Álgebra Básica

Equipo docente de la asignatura

31 de julio de 2020

Índice general

Capítulo 1

Conjuntos

1.1. Construcciones básicas

Comenzaremos dando una noción intuitiva de uno de los conceptos matemáticos más utilizados: el de conjunto. Sin embargo no daremos una definición rigurosa. ¿Sabes por qué?

Definición 1.1.1. Un **conjunto** es una colección de **elementos**. Normalmente están caracterizados por compartir alguna propiedad. Para que un conjunto esté bien definido debe ser posible discernir si un elemento arbitrario está o no en él.

Los conjuntos pueden definirse de manera **explícita**, citando todos los elementos de los que consta *entre llaves*,

$$A = \{1, 2, 3, 4, 5\},$$

o **implícita**, dando una o varias características que determinen si un elemento dado está o no en el conjunto,

$$A = \{\text{números naturales del 1 al 5}\}.$$

Advertencia 1.1.2. Los elementos de un conjunto *no están ordenados*, aunque vengan especificados como una lista, por tanto $A = \{3, 1, 2, 5, 4\}$. En una definición explícita *no se pueden repetir elementos*, así que $\{1, 1, 2, 3, 4, 5\}$ sería una manera incorrecta de expresar el conjunto A.

Ejemplo 1.1.3. (Conjuntos de números)

- $\mathbb{N}$, los números **naturales**: 1, 2, 3, …
- $\mathbb{N}_0$, los números naturales más el cero: 0, 1, 2, 3, …
- $\mathbb{Z}$, los números **enteros**: …, -2, -1, 0, 1, 2, …
- $\mathbb{Q}$, los números **racionales**: $\frac{p}{q}$.
- $\mathbb{R}$, los números **reales**.
- $\mathbb{C}$, los números **complejos**.

Definición 1.1.4. Dado un conjunto A, decimos que el elemento a **pertenece** a A, y lo denotamos $a \in A$, si a es un elemento del conjunto A.

Advertencia 1.1.5. Muchos símbolos matemáticos son **reversibles**, por ejemplo, $A \ni a$ significa lo mismo que $a \in A$. También muchos son **negables**, así $a \notin A$ significa que *a no* pertenece a A.

Por ejemplo, si $A = \{1, 2, 3, 4, 5\}$ entonces $1 \in A$ pero $6 \notin A$. Otra manera implícita de expresar este conjunto A es la siguiente:

$$A = \{n | n \in \mathbb{N} \wedge 1 \leq n \leq 5\}.$$

Se lee del siguiente modo: "A es el conjunto formado por los elementos n tales que n pertenece al conjunto los números naturales, n es mayor o igual que 1 y n es menor o igual que 5."

Definición 1.1.6. Dos conjuntos A y B son **iguales** $A = B$ cuando poseen los mismos elementos, es decir, cuando $x \in A \Leftrightarrow x \in B$.

Observación 1.1.7. Deducimos que dos conjuntos A y B son **distintos** $A \neq B$ si bien existe $x \in A$ tal que $x \notin B$ o bien existe $x \in B$ tal que $x \notin A$. En notación matemática: $A \neq B \Leftrightarrow (\exists x \in A | x \notin B) \vee (\exists x \in B | x \notin A)$.

Definición 1.1.8. El **conjunto vacío** $\emptyset$ es el que carece de elementos, es decir $\emptyset = \{\}$, o bien $\forall x, x \notin \emptyset$.
Un conjunto es **unitario** si contiene un único elemento, como por ejemplo $\{0\}$, $\{1\}$, $\{a\}$, {cartón de leche}, $\{\mathbb{N}\}$, ...

Advertencia 1.1.9. ¡Ojo! $x \in \{x\}$, pero $x \neq \{x\}$, de hecho, como demuestra la paradoja de Russell, es imposible que un conjunto pertenezca a sí mismo.

Definición 1.1.10. Dados dos conjuntos A y B, decimos que A está **contenido** en B o que A es un **subconjunto** de B, y lo denotamos $A \subset B$, si todo elemento de A pertenece a B, es decir $x \in A \Rightarrow x \in B$.

Advertencia 1.1.11. También se puede denotar $A \subset B$ como $A \subseteq B$. Hay que tener cuidado con la negación de estos dos símbolos. Tanto $A \not\subset B$ como $A \not\subseteq B$ significan que A no está contenido en B, o no es un subconjunto de B. Sin embargo $A \subsetneq B$ solo niega la igualdad, por lo que significa que A es un subconjunto de B pero que A no es igual a B, es decir, la contención es **estricta**. Por ejemplo, $\{2, 3, 5\} \subsetneq \{1, 2, 3, 4, 5\}$.

Observación 1.1.12. La contención es **transitiva**, $A \subset B \subset C \Rightarrow A \subset C$. También es **reflexiva**, $A \subset A$. Además, el vacío está contenido en cualquier conjunto $\emptyset \subset A$. Los subconjuntos de A distintos de $\emptyset$ y A se denominan **subconjuntos propios** de A.

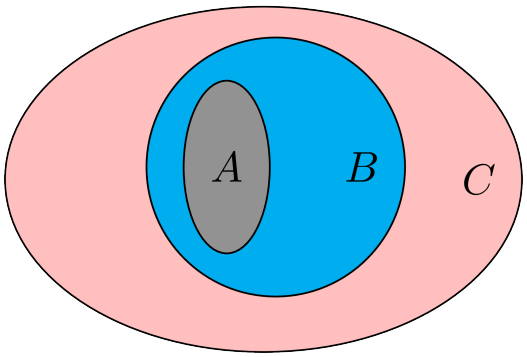

Figura 1.1: La contención es transitiva

El siguiente resultado caracteriza la igualdad entre dos conjuntos en términos de contenciones. Es la base de una técnica de prueba conocida como **doble inclusión**, que aplicaremos con frecuencia.

Proposición 1.1.13. $A = B \Leftrightarrow A \subset B$ *y* $A \supset B$.

Demostración. $A \subset B$ es lo mismo que $x \in A \Rightarrow x \in B$ y $A \supset B$ equivale a $x \in A \Leftarrow x \in B$, por tanto ambas simultáneamente significan $x \in A \Leftrightarrow x \in B$, que es lo mismo que $A = B$. □

Advertencia 1.1.14. Cualquier enunciado matemático debe venir seguido de una prueba. Se usan diversos términos para denominar a los enunciados matemáticos, de acuerdo con la percepción que tengamos de su importancia o dificultad. De mayor a menor:

- Teorema.
- Proposición.
- Lema.
- Corolario.

Los lemas suelen tener un carácter técnico y presentarse como pasos intermedios en la demostración de un resultado de mayor envergadura. Los corolarios se enuncian habitualmente después de un resultado más importante y su prueba suele ser obvia y omitirse.

Definición 1.1.15. Dados dos conjuntos A y B la **intersección** $A \cap B$ es el conjunto formado por aquellos elementos que pertenecen a ambos conjuntos, $A \cap B = \{x | x \in A \wedge x \in B\}$.

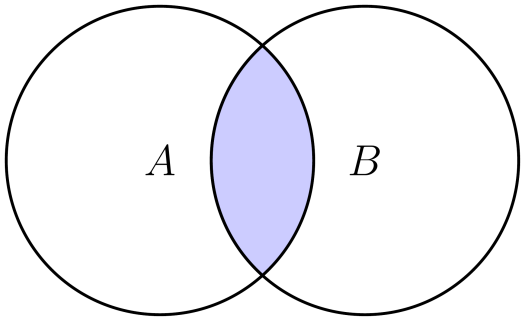

Figura 1.2: Intersección

Observación 1.1.16. Si $C \subset A$ y $C \subset B$ entonces $C \subset A \cap B$.

Teorema 1.1.17. *La intersección de conjuntos verifica las siguientes propiedades, donde A, B y C son conjuntos cualesquiera:*

- $A \cap B = B \cap A$ ***(conmutativa)***.
- $(A \cap B) \cap C = A \cap (B \cap C)$ ***(asociativa)***.
- $A \cap B \subset A$.
- $A \cap B \subset B$.
- $\emptyset \cap A = \emptyset$.
- $A \subset B \Leftrightarrow A \cap B = A$.

Demostración. Los elementos de $A \cap B$ son los que pertenecen a A y a B, que son los mismos que pertenecen a B y a A.

Las dos intersecciones triples son el mismo conjunto porque representan a los elementos que están en A, B y C.

Los elementos que están en A y en B están, en particular, en A. También en B.

La quinta igualdad la demostramos por doble inclusión. La inclusión $\supset$ es siem-

pre cierta y $\subset$ es consecuencia de un apartado anterior.

Demostremos la equivalencia del último apartado. Probemos primero $\Rightarrow$. Supongamos pues que $A \subset B$. Demostraremos la igualdad de la derecha por doble inclusión. La inclusión $\subset$ es siempre cierta. Veamos $\supset$. Como $A \subset B$, todo elemento de A está también en B, y por tanto en la intersección. Probemos ahora $\Leftarrow$. Esto es consecuencia de que $A \cap B \subset B$. □

Observación 1.1.18. Estas propiedades nos permiten definir inductivamente la **intersección** de una *cantidad finita* de conjuntos $A_1 \cap \cdots \cap A_n$. Consiste en los elementos que están en *todos* ellos.

Veamos el caso posiblemente infinito.

Definición 1.1.19. Dado un conjunto I, una **familia de conjuntos** indexada por I consiste en dar un conjunto A_i para cada $i \in I$. Se denota como $\{A_i\}_{i\in I}$.
La **intersección** de una familia de conjuntos se define como $\bigcap_{i\in I} A_i = \{x | \forall i \in I, x \in A_i\}$.

Si I es finito, esta definición coincide con la anterior, basta enumerar los elementos de I para comprobarlo. Esta definición es también válida para I infinito.

Ejemplo 1.1.20. (Una intersección infinita) Consideramos el conjunto de índices $I = \mathbb{N}$ y la familia de conjuntos $\{A_n\}_{n\in\mathbb{N}}$ dada por los intervalos $A_n = [0, \frac{1}{2^n})$. Todos estos intervalos contienen una cantidad infinita de números, pero su intersección es simplemente $\bigcap_{n\in\mathbb{N}} [0, \frac{1}{2^n}) = \{0\}$. En efecto, la inclusión $\supset$ es obvia porque $0 \in [0, \frac{1}{2^n})$ para todo $n \in \mathbb{N}$. Por otro lado, ningún número real positivo $x \in (0, \infty)$ puede pertenecer a la intersección ya que $x \notin [0, \frac{1}{2^n})$ para n suficientemente grande. Esto prueba $\subset$.

Definición 1.1.21. Dos conjuntos A y B son **disjuntos** si $A \cap B = \emptyset$.

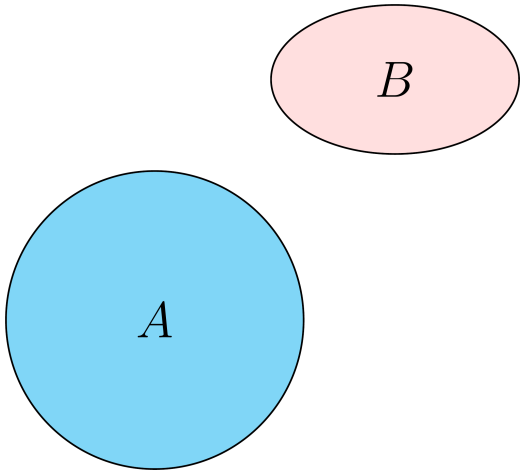

Figura 1.3: Disjuntos

Definición 1.1.22. Dados dos conjuntos A y B la **unión** $A \cup B$ es el conjunto formado por aquellos elementos que pertenecen al menos a uno de estos dos conjuntos, $A \cup B = \{x | x \in A \vee x \in B\}$.

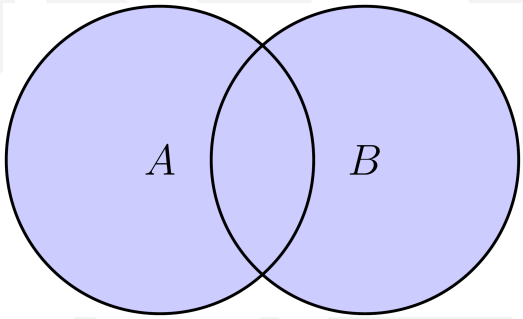

Figura 1.4: Unión

Observa que $A \cap B \subset A \cup B$.

Observación 1.1.23. Si $A \subset C$ y $B \subset C$ entonces $A \cup B \subset C$.

Teorema 1.1.24. *La unión de conjuntos verifica las siguientes propiedades, donde A, B y C son conjuntos cualesquiera:*

- $A \cup B = B \cup A$ ***(conmutativa)***.
- $(A \cup B) \cup C = A \cup (B \cup C)$ ***(asociativa)***.
- $\emptyset \cup A = A$ ***(elemento neutro)***.
- $A \subset A \cup B$.
- $B \subset A \cup B$.
- $A \subset B \Leftrightarrow B = A \cup B$.

Demostración. Los elementos de $A \cup B$ son los que pertenecen a A o a B, que son los mismos que pertenecen a B o a A.

Los dos uniones triples coinciden porque ambas representan el conjunto de elementos que pertenecen a A, a B o a C.

Como el vacío no tiene elementos, los elementos que pertenecen al vacío o a A son los que pertenecen a A.

Es obvio, por la propia definición, que tanto los elementos de A como los de B pertenecen a la unión.

Probemos la última equivalencia. Comenzamos demostrando $\Leftarrow$. Esto es una simple consecuencia de la inclusión $A \subset A \cup B$. Probemos ahora $\Rightarrow$. Supongamos pues que $A \subset B$. Tenemos que demostrar que $B = A \cup B$ y lo haremos por doble inclusión. La inclusión $\subset$ es cierta por el apartado anterior. Probemos la otra. Un elemento que está en A o en B ha de estar necesariamente en B ya que $A \subset B$. □

Observación 1.1.25. Estas propiedades nos permiten definir inductivamente la **unión** de una *cantidad finita* de conjuntos $A_1 \cup \cdots \cup A_n$. Consiste en los elementos que están en *alguno* de ellos.

Veamos ahora el caso posiblemente infinito.

Definición 1.1.26. La **unión** de una familia de conjuntos $\{A_i\}_{i \in I}$ se define como $\bigcup_{i \in I} A_i = \{x \mid \exists i \in I | x \in A_i\}$.

Igual que antes, si I es finito, esta definición coincide con la anterior, pero es también válida para I infinito.

Ejemplo 1.1.27. (Una unión infinita) Si consideramos la familia $\{[0, \frac{1}{2^n})\}_{n\in\mathbb{N}}$ del ejemplo de intersección infinita, tenemos que $\bigcup_{n\in\mathbb{N}}[0, \frac{1}{2^n}) = [0, \frac{1}{2})$ ya que $[0, \frac{1}{2})$ es uno de los conjuntos de esta familia y todos los demás $[0, \frac{1}{2^n})$ están contenidos en él.

Definición 1.1.28. Dados dos conjuntos A y B se define la **diferencia** $A\backslash B$, como el conjunto formado por los elementos de A que no están en B, $A\backslash B = \{x | x \in A \wedge x \notin B\}$.

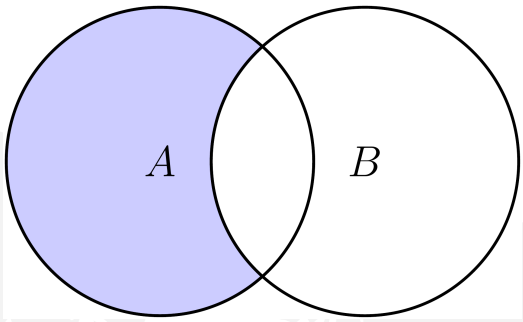

Figura 1.5: Diferencia

Advertencia 1.1.29. Observa que $A \setminus B \neq B \setminus A$. De hecho ambos conjuntos son disjuntos.

Definición 1.1.30. La **diferencia simétrica** $A\triangle B$ de dos conjuntos A y B se define como $A\triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

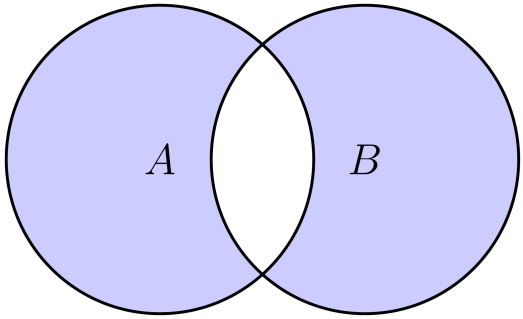

Figura 1.6: Diferencia simétrica

Teorema 1.1.31. (Leyes distributivas) *Dados tres conjuntos A, B y C:*

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Demostración. Probamos la primera por doble inclusión. La segunda la dejamos como ejercicio.

Comenzamos demostrando $\supset$. Sabemos que $A \cap B \subset A$ y $A \cap B \subset B \subset B \cup C$, por tanto $A \cap B \subset A \cap (B \cup C)$. También sabemos que $A \cap C \subset A$ y $A \cap C \subset C \subset B \cup C$, por tanto $A \cap C \subset A \cap (B \cup C)$. De aquí se deduce $\supset$.

Veamos ahora $\subset$. Dado $x \in A \cap (B \cup C)$ tenemos que $x \in A$ y $x \in B \cup C$. Por un lado, si $x \in B$ entonces $x \in A \cap B \subset (A \cap B) \cup (A \cap C)$. Por otro lado, si $x \in C$ entonces $x \in A \cap C \subset (A \cap B) \cup (A \cap C)$. De esto se sigue $\subset$. □

Los siguientes diagramas ilustran las leyes distributivas.

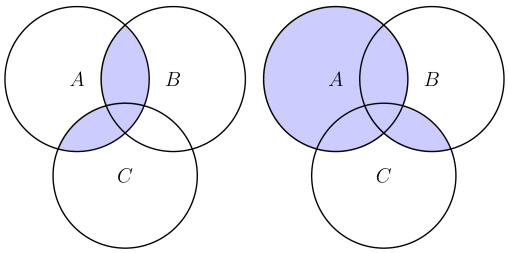

Figura 1.7: Leyes distributivas

Teorema 1.1.32. (Leyes de De Morgan) *Dados tres conjuntos A, B y C:*

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

Demostración. Probaremos la segunda ley de De Morgan por doble inclusión. La primera queda como ejercicio.

Comenzamos con $\supset$. Sea $x \in C \setminus A$. Tenemos entonces que $x \in C$ pero $x \notin A$, por tanto $x \notin A \cap B$ ya que $A \cap B \subset A$. Esto demuestra que $x \in C \setminus (A \cap B)$, por tanto $C \setminus A \subset C \setminus (A \cap B)$. Los papeles de A y B son intercambiables, así que también $C \setminus B \subset C \setminus (A \cap B)$. Esto demuestra $\supset$.

Para probar $\subset$, tomamos $x \in C \setminus (A \cap B)$. Esto quiere decir que $x \in C$ pero $x \notin A \cap B$. Esto último equivale a que bien $x \notin A$ o bien $x \notin B$. Si $x \notin A$ entonces $x \in C \setminus A$ y si $x \notin B$ entonces $x \in C \setminus B$. Por tanto $x \in (C \setminus A) \cup (C \setminus B)$. Esto prueba $\subset$. □

Las leyes de De Morgan quedan mejor explicadas por los siguientes diagramas.

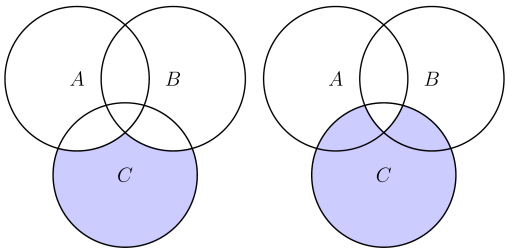

Figura 1.8: Leyes de De Morgan

Definición 1.1.33. El **producto cartesiano** de dos conjuntos A y B es el conjunto $A \times B$ cuyos elementos son los **pares ordenados** (a, b) cuya primera **coordenada** está en A, $a \in A$, y la segunda en B, $b \in B$, es decir $A \times B = \{(a, b) | a \in A \wedge b \in B\}$.

Ejemplo 1.1.34. (Un producto cartesiano) Si $A = \{1, 2, 3\}$ y $B = \{a, b\}$ entonces $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.

Observación 1.1.35. El vacío hace el papel de cero con respecto al producto cartesiano $A \times \emptyset = \emptyset = \emptyset \times B$.

Advertencia 1.1.36. En general, el producto cartesiano no es conmutativo $A \times B \neq B \times A$.

Ejercicio 1.1.37. Si A y B son finitos, ¿cuántos elementos tiene $A \times B$?

Observación 1.1.38. Análogamente, podemos definir el **producto cartesiano** de una cantidad finita de conjuntos $A_1 \times \cdots \times A_n$ como el formado por las **n-uplas** $(a_1, \ldots, a_n)$ tales que $a_i \in A_i$. Más generalmente, podemos definir el producto cartesiano de una familia arbitraria de conjuntos $\{A_i\}_{i\in I}$, $\prod_{i\in I} A_i = \{(a_i)_{i\in I} | a_i \in A_i\}$.

Ejemplo 1.1.39. (Un producto infinito) El producto infinito $\prod_{n\in\mathbb{N}} [0, \frac{1}{2^n})$ está formado por todas las sucesiones $(a_n)_{n\in\mathbb{N}}$ de números reales tales que $0 \leq a_n < \frac{1}{2^n}$ para todo $n \in \mathbb{N}$.

Definición 1.1.40. Dado un conjunto A, el **conjunto de las partes** de A es $\mathcal{P}(A) = \{\text{subconjuntos de } A\}$.

Observación 1.1.41. $B \subset A \Leftrightarrow B \in \mathcal{P}(A)$.

Ejemplo 1.1.42. (Las partes de $A = 1, 2, 3$) $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$.

Ejercicio 1.1.43. Si A es un conjunto con n elementos, ¿cuántos elementos tiene $\mathcal{P}(A)$? ¿Qué ocurre si A es infinito? ¿Es posible que $\mathcal{P}(A)$ sea vacío? ¿Y unitario?

Definición 1.1.44. En una situación concreta, un **conjunto universal** U es el que contiene a todos los posibles conjuntos del problema que tratamos.

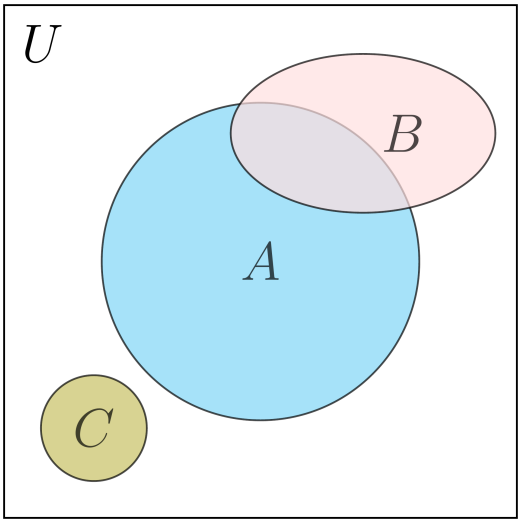

Figura 1.9: Conjunto universal

Definición 1.1.45. Fijado un conjunto universal U, el **complementario** de un conjunto A se denota $\bar{A}$ o A^c y se define como $\bar{A} = U \setminus A$.

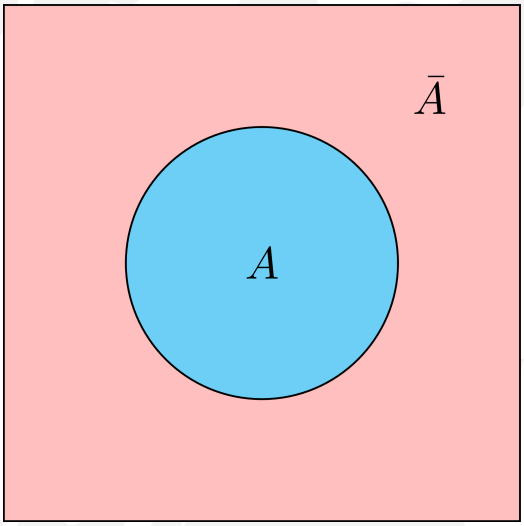

Figura 1.10: Complementario

Proposición 1.1.46. *Si tenemos fijado un conjunto universal U entonces $A \setminus B = A \cap \bar{B}$.*

Demostración. Como $A, B \subset U$,

$$\begin{aligned} A \setminus B &= \{x | x \in A \wedge x \notin B\} \\ &= \{x | x \in A \wedge (x \in U \wedge x \notin B)\} \\ &= \{x | x \in A \wedge x \in \bar{B}\} \\ &= A \cap \bar{B}. \end{aligned}$$

□

Proposición 1.1.47. *Dado un conjunto universal U:*

- $\bar{\bar{A}} = A$.
- $\bar{U} = \emptyset$.
- $\bar{\emptyset} = U$.

Demostración. Como $A \subset U$,

$$\begin{aligned} \bar{\bar{A}} &= U \setminus \bar{A} \\ &= \{x | x \in U \wedge x \notin \bar{A}\} \\ &= \{x | x \in U \wedge (x \notin U \vee x \in A)\} \\ &= \{x | x \in U \wedge x \in A\} \\ &= \{x | x \in A\} \\ &= A. \end{aligned}$$

Por otro lado,

$$\bar{U} = U \setminus U = \emptyset,$$

así que $U = \bar{\bar{U}} = \bar{\emptyset}$. □

1.2. Aplicaciones

Definición 1.2.1. Dados dos conjuntos A y B, una **aplicación** f de A en B, que se denota $f\colon A \to B$, es una regla que asocia a cada $a \in A$ un único elemento $f(a) \in B$, denominado **imagen** de a por f. También diremos

que $f(a)$ es el **valor** de f en a. Esto se denota también como $a \mapsto f(a)$, especialmente en diagramas como el siguiente,

$$\begin{array}{rcl} f\colon A & \longrightarrow & B, \\ a & \mapsto & f(a). \end{array}$$

También se puede colocar el nombre de la aplicación encima de la flecha,

$$A \xrightarrow{f} B.$$

El siguiente diagrama ilustra una aplicación

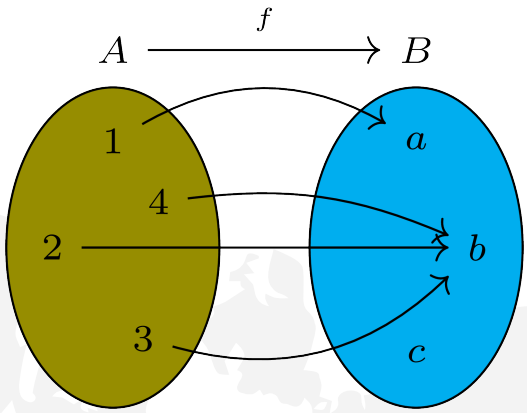

Figura 1.11: Aplicación

que se puede definir también del siguiente modo:

$$\begin{array}{rcl} A & \xrightarrow{f} & B, \\ 1 & \mapsto & a, \\ 2 & \mapsto & b, \\ 3 & \mapsto & b, \\ 4 & \mapsto & b. \end{array}$$

Sin embargo el diagrama siguiente no es una aplicación ya que la definición no se cumple por varias razones, ¿sabrías decir cuáles?

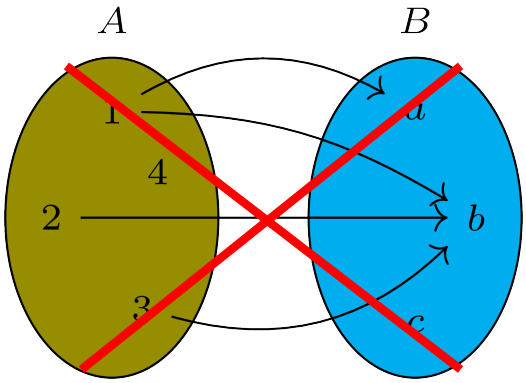

Figura 1.12: No aplicación

Advertencia 1.2.2. Para definir una aplicación hay que especificar lo siguiente:

- El conjunto de partida, también llamado **dominio**.
- El de llegada, o **codominio**.
- La imagen de cada elemento del conjunto de partida.

Si dos aplicaciones difieren en alguno de estos tres puntos se consideran diferentes.

Ejemplo 1.2.3. (Aplicaciones parecidas pero diferentes) La aplicación $f\colon \mathbb{N} \to \mathbb{N}$ definida como $f(n) = n$ es diferente de la aplicación $g\colon \mathbb{N} \to \mathbb{Z}$ definida como $g(n) = n$.

Ejemplo 1.2.4. (Algunas aplicaciones importantes)

- La **identidad** $1_A : A \to A$ se define como $1_A(a) = a$ para todo $a \in A$. Esta aplicación está definida para cualquier conjunto A.
- Dado un subconjunto $B \subset A$, la **inclusión** $i\colon B \to A$ se definie como $i(b) = b$ para todo $b \in B$.
- Dados dos conjuntos A y B y un elemento $b \in B$, la aplicación **constante** $c_b\colon A \to B$ se define como $c_b(a) = b$ para todo $a \in A$.

Ejercicio 1.2.5. Dado un conjunto A, ¿hay algun aplicación $\emptyset \to A$? ¿Y $A \to \emptyset$?.

Definición 1.2.6. Dadas dos aplicaciones

$$A \xrightarrow{f} B \xrightarrow{g} C$$

su **composición** $g \circ f \colon A \to C$ es la aplicación definida como $(g \circ f)(a) = g(f(a))$.

Proposición 1.2.7. *La composición de aplicaciones satisface las propiedades siguientes:*

- *Dadas tres aplicaciones*

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

se verifica que $h \circ (g \circ f) = (h \circ g) \circ f$ ***(asociativa)***.

- *Dada una aplicación* $f \colon A \to B$, *se tiene que* $f \circ 1_A = f = 1_B \circ f$ ***(elemento neutro)***.

