica que $\tau\sigma(i) = \tau(i) = j = \sigma(j) = \sigma\tau(i)$. De forma similar se verifica que si τ fija a i, entonces $\tau\sigma(i) = \sigma\tau(i)$. Esto demuestra que $\tau\sigma = \sigma\tau$. ■

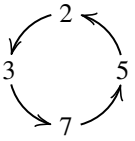
Consideremos ahora la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 7 & 1 & 2 & 6 & 5 \end{pmatrix} \in \Sigma_7$$

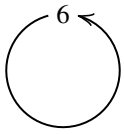
y el efecto que tiene aplicar repetidamente σ a los elementos de $\{1, \ldots, 7\}$. Cuando aplicamos σ por primera vez, ésta envía el 1 al 4. Como σ vuelva a actuar, ésta envía el 4 de regreso al 1, dando como resultado el "ciclo" de la imagen siguiente:



Ahora vemos qué pasa con los demás elementos. El menor de los enteros de $\{1, \dots, 7\}$ que no figura en el ciclo de arriba es el 2. Cuando σ actúa sobre el 2, éste es enviado al 3. Si σ actúa de nuevo, el 3 es enviado al 7, y si actúa otra vez, el 7 es enviado al 5. Al actuar σ sobre el 5, éste es enviado al 2, completándose así el ciclo



El menor (y el único) de los enteros del conjunto $\{1, \dots, 7\}$ que no está en el ciclo anterior es el 6, que queda fijado por σ y por tanto su ciclo es



La situación descrita por estos tres diagramas puede expresarse con la notación

$$(1\ 4)(2\ 3\ 7\ 5)(6),$$

que especifica el efecto que σ tiene sobre cada elemento de $\{1, \dots, 7\}$. Decimos entonces que hemos descompuesto σ en "producto de ciclos disjuntos". Si a los ciclos los definimos como ciertas permutaciones especiales, podemos dar completo sentido literal esas palabras.

Definición 4.41. Decimos que una permutación $\sigma \in \Sigma_n$ es un **ciclo de longitud k**, o que es un ***k*-ciclo**, si, para para ciertos $i_1, \dots, i_k \in \{1, \dots, n\}$, ésta verifica

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \dots \quad , \sigma(i_{k-1}) = i_k, \quad \sigma(i_k) = i_1$$

y

$$\sigma(i) = i$$

cuando $i \notin \{i_1, \dots, i_k\}$. Usaremos la notación

$$(i_1\ i_2\ i_3 \dots i_k)$$

para representar al k-ciclo que cumple dichas condiciones. A los 2-ciclos los llamamos **transposiciones**. Se trata de permutaciones que intercambian dos números $i_1, i_2 \in \{1, \dots, n\}$ y dejan fijos a todos los demás. Los ciclos de longitud 1 no mueven ningún elemento, así que todos ellos son la permutación identidad.

Observemos que la notación para un k-ciclo no es única, pues "rotar" las posiciones de sus números da lugar a la misma permutación. Por ejemplo

$$(i_1\ i_2\ i_3 \dots\ i_{k-1}\ i_k) = (i_k\ i_1\ i_2 \dots\ i_{k-2}\ i_{k-1}) = (i_2\ i_3\ i_4 \dots\ i_{k-1}\ i_k\ i_1),$$

o sea que hay k formas distintas de escribir el mismo k-ciclo. Puesto que existen

$$n(n-1)(n-2)\cdots(n-k+1)$$

k-tuplas ordenadas de elementos tomados de $\{1,\ldots,n\}$, el total de k-ciclos distintos en Σ_n es

$$\frac{1}{k}n(n-1)(n-2)\cdots(n-k+1). \tag{4.2}$$

Por otra parte, todo ciclo de longitud 1 es simplemente la identidad en Σ_n, que comúnmente representaremos por (1).

Proposición 4.42. *Toda permutación es un ciclo o un producto de ciclos.*

Demostración: Lo probaremos por inducción sobre el número m de elementos movidos por una permutación $\sigma \in \Sigma_n$. Si $m = 0$, el teorema es cierto, pues en ese caso $\sigma = (1)$. Supongamos el teorema cierto para todo entero menor que $m > 0$. Entonces σ mueve al menos un elemento, digamos i. Puesto que $\sigma^s(i) \in \{1,\ldots,n\}$, las potencias $\sigma^s(i)$ no pueden ser todas distintas, así que existen enteros s, t, con $s > t$, tales que $\sigma^s(i) = \sigma^t(i)$, o sea, que $\sigma^{s-t}(i) = i$, luego existe el menor entero $r > 0$ tal que $\sigma^r(i) = i$, o sea que existen a lo sumo $r \leq n$ potencias distintas de $\sigma(i)$. Más aún, las potencias

$$\sigma(i), \quad \sigma^2(i), \ldots \quad , \sigma^r(i)$$

son todas distintas, pues si dos de ellas fuesen iguales, digamos $\sigma^s(i) = \sigma^t(i)$ con $1 \leq t < s \leq r$ entonces $\sigma^{s-t}(i) = i$ con $s - t < r$, en contradicción con la minimalidad de r. Sea α el ciclo

$$\alpha = (\sigma(i) \quad \sigma^2(i) \quad \sigma^3(i) \quad \ldots \quad \sigma^r(i)).$$

Si $r = m$, entonces $\sigma = \alpha$ y el teorema se cumple. Si $r < m$, entonces sea S el conjunto de puntos fijados por α, y definamos $\beta \in \Sigma_n$ por

$$\beta(j) = \begin{cases} \sigma(j), & j \in S, \\ j, & j \notin S. \end{cases}$$

Entonces $\sigma = \alpha\beta$, donde β mueve a lo sumo $m - r$ elementos, así que, por hipótesis de inducción, β es un producto de ciclos, luego $\sigma = \alpha\beta$ es también un producto de ciclos. ■

El procedimiento con el que más arriba factorizamos

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 7 & 1 & 2 & 6 & 5 \end{pmatrix} = (1\ 4)(2\ 3\ 7\ 5)(6)$$

es de carácter general y puede usarse para factorizar cualquier permutación $\sigma \in \Sigma_n$. El resultado es siempre un producto de ciclos disjuntos, como lo establece el teorema siguiente.

Proposición 4.43. *Toda permutación se descompone de forma única, salvo el orden de los factores, en un producto de ciclos disjuntos.*

Demostración: Sean $\alpha_1 \cdots \alpha_k$ y $\beta_1 \cdots \beta_l$ dos descomposiciones de $\sigma \in \Sigma_n$ en ciclos disjuntos. Sin pérdida de generalidad, supondremos que $l \geq k$ y probaremos la proposición por inducción sobre l. El caso $l = 1$ es obvio. Supongamos la conclusión cierta para un entero $l-1$ y sean $\alpha_1 \cdots \alpha_k$ y $\beta_1 \cdots \beta_l$ dos descomposiciones de σ. Si σ mueve $i \in \{1, \ldots, n\}$, entonces un α_s y un β_t mueven a i. Puesto que los ciclos disjuntos conmutan, podemos asumir que se trata de β_l y de α_k. Observemos que entonces $\beta_l^j(i) = \sigma^j(i) = \alpha^j(i)$ para todo $j \geq 1$, por lo que $\beta_l = \alpha_k$, o sea que $\alpha_1 \cdots \alpha_{k-1} = \beta_1 \cdots \beta_{l-1}$. Por hipótesis de inducción, ambos miembros consisten de los mismos ciclos, de donde se sigue el resultado deseado. ■

Es inmediato que el inverso del ciclo $(i_1\ i_2\ i_3\ \ldots\ i_k)$ es el ciclo

$$(i_k\ i_{k-1}\ i_{k-2}\ \ldots\ i_1).$$

Si la descomposición en ciclos disjuntos de σ es $\sigma = \alpha_1 \cdots \alpha_s$, entonces

$$\sigma^{-1} = \alpha_s^{-1} \cdots \alpha_1^{-1} = \alpha_1^{-1} \cdots \alpha_s^{-1},$$

pues ciclos disjuntos conmutan. Así, calcular la inversa de σ consiste simplemente en invertir el orden de los elementos de cada ciclo en la descomposición de σ.

Ejemplo 4.44. Si $\sigma = (1\ 4)(2\ 3\ 7\ 5)(6) \in \Sigma_7$, entonces $\sigma^{-1} = (4\ 1)(5\ 7\ 3\ 2)(6)$. ◂

Nos referiremos como la **estructura de ciclos** de una permutación σ al número de k-ciclos que aparecen en la descomposición de σ en ciclos disjuntos para cada $0 \leq k \leq n$.

Ejemplo 4.45. ¿Cuántas permutaciones hay con estructura de ciclos $(\bullet\ \bullet\ \bullet)(\bullet\ \bullet)$ en Σ_5? Aplicando la fórmula (4.2), determinamos que hay $\frac{1}{3}(5 \cdot 4 \cdot 3) = 20$ ciclos de longitud 3. Obtenido este ciclo, no nos quedan más que 2 elementos para formar el 2-ciclo siguiente, luego éste sólo puede completarse de una manera y por tanto existen 20 permutaciones que son producto de un 3-ciclo y un 2-ciclo. ◂

En la factorización de una permutación σ en ciclos disjuntos, por lo regular omitimos los ciclos de longitud 1 que resultan de considerar los elementos fijados por σ, ya que dichos ciclos son todos la permutación identidad y resulta redundante escribirlos. Sin embargo, en ocasiones sí resulta útil incluirlos. Cuando incluimos un 1-ciclo para cada número fijado por σ, hablamos de una **factorización completa** de σ en producto de ciclos disjuntos.

Ejemplo 4.46. Sean $\sigma = (4\ 7\ 3\ 6)(5\ 2)(1)$ y $\tau = (1\ 5\ 6)(3\ 2\ 7)(4)$. Para calcular el producto $\sigma\tau$, podemos empezar por rastrear a dónde va a parar el primer número que veamos en la descomposición de τ, que es la primera en actuar por tratarse de una composición de aplicaciones. Haciéndolo así, vemos que τ envía el 1 al 5 y que luego σ envía el 5 al 2, por lo que nuestro producto comienza por "(1 2 …". Aplicando este mismo proceso ahora al 2, obtenemos "(1 2 3 …", y continuando de esta manera con cada número que vayamos obteniendo, llegamos al resultado $\sigma\tau = (1\ 2\ 3\ 5\ 4\ 7\ 6)$. ◂

Definición 4.47. Si σ y τ son dos permutaciones, a la permutación $\tau\sigma\tau^{-1}$ la llamamos **conjugada** de σ por τ, y la representamos por σ^τ.

Consideremos las permutaciones $\sigma = (4\ 7\ 3\ 6)(5\ 2)(1)$ y $\tau = (1\ 5\ 6)(3\ 2\ 7)(4)$. Al calcular

$$\begin{aligned}\sigma^\tau &= \Big((1\ 5\ 6)(3\ 2\ 7)(4)\Big)\Big((4\ 7\ 3\ 6)(5\ 2)(1)\Big)\Big((6\ 5\ 1)(7\ 2\ 3)(4)\Big)^{-1}\\ &= (4\ 3\ 2\ 1)(6\ 7)(5),\end{aligned}$$

observamos que σ y σ^τ tienen la misma estructura de ciclos, y que, además,

$$\sigma^\tau = \Big(\tau(4)\quad \tau(7)\quad \tau(3)\quad \tau(6)\Big)\Big(\tau(5)\quad \tau(2)\Big)\Big(\tau(1)\Big).$$

Se trata de una regla general:

Proposición 4.48. *Sean $\sigma, \tau \in \Sigma_n$. Si σ se expresa como un producto de ciclos disjuntos, entonces σ y σ^τ tiene la misma estructura de ciclos. Con más detalle, la descomposición en ciclos disjuntos de σ^τ se obtiene sustituyendo cada índice i por $\tau(i)$ en cada uno de los ciclos de la descomposición de σ.*

Demostración: Es fácil ver que la conjugada de un producto de permutaciones es el producto de las conjugadas de éstas, luego basta con demostrar el teorema para el caso particular de un solo ciclo $\alpha = (i_1\ i_2\ i_3\ \dots\ i_k)$. Sea

$$\beta = (\tau(i_1)\ \tau(i_2)\ \tau(i_3)\ \dots\ \tau(i_k)).$$

Hay que demostrar que $\tau\alpha\tau^{-1} = \beta$. Para esto, observemos que si $i \notin \{i_1, \dots, i_k\}$, entonces $\tau\alpha\tau^{-1}(\tau(i)) = \tau(i)$, pues $\alpha(i) = i$, así que $\tau\alpha\tau^{-1}$ y β dejan fijos a los mismos elementos. Por otra parte, si $i_j \in \{i_1, \dots, i_n\}$, entonces

$$\tau\sigma\tau^{-1}(\tau(i_j)) = \tau\sigma(i_j) = \begin{cases}\tau(i_{j+1}) & \text{si } j < k,\\ \tau(i_1) & \text{si } j = k,\end{cases}$$

o sea que $\tau\alpha\tau^{-1}(\tau(i_j)) = \beta(\tau(i_j))$, así que $\tau\alpha\tau^{-1}$ y β coinciden en todo punto y por lo tanto son iguales. ∎

Propongámonos ahora determinar si existe alguna relación entre dos permutaciones que tengan la misma estructura de ciclos. Consideremos, por ejemplo, las permutaciones $\sigma = (4\ 7\ 3)(5\ 2)(1\ 6)$ y $\alpha = (4\ 3\ 1)(6\ 7)(2\ 5)$ de Σ_7, y definamos $\tau : \{1, \dots, 7\} \to \{1, \dots, 7\}$ por

$$\begin{array}{ccccccccccccc} (& 4 & 7 & 3 &) & (& 5 & 2 &) & (& 1 & 6 &) \\ & \downarrow & \downarrow & \downarrow & & & \downarrow & \downarrow & & & \downarrow & \downarrow & \\ (& 4 & 3 & 1 &) & (& 6 & 7 &) & (& 2 & 5 &) \end{array}$$

Puesto que estamos considerando factorizaciones completas de σ y α en ciclos disjuntos, τ está bien definida y es biyectiva, luego $\tau = (4)(7\ 3\ 1\ 2)(6\ 5) \in \Sigma_7$. Tenemos entonces que

$$\begin{aligned}\alpha &= (4\ 3\ 1)(6\ 7)(2\ 5)\\ &= \Big(\tau(4)\quad \tau(7)\quad \tau(3)\Big)\Big(\tau(5)\quad \tau(2)\Big)\Big(\tau(1)\quad \tau(6)\Big)\\ &= \sigma^\tau,\end{aligned}$$

donde la última igualdad se da por la proposición 4.48. Ahora demostraremos esta relación en el caso general.

Teorema 4.49. *Dos permutaciones σ y α tienen la misma estructura de ciclos si y sólo si existe una permutación τ tal que $\alpha = \sigma^\tau$.*

Demostración: ($\Rightarrow$) Sean $\sigma, \alpha \in \Sigma_n$ de la misma estructura de ciclos. Entonces, a cada ciclo $(i_1\ i_2\ i_3\ \ldots\ i_k)$ en la descomposición de σ corresponde un ciclo $(j_1\ j_2\ j_3\ \ldots\ j_k)$ en la descomposición de α, y podemos definir la aplicación τ por $\tau(i_s) = j_s$ para cada ciclo de estas descomposiciones. Es evidente que se trata de una permutación de Σ_n, y la proposición 4.48 nos dice que $\alpha = \sigma^\tau$.

La afirmación recíproca es la proposición 4.48. ∎

Definición 4.50. Definimos la aplicación $\operatorname{sgn} : \Sigma_n \to \{-1, 1\}$, llamada **signatura** de una permutación de Σ_n, por

$$\operatorname{sgn}(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

para toda $\sigma \in \Sigma_n$.

Proposición 4.51. *Si $\sigma, \tau \in \Sigma_n$, entonces*

$$\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma).$$

Demostración: Sean $\tau, \sigma \in \Sigma_n$. Entonces

$$\begin{aligned}
\operatorname{sgn}(\tau\sigma) &= \prod_{i<j} \frac{\tau\sigma(i) - \tau\sigma(j)}{i - j} \\
&= \prod_{i<j} \frac{\tau\sigma(i) - \tau\sigma(j)}{\sigma(i) - \sigma(j)} \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j} \\
&= \prod_{i<j} \frac{\tau(i) - \tau(j)}{i - j} \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j} \\
&= \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma).
\end{aligned}$$

∎

El hecho siguiente es inmediato:

Proposición 4.52. *Si σ es una transposición, entonces* $\operatorname{sgn}(\sigma) = -1$.

