TEMA 2

ESTRUCTURAS ALGEBRAICAS

Índice

2.1. Conjuntos

Definición 2.1 (Intuitiva)**.** Un conjunto es una reunión en un todo de determinados objetos bien definidos y diferentes entre sí.

Llamamos *elementos* a los objetos que lo forman.

Para que un conjunto esté bien definido deben darse los siguientes *requisitos*:

- No debe existir ambigüedad en la definición de de los elementos.
- Todos los elementos deben ser diferentes.
- El propio conjunto no puede ser un elemento de sí mismo.
- El orden de definición de sus elementos es intrascendente.

Si a es un elemento del conjunto A, decimos que *a pertenece* a A y lo denotamos por $a \in A$. En caso contrario lo denotamos por $a \notin A$.

Los conjuntos generalmente se definen:

- Por extensión, enumerando uno a uno todos sus elementos, $\{a, b, c, d\}$
- Por comprensión, sus elementos quedan descritos de una forma implícita, $\{x \in \mathbb{N} \mid x \text{ es primo }\}$

Ejemplo 2.2. Los principales conjuntos numéricos ya son conocidos de estudios anteriores. Así, representamos por $\mathbb{N}$ al conjunto de todos los números naturales, $\mathbb{Z}$ a los números enteros, y $\mathbb{Q}$ y $\mathbb{R}$ los números racionales y reales, respectivamente.

Conjunto vacío Lo definimos como el conjunto carente de elementos, es decir, $\emptyset = \{\}$.

Definición 2.3 (Subconjuntos)**.** Decimos que A es un *subconjunto*de B (o que A está *incluído* en B), que representamos por $A \subseteq B$, si se satisface que

$$x \in A \implies x \in B$$

Es decir, todo elemento de A es elemento también de B (no necesariamente al revés).

Proposición 2.4. *Para todo conjunto* A *se cumple* $A \subseteq A$ *y* $\emptyset \subseteq A$*.*

Demostración. Probar que $A \subseteq A$ es (super)evidente por la definición 2.3, puesto que todo elemento de A es de A.

En cuanto a la prueba que $\emptyset \subseteq A$ no es tan evidente, aunque sí es trivial. La dificultad estriba en que no podemos elegir ningún elemento del conjunto vacío para comprobar que está en A. Por eso mismo se razona por *reducción al absurdo*. Si la afirmación fuese falsa, es decir $\emptyset$ no fuese subconjunto de A, entonces, siguiendo la defición 2.3, debe existir un elemento de $\emptyset$ que no estaría en A, y eso ¡es imposible! (o absurdo) porque $\emptyset$ no tiene elementos. $\square$

Nota. La proposición anterior nos dice que todo conjunto tiene al menos estos dos subconjuntos que se denominan *subconjuntos triviales*. Al resto de los subconjuntos de A los llamamos *subconjuntos propios*.

Definición 2.5 (Igualdad)**.** Decimos que $A = B$ si tienen exactamente los mismos elementos, es decir, si:

$$x \in A \Longleftrightarrow x \in B$$

Lo anterior se traduce diciendo que todo elemento de A es elemento de B, y viceversa, todo elemento de B es también elemento de A.

Proposición 2.6 (Principio de doble inclusión)**.** *La igualdad de conjuntos se puede expresar equivalentemente como una doble inclusión:*

$$\boxed{A = B \iff A \subseteq B \text{ y } B \subseteq A}$$

2.1.1. Conjunto de las Partes

Definición 2.7. Dado un conjunto A, llamaremos *partes de* A, $\mathcal{P}(A)$, al conjunto de todos los subconjuntos de A.

Ejercicio 2.8. *Define conjuntos cualesquiera de dos y tres elementos y halla sus conjuntos de las partes.*

Cardinal

Llamamos *cardinal* de un conjunto finito A al número de elementos que lo forman y lo denotamos por $|A|$.

También se define el cardinal de un conjunto infinito. Esto enlaza con los llamados *"números transfinitos"* que quedan fuera del ámbito de este curso.

Proposición 2.9. *Dado un conjunto A, si $|A| = n$, entonces $|\mathcal{P}(A)| = 2^n$.*

Demostración. Cada uno de los n elementos de A tiene 2 posibilidades, puede *estar* o *no estar* en un subconjunto de A. Por tanto el numero de subconjuntos posibles de A será 2^n.

□

2.1.2. Operaciones con conjuntos

Al igual que el $\emptyset$ suponemos la existencia de un conjunto $\mathcal{U}$ que llamaremos *universo o conjunto universal* que es el conjunto que contiene a todos los elementos posibles.

Sean entonces $A, B \subseteq \mathcal{U}$.

- Definimos la *unión* como $A \cup B = \{x \in \mathcal{U} \mid x \in A \text{ o } x \in B\}$.
- Y la *intersección* como $A \cap B = \{x \in \mathcal{U} \mid x \in A \text{ y } x \in B\}$

Definición 2.10. Decimos que A y B son *disjuntos* si $A \cap B = \emptyset$.

Llamamos *complementario* de A al conjunto $\bar{A} = \{x \in \mathcal{U} \mid x \notin A\}$.

Propiedades

Vienen expresadas en el cuadro 2.1. La prueba de algunas de estas propiedades son obvias. Otras se pueden probar usando el principio de doble inclusión (proposición 2.6).

Cuadro 2.1: Propiedades de las operaciones de conjuntos

Ley del doble complemento

$$\bar{\bar{A}} = A$$

Leyes Conmutativas

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

Leyes Asociativas

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

Leyes Distributivas

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

Leyes de Idempotencia

$$A \cup A = A \quad A \cap A = A$$

Leyes de Absorción

$$A \cup (A \cap B) = A \quad A \cap (A \cup B) = A$$

Leyes de Neutralidad

$$A \cup \emptyset = A \quad A \cap \mathcal{U} = A$$

Leyes de Dominación

$$A \cup \mathcal{U} = \mathcal{U} \quad A \cap \emptyset = \emptyset$$

Leyes del complemento

$$A \cup \bar{A} = \mathcal{U} \quad A \cap \bar{A} = \emptyset$$

Leyes de De Morgan

$$\overline{A \cup B} = \bar{A} \cap \bar{B} \quad \overline{A \cap B} = \bar{A} \cup \bar{B}$$

Obsérvese en las propiedades del cuadro 2.1, el llamado *principio de dualidad*. Si en una expresión cambiamos intersecciones por uniones (y viceversa) y conjuntos vacíos por universales (y viceversa), la nueva expresión es igualmente válida o igualmente falsa.

Ejemplo 2.11. Vamos a probar, por doble inclusión, la ley del doble complemento: $\bar{\bar{A}} = A$.