Demostración. Las aplicaciones cuya igualdad se plantea tienen el mismo dominio y codominio, por tanto bastará comprobar que las imágenes de los elementos del dominio coinciden.

Dado $a \in A$, por un lado

$$\begin{aligned} (h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\ &= h(g(f(a)), \\ ((h \circ g) \circ f)(a) &= (h \circ g)(f(a)) \\ &= h(g(f(a)). \end{aligned}$$

Por otro lado

$$\begin{aligned} (f \circ 1_A)(a) &= f(1_A(a)) \\ &= f(a) \\ &= 1_B(f(a)) \\ &= (1_B \circ f)(a). \end{aligned}$$

□

Definición 1.2.8. Una aplicación $f\colon A \to B$ es **invertible** si existe $g\colon B \to A$ tal que $g \circ f = 1_A$ y $f \circ g = 1_B$,

$$1_A \circlearrowleft A \underset{g}{\overset{f}{\leftrightarrows}} B \circlearrowright 1_B$$

Proposición 1.2.9. *La aplicación g de la definición anterior, si existe, es única.*

Demostración. Si hubiera otra $g'\colon B \to A$ tal que $g' \circ f = 1_A$ y $f \circ g' = 1_B$, entonces

$$\begin{aligned} g &= g \circ 1_B \\ &= g \circ (f \circ g') \\ &= (g \circ f) \circ g' \\ &= 1_A \circ g' = g'. \end{aligned}$$

□

Definición 1.2.10. Si $f\colon A \to B$ es invertible su aplicación **inversa** $f^{-1}\colon B \to A$ es la única que satisface $f^{-1} \circ f = 1_A$ y $f \circ f^{-1} = 1_B$,

$$1_A \circlearrowleft A \underset{f^{-1}}{\overset{f}{\leftrightarrows}} B \circlearrowright 1_B$$

Observación 1.2.11. La identidad $1_A\colon A \to A$ es invertible y $1_A^{-1} = 1_A$. Si $f\colon A \to B$ es invertible entonces $f^{-1}\colon B \to A$ también y $(f^{-1})^{-1} = f$.

Proposición 1.2.12. *Si tenemos dos aplicaciones invertibles*

$$A \xrightarrow{f} B \xrightarrow{g} C$$

entonces $g \circ f$ es invertible y $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Demostración. Basta observar que

$$\begin{aligned} (g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ (f \circ f^{-1}) \circ g^{-1} \\ &= g \circ 1_B \circ g^{-1} \\ &= g \circ g^{-1} \\ &= 1_C, \end{aligned}$$

y que

$$\begin{aligned}(f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ g) \circ f \\ &= f^{-1} \circ 1_B \circ f \\ &= f^{-1} \circ f \\ &= 1_A.\end{aligned}$$

□

Nos disponemos a dar una caracterización más asequible de las aplicaciones invertibles.

Definición 1.2.13. Sea $f\colon A \to B$ una aplicación.

- f es **inyectiva** o **uno-a-uno** si no existen dos elementos diferentes de A con la misma imagen.
- f es **sobreyectiva** si todo elemento de B es la imagen de algún elemento de A.
- f es **biyectiva** si es inyectiva y sobreyectiva.

En una aplicación inyectiva no puede ocurrir los siguiente:

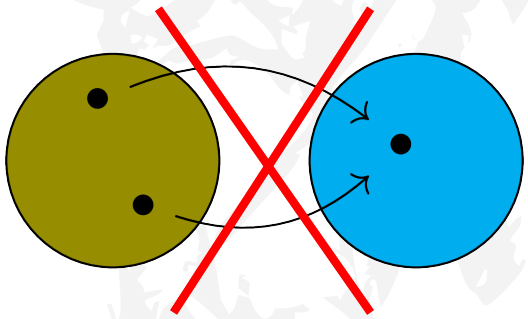

Figura 1.13: Aplicación no inyectiva

En una sobreyectiva está prohibida la siguiente situación:

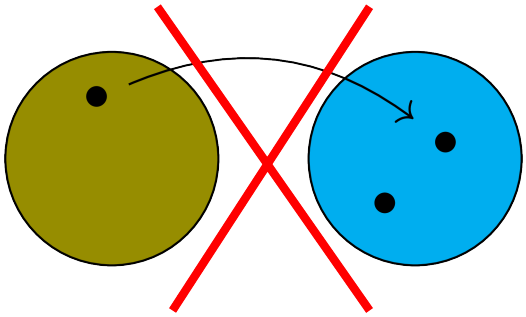

Figura 1.14: Aplicación no sobreyectiva

Observación 1.2.14. En notación matemática, $f\colon A \to B$ es **inyectiva** si, dados $a, a' \in A, f(a) = f(a') \Rightarrow a = a'$, y f es **sobreyectiva** si $\forall b \in B\ \exists a \in A | f(a) = b$. Las flechas de las aplicaciones inyectivas se denotan $f\colon A \hookrightarrow B$ y las de las sobreyectivas $f\colon A \twoheadrightarrow B$.

Advertencia 1.2.15. Es un error tristemente común el confundir la caracterización anterior de la inyectividad con la implicación $\Leftarrow$. En realidad esta impliciación es cierta para cualquier aplicación por la propia definición.

Lemma 1.2.16. *Una aplicación $f\colon A \to B$ es biyectiva $\Leftrightarrow \forall b \in B\ \exists! a \in A | f(a) = b$.*

Demostración. Veamos $\Rightarrow$. Supongamos pues que f es biyectiva. Si excluimos la condición de unicidad, el enunciado de la derecha es cierto por ser f sobreyectiva. La unicidad se deduce de ser f inyectiva, pues si existieran $a, a' \in A$ tales que $f(a) = b = f(a')$ entonces tendríamos que $a = a'$.

Veamos ahora $\Leftarrow$. Como ya hemos comentado, el enunciado de la derecha implicia la sobreyectividad de f ya que incluso la condición de unicidad no sería necesaria para esto. Para ver que f es inyectiva tomamos $a, a' \in A$ y suponemos que $f(a) = f(a')$. Tomando $b = f(a)$ tenemos que $f(a) = b$ y $f(a') = b$, así que por la unicidad $a = a'$, que es lo que teníamos que probar. □

Ejercicio 1.2.17. Si $f\colon A \to B$ es biyectiva y A es finito, ¿qué podemos decir de B? ¿Y si f es inyectiva? ¿Y si es sobreyectiva?

El siguiente tema versará en buena parte sobre el estudio de las aplicaciones biyectivas de un conjunto finito en sí mismo.

Teorema 1.2.18. *Una aplicación $f\colon A \to B$ es invertible $\Leftrightarrow$ es biyectiva.*

Demostración. Supongamos que f es invertible. Veamos que es sobreyectiva. Dado $b \in B$ tenemos que $f(f^{-1}(b)) = (f \circ f^{-1})(b) = 1_B(b) = b$, con lo que f es sobreyectiva. Si, dados $a, a' \in A$, $f(a) = f(a')$, entonces $f^{-1}(f(a)) = f^{-1}(f(a'))$. Como $f^{-1} \circ f = 1_A$ deducimos que $a = a'$, luego f es inyectiva.

Supongamos ahora que f es biyectiva. Definimos $g\colon B \to A$ del siguiente modo. Dado $b \in B$, definimos $g(b) \in A$ como el único elemento tal que $f(g(b)) = b$, que está bien definido por el lema anterior. Esto implica que $f \circ g = 1_B$. Veamos que $g \circ f = 1_A$. Ambas aplicaciones tienen a A como dominio y codominio, así que basta ver que toman los mismos valores, es decir que para todo $a \in A$, $(g \circ f)(a) = 1_A(a) = a$. Como f es inyectiva, esto equivale a probar que $f((g \circ f)(a)) = f(a)$. Tenemos también que $f((g \circ f)(a)) = (f \circ (g \circ f))(a)$. Usando la asociatividad de la composición y la identidad ya probada deducimos que en efecto

$$\begin{aligned} f \circ (g \circ f) &= (f \circ g) \circ f \\ &= 1_B \circ f \\ &= f. \end{aligned}$$

□

Observación 1.2.19. Las aplicaciones invertibles juegan en el ámbito de los conjuntos el mismo papel que las igualdades en el campo de los números, es por eso que se denotan

$$f\colon A \xrightarrow{\cong} B$$

o simplemente $f\colon A \cong B$. Por ejemplo, el producto cartesiano $A \times B$ no es conmutativo estrictamente hablando, pero hay una biyección

$$\begin{aligned} A \times B &\cong B \times A, \\ (a, b) &\mapsto (b, a). \end{aligned}$$

Decimos pues que el producto cartesiano es conmutativo *salvo biyección*. Lo mismo ocurre con la asociatividad del producto cartesiano,

$$\begin{aligned} (A \times B) \times C &\cong A \times (B \times C), \\ ((a, b), c) &\mapsto (a, (b, c)). \end{aligned}$$

Es más, ambos están en biyección con el producto triple, por ejemplo

$$\begin{array}{ccc}(A \times B) \times C & \cong & A \times B \times C, \\ ((a,b),c) & \mapsto & (a,b,c).\end{array}$$

Definición 1.2.20. Sea $f\colon A \to B$ una aplicación.

- La **imagen directa** de un subconjunto del dominio $U \subset A$ es el subconjunto del codominio $f(U) = \{b \in B \mid \exists a \in U | f(a) = b\} \subset B$.
- La **imagen inversa** de un subconjunto del codominio $V \subset B$ es subconjunto del dominio $f^{-1}(V) = \{a \in A | f(a) \in V\} \subset A$.

La **imagen** de la aplicación A se define como $\operatorname{im} f = f(A)$.

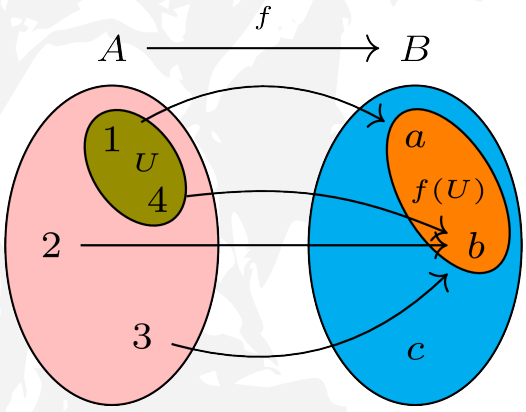

Figura 1.15: Imagen directa

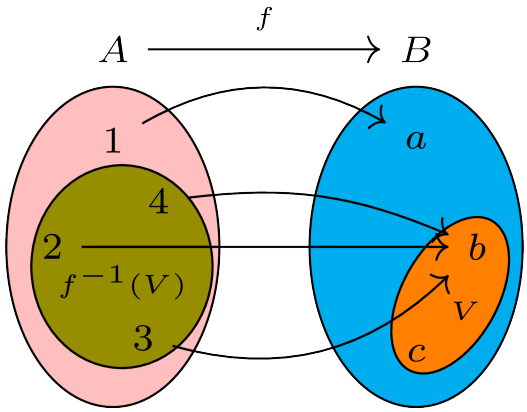

Figura 1.16: Imagen inversa

La imagen inversa recible otros nombres como **contraimagen**, **preimagen** o **anti-imagen**. La imagen directa también se denomina simplemente **imagen**.

Advertencia 1.2.21. Dada una aplicación $f\colon A \to B$, conviene no confundir la imagen de un elemento de A con la imagen directa de un subconjunto de A, aunque obviamente son conceptos relacionados, $f(\{a\}) = \{f(a)\}$.

Ejercicio 1.2.22. ¿Cuál es la imagen directa del subconjunto vacío? ¿Y su imagen inversa? ¿Dependen las respuestas a estas preguntas de quién sea $f\colon A \to B$?

Advertencia 1.2.23. La notación $f^{-1}(V)$ para la imagen inversa es confusa porque incorpora la notación usada para la inversa de la aplicación f, cuando esta existe. La imagen inversa está siempre definida, aun cuando f no es invertible y por tanto f^{-1} no existe. Si f es invertible, no hay ambigüedad ya que en este caso la imagen inversa $f^{-1}(V)$ de V a través de f coincide con la imagen directa de V a través de $f^{-1}\colon B \to A$. Para añadir aún más confusión, es habitual abusar de la terminología y denotar al subconjunto $f^{-1}(\{b\}) \subset A$ simplemente por $f^{-1}(b)$. El significado de esta expresión en cada caso se deducirá del contexto.

Observación 1.2.24.

- Una aplicación $f\colon A \to B$ es sobreyectiva si y solo si $\operatorname{im} f = f(A) = B$.
- Para toda aplicación $f\colon A \to B$, $f^{-1}(B) = A$.
- A partir de cualquier aplicación $f\colon A \to B$ podemos definir una sobreyectiva $\bar{f}\colon A \to \operatorname{im}(f)$ como $\bar{f}(a) = f(a)$. ¿En qué se diferencia

de la anterior?

- Las imágenes directa e inversa preservan inclusiones, es decir, dada una aplicación $f\colon A \to B$:
  - $U \subset U' \subset A \Rightarrow f(U) \subset f(U') \subset B$
  - $V \subset V' \subset B \Rightarrow f^{-1}(V) \subset f^{-1}(V') \subset A$.

¿Son ciertos los recíprocos de estas últimas implicaciones?

Proposición 1.2.25. *Dada una aplicación $f\colon A \to B$ y subconjuntos $U \subset A$ y $V \subset B$, se verifican las siguientes propiedades:*

- $U \subset f^{-1}(f(U))$.
- $f(f^{-1}(V)) \subset V$.

Demostración. Probaremos la segunda propiedad y dejaremos la primera como ejercicio. Dado $y \in f(f^{-1}(V))$ existe $x \in f^{-1}(V)$ tal que $y = f(x)$. Como $x \in f^{-1}(V), f(x) \in V$, así que $y \in V$. Esto es lo que había que demostrar. □

Proposición 1.2.26. *Dada una aplicación $f\colon A \to B$ y subconjuntos $U_1, U_2 \subset A$ y $V_1, V_2 \subset B$, se verifican las siguientes propiedades:*

1. $f(U_1 \cup U_2) = f(U_1) \cup f(U_2)$.
2. $f(U_1 \cap U_2) \subset f(U_1) \cap f(U_2)$.
3. $f^{-1}(V_1 \cup V_2) = f^{-1}(V_1) \cup f^{-1}(V_2)$.
4. $f^{-1}(V_1 \cap V_2) = f^{-1}(V_1) \cap f^{-1}(V_2)$.

Demostración. Vamos a probar 2 y 3. Los demás apartados son similares y quedan como ejercicio.

Dado $y \in f(U_1 \cap U_2)$ existe $x \in U_1 \cap U_2$ tal que $y = f(x)$. Como $x \in U_1$ y $x \in U_2$ deducimos que $y \in f(U_1)$ e $y \in f(U_2)$, por tanto $y \in f(U_1) \cap f(U_2)$.

Tenemos que $x \in f^{-1}(V_1 \cup V_2)$ si y solo si $f(x) \in V_1 \cup V_2$. Esto equivale a decir que $f(x) \in V_1$ o $f(x) \in V_2$, lo que es lo mismo, $x \in f^{-1}(V_1)$ o $x \in f^{-1}(V_2)$. Esto último es idéntico a afirmar que $x \in f^{-1}(V_1) \cup f^{-1}(V_2)$. □

Definición 1.2.27. La **restricción** de una aplicación $f\colon A \to B$ a un subconjunto $U \subset A$ es la aplicación $f|_U\colon U \to B$ definida como $f|_U(u) = f(u)$ para todo $u \in U$.

Ejercicio 1.2.28. ¿En qué se diferencian f y su restricción $f|_U$?

Definición 1.2.29. Dados dos conjuntos A y B, el **conjunto exponencial** es $B^A = \{\text{aplicaciones } A \to B\}$.

Ejemplo 1.2.30. (Un conjunto exponencial pequeño) El conjunto exponencial $\{a,b\}^{\{1,2\}} = \{f_1, f_2, f_3, f_4\}$ está formado por las cuatro aplicaciones siguientes:

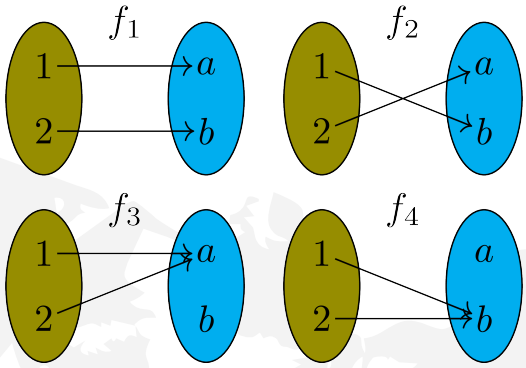

Figura 1.17: Conjunto exponencial

Ejercicio 1.2.31.

- Si A y B son finitos, ¿cuántos elementos tiene B^A?
- ¿Cuántos elementos hay en $A^\emptyset$?
- Dado un conjunto cualquiera A y otro unitario $\{e\}$, describe $A^{\{e\}}$ y $\{e\}^A$.

Definición 1.2.32. El **grafo** de una aplicación $f\colon A \to B$ es el conjunto

$$G_f = \{(a,b) \in A \times b | b = f(a)\} \subset A \times B$$

El grafo de la aplicación

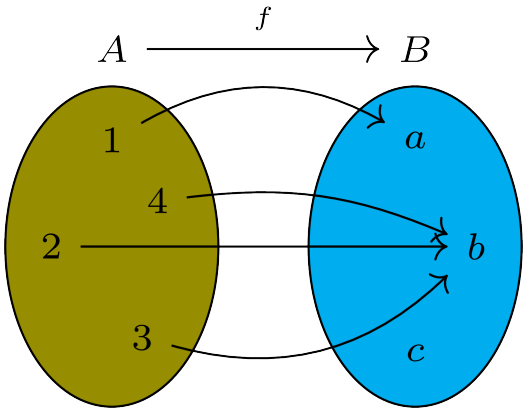

Figura 1.18: Aplicación

es el conjunto

$$G_f = \{(1,a),(4,b),(2,b),(3,b)\} \subset A \times B.$$

Observación 1.2.33. Las aplicaciones $f\colon A \to B$ se caracterizan porque para cada a está definido un único $f(a) \in B$. Por tanto un subconjunto $S \subset A \times B$ es el grafo de una aplicación f si para cada $a \in A$ existe un único $b \in B$ tal que $(a,b) \in S$. Este b sería $b = f(a)$.

1.3. Conjuntos cociente

Definición 1.3.1. Una **relación** R en un conjunto A es un subconjunto $R \subset A \times A$. Si $(a,b) \in R$ diremos que a **está relacionado con** b y lo denotaremos aRb, o simplemente $a \sim b$ cuando la relación R sea obvia por el contexto.
Una relación R es **de equivalencia** si satisface las siguientes propiedades:

- aRa para todo $a \in A$ (**reflexiva**).
- $aRb \Leftrightarrow bRa$ para $a,b \in A$ cualesquiera (**simétrica**).
- $aRb \wedge bRc \Rightarrow aRc$ para $a,b,c \in A$ (**transitiva**).

Ejemplo 1.3.2. (Relaciones de equivalencia)

- En el conjunto de los seres humanos, poseer el mismo grupo sanguíneo, es decir $x \sim y$ si x tiene el mismo grupo sanguíneo que y.
- En el conjunto de estudiantes del primer curso del Grado en Matemáticas de la Universidad de Sevilla, estar en el mismo grupo de Álgebra Básica.
- En $\mathbb{Z}$, tener la misma paridad, o equivalentemente $x \sim_2 y$ si $x - y$ es par.
- En $\mathbb{Z}$, dado $n \in \mathbb{Z}$, podemos definir la relación $\sim_n$ como $x \sim_n y$ si $x - y$ es divisible por n. Observa que $\sim_n = \sim_{-n}$.
- En un conjunto cualquiera A, la relación dada por la igualdad, $x \sim y$ si $x = y$.
- En un conjunto cualquiera A, la relación definida como $x \sim y$ para todo $x, y \in A$.

Ejercicio 1.3.3. Estudia si las siguientes relaciones en el conjunto de los seres humanos son de equivalencia:

- Ser hermano de. Es decir, $x \sim y$ si x es hermano de y.
- Ser hijo de.
- Ser la misma persona.
- Tener la misma edad.
- Llevarse menos de un año de edad.

Pon más ejemplos, definidos sobre los conjuntos que desees, de relaciones que satisfagan exactamente una o exactamente dos de las propiedades que se le demandan a las relaciones de equivalencia.

Definición 1.3.4. Dada una relación de equivalencia R en un conjunto A, la **clase (de equivalencia)** de $a \in A$ es el conjunto de los elementos relacionados con a, es decir $R(a) = \{b \in A | aRb\}$. Los elementos de $R(a)$ se denominan **representantes** de esta clase. El conjunto **cociente** de A por R es el formado por las clases de equivalencia de los elementos de A. La

proyección canónica es la aplicación sobreyectiva $\pi : A \twoheadrightarrow A/R$ definida como $a \mapsto R(a)$.

Observación 1.3.5. Cuando la relación de equivalencia se denota simplemente $\sim$ por ser sobreentendida, la clase de un elemento $a \in A$ se denota simplemente como $[a]$ o $\bar{a}$. Observa que, en virtud de la reflexividad, $a \in R(a)$ en cualquier relación de equivalencia.

Advertencia 1.3.6. En las relaciones de equivalencia, y por tanto en los cocientes, el problema que más confusión genera es que una misma clase de equivalencia puede tener muchos representantes diferentes. Esto dificulta la definición de aplicaciones que parten de cocientes $f: A/R \to B$, ya que si quiero definir $f(R(a))$ basándome en la elección de un representante, por ejemplo $a \in R(a)$, debo comprobar que la definición es independiente de cualquier otra elección posible del representante $b \in R(a)$.

Ejemplo 1.3.7. (Conjuntos cociente) Aquí identificamos los conjuntos cociente del ejemplo de arriba, en algunos casos estableciendo una biyección con otro conjunto más sencillo.

- $\{\text{Seres humanos}\}/\text{poseer el mismo grupo sanguíneo} \cong \{0, A, B, AB\}: [x] \mapsto$ grupo sanguíneo de cualquier representante.
- $\{\text{Estudiantes de primero de Matemáticas}\}/\text{estar en el mismo grupo de Álgebra Básica} \cong \{A, B, C, D, E, F\}: [x] \mapsto$ grupo al que pertenece un representante cualquiera.
- $\mathbb{Z}/\sim_2 = \{[0], [1]\}$.
- $\mathbb{Z}/\sim_n = \{[0], \dots, [n-1]\}$ si $n > 0$.
- En este caso la proyección natural es biyectiva $\pi : A \cong A/=$.
- $A/\sim$ es unitario.

Definición 1.3.8. Una **partición** de A es un subconjunto $P \subset \mathcal{P}(A)$ tal que:

- Los elementos de P son subconjuntos no vacíos de A.
- La unión de todos los elementos de P es A.
- Dos elementos distintos de P son siempre disjuntos.

La siguiente es una partición de un conjunto A formada por los subconjuntos $\{E_1, E_2, E_3, E_4, E_5\}$.

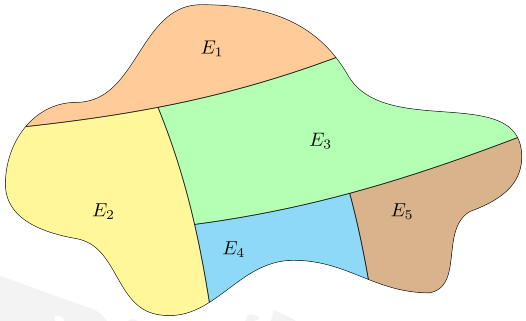

Figura 1.19: Partición

Proposición 1.3.9. *Si R una relación de equivalencia en un conjunto A, $aRb \Leftrightarrow R(a) = R(b)$.*

Demostración. $\Leftarrow$ En este caso aRb pues $a \in R(b)$.

$\Rightarrow$ Probemos $\subset$. Si $c \in R(a)$ es porque cRa. Como aRb, por la transitividad tenemos que cRb, así que $c \in R(b)$. La inclusión $\supset$ también es cierta porque, por la simetría, los papeles de a y b son intercambiables en el argumento anterior. □

Teorema 1.3.10. *Si R es una relación de equivalencia en A, entonces A/R es una partición de A. Es más, toda partición de A proviene de una relación de equivalencia.*

Demostración. Las clases que forman A/R no son vacías porque todas poseen algún representante. La unión de todas las clases es A, porque todo $a \in A$ pertenece a una clase, a la suya propia, $a \in R(a)$. Supongamos que dos clases $R(a)$ y $R(b)$ no

fueran disjuntas. Entonces existe $c \in R(a) \cap R(b)$. Esto significa que cRa y cRb. Por la simetría y la transitividad, aRb, luego por la proposición anterior $R(a) = R(b)$.

Si tenemos una partición P de A, podemos definir la relación de equivalencia $a \sim_P b$ si a y b pertenecen al mismo elemento de la partición. Es obvio que esta relación es simétrica. Es reflexiva porque, en virtud de la segunda propiedad de las particiones, todo elemento de A pertenece a alguno de P. Veamos la transitividad. Si $a \sim_P b \sim_P c$ entonces existen $U, V \in P$ tales que $a, b \in U$ y $b, c \in V$. Como $b \in U \cap V$ la tercera propiedad de las particiones nos asegura que $U = V$, así que $a \sim_P c$. Esta relación de equivalencia satisface $A/\sim_P = P$ por su propia definición, ya que el vacío no está en P. □

1.4. Factorización canónica de una aplicación

Teorema 1.4.1. (Propiedad universal de la proyección canónica) *Si $f\colon A \to B$ es una aplicación y R es una relación de equivalencia en A tal que $\$ a\ R\ b\ f(a) = f(b) \$$, entonces existe una única aplicación $\bar{f}\colon A/R \to B$ tal que $f = \bar{f} \circ \pi$,*

$$f\colon A \xrightarrow{\pi} A/R \xrightarrow{\bar{f}} B.$$

Demostración. Vamos a suponer que $\bar{f}$ existe y cumple las propiedades indicadas. De ahí deduciremos una fórmula forzosa para $\bar{f}$, con lo cual de existir será única. Luego veremos que la fórmula tiene sentido, luego $\bar{f}$ existirá.

Si $f = \bar{f} \circ \pi$ entonces dado $a \in A$,

$$\begin{aligned} f(a) &= (\bar{f} \circ \pi)(a) \\ &= \bar{f}(\pi(a)) \\ &= \bar{f}(R(a)). \end{aligned}$$

Definimos pues $\bar{f}$ mediante la fórmula $\bar{f}(R(a)) = f(a)$. Veamos que $\bar{f}$ está bien definida así. Para ello hemos de comprobar que si $R(a) = R(b)$ entonces $f(a) = f(b)$. Esto se deduce de la hipótesis ya que $R(a) = R(b)$ si y solo si aRb. □

Definición 1.4.2. Dada una aplicación $f\colon A \to B$, podemos definir relación de equivalencia $\sim_f$ en A asociada a f como $a \sim_f b$ si $f(a) = f(b)$.

Ejercicio 1.4.3. Prueba que $\sim_f$ es en efecto una relación de equivalencia. Describe el conjunto cociente y la partición asociada. Demuestra también que si R es una relación de equivalencia en A y $\pi : A \to A/R$ es la proyección natural entonces $\sim_\pi = R$.

Teorema 1.4.4. (Factorización canónica) *Dada una aplicación $f\colon A \to B$, existe una única aplicación $\bar{f}\colon A/\sim_f \to \operatorname{im} f$ tal que el siguiente diagrama es conmutativo*

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ A/\sim_f & \xrightarrow[\quad \bar{f} \quad]{} & \operatorname{im} f \end{array}$$

Figura 1.20: Factorización canónica

es decir, $f = i \circ \bar{f} \circ \pi$. Aquí π es la proyección canónica e i es la inclusión. Además, la aplicación $\bar{f}$ es biyectiva.

Demostración. Hemos visto con anterioridad que podemos definir una aplicación sobreyectiva $f' : A \twoheadrightarrow \operatorname{im} f$ como $f'(a) = f(a)$. Está claro que $f = i \circ f'$ ya que ambas posee el mismo dominio y codominio e $(i \circ f)(a) = i(f(a)) = f(a)$ para todo $a \in A$. Es más, como f y f' toman los mismos valores, $\sim_f = \sim_{f'}$.

El teorema anterior se puede aplicar a $f' : A \to \operatorname{im} f$ y a $\sim_f$. Esto da lugar a una aplicación $\bar{f}\colon A/\sim_f \to \operatorname{im} f$ que satisface $f' = \bar{f} \circ \pi$, así que $f = i \circ f' = i \circ (\bar{f} \circ \pi)$. La aplicación $\bar{f}$ es la única que se descompone de este modo, ya que la propia

descomposición fuerza una fórmula para su definición. En efecto, dado $a \in A$,

$$\begin{aligned} f(a) &= (i \circ \bar{f} \circ \pi)(a) \\ &= i(\bar{f}(\pi(a))) \\ &= i(\bar{f}([a])) \\ &= \bar{f}([a]). \end{aligned}$$

Veamos que $\bar{f}$ es biyectiva. Comenzamos por la sobreyectividad. Dado $b \in \operatorname{im} f$, como f' es sobreyectiva, existe $a \in A$ tal que $b = f(a) = \bar{f}([a])$. Esto prueba que $\bar{f}$ es sobreyectiva. Comprobemos ahora la inyectividad. Dados $[a], [b] \in A/\sim_f$, usando la anterior fórmula para $\bar{f}$ vemos que $\bar{f}([a]) = \bar{f}([b])$ si y solo si $f(a) = f(b)$, lo cual equivale a que $a \sim_f b$, que es lo mismo que decir $[a] = [b]$. Esto concluye la prueba. □

Este teorema nos proporciona un método muy eficiente para establecen una biyección de un conjunto cociente en otro.

Ejemplo 1.4.5. ($\mathbb{Z}$ módulo n) Vamos a dar una demostración rigurosa de que $\mathbb{Z}/\sim_n$ posee n elementos para $n > 0$. Para ello definimos la aplicación $f\colon \mathbb{Z} \to \mathbb{Z}$ tal que $f(m)$ es el resto no negativo de dividir m entre n.