Es posible descomponer una permutación en un producto de transposiciones, si bien no de forma única. Sin embargo, el teorema siguiente nos dice que el número de factores en una descomposición así es único módulo dos.

Teorema 4.53. *Toda permutación se descompone en un producto de transposiciones, y los números de transposiciones de dos descomposiciones de una misma permutación tienen la misma paridad.*

Demostración: Para la primera afirmación del teorema, basta probar que es cierta para un ciclo. En efecto, pues

$$(i_1\ i_2\ i_3\ \ldots\ i_k) = (i_1\ i_k)(i_1\ i_{k-1})(i_1\ i_{k-2})\cdots(i_1\ i_2).$$

Para la segunda afirmación, observamos que si $\alpha_1 \cdots \alpha_r$ y $\beta_1 \cdots \beta_s$ son dos factorizaciones de una permutación σ, entonces las proposiciones 4.52 y 4.51 nos dicen que

$$\operatorname{sgn}(\sigma) = (-1)^r = (-1)^s,$$

por lo que r y s son ambos pares o ambos impares. ■

Definición 4.54. Diremos que una permutación es **par** o **impar** según que ésta se descomponga en un número par o en un número impar de transposiciones, respectivamente. Equivalentemente, σ será una permutación par si $\operatorname{sgn}(\sigma) = 1$, y será impar si $\operatorname{sgn}(\sigma) = -1$.

4.4 SUBGRUPOS

Definición 4.55. Un subconjunto H de un grupo G se dice un **subgrupo** de G si H es él mismo un grupo respecto de la operación de G. Para que se da esta relación, escribiremos $H \leq G$.

Deducimos de inmediato que todo grupo G cuenta con al menos dos subgrupos: el subgrupo **trivial** $\{1\}$, que representaremos por 1 (o por 0 cuando se emplee la notación aditiva) y el grupo G mismo. Diremos que un subgrupo H de G es **propio** si $H \neq G$.

Supongamos que tenemos un subconjunto H de un grupo G. Sabemos que la asociatividad de la operación de G se cumple en particular para H. Por tanto, para que H sea un subgrupo la operación de G debe ser una operación en H (o sea, que la restricción a H de la operación del grupo debe ser cerrada en H), además de que H debe contener a la identidad de G y a los inversos de cada uno de sus elementos. Resumiendo:

Proposición 4.56. *Sea G es un grupo y $H \subset G$. Entonces $H \leq G$ si y sólo si se verifican las condiciones siguientes:*

(a) *$xy \in H$ para cualesquiera $x, y \in H$;*

(b) *$1 \in H$;*

(c) *$x^{-1} \in H$ para todo $x \in H$.*

No obstante, en muchas ocasiones podemos aplicar una forma más práctica de comprobar que estamos ante un subgrupo.

Proposición 4.57. *Sea G un grupo y H un subconjunto no vacío de G. Entonces $H \leq G$ si y sólo si para cualesquiera $x, y \in H$, tenemos $xy^{-1} \in H$.*

Demostración: La implicación es evidente. Para el recíproco, mostraremos que si $H \neq \emptyset$ y $xy^{-1} \in H$ para cualesquiera $x, y \in H$, entonces H cumple las condiciones (a)–(c) de la proposición 4.56. Comenzamos por observar que existe al menos un $a \in H$, y por tanto también $1 = aa^{-1} \in H$, de donde a su vez deducimos que si $x \in H$ entonces $x^{-1} = 1 \cdot x^{-1} \in H$. Finalmente, tenemos que si $x, y \in H$ entonces $y^{-1} \in H$ y por tanto $xy = x(y^{-1})^{-1} \in H$. ∎

Por otra parte, para grupos finitos, la comprobación de que un subconjunto no vacío es un subgrupo se reduce a verificar que el subconjunto es cerrado respecto de la operación de grupo.

Proposición 4.58. *Si G es un grupo finito y H un subconjunto no vacío de G, entonces $H \leq G$ si y sólo si $xy \in H$ para cualesquiera $x, y \in H$.*

Demostración: Desde luego que un subgrupo ha de cumplir con esa condición. Recíprocamente, si $xy \in H$ siempre que x y y sean elementos de H, entonces la restricción de la operación de G a H es una operación en H, luego resta comprobar que $1 \in H$ y que $x^{-1} \in H$ para todo $x \in H$. Para esto, tomemos un $x \in H$ (lo cual es posible por que $H \neq \emptyset$). Entonces $x^n \in H$ para todo entero positivo n, y como G es finito, las potencias de x no pueden ser todas distintas, o sea que existen enteros $i < j$ tales que $x^i = x^j$ y por tanto $1 = x^{j-i} \in H$ por ser $j - i > 0$. A demás, $x^{-1} = x^{j-i-1} \in H$, y como x es un elemento arbitrario de G, queda demostrado que H también contiene a los inversos de sus elementos. ∎

Ejemplo 4.59. Desde luego, $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$. ◂

Ejemplo 4.60. Si m es cualquier entero, entonces el conjunto

$$m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$$

formado por los múltiplos de k es un subgrupo de $\mathbb{Z}$. En particular, $0\mathbb{Z} = 0$, el subgrupo trivial. ◂

Ejemplo 4.61. Por la proposición 4.51, el conjunto de todas las permutaciones pares es cerrado respecto del producto de Σ_n, luego es un subgrupo de éste. A dicho subgrupo lo llamamos **grupo alternado** sobre n símbolos, y lo representamos por A_n. ◂

Ejemplo 4.62 (Grupo lineal especial). Sea $\mathrm{SL}(n, \mathbb{R})$ el subconjunto de $\mathrm{GL}(n, \mathbb{R})$ definido por

$$\mathrm{SL}(n, \mathbb{R}) = \{M \in \mathrm{GL}(n, \mathbb{R}) \mid \det M = 1\}.$$

Entonces $\mathrm{SL}(n, \mathbb{R})$ es un subgrupo de $\mathrm{GL}(n, \mathbb{R})$, como puede comprobarse mediante la relación $\det(AB) = \det A \cdot \det B$, válida para todo elemento de $\mathrm{GL}(n, \mathbb{R})$. Este subgrupo de $\mathrm{GL}(n, \mathbb{R})$ se conoce como el **grupo lineal especial** sobre $\mathbb{R}$. ◂

Ejemplo 4.63. Sean $r = (1\ 2\ 3\ 4)$ y $s = (1\ 2)(3\ 4)$ en Σ_4. Entonces el conjunto de todos los productos de la forma $r^i s^j$ es un subgrupo de Σ_4. Se deja al lector construir la tabla de multiplicar de este subgrupo y verificar que esta tabla coincide completamente con la del grupo diedral D_8 del ejemplo **??**. ◂

Si H y K son dos subgrupos de un grupo G, se comprueba sin dificultad que $H \cap H$ es también un subgrupo de G y que, de hecho, la intersección de cualquier familia de subgrupos de G es de nuevo un subgrupo de G. Derivado de esta observación tenemos el concepto siguiente.

Definición 4.64. Sea G un grupo y X un subconjunto de G. Si $\{H_i\}_{i\in I}$ es la familia de los subgrupos de G que contienen a X, decimos que $\bigcap_{i\in I} H_i$ es el subgrupo de G **generado** por X, y que X es un **generador** de dicho subgrupo, que representaremos por $\langle X\rangle$. Cuando $X = \{x_1, \dots, x_n\}$, $\langle X\rangle$ se representa también por $\langle x_1, \dots, x_n\rangle$.

Se deduce inmediatamente de esta definición que $\langle X\rangle$ es el menor de los subgrupos de G que contienen a X (respecto del orden dado por la inclusión de conjuntos). Puesto que $\langle X\rangle$ es un subgrupo, éste debe contener a las potencias (positivas y negativas) de los elementos de X y a los productos de las mismas. La proposición siguiente nos dice que, de hecho, $\langle X\rangle$ no contiene más que eso.

Proposición 4.65. *Sea G un grupo y X un subconjunto cualquiera de G. Entonces $\langle X\rangle$ es el subgrupo de G formado por todos los productos de potencias de elementos de X. En símbolos,*

$$\langle X\rangle = \left\{ \prod_{i=0}^{n} x_i^{k_i} \;\middle|\; n \in \mathbb{N}, x_i \in X, k_i \in \mathbb{Z} \right\}.$$

Demostración: Sea H el conjunto de tales productos. Es claro que H es un subgrupo de G por la proposición 4.57. Además, $X \subset H$ y por tanto $\langle X\rangle \subset H$ al ser $\langle X\rangle$ el menor de los subgrupos de G que contienen a X. Puesto que $\langle X\rangle$ contiene a cualquier producto de potencias de elementos de X, $\langle X\rangle$ contiene a H, luego $H = \langle X\rangle$. ■

Definición 4.66. Si G es un grupo y $x \in G$, al subgrupo

$$\langle x\rangle = \{x^k \mid k \in \mathbb{Z}\}$$

lo llamamos **grupo cíclico** generado por x.

En la notación aditiva, tenemos que $\langle x\rangle = \{kx \mid k \in \mathbb{Z}\}$. Así, por ejemplo, para el subgrupo $m\mathbb{Z}$ del grupo aditivo $\mathbb{Z}$ (véase el ejemplo 4.60) podemos escribir también

$$m\mathbb{Z} = \langle m\rangle.$$

Notemos que, puesto que todo subgrupo es él mismo un grupo, tiene sentido hablar no sólo de subgrupos cíclicos sino también de grupos cíclicos. He aquí algunos ejemplos de de dichos grupos.

Ejemplo 4.67. El grupo aditivo $\mathbb{Z}$ es un grupo cíclico infinito generado por 1 y también por -1. Por su parte, los grupos aditivos $\mathbb{Z}_n$ de las clases residuales módulo n son también cíclicos. Desde luego, $\mathbb{Z}_n = \langle [1]\rangle$. ◂

▸ **Ejercicio 4.68.** Encontrar un generador de $\mathbb{Z}_{12}$ que no sea [1].

Ejemplo 4.69. El grupo multiplicativo de las raíces n-ésimas de la unidad es cíclico de orden n y está generado, por ejemplo, por la raíz $\xi = e^{2\pi/n}$. En particular,

$$\{1, -1, i, -i\} = \langle i \rangle = \langle -i \rangle . \qquad \blacktriangleleft$$

▸ **Ejercicio 4.70.** Demostrar que todo grupo cíclico es abeliano.

Ejemplo 4.71. Para todo $n \geq 1$, el grupo Σ_n está generado por las transposiciones $(1\ 2), (1\ 3), \ldots, (1\ n)$. Esto es obvio para el caso $n = 1, 2$. Supongamos entonces que $n \geq 3$. Puesto que todo elemento de Σ_n es un producto de transposiciones, basta demostrar que toda transposición $i\ j$ es un producto de las transposiciones mencionadas. Esto es inmediato si i o j es 1, por lo que asumiremos que $1, i, j$ son distintos entre sí. Entonces

$$(i\ j) = (i\ j)^{(1\ i)} = (1\ i)(1\ j)(1\ i),$$

luego $(i\ j)$ tiene la forma deseada. $\blacktriangleleft$

4.5 HOMOMORFISMOS

Definición 4.72. Sean G y H dos grupos. Una aplicación $f : G \to H$ se dice un **homomorfismo** si

$$f(xy) = f(x)f(y) \tag{4.3}$$

para cualesquiera $x, y \in G$. En particular, si f es inyectivo decimos que es un **monomorfismo**, y si es sobreyectivo decimos que es un **epimorfismo**. Un homomorfismo de un grupo en sí mismo recibe el nombre de **endomorfismo**, o **automorismo** si dicho homomorfismo es un isomorfismo.

El lector debe advertir que en la relación (4.3) que caracteriza a los homomorfismos intervienen dos operaciones: del lado izquierdo, el producto xy es un producto en G, mientras que en el miembro derecho, $f(x)f(y)$ es un producto en H.

Antes de proporcionar ejemplos de homomorfismos de grupos, es conveniente conocer el concepto dado en la definición siguiente y también algunas de las propiedades más elementales de los homomorfismos.

Definición 4.73. Si $f : G \to H$ es un homomorfismo de grupos, el conjunto

$$\ker f = \{x \in G \mid f(x) = 1_H\}$$

es un subgrupo de G al que nos referiremos como su **núcleo**.

Proposición 4.74. *Si $f : G \to H$ es un homomorfismo de grupos, entonces*

(a) $f(1_G) = 1_H$;

(b) $f(x^{-1}) = f(x)^{-1}$;

(c) *para todo $n \in \mathbb{N}$, $f(x^n) = f(x)^n$.*

Demostración: (a) Tenemos $f(1_G) = f(1_G \cdot 1_G) = f(1_G)f(1_G)$, luego $f(1_G)$ debe ser la identidad de H de acuerdo con el caso particular de la proposición 4.30. El apartado (b) se sigue de que $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_G) = 1_H$, y (c) se demuestra fácilmente por inducción sobre n. ■

La demostración del los hechos siguientes se dejan como ejercicio al lector.

Proposición 4.75. *Si $f : G \to H$ es un homomorfismo de grupos, entonces*

(a) *si $K \leq G$, entonces $f(K) \leq H$. En particular, $f(G) \leq H$;*

(b) *si $J \leq H$, entonces $f^{-1}(J) \leq G$. En particular, $f^{-1}(1) = \ker f \leq G$.*

▸ **Ejercicio 4.76.** Demostrar la proposición 4.75.

Ejemplo 4.77. La aplicación $f : \mathbb{Z} \to \mathbb{Z}_n$ dada por $f(k) = [k]$, que por tanto envía a cada entero $k \in \mathbb{N}$ a su clase residual módulo n, es un homomorfismo de grupos por la proposición **??**, con $\ker f = \{kn \mid k \in \mathbb{Z}\} = n\mathbb{Z} = \langle n \rangle$. Se trata, desde luego, de un epimorfismo. ◂

Ejemplo 4.78. Sea $(\mathbb{R}^+, \cdot)$ el grupo multiplicativo de los números reales positivos y $(\mathbb{R}, +)$ el grupo aditivo de todos los números reales. La aplicación $\log : \mathbb{R}^+ \to \mathbb{R}$ es entonces un homomorfismo (de hecho, un isomorfismo) entre dichos grupos, como se deduce de la fórmula

$$\log xy = \log x + \log y,$$

válida para cualesquiera $x, y \in \mathbb{R}^+$. En este caso, tenemos que $\ker(\log) = 1$, el subgrupo trivial de $(\mathbb{R}^+, \cdot)$. ◂

Ejemplo 4.79 (Proyección canónica). Si G y H son dos grupos, las aplicaciones $\pi_G : G \times H \to G$ y $\pi_H : G \times H \to H$ dadas por $(g, h) \mapsto g$ y $(g, h) \mapsto h$, respectivamente, son claramente epimorfismos de grupos. Éstos reciben el nombre de **proyecciones canónicas** (de $G \times H$ en G y de $G \times H$ en H, respectivamente). ◂

Proposición 4.80. *Un homomorfismo de grupos $f : G \to H$ es un monomorfismo si y sólo si* $\ker f = 1$.

Demostración: Desde luego, si f es inyectivo entonces sólo hay uno $x \in G$ tal que $f(x) = 1_H$, y como 1_G siempre cumple esto, debe ser $\ker f = \{1_G\}$. Recíprocamente, supongamos que $\ker f$ es trivial y que $f(x) = f(y)$. Entonces $1_H = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$, y por tanto $xy^{-1} \in \ker f$, luego debe ser $xy^{-1} = 1_G$ y en consecuencia $x = y$, lo que demuestra que f es inyectiva. ■

4.6 GRUPOS CÍCLICOS

Definición 4.81. Si x es un elemento de un grupo G, el **orden** de x, representado por $|x|$, es el menor de los enteros positivos n tales que $x^n = 1$ (o $nx = 0$ en la notación aditiva). Si no existe tal entero, decimos que x es de **order infinto**, hecho que representaremos por $|x| = \infty$.