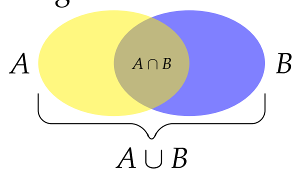
Demostración. (1) Si $x \in \bar{\bar{A}}$, entonces $x \notin \bar{A}$ luego $x \in A$ y (2) si $x \in A$, entonces $x \notin \bar{A}$, luego $x \in \bar{\bar{A}}$. $\square$

Ejercicio 2.12. *Aplicando el principio de dualidad, si probamos una ley por doble inclusión, automáticamente tenemos una prueba de la dual. Aprovecha este principio para probar todas las propiedades.*

Cardinal de la unión

Veremos en el tema 3 (Técnicas de Recuento) que el cardinal de la unión de conjuntos está relacionado con un principio básico de recuento llamado *principio de inclusión-exclusión*. De momento, para dos y tres conjuntos, el cardinal de la unión se puede enunciar del siguiente modo:

- $|A \cup B| = |A| + |B| - |A \cap B|$



Cuando calculamos el número de elementos de la unión $A \cup B$ sumamos los elementos que están en A y B, pero debemos restar los de la intersección porque se han sumado dos veces.

- De igual forma, para tres conjuntos tenemos

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

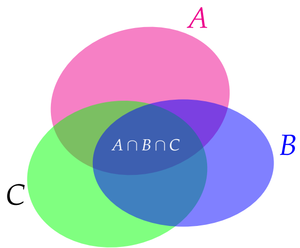


Figura 2.1: Inclusión-exclusión

Ejercicio 2.13. *Comprueba con ejemplos simples la veracidad del principio con dos y/o tres conjuntos sencillos.*

Ejercicio 2.14. *Extiende el principio de inclusión-exclusión para cuatro conjuntos.*

Otras operaciones de conjuntos:

Se usan con frecuencia otras operaciones de conjuntos que se pueden derivar de las descritas anteriormente. Las más importantes son:

Diferencia: $A - B = \{x \in \mathcal{U} \mid x \in A \text{ y } x \notin B\} = A \cap \overline{B}$

Diferencia simétrica: $A \vartriangle B = \{x \in \mathcal{U} \mid x \in A \text{ o (excluyente) } x \in B\} = (A \cup B) - (A \cap B)$

Ejercicio 2.15. *Demuestra que* $A \vartriangle B = (A - B) \cup (B - A)$.

Unión e Intersección generalizadas

Partimos de un conjunto (que puede ser finito o infinito) I al que llamamos conjunto de índices. Con este conjunto podemos diferenciar, a su vez, otros conjuntos A_i donde i es algún elemento de I, y, de esta forma, definir un nuevo conjunto de conjuntos (también llamado familia) $\{A_i \mid i \in I\}$.

Dada una familia de conjuntos, $\{A_i\}_{i\in I}$, definimos su unión y su intersección, respectivamente, como

$$\bigcup_{i\in I} A_i = \{x \in \mathcal{U} \mid \text{ existe } i \in I \text{ con } x \in A_i\}$$

y

$$\bigcap_{i\in I} A_i = \{x \in \mathcal{U} \mid x \in A_i \text{ para todo } i \in I\}$$

Cuando el conjunto de índices es numérico se suele cambiar la notación. Así, por ejemplo

$$\bigcup_{i\in\mathbb{N}} = \bigcup_{i=0}^{\infty}, \qquad \bigcap_{i\in\mathbb{Z}} = \bigcap_{i=-\infty}^{\infty}, \qquad \bigcup_{i\in\{3,\dots,100\}} = \bigcup_{i=3}^{100}$$

En los ejemplos siguientes consideramos los conjuntos $A_i = (i, i+1)$ que son intervalos abiertos de números reales,

$$(i, i+1) = \{x \in \mathbb{R} \mid i < x < i+1\}$$

Ejemplo 2.16. Comprueba que $\displaystyle\bigcup_{i=0}^{\infty}(i, i+1) = (0, \infty) - \mathbb{N}$

Ejercicio 2.17. *Calcula* $\displaystyle\bigcap_{i=0}^{\infty}(i, i+1)$.

2.1.3. Producto cartesiano y relaciones

Sea $\mathcal{U}$ un conjunto universal y $A, B \subseteq \mathcal{U}$.

Definición 2.18. Llamamos *par ordenado* a las listas del tipo (a, b) con $a \in A$ y $b \in B$.

Evidentemente, los pares ordenados no pertenecen al universo $\mathcal{U}$, sino que están en otro universo distinto. En este curso no vamos a entrar en formalizaciones rigurosas y dejamos la comprensión de este hecho a la intuición del alumno.

Igualdad de pares

$$(a, b) = (a', b') \text{ si y sólo si } a = a' \text{ y } b = b'$$

Definición 2.19. Se define el *producto cartesiano* de A por B como

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

Producto cartesiano de más de dos conjuntos El concepto de par ordenado se puede extender. Así se pueden definir las ternas (ordenadas): (a_1, a_2, a_3) y, más generalmente, las n-uplas: $(a_1, a_2, \ldots, a_n)$. También se extiende el producto cartesiano de n conjuntos $A_1 \times A_2 \times \cdots \times A_n$ como el conjunto de todas las n-uplas.

Ejemplo 2.20. Usaremos con mucha frecuencia el conjunto $\mathbb{R}^n$ que está definido como el producto cartesiano $\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$, es decir, todas las n-uplas de números reales.

Relaciones binarias

- Llamamos *relación (o correspondencia)* $\mathcal{R}$ de A en B a cualquier propiedad que asigna a cada elemento de A un subconjunto de B (posiblemente vacío).
- Si "a está relacionado con b" entonces $a \mathcal{R} b$, en caso contrario $a \not\mathcal{R} b$.
- Si $\mathcal{R}$ es una relación de A en B, llamamos *grafo* de $\mathcal{R}$ al subconjunto de $A \times B$ siguiente
$$G_{\mathcal{R}} = \{(a, b) \mid a \mathcal{R} b\}$$
- Inversamente, si $G \subseteq A \times B$, entonces define una única relación $\mathcal{R}_G$ de A en B del siguiente modo
$$a \mathcal{R}_G b \iff (a, b) \in G$$
Es decir, que todo subconjunto del producto cartesiano define una (única) relación cuyo grafo coincide con dicho subconjunto.

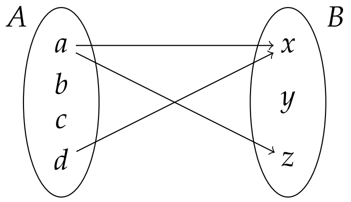
Representación de Relaciones

La relación de $A = \{a, b, c, d\}$ en $B = \{x, y, z\}$ definida por el *grafo*:

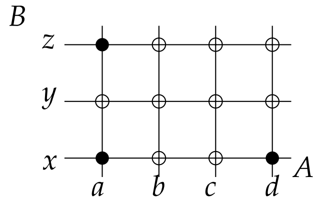
$$G_{\mathcal{R}} = \{(a, x), (a, z), (d, x)\} \tag{2.1}$$

se puede representar de muchas formas, entre otras, las siguientes:

- Diagrama de flechas:



- Diagrama cartesiano:



  Los "puntos negros" representan los elementos de la relación.

- Como una matriz de ceros y unos: $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

  Las filas representan los elementos de A y las columnas los de B, previamente ordenados. Los *unos* indican los elementos del producto cartesiano que pertenecen a la relación y, obviamente, los *ceros* los que no pertenecen.