La imagen de f es $\operatorname{im} f = \{0, \dots, n-1\}$. En efecto, el resto de la división es ≥ 0 y $< n$, lo cual demuestra $\subset$. Además, para $0 \leq m < n$, el cociente de la división es 0 y el resto es el propio m, por tanto también tenemos $\subset$.

Veamos ahora que $\sim_f = \sim_n$. Sean $m, m' \in \mathbb{Z}$. Dividimos ambos números entre n, $m = c \cdot n + f(m)$ y $m' = c' \cdot n + f(m')$. Tenemos que $m - m' = (c - c') \cdot n + (f(m) - f(m'))$ es también una división, porque $|f(m) - f(m')| < n$. Por tanto $f(m) = f(m')$ si y solo si $m - m'$ es divisible por n. Esto demuestra que ambas relaciones coinciden.

Aplicando el teorema de factorización, deducimos que hay una biyección $\bar{f}\colon \mathbb{Z}/\sim_n \cong \{0, \dots, n-1\}$ definida por $\bar{f}([m]) = f(m)$.

Capítulo 2

Grupos

2.1. Definiciones básicas

Definición 2.1.1. Un **grupo** es un par $(G, \star)$, donde G es un conjunto y $\star$ es una **operación binaria** en G, es decir una aplicación

$$\begin{array}{ccc} G \times G & \xrightarrow{\star} & G, \\ (x, y) & \mapsto & x \star y, \end{array}$$

que ha de satisfacer las propiedades siguentes:

- $(x \star y) \star z = x \star (y \star z)$ para todo $x, y, z \in G$ (**asociativa**).
- Existe un elemento $e \in G$ tal que $x \star e = x = e \star x$ para todo $x \in G$ (**elemento neutro**).
- Para todo $x \in G$ existe $x^{-1} \in G$ tal que $x \star x^{-1} = e = x^{-1} \star x$ (elemento **simétrico** o **inverso**).

Cuando la operación $\star$ se sobreentienda por el contexto, el grupo $(G, \star)$ se denotará simplemente G. En este caso también es frecuente sustituir el símbolo $\star$ por una mera yuxtaposición de símbolos, es decir $x \star y = xy$.

Ejemplo 2.1.2. (Ejemplos de grupos) Los siguientes son algunos grupos bien conocidos:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son grupos con la operación suma $+$. En este caso el elemento

neutro es el **cero** 0. El simétrico de un elemento x es su **opuesto** $-x$. Esta notación se denomina **aditiva** frente a la usada en la definición de grupo, que es la **multiplicativa**.

- $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ y $\mathbb{C} \setminus \{0\}$ son grupos con la multiplicación. ¿Cuál es el elemento neutro?
- El conjunto $\{1, -1\}$ con el producto.
- El conjunto $\{1, -1, i, -i\}$ con el producto.
- El conjunto $GL(n, k)$ de las matrices $n \times n$ con entradas en un cuerpo k y determinante no nulo, con la multiplicación de matrices.
- El **grupo trivial** $\{e\}$, con el producto definido como $e \star e = e$, que es el único posible.

Proposición 2.1.3. *El elemento neutro de un grupo $(G, \star)$ es único.*

Demostración. Si e y e' son elementos neutros de $(G, \star)$, entonces se tiene:

$$e = e \star e' = e',$$

donde la primera igualdad es cierta por ser e' un elemento neutro, y la segunda por serlo e. □

Proposición 2.1.4. *El simétrico de un elemento de un grupo $x \in G$ es único.*

Demostración. Sea $x \in G$, y sean y, z elementos simétricos de x, es decir, que satisfacen

$$\begin{aligned} x \star y &= e = y \star x, \\ x \star z &= e = z \star x. \end{aligned}$$

Entonces,

$$\begin{aligned} y &= y \star e \\ &= y \star (x \star z) \\ &= (y \star x) \star z \\ &= e \star z \\ &= z. \end{aligned}$$

□

Gracias al resultado anterior, podemos denotar x^{-1} al simétrico de x sin ambigüedad, o $-x$ si estamos usando notación aditiva. Cuando estudiamos los conjuntos demostramos un resultado análogo para aplicaciones biyectivas. Observa que $e^{-1} = e$.

Proposición 2.1.5. *Si $x, y \in G$ son elementos de un grupo tales que $x \star y = e$, entonces $y = x^{-1}$ y $x = y^{-1}$.*

Demostración. A partir de $x \star y = e$,

$$\begin{aligned} y &= e \star y \\ &= x^{-1} \star x \star y \\ &= x^{-1} \star e \\ &= x^{-1}. \end{aligned}$$

Análogamente,

$$\begin{aligned} x &= x \star e \\ &= x \star y \star y^{-1} \\ &= e \star y^{-1} \\ &= y^{-1}. \end{aligned}$$

□

Advertencia 2.1.6. ¡Ojo! El resultado análogo a la proposición anterior para aplicaciones es falso. Es posible encontrar aplicaciones $f\colon X \to Y$ y $g\colon Y \to X$ que no son biyectivas tales que $g \circ f = 1_X$ pero $f \circ g \neq 1_Y$. En cambio, si f o g es biyectiva y $g \circ f = 1_X$ es fácil probar que ambas son biyectivas, $f = g^{-1}$ y $g = f^{-1}$.

Corolario 2.1.7. *Todo elemento de un grupo $x \in G$ satisface $(x^{-1})^{-1} = x$.*

Demostración. Basta usar que $x \star x^{-1} = e$. □

Proposición 2.1.8. *Dados dos elementos $x, y \in G$ en un grupo, $(x \star y)^{-1} = y^{-1} \star x^{-1}$.*

Demostración. Basta comprobar que

$$\begin{aligned} (x \star y) \star (y^{-1} \star x^{-1}) &= x \star (y \star y^{-1}) \star x^{-1} \\ &= x \star e \star x^{-1} \\ &= x \star x^{-1} \\ &= e. \end{aligned}$$

□

También hemos probado con anterioridad una versión de la proposición anterior para aplicaciones biyectivas.

Los grupos poseen las siguientes **propiedades cancelativas** a izquierda y derecha.

Proposición 2.1.9. *Dados tres elementos de un grupo $x, y, z \in G$:*

- *Si $x \star y = x \star z$ entonces $y = z$.*
- *Si $y \star x = z \star x$ entonces $y = z$.*

Demostración. Si $x \star y = x \star z$ entonces

$$\begin{aligned} y &= x^{-1} \star (x \star y) \\ &= x^{-1} \star (x \star z) \\ &= z. \end{aligned}$$

La otra propiedad se prueba de manera análoga. □

Las **potencias** positivas de un elemento de un grupo $x \in G$ se definen como

$$x^n = x \star \overset{n}{\cdots} \star x, \quad n > 0.$$

Definimos además $x^0 = e$ y $x^n = (x^{-n})^{-1}$ si $n < 0$. Así definidas, las potencias satisfacen $x^m x^n = x^{m+n}$ y $(x^m)^n = x^{mn}$ para $m, n \in \mathbb{Z}$ cualesquiera. Además $x^1 = x$ y x^{-1} su inverso.

Definición 2.1.10. Diremos que un elemento de un grupo $x \in G$ tiene **orden finito** si existe un entero positivo $n > 0$ tal que $x^n = e$. En este caso, el **orden** de x, que denotaremos $o(x)$, es el menor entero positivo que cumple esta propiedad. Si $x \in G$ no tiene orden finito, diremos que tiene **orden infinito**.

Ejemplo 2.1.11. (Elementos de orden finito)

- En cualquier grupo, el elemento neutro es el único que tiene orden 1.
- En el grupo $\{1, -1, i, -i\}$ con el producto, el orden de -1 es 2, mientras que el orden de i y de $-i$ es 4.

- En $GL(n, \mathbb{Q})$, la siguiente matriz tiene orden n,

$$\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \end{pmatrix} = \left(\begin{array}{c|c} 0 & 1 \\ \hline I_{n-1} & 0 \end{array}\right).$$

Observación 2.1.12. Cuando el grupo está expresado con la notación aditiva, la notación exponencial se cambia por una multiplicativa, es decir,

$$n \cdot x = x + \overset{n}{\cdots} + x, \quad n > 0.$$

Definimos además $0 \cdot x = 0$ y $n \cdot x = -(-n) \cdot x$ si $n < 0$. De este modo, se satisface $m \cdot x + n \cdot x = (m + n) \cdot x$ y $n \cdot (m \cdot x) = (n \cdot m) \cdot x$ para todo $m, n \in \mathbb{Z}$. Además $1 \cdot x = x$ y $(-1) \cdot x = -x$.
Por tanto, en un grupo aditivo $x \in G$ tiene orden finito si $n \cdot x = 0$ para cierto $n > 0$ y el orden $o(x)$ es el mínimo.

Proposición 2.1.13. *Un elemento de un grupo $x \in G$ tiene orden infinito si y solo si todas sus potencias x^k con $k \in \mathbb{Z}$ son distintas.*

Demostración. En lugar de demostrar $A \Leftrightarrow B$ probaremos NO $A \Leftrightarrow$ NO B.
$\Rightarrow$ Si x es de orden $n > 0$ entonces $x^n = e = x^0$.
$\Leftarrow$ Si x tiene dos potencias iguales, digamos $x^r = x^s$ con $r > s$, entonces

$$\begin{aligned} x^{r-s} &= x^r \star x^{-s} \\ &= x^s \star x^{-s} \\ &= x^0 \\ &= e. \end{aligned}$$

Como $r - s > 0$, esto prueba que x tiene orden finito. □

Corolario 2.1.14. *Si G es un grupo finito, todo elemento tiene orden finito.*

Proposición 2.1.15. *Si $x \in G$ es un elemento de orden $o(x) = m$ en un grupo G, $x^n = e$ si y solo si m divide a n.*

Demostración. $\Leftarrow$ Si m divide a n entonces $n = m \cdot k$ para cierto entero k, así que

$$\begin{aligned} x^n &= x^{m \cdot k} \\ &= (x^m)^k \\ &= e^k \\ &= e. \end{aligned}$$

$\Rightarrow$ Si $n = 0$ el resultado se tiene porque todo entero divide al 0. Si no, podemos suponer que n es positivo ya que el signo no afecta a la divisibilidad y además, si n fuera negativo, $x^{-n} = (x^n)^{-1} = e^{-1} = e$.

Por definición de orden $n \geq m$. Sean c y r el cociente y el resto de la división de n por m, $n = m \cdot c + r$. El resto satisface $0 \leq r < m$. Basta probar que $r = 0$. Por reducción al absurdo, si $r > 0$ entonces

$$\begin{aligned} x^r &= x^{n-m\cdot c} \\ &= x^n \star (x^m)^{-c} \\ &= e \star e^{-c} \\ &= e. \end{aligned}$$

Como $0 < r < m$, esto contradice $o(x) = m$. □

Proposición 2.1.16. *Un elemento de un grupo $x \in G$ tiene orden finito si y solo si x^{-1} también. En este caso $o(x) = o(x^{-1})$.*

Demostración. Si $o(x) = n$ entonces

$$\begin{aligned} (x^{-1})^n &= x^{-n} \\ &= (x^n)^{-1} \\ &= e^{-1} \\ &= e. \end{aligned}$$

Por tanto x^{-1} es de orden finito y además $o(x^{-1}) \leq o(x)$.

Usando que $(x^{-1})^{-1} = x$, deducimos que $o(x) = o((x^{-1})^{-1}) \leq o(x^{-1})$, con lo que se tiene la igualdad, y también la otra implicación. □

Definición 2.1.17. Un grupo $(G, \star)$ es **conmutativo** o **abeliano** si $x \star y = y \star x$ para todo $x, y \in G$.

Ejemplo 2.1.18. (Grupo producto) Dados dos grupos $(G, \star)$ y $(H, *)$, el **producto cartesiano** $G \times H$ es un grupo con la siguiente operación binaria:

$$(g_1, h_1)(g_2, h_2) = (g_1 \star g_2, h_1 * h_2).$$

El elemento neutro para el producto es (e_G, e_H), es decir, el elemento neutro de cada grupo en cada una de las coordenadas.

2.2. El grupo simétrico

Definición 2.2.1. Dado un conjunto X, una **permutación** de X es una aplicación biyectiva $\sigma : X \to X$.

Proposición 2.2.2. *El conjunto* $\mathrm{Sim}(X)$ *de todas las permutaciones de un conjunto* X *es un grupo para la composición de aplicaciones, denominado* ***grupo simétrico****.*

Demostración. Basta recordar que la composición de aplicaciones biyectivas es biyectiva. El elemento neutro es 1_X. La existencia de inversas se probó también en el capítulo de conjuntos. □

Observación 2.2.3. El **grupo simétrico de** n **elementos** S_n es el grupo simétrico del conjunto $\{1, 2, \cdots, n\}$. Este grupo posee $n!$ elementos. Una manera concisa de representar una permutación de este conjunto es a través de una matriz con dos filas ($n = 5$):

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

En la primera aparecen los números del 1 al n. En la segunda fila, debajo de cada i aparece $\sigma(i)$. En el ejemplo anterior $\sigma(1) = 1$, $\sigma(2) = 5$, $\sigma(3) = 4$, etc.

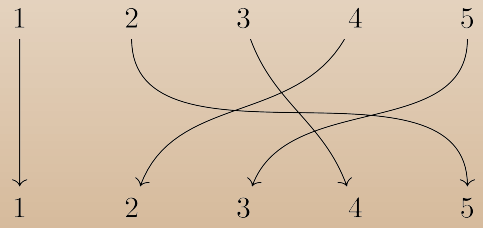

Figura 2.1: Permutación

El orden de las columnas no importa, es decir, la siguiente matriz denota la misma permutación que la anterior

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

si bien lo más común es que los números de la primera fila aparezcan ordenados, como en el primer caso.
La permutación identidad es la que tiene ambas fila iguales

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

La permutación inversa se obtiene simplemente al intercambiar las filas

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & 5 & 4 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}. \end{aligned}$$

Ejemplo 2.2.4. (Composición de permutaciones) La composición de permutaciones se puede realizar de manera gráfica del siguiente modo,

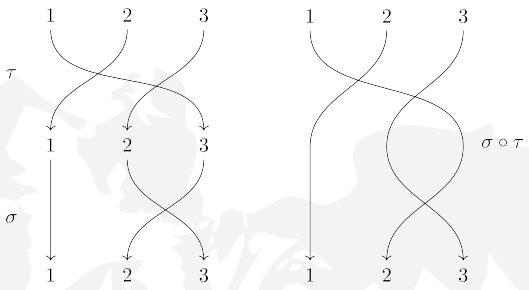

Figura 2.2: Composición

Con la notación matricial, la composición en S_n se puede llevar a cabo como en el siguiente ejemplo. Consideramos

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3.$$

Para calcular $\sigma \circ \tau$ reordenamos las columnas de σ de modo que su primera fila coincida con la segunda de τ:

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

La matriz de $\sigma \circ \tau$ consiste en la primera fila de τ seguida de la segunda de la última representación de σ,

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

Calculamos ahora $\tau \circ \sigma$,

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

y entonces

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

Observa que $\tau \circ \sigma \neq \sigma \circ \tau$. Esto demuestra que la composición de permutaciones no es conmutativa en general.

Este ejemplo se puede generalizar para demostrar que si X tiene al menos tres elementos el grupo $\mathrm{Sim}(X)$ no es abeliano.

2.3. Ciclos y trasposiciones

Definición 2.3.1. Dado un conjunto X el **soporte** de una permutación $\sigma : X \to X$ es el subconjunto

$$\mathrm{sop}(\sigma) = \{x \in X \mid \sigma(x) \neq x\}.$$

Decimos que $\sigma \in \mathrm{Sim}(X)$ es un **ciclo** de **longitud** n, o un n**-ciclo**, si su soporte es un conjunto finito de n elementos

$$\mathrm{sop}(\sigma) = \{x_1, x_2, \dots, x_n\}$$

y además

$$\begin{cases} \sigma(x_i) = x_{i+1}, & 1 \leq i < n, \\ \sigma(x_n) = x_1. \end{cases}$$

Este ciclo se denotará también

$$\sigma = (x_1\ x_2\ \cdots\ x_n).$$

Una **trasposición** es un ciclo de longitud 2.

Un ejemplo de ciclo (1 2 3 4 5) donde el soporte es el total:

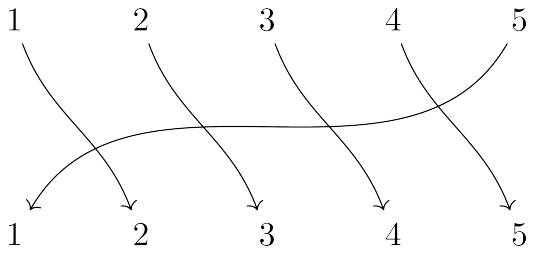

Figura 2.3: Un ciclo

Otro (1 3 4 5) donde el soporte es un subconjunto propio:

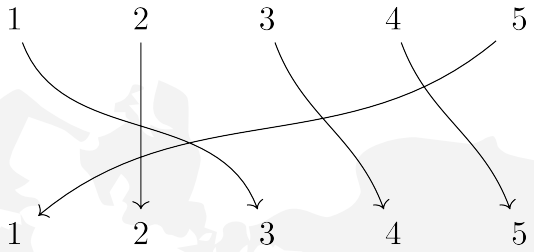

Figura 2.4: Otro ciclo

Otro ciclo más (1 4 3 5 2) que ofrece un aspecto diferente debido al orden de sus entradas:

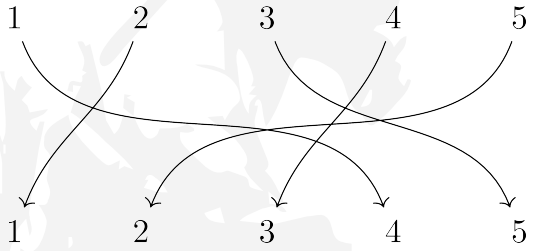

Figura 2.5: Otro ciclo más

¡El primer ejemplo de permutación que vimos también es un ciclo! Concretamente el (2 5 3 4):

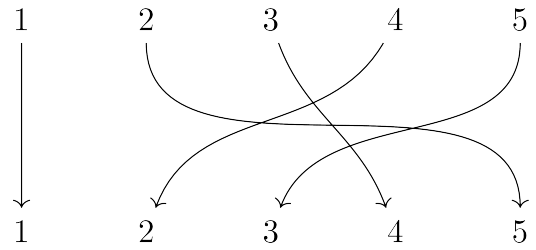

Figura 2.6: Permutación

Un ejemplo de trasposición (3 4) entre elementos consecutivos:

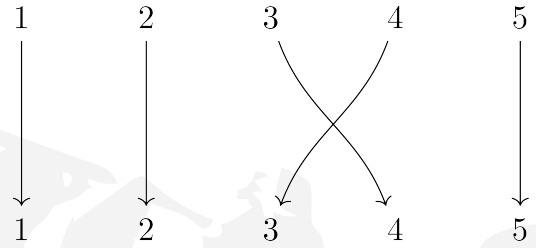

Figura 2.7: Un ciclo

Un ejemplo de trasposición (2 4) entre elementos *no* consecutivos:

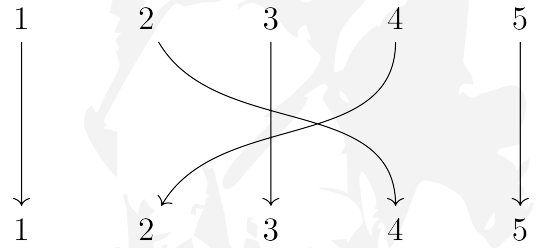

Figura 2.8: Otro ciclo

Advertencia 2.3.2. La notación de ciclo no es única, por ejemplo $(x_1\ x_2\ x_3) = (x_3\ x_1\ x_2) = (x_2\ x_3\ x_1)$.

Cualquier notación para los ciclos que quepa en una línea es intrínsecamente mala, lo ideal sería algo así:

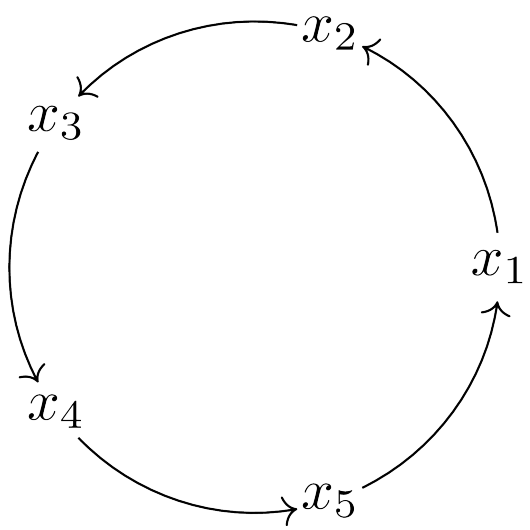

Figura 2.9: Ciclos circulares

Observación 2.3.3. Dada una permutación $\sigma \in \mathrm{Sim}(X)$, al ser $\sigma : X \to X$ biyectiva, $\sigma(x) = y$ si y solo si $x = \sigma^{-1}(y)$, por tanto σ y su inversa σ^{-1} tienen el mismo soporte, $\mathrm{sop}(\sigma) = \mathrm{sop}(\sigma^{-1})$.

Proposición 2.3.4. *El orden de un ciclo coincide con su longitud.*

Demostración. Sea $\sigma = (x_1 \ \cdots \ x_n) \in \mathrm{Sim}(X)$. Es fácil ver que $\sigma^k(x_1) = x_{1+k} \neq x_1$ para todo $1 \leq k < n$, así que $\sigma^k \neq 1_X$, pero $\sigma^n = 1_X$. □

Proposición 2.3.5. *Todo ciclo es producto de trasposiciones.*

Demostración. Es fácil comprobar que $(x_1 \ \cdots \ x_n) = (x_1 \ x_2) \cdots (x_{n-1} \ x_n)$. □

Definición 2.3.6. Dos permutaciones $\sigma, \tau \in \mathrm{Sim}(X)$ son **disjuntas** si sus soportes son disjuntos, $\mathrm{sop}(\sigma) \cap \mathrm{sop}(\tau) = \emptyset$.

Lemma 2.3.7. *Dada $\sigma \in \mathrm{Sim}(X)$, si $x \in \mathrm{sop}(\sigma)$ entonces $\sigma(x) \in \mathrm{sop}(\sigma)$.*

Demostración. En vez de $A \Rightarrow B$ probaremos NO $A \Leftarrow$ NO B.

Si $\sigma(x) \notin \operatorname{sop}(\sigma)$ entonces $\sigma(\sigma(x)) = \sigma(x)$. Como σ es inyectiva, esto implica que $\sigma(x) = x$, con lo que $x \notin \operatorname{sop}(x)$. □

Observación 2.3.8. El soporte de una permutación σ, si no es vacío, ha de tener al menos dos elementos ya que si $\operatorname{sop}(\sigma) = \{x\}$, como $\sigma(x) \in \operatorname{sop}(\sigma)$ tendríamos que $\sigma(x) = x$, así que $x \notin \operatorname{sop}(\sigma)$, que es una contradicción. Por tanto los ciclos de soporte no vacío tienen como poco longitud 2. El ciclo de longitud 0, denotado $()$, es la identidad. De hecho la identidad es la única permutación de soporte vacío.

Corolario 2.3.9. *Dada $\sigma \in \operatorname{Sim}(X)$, si $x \in \operatorname{sop}(\sigma)$ entonces $\sigma^n(x) \in \operatorname{sop}(\sigma)$ para todo $n \in \mathbb{Z}$.*

Demostración. Para $n = 0$ es obvio. Si $n > 0$, es consecuencia del lema anterior, por inducción. Si $n = -1$, se sigue también del lema anterior ya que $\operatorname{sop}(\sigma) = \operatorname{sop}(\sigma^{-1})$. De aquí se deduce también por inducción para todo $n < 0$. □

Proposición 2.3.10. *Si $\sigma, \tau \in \operatorname{Sim}(X)$ son permutaciones disjuntas entonces $\tau\sigma = \sigma\tau$.*

Demostración. Tenemos que demostrar que $\tau\sigma(x) = \sigma\tau(x)$ para todo $x \in X$.

Si $x \notin \operatorname{sop}(\sigma) \cup \operatorname{sop}(\tau)$ entonces $\sigma(x) = x = \tau(x)$, luego

$$\begin{aligned} \tau\sigma(x) &= \tau(x) \\ &= x \\ &= \sigma(x) \\ &= \sigma\tau(x). \end{aligned}$$

Si $x \in \operatorname{sop}(\sigma)$, como las permutaciones son disjuntas entonces $x \notin \operatorname{sop}(\tau)$, luego $\tau(x) = x$, así que $\sigma\tau(x) = \sigma(x)$. Es más, por el lema anterior $\sigma(x) \in \operatorname{sop}(\sigma)$, luego $\sigma(x) \notin \operatorname{sop}(\tau)$ y por tanto también $\tau\sigma(x) = \sigma(x)$.

Como los papeles de σ y τ son intercambiables, el argumento anterior también demuestra que $\tau\sigma(x) = \sigma\tau(x)$ si $x \in \operatorname{sop}(\tau)$. □

Advertencia 2.3.11. El recíproco no es cierto.

Teorema 2.3.12. *Toda permutación con soporte finito se puede descomponer como producto de ciclos disjuntos. Esta descomposición es única salvo orden.*

Demostración. Sea $\sigma \in \mathrm{Sim}(X)$ una permutación. Definimos una relación de equivalencia $\sim$ en X del siguiente modo: $x \sim y$ si existe $n \in \mathbb{Z}$ tal que $y = \sigma^n(x)$. Esta relación es de equivalencia:

- Reflexividad: $x \sim x$ es cierto para todo $x \in X$ ya que $x = 1_X(x) = \sigma^0(x)$.
- Simetría: $x \sim y \Leftrightarrow y \sim x$ pues $y = \sigma^n(x)$ es equivalente a $\sigma^{-n}(y) = x$.
- Transitividad: si $x \sim y \sim z$ entonces $y = \sigma^n(x)$ y $z = \sigma^m(y)$ para ciertos $n, m \in \mathbb{Z}$, luego $z = \sigma^m(\sigma^n(x)) = \sigma^{m+n}(x)$, así que $x \sim z$.

Las clases de equivalencia de esta relación se denominan **órbitas**. La órbita de $x \in X$ es

$$\overline{x} = \{\sigma^n(x) \mid n \in \mathbb{Z}\}.$$

Si $x \notin \mathrm{sop}(\sigma)$, entonces $\overline{x} = \{x\}$. Si $x \in \mathrm{sop}(\sigma)$, entonces $\overline{x} \subset \mathrm{sop}(\sigma)$ por el corolario anterior, y por tanto es un conjunto finito. Veamos que en general $\bar{x} = \{x, \sigma(x), \ldots, \sigma^{m-1}(x)\}$ para cierto $m > 0$. Esto nos va a llevar la mayor parte de esta prueba.

Probemos que existe $m > 0$ tal que $\sigma^m(x) = x$. En efecto, como $\overline{x} = \{\sigma^n(x) \mid n \in \mathbb{Z}\} \subset \mathrm{sop}(\sigma)$, que es finito, todos los $\sigma^n(x)$ no pueden ser distintos, así que han de existir $p, q \in \mathbb{Z}$, $p \neq q$, tales que $\sigma^p(x) = \sigma^q(x)$. Podemos suponer sin pérdida de generalidad que $p < q$, así que, aplicando σ^{-p} a la anterior igualdad deducimos que

$$\begin{aligned} x &= \sigma^{-p}(\sigma^p(x)) \\ &= \sigma^{-p}(\sigma^q(x)) \\ &= \sigma^{q-p}(x), \end{aligned}$$

por tanto podemos tomar $m = q - p > 0$.

Sea $m > 0$ el mínimo tal que $\sigma^m(x) = x$. Los elementos de $\{x, \sigma(x), \ldots, \sigma^{m-1}(x)\}$ son todos distintos. Lo veremos por reducción al absurdo. De lo contrario existirían $0 \leq p < q < m$ tales que $\sigma^p(x) = \sigma^q(x) = \sigma^p(\sigma^{q-p}(x))$. La aplicación σ^p es inyectiva por ser una permutación, así que esto implicaría que $x = \sigma^{q-p}(x)$, pero $0 < q - p < m$, lo que contradice la minimalidad de m.

Ahora tenemos que ver que, para todo $n \in \mathbb{Z}$, $\sigma^n(x) \in \{x, \sigma(x), \dots, \sigma^{m-1}(x)\}$. Basta comprobar que $\sigma^n(x) = \sigma^r(x)$, donde r es el resto no negativo de la división de n por m, $n = m \cdot c + r$, $0 \leq r < m$. En efecto,

$$\begin{aligned} \sigma^n(x) &= \sigma^{r+m\cdot c}(x) \\ &= \sigma^r((\sigma^m)^c(x)). \end{aligned}$$

Como $\sigma^m(x) = x$, entonces $(\sigma^m)^c(x) = x$ si $c \geq 0$. Es más, $\sigma^m(x) = x$ también implica que $x = \sigma^{-m}(x)$, así que $(\sigma^m)^c(x) = x$ también si $c < 0$. Por tanto, en efecto, $\sigma^n(x) = \sigma^r(x)$.

Hemos probado que σ se comporta sobre cada órbita $\bar{x} = \{x, \sigma(x), \dots, \sigma^{m-1}(x)\}$ como un ciclo de longitud m, ya que $\sigma^m(x) = x$, de hecho m era el menor entero positivo que satisfacía esta propiedad. Esto demuestra que σ es el producto de los ciclos asociados a las órbitas no unitarias de la anterior relación de equivalencia. Es decir, por cada órbita no unitaria $\bar{x}$, el ciclo $(x\ \sigma(x)\ \dots\ \sigma^{m-1}(x))$ aparece en la factorización de σ, donde m es el cardinal de $\bar{x}$. El orden de los factores de este producto no importa porque los ciclos son disjuntos, al ser sus soportes clases de una relacion de equivalencia. Hay una cantidad finita de órbitas no unitarias, ya que hemos visto que están contenidas en $\mathrm{sop}(\sigma)$, que es finito. La unicidad es obvia, pues las órbitas, y por tanto los ciclos, están determinados por σ y la relación de equivalencia asociada. □

Corolario 2.3.13. *Toda permutación con soporte finito puede descomponerse como producto de trasposiciones.*

Advertencia 2.3.14. La descomposición de una permutación como producto de trasposiciones no satisface ninguna propiedad de unicidad.