Si G es un grupo y $x \in G$ es de orden finito n, entonces la lista

$$1 = x^0, \qquad x^2, \qquad x^3, \dots \qquad , x^{n-1}.$$

exhibe sin repeticiones a todos los elementos del grupo cíclico $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$. En efecto, pues si ocurriese una repetición en la lista, digamos $x^i = x^j$ con $0 \leq i < j < n$, entonces tendríamos que $x^{j-i} = 1$ con $0 < j - i < n$, en contradicción con la suposición de que n es el orden de x. Por otra parte, el hecho de que la lista sea exhaustiva se deduce de que si k es cualquier entero entonces, por el algoritmo de la división, la potencia x^k puede escribirse como

$$x^k = x^{qn+r} = x^{qn}x^r = x^r \tag{4.4}$$

con $0 \leq r < n$, y por tanto dicha potencia está incluida en la lista de arriba. Así pues, $\langle x \rangle = \{1, x, x^2, \dots, x^{n-1}\}$, y en particular

$$|x| = |\langle x \rangle| .$$

Ejemplo 4.82. En el grupo de Klein (ejemplo 4.25), todo elemento distinto de la identidad es de orden 2, como podemos verificar observando que los elementos de la diagonal de su tabla de multiplicar son siempre la identidad. ◀

Ejemplo 4.83. En el grupo diedral D_8 (ejemplo **??**), r y r^3 son de orden 4, mientras que r^2 y cualquier reflexión de D_8 son de orden 2. ◀

Ejemplo 4.84. El grupo simétrico Σ_3 consiste de la identidad, tres transposiciones y dos 3-ciclos. Las transposiciones son de orden 2 y los 3-ciclos son de orden 3. ◀

Ejemplo 4.85 (Orden de un r-ciclo). En general, el orden de un ciclo de Σ_n es igual a la longitud del mismo. En efecto, pues si $\alpha = (i_1\ i_2\ i_3 \dots i_r)$, entonces $\alpha^k(i_j) = i_{j+k}$ para todo $j = 1, \dots, r$ y donde el índice $j + k$ se toma módulo r, así que $\alpha^k(i_j) = i_j$ si y sólo si $k \equiv 0 \,(\text{mód}\, r)$. Esto significa que $a^k = 1$ si y sólo si k es múltiplo de r, y por tanto debe ser $|\alpha| = r$. ◀

Observemos que la descomposición de x^k dada en (4.4) nos dice que tendremos

$$x^i = x^j \qquad \text{si y sólo si} \qquad i \equiv j \,(\text{mód}\, n) .$$

En particular, $x^k = 1$ si y sólo si $n \mid k$.

Por otra parte, cuando x es de orden infinito también tenemos $|x| = |\langle x \rangle| = \infty$, pues es evidente que en este caso las potencias de x son todas distintas. En particular, $x^k = 1$ si y sólo si $k = 0$.

Para referencia posterior, recopilamos en la proposición siguiente lo que hemos concluido hasta ahorita.

Proposición 4.86. *Sea G un grupo y x un elemento de G. Si x es de orden finito n, entonces*

(a) *$x^k = 1$ si y sólo si $n \mid k$;*

(b) $x^i = x^j$ *si y sólo si* $i \equiv j \pmod{n}$;

(c) *las distintas potencias de* x *son exactamente* $1, x^1, x^2, \ldots, x^{n-1}$;

(d) $|\langle x \rangle| = n$.

En cambio, si x *es de orden infinito,*

(e) *las potencias de* x *son todas distintas, y en particular* $x^k = 1$ *si y sólo si* $k = 0$;

(f) $|\langle x \rangle| = \infty$.

Supongamos que $G = \langle x \rangle$ es de orden finito n y que k es un entero positivo. Vamos a determinar cuándo es que un elemento $x^m \in G$ está en el subgrupo $\langle x^k \rangle$. Desde luego, esto ocurre si y sólo si $x^{tk} = x^m$ para algún entero t, que a su vez equivale a que $x^{tk-m} = 1$, y esto será cierto, de acuerdo con (a) de la proposición anterior, si y sólo si $n \mid tk - m$, o sea, si y sólo si $tk - sn = m$ para cierto $s \in \mathbb{Z}$. Esta última relación puede satisfacerse si y sólo si m es un múltiplo de $\operatorname{mcd}(k, n)$, lo que equivale a que $x^m \in \langle x^{\operatorname{mcd}(k,n)} \rangle$. Tenemos, por lo tanto, que

$$\langle x^k \rangle = \langle x^{\operatorname{mcd}(k,n)} \rangle .$$

Como consecuencia inmediata, deducimos que x^k será un generador de $G = \langle x \rangle$ si y sólo si k y el orden de G son primos relativos. De ser así, en particular tendremos que el orden de x^k será el mismo que el de x.

Por otra parte, si k es un divisor de $n = |x|$, entonces existe un entero m tal que $n = mk$ y por tanto que $x^{mk} = 1$, luego es claro que m tiene que ser el orden de x^k. Así pues, cuando $k \mid n$,

$$|x^k| = \frac{n}{k}.$$

Ahora bien, si k es arbitrario, el hecho de que $\langle x^k \rangle = \langle x^{\operatorname{mcd}(k,n)} \rangle$ nos dice que $|x^k| = |x^{\operatorname{mcd}(k,n)}|$, y como $\operatorname{mcd}(k, n)$ es un divisor de n, tenemos que

$$|x^k| = \frac{n}{\operatorname{mcd}(k, n)}.$$

El teorema siguiente reúne las conclusiones de arriba.

Teorema 4.87. *Sea* G *un grupo y sea* $x \in G$ *de orden finito* n. *Para todo entero* k, *se verifican los hechos siguientes:*

(a) $\langle x^k \rangle = \langle x^{\operatorname{mcd}(k,n)} \rangle$. *En particular,* $\langle x^k \rangle = \langle x \rangle$ *si y sólo si* k *y* n *son primos relativos;*

(b) $|x^k| = \dfrac{n}{\operatorname{mcd}(k, n)}$. *En particular, si* $k \mid n$ *entonces* $|x^k| = \dfrac{n}{k}$.

Apliquemos los resultados que hemos juntado hasta el momento a un grupo cíclico finito concreto, el grupo aditivo $\mathbb{Z}_{12}$. Este grupo está generado por $[1]$ y por tanto

$|[1]| = 12$. Puesto que toda clase $[k] \in \mathbb{Z}_{12}$ es de la forma $k[1]$, el inciso (b) de la proposición anterior, adaptado a la notación aditiva de $\mathbb{Z}_{12}$, nos da que

$$|[k]| = |k[1]| = \frac{n}{\operatorname{mcd}(k, 12)}.$$

En particular, cuando $k \mid 12$ tendremos

$$|[k]| = \frac{k}{12}.$$

Con estas fórmulas, determinamos que los órdenes de los elementos de $\mathbb{Z}_{12}$ son como se indican en la tabla siguiente.

$[x]$	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
$\lvert[x]\rvert$	12	6	4	3	12	2	12	3	4	6	12

Una forma de visualizar por qué, por ejemplo, $|[2]| = \frac{12}{2}$, es mediante un grafo circular que represente el cálculo de $\langle[k]\rangle$. Dicho grafo se obtiene disponiendo los elementos del grupo $\mathbb{Z}_{12}$ en un arreglo circular y uniendo el elemento $i[k]$ con el elemento $(i+1)[k]$ para cada $i = 0, 1, 2, \ldots$ hasta que regresemos de nuevo a la identidad $[0]$. Por ejemplo, el grafo circular que representa la generación del subgrupo

$$\langle[2]\rangle = \{[0], [2], [4], [6], [8], [10]\}.$$

es el que se muestra en la figura 4.1. Para obtener este grafo simplemente recorremos los vértices de dos en dos, empezando desde la identidad $[0]$ y uniendo los vértices que encontremos en el recorrido.

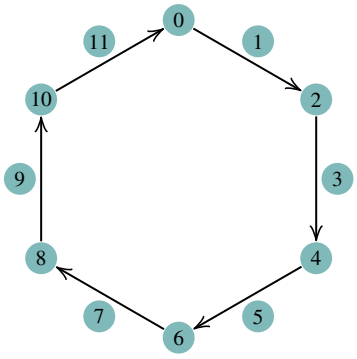


Figura 4.1. Grafo circular para los múltiplos de [2] en $\mathbb{Z}_{12}$.

Desde luego, para construir el grafo correspondiente a la multiplicación por [3], hacemos lo mismo pero avanzando de tres en tres vértices, como se muestra en la figura 4.2.

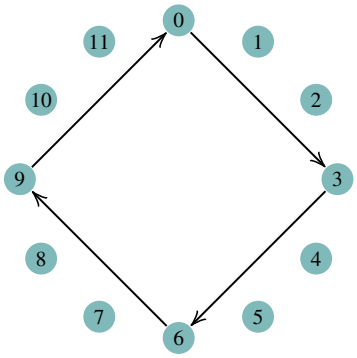


Figura 4.2. Grafos circulares para los múltiplos de [2] y los de [3] en $\mathbb{Z}_{12}$.

Usando el teorema 4.87, encontramos también que los generadores de $\mathbb{Z}_{12}$ son las clases [1], [5], [7], [11], pues son éstas las clases cuyos elementos son primos relativos de 12. La figura 4.3 nos permite contemplar el grafo circular para el cálculo de $\langle [5] \rangle = \mathbb{Z}_{12}$.

Consideremos ahora el grupo $\mathbb{Z}_{20}$ y los subgrupos $\langle [4] \rangle$ y $\langle [8] \rangle$. Si calculamos sus elementos de forma explícita, encontramos que dichos grupos son iguales, aunque esto se determina con mayor facilidad mediante el inciso (a) de la proposición **??**, que nos dice que

$$\langle [8] \rangle = \langle [\mathrm{mcd}\,(8, 20)] \rangle = \langle [4] \rangle .$$

La figura 4.4 muestra el grafo circular correspondiente al cálculo de estos subgrupos.

Recordemos que, para todo entero n, la aplicación ϕ de Euler nos da el número $\phi(n)$ de enteros entre 0 y n que son primos relativos de n. Así, como consecuencia inmediata del teorema 4.87, tenemos que

Corolario 4.88. *Si x es de orden finito, existen exactamente $\phi(n)$ generadores de $\langle x \rangle$.*

Algo más que podemos deducir fácilmente del teorema 4.87 es que

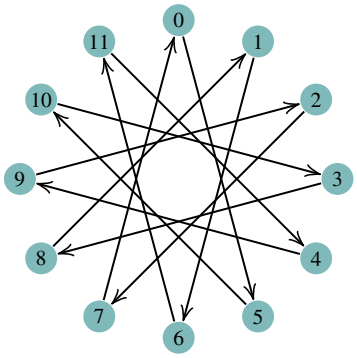


Figura 4.3. Grafo circular para la multiplicación por $[5] \in \mathbb{Z}_{12}$.

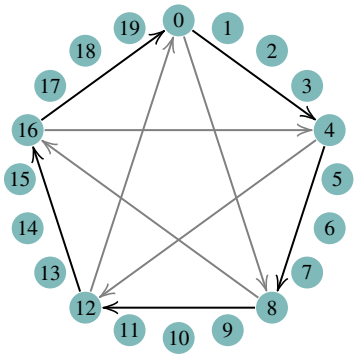


Figura 4.4. Grafos circulares para la multiplicación por [4] y por [8] en $\mathbb{Z}_{20}$, en los que se observa que $\langle[4]\rangle = \langle[8]\rangle$.

Corolario 4.89. *Si G es un grupo finito, entonces el número de elementos de G de orden d es un múltiplo de $\phi(d)$.*

Demostración: Si x y y son dos elementos de G de orden d, entonces o bien $\langle x\rangle = \langle y\rangle$ o bien $\langle x\rangle \cap \langle y\rangle = 1$, de manera que todo elemento de orden d está en exactamente un subgrupo cíclico de G de orden d. Entonces, si G cuenta con k subgrupos así (donde k es finito por serlo el orden de G), habrá precisamente $k\phi(d)$ elementos de orden d en G. ■

Hasta ahora la información que hemos encontrado sobre los subgrupos de un grupo cíclico está limitada al caso en que éstos son a su vez cíclicos. Resulta que no es necesario contemplar subgrupos de otro tipo, pues

Teorema 4.90. *Todo subgrupo de un grupo cíclico es cíclico.*

Demostración: Supongamos que $G = \langle x\rangle$ y que H es un subgrupo de G. Si $H = 1$, entonces H es trivialmente cíclico. Supongamos pues que existe al menos un entero positivo k tal que $x^k \in H$. Entonces existe el menor entero m tal que $x^m \in H$. Vamos a demostrar que $H = \langle x^m\rangle$. En efecto, pues si $x^k \in H$ con k un entero positivo, debe ser k un múltiplo de m, ya que por el algoritmo de la división podemos escribir $k = qm+r$ con $0 \leq r < m$, y si fuese $r > 0$ tendríamos $x^r = x^{k-qm} = x^k x^{-qm} \in H$, en contradicción con la minimalidad de m. Por tanto, es $r = 0$ y con ello k es un múltiplo de m. Esto demuestra que todo elemento de H es una potencia de x^m, o sea que $H = \langle x^m\rangle$. ■

En la demostración anterior vimos que si $G = \langle x\rangle$ y $H \leq G$, entonces $H = \langle x^m\rangle$ con m el menor entero positivo tal que $x^m \in H$. Cuando G es de orden finito n, tenemos que además $m \mid n$, pues de otro modo $n = qm + r$ con $0 < r < m$, lo que no puede ser por que $x^r = x^n x^{-qm} = x^{-qm} \in H$, en contradicción con la minimalidad de m.

Si $G = \langle x\rangle$ es un grupo cíclico infinito entonces las potencias de x son todas distintas, luego todo subgrupo $H \leq G$ también es cíclico infinito. En cambio, si G es de orden finito, los teoremas 4.90 y 4.87 nos permiten establecer lo siguiente.

Teorema 4.91. *Sea $G = \langle x \rangle$ de orden finito. Si $H \leq G$, el orden de H divide al orden de G. Recíprocamente, si d es un divisor del orden de G, entonces G tiene un único subgrupo de orden d.*

Demostración: Sea n el orden de G. En la demostración del teorema 4.90 vimos que si $H \leq G$ entonces $H = \langle x^m \rangle$ donde m es el menor entero positivo tal que $x^m \in H$, que como vimos cumple también que $m \mid n$, luego por (b) del teorema 4.87 el orden de $|H| = n/m$, que es un divisor de n.

Recíprocamente, sea d un divisor de $n = |G|$. Entonces $H = \left\langle x^{n/d} \right\rangle$ es un subgrupo de orden d por (b) del teorema 4.87. Para ver que éste es el único subgrupo de dicho orden, supongamos que $K \leq G$ con $|K| = d$. Entonces $K = \langle x^m \rangle$ donde m es el menor de los enteros tales que $x^m \in K$, y como también $m \mid n$, el inciso (b) del teorema 4.87 nos da que

$$d = |x^m| = \frac{n}{m}$$

y por tanto que $m = n/d$, es decir, $K = \langle x^m \rangle = \left\langle x^{n/d} \right\rangle$. ■

Resulta pues que un grupo $G = \langle x \rangle$ de orden finito n tiene un único subgrupo H_d para cada divisor $d \mid n$. Más adelante demostraremos que esta característica es exclusiva de los grupos cíclicos (o sea, que cualquier grupo que cumpla esto deberá ser cíclico).

Observemos que el corolario 4.88 nos permite establecer con facilidad una fórmula elemental de la teoría de números: si n es cualquier entero positivo, entonces

$$n = \sum_{d|n} \phi(d). \tag{4.5}$$

En efecto, pues supongamos que $\langle x \rangle$ es de orden n. Entonces para cada divisor d de n existe exactamente un subgrupo $H_d = \left\langle x^{n/d} \right\rangle$ de orden d, y si $\text{gen}\left(H_d\right)$ representa el conjunto de los generadores de H_d, entonces, como ya vimos,

$$\left|\text{gen}\left(H_d\right)\right| = \phi(d).$$

Puesto que todo elemento de $\langle x \rangle$ es generador de un único H_d para algún $d \mid n$, tenemos que $\langle x \rangle$ es la unión disjunta

$$\langle x \rangle = \bigcup_{d|n} \text{gen}\left(H_d\right),$$

de donde se sigue que

$$n = |\langle x \rangle| = \sum_{d|n} \left|\text{gen}\left(H_d\right)\right| = \sum_{d|n} \phi(d).$$

Terminamos esta sección mostrando que no es necesario adoptar un enfoque abstracto al tratar con grupos cíclicos, si no que podemos concentrarnos por completo en los grupos $\mathbb{Z}$ y $\mathbb{Z}_n$, ya que, en esencia, éstos son los únicos grupos cíclicos que existen.