Obviamente, si el grafo de la relación no es un conjunto finito, las anteriores representaciones no siempre son viables. A veces es posible algún tipo de representación gráfica, principalmente cuando los conjuntos que definen la relación son numéricos.

Indicación: Observa que se corresponde con la gráfica de una circunferencia. Ayúdate de un programa de cálculo si tienes dificultades con la representación.

Ejercicio 2.21. *Usa un diagrama cartesiano para representar la relación entre números reales cuyo grafo es el siguiente:*

$$G_{\mathcal{R}} = \{(x, y) \mid (x+1)^2 + (y-1)^2 = 1\} \subseteq \mathbb{R} \times \mathbb{R}$$

Dominio e Imagen

Desde ahora identificamos completamente una relación $\mathcal{R}$ con su grafo, es decir cuando una relación $\mathcal{R}$ está definida desde el conjunto A hasta el conjunto B, representaremos $\mathcal{R} \subseteq A \times B$, aunque formalmente lo que estamos diciendo es que su grafo es el que está contenido.

Dada una relación $\mathcal{R} \subseteq A \times B$, es decir, $G_{\mathcal{R}} \subseteq A \times B$, según lo anterior, se definen los subconjuntos *dominio* e *imagen o codominio* de $\mathcal{R}$ como

$$\operatorname{Dom} \mathcal{R} = \{x \in A \mid \text{ existe } b \in B \text{ con } x \,\mathcal{R}\, b\}$$
$$\operatorname{Img} \mathcal{R} = \{x \in B \mid \text{ existe } a \in A \text{ con } a \,\mathcal{R}\, x\}$$

Ejercicio 2.22. *En la relación* $\mathcal{R} = \{(a,x),(a,z),(d,x)\}$ *ya vista en* (2.1), *página* 29, *el conjunto* $A = \{a,b,c,d\}$ *y* $B = \{x,y,z\}$ *son los conjuntos inicial y final, respectivamente. ¿Podrías escribir el dominio y la imagen de* $\mathcal{R}$*?*

Ejercicio 2.23. *Escribe el dominio y la imagen de la relación que se define en el ejercicio* 2.21.

Relación identidad Para cualquier conjunto A siempre existe una relación definida

$$\mathcal{I}_A = \{(x,x) \mid x \in A\} \subseteq A \times A \tag{2.2}$$

que llamaremos *relación identidad*. Cuando no hay duda se suprime el subíndice, por tanto $\mathcal{I}$.

2.2. Relaciones internas

Decimos que una relación binaria es interna cuando el conjunto inicial y final coinciden, es decir, $G_{\mathcal{R}} \subseteq A \times A$.

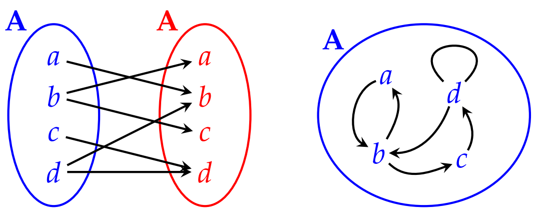


Figura 2.2: Las gráficas representan a la misma relación interna. La segunda es más habitual en relaciones internas.

Propiedades

Algunas propiedades de las relaciones binarias en A son las siguientes:

Reflexiva: Para todo $a \in A$ se tiene $a \,\mathcal{R}\, a$
Antirreflexiva: Para todo $a \in A$ se tiene $a \not\mathcal{R} a$
Simétrica: Para todo $a, b \in A$, si $a \,\mathcal{R}\, b$ entonces $b \,\mathcal{R}\, a$
Antisimétrica: Para todo $a, b \in A$, si $a \,\mathcal{R}\, b$ y $b \,\mathcal{R}\, a$ entonces $a = b$
Transitiva: Para todo $a, b, c \in A$, si $a \,\mathcal{R}\, b$ y $b \,\mathcal{R}\, c$ entonces $a \,\mathcal{R}\, c$
Circular: para todo $a, b, c \in A$ tales que $a \,\mathcal{R}\, b$ y $b \,\mathcal{R}\, c$, se cumple que $c \,\mathcal{R}\, a$.

Ejercicio 2.24. *Observa que la relación identidad* $\mathcal{I}$ *definida en* (2.2) *es una relación interna. Indica cúales de las anteriores propiedades verifica.*

Ejercicio 2.25. *Da ejemplos de relaciones binarias internas en el conjunto* $A = \{a, b, c, d\}$ *que cumplan las propiedades anteriores, por ejemplo:*

- $\mathcal{R} = \{(a, c), (b, c)\}$ *es antirreflexiva.*

2.2.1. Relaciones de equivalencia

Una relación binaria interna se dice que es *de equivalencia* si es reflexiva, simétrica y transitiva.

Ejercicio 2.26. *Da varios ejemplos de relación de equivalencia sobre el conjunto* $A = \{a, b, c, d, e\}$.

Las relaciones de equivalencias están relacionadas con otro concepto llamado *partición*.

Definición 2.27. Dado un conjunto $A \neq \emptyset$, decimos que una familia de subconjuntos no vacíos de A, $\{A_i\}_{i\in I}$, es una *partición de* A si satisfacen las dos condiciones siguientes:

1. $\bigcup_{i\in I} A_i = A$

2. Para todo $i, j \in I$ con $i \neq j$ se tiene que $A_i \cap A_j = \emptyset$. Es decir, son disjuntos por pares.

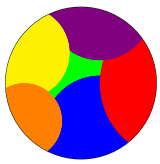


Figura 2.3: Relación de equivalencia y partición.

A cada uno de los subconjuntos A_i se le llama *parte* de A relativa a la partición.

Definición 2.28 (Clases de equivalencia)**.** Si en un conjunto A hay definida una relación de equivalencia $\mathcal{R}$, cada elemento $a \in A$ se puede agrupar en un subconjunto formado por él mismo y todos los elementos que se relacionan con él. A dicho subconjunto de A se le llama *clase de equivalencia* y se representa

$$[a] = \{x \in A \mid a \mathcal{R} x\}$$

Según la anterior definición podría ocurrir que ciertas clases coincidieran, es decir, algunos elementos $a, b \in A$, cumplen $a \neq b$ y, en cambio, $[a] = [b]$. Al ser subconjuntos podemos preguntarnos algo más ¿se pueden solapar las clases?, es decir, ¿pueden existir $a, b \in A$, con $[a] \neq [b]$ y $[a] \cap [b] \neq \emptyset$? La respuesta nos la da el siguiente e importante teorema.