Ejemplo 2.3.15. (Descomposición como producto de ciclos) Consideremos la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} \in S_7.$$

Las órbitas son:

$$\begin{aligned} \overline{1} &= \{1, 3, 5, 4\}, \\ \overline{2} &= \{2, 6\}, \\ \overline{7} &= \{7\}. \end{aligned}$$

Por tanto $\sigma = (1\ 3\ 5\ 4)(2\ 6) = (2\ 6)(1\ 3\ 5\ 4) = (1\ 3)(3\ 5)(5\ 4)(2\ 6)$.

Proposición 2.3.16. *Si $\sigma \in S_n$ se descompone como producto de c ciclos disjuntos de longitudes respectivas $l_1, \dots, l_c$ entonces el orden de σ es el múltiplo común mínimo de $l_1, \dots, l_c$.*

Demostración. Sea $\sigma = \sigma_1 \cdots \sigma_c$ la descomposición de σ como producto de ciclos disjuntos, donde cada σ_i es un ciclo de longitud l_i. Como las permutaciones disjuntas conmutan,

$$\sigma^k = \sigma_1^k \cdots \sigma_c^k$$

para todo $k \geq 1$. Aquí estamos usando que el soporte de cada σ_i^k está contenido en el de σ_i pues si $\sigma_i(x) = x$ entonces $\sigma_i^k(x) = x$ para todo $k \geq 1$. Por tanto, la descomposición de σ^k como producto de ciclos disjuntos se obtendrá descomponiendo cada σ_i^k y haciendo el producto de todas estas descomposiciones. Por la unicidad de la descomposición de una permutación como producto de ciclos disjuntos, $\sigma^k = 1$ si y solo si $\sigma_i^k = 1$ para todo $i = 1, \dots, c$. Si esto ocurre, es que k es divisible por el orden de σ_i para todo i, es decir $l_i | k$ para todo i. El mínimo valor de k para el que esto pasa es, por definición, el múltiplo común mínimo de $l_1, \dots, l_c$. □

2.4. El signo de una permutación

Definición 2.4.1. Un par (i, j) de números $1 \leq i, j \leq n$ es una **inversión** de $\sigma \in S_n$, si $i < j$ pero $\sigma(i) > \sigma(j)$.

Ejemplo 2.4.2. (Inversiones) Las inversiones se corresponden con los cruces en la representación de la permutación como diagrama de flechas:

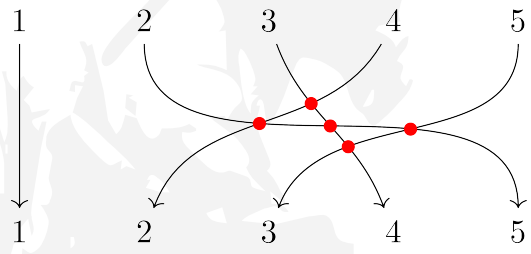

Figura 2.10: Inversiones

Las inversiones de esta permutación son $(2,3)$, $(2,4)$, $(2,5)$, $(3,4)$ y $(3,5)$.

Esto es así siempre que dibujemos el diagrama respetando las dos reglas siguientes:

- Dos flechas se cruzan como máximo en un punto.
- En un prunto de cruce nunca concurren más de dos flechas.

Estas configuraciones prohibidas se comprenden mejor con diagramas que muestran lo que *no* puede pasar:

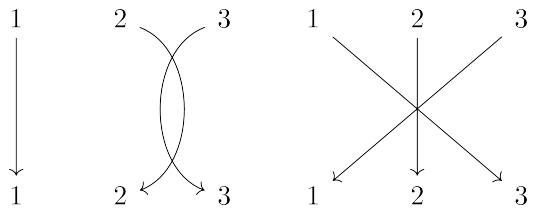

Figura 2.11: Configuraciones prohibidas

Siempre podemos evitarlas moviendo un poco las flechas.

Definición 2.4.3. El **signo** de una permutación $\sigma \in S_n$ se define como

$$\text{signo}(\sigma) = (-1)^{\text{nº de inversiones de } \sigma}.$$

Decimos que σ es **par** si $\text{signo}(\sigma) = +1$ e **impar** si $\text{signo}(\sigma) = -1$.

Obviamente, σ es par si tiene un número par de inversiones, e igualmente en el caso impar. La permutación del ejemplo anterior es impar.

Ejemplo 2.4.4. (S_3) El grupo S_3 tiene $3! = 6$ elementos, que son los siguientes:

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

Las permutaciones pares de S_3 son $()$, (123) y (132) y las impares son (12), (13) y (23).

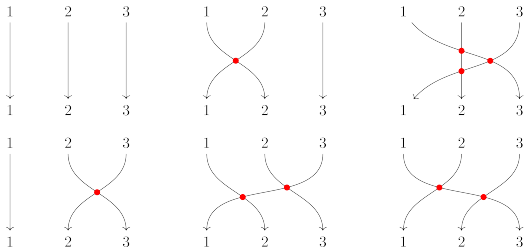

Figura 2.12: S3

Proposición 2.4.5. *Todas las trasposiciones son impares.*

Demostración. Las inversiones de una trasposición $(i\,j) \in S_n$ con $i < j$ son:

$$(i,j),$$
$$(i,i+1),\dots,(i,j-1),$$
$$(i+1,j),\dots,(j-1,j).$$

En total hay $1 + 2(j-i-1)$ inversiones, y este es un número impar.

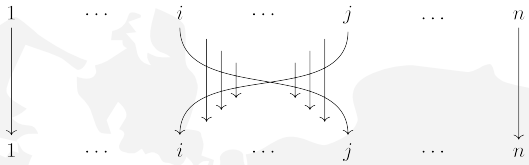

Figura 2.13: Inversiones de una trasposición

□

Proposición 2.4.6. *Dadas dos permutaciones $\sigma, \tau \in S_n$:*

- $\text{signo}(\sigma\tau) = \text{signo}(\sigma)\,\text{signo}(\tau)$.
- $\text{signo}(\sigma^{-1}) = \text{signo}(\sigma)$.

Demostración. Consideremos el diagrama de $\sigma\tau$ que se obtiene dibujando el diagrama de τ encima del de σ. Este diagrama representa a la permutación $\sigma\tau$, aunque haya pares de flechas que se crucen dos veces, una en la parte de τ y otra en la de σ.

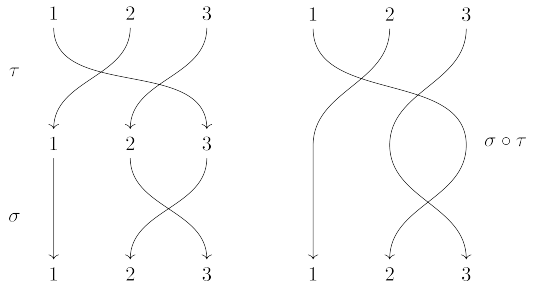

Figura 2.14: Composición

Las inversiones de $\sigma\tau$ se corresponden con los cruces de flechas que se cruzan solo en la parte de σ o solo en la de τ, pero no en ambas. Por tanto, para obtener el número de inversiones de $\sigma\tau$, hay que sumar los cruces de los diagramas de σ y τ y restarle el número par de cruces entre flechas que se cruzan dos veces, una en la parte de σ y otra en la de τ. Esto prueba que el número de inversiones de $\sigma\tau$ tiene la misma paridad que la suma del número de inversiones de σ y de τ. De aquí se deduce la primera fórmula.

La segunda fórmula es obvia porque el diagrama de σ^{-1} se obtiene a partir del de σ haciendo una simetría horizontal. El número de cruces es el mismo. □

Corolario 2.4.7. *Una permutación $\sigma \in S_n$ es par si y solo si es producto de un número par de trasposiciones.*

Demostración. En efecto, si $\sigma = \tau_1 \cdots \tau_r$ donde cada τ_i es una trasposición, entonces

$$\text{signo}(\sigma) = \text{signo}(\tau_1) \cdots \text{signo}(\tau_r) = (-1)^r.$$

□

Este corolario es también cierto cambiando *par* por *impar*.

Corolario 2.4.8. *El signo de un ciclo de longitud l es $(-1)^{l-1}$.*

Este corolario, que es consecuencia de la descomposición de un ciclo como producto de trasposiciones vista antes, nos dice que un ciclo de longitud par es impar y un ciclo de longitud impar es par.

Teorema 2.4.9. (Fórmula de Cauchy) *Si $\sigma \in S_n$ se descompone como producto de c ciclos disjuntos y $\mathrm{sop}(\sigma)$ tiene s elementos entonces*

$$\mathrm{signo}(\sigma) = (-1)^{s-c}.$$

Demostración. Sea $\sigma = \sigma_1 \cdots \sigma_c$ la descomposición de σ como producto de ciclos disjuntos. Sea l_i la longitud del ciclo σ_i, $i = 1, \ldots, c$. El número de elementos del soporte de σ es $s = \sum_{i=1}^{c} l_i$ y

$$\begin{aligned} \mathrm{signo}(\sigma) &= \mathrm{signo}(\sigma_1) \cdots \mathrm{signo}(\sigma_c) \\ &= (-1)^{l_1 - 1} \cdots (-1)^{l_c - 1} \\ &= (-1)^{\sum_{i=1}^{c} (l_i - 1)} \\ &= (-1)^{s-c}. \end{aligned}$$

□

2.5. Subgrupos

Definición 2.5.1. Un subconjunto $H \subset G$ de un grupo G es un **subgrupo** de G si se dan las siguientes condiciones:

- $e \in H$, es decir, el elemento neutro de G está en H.
- Si $x, y \in H$ entonces $xy \in H$.
- Si $x \in H$ entonces $x^{-1} \in H$.

Observación 2.5.2. Un subgrupo $H \subset G$ es un grupo por derecho propio con la operación binaria heredada de G.

Ejemplo 2.5.3. (Ejemplo)

- El subgrupo **trivial** $\{e\} \subset G$ y el **total** $G \subset G$.
- Los subgrupos aditivos $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

- Los subgrupos multiplicativos $\{\pm 1\} \subset \mathbb{Q} \setminus \{0\} \subset \mathbb{R} \setminus \{0\} \subset \mathbb{C} \setminus \{0\}$.
- $(0, +\infty) \subset \mathbb{R} \setminus \{0\}$.
- El subgrupo $SL(n,k) = \{A \mid |A| = 1\} \subset GL(n,k)$ de matrices $n \times n$ sobre un cuerpo k de determinante 1.
- El subgrupo de Klein $\{(), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subset S_4$.

Proposición 2.5.4. *Dado un grupo G, $H \subset G$ es un subgrupo si y solo si se satisfacen las dos condiciones siguientes:*

- $H \neq \emptyset$
- *Si $x, y \in H$ entonces $x^{-1}y \in H$.*

Demostración. $\Rightarrow$ Como $e \in H$, H no es vacío. Si $x, y \in H$, tenemos que también $x^{-1} \in H$, así que $x^{-1}y \in H$.

$\Leftarrow$ Como $H \neq \emptyset$ ha de existir algún $z \in H$, así que $e = z^{-1}z \in H$. Dado $x \in H$, como $e \in H$ tenemos que $x^{-1} = x^{-1}e \in H$. Es más, dados $x, y \in H$, como también $x^{-1} \in H$ deducimos que $xy = (x^{-1})^{-1}y \in H$. □

Definición 2.5.5. Dado un grupo G y un subconjunto $X \subset G$, si definimos $X^{-1} = \{x^{-1} \mid x \in X\}$, el **subgrupo generado por** X se define como

$$\langle X \rangle = \{y \in G \mid \exists n \geq 0, x_1, \dots, x_n \in X \cup X^{-1}; y = x_1 \cdots x_n\} \subset G.$$

Proposición 2.5.6. *Para cualquier subconjunto $X \subset G$ de un grupo G, $\langle X \rangle \subset G$ es un subgrupo.*

Demostración. Tenemos que $e \in G$ ya que e es el producto de una cantidad nula de elementos ($n = 0$). Por otro lado, dados $y, \bar{y} \in \langle X \rangle$, tenemos que $y = x_1 \cdots x_p$ e $\bar{y} = \bar{x}_1 \cdots \bar{x}_q$ donde $x_i, \bar{x}_j \in X \cup X^{-1}$. Por definición, si $x \in X$ entonces $x^{-1} \in X^{-1}$. Es más, si $z \in X^{-1}$ entonces $z = x^{-1}$ para algún $x \in X$, por tanto $z^{-1} = (x^{-1})^{-1} = x \in X$. Esto prueba que los inversos de los elementos de $X \cup X^{-1}$ están también en $X \cup X^{-1}$, por tanto el elemento

$$\begin{aligned} y^{-1}\bar{y} &= (x_1 \cdots x_p)^{-1}(\bar{x}_1 \cdots \bar{x}_q) \\ &= x_p^{-1} \cdots x_1^{-1}\bar{x}_1 \cdots \bar{x}_q \end{aligned}$$

también está en $\langle X \rangle$. □

En general, $\langle \emptyset \rangle = \{e\}$ es el subgrupo trivial.

Ejemplo 2.5.7. (Generadores de S_n)

$$\begin{aligned} S_n &= \langle \text{ciclos} \rangle \\ &= \langle \text{trasposiciones} \rangle \\ &= \langle (1\ 2), \dots, (n-1\ n) \rangle \\ &= \langle (1\ 2), \dots, (1\ n) \rangle \\ &= \langle (1\ 2), (1\ \dots\ n) \rangle. \end{aligned}$$

Observa que hemos omitido las llaves en los conjuntos anteriores, es decir, no hemos escrito $\langle \{(1\ 2), (1\ \dots\ n)\} \rangle$. Lo hacemos para no sobrecargar la notación.

Definición 2.5.8. Un grupo G es **cíclico** si existe $x \in G$ tal que $G = \langle x \rangle$.

Observación 2.5.9. Observa que en general $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$. ¡Ojo! Si x tiene orden infinito, todas estas potencias son distintas según hemos visto antes, luego $\langle x \rangle$ es infinito. Sin embargo, si x tiene orden finito habrá potencias de x con exponente distinto que sean iguales . En cualquier caso $\langle x \rangle$ es abeliano ya que

$$x^p x^q = x^{p+q} = x^{q+p} = x^q x^p.$$

Proposición 2.5.10. *Si $x \in G$ es de orden n entonces $\langle x \rangle = \{e, x, \dots, x^{n-1}\}$ es un subgrupo de n elementos.*

Demostración. Veamos por reducción al absurdo que todos los elementos de $\{e, x, \dots, x^{n-1}\}$ son diferentes. Supongamos que dos de ellos fueran iguales $x^p = x^q$, $p \neq q$. Podemos suponer sin pérdida de generalidad que $p > q$. Entonces

$$\begin{aligned} x^{p-q} &= x^p x^{-q} \\ &= x^q x^{-q} \\ &= e. \end{aligned}$$

Esto es imposible porque $1 \leq p - q \leq n - 1$ y $o(x) = n$.

La inclusión $\langle x \rangle \supset \{e, x, \dots, x^{n-1}\}$ es obvia. Para probar la otra $\subset$, tomamos una potencia cualquiera x^d y realizamos la división de d por n, $d = cn + r$, $0 \leq r < n$.

Entonces

$$\begin{aligned} x^d &= x^{cn+r} \\ &= (x^n)^c x^r \\ &= e^c x^r \\ &= e x^r \\ &= x^r, \end{aligned}$$

y $x^r \in \{e, x, \dots, x^{n-1}\}$. Esto termina la demostración. □

Ejemplo 2.5.11. (¿Es S_n cíclico?) Tenemos que $S_2 = \langle (1\ 2) \rangle$, pero S_n no es cíclico para ningún otro $n > 2$. Veámoslo. Todo elemento $\sigma \in S_n$ se puede descomponer como producto de c ciclos disjuntos de longitud $l_1, \dots, l_c$. El número de elementos del soporte de σ es $l_1 + \cdots + l_c \leq n$. Es fácil pero tedioso ver que

$$o(\sigma) = \text{mcm}(l_1, \dots, l_c) \leq l_1 \cdots l_c < n!$$

excepto si $n = 2$, $c = 1$ y $l_1 = 2$. Por tanto $|\langle \sigma \rangle| = o(\sigma) < n! = |S_n|$, así que la inclusión $\langle \sigma \rangle \subset S_n$ ha de ser siempre estricta si $n > 2$.

2.6. El teorema de Lagrange

Definición 2.6.1. Dado un grupo G y un subgrupo $H \subset G$, definimos la siguiente relación en G:

$$x \sim_H y \Leftrightarrow x^{-1}y \in H.$$

Proposición 2.6.2. *La relación $\sim_H$ es de equivalencia.*

Demostración.

- Reflexiva: $x \sim_H x$ pues $x^{-1}x = e \in H$.
- Simétrica: si $x \sim_H y$ es porque $x^{-1}y \in H$, entonces $(x^{-1}y)^{-1} \in H$ y

$$\begin{aligned} (x^{-1}y)^{-1} &= y^{-1}(x^{-1})^{-1} \\ &= y^{-1}x, \end{aligned}$$

  luego $y^{-1}x \in H$, es decir $y \sim_H x$.
- Transitiva: si $x \sim_H y \sim_H z$ es porque $x^{-1}y, y^{-1}z \in H$, luego $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, así que $x \sim_H z$.

□

Observación 2.6.3. El conjunto cociente de G por la relación de equivalencia $\sim_H$ se denota $G/H := G/\sim_H$.

Ejemplo 2.6.4. (Cocientes de grupos)

- Si $G \subset G$ es el subgrupo total, $x \sim_G y$ siempre, para todo $x, y \in G$, así que G/G es unitario, pues hay una única clase de equivalencia.
- Si consideramos el subgrupo trivial $\{e\} \subset G$, $x \sim_{\{e\}} y$ si y solo si $x = y$. Por tanto todas las clases de equivalencia son unitarias y la proyección natural $\pi : G \to G/\{e\}$ es biyectiva.
- Sea $\langle n \rangle \subset \mathbb{Z}$ el subgrupo cíclico generado por un entero $n \in \mathbb{Z}$ no trivial $n \neq 0$. Los elementos de $\langle n \rangle$ son los múltiplos de n. En este caso, $x \sim_{\langle n \rangle} y$ si y solo si $n|(x - y)$, por tanto se trata de la relación $\sim_n$ considerada en el tema de conjuntos, cuyo cociente, según vimos, es

$$\mathbb{Z}/\langle n \rangle = \{[0], \dots, [n-1]\}.$$

Este cociente se denomina $\mathbb{Z}$ **módulo** n.

Proposición 2.6.5. *Dado un grupo G, un subgrupo $H \subset G$ y un elemento $x \in G$, la clase de equivalencia de x para la relación $\sim_H$ es*

$$[x] = xH := \{xh \mid h \in H\}.$$

Demostración. $\supset$ Dado $xh \in xH$, como $x^{-1}(xh) = h \in H$, $x \sim_H xh$, luego $xh \in [x]$.

$\subset$ Dado $y \in [x]$, como $x \sim_H y$ tenemos que $x^{-1}y \in H$ así que $y = x(x^{-1}y) \in xH$. □

Observación 2.6.6. La clase de equivalencia xH se denomina **clase a izquierda**. Podemos definir otra relación de equivalencia en G:

$$x \,{}_H\!\sim y \Leftrightarrow xy^{-1} \in H.$$

En este caso las clases de equivalencia son de la forma $Hx = \{hx \mid h \in H\}$, $x \in G$, y se llaman **clases a derecha**. En general, las relaciones $\sim_H$ y ${}_H\!\sim$

son diferentes, por tanto las clases a izquierda no tienen por qué coincidir con las clases a la derecha. Ambas relaciones son iguales si G es abeliano, y en ese caso las clases a izquierda y a derecha de cada elemento de G coinciden.

Definición 2.6.7. El **orden** $|G|$ de un grupo G es su número de elementos. Dado un grupo G, el **índice** de un subgrupo $H \subset G$, denotado $[G : H]$, es el número de clases de equivalencia para la relación $\sim_H$, es decir, el número de elementos de G/H.

Teorema 2.6.8. (de Lagrange) *Si G es un grupo finito y $H \subset G$ es un subgrupo, entonces $|H|$ divide a $|G|$ y $[G : H] = |G|/|H|$.*

Demostración. Como G es finito, habrá solo un número finito de clases de equivalencia $[G : H] = n$,

$$G/H = \{x_1H, \dots, x_nH\}.$$

Al ser G unión disjunta de estas clases,

$$|G| = \#(x_1H) + \cdots + \#(x_nH).$$

Para cualquier $x \in G$, la aplicación $f\colon H \to xH$ definida como $f(h) = xh$ es biyectiva. En efecto, es sobreyectiva por definición de xH. Además es inyectiva porque si $f(h_1) = f(h_2)$ entonces $xh_1 = xh_2$ y por la propiedad cancelativa $h_1 = h_2$. Por tanto $\#(xH) = |H|$ para todo $x \in G$, así que deducimos de la ecuación anterior que $|G| = n|H|$. □

Corolario 2.6.9. *Dado un grupo finito G y $x \in G$, el orden de x divide al orden de G.*

Demostración. Como el orden de x es el número de elementos del subgrupo $\langle x \rangle \subset G$, se deduce del teorema de Lagrange. □

Corolario 2.6.10. *Si G es un grupo cuyo orden es un número primo p, entonces G es cíclico.*

Demostración. Sea $x \in G$ un elemento no trivial, como $\langle x \rangle \subset G$ no es el subgrupo trivial y $o(x) = |\langle x \rangle|$ divide a $|G| = p$, no queda más remedio que $o(x) = |\langle x \rangle| = p$, así que $\langle x \rangle = G$ ya que ambos tienen el mismo número de elementos. □

Ejercicio 2.6.11. Hemos visto que el orden de cualquier subgrupo de G divide a $|G|$. Dado un divisor n de $|G|$, ¿existe algún subgrupo de G de orden n? Considera los casos $G = S_2, S_3, S_4$.

2.7. Homomorfismos

Definición 2.7.1. Dados dos grupos G y H, un **homomorfismo** $f\colon G \to H$ es una aplicación tal que $f(xy) = f(x)f(y)$ para todo $x, y \in G$.

Ejemplo 2.7.2. (Homomorfismos)

1. La **identidad** $1_G\colon G \to G$.
2. La **inclusión** de un subgrupo $H \subset G$, $i\colon H \hookrightarrow G$.
3. El **signo** de una permutación, signo$\colon S_n \to \{\pm 1\}$.
4. El **determinante** $GL(n,k) \to k \setminus \{0\}, A \mapsto |A|$.
5. Dado un grupo G y un elemento $x \in G$, la **conjugación** por x, $c_x\colon G \to G$, $c_x(y) = x^{-1}yx$.
6. Dado un grupo G y un elemento $x \in G$, la aplicación $f_x\colon \mathbb{Z} \to G$ definida como $f_x(n) = x^n$.
7. Dado $n \in \mathbb{Z}$, la **multiplicación** por n, es decir, la aplicación $f\colon \mathbb{Z} \to \mathbb{Z}$ definida como $f(x) = nx$.
8. Si G es un grupo abeliano multiplicativo, la **exponenciación** $f\colon G \to G$, $f(x) = x^n$, es un homomorfismo ya que

$$f(xy) = (xy)^n = (xy) \overset{n}{\cdots} (xy) = x^n y^n = f(x)f(y).$$

9. La aplicación **exponencial** $f\colon \mathbb{R} \to (0, +\infty), f(x) = e^x$, es un homomorfismo del grupo aditivo $\mathbb{R}$ en el grupo multiplicativo $(0, +\infty)$.

Los homomorfismos preservan el elemento neutro y los simétricos.

Proposición 2.7.3. *Si $f\colon G \to H$ es un homomorfismo, entonces:*

- $f(e) = e$.
- $f(x^{-1}) = f(x)^{-1}$ *para todo* $x \in G$.

Demostración. Como $e = ee$,

$$f(e) = f(ee) = f(e)f(e).$$

Usando la propiedad cancelativa deducimos que $e = f(e)$.
Al ser $e = xx^{-1}$ deducimos que

$$e = f(e) = f(xx^{-1}) = f(x)f(x^{-1}),$$

por tanto $f(x^{-1}) = f(x)^{-1}$. □

Corolario 2.7.4. *La imagen de un homomorfismo $f\colon G \to H$ es un subgrupo* $\mathrm{im} f \subset H$.

Demostración. Por definición de homomorfismo, el producto de dos elementos de $\mathrm{im} f$ está en $\mathrm{im} f$. Es más, por la proposición anterior $e \in \mathrm{im} f$ y el inverso de un elemento de $\mathrm{im} f$ están en $\mathrm{im} f$. □

La composición de homomorfismos es un homomomorfismo.

Proposición 2.7.5. *Dados dos homomorfismos como en el siguiente diagrama,*

$$G \xrightarrow{f} H \xrightarrow{g} K,$$

la composición $g \circ f\colon G \to K$ es un homomorfismo.

Demostración. Basta observar que, dados $x, y \in G$,

$$\begin{aligned}(g \circ f)(xy) &= g(f(xy)) \\ &= g(f(x)f(y)) \\ &= g(f(x))g(f(y)) \\ &= (g \circ f)(x)(g \circ f)(y).\end{aligned}$$

□

Definición 2.7.6. Un **monomorfismo** $f\colon G \hookrightarrow H$ es un homomorfismo inyectivo. Un **epimorfismo** $f\colon G \twoheadrightarrow H$ es un homomorfismo sobreyectivo. Un **isomorfismo**

$$f\colon G \xrightarrow{\cong} H$$

es un homomorfismo biyectivo.

De los homomorfismos del ejemplo anterior, son isomorfismos los siguientes: 1, 3 para $n = 2$, 4 para $n = 1$, 5 ya que c_x tiene inverso $c_{x^{-1}}$, 7 y 8 si $n = \pm 1$, y 9. Además, 2 es un monomorfismo, 3 es epimorfismo para todo $n \geq 2$ y 4 es epimorfismo para todo $n \geq 1$.

Proposición 2.7.7. *La composición de isomorfismos es un isomorfismo.*

Demostración. Se deduce de que ya sabemos que la composición de homomorfismos es un homomorfismo y que la composición de aplicaciones biyectivas es biyectiva. □

Proposición 2.7.8. *Si $f\colon G \to H$ es un isomorfismo entonces la aplicación inversa $f^{-1}\colon H \to G$ también.*

Demostración. Dados $x, y \in H$ cualesquiera, hemos de probar que

$$f^{-1}(xy) = f^{-1}(x)f^{-1}(y).$$

Como f es inyectivo, bastará comprobar que

$$f(f^{-1}(xy)) = f(f^{-1}(x)f^{-1}(y)).$$

Por un lado, por ser f^{-1} la inversa de f,

$$f(f^{-1}(xy)) = (f \circ f^{-1})(xy) = 1_H(xy) = xy.$$

Por otro lado, como f es un homomorfismo,

$$\begin{aligned} f(f^{-1}(x)f^{-1}(y)) &= f(f^{-1}(x))f(f^{-1}(y)) \\ &= (f \circ f^{-1})(x)(f \circ f^{-1})(y) \\ &= 1_H(x)1_H(y) \\ &= xy. \end{aligned}$$

□

Ejemplo 2.7.9. (Isomorfismos inversos) Los inversos de los isomorfismos 1, 5 y 9 del ejemplo anterior son, respectivamente, $1_G^{-1} = 1_G$, $(c_x)^{-1} = c_{x^{-1}}$, y el isomorfismo $f^{-1}\colon (0,+\infty) \to \mathbb{R}$ definido por $f^{-1}(x) = \log(x)$.

Definición 2.7.10. Dos grupos G y H son **isomorfos**, y lo denotamos $G \cong H$, si existe un isomorfismo

$$f\colon G \xrightarrow{\cong} H.$$

Proposición 2.7.11. *La relación de ser isomorfos es de equivalencia.*

Demostración. Es reflexiva $G \cong G$ porque la identidad es un isomorfismo $1_G\colon G \to G$. La simetría se sigue de que si $G \cong H$ es por que hay algún isomorfismo

$$f\colon G \xrightarrow{\cong} H.$$

El isomorfismo inverso

$$f^{-1}\colon H \xrightarrow{\cong} G$$

prueba que $H \cong G$. La transitividad es consecuencia de que si $G \cong H \cong K$ es porque hay isomorfismos

$$G \underset{\cong}{\xrightarrow{f}} H \underset{\cong}{\xrightarrow{g}} K.$$

Entonces la composición es un isomorfismo

$$g \circ f\colon G \xrightarrow{\cong} K,$$

así que $G \cong K$. □

Proposición 2.7.12. *Si $f\colon G \twoheadrightarrow H$ es un epimorfismo y G es cíclico entonces H también.*

Demostración. Sea $x \in G$ un generador, $G = \langle x \rangle$. Veamos que $f(x) \in H$ es también un generador, es decir $H = \langle f(x) \rangle$. Para ello, tenemos que probar que todo elemento $y \in H$ es una potencia de $f(x)$. Como f es sobreyectivo, existe $z \in G$ tal que $f(z) = y$. Como $G = \langle x \rangle$, existe $n \in \mathbb{Z}$ tal que $z = x^n$, luego $y = f(z) = f(x)^n$. □

Proposición 2.7.13. *Un grupo G es cíclico infinito si y solo si es isomorfo a $\mathbb{Z}$.*

Demostración. $\Rightarrow$ Sea $x \in G$ un generador, $G = \langle x \rangle$. Consideramos el homomorfismo $f_x \colon \mathbb{Z} \to G$ definido anteriormente como $f_x(m) = x^m$. Este homomorfismo es sobreyectivo por ser x un generador del grupo cíclico G. Como el orden de x es infinito, todas las potencias de x son distintas según hemos visto antes, luego f_x es inyectivo, así que f_x es el isomorfismo que andábamos buscando.