Teorema 4.92. *Todo grupo cíclico infinito es isomorfo a $\mathbb{Z}$ y todo grupo cíclico finito lo es a $\mathbb{Z}_n$.*

Demostración: Sea $\langle x\rangle$ cíclico. Es evidente que la aplicación $f : \mathbb{Z} \to \langle x\rangle$ dada por $f(k) = x^k$ es un epimorfismo de grupos. Si ker f es trivial, entonces f es un isomorfismo y por tanto $\langle x\rangle \simeq \mathbb{Z}$. Supongamos ahora que ker $f \neq 0$. Entonces existe el menor entero positivo m tal que $m \in \ker f$, y de hecho ker $f = m\mathbb{Z}$. Observamos que $f(i) = f(j)$ si y sólo si $i - j \in \ker f = m\mathbb{Z}$, o sea, si y sólo si las clases residuales $[i]_m$ y $[j]_m$ son iguales en $\mathbb{Z}_m$. Así pues, $x^i = x^j$ si y sólo si $[i]_m = [j]_m$, por lo que la aplicación $g : \langle x\rangle \to \mathbb{Z}_m$ dada por $x^k = [k]$ está bien definida y es inyectiva. Puesto que claramente se trata de un epimorfismo, concluimos que $\langle x\rangle \simeq \mathbb{Z}_m$. ■

4.7 CLASES LATERALES; EL TEOREMA DE LAGRANGE

En esta sección obtendremos uno de los resultados elementales más importantes de la teoría de grupos finitos: el teorema de Lagrange. En la sección anterior demostramos que el orden de todo subgrupo de un grupo cíclico G divide al orden de G (teorema 4.91). El teorema de Lagrange nos dice que esta relación entre el orden de un grupo y sus subgrupos no es exclusiva de los grupos cíclicos, sino que en realidad se cumple para todo tipo de grupos. Este hecho tan notable se demuestra con facilidad tras conocer los conceptos que introduciremos a continuación.

Definición 4.93. Sea G un grupo y $H \leq G$. Decimos que dos elementos x y y de G son **congruentes por la derecha módulo H** si

$$xy^{-1} \in H,$$

hecho que indicaremos mediante la notación $x \equiv_d y \,(\text{mód } H)$. Similarmente, x y y serán **congruentes por la izquierda módulo H**, en símbolos $x \equiv_i y \,(\text{mód } H)$, si $x^{-1}y \in H$.

En otras palabras, x y y son congruentes por la derecha módulo un subgrupo H si $x = hy$ para algún $h \in H$, y lo son por la izquierda módulo H si existe un $h \in H$ tal que $x = yh$. Se verifica de inmediato que estas congruencias son relaciones de equivalencia.

Definición 4.94. Sea H un subgrupo de un grupo G. Llamamos **clase lateral derecha** (resp. **clase lateral izquierda**) de x por H, representada Hx (resp. xH), a la clase de equivalencia de $x \in G$ por la relación de congruencia por la derecha módulo H (resp. por la relación de congruencia izquierda módulo H).

Desde luego,

$$Hx = \{hx \mid h \in H\} \qquad \text{y} \qquad xH = \{xh \mid h \in H\},$$

y por lo tanto $xH = Hx = H$ siempre que $x \in H$. En particular, $1H = H1 = H$. Además, puesto que las clases laterales son clases de equivalencia, tenemos que

$$xH \cap yH \neq \varnothing \qquad \text{implica} \qquad xH = yH.$$

En particular, si $y \in xH$ entonces $yH = xH$.

Cuando empleamos la notación aditiva para la operación de un grupo G, las clases laterales derecha e izquierda de un subgrupo H por un elemento $x \in G$ se representan, respectivamente, por

$$H + x = \{h + x \mid h \in H\} \qquad \text{y} \qquad x + H = \{x + h \mid h \in H\}.$$

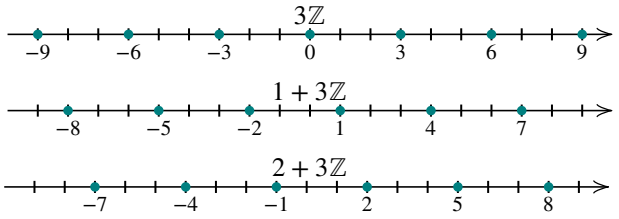


Figura 4.5. Las 3 clases laterales del subgrupo $3\mathbb{Z}$ en $\mathbb{Z}$.

Ejemplo 4.95. El grupo $\mathbb{Z}$ es abeliano y por tanto $x + H = H + x$ para todo subgrupo suyo H y todo entero x. Ahora bien, los subgrupos de $\mathbb{Z}$ son todos de la forma $m\mathbb{Z}$ para algún entero m de acuerdo con el teorema 4.90, y $x, y \in \mathbb{Z}$ son congruentes módulo el subgrupo $m\mathbb{Z}$ si y sólo si $x - y \in m\mathbb{Z}$, es decir, si y sólo si $x \equiv y \,(\text{mód}\, m)$. Por tanto, $x + m\mathbb{Z} = y + m\mathbb{Z}$ si y sólo si $x \equiv y \,(\text{mód}\, m)$, de manera que $m\mathbb{Z}$ tiene exactamente $m - 1$ clases laterales distintas:

$$m\mathbb{Z}, \qquad 1 + m\mathbb{Z}, \qquad 2 + m\mathbb{Z}, \ldots, \qquad (m-1) + m\mathbb{Z}. \qquad \blacktriangleleft$$

Ejemplo 4.96. El grupo circular S^1 de los números complejos cuyo módulo es la unidad es un subgrupo de $\mathbb{C}^*$, el grupo multiplicativo de los números complejos no nulos. Si $z \in \mathbb{C}$ y $r = |z|$, entonces

$$zS^1 = \{re^\theta \mid \theta \in [0, 2\pi)\}.$$

Así, la clase lateral zS^1 es la circunferencia del plano complejo con centro en el origen y radio $r = |z|$. Por lo tanto, $zS^1 = wS^1$ si y sólo si $|z| = |w|$. $\blacktriangleleft$

Ejemplo 4.97. Consideremos el subgrupo $H = \mathrm{SL}(n, \mathbb{R})$ del grupo $\mathrm{GL}(n, \mathbb{R})$. Si $A \in \mathrm{GL}(n, \mathbb{R})$, entonces la clase lateral AH consiste de las matrices cuyo determinante es igual a $\det A$. Por ejemplo,

$$\begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix} \mathrm{SL}(2, \mathbb{R}) = \{M \in \mathrm{GL}(2, \mathbb{R}) \mid \det M = 5\}. \qquad \blacktriangleleft$$

Ejemplo 4.98. Sea $f : G \to H$ un homomorfismo de grupos. Entonces

$$f^{-1}(f(g)) = \{x \in G \mid f(x) = f(g)\} = g \ker f$$

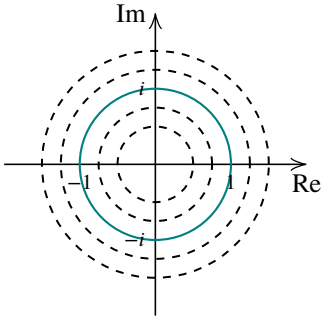


Figura 4.6. Clases laterales del grupo circular S^1.

para todo $g \in G$. En efecto, pues vemos que Tenemos

$$f(x) = f(y) \Leftrightarrow f(xy^{-1}) = 1_H \Leftrightarrow xy^{-1} \in \ker f \Leftrightarrow x \ker f = y \ker f.$$

para cualesquiera $x, y \in G$. ◀

Proposición 4.99. *Si x y y son elementos de un grupo G y $H < G$, entonces $x \equiv_d y \pmod H$ si y sólo si $x^{-1} \equiv_l y^{-1} \pmod H$.*

Demostración: Tenemos que $xy^{-1} \in H$ si y sólo si $yx^{-1} = (xy^{-1})^{-1} \in H$. ■

Proposición 4.100. *Si G es un grupo y $H \leq G$, hay tantas clases laterales derechas como izquierdas por el subgrupo H. Con más precisión:*

$$|\{Hx \mid x \in G\}| = |\{xH \mid x \in G\}|.$$

Demostración: Definimos la aplicación f de $\{Hx \mid x \in G\}$ en $\{xH \mid x \in G\}$ por $f(Hx) = x^{-1}H$. De la proposición anterior se deduce que f está bien definida y que es una biyección. ■

Definición 4.101. Si G es un grupo y $H \leq G$, el cardinal del conjunto de las clases laterales derechas (o izquierdas) de H se dice **índice** de H en G y se representa por $[G : H]$. En símbolos,

$$[G : H] = |\{Hx \mid x \in G\}| = |\{xH \mid x \in G\}|.$$

Proposición 4.102. *Sea G un grupo. Cualesquiera dos clases laterales de $H < G$ tienen el mismo cardinal. En particular, $|Hx| = |H| = |xH|$.*

Demostración: Se verifica fácilmente que la aplicación $f : H \to xH$ dada por $f(h) = xh$ es una biyección. ■

Estas observaciones respecto del cardinal de las clases laterales nos dan de inmediato el resultado principal de esta sección.

Teorema 4.103 (Lagrange). *El orden de todo subgrupo H de un grupo finito G divide al orden de G, con*

$$|G| = [G : H]|H|.$$

Corolario 4.104. *El orden de todo elemento x de un grupo finito G es un divisor del orden de G, y por tanto $x^{|G|} = 1$.*

Del corolario anterior podemos deducir deducir algunos resultados conocidos de la teoría de números.

Corolario 4.105 (Euler). *Si x y n son enteros positivos con* $\operatorname{mcd}(x, n) = 1$*, entonces*

$$x^{\phi(n)} \equiv 1 \,(\operatorname{mód} n)\,.$$

Demostración: Si $(x, n) = 1$ entonces $[x] \in U(\mathbb{Z}_n)$, y por el corolario anterior $\phi(n) = \left|U(\mathbb{Z}_n)\right|$ es un múltiplo del orden de $[x]$, luego debemos tener $[x]^{\phi(n)} = [1]$, de donde se sigue el resultado deseado. ■

Corolario 4.106 (Fermat). *Si p es un número primo y x un entero cualquiera, entonces*

$$x^p \equiv x \,(\operatorname{mód} p)\,.$$

Demostración: Si p es primo entonces $\phi(p) = p - 1$, luego el corolario anterior nos da que $x^{p-1} \equiv 1 \,(\operatorname{mód} p)$, de donde se sigue la congruencia deseada. ■

Como consecuencia inmediata del teorema de Lagrange obtenemos la clasificación de todos los grupos de orden primo.

Corolario 4.107. *Todo grupo de orden un número primo es cíclico.*

Demostración: Sea G un grupo de orden primo p y $x \neq 1$ un elemento de G. Entonces $|x| > 1$ y $|x|$ divide a p por el corolario 4.104, pero como p es primo, necesariamente $|x| = p$, luego x ha de ser un generador de G. ■

Corolario 4.108. *Salvo isomorfía, los únicos grupos de orden* 4 *son $\mathbb{Z}_4$ y el grupo* **V** *de Klein.*

Demostración: Sea G un grupo no cíclico de orden 4. Si $x \neq 1$ es elemento de G, entonces el orden de x debe ser 4 o 2, pero como G no es cíclico debe ser $|x| = 2$. Así pues, todo elemento no neutro de G es de orden 2, que es precisamente la cualidad que caracteriza al grupo **V**. ■

El hecho siguiente en relación a los subgrupos de índice 2 nos servirá para demostrar que el grupo alternado A_4 no tiene un subgrupo de orden 6 pese a que dicho número es un divisor del orden de A_4, proporcionando así un contraejemplo al recíproco del teorema de Lagrange.

Proposición 4.109. *Si H es un subgrupo de un grupo G con $[G : H] = 2$, entonces $x^2 \in H$ para todo $x \in G$.*

Demostración: Si $x \in H$ entonces obviamente $x^2 \in H$, y si $a = a^2a^{-1} \notin H$ entonces $aH \neq a^2H$, luego $[G : H] = 2$ implica que $a^2H = H$ y por tanto que $a^2 \in H$. ■

Proposición 4.110. *El grupo A_4 no tiene ningún subgrupo de orden* 6.

Demostración: Si H fuera tal subgrupo, entonces H contendría a los cuadrados de todo elemento de A_4. Sin embargo, los inversos de los 3-ciclos de A_4 son todos de esa forma, pues $1 = (a\ b\ c)^3 = (a\ b\ c)(a\ b\ c)^2$, o sea que $(a\ b\ c)^{-1} = (a\ b\ c)^2$. Así, puesto que $x \in H$ si y sólo si $x^{-1} \in H$, el subgrupo H contiene a todos los 8 ciclos de longitud 3, en contradicción con que $|H| = 6$. ■

Definición 4.111. Sea G un grupo y sea $\mathcal{P}^*(G)$ la colección de los subconjuntos no vacíos de G. Si $H, K \in \mathcal{P}^*(G)$, el **producto** de H y K (en ese orden) es el elemento XY de $\mathcal{P}^*(G)$ dado por

$$XY = \{hk \mid h \in H, k \in K\}.$$

Cuando $K = x$, escribiremos Hx y xH en lugar de $H\{x\}$ y $\{x\}H$, respectivamente.

La asociatividad del producto en G nos da la asociatividad del producto en $\mathcal{P}^*(G)$, o sea que

$$(XY)Z = X(YZ)$$

para cualesquiera $X, Y, Z \in \mathcal{P}^*(G)$. Además, es claro que $1H = H1 = H$, luego $\{1\} \in \mathcal{P}^*(G)$ es una identidad en $\mathcal{P}^*(G)$, por lo que $\mathcal{P}^*(G)$ tiene estructura de monoide (definición 4.12). Sin embargo, $\mathcal{P}^*(G)$ no es nunca un grupo salvo en el caso trivial $G = \{1\}$, pues en cualquier otro caso existirán subconjuntos de G que no tienen inverso.

Si H es un subgrupo de G, entonces obviamente

$$HH = H,$$

y lo recíproco también es cierto cuando H es de orden finito, como se deduce de la proposición 4.58. No obstante, el lector debe estar prevenido de que el producto HK de dos subgrupos H y K de G no es en general un subgrupo, aunque la proposición de abajo nos da un criterio para determinar cuándo sí lo es. Más adelante (por ejemplo, en la proposición 4.128) veremos otras condiciones bajo las cuales el producto de subgrupos es de nuevo un subgrupo.

Proposición 4.112. *Sean H y K subgrupos de un grupo G. Entonces HK es un subgrupo de G si y sólo si $HK = KH$.*

Demostración: Para todo subconjunto X de G, definamos $X^{-1} = \{x^{-1} \mid x \in X\}$. Si H es un subgrupo de G, obviamente $H^{-1} = H$. Por tanto, si $HK \leq G$,

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH.$$

Recíprocamente, si $HK = KH$, tendremos que $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$, o sea que HK cerrado respecto a la toma de inversos. A demás

$$(HK)(HK) = (HK)(KH) = H(KK)H = HKH = HHK = HK,$$

de manera que también es cerrado respecto a la operación del grupo. Puesto que es claro que $1 \in HK$, la proposición 4.56 nos dice que $HK \leq G$. ■

En esta sección, nuestro interés principal en relación al producto de subconjuntos de un grupo es el resultado siguiente.