Teorema 2.29. *Sea $\mathcal{R} \subseteq A \times A$ una relación de equivalencia y $a, b \in A$, entonces se tiene:*

1. $a \in [a]$
2. $a \,\mathcal{R}\, b \iff [a] = [b]$
3. $[a] \neq [b] \iff [a] \cap [b] = \emptyset$

Demostración.
1. Es evidente por la propiedad reflexiva. Como $a \,\mathcal{R}\, a \Rightarrow a \in [a]$.
2. Suponemos (hipótesis) que $a \,\mathcal{R}\, b$ (o bien $b \,\mathcal{R}\, a$), entonces, por la propiedad transitiva:

$$\begin{aligned} x \in [a] &\Rightarrow x \,\mathcal{R}\, a \text{ (y } a \,\mathcal{R}\, b \text{, hip.)} \Rightarrow x \,\mathcal{R}\, b \Rightarrow x \in [b] \text{ que prueba } [a] \subseteq [b] \\ x \in [b] &\Rightarrow x \,\mathcal{R}\, b \text{ (y } b \,\mathcal{R}\, a \text{, hip.)} \Rightarrow x \,\mathcal{R}\, a \Rightarrow x \in [a] \text{ que prueba } [b] \subseteq [a] \end{aligned}$$

luego (por la doble inclusión) $[a] = [b]$.
Inversamente, ahora la hipótesis es $[a] = [b]$, entonces, como sabemos (apartado 1) que $a \in [a] \Rightarrow a \in [b]$, luego $a \,\mathcal{R}\, b$.

3. Hipótesis $[a] \neq [b]$. Si $x \in [a] \cap [b] \Rightarrow x \in [a]$ y $x \in [b] \Rightarrow a \,\mathcal{R}\, x$ y $x \,\mathcal{R}\, b \Rightarrow a \,\mathcal{R}\, b$, luego por 2. $[a] = [b]$, que contradice la hipótesis. De aquí no puede haber ningún elemento en la intersección $[a] \cap [b]$, es decir $[a] \cap [b] = \emptyset$.
Hipótesis $[a] \cap [b] = \emptyset$. Sabemos que $[a] \neq \emptyset$ y $[b] \neq \emptyset$, entonces trivialmente $[a] \neq [b]$, puesto que si fuesen iguales no tendrían intersección vacía. $\square$

Corolario 2.30. *Las clases de equivalencia de una relación $\mathcal{R}$ en A establecen una partición de A.*

En la figura 2.3 una relación de equivalencia establece una partición en el círculo (considerado como un conjunto de puntos). Las clases de equivalencia son los colores.

Demostración. Claramente A es la unión de todas las clases de equivalencia, puesto que cada elemento de a está en, al menos, una clase (la propia $[a]$). Por otro lado, el apartado 3 del teorema anterior garantiza que dos clases distintas son disjuntas. $\square$

Nota. El recíproco del corolario anterior también es cierto. Es decir, cualquier partición de un conjunto A define una relación de equivalencia. Dos elementos están relacionados si y solo sí pertenecen a la misma parte (es evidente que esta relación es reflexiva, simétrica y transitiva). Claramente las clases coinciden con las partes.

Definición 2.31 (Conjunto cociente)**.** Dada $\mathcal{R}$ en A, al conjunto formado por las clases de equivalencia, que denotamos por $A/\mathcal{R}$

Ejercicio 2.32. *Establece los conjuntos cocientes de las relaciones dadas en el ejercicio 2.26*

2.2.2. Los enteros modulares.

Vamos a definir los conjuntos de enteros modulares que son conjuntos simples y finitos y que se pueden dotar de operaciones (suma y producto), construidos a partir de una relación de equivalencia (congruencia modular) como conjuntos cocientes. Estos enteros son muy usados en aplicaciones de distintas áreas de las ciencias. A título de ejemplo invito a los estudiantes a investigar el algoritmo RSA muy usado en codificación de comunicaciones (cifradas) entre ordenadores.

Definición 2.33. Dos números enteros $a, b \in \mathbb{Z}$ se dicen que son *congruentes módulo* **n** si y solo si su diferencia es múltiplo de n.

$$a \equiv_n b \iff \text{existe } k \in \mathbb{Z} \text{ tal que } b - a = kn$$

Es fácil comprobar que es una relación de equivalencia en $\mathbb{Z}$.

Ejemplo 2.34. Algunos enteros se relacionan mediante la relación $\equiv_7$ y otros no. Comprueba, por ejemplo, que $3 \equiv_7 -11$. En cambio 3 no se relaciona, por ejemplo, con 1.

Ejercicio 2.35. *Prueba que, efectivamente, la relación $\equiv_n$ es de equivalencia en $\mathbb{Z}$ (para cualquier n).*

Definición 2.36. Representamos por $\mathbb{Z}_n$ al conjunto cociente $\mathbb{Z}/\equiv_n$ definido por la relación de equivalencia "congruencia módulo n".

Los conjuntos $\mathbb{Z}_n$ tienen exactamente n elementos

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-2], [n-1]\}$$

Debes tener en cuenta las siguients observaciones:

1. Las clases tienen infinitos representantes. De hecho, tienen un comportamiento cíclico. Así, por ejemplo, en $\mathbb{Z}_6$, tenemos que

$$\begin{array}{rcl}
\cdots = [-12] = [-6] = & [\mathbf{0}] & = [6] = [12] = [18] = \cdots \\
\cdots = [-11] = [-5] = & [\mathbf{1}] & = [7] = [13] = [19] = \cdots \\
\cdots = [-10] = [-4] = & [\mathbf{2}] & = [8] = [14] = [20] = \cdots \\
& \vdots & \\
\cdots = [-7] = [-1] = & [\mathbf{5}] & = [11] = [17] = [23] = \cdots
\end{array}$$

2. Diremos que una clase está en *forma canónica* si es la forma $[a]$ donde a es un número entero entre 0 y $n-1$ (ambos inclusive).

3. Las clases $[a]$ y $[b]$ son iguales si a y b son congruentes (módulo n).

4. Si a es postivo, la clase $[a]$ es igual a la clase $[r]$ donde r es el resto de dividir a entre n. Así la clase $[r]$ está en forma canónica.

Ejemplo 2.37. Tiene interés el conjunto $\mathbb{Z}_2 = \{[0], [1]\}$. En general, en computación se emplean con mucha frecuencia los $\mathbb{Z}_p$ donde p es un número primo.

Ejercicio 2.38. *Expresa los siguientes enteros modulares de $\mathbb{Z}_{13}$ en forma canónica:*

$$[-11] = \qquad , [101] = \qquad , [-101] = \qquad , [11] =$$

2.2.3. Relaciones de orden

Una relación binaria interna se dice que es *de orden* si es reflexiva, antisimétrica y transitiva.

Por ejemplo, si $A = \{$divisores positivos de $60\}$, la relación binaria en A

$$m \mathcal{R} n \iff m \text{ divide a } n$$

es una relación de orden.

Las relaciones de orden en conjuntos fintos se pueden representar por los llamados *diagramas de Hasse*. El ejemplo anterior se puede representar con el diagrama de Hasse de la figura al margen.

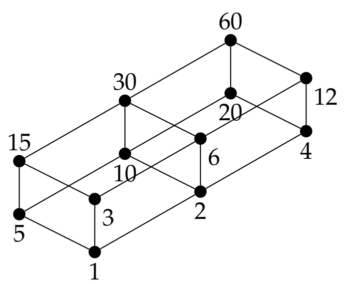


Figura 2.4: Diagrama de Hasse

Orden total y orden parcial

Dos elementos $a, b \in A$ son *comparables* si $a \mathcal{R} b$ o $b \mathcal{R} a$. Una relación de orden es *total* si todos los elementos son comparables entre sí; en otro caso decimos que es *parcial*. El diagrama de la figura 2.4 representa un orden parcial.