$\Leftarrow$ Esta implicación es obvia, porque la propiedad de ser cíclico y el orden se preservan por isomorfismos. □

Proposición 2.7.14. *Si X e Y son conjuntos cualesquiera y $f \colon X \to Y$ es una aplicación biyectiva, entonces*

$$\begin{array}{rccl} \phi_f \colon & \mathrm{Sim}(X) & \longrightarrow & \mathrm{Sim}(Y), \\ & \sigma & \mapsto & f \circ \sigma \circ f^{-1}, \end{array}$$

es un isomorfismo.

Demostración. Si $\sigma \colon X \to X$ es biyectiva entonces $f \circ \sigma \circ f^{-1} \colon Y \to Y$ también, por ser composición de aplicaciones biyectivas. Por tanto ϕ_f es una aplicación bien definida. Veamos que es un homomorfismo. Dados $\tau, \sigma \in \mathrm{Sim}(X)$:

$$\begin{array}{rcl} \phi_f(\tau) \circ \phi_f(\sigma) & = & (f \circ \tau \circ f^{-1}) \circ (f \circ \sigma \circ f^{-1}) \\ & = & f \circ (\tau \circ \sigma) \circ f^{-1} \\ & = & \phi_f(\tau \circ \sigma). \end{array}$$

Para ver que ϕ_f es un isomorfismo, basta comprobar que $\phi_{f^{-1}} \colon \mathrm{Sim}(Y) \to \mathrm{Sim}(X)$ es su inversa. En efecto, $\phi_{f^{-1}} \circ \phi_f = 1_{\mathrm{Sim}(X)}$ ya que ambas son aplicaciones que parten de $\mathrm{Sim}(X)$ y llegan a $\mathrm{Sim}(X)$ y además toman el mismo valor en cualquier $\sigma \in \mathrm{Sim}(X)$, pues

$$\begin{array}{rcl} (\phi_{f^{-1}} \circ \phi_f)(\sigma) & = & \phi_{f^{-1}}(\phi_f(\sigma)) \\ & = & \phi_{f^{-1}}(f \circ \sigma \circ f^{-1}) \\ & = & f^{-1} \circ (f \circ \sigma \circ f^{-1}) \circ (f^{-1})^{-1} \\ & = & \sigma \\ & = & 1_{\mathrm{Sim}(X)}(\sigma). \end{array}$$

Aquí usamos que $(f^{-1})^{-1} = f$. Por esto mismo, los papeles de f y f^{-1} son intercambiables, así que también está probada la otra igualdad, $\phi_f \circ \phi_{f^{-1}} = 1_{\mathrm{Sim}(Y)}$. □

Definición 2.7.15. Dado un homomorfismo $f\colon G \to H$, su **núcleo** es

$$\ker f = \{x \in G \mid f(x) = e\} \subset G.$$

Proposición 2.7.16. *El núcleo de un homomorfismo $f\colon G \to H$ es un subgrupo* $\ker f \subset G$.

Demostración. Como $f(e) = e$, $e \in \ker f$. Si $x, y \in \ker f$ entonces

$$f(xy) = f(x)f(y) = ee = e,$$

luego $xy \in \ker f$. Es más, si $x \in \ker f$ entonces

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

así que $x^{-1} \in \ker f$. □

Definición 2.7.17. El **grupo alternado** es el subgrupo $A_n \subset S_n$ formado por las permutaciones pares.

El grupo alternado es un subgrupo porque es el núcleo del homomorfismo signo$\colon S_n \to \{\pm 1\}$.

Proposición 2.7.18. *Un homomorfismo $f\colon G \to H$ es inyectivo si y solo si* $\ker f = \{e\}$.

Demostración. $\Rightarrow$ La inclusión $\supset$ es obvia. Para ver $\subset$ tomamos $x \in \ker f$. Como $f(x) = e = f(e)$ y f es inyectivo deducimos que $x = e$.

$\Leftarrow$. Sean $x, y \in G$ tales que $f(x) = f(y)$. Entonces

$$\begin{aligned} f(x^{-1}y) &= f(x^{-1})f(y) \\ &= f(x)^{-1}f(x) \\ &= e, \end{aligned}$$

es decir, $x^{-1}y \in \ker f = \{e\}$, por tanto $x^{-1}y = e$ y despejando vemos que $y = x$. □

Observación 2.7.19. Esta proposición demuestra que para probar que un homomorfismo $f\colon G \to H$ es inyectivo basta demostrar que si $f(x) = e$ entonces $x = e$.

2.8. Grupos cociente

Definición 2.8.1. Dado un grupo G, un subgrupo $K \subset G$ es **normal** si $g^{-1}kg \in K$ para todo $g \in G$ y $k \in K$.

Advertencia 2.8.2. La noción de subrgupo normal $K \subset G$ depende tanto de K como de G. Si variamos alguno de los dos, la situación puede cambiar.

Ejemplo 2.8.3. (Subgrupos (no) normales) Dado un grupo cualquiera G, los subgrupos trivial y total $\{e\}$ y G son normales. El subgrupo $K = \{(), (1\ 2)\} \subset S_3$ no es normal puesto que

$$(1\ 3)^{-1}(1\ 2)(1\ 3) = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin K.$$

Proposición 2.8.4. *Si G es abeliano, todo subgrupo $K \subset G$ es normal.*

Demostración. Dados $g \in G$ y $k \in K$,

$$\begin{aligned} g^{-1}kg &= g^{-1}gk \\ &= ek \\ &= k \in K. \end{aligned}$$

□

Proposición 2.8.5. *Dado un grupo G y un subrgupo $K \subset G$, los siguientes enunciados son equivalentes:*

1. *$K \subset G$ es normal.*
2. *$gK = Kg$ para todo $g \in G$.*
3. *Las relaciones $\sim_K$ y $_K\sim$ coinciden.*

Demostración. Las propiedades segunda y tercera coinciden porque la correspondencia existente entre relaciones de equivalencia y particiones. Veamos pues que las dos primeras también coinciden.

1. $\Rightarrow$ 2. Veamos primero $\supset$. Todo elemento de Kg es de la forma kg con $k \in K$. Por ser $K \subset G$ normal, $g^{-1}kg \in K$, así que $kg = g(g^{-1}kg) \in gK$.

Veamos $\subset$. Todo elemento de gK es de la forma gk con $k \in K$. Por ser $K \subset G$ normal y $g^{-1} \in G$, $gkg^{-1} = (g^{-1})^{-1}kg^{-1} \in K$, así que $gk = (gkg^{-1})g \in Kg$.

2. $\Rightarrow$ 1. Dados $k \in K$ y $g \in G$, como $kg \in Kg = gK$, existe $k' \in K$ tal que $kg = gk'$, así que $g^{-1}kg = k' \in K$. Por tanto $K \subset G$ es normal. □

Como veremos a lo largo de este epígrafe, los subgrupos normales de G coinciden con aquellos que son el núcleo de algún homomorfismo que parte de G.

Proposición 2.8.6. *El núcleo de un homomorfsimo $f\colon G \to H$ es un subgrupo normal* $\ker f \subset G$.

Demostración. Dados $g \in G$ y $k \in \ker f$,

$$\begin{aligned} f(g^{-1}kg) &= f(g)^{-1}f(k)f(g) \\ &= f(g)^{-1}ef(g) \\ &= f(g)^{-1}f(g) \\ &= e. \end{aligned}$$

Por tanto $g^{-1}kg \in \ker f$. □

La propiedad más importante de los subgrupos normales $K \subset G$ es que sirven para dotar de estructura de grupo al cociente G/K.

Teorema 2.8.7. *Dado un grupo G y un subgrupo normal $K \subset G$, entonces el conjunto cociente G/K posee una única estructura de grupo tal que la proyección natural $\pi : G \twoheadrightarrow G/K$ es un homomorfismo. El núcleo de esta proyección es* $\ker \pi = K$

Demostración. Comenzamos viendo que si G/K es un grupo y π es un homomorfismo, entonces hay una única elección posible para la operación binaria que dota a G/K de estructura de grupo. En efecto, dados $xK, yK \in G/K$, como $\pi(x) = xK$ y $\pi(y) = yK$, tenemos que

$$(xK)(yK) = \pi(x)\pi(y) = \pi(xy) = (xy)K.$$

Basta por tanto demostrar que la fórmula

$$(xK)(yK) = (xy)K$$

define una operación binaria en G/K que satisface las propiedades requeridas. Lo más difícil es ver que la aplicación

$$\begin{array}{rcl}(G/K)\times(G/K) & \longrightarrow & G/K,\\ (xK,yK) & \mapsto & (xy)K,\end{array}$$

está bien definida. Observa que la imagen de un par podría depender de la elección de representantes de las clases a izquierda. Veamos que esto no ocurre. Para ello, dados $x, y \in G$ cualesquiera, debemos comprobar que si $xK = \bar{x}K$ e $yK = \bar{y}K$ entonces $(xy)K = (\bar{x}y)K = (x\bar{y})K$, ya que de aquí se deduce que $(xy)K = (\bar{x}\bar{y})K$.

Por un lado, si $yK = \bar{y}K$ entonces $y \sim_K \bar{y}$, es decir $y^{-1}\bar{y} \in K$, por tanto

$$\begin{array}{rcl}(xy)^{-1}(x\bar{y}) & = & y^{-1}x^{-1}x\bar{y}\\ & = & y^{-1}e\bar{y}\\ & = & y^{-1}\bar{y} \in K,\end{array}$$

así que $xy \sim_K x\bar{y}$, es decir $(xy)K = (x\bar{y})K$.

Por otro lado, si $xK = \bar{x}K$ entonces $x \sim_K \bar{x}$, es decir $x^{-1}\bar{x} \in K$. Como $K \subset G$ es normal, esto implica que $y^{-1}x^{-1}\bar{x}y \in K$, luego

$$(xy)^{-1}(\bar{x}y) = y^{-1}x^{-1}\bar{x}y \in K,$$

esto es, $xy \sim_K \bar{x}y$, o lo que es lo mismo, $(xy)K = (\bar{x}y)K$.

Este producto en G/K satisface la propiedad asociativa porque, a nivel de representantes, está definido como en G, y el producto del grupo G satisface la propiedad asociativa. Por la misma razón eK es un elemento neutro en G/K y el inverso de xK es $(xK)^{-1} = x^{-1}K$.

Con respecto al núcleo, basta observar que, dado $x \in G$, $\pi(x) = xK = eK$ si y solo si $e \sim_K x$, lo cual ocurre si y solo si $x = e^{-1}x \in K$. □

Observación 2.8.8. El grupo cociente G/K se denomina G **módulo** K y la clase xK también se llama x módulo K. El teorema anterior demuestra que xK es el elemento neutro de G/K si y solo si $x \in K$. También prueba que todo subgrupo normal es el núcleo del algún homomorfismo.

Corolario 2.8.9. *Para cualquier grupo G, la proyección natural $\pi\colon G \xrightarrow{\cong} G/\{e\}$ es un isomorfismo.*

Hemos identificado entonces subgrupos normales con núcleos de homomorfismos. No podemos hacer lo mismo con las imágenes de homomorfismos.

Advertencia 2.8.10. Si G es un grupo y $H \subset G$ es un subgrupo que no es normal, la imagen de la inclusión $i\colon H \hookrightarrow G$ es $\operatorname{im} i = H$, por tanto la imagen de un homomorfismo, en general, no es normal en el grupo de llegada.

Veamos ahora una versión del teorema de factorización de aplicaciones para grupos y homomorfismos.

Teorema 2.8.11. (Primer teorema de isomorfía) *Dado un homomorfismo de grupos $f\colon G \to H$, existe un único homomorfismo $\bar{f}\colon G/\ker f \to \operatorname{im} f$ tal que el siguiente diagrama es conmutativo*

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/\ker f & \xrightarrow[\bar{f}]{} & \operatorname{im} f \end{array}$$

Figura 2.15: Primer teorema de isomorfía

es decir, $f = i \circ \bar{f} \circ \pi$. Aquí π es la proyección canónica e i es la inclusión. Además, $\bar{f}$ es un isomorfismo.

Demostración. La factorización es la del homomorfismo f visto solo como aplicación. Basta ver que la relación de equivalencia en G definida por la aplicación f es la misma que la que define el subgrupo $\ker f$. Por comodidad, llamaremos $K = \ker f$. Dados $x, y \in G$, $x \sim_K y \Leftrightarrow x^{-1}y \in K \Leftrightarrow f(x^{-1}y) = e$. Como $f(x^{-1}y) = f(x)^{-1}f(y)$ esto es el elemento neutro si y solo si $f(x) = f(y)$, lo que equivale a $x \sim_f y$. Habría que comprobar también que $\bar{f}$ es un homomorfismo. Esto es cierto porque, recordemos, esta aplicación se define como f sobre los representantes, es decir,

$\bar{f}(xK) = f(x)$ y f es un homomorfismo, así que

$$\begin{aligned}\bar{f}((xK)(yK)) &= \bar{f}((xy)K)\\ &= f(xy)\\ &= f(x)f(y)\\ &= \bar{f}(xK)\bar{f}(yK).\end{aligned}$$

□

Corolario 2.8.12. *Dado $n \geq 2$, el orden del correspondiente grupo alternado es A_n es $|A_n| = \frac{n!}{2}$, por tanto en S_n hay tantas permutaciones pares como impares.*

Demostración. El homomorfismo signo$\colon S_n \to \{\pm 1\}$ es sobreyectivo, luego im signo $= \{\pm 1\}$. Como $A_n = \ker$ signo, el primer teorema de isomorfía proporciona un isomorfismo $\frac{S_n}{A_n} \cong \{\pm 1\}$. Usando el teorema de Lagrange, vemos que

$$\begin{aligned}2 &= |\{\pm 1\}|\\ &= [S_n : A_n]\\ &= \frac{|S_n|}{|A_n|}\\ &= \frac{n!}{|A_n|}.\end{aligned}$$

De aquí se deduce el resultado despejando. □

Corolario 2.8.13. *Un grupo G es cíclico de orden n si y solo si es isomorfo a $\mathbb{Z}/\langle n\rangle$.*

Demostración. $\Rightarrow$ Sea $x \in G$ un generador, $G = \langle x\rangle$. Consideramos el homomorfismo $f_x\colon \mathbb{Z} \to G$ definido anteriormente como $f_x(m) = x^m$. Este homomorfismo es sobreyectivo por ser x un generador del grupo cíclico G, así que im$f_x = G$. Como el orden de x coincide con el de G, que es n, sabemos que $m \in \ker f_x \Leftrightarrow f_x(m) = x^m = e \Leftrightarrow n|m \Leftrightarrow m \in \langle n\rangle$, así que $\ker f_x = \langle n\rangle$. Por tanto el primer teorema de isomorfía nos da el isomorfismo deseado $\overline{f_x}\colon \mathbb{Z}/\langle n\rangle \cong G$.

$\Leftarrow$ Esta implicación es obvia, porque la propiedad de ser cíclico y el orden se preservan por isomorfismos. □

Teorema 2.8.14. (de Cayley) *Todo grupo G es isomorfo a un subgrupo de un grupo de permutaciones. Si G es finito de orden n, entonces G isomorfo*

a un subgrupo de S_n.

Demostración. Definimos la aplicación

$$f\colon G \to \mathrm{Sim}(G)$$

del siguiente modo. Dado $g \in G$,

$$f(g)\colon G \longrightarrow G$$

es la aplicación definida como

$$f(g)(x) = gx.$$

Esta aplicación es biyectiva, por tanto es una permutación del conjunto G. Para comprobarlo, demostraremos que $f(g^{-1})\colon G \longrightarrow G$ es su inversa, es decir, que

$$f(g) \circ f(g^{-1}) = 1_G = f(g^{-1}) \circ f(g).$$

Las tres aplicaciones parten de G y llegan a G, así que basta probar que toman los mismos valores sobre cada $x \in G$. En efecto, por un lado,

$$\begin{aligned}(f(g) \circ f(g^{-1}))(x) &= f(g)(f(g^{-1})(x)) \\ &= f(g)(g^{-1}x) \\ &= g(g^{-1}x) \\ &= (gg^{-1})x \\ &= ex \\ &= x \\ &= 1_G(x).\end{aligned}$$

Esto demuestra que $f(g) \circ f(g^{-1}) = 1_G$. La otra igualdad, $f(g^{-1}) \circ f(g) = 1_G$, se sigue ahora del hecho de que los papeles de g y g^{-1} son intercambiables, ya que $(g^{-1})^{-1} = g$.

Veamos que f es un homomorfismo. En efecto, dados $g_1, g_2 \in G$, $f(g_1g_2) = f(g_1) \circ f(g_2)$ ya que ambas son permutaciones de G y, para todo $x \in G$,

$$\begin{aligned}(f(g_1) \circ f(g_2))(x) &= f(g_1)(f(g_2)(x)) \\ &= f(g_1)(g_2x) \\ &= g_1(g_2x) \\ &= (g_1g_2)x \\ &= f(g_1g_2)(x).\end{aligned}$$

Veamos que f es inyectiva, es decir, que $\ker f = \{e\}$. En efecto, si $g \in \ker f$ entonces $f(g) = 1_G$ luego

$$\begin{aligned} g &= ge \\ &= f(g)(e) \\ &= 1_G(e) \\ &= e. \end{aligned}$$

Como $\ker f = \{e\}$, el primer teorema de isomorfía nos dice que

$$G \cong \frac{G}{\{e\}} \cong \operatorname{im} f \subset \operatorname{Sim}(G).$$

Esto demuestra la primera parte del teorema.

Para la segunda parte, basta observar que, como G tiene n elementos, cualquier enumeración de los mismos $G = \{x_1, \dots, x_n\}$ da lugar a una aplicación biyectiva $\psi : G \to \{1, \dots, n\}$ definida como $\psi(x_i) = i$ para todo i. Según hemos visto antes, esta biyección da lugar a un isomorfismo $\phi_\psi : \operatorname{Sim}(G) \cong S_n$. Argumentando como antes, vemos que $G \cong \operatorname{im}(\phi_\psi \circ f) \subset S_n$. □

Capítulo 3

Enteros

3.1. Anillos

Definición 3.1.1. Un **anillo** es un grupo abeliano aditivo R equipado con otra operación binaria, llamada *multiplicación* o *producto*,

$$\begin{array}{rcl} R \times R & \to & R, \\ (a, b) & \mapsto & ab, \end{array}$$

que satisface las siguientes propiedades, donde $a, b, c \in R$ son elementos cualesquiera:

- Asociativa:

$$a(bc) = (ab)c.$$

- Distributiva:

$$\begin{array}{rcl} a(b + c) & = & ab + ac, \\ (a + b)c & = & ac + bc. \end{array}$$

- Existencia de elemento neutro $1 \in R$ para el producto:

$$1a = a = a1.$$

Un anillo es **conmutativo** si además el producto satisface la siguiente propiedad adicional:

- Conmutativa:

$$ab = ba.$$

Observación 3.1.2. En todo anillo, el elemento neutro del producto es único. Esto se demuestra igual que la unicidad del elemento neutro de un grupo. El producto en un anillo se denotará a veces $a \cdot b$, pero casi siempre lo haremos por yuxtaposición ab.

Advertencia 3.1.3. El producto de un anillo no lo dota de estructura de grupo.

Ejemplo 3.1.4. (Clásicos) Los números enteros $\mathbb{Z}$, racionales $\mathbb{Q}$, reales $\mathbb{R}$ y complejos $\mathbb{C}$ son anillos, pero los naturales $\mathbb{N}$ no.

Ejemplo 3.1.5. (Polinomios) Dado un anillo conmutativo R, podemos considerar su anillo de **polinomios** $R[x]$ en una variable x, cuyos elementos $p(x) \in R[x]$ son de la forma

$$p(x) = a_n x^n + \cdots + a_1 x + a_0$$

con *coeficientes* $a_i \in R$, $1 \leq i \leq n$. En ocasiones los denotaremos como si fueran series

$$p(x) = \sum_{n \geq 0} a_n x^n$$

dando por supuesto que *casi todos* los coeficientes son 0. Esto facilita la definición de la suma y la multiplicación

$$\sum_{n \geq 0} a_n x^n + \sum_{n \geq 0} b_n x^n = \sum_{n \geq 0} (a_n + b_n) x^n,$$

$$\left(\sum_{i \geq 0} a_i x^i \right) \left(\sum_{j \geq 0} b_j x^j \right) = \sum_{n \geq 0} \left(\sum_{i+j=n} a_i b_j \right) x^n.$$

Los anillos de polinomios en varias variables se definen inductivamente

$$R[x_1, \dots, x_{n-1}, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

Ejemplo 3.1.6. (Matrices) Dado un entero n y un anillo conmutativo R, el conjunto $M(n, R)$ de las matrices $n \times n$ con entradas en R es un anillo con la suma y el producto de matrices habituales. Para $n \geq 2$, este anillo no es conmutativo.

Ejemplo 3.1.7. (El anillo trivial) El conjunto unitario $R = \{0\}$, dotado de las únicas operaciones suma y multiplicación posibles, es un anillo. Aquí obviamente $1 = 0$.

Proposición 3.1.8. *En un anillo R, $1 = 0$ si y solo si $R = \{0\}$.*

Demostración. $\Leftarrow$ Obvio.
$\Rightarrow$ Dado $a \in R$, $a = 1a = 0a = 0$. □

Ejemplo 3.1.9. (Anillos de Boole) Dado un conjunto X, el conjunto $\mathcal{P}(X) = \{A | A \subset X\}$ formado por los subconjuntos de X es un anillo, denominado **anillo de Boole**, donde la suma es la *diferencia simétrica*,

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

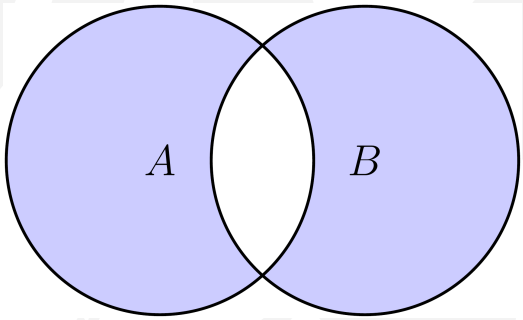

Figura 3.1: Diferencia simétrica

y el producto es la intersección,

$$AB = A \cap B.$$

¿Cuál es el 0? ¿Y el 1? ¿Y $-A$? ¿Y A^2? Dibuja $A + B + C$ para tres conjuntos en posición general.

Ejemplo 3.1.10. (Anillo producto) Dados dos anillos R y S, el **producto cartesiano** $R \times S$ es un anillo definido sobre el grupo producto las siguiente multiplicación:

$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

El elemento neutro para el producto es $(1, 1)$, es decir, el elemento neutro para el producto de cada anillo en cada una de las coordenadas.

Proposición 3.1.11. *En un anillo cualquiera R se cumplen las siguientes propiedades para todo $a \in R$:*

- $0a = 0 = a0$.
- $(-1)a = -a = a(-1)$.

Demostración. Como $0 = 0 + 0$,

$$\begin{aligned} a0 &= a(0 + 0) \\ &= a0 + a0. \end{aligned}$$

Cancelando un $a0$ de cada lado obtenemos que $0 = a0$. La igualdad $0a = 0$ se demuestra análogamente.

Al ser $0 = 1 + (-1)$ tenemos que

$$\begin{aligned} 0 &= a0 \\ &= a(1 + (-1)) \\ &= a1 + a(-1) \\ &= a + a(-1). \end{aligned}$$

Despejando deducimos que $-a = a(-1)$. La igualdad $-a = (-1)a$ se prueba de un modo similar. □

Definición 3.1.12. Un subconjunto $S \subset R$ de un anillo R es un **subanillo** si es un subgrupo aditivo y además:

- $1 \in S$.
- $ab \in S$ para todo $a, b \in S$.

Observación 3.1.13. Un subanillo $S \subset R$ es un anillo por derecho propio con la suma y la multiplicación heredadas de S. El total $R \subset R$ es obviamente un subanillo.

Advertencia 3.1.14. El subconjunto $\{0\} \subset R$ no es un subanillo, a menos que sean iguales.

Ejemplos de subanillos son $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ y $R \subset R[x]$.

Ejercicio 3.1.15. Dado un entero primo $p \in \mathbb{Z}$, comprueba que

$$S = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\} \subset \mathbb{Q}$$

es un subanillo.

Ejercicio 3.1.16. Comprueba que

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subset M(2, \mathbb{R})$$

es un subanillo.

Definición 3.1.17. Una **unidad** $u \in R$ es un elemento de un anillo tal que existe $u^{-1} \in R$, denominado **inverso** de u, de modo que

$$uu^{-1} = 1 = u^{-1}u.$$

Un **cuerpo** es un anillo conmutativo no trivial donde todos los elementos no nulos son unidades.

Las unidades de $\mathbb{Z}$ son $\{1, -1\}$, mientras que $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos. Dado un cuerpo k, las unidades de $M(n, k)$ son el grupo $GL(n, k)$ de matrices $n \times n$ de determinante no nulo.

Observación 3.1.18. El elemento inverso u^{-1} de una unidad u es único. Esto se demuestra igual que la unicidad de los inversos en un grupo. Si u es una unidad entonces u^{-1} también y $(u^{-1})^{-1} = u$. Dividir por una unidad es multiplicar por el inverso $\frac{a}{u} = au^{-1}$. Los elementos 1 y -1 son siempre unidades (no necesariamente distintas) cuyos inversos son ellos

mismos. El subconjunto $R^\times \subset R$ formado por las unidades de un anillo R es un grupo con la multiplicación. El grupo multiplicativo $R^\times$ es abeliano si el anillo R es conmutativo. La propiedad de ser un cuerpo se preserva por isomorfismos.

3.2. Homomorfismos

Los homomorfismos de anillos son aplicaciones entre anillos que preservan la estructura.

Definición 3.2.1. Dados dos anillos R y S, un **homomorfismo** $f\colon R \to S$ es un homomorfismo entre los correspondientes grupos aditivos tal que, además, para todo $a, b \in R$,

$$\begin{aligned} f(ab) &= f(a)f(b), \\ f(1) &= 1. \end{aligned}$$

Un **monomorfismo** $f\colon R \hookrightarrow S$ es un homomorfismo inyectivo. Un **epimorfismo** $f\colon R \twoheadrightarrow S$ es un homomorfismo sobreyectivo. Un **isomorfismo**

$$f\colon R \xrightarrow{\cong} S$$

es un homomorfismo biyectivo.

La identidad $\mathrm{id}_R\colon R \to R$ es un isomorfismo.

Ejemplo 3.2.2. (La inclusión) Si R es un anillo y $S \subset R$ es un subanillo, la **inclusión** $i\colon S \hookrightarrow R$, $i(a) = a$, es un homomorfismo. ¿Qué diferencia a la inclusión de la identidad?

Ejemplo 3.2.3. (La evaluación) Dado un anillo conmutativo R y $a \in R$ está definido el homomorfismo de **evaluación** $ev_a\colon R[x] \to R$ como $ev_a(p(x)) = p(a)$.

Ejemplo 3.2.4. (Los complejos como matrices) Si $S \subset M(2, \mathbb{R})$ es el subanillo del ejercicio anterior, podemos definir un isomorfismo $f\colon \mathbb{C} \cong S$ como

$$f(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Compruébalo.

Proposición 3.2.5. *Dado un homomorfismo $f\colon R \to S$, su imagen $\mathrm{im} f \subset S$ es un subanillo.*

Demostración. Como f es un homomorfismo entre los grupos aditivos subyacentes, $\mathrm{im} f \subset S$ es un subgrupo aditivo. Es más,

- $1 = f(1) \in \mathrm{im} f$.
- $f(a)f(b) = f(ab) \in \mathrm{im} f$ para todo $a, b \in R$.

□

Proposición 3.2.6. *Si $f\colon R \to S$ es un homomorfismo de anillos y $u \in R$ es una unidad, entonces $f(u) \in S$ es una unidad y $f(u^{-1}) = f(u)^{-1}$.*

Demostración. Como $uu^{-1} = 1 = u^{-1}u$, aplicando el homomorfismo f deducimos que

$$\begin{aligned} f(u)f(u^{-1}) &= f(uu^{-1}) \\ &= f(1) \\ &= 1 \\ &= f(u^{-1}u) \\ &= f(u^{-1})f(u). \end{aligned}$$

El resultado se deduce de estas ecuaciones. □

Corolario 3.2.7. *Todo homomorfismo de anillos $f\colon R \to S$ se restringe a un homomorfismo entre sus grupos de unidades $f_{|R^\times}\colon R^\times \to S^\times$.*

Proposición 3.2.8. *Dados dos homomorfismos de anillos*

$$R \xrightarrow{f} S \xrightarrow{g} T$$

la composición $g \circ f\colon R \to T$ también es un homomorfismo. Lo mismo es cierto para isomorfismos.

Demostración. Comenzamos probando la primera parte. La composición $g \circ f$ es un homomorfismo de grupos aditivos. Tenemos que

$$\begin{aligned} (g \circ f)(1) &= g(f(1)) \\ &= g(1) \\ &= 1. \end{aligned}$$

Es más, dados $a, b \in R$, $(g \circ f)(ab) = (g \circ f)(a)(g \circ f)(b)$. Esto se comprueba igual que se hizo para los grupos.