Teorema 4.113. *Sean H y K subgrupos finitos de un grupo G. Entonces*

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Demostración: Sea $H \cap K = \{x_1, \dots, x_n\}$ y $f : H \times K \to HK$ la sobreyección dada por $f(h,k) = hk$. Vamos a demostrar que para cada $x \in HK$, tenemos $|f^{-1}(\{x\})| = n$, de donde se sigue que

$$|H||K| = |H \times K| = |HK|n = |HK||H \cap K|.$$

Sean $h \in H$ y $k \in K$ fijos y definamos $h_i = hx_i$ y $k_i = x_i k^{-1}$ para cada $i = 1, \dots, n$. Es inmediato que $f(h_i, k_i) = f(h,k)$ para todo $i = 1, \dots, n$, así que $|f^{-1}(\{hk\})| \geq n$. Por otra parte, si $f(h', k') = f(h,k)$, entonces $h'k' = hk$, es decir, $h^{-1}h' = kk'^{-1} \in H \cap K$, luego $h' = hx_i = h_i$ y $k' = x_i k^{-1} = k_i$ para algún $i = 1, \dots, n$, y por lo tanto $|f^{-1}(\{hk\})| \leq n$. Esto demuestra que $|f^{-1}(\{x\})| = n$. ∎

Observemos que si dividimos la igualdad del teorema anterior entre K, obtenemos

$$\frac{|H|}{|H \cap K|} = \frac{|HK|}{|K|},$$

de modo que si HK es a su vez un grupo, tendremos

$$[H : H \cap K] = [HK : K]. \tag{4.6}$$

Teorema 4.114. *Si G es un grupo de orden $2p$ con p un número primo, entonces $G \simeq \mathbb{Z}_{2p}$ o $G \simeq D_{2p}$.*

Demostración: Sabemos que el teorema es cierto para $p = 2$, pues los únicos subgrupos de orden 4 son $\mathbb{Z}_4$ y $\mathbf{V} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, y este último es D_4 de acuerdo con la definición **??**. Supongamos pues que $p > 2$ y que $G \not\simeq \mathbb{Z}_{2p}$, de tal manera que todos los elementos de G son de orden menor a $2p$. Vamos a demostrar que esto implica que $G \simeq D_{2p}$. Comenzamos por comprobar que G tiene un elemento de orden p, pues si no fuese así todo elemento no neutro de G sería de orden 2, lo que implicaría que G es isomorfo al producto $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ de $p > 2$ copias de $\mathbb{Z}_2$, y por tanto contendría un subgrupo isomorfo a $\mathbf{V}$, lo que no puede ser por que $|\mathbf{V}| = 4 \nmid 2p$ para $p > 2$. Sea pues r un elemento de G de orden p. Entonces $[G : \langle r \rangle] = 2$ y por tanto $\langle r \rangle$ contiene a todos los cuadrados de elementos de G. Tomando un $s \notin \langle r \rangle$, el hecho de que $s^2 \in \langle r \rangle$ implica que $s \notin \langle s^2 \rangle$ y por tanto que $|s^2| < |s|$, y como $|s^2| = |s| / \operatorname{mcd}(2, |s|)$, $|s|$ tiene que ser divisible entre 2 y así $|s| \neq p$, luego necesariamente $|s| = 2$. De todo esto concluimos también que $\langle r \rangle \cap \langle s \rangle = \{1\}$, o sea que $|\langle r, s \rangle| = 2p$. Puesto que $rs \notin \langle r \rangle$, rs es de orden 2, de donde se sigue que $rs = sr^{-1}$. ∎

Definición 4.115. Sea G un grupo. Si existe un entero positivo n tal que $x^n = 1$ para todo $x \in G$, decimos que G es de **exponente finito**, y llamamos **exponente** al menor de los enteros n que cumplen esto.

4.8 SUBGRUPOS NORMALES

Definición 4.116. Un subgrupo N de un grupo G se dice **normal** en G si para todo $x \in G$, $xN = Nx$. Para indicar que éste es el caso, escribiremos

$$N \trianglelefteq G.$$

Así pues, cuando tenemos un subgrupo normal podemos hablar de sus clases laterales sin aclarar por qué lado se están considerando. Antes de dar ejemplos de subgrupos normales, conviene contar con diversas maneras de verificar la normalidad de un subgrupo.

Proposición 4.117. *Sea G un grupo y N un subgrupo de G. Son equivalentes los enunciados siguientes:*

(a) $N \trianglelefteq G$;

(b) *toda clase lateral izquierda de N en G es una clase lateral derecha de N en G;*

(c) *para todo $x \in G$, $xNx^{-1} = N$, con $xNx^{-1} = \{xnx^{-1} \mid n \in N\}$;*

(d) *para todo $x \in G$, $xNx^{-1} \subset N$;*

Demostración: La implicación (a) $\Rightarrow$ (b) es obvia. Para ver que además (b) $\Rightarrow$ (a), supongamos que $xN = Ny$ para algún $y \in G$. Entonces $x \in xN \cap Nx = Ny \cap Nx$, pero entonces $xN = Ny = Nx$, ya que dos clases laterales o son disjuntas o son iguales.

(a) $\Rightarrow$ (d) Todo xn con $x \in G$ y $n \in N$ es de la forma $n'x$ con $n' \in N$. luego $xnx^{-1} = n'xx^{-1} = n' \in N$ y por tanto $xNx^{-1} \subset N$.

(d) $\Rightarrow$ (c) Si $xNx^{-1} \subset N$, entonces, para todo $n \in \mathbb{N}$, $x(n^{-1})x^{-1} = n'$ con $n' \in N$, y así $n = x(n'^{-1})x^{-1} \in xNx^{-1}$, de donde se deduce la inclusión inversa y por lo tanto la igualdad de xNx^{-1} y N.

(c) $\Rightarrow$ (a) Tenemos $Nx = (xNx^{-1})x$, y es inmediato que este último conjunto es xN. ■

Ejemplo 4.118. Si G es un grupo abeliano, es inmediato que todo subgrupo H de G es normal en G: si $x \in G$ y $h \in H$, entonces $xhx^{-1} = xx^{-1}h = h \in H$, luego $xHx^{-1} \subset H$ y así $H \trianglelefteq G$. ◂

Ejemplo 4.119. Si G es un grupo, el conjunto

$$Z(G) = \{g \in G \mid xg = gx \text{ para todo } x \in G\},$$

formado por los elementos de G que conmutan con todo elemento de G, se llama **centro** de G, y se comprueba sin dificultad que $Z(G) \trianglelefteq G$. ◂

Ejemplo 4.120. El grupo alternado A_n es normal en Σ_n. Para ver esto, recordemos que la proposición 4.48 nos dice que $\tau\sigma\tau^{-1} = \sigma^\tau$ y σ tienen la misma estructura de ciclos para cualesquiera $\sigma, \tau \in \Sigma_n$, luego σ^τ será par si σ lo es, y por lo tanto $\tau A_n \tau^{-1} \subset A_n$, es decir, $A_n \trianglelefteq \Sigma_n$. ◂

Ejemplo 4.121. Sea G un grupo y $H \leq G$ con $[G : H] = 2$. Entonces las únicas clases laterales de H son H y $G \setminus H$. Si $x \in H$ entonces $xH = H = Hx$, y si $x \notin H$ entonces $xH = G \setminus H = Hx$. Por tanto, en cualquier caso $xH = Hx$ y así $H \trianglelefteq G$. Observemos que la conclusión de este ejemplo nos da otro argumento del por qué $A_n \trianglelefteq \Sigma_n$. ◀

Ejemplo 4.122. En el grupo diedral D_8, los subgrupos $\langle r \rangle$, $\langle s, r^2 \rangle$ y $\langle rs, r^2 \rangle$ son de orden 4 y por tanto de índice 2. Como vimos en el ejemplo 4.121, esto implica que tales subgrupos son normales en D_8. Puesto que $|\langle s \rangle| = 2$, también $[\langle s, r^2 \rangle : \langle s \rangle] = 2$, luego se dan las relaciones $\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$. Sin embargo, no es cierto que $\langle s \rangle \trianglelefteq D_8$, pues por ejemplo

$$r\langle s \rangle = \{r, rs\} \qquad \text{y} \qquad \langle s \rangle r = \{r, sr\},$$

y como $rs \neq sr$, estas clases son distintas y por lo tanto $\langle s \rangle$ no puede ser normal en D_8. Este ejemplo demuestra que la relación de ser un subgrupo normal no es en general transitiva. ◀

Ejemplo 4.123. Sea K el subconjunto de Σ_4 formado por la identidad y las permutaciones cuya estructura de ciclos es $(a\ b)(c\ d)$. En Σ_4 existen

$$\frac{1}{2}\left(\frac{1}{2}(4 \cdot 3) \cdot \frac{1}{2}(2 \cdot 1)\right) = 3$$

permutaciones con la estructura indicada. Con más detalle, tenemos que

$$K = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

y es fácil comprobar que $K \leq A_4 \leq \Sigma_4$ y que, de hecho, K es isomorfo a $\mathbf{V}$, el grupo de 4 de Klein. Puesto que la conjugación de permutaciones preserva la estructura de ciclos (teorema 4.49), tenemos que si $\alpha \in K$ entonces $\alpha^\sigma = \sigma\alpha\sigma^{-1} \in K$ para toda permutación $\sigma \in \Sigma_4$, por lo que $K \trianglelefteq \Sigma_4$ y también $K \trianglelefteq A_4$. Conviene observar de paso que Σ_4 contiene otros subgrupos isomorfos a $\mathbf{V}$ que no son normales en Σ_4, como es el caso del subgrupo $\langle (1\ 2), (3\ 4) \rangle$. ◀

Uno de los ejemplos más importantes de un subgrupo normal nos la da la proposición siguiente.

Proposición 4.124. *Para todo homomorfismo de grupos $f : G \to H$,* $\ker f$ *es un subgrupo normal de G.*

Demostración: Si $n \in \ker f$, entonces para todo $x \in G$ tendremos

$$f(xnx^{-1}) = f(x)f(n)f(x^{-1}) = f(x)f(x)^{-1} = 1_H$$

y por tanto $x(\ker f)x^{-1} \subset \ker f$, o sea que $\ker f \trianglelefteq G$. ■

Ejemplo 4.125. La proposición 4.124 nos da otra razón más del por qué $A_n \trianglelefteq \Sigma_n$, ya que sgn (la signatura de permutaciones) es un homomorfismo de Σ_n en el grupo multiplicativo $\{1, -1\}$ y por definición $A_n = \ker(\text{sgn})$. ◀

Otro hecho elemental, cuya demostración se deja como ejercicio al lector, es que los homomorfismos de grupos conservan la relación de normalidad:

Proposición 4.126. *Si $f : G \to H$ es un homomorfismo de grupos. Si $N \trianglelefteq G$ y $M \trianglelefteq H$, entonces $f(N) \trianglelefteq f(G)$ y $f^{-1}(M) \trianglelefteq G$.*

Para concluir esta sección, presentamos algunos resultados básicos en relación a los subgrupos normales.

Proposición 4.127. *Si G es un grupo y $N \trianglelefteq G$, entonces para todo $H \leq G$, $(H \cap N) \trianglelefteq H$.*

Demostración: Sea $x \in H$ y $n \in (H \cap N)$. Puesto que N es normal en G, $xnx^{-1} \in N$, y como $x, n \in H$, también $xnx^{-1} \in H$, luego $xnx^{-1} \in (H \cap N)$. Esto demuestra que $H \cap N$ es normal en H. ■

Si S y T son subconjuntos de un grupo G, usaremos la notación $\langle S, T\rangle$ para representar el subgrupo de G generado por $S \cup T$. Más en general, si $S_1, \ldots, S_n$ son subconjuntos de G, definimos

$$\langle S_1, \ldots, S_n\rangle = \langle S_1 \cup \cdots \cup S_n\rangle .$$

Proposición 4.128. *Si N y H son subgrupos de un grupo G y $N \trianglelefteq G$, entonces $NH \leq G$, y de hecho*

$$\langle N, H\rangle = NH = HN.$$

Más aún, si también H es normal en G, entonces $NH \trianglelefteq G$.

Demostración: Desde luego, $NH \subset \langle N, H\rangle$. Por otra parte, el hecho de que $N \trianglelefteq G$ implica que $NH = HN$, así que NH es un subgrupo de G por la proposición 4.112, y como claramente contiene a $N \cup H$, debe ser $\langle N, H\rangle \subset NH$. Esto demuestra que $\langle N, H\rangle = NH = HN$.

Si $H \trianglelefteq G$, entonces $xNH = (xN)H = (Nx)H = N(xH) = N(Hx) = NHx$, luego $NH \trianglelefteq G$. ■

Si N_1 y N_2 son subgrupos normales de un grupo G, entonces

$$N_1 \cap N_2 \trianglelefteq G,$$

pues si $n \in N_1 \cap N_2$ entonces $xnx^{-1} \in N_1$ y $xnx^{-1} \in N_2$ para todo $x \in G$ por ser $N_1, N_2 \trianglelefteq G$, y de esto se sigue que $xnx^{-1} \in N_1 \cap N_2$ y por tanto que

$$x(N_1 \cap N_2)x^{-1} \subset N_1 \cap N_2,$$

que nos dice que $N_1 \cap N_2 \trianglelefteq G$. Esta conclusión y la de la proposición 4.128 puede generalizarse a cualquier familia de subgrupos normales.

Proposición 4.129. *Sea G un grupo y $\{N_i\}_{i\in I}$ una familia de subgrupos normales de G. Entonces*

(a) $\langle N_i\rangle_{i\in I} \trianglelefteq G$;

(b) $\bigcap_{i\in I} N_i \trianglelefteq G$.

Demostración: (a) Sea $\{H_j\}_{i\in J}$ la familia de subgrupos de G que contienen a todo N_i y x un elemento cualquiera de G. Entonces $N_i = xN_ix^{-1} \subset xH_jx^{-1}$ para todo $i \in I$ y todo $j \in J$, o sea que $\{xH_jx^{-1}\}_{i\in J} = \{H_j\}_{i\in J}$. Por lo tanto, si $h \in \langle N_i\rangle_{i\in I}$, también $xhx^{-1} \in \langle N_i\rangle_{i\in I}$, luego este subgrupo es normal en G.

(b) Se deduce de que $n \in N_i$ implica $xnx^{-1} \in N_i$ para todo $i \in I$. ■

La proposición anterior y el subgrupo $K \trianglelefteq A_4$ identificado en el ejemplo 4.123 pueden usarse para dar otra demostración de que A_4 no tiene ningún subgrupo de orden 6 (proposición 4.110): si fuese $H \leq A_4$ con $H = 6$, entonces $[G : H] = 2$ y por tanto $H \trianglelefteq A_4$, luego $H \cap K \trianglelefteq A_4$, pero el hecho de que

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = \frac{6 \cdot 4}{|H \cap K|} \leq 12$$

y de que $|H \cap K|$ es divisor común de $|H|$ y de $|K|$ implican que $|H \cap K| = 2$, por lo que $H \cap K$ contiene exactamente una permutación no neutra de estructura $(a\ b)(c\ d)$. No obstante, encontramos que

$$[(a\ b)(c\ d)]^{(a\ b\ c)} = (b\ c)(a\ d) \notin H \cap K,$$

en contradicción con que $H \cap K \trianglelefteq A_4$.

EJERCICIOS

4.1. Sea H el subgrupo de Σ_4 formado por las permutaciones que fijan 4. ¿Es H normal en Σ_4?

Solución: No lo es. Por ejemplo, $(1\ 2) \in H$, pero $(1\ 2)^{(2\ 4)} = (1\ 4) \notin H$.

4.2. Sea G un grupo y $N \leq G$. Demostrar que $N \trianglelefteq G$ si y sólo si la congruencia izquierda módulo N es una relación de congruencia en G. (Desde luego, la situación es la misma para las congruencias derechas).

Solución: Supongamos que $N \trianglelefteq G$ y que $xN = x'N$ y $yN = y'N$. Entonces

$$xyN = x(Ny) = x(Ny') = (x'N)y' = x'(Ny') = x'(y'N) = x'y'N,$$

lo que muestra que $x \equiv_i x'$ (mód N) y $y \equiv_i y'$ (mód N) implican $xx' \equiv yy'$ (mód N), lo que significa que $\cdot \equiv_i \cdot$ (mód N) es de congruencia en G.

Recíprocamente, supongamos que la congruencia izquierda módulo N es una relación de congruencia en G, y sea $n \in N$. Puesto que $xnN = xN$ y $x^{-1}N = x^{-1}N$ para todo $x \in G$, tenemos que

$$xnx^{-1}N = xx^{-1}N = N,$$

o sea que $xnx^{-1} \in N$ y por tanto $xNx^{-1} \subset N$, así que $n \trianglelefteq G$ por la proposición 4.117.

4.3. Demostrar que si H es un subgrupo de G, también lo es xHx^{-1} para todo $x \in G$, y de hecho $H \simeq xHx^{-1}$.

4.4. Sea G un grupo finito. Demostrar que si H es el único subgrupo de G de orden n, entonces $H \trianglelefteq G$.

4.5. Demostrar que todos los subgrupos de el grupo $\mathbb{H}$ de los cuaterniones son normales.

4.6. Demostrar que el centro de Σ_n es trivial para $n \geq 3$.

4.9 GRUPOS COCIENTE

Si N es un subgrupo normal de G, podemos hablar del conjunto de las clases laterales de N en G sin necesidad de aclarar si se trata de clases laterales derechas o izquierdas. Observamos que si $xN = x'N$ y $yN = y'N$, entonces la normalidad de N implica que

$$xyN = x(Ny) = x(Ny') = (x'N)y' = x'(Ny') = x'(y'N) = x'y'N,$$

luego la multiplicación de clases laterales dada por $(xN)(yN) = xyN$ es una operación bien definida en el conjunto de todas ellas. Es inmediato verificar que se trata de una operación asociativa y que tiene a N como elemento neutro y a $x^{-1}N$ como inverso de xN para todo $x \in N$. Estas observaciones le dan validez a la definición siguiente.

Definición 4.130. Si G es un grupo y N un subgrupo normal de G, llamamos **grupo cociente** de G por N al conjunto de clases laterales de N en G junto con la multiplicación de clases dada por

$$(xN)(yN) = xyN$$

para cualesquiera $x, y \in G$. A dicho grupo lo representaremos por G/H.