2.3. Funciones

Definición 2.39. Decimos que una relación $f \subseteq A \times B$ es una *función* o *aplicación* si satisface las dos condiciones siguientes:

1. $\operatorname{Dom} f = A$
2. Si $(a,b) \in f$ y $(a,c) \in f$ entonces $b = c$

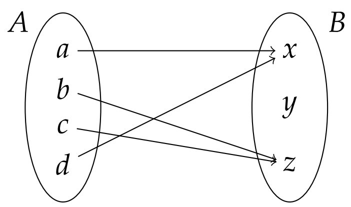


Figura 2.5: Ejemplo de función.

En la figura 2.5 se representa un diagrama que se corresponde con una función, puesto que cumple las dos condiciones de la definición.

Ejercicio 2.40. *Representa gráficamente dos relaciones que* no sean funciones, *una de ellas porque no cumpla la condición 1. y la otra porque no cumpla la condición 2. de la definición 2.39.*

Nota. Un función la representamos de la forma $f\colon A \to B$. Además $(a,b) \in f$ lo escribimos $f(a) = b$ y diremos que *b es imagen de a* o que *a es origen de b*.

Estamos acostumbrados a la anterior notación, que es la usual. A veces se pierde rigurosidad como, por ejemplo, cuando se dice que $f\colon \mathbb{R} \to \mathbb{R}$ definida $f(x) = \frac{1}{x}$ es una función. En realidad, siendo rigurosos, no lo es, puesto que $0 \notin \operatorname{Dom}(f)$. En muchas ocasiones se "sobreentiende" que las funciones están definidas en su dominio.

Así, $f(A) = \operatorname{Img} f$.

Si X es subconjunto de A, representamos $f(X)$ el subconjunto de B de todas las imágenes de los elementos de X, es decir,

$$f(X) = \{f(x) \mid x \in X\}$$

Dado Y subconjunto de B, representamos por $f^{-1}(Y)$ al subconjunto de A de los elementos cuyas imágenes están en Y, es decir,

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$$

Ejemplo 2.41. La relación identidad $\mathcal{I}_A\colon A \to A$ descrita en (2.2), es efectivamente una función que depende únicamente del conjunto A en la que se define. Estas funciones reciben el nombre de *función identidad* en A.

2.3.1. Composición e inversa de Funciones

Observa que ,para funciones, $g \circ f$ se entiende que *primero se aplica* f y posteriormente g.

Si tenemos dos funciones $f\colon A \to B$ y $g\colon B \to C$ podemos construir una nueva función llamada *función compuesta* de f con g a la siguiente:

$$g \circ f\colon A \to C \text{ siendo } (g \circ f)(x) = g(f(x)) \tag{2.3}$$

Propiedades.

1. Cuando una función $f\colon A \to B$ se compone con la función identidad, se queda invariante, es decir
$$f \circ \mathcal{I}_A = f \qquad \text{y} \qquad \mathcal{I}_B \circ f = f \tag{2.4}$$

2. Es fácil probar que la *composición de funciones es asociativa*, es decir, si $f\colon A \to B$, $g\colon B \to C$ y $h\colon C \to D$, se tiene
$$(h \circ g) \circ f = h \circ (g \circ f) \tag{2.5}$$

3. En cambio, la composición *no es conmutativa*, incluso cuando es posible. Por ejemplo, $f\colon A \to A$ y $g\colon A \to A$, en general $f \circ g \neq g \circ f$. Dejamos que el estudiante busque ejemplo de esto.

Función inversa

Si $f\colon A \to B$ es una función, podemos expresarla en forma de relación del siguiente modo:
$$f = \{(a, f(a)) \mid a \in A\} \subseteq A \times B$$
Invirtiendo el orden de los pares obtenemos otra relación
$$f^{-1} = \{(f(a), a) \mid a \in A\} \subseteq B \times A$$
y esta nueva relación f^{-1} NO es necesariamente una función.

Ejercicio 2.42. *Escribe distintos contraejemplos donde no se verifique 1. o 2. de la definición.*

Definición 2.43. Diremos que la función f es *invertible* si la relación f^{-1} es una función.

Teorema 2.44. *Sea $f\colon A \to B$ una función invertible. f^{-1} es la única función que cumple*
$$f^{-1} \circ f = \mathcal{I}_A \qquad f \circ f^{-1} = \mathcal{I}_B$$

Demostración. Efectivamente, por definición de f^{-1}, la imagen del elemento $f(a)$ es el propio a, es decir, $f^{-1}(f(a)) = a$, por tanto $f^{-1} \circ f = \mathcal{I}_A$.

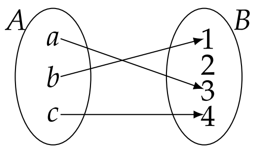
Para probar la otra igualdad, sea b cualquier elemento de B, y sea $a = f^1(b) \in A$, es decir $(b, a) \in f^{-1}$, luego $(a, b) \in f$. Dicho de otra forma $f(a) = b$, o bien $f(f^{-1}(b)) = b$. De aquí $f \circ f^{-1} = \mathcal{I}_B$.

Nos queda comprobar que es única. Sea $g\colon B \to A$ una función cumpliendo ambas igualdades, es decir
$$g \circ f = \mathcal{I}_A \qquad \text{y} \qquad f \circ g = \mathcal{I}_B$$
entonces $(g \circ f) \circ f^{-1} = \mathcal{I}_A \circ f^{-1}$ y por las propiedades (2.4) y (2.5) tenemos $g = f^{-1}$. □

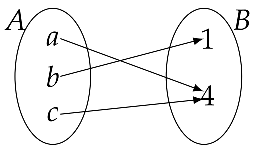
2.3.2. Tipos de funciones

Definición 2.45. Sea $f\colon A \to B$ una función.

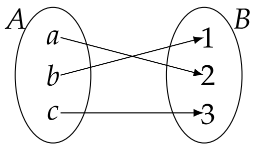
- f es *inyectiva* si y solo si $f(x) = f(x')$ implica que $x = x'$



- f es *sobreyectiva* si y solo si $\mathrm{Im}(f) = B$.



- f es *biyectiva* si y solo si es inyectiva y sobreyectiva.



Teorema 2.46. *Una función es invertible si y solo si es biyectiva.*

Ejercicio 2.47. *Pon dos ejemplos de funciones invertibles discretas y dos ejemplos de funciones invertibles continuas (en $\mathbb{R}$).*

2.4. Estructuras algebraicas

Dado un conjunto A, llamamos **operación binaria interna** o **ley de composición interna** a cualquier función de $A \times A$ en A.

$$*\colon A \times A \to A \qquad *(a,b) = c \qquad a * b = c$$

Llamamos **operación binaria externa** o **ley de composición externa** a cualquier función de alguno de los tipos:

$$*\colon A \times B \to A \qquad *\colon A \times B \to B \qquad *\colon A \times B \to C$$

Las leyes de composición internas pueden tener (o no) unas propiedades y unos elementos notables que exponemos a continuación.