El enunciado para isomorfismos se deduce de que la composición de aplicaciones biyectivas es biyectiva. □

Proposición 3.2.9. *Si $f\colon R \to S$ es un isomorfismo de anillos entonces la aplicación inversa $f^{-1}\colon S \to R$ también.*

Demostración. Sabemos que $f^{-1}\colon S \to R$ es biyectiva y un homomorfismo de grupos aditivos. Falta por ver que f^{-1} preserva el elemento neutro para el producto y los productos. Como f es inyectivo, para ver que $f^{-1}(1) = 1$ basta comprobar que $f(f^{-1}(1)) = f(1)$. Esto es cierto pues

$$f(f^{-1}(1)) = (f \circ f^{-1})(1) = 1_S(1) = 1$$

y además $f(1) = 1$ por ser f un homomorfismo de anillos. La demostración de que f^{-1} preserva productos se hace igual que en el caso de grupos. □

El anillo de los enteros cumple la siguiente curiosa propiedad, que en términos categóricos se denomina ser *inicial* en la categoría de los anillos.

Proposición 3.2.10. *Para todo anillo R existe un único homorfismo $f\colon \mathbb{Z} \to R$.*

Demostración. Cualquier homomorfismo $f\colon \mathbb{Z} \to R$ satisface $f(0) = 0$ y $f(1) = 1$. Por tanto, si $n > 0$ en $\mathbb{Z}$,

$$\begin{aligned} f(n) &= f(1+\overset{n}{\cdots}+1) \\ &= f(1)+\overset{n}{\cdots}+f(1) \\ &= 1+\overset{n}{\cdots}+1, \\ f(-n) &= -f(n). \end{aligned}$$

Es fácil comprobar que estas fórmulas definien un homomorfismo, que ha de ser único. □

3.3. Ideales

Advertencia 3.3.1. En adelante, todos los anillos que consideremos serán conmutativos.

Existe otro tipo destacado de subconjunto de un anillo que juega un papel más importante que los subanillos.

Definición 3.3.2. Dado un anillo R, un **ideal** $I \subset R$ es un subgrupo aditivo tal que $ra \in I$ para todo $r \in R$ y $a \in I$.

En $\mathbb{Z}$ los números pares forman un ideal.

Ejemplo 3.3.3. (Ideales) Dado un anillo cualquiera R, los siguientes son ejemplos de ideales:

- El total $R \subset R$.
- El trivial $\{0\} \subset R$.
- Dado $a \in R$, el **ideal principal** generado por a está formado por sus múltiplos

$$(a) = \{ra \mid r \in R\} \subset R.$$

Observa que, si $R = \mathbb{Z}$, dado $n \in \mathbb{Z}$, $(n) = \langle n \rangle$.

Más adelante veremos que no hay más subgrupos de $\mathbb{Z}$ que estos y que por tanto coinciden con los ideales.

Proposición 3.3.4. *El **núcleo** de un homomorfismo $f\colon R \to S$,*

$$\ker f = \{a \in R \mid f(a) = 0\},$$

es un ideal $\ker f \subset R$.

Demostración. Sabemos que $\ker f \subset R$ es un subgrupo aditivo. Queda probar la condición de ideal. Si $a \in \ker f$ y $r \in R$ entonces $f(ra) = f(r)f(a) = f(r)0 = 0$ luego $ra \in \ker f$. □

Por tanto, en $R[x]$, los polinomios $f(x)$ tales que $f(1) = 0$ forman un ideal pues constituyen el núcleo del homomorfismo $ev_1\colon R[x] \to R$ de evaluación en $1 \in R$. De hecho podríamos evaluar en cualquier otro elemento de R.

Observación 3.3.5. Un homomorfismo de anillos $f\colon R \to S$ es inyectivo si y solo si $\ker f = \{0\}$, ya que esto es cierto a nivel de grupos. Dicho de otro modo, para probar la inyectividad de f basta ver que si $a \in R$ es tal que $f(a) = 0$ entonces $a = 0$.

Veamos ahora la relación entre ideales y unidades.

Proposición 3.3.6. *Un ideal $I \subset R$ contiene una unidad $\Leftrightarrow I = R$.*

Demostración. $\Leftarrow$ Obvio porque $1 \in R = I$ es una unidad.

$\Rightarrow$ Si $u \in I \subset R$ es una unidad, $u^{-1} \in R$ y por ser I un ideal $1 = uu^{-1} \in I$.

Si $1 \in I$ y $a \in R$ entonces $1a = a \in I$, por tanto $R \subset I$, así que $I = R$. □

Corolario 3.3.7. *Un anillo es un cuerpo $\Leftrightarrow$ tiene solo dos ideales (necesariamente el total y el trivial).*

Demostración. $\Rightarrow$ Sea k un cuerpo. Los cuerpos, en tanto que anillos no triviales, tienen al menos dos ideales: el trivial y el total. Si $I \subset k$ es un ideal no trivial entonces existe un elemento $a \in I \subset k$ no nulo. Como k es un cuerpo este elemento ha de ser una unidad, así que $I = k$.

$\Leftarrow$ Sea R un anillo cuyos dos únicos ideales son $\{0\}$ y R. En particular R no es trivial. Sea $a \in R$ un elemento no trivial. Como $a \in (a)$, este ideal no puede ser el trivial, así que ha de ser el total $(a) = R$. Al ser $1 \in R = (a)$ ha de existir un elemento $r \in R$ tal que $ra = 1$, así que a es una unidad. □

Corolario 3.3.8. *Si $f\colon k \to R$ es un homomorfismo de anillos donde k es un cuerpo y R no es trivial entonces f es inyectivo.*

Demostración. El ser $f\colon k \to R$ un homomorfismo, $f(1) = 1$. Como R no es trivial, $1 \neq 0$ luego $1 \notin \ker f \subset k$ no puede ser el total. Por ser k es un cuerpo la única opción posible es $\ker f = \{0\}$, luego f es inyectivo. □

3.4. Cocientes

Teorema 3.4.1. *Dado un anillo R y un ideal $I \subset R$, existe una única estructura de anilo en el grupo cociente R/I tal que la proyección natural $\pi : R \twoheadrightarrow R/I$, $\pi(a) = a + I$, es un homomorfismo de anillos. El núcleo de esta proyección es* $\ker \pi = I$.

Demostración. Partimos de que el correspondiente enunciado para grupos ya se ha probado.

Si R/I fuera un anillo y $\pi : R \to R/I$ un homomorfismo entonces

$$\begin{aligned}(a+I)(b+I) &= \pi(a)\pi(b)\\ &= \pi(ab)\\ &= (a+b)+I.\end{aligned}$$

Veamos que esta fórmula para la multiplicación, necesariamente única si queremos que π sea un homomorfismo, define una operación binaria en R/I. Para ver que está bien definida hay que comprobar que

$$\left.\begin{array}{l} a+I=a'+I \\ b+I=b'+I \end{array}\right\} \Rightarrow (ab)+I=(a'b')+I.$$

Esto equivale a

$$\left.\begin{array}{l} a-a'\in I \\ b-b'\in I \end{array}\right\} \Rightarrow ab-a'b'=(a-a')b+a'(b-b')\in I.$$

Las propiedades que el producto y la suma deben satisfacer se cumplen obviamente pues se derivan de las correspondientes propiedades de la suma y el producto en R, por tanto R/I es un anillo. El elemento neutro para el producto de R/I es $1+I$. □

Ejemplo 3.4.2. ($\mathbb{Z}/(n)$) Dado $n\in\mathbb{Z}$, vamos a estar particularmente interesados en los anillos $\mathbb{Z}/(n)$. Según hemos visto en el capítulo de grupos, si $n=0$ entonces $\mathbb{Z}\cong\mathbb{Z}/(0)$. Si $n\neq 0$, podemos suponer que $n>0$ ya que $(n)=(-n)$. En este caso, vimos en el capítulo de conjuntos que

$$\mathbb{Z}/(n)=\{[0],\dots,[n-1]\}.$$

Es más, dado $m\in\mathbb{Z}$, $[m]=[r]$, donde r es el resto no negativo de la división de m por n, $m=c\cdot n+r$, ya que $0\leq r<n$ y $m-r=c\cdot n\in(n)$.

Teorema 3.4.3. (Primer Teorema de Isomorfía) *Dado un homomorfismo $f\colon R\to S$, existe un único homomorfismo $\bar{f}\colon R/\ker f\to \mathrm{im} f$ tal que f factoriza como $f=i\circ\bar{f}\circ p$, es decir, f encaja en el siguente* ***diagrama conmutativo****,*

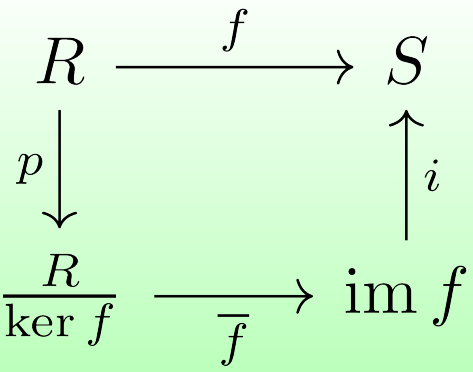

Figura 3.2: Primer teorema de isomorfía para anillos

Aquí π es la proyección natural e i es la inclusión. Además $\bar{f}$ es un isomorfismo.

Demostración. La factorización es la vista para grupos. Basta por tanto ver que $\bar{f}$ preserva el 1 y los productos. Recordemos que esta aplicación está definida como $\bar{f}(a+I) = f(a)$. De este modo,

$$\begin{aligned} \bar{f}(1+I) &= f(1) \\ &= 1, \\ \bar{f}((a+I)(b+I)) &= \bar{f}((ab)+I) \\ &= f(ab) \\ &= f(a)f(b) \\ &= \bar{f}(a+I)\bar{f}(b+I). \end{aligned}$$

□

Corolario 3.4.4. *Dado un anillo cualquiera R, la proyección natural $\pi\colon R \cong R/(0)$ es un isomorfismo.*

Demostración. Basta aplicarle el primer teorema de isomorfía a la identidad $1_R\colon R \to R$. □

Corolario 3.4.5. $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Demostración. Consideremos el homomorfismo $f\colon \mathbb{R}[x] \to \mathbb{C}$ definido como $f(p(x)) = p(i)$. Este homomorfismo está bien definido porque es la composición

de la inclusión $\mathbb{R}[x] \subset \mathbb{C}[x]$ y la evaluación $ev_i \colon \mathbb{C}[x] \to \mathbb{C}$. Es sobreyectivo ya que dado $a+ib \in \mathbb{C}, f(bx+a) = a+ib$ por tanto $\operatorname{im} f = \mathbb{C}$. Usando el primer teorema de isomorfía, basta ahora ver que $\ker f = (x^2+1) \subset \mathbb{R}[x]$. La inclusión $\supset$ es sencilla porque todo elemento $p(x) \in (x^2+1)$ es múltiplo del polinomio x^2+1, es decir, de la forma $p(x) = (x^2+1)q(x)$ y entonces $f(p(x)) = p(i) = (i^2+1)q(i) = 0$. Para ver $\subset$, tomamos ahora un elemento arbitrario $p(x) \in \ker f$, es decir, tal que $p(i) = 0$. Dividimos $p(x)$ entre x^2+1, obteniendo así una expresión en $\mathbb{R}[x]$ de la forma

$$p(x) = c(x)(x^2+1) + r(x).$$

Como x^2+1 tiene grado 2, el resto $r(x)$, si no es trivial, tendrá grado < 2, es decir, en cualquier caso $r(x) = ax + b$ para ciertos $a, b \in \mathbb{R}$. Entonces,

$$\begin{aligned} 0 &= p(i) \\ &= c(i)(i^2+1) + r(i) \\ &= b + ia. \end{aligned}$$

Un número complejo es cero si y solo si su parte real y su parte imaginaria son cero, $b = a = 0$. Por tanto $r(x) = 0$ y $p(x) = c(x)(x^2+1) \in (x^2+1)$. □

3.5. Dominios

Definición 3.5.1. Dado un anillo R, un **divisor de cero** es un elemento $a \in R$ no nulo, $a \neq 0$, tal que existe otro $b \in R$, $b \neq 0$, de modo que $ab = 0$. Un anillo no trivial R es un **dominio (de integridad)** si no posee divisores de cero.

El anillo $\mathbb{Z}$ y los cuerpos son dominios.

Observación 3.5.2. Dicho de otro modo, R es un dominio cuando dados $a, b \in R$ tales que $ab = 0$ entonces $a = 0$ o $b = 0$. Los subanillos de un dominio también son dominios. El 1 y el -1 nunca son divisores de cero. En general, una unidad nunca puede ser un divisor de cero. La propiedad de ser un dominio se preserva por isomorfismos.

Ejemplo 3.5.3. (Un anillo que no es un dominio) Como conjunto, el anillo $\mathbb{Z}/(4)$ es

$$\mathbb{Z}/(4) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}.$$

El elemento neutro para la suma es $\bar{0}$, por tanto $\bar{2} \neq \bar{0}$. Sin embargo $\bar{2}\cdot\bar{2} = \bar{4} = \bar{0}$ ya que $4 \in (4)$. Esto prueba que $\bar{2}$ es un divisor de cero en este anillo. ¿Hay algún otro?

Ejercicio 3.5.4. Da mas ejemplos de anillos $\mathbb{Z}/(n)$ que **no** sean dominios.

La siguiente propiedad de los dominios se conoce como **propiedad cancelativa**.

Proposición 3.5.5. *En un dominio, si $ab = ac$ y $a \neq 0$ entonces $b = c$.*

Demostración. En un anillo R, la ecuación $ab = ac$ equivale a $a(b - c) = 0$. Si $a \neq 0$ y R es un dominio entonces no queda otra opción que $b - c = 0$, lo cual equivale a $b = c$. □

En general, la propiedad cancelativa es cierta si a es una unidad, ya que en ese caso podemos multiplicar a izquierda por el inverso de a.

Proposición 3.5.6. *Si R es un dominio entonces $R[x]$ también.*

Demostración. Dados dos polinomios no nulos $p(x) = a_n x^n + \cdots$ y $q(x) = b_m x^m + \cdots$ de grados respectivos n y m ($a_n \neq 0 \neq b_m$), su producto $p(x)q(x) = a_n b_m x^{n+m} + \cdots$ es no nulo de grado $n + m$ ya que $a_n b_m \neq 0$ por ser R un dominio. □

Corolario 3.5.7. *Si R es un dominio entonces $R[x_1, \ldots, x_n]$ también.*

Proposición 3.5.8. *Todo dominio finito R es un cuerpo.*

Demostración. Sea $a \in R$ un elemento no nulo. Por ser R un dominio, la propiedad cancelativa demuestra que la aplicación

$$\begin{array}{ccc} R & \longrightarrow & R, \\ x & \mapsto & a \cdot x, \end{array}$$

es inyectiva. Toda aplicación inyectiva entre conjuntos finitos con el mismo número de elementos es biyectiva. Por tanto, existe $b \in R$ tal que $a \cdot b = 1$. Como R es conmutativo, esto implica que a es una unidad con inversa $a^{-1} = b$. □

Ejemplo 3.5.9. (Cuerpos finitos) Si $p \in \mathbb{Z}$ es un primo entonces $\mathbb{Z}/(p)$ es un cuerpo con p elementos. En efecto, sabemos que este anillo tiene p elementos, así que en virtud de la proposición anterior basta comprobar que es un dominio. Dados $\bar{m}, \bar{n} \in \mathbb{Z}/(p)$, si $\bar{m} \cdot \bar{n} = \overline{mn} = \bar{0}$ entonces $mn \in (p)$, es decir, p divide a mn. Pero como p es primo, para que esto ocurra p ha de dividir a m o bien a n. En el primero de los casos $\bar{m} = \bar{0}$ y en el segundo $\bar{n} = \bar{0}$, así que no puede haber divisores de 0 en $\mathbb{Z}/(p)$. Este cuerpo también se denota $\mathbb{F}_p$.

Ejercicio 3.5.10. ¿Hay cuerpos finitos cuyo número de elementos no sea primo?

3.6. Ideales primos

Definición 3.6.1. Los ideales distintos del total se denominan **propios**. Un ideal $I \subsetneq R$ es **primo** si dados $a, b \in R$ tales que $ab \in I$ entonces $a \in I$ o $b \in I$.

Observación 3.6.2. Un ideal $I \subset R$ es propio si y solo si R/I no es trivial. La propiedad de ser un dominio se preserva por isomorfismos.

Proposición 3.6.3. *Un ideal $I \subset R$ es primo $\Leftrightarrow$ R/I es un dominio.*

Demostración. Ser un ideal propio se corresponde con tener un cociente no trivial. Veamos la equivalencia del resto de propiedades.

$\Rightarrow$ Veamos que no hay divisores de cero en R/I. Dados $\bar{a}, \bar{b} \in R/I$, si $\bar{a}\bar{b} = \overline{ab} = \bar{0}$ entonces $ab \in I$. Como I es primo, esto implica que $a \in I$ o $b \in I$, es decir $\bar{a} = \bar{0}$ o $\bar{b} = \bar{0}$. Por tanto no hay divisores de cero en R/I

$\Leftarrow$ Veamos que I es primo. Dados $a, b \in R$, si $ab \in I$ entonces $\bar{a}\bar{b} = \overline{ab} = \bar{0}$, así que por ser R/I un dominio, entonces $\bar{a} = \bar{0}$ o $\bar{b} = \bar{0}$, es decir $a \in I$ o $b \in I$. Esto prueba que I es primo. □

Corolario 3.6.4. *El ideal trivial $(0) \subset R$ es primo $\Leftrightarrow$ R es un dominio.*

Demostración. Esto es consecuencia de que hay un isomorfismo de anillos $R \cong R/(0)$. □

Proposición 3.6.5. *Un ideal principal $(n) \subset \mathbb{Z}$ es primo $\Leftrightarrow$ $n = 0$ o n es un entero primo.*

Demostración. $\Leftarrow$ El ideal (0) es primo porque $\mathbb{Z}$ es un dominio, y si n es un entero primo ya hemos visto antes que entonces $\mathbb{Z}/(n)$ es un dominio, así que (n) también sería primo en este caso.

$\Rightarrow$ Por reducción al absurdo, si $n \neq 0$ no fuera un entero primo, entonces factorizaría $n = ab$ como producto de dos enteros $a, b \in \mathbb{Z}$, $a, b \neq \pm 1$. Por tanto, $1 < |a|, |b| < |n|$, así que n no divide a a ni a b, luego $\bar{a} \neq \bar{0} \neq \bar{b}$ en $\mathbb{Z}/(n)$. Sin embargo $\bar{a}\bar{b} = \overline{ab} = \bar{n} = \bar{0}$ pues $n \in (n)$. □

Definición 3.6.6. La **característica** de un dominio de integridad R es el orden de $1 \in R$ en el grupo aditivo, es decir, el menor entero $n \geq 1$ tal que

$$1 + \overset{n}{\cdots} + 1 = 0.$$

Si no existe tal n decimos que R es de característica 0.

Los dominios $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ tienen característica 0 mientras que $\mathbb{Z}/(p)$ tiene característica p para $p \in \mathbb{Z}$ primo. Más adelante veremos que la característica de un dominio cualquiera es 0 o un número entero primo.

3.7. Divisibilidad en $\mathbb{Z}$

En esta sección formalizaremos propiedades de los números enterios relacionadas con la divisibilidad. La mayor parte son bien conocidas. Usaremos sin demostrarlo el siguiente resultado básico de la teoría de conjuntos.

Teorema 3.7.1. (Principio de buena ordenación) *Todo subconjunto no vacío de $\mathbb{Z}$ acotado inferiormente posee un mínimo, necesariamente único.*

Definición 3.7.2. Dados $a, b \in \mathbb{Z}$, decimos que a **divide** a b, y escribimos $a|b$, si existe $c \in \mathbb{Z}$ tal que $ac = b$. También se dice que b es **divisible** por a.

Observación 3.7.3. Todos los enteros dividen al 0, pero el 0 solo se divide a sí mismo. El 1 solo es divisible por ± 1. Obsverva que si $a|b$ y $b \neq 0$ entonces $|a| \leq |b|$.

Proposición 3.7.4. *Las unidades de $\mathbb{Z}$, 1 y -1, son los dos únicos enteros que dividen a todos los demás.*

Demostración. Es obvio que 1 y -1 dividen a cualquier otro $a \in \mathbb{Z}$ ya que $1a = a$ y $(-1)(-a) = a$. Si $b \in \mathbb{Z}$ divide a cualquier otro entero, en particular divide a $1 \in \mathbb{Z}$. El 1 solo es divisible por sí mismo y por -1, luego $b = \pm 1$. □

Proposición 3.7.5. *Dados $a, b, c \in \mathbb{Z}$, se satisfacen las siguientes propiedades.*

1. *$a|a$ (**reflexiva**) y $-a|a$.*
2. *si $a|b$ y $b|c$ entonces $a|c$ (**transitiva**).*
3. *$a|b$ y $b|a$ si y solo si $a = \pm b$.*
4. *Si $a|b$ y $a|c$ entonces $a|(b + c)$.*
5. *Si $a|b$ entonces $a|bc$, para todo $c \in \mathbb{Z}$.*

Demostración. El primer apartado se satisface porque $a1 = a$ y $(-a)(-1) = a$.

En el supuesto de 2, $ar = b$ y $bs = c$ para ciertos $r, s \in \mathbb{Z}$, luego $a(rs) = (ar)s = bs = c$, así que $a|c$.

Con respecto a 3, $\Leftarrow$ se ha probado en 1. Veamos $\Rightarrow$. Bajo estas hipótesis, $ar = b$ y $bs = a$ para ciertos $r, s \in \mathbb{Z}$, luego $a(rs) = (ar)s = bs = a$. Por la propiedad cancelativa del dominio $\mathbb{Z}$, $rs = 1$, así que r y s son unidades mutuamente inversas, por lo tanto $r = s = \pm 1$ y en consecuencia $a = \pm b$.

En las condiciones de 4, $ar = b$ y $as = c$ para ciertos $r, s \in \mathbb{Z}$, luego $a(r+s) = ar + as = b + c$, y por tanto $a|(b + c)$.

Por último, en 5, $ar = b$ para cierto $r \in \mathbb{Z}$, así que $a(rc) = (ar)c = bc$, luego $a|c$. □

A estas alturas de la vida, vamos a aprender a dividir.

Teorema 3.7.6. (División euclídea) *Dados $D, d \in \mathbb{Z}$, $d \neq 0$, existen $c, r \in \mathbb{Z}$ únicos tales que:*

- $D = dc + r$,
- $0 \leq r < |d|$.

Demostración. El subconjunto

$$S = \{D - dx \mid (x \in \mathbb{Z}) \wedge (D - dx \geq 0)\} \subset \mathbb{Z}$$

no es vacío. En efecto, si $D \geq 0$ tomamos $x = -dD$ y entonces $D - dx = D + d^2D = D(1 + d^2) \geq 0$, y si $D < 0$ tomamos $x = dD$ y $D - dx = D - d^2D = D(1 - d^2) \geq 0$ ya que, como $d \neq 0$, $d^2 \geq 1$.

Como S está acotado inferiormente por 0, ha de tener un mínimo $r \in S$ por el principio de buena ordenación. Este mínimo se alcanzará para cierto valor de $x = c \in \mathbb{Z}$, y por tanto $r = D - dc \geq 0$, es decir, $D = dc + r$. Veamos que $r < |d|$. Por reducción al absurdo, si $r \geq |d|$ entonces $r' = r - |d| \geq 0$. Es más, como $d \neq 0$, $r' < r$, pero $r' \in S$ ya que $r' = r \pm d = D - dc \pm d = D - d(c \mp 1)$. Esto contradice la minimalidad de $r \in S$.

Veamos ahora la unicidad del cociente y del resto. Supongamos que también $D = dc' + r'$ para ciertos $c', r' \in \mathbb{Z}$ con $0 \leq r' < |d|$. Entonces $dc + r = dc' + r'$. Si $r = r'$ entonces $dc = dc'$. Como $d \neq 0$ podemos aplicar la propiedad cancelativa y deducimos que $c = c'$. Veamos que es imposible que $r \neq r'$. De lo contrario, podemos suponer sin pérdida de generalidad que $r > r'$. Como $0 \leq r, r' < |d|$ entonces $0 < r - r' < |d|$, pero $r - r' = d(c' - c)$, que es divisible por d, así que $|d| \leq |r - r'|$, lo cual entra en contradicción. □

Observación 3.7.7. En las circunstancias anteriores, decimos que D es el **dividendo**, d es el **divisor**, c es el **cociente** y r es el **resto** de la **división euclídea** de D entre d. Es frecuente relajar la segunda condición del teorema y pedir solo que $0 \leq |r| < |d|$. En este caso, el cociente y el resto no tienen por qué ser únicos. Más concretamente, si la división no es exacta siempre hay dos restos posibles, uno positivo y otro negativo, por ejemplo $14 = 3 \cdot 4 + 2 = 3 \cdot 5 + (-1)$.

Proposición 3.7.8. *Dados $D, d \in \mathbb{Z}$, $d \neq 0$, $d|D$ si y solo si el resto de la división*

de D entre d es $r = 0$.

Demostración. $\Rightarrow$ Si $d|D$ entonces existe $c \in \mathbb{Z}$ tal que $dc = D$, luego $D = dc + 0$ es una división euclídea con resto $r = 0$.

$\Leftarrow$ Recíprocamente, si en la división euclídea $D = dc + r$ tenemos que $r = 0$, entonces $d|D$. □

Observación 3.7.9. Cuando las condiciones equivalentes de la proposición anterior se dan, decimos que la división euclídea de D entre d es **exacta**. Es frecuente relajar la segunda condición del teorema y pedir solo que $0 \leq |r| < |d|$. En este caso, el cociente y el resto no tienen por qué ser únicos. Más concretamente, si la división no es exacta siempre hay dos restos posibles, uno positivo y otro negativo, por ejemplo $14 = 3 \cdot 4 + 2 = 3 \cdot 5 + (-1)$.

Ahora podemos demostrar que todos los subgrupos de $\mathbb{Z}$ son cíclicos.

Teorema 3.7.10. *Todos los subgrupos de $\mathbb{Z}$ son cíclicos.*

Demostración. Sea $H \subset \mathbb{Z}$ un subrgupo cualquiera. El subgrupo trivial $H = \{0\}$ es cíclico pues está generado por el elemento neutro $H = \langle 0 \rangle$. Supongamos que $H \neq \{0\}$ entonces existe algún elemento $m \in H$ no nulo $m \neq 0$. De hecho existe algún elemento positivo, ya que si $m < 0$ entonces $-m \in H$, por ser H un subgrupo, y $-m > 0$.

Sea

$$S = \{m \in H \mid m > 0\} \subset \mathbb{Z}.$$

Por el principio de buena ordenación, hay un mínimo $n \in S$. Veamos que $\langle n \rangle = H$. Por definición, $\langle n \rangle$ está formado por los múltiplos de n. La inclusión $\subset$ es cierta ya que $n \in H$, H es un subgrupo y cualquier múltiplo de n se obtiene sumando n o $-n$ consigo mismo un número determinado de veces. Para ver $\supset$, tenemos que comprobar que todos los elementos de H son múltiplos de n. Sea $a \in H$. Realizamos la división euclídea de a por n: $a = nc + r$, $0 \leq r < n$. Si $r = 0$ entonces $a = nc \in \langle n \rangle$. Veamos por reducción al absurdo que es imposible que $r \neq 0$. De lo contrario, $0 < r < n$. Es más, $r = a - nc \in H$ pues $a \in H$, $nc \in \langle n \rangle \subset H$ y H es un subgrupo. Por tanto $r \in S$, pero $r < n$, y esto contradeciría

la minimalidad de n. □

Observación 3.7.11. En la demostración hemos visto que todo subgrupo $H \subset \mathbb{Z}$ está generado por el menor $n \in H$, $n > 0$.

Corolario 3.7.12. *Todo subgrupo de $\mathbb{Z}$ es un ideal principal y todo ideal de $\mathbb{Z}$ es principal.*

Demostración. Hemos visto que todo subgrupo $H \subset \mathbb{Z}$ es cíclico, es decir $H = \langle n \rangle$ para cierto $n \in \mathbb{Z}$. Anteriormente habíamos observado que $\langle n \rangle = (n)$ coincide con el ideal principal formado por los múltiplos de n.

Si $I \subset \mathbb{Z}$ es un ideal, en particular es un subgrupo, así que existe $n \in \mathbb{Z}$ tal que $I = \langle n \rangle = (n)$. □

3.8. Divisor común máximo

Definición 3.8.1. Dados dos enteros a y b, diremos que $d \in \mathbb{Z}$ es un **divisor común máximo** de a y b y denotaremos $d = \mathrm{mcd}(a, b)$, si verifica las siguientes propiedades:

1. $d|a$ y $d|b$.
2. Si d' es tal que $d'|a$ y $d'|b$ entonces $d'|d$.

Si 1 es un divisor común máximo de a y b, se dice que a y b son **coprimos** o **primos entre sí**.

Observación 3.8.2. El divisor común máximo se suele denominar **máximo común divisor**, pero me suena a anglicismo. Como la divisibilidad no depende del signo, si d es un divisor común máximo de a y b entonces $-d$ también. La única posibilidad de que $\mathrm{mcd}(a, b) = 0$ es que $a, b = 0$.

Un poco maś abajo probaremos la existencia de un divisor común máximo para cualquier par de enteros a y b. Hasta entonces, cada vez que hablemos del divisor común máximo de dos enteros daremos por hecho que lo estamos haciendo

"caso de existir". De hecho, la existencia se probará reduciendo el cálculo de un divisor común máximo de dos enteros cualesquiera al de otros cuya existencia conozcamos.

Proposición 3.8.3. *Si d y d' son divisores comunes máximos de a y b entonces $d' = \pm d$.*

Demostración. En efecto, porque las condiciones de la definición aseguran que $d|d'$ y $d'|d$. □

Proposición 3.8.4. *El divisor común máximo de dos enteros satisface las siguientes propiedades:*

1. $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, a)$.
2. $\mathrm{mcd}(a, b) = \mathrm{mcd}(\pm a, \pm b)$.
3. $\mathrm{mcd}(a, b) = b \Leftrightarrow b|a$.
4. $\mathrm{mcd}(0, b) = b$.

Demostración. Las dos primeras son obvias porque la definición no depende del orden de los enteros y la relación de divisibilidad no depende de signos. Probemos la tercera.