Ejemplo 4.131. De la discusión del ejemplo 4.95 deducimos que los grupos cociente que podemos formar a partir del grupo $\mathbb{Z}$ son los de la forma

$$\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}.$$

En este caso observamos también que

$$\mathbb{Z}/m\mathbb{Z} = \langle 1 + m\mathbb{Z} \rangle,$$

luego dicho grupo cociente es cíclico de orden m y por tanto debe ser

$$\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$$

en virtud del teorema 4.92. ◀

Ejemplo 4.132. En el ejemplo 4.123 vimos que

$$K = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

es un subgrupo normal de A_4 (y también de Σ_4), por lo que podemos formar el grupo cociente A_4/K. Puesto que $\left|A_4/K\right| = \left|A_4\right|/|K| = 12/4 = 3$, el grupo A_4/K debe ser cíclico por el corolario 4.107, de modo que

$$A_4/K \simeq \mathbb{Z}_3$$

de acuerdo con el teorema 4.92. ◀

Ejemplo 4.133. Consideremos el subgrupo $\langle r^2 \rangle$ del grupo diedral D_8 generado por la rotación r de 90° grados y una reflexión s. De la relación $rs = sr^{-1}$ obtenemos que $r^i s = sr^{-i}$ para todo entero i, y en particular $r^2 s = sr^{-2} = sr^2$ por ser r^2 inverso de sí mismo. De esta última igualdad se deduce fácilmente que r^2 conmuta con todo elemento de D_8 y por tanto que $\langle r^2 \rangle \trianglelefteq D_8$, luego existe el grupo cociente $D_8/\langle r^2 \rangle$, cuyos elementos son las $|D_8|/|\langle r^2 \rangle| = 8/2 = 4$ clases laterales

$$\langle r^2 \rangle = \{1, r^2\} \qquad r\langle r^2 \rangle = r, r^3$$
$$s\langle r^2 \rangle = \{s, sr^2\} \qquad rs\langle r^2 \rangle = rs, r^3 s.$$

Comprobamos fácilmente que ninguna de estas clases genera a $D_8/\langle r^2 \rangle$, luego el corolario 4.108 nos dice que debe ser

$$D_8/\langle r^2 \rangle \simeq \mathbf{V},$$

con $\mathbf{V}$ el grupo de 4 de Klein. ◀

Ya hemos visto, con el contraejemplo dado en la proposición 4.110, que el recíproco del teorema de Lagrange no es cierto en lo general. Sin embargo, más adelante (teorema 4.162, conocido como teorema de Cauchy) veremos que este teorema admite un recíproco parcial, siendo cierto para el caso en que el divisor del orden del grupo es un número primo. De momento, los resultados con los que contamos nos permiten dar una demostración de este hecho cuando el grupo en cuestión es abeliano, pues en ese caso todos los subgrupos son normales y tenemos la posibilidad de formar grupos cocientes en todo momento.

Teorema 4.134. *Si G es un grupo abeliano y p es un número primo divisor del orden de G, entonces G tiene un elemento de orden p.*

Demostración: Lo demostraremos por inducción sobre $|G|$. El caso base, $|G| = 1$, se verifica trivialmente por que en ese caso $|G|$ no tiene divisores primos. Supongamos ahora que el resultado es cierto para grupos de orden menor a $|G|$ y sea x un elemento no neutro de G. Si p divide al orden de x entonces el resultado es inmediato, pues en ese caso $|x| = kp$ para algún entero k y el apartado (b) del teorema 4.87 nos da que $|x^k| = kp/k = p$. Supongamos pues que $p \nmid |x|$. Siendo ese el caso, p será entonces un divisor de

$$|G/\langle x \rangle| = \frac{|G|}{|x|},$$

y como $|x| > 1$, el número de arriba es menor que $|G|$, por lo que podemos aplicar la hipótesis de inducción al grupo cociente $G/\langle x \rangle$ para obtener un elemento $y\langle x \rangle$ de orden p, lo que significa que $y^p \in \langle x \rangle$, y esto en particular implica que $y \neq y^p$, pues de otro modo $y \in \langle x \rangle$ y $y\langle x \rangle$ sería neutro y por tanto no podría ser de orden p. Ahora bien, por el apartado (b) del teorema 4.87, tenemos

$$|y^p| = \frac{|y|}{\operatorname{mcd}(p, |y|)},$$

y esto junto con el hecho de que $y \neq y^p$ nos dice que debe ser $\text{mcd}\,(p, |y|) \neq 1$, y al ser p un número primo, esto a su vez implica que $p \mid |y|$. Así, $|y| = kp$ para cierto $k \in \mathbb{Z}$ y por tanto $\left|y^k\right| = kp/k = p$. ■

Si G es de orden finito, entonces el teorema de Lagrange nos dice que $x^{|G|} = 1$ para todo $x \in G$. Puesto que $x^n = 1$ implica que $|x|$ divide a n, resulta que el exponente de G es múltiplo del orden de todo elemento $x \in G$. Por otra parte, el múltiplo m de los órdenes de los elementos de G cumple con $x^m = 1$ para todo $x \in G$, así que el exponente de G es el mínimo común múltiplo de los órdenes de los elementos de G. En particular, esto implica que un número primo p es factor del exponente de G si y sólo si lo es de $|x|$ para al menos un $x \in G$. Esta observación nos sirve para comprender mejor la siguiente demostración alternativa del teorema anterior (basada en Lang 2005, p. 33).

Demostración alternativa: Demostramos primero que si n es un exponente de G, entonces $|G|$ debe dividir alguna potencia de n. Procedemos por inducción sobre $|G|$, donde el caso base $|G| = 1$ es inmediato. Supongamos la afirmación cierta para grupos abelianos de orden menor al de G, y sea $x \neq 1$ un elemento de G. Es claro que n es un exponente de $G/\langle x\rangle$, luego la hipótesis de inducción nos da que $|G/H|$ divide una potencia de n, pero como $|x|$ divide a n y

$$|G| = |G/H|\,|H|\,,$$

resulta que $|G|$ también divide a una potencia de n.

Supongamos ahora que p es un divisor primo del orden de G. Entonces una potencia de p divide una potencia de n, un exponente de G. Puesto que p es primo, p debe dividir a n mismo, luego algún elemento de G es de orden un múltiplo de p, digamos $x \in G$ con $|x| = pm$. Entonces x^m es un elemento de G de orden p. ■

Proposición 4.135. *Sea G un grupo y $Z(G)$ el centro de G. Si $G/Z(G)$ es cíclico, entonces G es abeliano.*

Demostración: Supongamos que $G/Z(G)$ está generado por $gZ(G)$ y que x es un elemento cualquiera de G. Entonces $xZ(G) \in g^kZ(G)$ para algún $k \in \mathbb{Z}$, lo que significa que $x = g^kz$ para cierto $z \in Z(G)$. Puesto que z conmuta con cualquier elemento de G, tenemos que $gx = g^{k+1}z = g^kzg = xg$, o sea que $g \in Z(G)$ y por tanto $G/Z(G) = \langle Z(G)\rangle = 1$, de donde se sigue que $G = Z(G)$, luego G es abeliano. ■

Definición 4.136. Si G es un grupo y $N \trianglelefteq G$, la aplicación $\pi : G \to G/N$ dada por

$$x \mapsto xN$$

para todo $x \in G$, es un epimorfismo de grupos, que llamaremos **epimorfismo canónico** (o también **proyección canónica**) de G en el grupo cociente G/N.

Los conceptos anteriores nos permiten establecer el recíproco de la proposición 4.124.

Proposición 4.137. *Si N es un subgrupo normal de un grupo G, entonces N es el núcleo del epimorfismo canónico $\pi : G \to G/N$.*

Demostración: Dicho epimorfismo está dado por $\pi(x) = xN$. Por lo tanto, $x \in \ker\pi$ si y sólo si $xN = N$, lo cual ocurre si y sólo si $x \in N$. En otras palabras, $N = \ker\pi$. ■

4.10 TEOREMAS DE ISOMORFÍA

En la proposición 4.124 vimos que si $f : G \to H$ es un homomorfismo de grupos, entonces $\ker f$ es un subgrupo normal de G, así que dado cualquier homomorfismo de grupos $f : G \to H$ siempre podemos formar el grupo cociente $G/\ker f$. Vamos a ver que este grupo cociente guarda una estrecha relación con la imagen del homomorfismo f.

Teorema 4.138. *Sea $\phi : G \to H$ un homomorfismo de grupos y $N \trianglelefteq G$ tal que $N \leq \ker \phi$. Entonces existe un único homomorfismo $\phi^* : G/N \to H$ tal que*

$$\phi^* \circ \pi = \phi.$$

Además, $\operatorname{im} \phi^* = \operatorname{im} \phi$ *y ϕ^* es inyectiva cuando $N = \ker \phi$.*

Demostración: Observemos que la condición $\phi^* \circ \pi = \phi$, nos obliga a definir $\phi^*(xN) = \phi^*(\pi(x)) = \phi(x)$, de manera que ϕ^* está unívocamente determinada por ϕ, luego sólo resta verificar que ϕ^* está bien definida por la fórmula $\phi^*(xN) = \phi(x)$. Para esto, supongamos que $xN = yN$. Entonces $xy^{-1} \in N \subset \ker \phi$ y por tanto $\phi(xy^{-1}) = 1$, de donde se sigue que $\phi(x) = \phi(y)$. Esto comprueba que ϕ^* está bien definida.

Que ϕ^* sea un homomorfismo se deduce inmediatamente de que ϕ lo es:

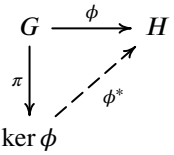
$$\phi^*(xNyN) = \phi^*(xyN) = \phi(xy) = \phi(x)\phi(y) = \phi^*(xN)\phi^*(yN).$$

Es evidente que $\operatorname{im} \phi^* = \operatorname{im} \phi$, y como

$$\ker \phi^* = \{xN \mid \phi(x) = 1\} = \{xN \mid x \in \ker \phi\} = (\ker \phi)/N,$$

la proposición 4.80 nos dice que ϕ^* es inyectiva cuando $(\ker \phi)/N = \{N\}$, lo cual ocure cuando $N = \ker \phi$. ■

La conclusión principal del teorema anterior se puede resumir diciendo que si $\phi : G \to H$ es un homomorfismo de grupos y $N \leq \ker \phi$ es normal en G, entonces existe un único homomorfismo ϕ^* tal que el diagrama siguiente es conmutativo:



Corolario 4.139 (Primer teorema de isomorfía). *Si $f : G \to H$ es un homomorfismo de grupos, entonces*

$$G/(\ker f) \cong \operatorname{im} f.$$

Tenemos así la siguiente "descomposición canónica" de un homomorfismo de grupos $f : G \to H$:

$$G \xrightarrow{\pi} G/(\ker f) \xrightarrow{f^*} \operatorname{im} f \xrightarrow{\subset} H.$$

Veamos algunos ejemplos en los que se usa el primer teorema de isomorfía para clasificar grupos cociente.

Ejemplo 4.140. Ya habíamos visto que $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$ en el ejemplo 4.131, y ahora podemos llegar a la misma conclusión con más elegancia observando que la aplicación $f : \mathbb{Z} \to \mathbb{Z}_m$ dada por $x \mapsto [x]$ es un epimorfismo con núcleo $\ker f = \{x \in \mathbb{Z} \mid [x] = [1]\} = \{kn \mid k \in \mathbb{Z}\} = n\mathbb{Z}$, luego por el primer teorema de isomorfía

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n \qquad \blacktriangleleft$$

La isomorfía descrita en el ejemplo siguiente es más interesante y probablemente algo inesperada.

Ejemplo 4.141. Sea S^1 el grupo circular formado por los números complejos $e^{i\theta}$ y $\mathbb{R}$ el grupo aditivo de números reales, y sea $f : \mathbb{R} \to S^1$ dada por $x \mapsto e^{2\pi i\theta}$. Puesto que $e^{i\theta}e^{i\phi} = e^{i(\theta+\phi)}$, f es un homomorfismo, claramente sobreyectivo, cuyo núcleo $\ker f$ consiste de todos los $x \in \mathbb{R}$ tales que $e^{2\pi ix} = 1$, o sea que $\ker f = \mathbb{Z}$, así que el primer teorema de isomorfía nos dice que

$$\mathbb{R}/\mathbb{Z} \simeq S^1. \qquad \blacktriangleleft$$

Del primer teorema de isomorfía se desprenden a su vez otros hechos importantes sobre grupos cociente.

Teorema 4.142 (Segundo teorema de isomorfía). *Sean H y N subgrupos de un grupo G con $N \trianglelefteq G$. Entonces N es un subgrupo normal de HN y $N \cap H$ es un subgrupo normal de H. Más aún,*

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

Demostración: Sabemos por la proposición 4.128 que NH es un subgrupo de G, y como $N \leq HN$ es normal en todo G, en particular lo es en HN, así que podemos formar el grupo cociente HN/N. Vemos que la aplicación $\phi : H \to HN/N$ dada por $\phi(h) = hN$ es un homomorfismo, pues

$$\phi(xy) = xyN = (xN)(yN) = \phi(x)\phi(y).$$

Además,

$$\ker\phi = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N,$$

y como ϕ es claramente sobreyectiva, el primer teorema de isomorfía nos dice que $H/(H \cap N) \cong HN/N$. ∎

Teorema 4.143 (Tercer teorema de isomorfía). *Sea G un grupo y $N \trianglelefteq H \trianglelefteq G$. Entonces H/N es un subgrupo normal de G/N y*

$$(G/N)/(H/N) \cong G/H.$$

Demostración: Definimos la aplicación $\phi : G/N \to G/H$ por $\phi(xN) = xH$. Esta aplicación está bien definida, pues si $xN = yN$ entonces $xy^{-1} \in N$ y así $xy^{-1} \in H$

puesto que $N \leq H$, o sea que $xH = yH$. Se trata claramente de una sobreyección, y como

$$\phi(xNyN) = \phi(xyN) = xyH = (xH)(yH) = \phi(xN)\phi(yN),$$

esta aplicación es además un homomorfismo con

$$\ker \phi = \{xN \in G/N \mid xH = H\} = \{xN \in G/N \mid x \in H\} = H/N.$$

El resultado se sigue, por tanto, del primer teorema de isomorfía. ■

Teorema 4.144. *Si G es un grupo, entonces*

$$G/\mathbf{Z}(G) \cong \mathrm{inn}(G).$$

Demostración: Sea $f : G \to \mathrm{aut}(G)$ dada por $f(x) = \phi_x$, donde $\phi_x \in \mathrm{aut}(G)$ está dada por $\phi_x(g) = xgx^{-1}$. Puesto que $\phi_x \circ \phi_y = \phi_{xy}$, tenemos que

$$f(xy) = \phi_{xy} = \phi_x \circ \phi_y = f(x)f(y),$$

así que f es un homomorfismo de G en $\mathrm{aut}(G)$. Por supuesto, $\mathrm{im}\, f = \mathrm{inn}(G)$, y como

$$\begin{aligned}\ker f &= \{x \in G \mid \phi_x = \mathrm{id}_G\} \\ &= \{x \in G \mid xgx^{-1} = g \text{ para todo } g \in G\} \\ &= \{x \in G \mid xg = gx \text{ para todo } g \in G\} \\ &= \mathbf{Z}(G),\end{aligned}$$

el corolario 4.139 nos da el resultado buscado. ■

Teorema 4.145 (Teorema de correspondencia). *Sea $f : G \to H$ un epimorfismo de grupos, $S_f(G)$ el conjunto de los subgrupos de G que contienen a $\ker f$ y $S(H)$ el conjunto de todos los subgrupos de H. Entonces la fórmula $\Phi : K \mapsto f(K)$ establece una correspondencia biunívoca Φ entre $S_f(G)$ y $S(H)$ que, además, preserva la relación de normalidad: si $K \in S_f(G)$ con $K \trianglelefteq G$, también $\Phi(K) \trianglelefteq H$.*

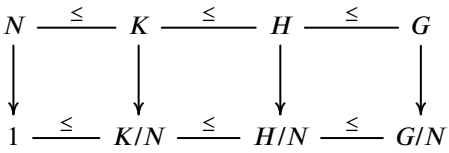
Demostración: Sabemos que $\Phi(K)$ es un subgrupo de H para todo $K \leq G$ y que $f^{-1}(J)$ es un subgrupo de G para todo $J \leq H$, y como siempre es cierto que $\ker f \leq f^{-1}(J)$, tenemos que $f^{-1}(J) \in S_f(G)$, de modo que Φ es sobreyectiva. Por otra parte, si $x \in f^{-1}(f(K))$ para $K \leq G$, entonces $x \in k \ker f$ para algún $k \in K$, luego si K contiene a $\ker f$ tendremos $x \in K$, de donde se sigue que $f^{-1}(f(K)) = K$ y por tanto que Φ es inyectiva.