Propiedades

Asociativa

Sea $*$ una operación interna en A. Decimos que $*$ tiene propiedad asociativa si satisface:

$$\text{Para todo } a, b, c \in A, \qquad a * (b * c) = (a * b) * c.$$

Conmutativa

Sea $*$ una operación interna en A. Decimos que $*$ tiene propiedad conmutativa si satisface:

$$\text{Para todo } a, b \in A, \qquad a * b = b * a.$$

Distributivas

Sean $*$ y Δ dos operaciones internas en A.

- Decimos que Δ es distributiva por la izda. respecto de $*$ si satisface:

$$\forall a, b, c \in A, \qquad a \,\Delta\, (b * c) = (a \,\Delta\, b) * (a \,\Delta\, c).$$

- Decimos que Δ es distributiva por la dcha. respecto de $*$ si satisface:

$$\forall a, b, c \in A, \qquad (b * c) \,\Delta\, a = (b \,\Delta\, a) * (c \,\Delta\, a).$$

- Decimos que Δ es distributiva respecto de $*$ si lo es por la izda. y por la dcha.

Ejemplos 2.48.

1. En $\mathbb{Z}$ el producto es distributivo respecto de la suma, pero no al contrario.

2. Si $\mathcal{U}$ es un conjunto, en $\mathcal{P}(\mathcal{U})$ la unión distribuye respecto de la intersección. Al contrario del ejemplo anterior, también la intersección distribuye respecto de la unión.

Elementos Notables

Elemento Neutro

Un elemento $e \in A$ es neutro para $*$ si satisface que

$$\forall a \in A, \quad a * e = e * a = a.$$

Proposición 2.49. *El elemento neutro, si existe, es único.*

Demostración. Si existiesen dos elementos neutros tienen que ser el mismo. Esto prueba la unicidad.

Supongamos e_1 y e_2 dos neutros para la operación $*$. Entonces:

$$\left.\begin{array}{l}\text{Por ser } e_1 \text{ neutro: } e_1 * e_2 = e_2 \\ \text{Por ser } e_2 \text{ neutro: } e_1 * e_2 = e_1\end{array}\right\} \Rightarrow e_1 = e_2$$

□

Ejemplo 2.50. En el conjunto de las matrices cuadradas $n \times n$ la matriz identidad es el elemento neutro para el producto.

Simétrico de un elemento

Sea $*$ una operación interna en A y $e \in A$ el elemento neutro. Decimos que a' *es el simétrico de* a si satisface que

$$\boxed{a * a' = a' * a = e.}$$

El simétrico de un elemento no tiene porqué ser único, salvo para operaciones con la propiedad asociativa.

Si un elemento tiene simétrico decimos que es *simetrizable*. Además, claramente, si a' es un simétrico de a, entonces a es un simétrico de a'.

Proposición 2.51. *Sea $*$ una operación interna con propiedad asociativa.*

1. *Si un elemento es simetrizable, su simétrico es único.*
2. $(a')' = a$
3. *Si $a, b \in A$ son elementos simetrizables, $a * b$ también lo es y su simétrico es $(a * b)' = b' * a'$.*

Demostración.

1. Supongamos que a'_1 y a'_2 son simétricos de a. Entonces:
$$a'_1 = e * a'_1 = (a'_2 * a) * a'_1 = a'_2 * (a * a'_1) = a'_2 * e = a'_2$$
Observa que en la tercera igualdad se hace uso de la asociatividad.
2. Siguiendo la definición de elemento simétrico, a es simétrico de a' al igual que $(a')'$. Por el punto anterior éstos tienen que ser el mismo, es decir $a = (a')'$.
3. Es fácil comprobar que
$$(a * b) * (b' * a') = e$$
y
$$(b' * a') * (a * b) = e$$
y, como el simétrico es único, se tiene $(a * b)' = (b' * a')$. □

Cuando estamos con una operación *suma* al elemento neutro se le suele representar con el símbolo 0, en lugar del símbolo genérico e. Igualmente, cuando la operación es un producto que se suele denominar como "identidad" y se emplea el símbolo 1 y en ocasiones el símbolo I.

En la suma al simétrico se le llama *elemento opuesto* y se representa con el signo *menos*, así el opuesto de a es el elemento $-a$. En el producto, al elemento simétrico de a se le llama *inverso* y se representa como a^{-1}.

Elementos regulares

Sea $*$ una operación interna en A y $c \in A$. Decimos que:

- c es regular por la izquierda si

$$\forall\, a, b \in A, \quad c * a = c * b \Longrightarrow a = b.$$

- c es regular por la derecha si

$$\forall\, a, b \in A, \quad a * c = b * c \Longrightarrow a = b.$$

- Decimos que c es *regular* si lo es por la izquierda y por la derecha

Si todos los elementos de A son regulares, decimos que $*$ satisface la *ley de simplificación*.

Proposición 2.52. *Si $*$ una operación interna en A con propiedad asociativa, todo elemento simetrizable es regular.*

Elementos absorbentes

Sea $*$ una operación interna en A y $c \in A$. Decimos que c es un elemento absorbente si se satisface que:

$$\forall a \in A\,, \quad a * c = c * a = c.$$

Ejemplo 2.53. La matriz $0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$ es un elemento absorbente para el producto de matrices cuadradas.

Ejercicio 2.54. *¿Puede existir más de un elemento absorbente para la misma operación en un conjunto? Justifica la respuesta.*

$(A, *)$	Semigrupo	Monoide	Grupo
Asociativa	•	•	•
Elem. neutro		•	•
Elem. simét.			•
Conmutativa	Semigrupo Conmutativo	Monoide conmutativo	Grupo Abeliano

Cuadro 2.2: Estructuras con una operación binaria.

2.4.1. Estructuras algebraicas con una operación

Las estructuras algebraicas más simples constan de un conjunto con una única operación interna definida sobre él. Las más importantes las describimos en el cuadro 2.2.

Ejemplos 2.55.

1. Para los enteros positivos m y n el conjunto

$$\mathcal{M}_{m\times n} = \{\text{matrices reales de orden } m \times n\}$$

   con la suma, es decir, $(\mathcal{M}_{m\times n}, +)$ es un grupo abeliano.

2. $(\mathcal{M}_{n\times n}, \cdot)$ es un monoide NO conmutativo y no es grupo, puesto que existen elementos que no tienen simétrico, por ejemplo la matriz 0. ¿Existen otros elementos que no tienen simétrico? ¿Podrías poner algún ejemplo para $n = 2$?

Ejercicio 2.56. *¿Qué estructura algebraica tienen los siguientes conjuntos numéricos con la operación suma* $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$ *y* $(\mathbb{Z}^+, +)$*?*

Ejemplos 2.57.

- $(\mathbb{Z}, +)$ es un grupo abeliano.
- $(\mathbb{R} - \{0\}, \cdot)$ es un grupo abeliano.
- El conjunto $S(A)$ de todas las funciones biyectivas en un conjunto A forman un grupo con la operación composición. Este grupo se suele representar con notación multiplicativa $(S(A), \cdot)$ y recibe el nombre de *Grupo Simétrico*.

  Si A es finito con n elementos, entonces el Grupo Simétrico se representa por S_n y tiene $n!$ elementos.