$\Rightarrow$ Si $b = \mathrm{mcd}(a, b)$ entonces en particular $b|a$.

$\Leftarrow$ Si $b|a$ entonces b divide a a y a b, y si $d|a$ y $d|b$ entonces en particular $d|b$, con lo que b satisface la definición de $\mathrm{mcd}(a, b)$.

La cuarta es consecuencia de la tercera. □

Proposición 3.8.5. *Dados $a, b \in \mathbb{Z}$ tales que $a = bc + r$ entonces* $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$.

Demostración. Sea $d \in \mathbb{Z}$. Basta ver que $d|a$ y $d|b$ si y solo si $d|b$ y $d|r$. De otro modo, suponiendo que $d|b$, basta comprobar que $d|a$ si y solo si $d|r$. Supongamos pues que $d|b$. Si $d|r$ entonces $d|(bc + r) = a$. Recíprocamente, si $d|a$ entonces $d|(a - bc) = r$. □

En la división anterior, $a = bc + r$ podría ser la división euclídea de a entre b, incluso con resto negativo, pero no es necesario.

Ejemplo 3.8.6. (Algoritmo de Euclides) Dados dos enteros $a, b \in \mathbb{Z}$, podemos calcular su divisor común máximo por el siguiente procedimiento. Podemos suponer sin pérdida de generalidad que $|a| \geq |b|$. Denotamos $r_0 = a$, $r_1 = b$. Para

cada $n \geq 1$ tal que $r_n \neq 0$, calculamos la división euclídea de r_{n-1} entre r_n, y denominamos r_{n+1} a su resto

$$r_{n-1} = r_n c_n + r_{n+1}.$$

En virtud de la proposición anterior,

$$\begin{aligned} \mathrm{mcd}(a,b) &= \mathrm{mcd}(r_0, r_1) \\ &\vdots \\ &= \mathrm{mcd}(r_n, r_{n+1}). \end{aligned}$$

Si $r_{n+1} = 0$ para algún $n \geq 0$ entonces $\mathrm{mcd}(a,b) = r_n$. En virtud de las propiedades de la división euclídea, en cada paso disminuye el tamaño del resto $|r_n| > |r_{n+1}| \geq 0$. Esto garantiza que el procedimiento para calcular $\mathrm{mcd}(a,b)$ se acaba como máximo tras realizar $|b|$ divisiones euclídeas. En este procedimiento podemos usar divisiones euclídeas con resto negativo.

Por ejemplo, calculemos $\mathrm{mcd}(156, 58)$. Con divisiones con resto positivo:

$$\begin{aligned} 156 &= 58 \cdot 2 + 40, \\ 58 &= 40 \cdot 1 + 18, \\ 40 &= 18 \cdot 2 + 4, \\ 18 &= 4 \cdot 4 + 2, \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

Por tanto $\mathrm{mcd}(156, 58) = 2$. Si permitimos divisiones con resto negativo, vamos más rápido:

$$\begin{aligned} 156 &= 58 \cdot 3 - 18, \\ 58 &= (-18) \cdot (-3) + 4, \\ -18 &= 4 \cdot (-5) + 2, \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

Corolario 3.8.7. *Dos $a, b \in \mathbb{Z}$ cualesquiera siempre tienen un divisor común maximo, que es único salvo signo.*

Teorema 3.8.8. (Identidad de Bézout) *Dados dos enteros $a, b \in \mathbb{Z}$, si $d = \mathrm{mcd}(a,b)$ entonces existen $\alpha, \beta \in \mathbb{Z}$ tales que $d = a\alpha + b\beta$.*

Demostración. Si lo probamos para un divisor común máximo será cierto para su opuesto cambiando el signo de $\alpha, \beta \in \mathbb{Z}$. Supongamos pues que d se ha calculado medialte el algoritmo de Euclides:

$$\begin{aligned} a &= bc_1 + r_2 \\ b &= r_2c_2 + r_3 \\ r_2 &= r_3c_3 + r_4 \\ &\vdots \\ r_{n-3} &= r_{n-2}c_{n-2} + r_{n-1} \\ r_{n-2} &= r_{n-1}c_{n-1} + d \\ r_{n-1} &= dc_n + 0. \end{aligned}$$

Despejamos los restos de todas las divisiones

$$\begin{aligned} r_2 &= a - bc_1 \\ r_3 &= b - r_2c_2 \\ r_4 &= r_2 - r_3c_3 \\ &\vdots \\ r_{n-2} &= r_{n-4} - r_{n-3}c_{n-3} \\ r_{n-1} &= r_{n-3} - r_{n-2}c_{n-2} \\ d &= r_{n-2} - r_{n-1}c_{n-1}, \end{aligned}$$

y en cada una sustituimos el resto anterior:

$$\begin{aligned} d &= r_{n-2} - r_{n-1}c_{n-1} \\ &= r_{n-2} - (r_{n-3} - r_{n-2}c_{n-2})c_{n-1} \\ &= r_{n-2}(1 + c_{n-2}c_{n-1}) - r_{n-3} \\ &= (r_{n-4} - r_{n-3}c_{n-3})(1 + c_{n-2}c_{n-1}) - r_{n-3} \\ &= r_{n-4}(1 + c_{n-2}c_{n-1}) - r_{n-3}(1 + c_{n-3} + c_{n-3}c_{n-2}c_{n-1}) \\ &= \cdots \end{aligned}$$

Al final, nos queda una combinación lineal de a y b, y basta con agrupar coeficientes para hallar α y β. □

Ejemplo 3.8.9. (Identidad de Bézout) Hallemos esta identidad para $2 = \mathrm{mcd}(156, 58)$. Con las divisiones con resto positivo:

$$\begin{aligned} 40 &= 156 - 58 \cdot 2, \\ 18 &= 58 - 40 \cdot 1, \\ 4 &= 40 - 18 \cdot 2, \\ 2 &= 18 - 4 \cdot 4, \end{aligned}$$

así que

$$\begin{aligned} 2 &= 18 - 4 \cdot 4 \\ &= 18 - (40 - 18 \cdot 2) \cdot 4 \\ &= 18 \cdot 9 - 40 \cdot 4 \\ &= (58 - 40 \cdot 1) \cdot 9 - 40 \cdot 4 \\ &= 58 \cdot 9 - 40 \cdot 13 \\ &= 58 \cdot 9 - (156 - 58 \cdot 2) \cdot 13 \\ &= 58 \cdot 35 - 156 \cdot 13. \end{aligned}$$

La identidad de Bézout queda como sigue:

$$2 = 156 \cdot (-13) + 58 \cdot 35.$$

Si permitimos divisiones con resto negativo:

$$\begin{aligned} -18 &= 156 - 58 \cdot 3, \\ 4 &= 58 - (-18) \cdot (-3), \\ 2 &= -18 - 4 \cdot (-5), \end{aligned}$$

luego

$$\begin{aligned} 2 &= -18 - 4 \cdot (-5) \\ &= -18 - (58 - (-18) \cdot (-3)) \cdot (-5) \\ &= (-18) \cdot 16 - 58 \cdot (-5) \\ &= (156 - 58 \cdot 3) \cdot 16 - 58 \cdot (-5) \\ &= 156 \cdot 16 - 58 \cdot 43. \end{aligned}$$

Obtenemos así otra identidad de Bézout:

$$2 = 156 \cdot 16 + 58 \cdot (-43).$$

En particular observamos que los coeficientes de la identidad de Bézout no son únicos. De hecho, puedes comprobar que si $a \neq 0 \neq b$ hay infinitas posibilidades.

Teorema 3.8.10. (de Euclides) *Si* $a, b, c \in \mathbb{Z}$ *son tales que* $c|ba$ *y* $\text{mcd}(c, a) = 1$ *entonces* $c|b$.

Demostración. Tomamos una identidad de Bézout $1 = a\alpha + c\beta$ y multiplicamos por b, $b = ba\alpha + bc\beta$. Como $c|ab$ y obviamente $c|bc$ deducimos que $c|b$. □

Definición 3.8.11. Dados dos enteros a y b, diremos que $m \in \mathbb{Z}$ es un **múltiplo común mínimo** de a y b y denotaremos $m = \text{mcm}(a, b)$, si verifica las siguientes propiedades:

1. $a|m$ y $b|m$.
2. Si m' es tal que $a|m'$ y $b|m'$ entonces $m|m'$.

Lemma 3.8.12. *Dados $a, b \in \mathbb{Z}$, alguno de ellos no nulo, si denotamos $d = \text{mcd}(a, b)$, los enteros $\frac{a}{d}$ y $\frac{b}{d}$ son coprimos.*

Demostración. Consideramos la identidad de Bézout $d = a\alpha + b\beta$. Podemos dividir por d y queda

$$1 = \frac{a}{d}\alpha + \frac{b}{d}\beta.$$

Sea $d' = \text{mcd}(\frac{a}{d}, \frac{b}{d})$. Como $d'|\frac{a}{d}$ y $d'|\frac{b}{d}$, d' también divide al término de la derecha, así que $d'|1$, luego $d' = \pm 1$. □

Proposición 3.8.13. *Dados $a, b \in \mathbb{Z}$, alguno de ellos no nulo, si denotamos $d = \text{mcd}(a, b)$, $\frac{ab}{d} = \text{mcm}(a, b)$.*

Demostración. Como $d|a$ y $d|b$,

$$m = \frac{ab}{d} = \frac{a}{d}b = a\frac{b}{d},$$

luego $a|m$ y $b|m$. Supongamos que $a|m'$ y $b|m'$. Entonces $m' = ar = bs$ para ciertos $r, s \in \mathbb{Z}$, luego

$$d\frac{a}{d}r = d\frac{b}{d}s.$$

Podemos cancelar $d \neq 0$, ya que a o b es no nulo, así que

$$\frac{a}{d}r = \frac{b}{d}s.$$

Como $\frac{a}{d}$ divide al término de la derecha y es coprimo con $\frac{b}{d}$, entonces, por el teorema de Euclides, $\frac{a}{d}|s$, luego

$$m = b\frac{a}{d} \mid bs = m'.$$

□

Corolario 3.8.14. *Dados $a, b \in \mathbb{Z}$ cualesquiera,* $\mathrm{mcm}(a, b)$ *existe.*

Demostración. Ya lo hemos probado si a o b no es nulo. Es fácil comprobar a partir de la definición que $\mathrm{mcm}(0, 0) = 0$. □

3.9. Primos

Definición 3.9.1. Un entero $p \in \mathbb{Z}$ es **primo** si y solo si $p \neq \pm 1$ y p solo es divisible por $\pm p$ y por ± 1.

Observación 3.9.2. Observa que el 0 no es primo. Como la relación divisibilidad es independiente de signos, un entero p es primo si y solo si $-p$ es primo.

Proposición 3.9.3. *Dados dos enteros $a, p \in \mathbb{Z}$ con p primo, si $p \nmid a$ entonces* $\mathrm{mcd}(a, p) = 1$.

Demostración. Sea $d = \mathrm{mcd}(a, p)$. Como $d|p$, $d = \pm p$ o ± 1, pero $d|a$, así que $d \neq \pm p$. Sabemos que $p \neq \pm 1$, luego $d = 1$. □

Corolario 3.9.4. *Si $a, b, p \in \mathbb{Z}$ son tales que p es primo, $p|ba$ y $p \nmid a$, entonces $p|b$.*

Proposición 3.9.5. *Un entero no nulo $n \in \mathbb{Z}$ no es primo si y solo si se descompone como $n = n_1 n_2$ con $n_1, n_2 \neq \pm 1$.*

Demostración. $\Leftarrow$ Supongamos por reducción al absurdo que $n = p$ fuera primo. Entonces, como $n_i | n = p$, $n_i = \pm 1, \pm p$. La posibilidad $n_i = \pm 1$ queda descartada por hipótesis, luego $n_i = \pm p$, y por tanto $p = n = \pm p^2$. Esto es una contradicción ya que el primo $p \neq 0, \pm 1$, así que $|p| \geq 2$ y por tanto $|p| < |p|^2$.

$\Rightarrow$ Como n no es primo, es divisible por algún $n_1 \neq \pm 1, \pm n$, $n = n_1 n_2$. Es imposible que $n_2 = \pm 1$ ya que entonces $n_1 = \pm n$. □

Teorema 3.9.6. (fundamental de la aritmética) *Todo entero $n \in \mathbb{Z}$, $n \neq 0, \pm 1$, se descompone como producto finito de primos de manera única salvo orden y signo.*

Demostración. Veamos primero la existencia de la descomposición. Lo haremos por inducción en $|n|$. Si n ya es primo, no hay nada que hacer. Si no $n = n_1 n_2$ para ciertos $n_i \neq \pm 1$, por tanto $|n_i| < |n|$ y, por hipótesis de inducción, cada n_i es un producto finito de primos, así que lo mismo es cierto para $n_1 n_2 = n$.

Veamos ahora la unicidad. Sean

$$p_1 \cdots p_m = q_1 \cdots q_n$$

dos productos de primos. Tenemos que ver que $m = n$ y que, salvo orden, $p_i = \pm q_i$ para cada i. Podemos suponer sin pérdida de generalidad que $m \leq n$. Lo demostraremos por inducción en m.

Comenzamos por el caso $m = 1$, es decir

$$p_1 = q_1 \cdots q_n.$$

En este caso hay que ver que $n = 1$ y que $p_1 = q_1$. Veremos primero por inducción en n que $p_1 | q_i$ para cierto $1 \leq i \leq n$. En efecto,

$$p_1 | q_1 (q_2 \cdots q_n).$$

Si $p_1 | q_1$ entonces ya estaría. Si no, tendríamos que $p_1 | q_2 \cdots q_n$ y por hipótesis de inducción $p_1 | q_i$ para cierto $2 \leq i \leq n$.

Ya hemos visto que $p_1 | q_i$ para cierto $1 \leq i \leq n$. Reordenando el producto de la derecha, podemos suponer que $i = 1$. Como p_1 y q_1 son primos, $p_1 = \pm q_1$. Dividiendo la ecuación por p_1 obtenemos que

$$1 = \pm q_2 \cdots q_n.$$

Como el 1 solo es divisible por ± 1, que no es primo, la única posibilidad es que no haya ningún primo en el producto de la derecha, es decir $n = 1$. Esto termina la prueba del caso $m = 1$.

Supongamos ahora el resultado cierto para $m - 1$. Como

$$p_1 \mid p_1 \cdots p_m = q_1 \cdots q_n,$$

por lo anterior $p_1 = \pm q_i$ y podemos suponer que $i = 1$. Dividimos por p_1 a ambos lados de la igualdad y queda

$$p_2 \mid p_1 \cdots p_m = \pm q_2 \cdots q_n.$$

Por hipótesis de inducción, deducimos que $m - 1 = n - 1$, es decir $m = b$, y que también $p_i = \pm q_i$ para $i \geq 2$. □

Teorema 3.9.7. *Hay infinitos enteros primos.*

Demostración. Por reducción al absurdo, de no ser cierto habría una cantidad finita de primos: $p_1, \ldots, p_n > 1$ y sus opuestos. El entero $n = p_1 \cdots p_n + 1 > 1$ es un producto de primos, así que debe haber algún $p_i | n$, luego $p_i | (n - p_1 \cdots p_n) = 1$, así que $p_i = \pm 1$, con lo que p_i no sería primo. □

Proposición 3.9.8. *Dados dos enteros $a, b \in \mathbb{Z}$ factorizados como productos finitos de potencias de primos,*

$$a = \pm \prod_{\substack{p>0 \\ primo}} p^{r_p},$$
$$b = \pm \prod_{\substack{p>0 \\ primo}} p^{s_p},$$

tenemos que $a|b$ si y solo si $r_p \leq s_p$ para todo p.

Demostración. La implicación $\Leftarrow$ es obvia. Veamos $\Rightarrow$. Supongamos que $b = ac$. Si $c = \pm 1$ no hay nada que probar. En caso contrario, sea

$$c = \pm \prod_{\substack{p>0 \\ \text{primo}}} p^{t_p}$$

la factorización de c como potencia de primos. Entonces,

$$ac = \pm \prod_{\substack{p>0 \\ \text{primo}}} p^{r_p + t_p}.$$

Por la unicidad de las factorizaciones como producto de primos, $s_p = r_p + t_p$ para todo p, así que $r_p \leq s_p$ ya que los exponentes son ≥ 0. □

Corolario 3.9.9. *Dados dos enteros $a, b \in \mathbb{Z}$ factorizados como productos finitos de potencias de primos,*

$$\begin{aligned} a &= \pm \prod_{\substack{p>0 \\ primo}} p^{r_p}, \\ b &= \pm \prod_{\substack{p>0 \\ primo}} p^{s_p}, \end{aligned}$$

tenemos que

$$\begin{aligned} \operatorname{mcd}(a,b) &= \pm \prod_{\substack{p>0 \\ primo}} p^{\min(r_p,s_p)}, \\ \operatorname{mcm}(a,b) &= \pm \prod_{\substack{p>0 \\ primo}} p^{\max(r_p,s_p)}. \end{aligned}$$

Demostración. El enunciado sobre el divisor común maximo es consecuencia de la proposición anterior, y sobre el múltiplo común mínimo se deduce de que $\operatorname{mcm}(a,b) = ab/\operatorname{mcd}(a,b)$. □

3.10. Congruencias

Definición 3.10.1. Dados tres enteros $a, b, n \in \mathbb{Z}$, decimos que a es **congruente** con b módulo n, y lo denotamos $a \equiv b \bmod n$, si $\bar{a} = \bar{b}$ en $\mathbb{Z}/(n)$, es decir, si $n|(a-b)$.

Proposición 3.10.2. *Dados $a, b, n \in \mathbb{Z}$, la ecuación $ax \equiv b \bmod n$ tiene solución si y solo si $\operatorname{mcd}(a,n)$ divide a b.*

Demostración. Denotemos $d = \operatorname{mcd}(a,n)$.

$\Rightarrow$ Supongamos que $c \in \mathbb{Z}$ es una solución. Entonces $n|(ac-b)$, es decir, $ac - b = ne$ para cierto entero e. Por tanto $d|(ac-ne) = b$.

$\Leftarrow$ Por hipótesis $b = dc$ para cierto $c \in \mathbb{Z}$. Tomamos una identidad de Bézout $d = a\alpha + n\beta$, la multiplicamos por c, $b = dc = a\alpha c + n\beta c$ y observamos que al proyectar a $\mathbb{Z}/(n)$ obtenemos $\bar{b} = \overline{a\alpha c}$, así que $x = \alpha c$ es una solución. □

Teorema 3.10.3. (chino del resto) *Dados enteros $m_1, \dots, m_n \geq 1$ coprimos dos a dos y $a_1, \dots, a_n \in \mathbb{Z}$ cualesquiera, el siguiente sistema de ecuaciones en congriencias tiene solución:*

$$\begin{array}{rcll} x & \equiv & a_1 & \text{mód } m_1, \\ & \vdots & & \\ x & \equiv & a_n & \text{mód } m_n. \end{array}$$

Es más, si $c \in \mathbb{Z}$ es una solución entonces el conjunto de todas sus soluciones es la clase $\bar{c} \in \mathbb{Z}/(m_1 \cdots m_n)$.

Demostración. Denotamos $M = m_1 \cdots m_n$ y $M_i = M/m_i$. Al ser los $m_i > 1$, factorizan de manera no trivial como producto de primos. Como $\text{mcd}(m_i, m_j) = 1$ si $i \neq j$, en la factorización de m_i y m_j no aparecen primos comunes, así que tampoco aparecen en la factorizacion de m_i y M_i, luego $\text{mcd}(m_i, M_i) = 1$. Tomamos identidades de Bézous para estos últimos,

$$m_i\alpha_i + M_i\beta_i = 1.$$

Veamos que

$$c = \sum_{j=1}^{n} a_j M_j \beta_j$$

es una solución. En efecto, $M_j \equiv 0 \bmod m_i$ para todo $j \neq i$ y, en virtud de la identidad de Bézout, $M_i\beta_i \equiv 1 \bmod m_i$, así que $c \equiv a_i \bmod m_i$.

Veamos que el conjunto de todas las soluciones del sistema es la clase de c módulo M. Es decir, que c' es una solución del sistema si y solo si $c \equiv c' \bmod M$.

$\Leftarrow$ Si $c \equiv c' \bmod M$ entonces $c \equiv c' \bmod m_i$ para todo i ya que $m_i | M$, por tanto c' también es solución.

$\Rightarrow$ Si c' es otra solución del sistema, entonces $c - c' \equiv 0 \bmod m_i$ para todo i, es decir $m_i | (c - c')$ para todo i, así que $c - c'$ es divisible por el múltiplo común mínimo de los m_i. Como son coprimos dos a dos, este múltiplo común mínimo es M, por tanto $c \equiv c' \bmod M$. □

Proposición 3.10.4. *Dados dos enteros coprimos m y n, tenemos un isomorfismo de anillos*

$$\begin{array}{ccc} \dfrac{\mathbb{Z}}{(mn)} & \xrightarrow{\cong} & \dfrac{\mathbb{Z}}{(m)} \times \dfrac{\mathbb{Z}}{(n)}, \\ \bar{x} & \mapsto & (\bar{x}, \bar{x}). \end{array}$$

Demostración. El único homomorfismo existente

$$f\colon \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{(m)} \times \frac{\mathbb{Z}}{(n)}$$

ha de satisfacer $f(1) = (\bar{1}, \bar{1})$, por tanto, como f preserva sumas, es fácil ver que $f(x) = (\bar{x}, \bar{x})$ para cualquier entero positivo x. Es más, $f(0) = (\bar{0}, \bar{0})$ por ser f un homomorfismo de anillos, y $f(x) = (\bar{x}, \bar{x})$ también para enteros negativos ya que f preserva opuestos.

El homomorfismo f es sobreyectivo. En efecto, dado un par $(\bar{a}, \bar{b}) \in \frac{\mathbb{Z}}{(m)} \times \frac{\mathbb{Z}}{(n)}$, cualquier solución de

$$\begin{aligned} x &\equiv a \mod m, \\ x &\equiv b \mod n, \end{aligned}$$

satisface $f(x) = (\bar{a}, \bar{b})$ por definición, y este sistema de ecuaciones en congruencias posee soluciones por el teorema chino del resto.

El núcleo de f es el conjunto de soluciones del siguiente sistema de ecuaciones en conrguencias

$$\begin{aligned} x &\equiv 0 \mod m, \\ x &\equiv 0 \mod n, \end{aligned}$$

En virtud del teorema chino, este conjunto es la clase del 0 en $\mathbb{Z}/(mn)$, es decir, el ideal (mn). Por tanto, el primer teorema de isomorfía para homomorfismo de anillos nos dice que el homomorfismo del enunciado está bien definido y es un isomorfismo,

$$\begin{array}{rccc} \bar{f}\colon & \dfrac{\mathbb{Z}}{(mn)} & \xrightarrow{\cong} & \dfrac{\mathbb{Z}}{(m)} \times \dfrac{\mathbb{Z}}{(n)}, \\ & \bar{x} & \mapsto & (\bar{x}, \bar{x}). \end{array}$$

□

Definición 3.10.5. Dado $n \in \mathbb{Z}$, denotamos

$$U_n = \left(\frac{\mathbb{Z}}{(n)}\right)^{\times}$$

al grupo de las unidades del anillo $\mathbb{Z}/(n)$. La **función ϕ de Euler** $\phi\colon \mathbb{Z} \to \mathbb{N}$, también llamada **indicatriz**, se define como $\phi(n) = |U_n|$.

Como los ideales $(-n) = (n)$ coinciden $\phi(-n) = \phi(n)$.

El siguiente resultado es un corolario de la proposición anterior.

Corolario 3.10.6. *Dados dos enteros coprimos m y n, tenemos un isomorfismo de grupos $U_{mn} \cong U_m \times U_n$, en particular $\phi(mn) = \phi(m)\phi(n)$.*

Proposición 3.10.7. *El grupo de las unidades de $\mathbb{Z}/(n)$ es*

$$U_n = \{\bar{a} \mid \mathrm{mcd}(a, n) = 1\} \subset \mathbb{Z}/(n).$$

Demostración. $\Leftarrow$ Si $\mathrm{mcd}(a, n) = 1$, tomamos una identidad de Bézout $1 = a\alpha + n\beta$, la proyectamos a $\mathbb{Z}/(n)$ y obtenemos $\bar{1} = \bar{a}\bar{\alpha} + \bar{n}\bar{\beta} = \bar{a}\bar{\alpha}$, así que $\bar{a}$ es una unidad con inversa $\bar{a}^{-1} = \bar{\alpha}$.

$\Rightarrow$ Sea $\bar{b}$ el inverso de $\bar{a}$. Entonces $\bar{a}\bar{b} = \overline{ab} = \bar{1}$, es decir, $n|(ab-1)$ y por tanto $ab - 1 = nc$ para cierto entero c. Si $d = \mathrm{mcd}(a, n)$ entonces $d|(ab - nc) = 1$, así que $d = 1$. □

Proposición 3.10.8. *Dado un entero primo $p > 0$ y $r \geq 0$, $\phi(p^r) = (p-1)p^{r-1}$.*

Demostración. El anillo $\mathbb{Z}/(p^r)$ tiene p^r elementos. Cada uno de ellos, tiene un único representante $0 \leq a < n$. Para hallar $\phi(p^r)$, tenemos pues que contar los enteros $0 \leq a < n$ coprimos con p^r, es decir, los que no son múltiplos de p. Los enteros $0 \leq b < n$ que sí son múltiplos de p son

$$0p, 1p, 2p, 3p, \ldots, (p^{r-1} - 1)p.$$

De estos hay p^{r-1}, por tanto que no sean múltiplos de p hay $p^r - p^{r-1} = (p - 1)p^{r-1}$. □

Corolario 3.10.9. *Si el entero n factoriza salvo signo como potencia de primos positivos distintos del siguiente modo $n = \pm p_1^{r_1} \cdots p_m^{r_m}$ entonces*

$$\phi(n) = (p_1 - 1)p_1^{r_1 - 1} \cdots (p_m - 1)p_m^{r_m - 1}.$$

Demostración. Por inducción en el número m de primos distintos que aparecen en la factorización. Para un solo primo, es la proposición anterior. Si es cierto para $m-1$ primos, usamos que $p_1^{r_1} \cdots p_{m-1}^{r_{m-1}}$ y $p_m^{r_m}$ son coprimos y aplicamos la hipótesis de inducción:

$$\begin{aligned} \phi(m) &= \phi(p_1^{r_1} \cdots p_{m-1}^{r_{m-1}})\phi(p_m^{r_m}) \\ &= (p_1 - 1)p_1^{r_1 - 1} \cdots (p_{m-1} - 1)p_{m-1}^{r_{m-1} - 1}(p_m - 1)p_m^{r_m - 1}. \end{aligned}$$

□

Teorema 3.10.10. (de Euler) *Dados dos enteros coprimos a y n,* $a^{\phi(n)} \equiv 1$ *mod n.*

Demostración. Por las hipótesis, $\bar{a} \in \mathbb{Z}/(n)$ es una unidad, es decir, $\bar{a} \in U_n$, por tanto el orden de $\bar{a}$ en este grupo U_n divide a $|U_n| = \phi(n)$, así que $\bar{a}^{\phi(n)} = \bar{1}$. □

El siguiente corolario se conoce como **teorema pequeño de Fermat**.

Corolario 3.10.11. *Si a es un entero y p es un primo tal que* $p \nmid a$*, entonces* $a^{p-1} \equiv 1$ *mod p.*

Capítulo 4

Polinomios

4.1. Anillos de polinomios

Definición 4.1.1. Dado un anillo R un **polinomio** en una **variable** x con **coeficientes** en R es una expresión de la forma

$$f = f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

donde los **coeficientes** $a_0, \ldots, a_n \in R$ y $n \geq 0$. También se puede denotar como si fuera una serie

$$p(x) = \sum_{n \geq 0} a_n x^n$$

dando por supuesto que **casi todos** los coeficientes son cero, es decir, todos excepto una cantidad finita. El **polinomio trivial** 0 es aquel cuyos coeficientes son todos nulos. El **monomio** de **grado** i de $f(x)$ es $a_i x^i$ y su coeficiente es a_i. El **grado** de un polinomio no trivial $f(x)$ es el mayor $n \geq 0$ tal que su coeficiente de grado n es no nulo $a_n \neq 0$. En este caso decimos que $a_n x^n$ es su **monomio líder** y a_n su **coeficiente líder**. Su **término independiente** es a_0. Un polinomio es **mónico** si su coeficiente líder es $1 \in R$. Los **polinomios constantes** son los de grado 0 y el nulo. El conjunto de los polinomios en una variable x con coeficientes en R se denota $R[x]$.

Observación 4.1.2. El polinomio trivial no tiene asignado ningún grado según esta definición, pero podemos considerar que su grado es $-\infty$, ya que esta convención es compatible con fórmulas posteriores.

Recordemos que el conjunto $R[x]$ es un anillo con la suma y el producto definidos en un ejemplo anterior. Además $R \subset R[x]$ es un subanillo formado por los polinomios constantes. Hemos visto en la prueba de una proposición anterior que si R es un dominio entonces $R[x]$ también y dados $f, g \in R[x]$ se tiene que

$$\deg(fg) = \deg(f) + \deg(g).$$

Además,

$$\deg(f + g) \leq \text{máx}\{\deg(f), \deg(g)\}$$

dándose la igualdad si $\deg(f) \neq deg(g)$, ya que entonces el coeficiente líder de la suma será el mismo que el del polinomio de mayor grado.