Finalmente, el hecho de que Φ haga corresponder subgrupos normales con subgrupos normales se sigue de la sobreyectividad de f y de la proposición 4.126. ■

El teorema 4.145 tiene un corolario muy útil.

Corolario 4.146. *Si N es un subgrupo normal de G, entonces todo subgrupo de G/N es de la forma K/N para un único $K \leq G$ que contiene a N.*

El diagrama de abajo ilustra la correspondencia que, de acuerdo con el corolario anterior, existe entre los subgrupos de G que contienen a N y los subgrupos de G/N.



EJERCICIOS

4.7. Demostrar que $(\mathbb{Z} \oplus \mathbb{Z})/\langle (m,0),(0,n)\rangle \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Solución: Sea $\phi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ dada por $\phi : (x,y) \mapsto (x,y)$. Es inmediato que ϕ es un epimorfismo de grupos, y $\ker\phi$ consiste de los $(x,y) \in \mathbb{Z} \oplus \mathbb{Z}$ en los que x es múltiplo de m y y es múltiplo de n, o sea que $\ker\phi = \{(mk,0)+(0,nl) \mid m,n \in \mathbb{Z}\} = \langle (m,0),(0,n)\rangle$. El resultado buscado es consecuencia del primer teorema de isomorfía.

4.8. Demostrar que para cualesquiera grupos G y H, $(G \oplus H)/(1 \oplus H) \cong G$.

Solución: Sea π_G la proyección de $G \oplus H$ en G, o sea que $(g,h) \mapsto g$ para todo $(g,h) \in G \oplus H$. Entonces $\ker\pi_G = \{(1,h) \mid h \in H\} = 1 \oplus H$, de donde se sigue el resultado deseado.

4.9. ¿Existe algún epimorfismo $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \to \mathbb{Z}_4 \oplus \mathbb{Z}_4$?

Solución: No, no puede existir tal epimorfismo. Para probarlo, supongamos lo contrario, y sea ϕ el epimorfismo descrito. Entonces el primer teorema de isomorfía nos da $\left|(\mathbb{Z}_8 \oplus \mathbb{Z}_2)/\ker\phi\right| = \left|\mathbb{Z}_4 \oplus \mathbb{Z}_4\right| = 8$, luego tiene que ser $\ker\phi = 1$ y con ello ϕ es inyectivo y por tanto un isomorfismo, lo que es imposible por que $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ no tiene un elemento de orden 8.

4.10. ¿Existe algún epimorfismo $\mathbb{Z}_{16} \oplus \mathbb{Z}_2 \to \mathbb{Z}_4 \oplus \mathbb{Z}_4$?

Solución: Supongamos que existe tal homomorfismo ϕ. Entonces $|\ker\phi| = 2$ y por tanto $\ker\phi \cong \mathbb{Z}_2$, así que $(\mathbb{Z}_{16} \oplus \mathbb{Z}_2)/\ker\phi \cong \mathbb{Z}_{16} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$, lo que no es posible por que $\mathbb{Z}_4 \oplus Z_4$ no es cíclico.

4.11. Sea p un número primo impar. Si H es un grupo de orden impar, demostrar que no existe ningún homomorfismo no trivial $D_{2p} \to H$.

Solución: Si $\phi : D_{2p} \to H$ es un homomorfismo, entonces $\ker\phi$ debe ser de orden 1, 2, p o $2p$. Desde luego, no puede ser $|\ker\phi| = 1$ o p por que entonces $\phi(D_{12}) = 2p$ o 2, y ninguno de estos números divide $|H|$. Tampoco puede ser $|\ker\phi| = 2$, pues el hecho de que p sea un primo impar implica que D_{2p} no tiene un subgrupo normal de orden 2. Así pues, la única posibilidad es que $\ker\phi = D_{2p}$ y por tanto que ϕ sea trivial.

4.11 ACCIONES DE GRUPO

Comenzaremos esta sección con la observación siguiente.

Teorema 4.147. *Todo grupo es isomorfo a un grupo de permutaciones.*

Demostración: Esto es consecuencia de que los elementos de un grupo son permutados al multiplicarlos por un elemento fijo del grupo. Con más detalle, sea G un grupo y Σ_G el grupo de las permutaciones de los elementos de G. Para cada $g \in G$, definimos una aplicación $\tau_g : G \to G$ por $\tau_g : x \mapsto gx$. Entonces

$$(\tau_g \circ \tau_{g^{-1}})(x) = g(g^{-1}x) = x$$

para todo $x \in G$, lo que nos dice que todo τ_g es invertible y por tanto una biyección, de donde se sigue que $\tau_g \in \Sigma_G$ para todo $g \in G$. Observamos también que

$$\tau_{gh}(x) = ghx = \tau_g(\tau_h(x)) = (\tau_g\tau_h)(x),$$

lo que nos dice que la aplicación $\Phi : G \to \Sigma_G$ dada por $g \mapsto \tau_h$ es un homomorfismo de grupos. Si ocurre que $\tau_g = \tau_h$, entonces $gx = hx$ para todo $x \in G$, y el caso $x = 1$ nos da la igualdad $g = h$, de donde se sigue que Φ es inyectivo, de modo que $G \cong \operatorname{im}\Phi \leq \Sigma_G$. ■

Cuando G es de orden finito n, el teorema anterior nos dice que G es isomorfo a un subgrupo de Σ_n, pues en ese caso sabemos que $\Sigma_G \cong \Sigma_n$.

Más general e importante es el hecho siguiente.

Teorema 4.148. *Sea G un grupo y H un subgrupo de G de índice finito n. Entonces existe un homomorfismo $\Phi : G \to \Sigma_n$ cuyo núcleo está contenido en H.*

Demostración: Sea G/H el conjunto de las clases laterales de H en G. Puesto que no estamos asumiendo que H es normal en G, dicho conjunto no es necesariamente un grupo cociente, aunque aquí no necesitamos que lo sea. Lo que hacemos es definir, para cada $g \in G$, una aplicación $\tau_g : G/H \to G/H$ por $\tau_g : xH \mapsto gxH$. Se verifica entonces sin dificultad que cada una de estas aplicaciones es un biyección y por tanto elementos de $\Sigma_{G/H} \cong \Sigma_n$. También es fácil comprobar que $\tau_g\tau_h = \tau_{gh}$, de manera que la aplicación $\Phi : G \to \Sigma_{G/H}$ que envía a cada $g \in G$ con la permutación τ_g es un homomorfismo de grupos. Además, si $\Phi(g) = \tau_1 = 1_{G/H}$, entonces $gxH = xH$ para todo $x \in G$, y del caso $x = 1_G$ obtenemos que $gH = H$, de donde se sigue que $g \in H$ y por tanto que $\ker\Phi \leq H$. ■

Notemos que el teorema de Cayley (4.147) se deduce del anterior tomando $H = \{1\}$.

Corolario 4.149. *Sea H un subgrupo G de índice n. Si G no tiene subgrupos normales contenidos en H además del subgrupo trivial, entonces G es isomorfo a un subgrupo de Σ_n.*

Demostración: Por el teorema 4.148, existe un homomorfismo $\Phi : G \to \Sigma_{G/H}$ y su núcleo es un subgrupo normal de G contenido en H, luego por hipótesis dicho núcleo debe ser trivial, de donde se sigue que el homomorfismo $G \to \Sigma_n$ es inyectivo, luego $G \cong \operatorname{im}\Phi \leq \Sigma_{G/H} \cong \Sigma_n$. ■

Corolario 4.150. *Si H es un subgrupo de G de índice p, donde p es el menor de los primos que dividen al orden de G, entonces H es normal en G.*

Demostración: Sea G/H el conjunto de clases laterales de H en G, y sea $\Phi : G \to \Sigma_p$ el homomorfismo del corolario 4.149. Entonces $\ker\Phi \leq H$ y, por el primer teorema de isomorfía (corolario 4.139), $G/(\ker\Phi)$ es isomorfo a un subgrupo de Σ_p, o sea que $|G/(\ker\Phi)|$ divide a $\left|\Sigma_p\right| = p!$. Puesto que $|G| = |\ker\Phi|\,|G/(\ker\Phi)|$, todo divisor de $|G/(\ker\Phi)|$ es divisor del orden de G, pero como ningún entero mayor que 1 y menor que p divide a $|G|$, $|G/(\ker\Phi)|$ es 1 o es p. Pero como $|G/(\ker\Phi)| = [G : H][H : K] = p[H : K] \geq p$, debe ser $|G/(\ker\Phi)| = p$. Así pues, $\ker\Phi$ y H tienen el mismo índice, y como $\ker\Phi \leq H$, debe ser $\ker\Phi = H$, luego $H \trianglelefteq G$. ■

Ahora introduciremos un concepto y una notación más conveniente para hablar de los homomorfismos de un grupo G en un grupo simétrico dado. Supongamos que tenemos un homomorfismo

$$\Phi : G \to \Sigma_X,$$

donde X es un conjunto cualquiera, y sea σ_g la permutación correspondiente a $g \in G$ a través de este homomorfismo. Entonces la operación

$$G \times X \to X,$$

dada por,

$$g \cdot x = \sigma_g(x),$$

verifica las propiedades siguientes:

(a) Para todo $x \in X$, $1 \cdot x = x$. En efecto, pues Φ es un homomorfismo y por tanto σ_1 es la permutación identidad, o sea que $1 \cdot x = \sigma_1(x) = x$ para todo $x \in X$.

(b) Si $g, h \in G$, entonces $g \cdot (h \cdot x) = (gh) \cdot x$ para todo $x \in X$. Esto es, de nuevo, consecuencia inmediata de que Φ sea un homomorfismo, pues esto nos dice que $\sigma_g\sigma_h = \sigma_{gh}$ y por tanto que $(gh) \cdot x = \sigma_{gh}(x) = \sigma_g(\sigma_h(x)) = g \cdot (h \cdot x)$.

Recíprocamente, si G es un grupo y X un conjunto, cualquier operación externa $\cdot : G \times X \to X$ que tenga las propiedades de arriba induce un homomorfismo $\Phi : G \to \Sigma_X$, con $\Phi(g) = \sigma_g$ la permutación definida por

$$\Phi(g)(x) = \sigma_g(x) = g \cdot x$$

para todo $x \in X$. Verificar que Φ es en efecto un homomorfismo se deja como ejercicio al lector.

Con las observaciones de arriba queda motivada la definición siguiente.

Definición 4.151. Sea G un grupo y X un conjunto. Una **acción** de G en X es una operación

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

que verifica las propiedades siguientes:

(a) $g(hx) = (gh)x$ para cualesquiera $g, h \in G$ y $x \in X$;

(b) $1x = x$ para todo $x \in G$.

Si tenemos una acción de G en X, decimos también que G **actúa** en el conjunto X, o que X es un ***G*-conjunto**.

Con esta nueva terminología, la discusión de los párrafos previos nos dicen que la acción de un grupo G en un conjunto X no es más que una forma conveniente de hablar de un homomorfismo $G \to \Sigma_X$.

Ejemplo 4.152 (Teorema de Cayley). La demostración del teorema de Cayley nos dice que todo grupo G actúa sobre sí mismo mediante "traslaciones izquierdas", es decir, si para cada $g \in G$ definimos una aplicación $\tau_g : G \to G$ por $\tau_g(x) = gx$ para todo $x \in G$, entonces $g \cdot x = \tau_g(x) = gx$ es una acción de G en sí mismo. ◀

Así, por ejemplo, el teorema de Cayley nos dice que todo grupo actúa sobre sí mismo a través de las "traslaciones izquierdas", es decir, la operación $\cdot : G \times G \to G$ dada por

$$g \cdot x = \tau_g(x) = gx,$$

es decir, donde la acción es simplemente la operación del grupo.

Ejemplo 4.153 (Conjugación). Todo grupo G actúa en sí mismo por medio de la conjugación por elementos de G. En efecto, pues sí $g \cdot x = gxg^{-1}$, entonces obviamente $1 \cdot x = x$, y también $g \cdot (h \cdot x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = gh \cdot x$. ◀

Definición 4.154. Sea G un grupo que actúa sobre un conjunto X. Llamamos **órbita** de $x \in X$ al conjunto

$$\mathcal{O}_G(x) = \{gx \mid g \in G\},$$

y llamamos **estabilizador** de $x \in X$, representado por G_x, al conjunto de todos los elementos de G que fijan a x bajo la acción del grupo. En símbolos,

$$G_x = \{g \in G \mid gx = x\}.$$

Se verifica de inmediato que $G_x \leq G$. Cuando $G_x = \{1\}$, decimos que la acción de G en X es **fiel**.

También es inmediato que la relación de "estar en la misma órbita" es de equivalencia. Cuando $\mathcal{O}_G(x) = X$, es decir, cuando existe una única órbita, decimos que la acción de grupo es **transitiva**. Observemos que esto equivale a que para todo $y \in X$ existe un $g \in G$ tal que $y = gx$.

Definición 4.155. Cuando un grupo G actúa en sí mismo mediante conjugación, la órbita de $x \in G$ se dice **clase de conjugación** de x en G y se representa por x^G, y al estabilizador de x se le llama **centralizador** de x en G y se representa por $\mathbf{C}_G(x)$. Diremos que $x, y \in G$ son **conjugados** si ambos elementos están en la misma clase de conjugación, es decir, si existe $g \in G$ tal que $y = gxg^{-1}$.

Así pues, si G es un grupo y $x \in G$, tenemos

$$x^G = \{x^g \mid g \in G\} = \{gxg^{-1} \mid g \in G\}.$$

Teorema 4.156 (Teorema órbita-estabilizador). *Si un grupo G actúa en un conjunto X, entonces, para todo $x \in X$,*

$$\left|\mathcal{O}_G(x)\right| = [G : G_x].$$

Demostración: Observamos que

$$gx = hx \quad \Leftrightarrow \quad (h^{-1}g)x = x \quad \Leftrightarrow \quad h^{-1}g \in G_x \quad \Leftrightarrow \quad gG_x = hG_x,$$

lo que demuestra tanto que $gx \mapsto hG_x$ está bien definida como que es inyectiva. Puesto que la sobreyectividad de esta aplicación es evidente, tenemos que se trata de una biyección, de manera que $\left|\mathcal{O}_G(x)\right| = \left|G/G_x\right| = [G : G_x]$. ■

Aplicando el teorema órbita-estabilizador a la acción dada por la conjugación, obtenemos el corolario siguiente.

Corolario 4.157. *Para todo elemento x de un grupo G se verifica que*

$$\left|x^G\right| = [G : \mathbf{C}_G(x)]. \tag{4.7}$$

Veamos algunos ejemplos en los que se aplica el corolario anterior.