- El conjunto de todas las matrices reales cuadradas de orden n con determinante distinto de cero (invertibles) forman un grupo multiplicativo y recibe el nombre de *Grupo Lineal General* de orden n, que se representa $GL(n)$

- En el conjunto de enteros modulares $\mathbb{Z}_n$ se define la suma de la forma habitual

$$[a] + [b] = [a + b]$$

  Esta suma es una ley de composición interna, puesto que no depende de los representantes de las clases que se elijan. Entonces para cualquier entero positivo n, la estructura $(\mathbb{Z}_n, +)$ *es un grupo abeliano.*

Esto quiere decir que si $[a] = [a']$ y $[b] = [b']$, entonces $[a + b] = [a' + b']$. Prueba este resultado como ejercicio.

Ejercicio 2.58. *En este ejercicio, por comodidad, suprimimos los corchetes de los elementos de $\mathbb{Z}_n$. Completa las siguientes tablas de los grupos.*

$\mathbb{Z}_2$

+	0	1
0		
1		0

$\mathbb{Z}_3$

+	0	1	2
0			
1		2	0
2			

$\mathbb{Z}_6$

+	0	1	2	3	4	5
0						
1						
2						1
3						
4						
5						

2.4.2. Estructuras algebraicas con dos operaciones

En el cuadro 2.3 exponemos las estructuras básicas con dos operaciones. La estructura más simple es el anillo. Verás que todas son propiedades conocidas, excepto el concepto de *divisor de cero* que explicaremos con más detalle más adelante.

Para estas estructuras usamos las notaciones aditiva y multiplicativa.

Anillos

Las propiedades de los anillos vienen expresadas en el cuadro 2.3. Así, $(A, +, \cdot)$ es un anillo si se verifica:

Si, además, el producto tiene neutro, es un *anillo unitario*, y si es conmutativo, es un *anillo conmutativo*.

1. $(A, +)$ es un grupo abeliano.
2. $(A, \cdot)$ es un semigrupo.
3. El producto es distributivo respecto de la suma.

En los anillos se tiene una conocida regla que habéis venido usando desde los estudios primarios.

Teorema 2.59 (Regla de los Signos)**.** *Sea A un anillo. Para todo $a, b \in A$ se cumple*

$(A,+)$	Anillo	Cuerpo
Asociativa	•	•
Conmutativa	•	•
Elem. neutro 0	•	•
Elem. opuesto	•	•
$(A,\cdot)$		
Asociativa	•	•
Distributiva resp. +	•	•
Elem. neutro 1	A. Unitario	•
Conmutativa	A. Conmutativo	•
Elem. inverso para $\neq 0$		•
Ausencia divisores de 0		•

Cuadro 2.3: Estructuras con dos operaciones binarias.

I. $0 \cdot a = a \cdot 0 = 0$

II. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

III. $a \cdot b = (-a) \cdot (-b)$

Demostración.

I. Sabemos que $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$,
luego simplificando en el grupo $(A,+)$ tenemos $a \cdot 0 = 0$.

II. Comprobamos que

$$a \cdot (-b) + (a \cdot b) = a \cdot ((-b) + b) = a \cdot 0 = 0 \Rightarrow a \cdot (-b) = -(a \cdot b)$$

De la misma forma se prueba $(-a) \cdot b = -(ab)$.

III. Es evidente a partir del apartado anterior y del apartado 2 de la proposicion 2.51 que establece $(a')' = a$.

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

□

Ejemplo 2.60 (Anillos de enteros modulares)**.** A los conjuntos $\mathbb{Z}_n$ se les dota de suma y producto

$$[n] + [m] = [n+m]$$
$$[n] \cdot [m] = [nm]$$

y tiene estructura de anillo $(\mathbb{Z}_n, +, \cdot)$.

Ejercicio 2.61. *Construye las tablas de suma y producto de $\mathbb{Z}_6$ y comprueba que es anillo.*

Definición 2.62. Un elemento $a \in A - \{0\}$ es *divisor de cero* si:

$$\text{existe } b \in A - \{0\} \text{ tal que } \; ab = 0 \; \text{ o } \; ba = 0$$

Claramente, si a es divisor de cero también b lo es.

El siguiente resultado caracteriza los divisores de cero de un anillo.

Proposición 2.63. *Sea A un anillo y $a \in A$, $a \neq 0$. Entonces a es un elemento regular para el producto si y solo si no es divisor de cero.*

Demostración. Veamos la primera implicación. Sea a es un elemento regular y supongamos que a es divisor de cero, es decir existe $b \in A, b \neq 0$ tal que, p.e. $a \cdot b = 0 \Rightarrow a \cdot b = a \cdot 0 \Rightarrow b = 0$, que es una contradicción.

Inversamente, si a no es divisor de cero y no fuese regular a la izquierda, por ejemplo, existen $x, y \in A$ distintos tales que $a \cdot x = a \cdot y$, luego $a \cdot (x - y) = 0$. Por tanto, como $x - y \neq 0$ contradice que a no es divisor de cero. $\square$

Corolario 2.64. *Si A es un anillo sin divisores de cero, todos los elementos distintos de 0 son regulares para el producto.*

Demostración. Evidente. $\square$

Ejercicio 2.65. *Comprueba que $\mathbb{Z}_3$, $\mathbb{Z}_5$ y $\mathbb{Z}_7$ no tienen divisores de cero. En cambio los anillos Z_4, $\mathbb{Z}_6$ y $\mathbb{Z}_8$ si tienen.*

Ejemplos 2.66.

1. Los números enteros $(\mathbb{Z}, +, \cdot)$ forman un anillo sin divisores de cero.

2. Los polinomios con coeficientes reales forman otro anillo. Tampoco existen divisores de cero en este anillo

3. Los siguientes conjuntos numéricos racionales $\mathbb{Q}$, reales $\mathbb{R}$ y complejos $\mathbb{C}$, dotados con la suma y el producto son ejemplos de anillos, pero con alguna propiedad muy importante que pasan a llamarse *cuerpos*.

4. Las matrices cuadradas $(\mathcal{M}_{n\times n}, +, \cdot)$ son el ejemplo más importante de estructura de anillo (conmutativo unitario), donde existen divisores de cero.

Ejercicio 2.67. *Pon algún ejemplo de matrices cuadradas de orden $n = 3$ que sean divisores de cero. Es decir, encuentra dos matrices 3×3 no nulas que multiplicadas den la matriz cero.*

Cuerpos

Los cuerpos son las estructuras algebraicas con dos operaciones que más usaremos en este curso. Se puede definir un cuerpo como una estructura $(K, +, \cdot)$ que verifica:

- $(K, +)$ es grupo abeliano.
- $(K - \{0\}, \cdot)$ es también grupo abeliano.
- La operación $\cdot$ es distributiva respecto de $+$.

Daremos las siguientes propiedades de los cuerpos (sin demostración).

Proposición 2.68.

1. *Los cuerpos no tienen divisores de cero.*
2. *En un cuerpo, las ecuaciones $ax = b$ y $xa = b$ con $a \neq 0$ tienen solución única.*

Ejemplos 2.69.