Teorema 4.1.3. *Si R es un dominio entonces $R[x]^\times = R^\times$.*

Demostración. Las unidades de R también son unidades de $R[x]$ vistas como polinomios constantes ya que $R \subset R[x]$ es un subanillo. Recíprocamente, si $f \in R[x]$ es una unidad y f^{-1} es su inversa, $ff^{-1} = 1$ entonces

$$\begin{aligned} 0 &= \deg(1) \\ &= \deg(ff^{-1}) \\ &= \deg(f) + \deg(f^{-1}). \end{aligned}$$

Por tanto

$$\deg(f) = -\deg(f^{-1}).$$

Como el grado de un polinomio es siempre ≥ 0, los grados que aparecen a ambos lados de la última ecuación han de ser 0, así que f es una unidad de R. □

En adelante consideraremos casi siempre el anillo de polinomios $k[x]$ con coeficientes en un cuerpo k, que es un dominio. Sus unidades son $k^\times = k \setminus \{0\}$. El grado de un polinomio se puede usar como una medida de tamaño, al igual que

el valor absoluto en los enteros. Esto nos permite realizar divisiones euclídeas en $k[x]$.

Observación 4.1.4. La definición de **divisibilidad** vista en $\mathbb{Z}$ tiene también sentido en $k[x]$ y satisface las mismas propiedades elementales, excepto las que aquí reseñamos. El polinomio 1 es divisible por cualquier unidad, no solo por ± 1. Además, $f|g$ y $g|f$ si y solo si existe una unidad $\alpha \in k^\times$ tal que $f = \alpha \cdot g$. Esta unidad no tiene por qué ser ± 1.

Teorema 4.1.5. (División euclídea) *Dados $D, d \in k[x]$, $d \neq 0$, existen $c, r \in k[x]$ únicos tales que*

- $D = d \cdot c + r$,
- $\deg(r) < \deg(d)$.

Demostración. Probamos primero la existencia. Si $\deg(D) < \deg(d)$ podemos tomar $c = 0$, $r = D$. Supongamos ahora que $\deg(D) \geq \deg(d)$. Denotamos $\deg(D) = n$ y $\deg(d) = m$. Sean y sean $a_n x^n$ y $b_m x^m$ los monomios líderes de D y d, respectivamente. Llamamos

$$c_1 = \frac{a_n}{b_m} x^{n-m}.$$

El polinomio

$$D_1 = D - d \cdot c_1$$

es de grado estrictamente menor que D ya que los monomios líderes de los polinomios de la derecha cancelan al restarlos. Al despejar en la ecuación anterior obtenemos

$$D = d \cdot c_1 + D_1.$$

Si $\deg(D_1) < \deg(d)$ entonces podemos tomar y $r = D_1$. Si $\deg(D_1) \geq \deg(d)$, construimos polinomios c_2 y D_2 por el mismo procedimiento, de modo que

$$D_1 = d \cdot c_2 + D_2,$$

y si fuera necesario continuamos hasta que $\deg(D_n) < \deg(d)$. Este procedimiento termina en un número finito de pasos porque $\deg(D_{i+1}) < \deg(D_i)$ por construcción. Llegados a este punto

$$\begin{aligned} D &= d \cdot c_1 + D_1, \\ D_1 &= d \cdot c_2 + D_2, \\ &\vdots \\ D_{n-1} &= d \cdot c_n + D_n, \end{aligned}$$

podemos tomar $c = c_1 + \cdots + c_n$ y $r = D_n$.

Veamos ahora la unicidad. Supongamos que

$$D = d \cdot c + r = d \cdot c' + r'$$

con $\deg(r), \deg(r') < \deg(d)$. Entonces

$$r - r' = (c' - c)d.$$

Si $c \neq c'$ entonces el polinomio de la derecha tiene grado $\geq \deg(d)$, pero el de la izquierda tiene grado $\leq$ máx$\{\deg(r), \deg(r')\} < \deg(d)$, así que la única posibilidad es que $c = c'$ y por tanto $r = r'$. □

Observación 4.1.6. En las circunstancias anteriores, decimos que D es el **dividendo**, d es el **divisor**, c es el **cociente** y r es el **resto** de la **división euclídea** de D entre d.

Ejemplo 4.1.7. (Una división euclídea)

Sean

$$\begin{aligned} D &= x^5 - \frac{1}{2}x^3 + 2x^2 - 3x + 3, \\ d &= 2x^3 - \frac{2}{3}x^2 + 3x - 1, \end{aligned}$$

dos polinomios de $\mathbb{Q}[x]$. Comenzamos tomando

$$D_1 = D - \frac{1}{2}x^2 \cdot d = \frac{1}{3}x^4 - 2x^3 + \frac{5}{2}x^2 - 3x + 3.$$

Como $\deg(D_1) \geq \deg(d)$, tomamos ahora

$$D_2 = D_1 - \frac{1}{6}x \cdot d = -\frac{17}{9}x^3 + 2x^2 - \frac{17}{6}x + 3.$$

De nuevo $\deg(D_2) \geq \deg(d)$, así que tomamos

$$D_3 = D_2 + \frac{17}{18} \cdot d = \frac{37}{27}x^2 + \frac{37}{18}.$$

Como finalmente $\deg(D_3) < \deg(d)$, podemos tomar

$$\begin{aligned} c &= \frac{1}{2}x^2 + \frac{1}{6}x - \frac{17}{18}, \\ r &= D_3 = \frac{37}{27}x^2 + \frac{37}{18}. \end{aligned}$$

La siguiente proposición se prueba igual que para $\mathbb{Z}$.

Proposición 4.1.8. *Dados $D, d \in k[x]$, $d \neq 0$, $d|D$ si y solo si el resto de la división de D entre d es $r = 0$.*

El siguiente teorema es análogo del que decía que todos los subgrupos de $\mathbb{Z}$ son cíclicos.

Teorema 4.1.9. *Todo ideal $I \subset k[x]$ es principal.*

Demostración. El ideal trivial es principal $\{0\} = (0)$ generado por el 0. Si $I \neq \{0\}$, consideramos el conjunto Sea

$$S = \{\deg(f) \mid 0 \neq f \in I\} \subset \mathbb{Z}.$$

Por el principio de buena ordenación, hay un mínimo $n \in S$. Sea $f \in I$ un polinomio no nulo donde se alcanza el mínimo $\deg(f) = n$. Veamos que $(f) = I$. Por definición, (f) está formado por los múltiplos de f. La inclusión $\subset$ es cierta ya que $f \in I$ y $I \subset k[x]$ es un ideal, por tanto los múltiplos de f están también en I. Para ver $\supset$, tenemos que comprobar que todos los elementos de I son múltiplos de f. Sea $g \in I$. Realizamos la división euclídea de g por f: $g = f \cdot c + r$, $\deg(r) < n$. Si $r = 0$ entonces $g = f \cdot c \in (f)$. Veamos por reducción al absurdo que es imposible que $r \neq 0$. En efecto, en dicho caso $0 \neq r = g - f \cdot c \in I$ pues $g \in I, f \cdot c \in (f) \subset I$ y I es un ideal. Por tanto $\deg(r) \in S$, pero $\deg(r) < n$, y esto contradeciría la minimalidad de n. □

Definición 4.1.10. Una **raíz** de un polinomio $f \in R[x]$ es un elemento $a \in R$ tal que $f(a) = 0$.

Un resultado específico del anillo que nos ocupa es el siguiente.

Corolario 4.1.11. *El elemento $a \in k$ es una raíz de $f \in k[x]$ si y solo si $(x-a)|f$.*

Demostración. Realizamos la división euclídea

$$f(x) = (x-a)\cdot q + r.$$

Como $\deg(r) < \deg(x-a) = 1$, el polinomio r es constante $r \in k$, así que

$$f(a) = (a-a)\cdot q(a) + r = r,$$

y sabemos que $r = f(a) = 0$ si y solo si $(x-a)|f$. □

Observación 4.1.12. En general, los divisores de grado 1 de un polinomio $f \in k[x]$ se corresponden con sus raíces, ya que $(ax-b)|f$, $a \neq 0$, si y solo si $(x-\frac{b}{a})|f$, pues para la relación de divisibilidad es irrelevante el producto por unidades.

El corolario anterior justifica la siguiente definición, que se usará más adelante.

Definición 4.1.13. La **multiplicidad** de una raíz a de $f \in k[x]$ es el máximo $n \geq 1$ tal que $(x-a)^n|f$.

Corolario 4.1.14. *Un polinomio no nulo $f \in k[x]$ de grado n tiene a lo sumo n raíces distintas en k.*

Demostración. Por inducción en $n = \deg(f)$. Si $n = 0$, entonces f es un polinomio constante no nulo, luego no tiene raíces. Sea ahora $n > 0$. Suponemos, por hipótesis de inducción, que todo polinomio de grado $n-1$ tiene a lo sumo $n-1$ raíces distintas. Si f no tuviera raíces no habría nada que probar. Si f tiene una raíz $a \in k$ entonces $f = (x-a)g$ para cierto polinomio g, necesariamente de grado $n-1$. Bastará probar que las raíces de f son las raíces de g y además a. En efecto, $b \in k$ es una raíz de f si y solo si $f(b) = (b-a)g(b) = 0$. Como k es un dominio, para que esto ocurra ha de suceder bien que $g(b) = 0$ o bien que $b = a$. □

Observación 4.1.15. Los conceptos de **divisor común máximo** y **múltiplo común mínimo** en $k[x]$ se definen como en $\mathbb{Z}$ y satisfacen las mismas propieades, excepto las que ahora señalamos. Estos conceptos están bien definidos salvo producto por unidades. Si d y d' son dos divisores comunes máximos de $f, g \in k[x]$ entonces existe $\alpha \in k^\times$ tal que $d' = \alpha \cdot d$, e igual para los múltiplos comunes mínimos. Además, $\mathrm{mcd}(f,g) = \mathrm{mcd}(\alpha \cdot f, \beta \cdot g)$ para todo $\alpha, \beta \in k^\times$. Destacamos que el divisor común máximo se puede calcular medialte el **algoritmo de Euclides** y que satisface la **identidad de Bézout**.

Ejemplo 4.1.16. (Algoritmo de Euclides) Hallemos el divisor común máximo de los siguientes polinomios de $\mathbb{Q}[x]$, consideramos en el ejemplo anterior:

$$\begin{aligned} f &= x^5 - \frac{1}{2}x^3 + 2x^2 - 3x + 3, \\ g &= 2x^3 - \frac{2}{3}x^2 + 3x - 1. \end{aligned}$$

Allí vimos que la división euclídea de f por g es

$$f = g \cdot \left(\frac{1}{2}x^2 + \frac{1}{6}x - \frac{17}{18}\right) + \left(\frac{37}{27}x^2 + \frac{37}{18}\right).$$

Ahora tenemos que dividir g por el resto. Esta división resulta ser exacta,

$$g = \left(\frac{37}{27}x^2 + \frac{37}{18}\right)\left(\frac{54}{37}x - \frac{18}{37}\right) + 0,$$

por tanto el divisor común máximo es el último resto no nulo,

$$\mathrm{mcd}(f,g) = \frac{37}{27}x^2 + \frac{37}{18}$$

y una identidad de Bézout se obtiene simplemente despejando de la primera división euclídea,

$$\frac{37}{27}x^2 + \frac{37}{18} = f \cdot 1 + g \cdot \left(-\frac{1}{2}x^2 - \frac{1}{6}x + \frac{17}{18}\right).$$

podemos conseguir otro divisor común máximo con coeficientes enteros multiplicando por la unidad $\frac{54}{37} \in \mathbb{Q}^\times$,

$$2x^2 + 3 = f \cdot \frac{54}{37} + g \cdot \left(-\frac{27}{37}x^2 - \frac{9}{37}x + \frac{51}{37}\right).$$

4.2. Irreducibles

Definición 4.2.1. Polinomio irreducible Sea $f \in k[x]$. Decimos que f es **primo** si solo es divisible por α y $\alpha \cdot f$, $\alpha \in k^\times$. Decimos que f es **irreducible** si no es nulo y además, si $f = gh$ entonces bien g o bien h es una unidad.

Observación 4.2.2. El 0 no es primo y $f \in k[x]$ es primo si y solo si lo es $\alpha \cdot f$, $\alpha \in k^\times$. Los polinomios de grado 1 son todos irreducibles por la fórmula del grado de un producto. Los resultados elementales sobre primos y divisibilidad que vimos en $\mathbb{Z}$ siguien siendo ciertos en $k[x]$, con alguna salvedad que reflejamos en los enunciados de los resultados siguientes.

Proposición 4.2.3. *Un polinomio $f \in k[x]$ de grado 2 o 3 es irreducile si y solo si no tiene raíces en k.*

Demostración. Demostraremos ambas implicaciones por reducción al absurdo.

$\Rightarrow$ Si $a \in k$ es una raíz de f entonces $f = (x-a)g$, luego $2 \leq \deg(f) = 1 + \deg(g)$, así que g no puede ser una unidad, pues tendría grado 0, luego f sería reducible.

$\Leftarrow$ Supongamos que f es reducible y por tanto se descompone como $f = gh$, donde g y h no son unidades y por tanto $\deg(g), \deg(h) \geq 1$. Entonces $3 \geq \deg f = \deg g + \deg(h)$, por tanto bien $\deg(g) = 1$ o bien $\deg(h) = 1$, así que f tiene alguna raíz en k. □

Proposición 4.2.4. *Un polinomio no nulo $f \in k[x]$ es primo si y solo si es irreducible.*

Demostración. $\Rightarrow$ Si $f = gh$, como $f|gh$ entonces $f|g$ o $f|h$. Como los papeles de g y h son intercambiables, podemos suponer que $f|g$, es decir $g = fc$. Entonces $f = gh = fch$. Como f no es nulo, el resto de polinomios tampoco. Tenemos que $\deg(f) = \deg(f) + \deg(c) + \deg(h)$. Al ser el grado de un polinomio no nulo ≥ 0 deducimos que $\deg(c) = \deg(h) = 0$. Es decir, h es una constante no nula, y por tanto una unidad.

$\Leftarrow$ Supongamos que $g|f$, es decir, $f = gc$ para cierto $c \in k[x]$. Como f no es nulo, g y c tampoco. Si $\deg(g) = 0$ entonces g es una constante no nula, es decir

una unidad. Si $\deg(g) = \deg(f)$ entonces c es una unidad, $c \in k^\times$, por el mismo argumento, así que $g = c^{-1}f$. Queda por analizar qué ocurre si $0 < \deg(g) < \deg(f)$. Como $\deg(f) = \deg(g) + \deg(c)$, entonces también $0 < \deg(c) < \deg(f)$, por lo que g y c no serían unidades. Esto contradeciría la irreducibilidad de f. □

El siguiente teorema se prueba igual que para $\mathbb{Z}$, reemplazando el valor absoluto por el grado.

Teorema 4.2.5. (fundamental de la aritmética) *Todo polinomio no constante de $k[x]$ se descompone como producto finito de polinomios irreducibles de manera única salvo orden y producto por unidades.*

Corolario 4.2.6. *Todo polinomio no constante de $k[x]$ se descompone como producto de una unidad y una cantidad finita de polinomios mónicos irreducibles de manera única salvo orden.*

Demostración. Basta tomar una factorización dada por el teorema anterior y sacar factor común todos los coeficientes líderes. □

La demostración del siguiente teorema también es igual que su versión entera.

Teorema 4.2.7. *En $k[x]$ hay infinitos polinomios mónicos irreducibles.*

Si k es infinito, los polinomios $x - a$, $a \in k$, son un conjunto infinito de irreducibles, pero el teorema es también cierto cuando k es finito.

4.3. Coeficientes complejos y reales

Teorema 4.3.1. (fundamental del álgebra) *Todo polinomio $f \in \mathbb{C}[x]$ de grado positivo tiene una raíz en $\mathbb{C}$.*

Corolario 4.3.2. *Los polinomios irreducibles de $\mathbb{C}[x]$ son los de grado* 1.

Demostración. Sabemos que los polinomios de grado 1 son irreducibles. Si f es de grado > 1 y a es una raíz de f entonces $f = (x - a)g$. Como $\deg(f) = \deg(x -$

$a) + \deg(g) = 1 + \deg(g)$ entonces $\deg(g) \geq 1$, así que ni $x - a$ ni g son unidades, por lo que f no es irreducible. □

Corolario 4.3.3. *Todo polinomio $f \in \mathbb{C}[x]$ de grado $n > 0$ factoriza de manera única como*

$$f = b \prod_{i=1}^{n} (x - a_i)$$

donde $a_i, b \in \mathbb{C}$, $b \neq 0$.

Observa que $\mathbb{R}[x] \subset \mathbb{C}[x]$ pues $\mathbb{R} \subset \mathbb{C}$. Esto nos permite hablar de raíces complejas de polinomios con coeficientes reales.

Proposición 4.3.4. *Si $a \in \mathbb{C}$ es una raíz de $f \in \mathbb{R}[x]$ entonces su conjugado $\bar{a}$ también. Además, ambas tienen la misma multiplicidad.*

Demostración. Consideramos el homomorfismo de anillos $c\colon \mathbb{C}[x] \to \mathbb{C}[x]$ definido como

$$c(a_n x^n + \cdots + a_0) = \bar{a}_n x^n + \cdots + \bar{a}_0.$$

Observa que c se comporta como la identidad sobre $\mathbb{R}[x]$. Si a es raíz de f entonces $(x-a)|f$ en $\mathbb{C}[x]$. Como c es un homomorfismo, esto implica que $x - \bar{a} = c(x - a)|c(f) = f$. Esto demuestra que $\bar{a}$ es raíz de f.

Análogamente se demuestra que si $(x - a)^n|f$ entonces $(x - \bar{a})^n|f$, por tanto la multiplicidad de $\bar{a}$ es $\geq$ que la de a. Como esto vale para cualquier a y $\bar{\bar{a}} = a$, deducimos la otra desigualdad. □

Proposición 4.3.5. *Todo polinomio en $\mathbb{R}[x]$ de grado > 0 factoriza de manera única como producto de un escalar no nulo y polinomios irreducibles de grados 1 y 2.*

Demostración. Tomamos la descomposición en $\mathbb{C}[x]$,

$$f = b \prod_{i=1}^{n} (x - a_i).$$

Agrupamos los factores de grado 1 correspondientes a raíces complejas conjugadas

$$(x - a)(x - \bar{a}) = x^2 - 2\,\mathrm{Re}(a)x + |a|^2.$$

Este es un polinomio mónico de grado 2 en $\mathbb{R}[x]$ sin raíces reales, por tanto irreducible. El resultado es la descomposición deseada, que sabemos que es única. □

Corolario 4.3.6. *Los polinomios irreducibles en $\mathbb{R}[x]$ son los de grado 1 y los de grado 2 sin raíces en $\mathbb{R}$.*

4.4. Coeficientes enteros y racionales

Las nociones de divisibilidad e irreducibilidad tienen también sentido en $\mathbb{Z}[x]$. En este apartado estudiaremos cómo se relacionan estos aspectos en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$ y veremos algunos criterios sencillos de irreducibilidad en $\mathbb{Z}[x]$.

Teorema 4.4.1. (Ruffini) *Si un polinomio $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ tiene una raíz racional, $\frac{a}{b}$ en forma reducida, entonces $a|a_0$ y $b|a_n$*

Demostración. Sabemos que

$$0 = f\left(\frac{a}{b}\right) = a_n\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_{n-1}\frac{a}{b} + a_0.$$

Multiplicamos por b^n, &0 $= a_n a^n + a_{n-1}a^{n-1}b + \cdots + a_1 a b^{n-1} + a_0 b^n$\$ y deducimos las dos condiciones de divisibilidad el enunciado despejando primero el último sumando y luego el primero. □

Definición 4.4.2. Un polinomio no nulo $f = f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ es **primitivo** si el divisor común máximo de sus coeficientes es 1, es decir, si no existe ningún primo $p \in \mathbb{Z}$ tal que $p|a_i$ para todo $1 \leq i \leq n$.

Los únicos polinomios constantes primitivos son ± 1.

Lemma 4.4.3. *Dado $f = f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ no nulo existe una constante $c \in \mathbb{Q}$, llamada **contenido**, y un polinomio primitivo $f_0(x) \in \mathbb{Z}[x]$ tal que*

$$f(x) = c \cdot f_0(x).$$

Además c y $f_0(x)$ son únicos salvo signo. Denotaremos $c = \mathrm{cont}(f)$.

Demostración. Veamos la existencia. Podemos quitar denominadores de los coeficientes de $f(x)$ multiplicando por una constante $d \in \mathbb{Z}$ no nula,

$$d \cdot f(x) \in \mathbb{Z}[x].$$

Si e es el divisor común máximo de los coeficientes de $d \cdot f(x)$ vemos que podemos tomar

$$\begin{aligned} f_0 &= \frac{d}{e} \cdot f(x), \\ c &= \frac{e}{d}. \end{aligned}$$

Probemos ahora la unicidad. Supongamos que $c \cdot f_0(x) = c' \cdot f_0'(x)$ siendo $f_0(x), f_0'(x) \in \mathbb{Z}[x]$ primitivos. Podemos además suponer sin pérdida de generalidad que $c, c' \in \mathbb{Z}$, multiplicando por un denominador común si fuera necesario. Como el divisor común máximo de los coeficientesde $f_0(x)$ es 1, el divisor común máximo de los coeficientes de $c \cdot f_0(x)$ es c. Análogamente el divisor común máximo de los coeficientes de $c' \cdot f_0'(x)$ es c'. Por la unicidad del divisor común máximo, c y c' son asociados, es decir $c' = u \cdot c$ donde $u \in \mathbb{Z}$ es una unidad. Por tanto, por la propiedad cancelativa, $f_0(x) = u \cdot f_0'(x)$. □

Observación 4.4.4. Si el contenido de un polinomio $f(x) \in \mathbb{Q}[x]$ está en $\mathbb{Z}$ entonces $f(x) \in \mathbb{Z}[x]$. Recíprocamente, el contenido de un polinomio $f(x) \in \mathbb{Z}[x]$ es el divisor común máximo de sus coeficientes, en particular $\text{cont}(f) \in \mathbb{Z}$. Es más, dada una constante $a \in \mathbb{Z}$ tenemos que $a | f(x)$ si y solo si $a | \text{cont}(f)$. Un polinomio $f(x) \in \mathbb{Z}[x]$ es primitivo si y solo si $\text{cont}(f) = 1$.

Teorema 4.4.5. (Lema de Gauss) *El producto de polinomios primitivos en $\mathbb{Z}[x]$ es primitivo.*

Demostración. Dado un primo $p \in \mathbb{Z}$, consideramos el homomorfismo de **reducción módulo** p

$$\phi_p \colon \mathbb{Z}[x] \longrightarrow (\mathbb{Z}/(p))[x]$$

definido en las constantes como $\phi_p(a) = \bar{a}$, $a \in \mathbb{Z}$, tal que $\phi_p(x) = x$. Es decir,

$$\phi_p(a_n x^n + \cdots + a_1 x + a_0) = \bar{a}_n x^n + \cdots + \bar{a}_1 x + \bar{a}_0.$$

El homomorfismo ϕ_p consiste simplemente en reducir los coeficientes módulo (p). En particular $f \in$
mathbbQerϕ_p si y solo si p divide a todos los coeficientes de f. Por tanto $f \in \mathbb{Z}[x]$ es primitivo si y solo si $\phi_p(f) \neq 0$ para todo $p \in \mathbb{Z}$ primo. Si $f, g \in \mathbb{Z}[x]$ son primitivos entonces

$$\phi_p(f \cdot g) = \phi_p(f) \cdot \phi_p(g) \neq 0$$

para todo $p \in \mathbb{Z}$ primo ya que $(\mathbb{Z}/(p))[x]$ es un dominio. Es decir, $f \cdot g$ también es primitivo. □

Corolario 4.4.6. *Dados* $f, g \in \mathbb{Q}[x]$ *tenemos que* $\operatorname{cont}(f \cdot g) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$.

Demostración. Tomamos $f, g \in \mathbb{Q}[x]$ y los descomponemos

$$\begin{aligned} f &= c \cdot f_0, \\ g &= d \cdot g_0, \end{aligned}$$

con $c, d \in \mathbb{Q}$ y $f_0, g_0 \in \mathbb{Z}[x]$ primitivos. Entonces

$$f \cdot g = (c \cdot d) \cdot (f_0 \cdot g_0).$$

Como $f_0 \cdot g_0$ es primitivo por el Lema de Gauss, esta es una descomposición válida del producto $f \cdot g$, así que $c \cdot d$ es su contenido. □

Proposición 4.4.7. *Dados* $f, g \in \mathbb{Z}[x]$*, si* $g|f$ *en* $\mathbb{Q}[x]$ *y* g *es primitivo entonces* $g|f$ *en* $\mathbb{Z}[x]$.

Demostración. Supongamos que $f = g \cdot q$ en $\mathbb{Q}[x]$. Como g es primitivo,

$$\operatorname{cont}(f) = \operatorname{cont}(g) \operatorname{cont}(q) = \operatorname{cont}(q).$$

Como $f \in \mathbb{Z}[x]$ su contenido está en $\mathbb{Z}$, y como este coindice con el de q, entonces $q \in \mathbb{Z}[x]$, por lo que $g|f$ en $\mathbb{Z}[x]$. □

Proposición 4.4.8. *Un polinomio* $f \in \mathbb{Z}[x]$ *no constante es irreducible en* $\mathbb{Z}[x]$ $\Leftrightarrow$ *f es primitivo e irreducible en* $\mathbb{Q}[x]$.

Demostración. $\Leftarrow$ Supongamos que por reducción al absurdo que f no es irreducible en $\mathbb{Z}[x]$. Lo descomponemos como producto de divisores propios $f = gh$ en $\mathbb{Z}[x]$. Si g fuera constante entonces dividiría al contenido de f, que es 1, por tanto g sería una unidad, lo cual entra en contradicción con que sea un divisor propio. Lo mismo ocurriría si h fuera constante. Si g y h no son constantes entonces también son divisores propios de f en $\mathbb{Q}[x]$, pues no podrían ser unidades, luego f no sería irreducible.

mathbbZightarrow Si f no fuera primitivo tampoco sería irreducible en $\mathbb{Z}[x]$ pues su contenido sería un divisor propio. Supongamos por reducción al absurdo que f tiene un divisor propio g en $\mathbb{Q}[x]$. Aquí ser un divisor propio significa que $0 <$ grado de $g <$ grado de f. Multiplicando por una constante no nula de $\mathbb{Q}$ si fuera necesario (por el inverso del contenido), podemos suponer que $g \in \mathbb{Z}[x]$ y es primitivo. Por la proposción anterior g también divide a f en $\mathbb{Z}[x]$ y por tanto es un divisor propio por cuestión de grados. □

Observación 4.4.9. Una constante $a \in \mathbb{Z}$ es irreducible en $\mathbb{Z}[x]$ si y solo si lo es en $\mathbb{Z}$.

Finalmente veremos un par de condiciones suficientes más avanzadas para la irreducibilidad de un polinomio.

Proposición 4.4.10. *Si $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ es un polinomio primitivo de grado $n > 0$, $p \in \mathbb{Z}$ es un primo que no divide a_n y la reducción de f módulo p es irreducible en $(\mathbb{Z}/(p))[x]$, entonces f es irreducible en $\mathbb{Z}[x]$.*

Demostración. Usaremos el homomorfismo $\phi_p \colon \mathbb{Z}[x] \to (\mathbb{Z}/(p))[x]$ de reducción módulo p introducido en la demostración del Lema de Gauss. En general,

$$\text{grado}(\phi_p(f)) \leq \text{grado}(f).$$

La condición sobre a_n equivale a decir que concretamente para el polinomio f del enunciado

$$\text{grado}(\phi_p(f)) = \text{grado}(f).$$

Reduzcamos al absurdo. Si f fuera reducible se descompondría como producto de dos divisores propios $f = gh$. Como f es primitivo, ni g ni h puede ser constante, es decir

$$\text{grado}(g), \text{grado}(h) > 0.$$

Al ser ϕ_p un homomorfismo,

$$\phi_p(f) = \phi_p(g)\phi_p(h).$$

Ninguna de las desigualdades

$$\begin{aligned} \text{grado}(\phi_p(g)) &\leq \text{grado}(g), \\ \text{grado}(\phi_p(h)) &\leq \text{grado}(h), \end{aligned}$$

puede ser estricta ya que de ser así

$$\text{grado}(\phi_p(f)) = \text{grado}(\phi_p(g)) + \text{grado}(\phi_p(h)) < \text{grado}(g) + \text{grado}(h) = \text{grado}(f),$$

pero $\text{grado}(\phi_p(f)) = \text{grado}(f)$. Las dos igualdades de la ecuación anterior son ciertas porque tanto $\mathbb{Z}$ como $\mathbb{Z}/(p)$ son dominios, el segundo por ser p primo. Por tanto,

$$\text{grado}(\phi_p(g)), \text{grado}(\phi_p(h)) > 0$$

y tanto $\phi_p(g)$ como $\phi_p(h)$ serían divisores propios de $\phi_p(f)$, que no sería irreducible. □

Teorema 4.4.11. (Criterio de Eisenstein) *Si $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ es un polinomio primitivo de grado $n > 0$ y $p \in \mathbb{Z}$ es un primo tal que:*

- *p no divide a_n,*
- *p divide a $a_{n-1}, \ldots, a_0$,*
- *p^2 no divide a a_0,*

entonces f es irreducible en $\mathbb{Z}[x]$.

Demostración. Esta demostración transcurre de manera exactamente igual que la anterior hasta la última frase, que no es válida en este caso. A partir de ahí continuamos del siguiente modo. Si $b_0, c_0 \in \mathbb{Z}$ son los términos independientes de g y

h entonces $a_0 = b_0c_0$. Como $p|a_0$ y p es primo, $p|b_0$ o $p|c_0$, pero no puede dividir a ambos a la vez ya que p^2 no divide a a_0. Esto prueba que bien $\phi_p(g)$ o bien $\phi_p(h)$ tiene término independiente no nulo. Por las condiciones del enunciado, $\phi_p(f) = \bar{a}_n x^n$ con $\bar{a}_n \neq 0$. Al ser $\phi_p(f) = \phi_p(g)\phi_p(h)$ un monomio y $\mathbb{Z}/(p)$ es un dominio, también $\phi_p(g)$ y $\phi_p(h)$ han de ser monomios. Como uno de ellos tiene término independiente no nulo, entonces ha de tener grado 0, lo que contradice el cálculo al que se llega en la última ecuación de la demostración anterior. □