Ejemplo 4.158 (Centralizador de un r-ciclo). Sea σ un ciclo de Σ_n de longitud r. Puesto que dos ciclos son conjugados si y sólo si tienen la misma longitud (teorema 4.49), tenemos que

$$\left|\sigma^{\Sigma_n}\right| = \frac{1}{r}n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{r(n-r)!},$$

luego la fórmula (4.7) nos da

$$\left|\mathbf{C}_{\Sigma_n}(\sigma)\right| = \frac{\left|\Sigma_n\right|}{\left|\sigma^{\Sigma_n}\right|} = r(n-r)!.$$

A partir de este conteo podemos determinar cuáles son todas las permutaciones que conmutan con σ. Desde luego, toda potencia de σ conmuta con ésta, luego tenemos identificadas r permutaciones que están en $\mathbf{C}_{\Sigma_n}(\sigma)$. También sabemos que cualquier permutación que fije los símbolos movidos por σ estará en su centralizador, y de estas permutaciones hay $(n-r)!$. Si representamos por Σ_{n-r} al conjunto de las permutaciones que fijan los r números movidos por σ, entonces

$$\mathbf{C}_{\Sigma_n}(\sigma) = \{\sigma^i\tau \mid \tau \in \Sigma_{n-r} \text{ y } 0 \leq i \leq r-1\},$$

pues el conjunto del lado contiene $r(n-r)!$ permutaciones que conmutan con σ. ◀

Ejemplo 4.159 (Clases de conjungación en A_4). En este ejemplo vamos a calcular las clases de conjugación que hay en el grupo alternado A_4, y aprovecharemos los resultados obtenidos para dar otra demostración de que A_4 no contiene ningún subgrupo de orden 6 (proposición 4.110). Para comenzar, recordemos que A_4 está formado por la identidad,

3 permutaciones de estructura $(\bullet\ \bullet)(\bullet\ \bullet)$ y los 8 ciclos de longitud 3. Tomemos primero $\sigma = (1\ 2)(3\ 4)$ y consideremos su clase de conjugación en todo el grupo simétrico Σ_n. Por su estructura de ciclos, sabemos que $\left|\sigma^{\Sigma_n}\right| = 3$, de manera que

$$\left|\mathbf{C}_{\Sigma_4}(\sigma)\right| = \frac{24}{3} = 8.$$

Puesto que $\sigma \in \mathbf{V} \leq A_4$, donde $\mathbf{V}$ es el subgrupo isomorfo al grupo de Klein formado por las permutaciones con la estructura $(\bullet\ \bullet)(\bullet\ \bullet)$, existen al menos $|\mathbf{V}| = 4$ elementos de $\mathbf{C}_{\Sigma_4}(\sigma)$ que están en A_4 y por tanto en $\mathbf{C}_{A_4}(\sigma)$, luego este último centralizador contiene al menos 4 elementos. Por otra parte, puesto que $\mathbf{C}_{A_4}(\sigma)$ es un subgrupo tanto de A_4 como de $\mathbf{C}_{\Sigma_4}(\sigma)$, su orden debe ser un divisor común de 8 y 12, luego sólo es posible que

$$\left|\mathbf{C}_{A_4}(\sigma)\right| = 4,$$

o sea que de hecho $\mathbf{C}_{A_4}(\sigma) = \mathbf{V}$. Usando de nuevo la fórmula (4.7) obtenemos que

$$\left|\sigma^{A_4}\right| = \frac{12}{4} = 3,$$

luego las tres permutaciones de estructura $(\bullet\ \bullet)(\bullet\ \bullet)$ son conjugadas en A_4.

Pasemos ahora a las clases de conjugación de los 3-ciclos de A_4. Tomemos uno de ellos, digamos $\tau = (1\ 2\ 3)$. Por la fórmula obtenida en el ejemplo 4.158, $\mathbf{C}_{\Sigma_4}(\tau) = 3(4-3)! = 3$, y de hecho

$$\mathbf{C}_{\Sigma_4}(\tau) = \{1, \tau, \tau^2\} = \langle\tau\rangle \leq A_4,$$

de donde se sigue que $\mathbf{C}_{\Sigma_4}(\tau) = \mathbf{C}_{A_4}(\tau)$ y por tanto que

$$\left|\tau^{A_4}\right| = \frac{12}{3} = 4.$$

Puesto que A_4 contiene 8 ciclos de longitud 3, resulta que dichos ciclos están separados en dos clases de conjugación. En particular, esto implica que no todos los 3-ciclos son conjugados. El siguiente código de *Mathematica* nos dice cuáles exactamente son estas dos clases de conjugación:

```
GroupOrbits[AlternatingGroup[4],
  {Cycles[{{1, 2, 3}}], Cycles[{{1, 3, 2}}]}]
    /. {Cycles[{x_}] :> x} // Column
```

```
{{1,2,3},{1,3,4},{1,4,2},{2,4,3}}
{{1,2,4},{1,3,2},{1,4,3},{2,3,4}}
```

Así pues,

$$(1\ 2\ 3)^{A_4} = \{(1\ 2\ 3),\quad (1\ 3\ 4),\quad (1\ 4\ 2),\quad (2\ 4\ 3)\},$$
$$(1\ 3\ 2)^{A_4} = \{(1\ 3\ 2),\quad (1\ 4\ 3),\quad (1\ 2\ 4),\quad (2\ 3\ 4)\}.$$

Notemos que $(1\ 3\ 2) = (1\ 2\ 3)^{-1}$, y que la clase de conjugación de $(1\ 2\ 3)^{-1}$ consiste de los inversos de los elementos de la clase de $(1\ 2\ 3)$.

Para terminar, observemos que el hecho de que A_4 esté particionado en clases de conjugación de cardinales $1, 3, 4, 4$ nos permite concluir que A_4 no contiene ningún subgrupo de orden 6, pues dicho grupo así sería de índice 2 y por tanto normal en A_4, o sea que sería unión disjunta de clases de conjugación, lo que no puede ser, por que entre los cardinales mencionados no los hay que sumen 6.

Otra forma de comprobar lo anterior es utilizar el hecho de que si σ es un 3-ciclo, entonces σ y σ^{-1} pertenecen a distintas clases de conjugación, como observamos al calcular de forma explícita las dos clases de conjugación de los 3-ciclos. Así, si $H \leq A_4$ fuese de orden 6, tendría que contener un 3-ciclo (pues en todo A_4 sólo hay 4 elementos que no lo son), luego contendría a su inverso, pero entonces la normalidad de H implicaría que contiene a todos los 3-ciclos, o sea que H tendría al menos 8 elementos, una contradicción. ◂

Ejemplo 4.160 (Conjugación de 3-ciclos en A_5). En este ejemplo vamos a mostrar que todos los 3-ciclos son conjugados en A_5. Para esto, consideremos el ciclo $\sigma = (1\ 2\ 3)$ y su clase de conjugación en Σ_5. Por el resultado del ejemplo 4.158, tenemos

$$\left|\mathbf{C}_{\Sigma_5}(\sigma)\right| = 3(5-2)! = 6,$$

y como $\mathbf{C}_{A_n}(\sigma)$ es subgrupo de dicho centralizador y también de A_5, su orden debe ser 6, 3 o 2, pero no puede ser 6 por que no todo elemento de $\mathbf{C}_{\Sigma_5}(\sigma)$ está en A_5 (por ejemplo, la transposición 4 5). Puesto que $\{1, \sigma, \sigma^2\} \leq \mathbf{C}_{A_n}(\sigma)$, debe ser $\left|\mathbf{C}_{A_n}(\sigma)\right| = 3$, y así resulta que

$$\left|\sigma^{A_5}\right| = \frac{60}{3} = 20,$$

de modo que σ^{A_5} contiene a los 20 ciclos de longitud 3 que hay en Σ_5. En otras palabras, cualesquiera dos 3-ciclos son conjugados en A_5. ◂

El teorema siguiente generaliza la conclusión obtenida en el ejemplo anterior.

Teorema 4.161. *Para todo $n \geq 5$, cualesquiera dos ciclos de longitud 3 son conjugados en A_n.*

Demostración: Sea $n \geq 5$ y $\sigma \in A_n$ un 3-ciclo. Entonces existe una transposición $(i\ j)$ disjunta de σ y por tanto contenida en $\mathbf{C}_{\Sigma_n}(\sigma)$. Puesto que $(i\ j) \neq A_n$ y $[\Sigma_n, A_n] = 2$, tenemos

$$\Sigma_n = \langle (i\ j) \rangle\, A_n = \mathbf{C}_{\Sigma_n}(\sigma) A_n.$$

Puesto que también $\mathbf{C}_{A_n}(\sigma) = \mathbf{C}_{\Sigma_n}(\sigma) \cap A_n$, la ecuación (4.6) nos da

$$\begin{aligned}[\Sigma_n : \mathbf{C}_{\Sigma_n}(\sigma)] &= [\mathbf{C}_{\Sigma_n}(\sigma) A_n : \mathbf{C}_{\Sigma_n}(\sigma)] \\ &= [A_n : \mathbf{C}_{\Sigma_n}(\sigma) \cap A_n] \\ &= [A_n : \mathbf{C}_{A_n}(\sigma)].\end{aligned}$$

En otras palabras, $\left|\sigma^{A_n}\right| = \left|\sigma^{\Sigma_n}\right|$, de donde se sigue el resultado deseado. ■

Nota: El teorema anterior puede demostrarse de manera más elemental: si $\sigma = (i_1\ i_2\ i_3)$ es un 3-ciclo en A_n con $n \geq 5$, entonces existe un par de enteros distintos i_4 e i_5 que son fijados por σ, y por tanto una permutación $\tau \in \Sigma_n$ tal que $\tau(k) = i_k$ para $k = 0, \ldots, 5$. Puesto que una de las permutaciones τ y $\rho = (i_4\ i_5)\tau$ está en A_n y

$$\tau(1\ 2\ 3)\tau^{-1} = (i_1\ i_2\ i_3) = \rho(1\ 2\ 3)\rho^{-1},$$

tenemos que todo 3-ciclo es conjugado de cualquier otro 3-ciclo en A_n.

Puesto que las órbitas inducidas por una acción de un grupo finito G en un conjunto X son clases de equivalencia, éstas forman una partición de X, lo que nos dice que el orden de G puede expresarse como

$$|X| = \sum \left|\mathcal{O}_G(x_i)\right| = \sum [G : G_{x_i}],$$

donde cada x_i es un representante de una órbita. Para la acción de G en sí mismo dada por la conjugación ($g \cdot x = gxg^{-1}$), la fórmula de arriba se convierte en

$$|G| = \sum \left|x_i^G\right| = \sum [G : \mathbf{C}_G(x_i)],$$

donde los sumatorios recorren los distintos representantes x_i de las clases de conjugación que particionan a X. Puesto que $x^G = \{x\}$ si y sólo si $x \in \mathbf{Z}(G)$, podemos escribir

$$|G| = |\mathbf{Z}(G)| + \sum [G : \mathbf{C}_G(x_i)],$$

donde el sumatorio de la derecha itera sobre representantes únicos x_i de todas las clases de conjugación con más de un elemento. Esta fórmula recibe el nombre de **ecuación de clases**, y es de gran importancia en la teoría de grupos finitos. Por ejemplo, con ella podemos probar un resultado que habíamos prometido.

Teorema 4.162 (Cauchy). *Si p es un número primo que divide al orden de un grupo finito G, entonces G tiene un elemento de orden p.*

Demostración: Esto ya lo sabíamos para grupos abelianos (teorema 4.134), así que supondremos que G no es abeliano y por tanto que no todo elemento de G está en $\mathbf{Z}(G)$. La demostración la daremos por inducción sobre n, donde $np = |G|$. Para $n = 1$ el teorema es cierto, pues en tal caso G es cíclico de acuerdo con el corolario 4.107. Supongamos ahora el teorema cierto para todo natural menor que n, y sea $x \in G$. Si $x \notin \mathbf{Z}(G)$ entonces x no conmuta con al menos un elemento de G y por ello $\left|\mathbf{C}_G(x)\right| < |G|$. Se sigue de esto y de la hipótesis de inducción que si p divide $\left|\mathbf{C}_G(x)\right|$ entonces $\mathbf{C}_G(x)$ tiene un elemento de orden p. Por otra parte, si p no divide al orden de $\mathbf{C}_G(x)$, entonces, como divide a $|G| = \left|\mathbf{C}_G(x)\right| [G : \mathbf{C}_G(x)]$, debe dividir a $G : \mathbf{C}_G(x)$. Así pues, si cada x_i es un representante de cada clase de conjugación con más de un elemento, la ecuación de clases

$$|G| = |\mathbf{Z}(G)| + \sum [G : \mathbf{C}_G(x_i)]$$

nos dice que $p \mid |\mathbf{Z}(G)|$, y como $\mathbf{Z}(G)$ es abeliano, éste contiene un elemento de orden p de acuerdo con el teorema 4.134. ∎

Definición 4.163. Sea p un número primo y G un grupo. Decimos que G es un **p-grupo** si todo elemento suyo es de orden una potencia de p.

El siguiente corolario nos da una caracterización alternativa de los p-grupos para grupos de orden finito.

Corolario 4.164. *Sea p un número primo y G un grupo de orden finito. Entonces G es un p-grupo si y sólo si su orden es potencia de p.*

Demostración: La suficiencia es consecuencia inmediata del teorema de Lagrange. Para establecer el recíproco, supongamos que todo elemento de G es de orden una potencia de p. Entonces ningún primo $q \neq p$ puede ser divisor del orden de G, pues de otro modo el teorema de Cauchy nos daría un elemento $x \in G$ de orden q, en contradicción con la hipótesis de que $|x| = p^m$ para cierto natural m. Se sigue de esto que el orden de G debe ser una potencia de p. ■

Teorema 4.165. *El centro de todo p-grupo finito es no trivial.*

Demostración: Si G es abeliano el teorema es trivialmente cierto, pues entonces $G = \mathbf{Z}(G)$. Supongamos pues que existe al menos un $x \notin \mathbf{Z}(G)$, y consideremos la ecuación de clases,

$$|G| = |\mathbf{Z}(G)| + \sum [G : \mathbf{C}_G(x_i)].$$

Puesto que $x_i \notin \mathbf{Z}(G)$, $\left|\mathbf{C}_G(x_i)\right| \leq |G|$, y como cada uno de estos centralizadores es también un p-grupo, sus índices son todos de la forma p^k para cierto entero $k > 0$, luego la ecuación de clases nos dice que p divide a $|\mathbf{Z}(G)|$, luego en particular $|\mathbf{Z}(G)| > 1$.■

Corolario 4.166. *Sea p un número primo. Entonces todo grupo de orden p^2 es abeliano.*

Demostración: Sea $|G| = p^2$. Entonces el centro de G es no trivial, y por tanto $|\mathbf{Z}(G)| = p$ o p^2, es decir, $|G/\mathbf{Z}(C)| = p$ o 1. En ambos casos $G/\mathbf{Z}(G)$ es cíclico, luego G es abeliano por la proposición 4.135. ■

Corolario 4.167. *Sea G un p-grupo finito. Si G es simple, entonces $|G| = p$.*

Demostración: Puesto que $\mathbf{Z}(G) \trianglelefteq G$ no es trivial, debe ser $\mathbf{Z}(G) = G$, o sea que G es abeliano, luego G es simple únicamente si no tiene subgrupos propios, lo que sólo puede ser si $|G| = p$. ■

EJERCICIOS

4.12. Sea G un grupo y A un subgrupo abeliano de G. Demostrar que G/A actúa en A mediante conjugación, y obtener un homomorfismo $G/A \to \mathrm{aut}(A)$.

Solución: Sea $gA \cdot a = gag^{-1}$ para cualesquiera $g \in G$ y $a \in A$. La operación dada por esta fórmula está bien definida, pues si $gA = hA$ entonces $g^{-1}h \in A$, lo que significa que $g^{-1}h$ conmuta con todo elemento de A, luego

$$(gag^{-1})(hah^{-1})^{-1} = ga(g^{-1}h)a^{-1}h^{-1} = gaa^{-1}(g^{-1}h)h^{-1} = 1,$$

de donde se sigue que $gag^{-1} = hah^{-1}$. Se verifica de inmediato que $A \cdot a = a$ y que $gA \cdot (hA \cdot a) = ghA \cdot a$, de modo que la operación que hemos definido es una acción de G/A en A. Si $f_g \in \mathrm{aut}(A)$,

con $f_g : a \mapsto gag^{-1}$, entonces $gA \cdot a = f_g(a)$ para todo $a \in A$, de manera que esta acción de G/A en A no es otra cosa que un homomorfismo $G/A \to \mathrm{aut}(A)$ que envía a cada gA con el automorfismo f_g de A.

4.13. Demostrar que si G contiene un elemento x con exactamente dos conjugados, entonces G contiene un grupo normal propio no trivial.

Solución: Por el teorema órbita-estabilizador (teorema 4.156), $2 = \left|x^G\right| = [G : \mathbf{C}_G(x)]$, luego $\mathbf{C}_G(x) \trianglelefteq G$, pues hemos visto en el ejemplo 4.121 que todo subgrupo de índice 2 es normal. Está claro que $\mathbf{C}_G(x)$ es un subgrupo propio de G, y es no trivial por que $x \neq 1$ y así $|G| \geq 3$.

Bibliografía

Enderton, H. B. (1977). *Elements of Set Theory*. Academic Press, London.

Gallian, J. (2016). *Contemporary Abstract Algebra*. Cengage Learning, Boston, MA, USA.

Halmos, P. R. (1960). *Naive Set Theory*. Van Nostrand, Amsterdam.

Hungerford, T. W. (2012). *Algebra*. Springer, New York, NY, USA.

Jacobson, N. (2012). *Basic Algebra I*. Second. Courier Corporation.

Jones, G. y J. Jones (2012). *Elementary Number Theory*. Springer, London, England, UK.

Lang, S. (2005). *Algebra*. Springer, New York, NY, USA.

Pinter, C. C. (1971). *Set Theory*. Addison-Wesley.

Rotman, J. J. (2002). *Advanced Modern Algebra*. Prentice Hall, Upper Saddle River, NJ, USA.

— (2012). *An Introduction to the Theory of Groups*. Springer, New York, NY, USA.

Stoll, R. R. (1961). *Set Theory and Logic*. W. H. Freeman and Company, New York.