1. Los cuerpos finitos $\mathbb{Z}_p$, donde p es un número primo, se usan en distintas aplicaciones de las matemáticas a las ingenierías, aunque se quedan fuera del ámbito de esta asignatura.
2. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos. El cuerpo más conocido y que más usaremos será el de los números reales $(\mathbb{R}, +, \cdot)$. En este curso vamos a hacer una extensión de dicho cuerpo de los números reales al cuerpo de los números complejos $(\mathbb{C}, +, \cdot)$.

2.5. El cuerpo de los números complejos

Los números reales tienen muchas propiedades agradables. Hay operaciones tales como suma, resta, multiplicación, así como la división por cualquier número real, excepto cero. Hay leyes útiles que regirán estas operaciones como las leyes conmutativa y distributiva. También puede tomar los límites y hacer Cálculo. Pero no se puede tomar la raíz cuadrada de -1 o lo que es lo mismo no puede encontrar una raíz de la ecuación

$$x^2 + 1 = 0. \tag{2.6}$$

La mayoría de vosotros ha oído que hay un ”nuevo"número i (llamada raiz imaginaria) que es una raíz de la ecuación anterior. Es decir, $i^2 + 1 = 0$ o $i^2 = -1$. Vamos a demostrar que cuando el cuerpo de números reales se amplía a un nuevo cuerpo llamado los *números complejos*, que incluye i, no sólo ganamos un número con propiedades interesantes, sino que, además, no se pierde ninguna de las propiedades agradables que hemos tenido antes.

2.5.1. Definiciones y propiedades algebraicas

Hay muchas maneras equivalentes a pensar un número complejo, cada una de las cuales es útil en por derecho propio. Comenzamos con la definición formal de un número complejo. A continuación, interpretaremos esta definición formal en otra más útil y más fácil de trabajar con lenguaje algebraico.

Los números complejos se pueden definir como pares de números reales,

$$\mathbb{C} = \{(x, y) : x, y \in \mathbb{R}\},$$

equipada con la adición

$$\boxed{(x, y) + (a, b) = (x + a, y + b)}$$

y la multiplicación

$$\boxed{(x, y) \cdot (a, b) = (xa - yb, xb + ya).}$$

Estas operaciones binarias en $\mathbb{C}$ son es un extensión de las de $\mathbb{R}$, en el sentido de que los números complejos de la forma $(x, 0)$ se identifican con los números reales y

Podemos pensar que los números reales se incrustan en $\mathbb{C}$ como los números complejos cuya segunda coordenada es cero.

$$(x, 0) + (y, 0) = (x + y, 0) \text{ y } (x, 0) \cdot (y, 0) = (xy, 0).$$

Teorema 2.70. *El conjunto $\mathbb{C}$ antes definido, dotado de las operaciones de suma y producto anteriores tiene una estructura de cuerpo $(\mathbb{C}, +, \cdot)$.*

Además podemos añadir:

- $(0, 0)$ *es el elemento neutro para la suma.*
- $(1, 0)$ *es el elemento neutro para el producto (también llamado unidad).*
- *El opuesto de (x, y) es $(-x, -y)$ (simétrico para la suma).*
- *El inverso (simétrico para el producto) de $(x, y) \neq (0, 0)$ es*

$$\boxed{(x, y)^{-1} = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right).}$$

Si pensamos en el espíritu de nuestra observación sobre la inclusión de $\mathbb{R}$ en $\mathbb{C}$, es decir, de $(x, 0)$ e $(y, 0)$ como la números reales x e y, esto significa que podemos escribir cualquier número complejo (x, y) como lineal combinación de $(1, 0)$ y $(0, 1)$,

$$(x, y) = (x, 0) \cdot (1, 0) + (y, 0) \cdot (0, 1)$$

Así que si le damos a $(0,1)$ un nombre especial i, también llamado unidad imaginaria, entonces el número complejo que que llamábamos (x,y) puede escribirse como

$$x \cdot 1 + y \cdot i,$$

o, más corto, $x + iy$. Esta manera de expresar los números complejos recibe el nombre de *expresión o forma rectangular* o, a veces, expresión o forma binomial.

El número real x se llama la parte real y al número real y parte imaginaria del número complejo $x + iy$, a menudo denotado como

$$\operatorname{Re}(x+iy) = x \text{ e } \operatorname{Im}(x+iy) = y.$$

La manera de expresar un número complejo en parte real y parte imaginaria de También es fácil probar que $i = (0,1)$ es la raiz de de la ecuación (2.6), es decir

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

Teorema 2.71 (Fundamental del Álgebra)**.** *Todo polinomio no constante de grado n tiene n raíces (contando multiplicidad) en $\mathbb{C}$.*

Se dice que $\mathbb{C}$ es algebraicamente cerrado.

La demostración de este teorema requiere una maquinaria importante, curiosamente más del cálculo que del álgebra, por lo que se pospone dicha prueba.

2.5.2. Del álgebra a la geometría y viceversa

La notación (x,y) de los complejos sugiere que se puede pensar en éste como un vector real de dos dimensiones. Al trazar estos vectores en el plano $\mathbb{R}^2$, llamamos al eje x el *eje real* y al eje y el *eje imaginario*. La suma que se definió para los números complejos coincide con la suma de vectores. Pero este parecido acaba con la multiplicación: no hay multiplicación "usual"de dos vectores en $\mathbb{R}^2$ que devuelva otro vector, y, por supuesto, ninguno que esté de acuerdo con nuestra definición de el producto de dos números complejos.

Cualquier vector en $\mathbb{R}^2$ se define por sus dos coordenadas, pero también se determina por su longitud y el ángulo que forma con, por ejemplo, el eje real positivo, vamos a definir estos conceptos más a fondo.

Valor absoluto y argumento. El *valor absoluto (a veces también llamado el módulo)* de $z = x + iy$ es su longitud visto como vector de $\mathbb{R}^2$

$$r = |z| = \sqrt{x^2+y^2} \in \mathbb{R}^+ \cup \{0\}$$

y *un argumento* de $z = x + iy$ es un número $\theta \in \mathbb{R}$ tal que

$$x = r\cos\theta \text{ e } y = r\operatorname{sen}\theta.$$

Un número complejo tiene un número infinito de argumentos, por ejemplo, el número 1= $1 + 0i$ se encuentra en el eje x, y también lo ha hecho el argumento 0, pero podría muy bien decir tiene argumento 2π, 4π, -2π, o $2k\pi$ para cualquier entero k. El número $0 = 0 + 0i$ tiene un módulo 0, y cada número θ es un argumento. Aparte del caso excepcional de 0, para cualquier complejo número z, los argumentos de z todos difieren en un múltiplo entero de 2π.

Para cada número complejo z llamaremos $\arg z$ al conjunto de todos los argumentos. En realidad $\arg : \mathbb{C} \to \mathbb{R}$ es una relación que no es una función. Por convenio, para $z \neq 0$, se establece el *argumento principal* como el (único) argumento θ que pertenece al intervalo $\theta \in (-\pi, \pi]$. Al argumento principal se le suele representar como $\operatorname{Arg} z \colon \mathbb{C}^* \to (-\pi, \pi] \subseteq \mathbb{R}$ que sí es una función.

Representamos $\mathbb{C}^* = \mathbb{C} - \{0\}$.

En la figura 2.7 se puede observar el significado geométrico del módulo y del argumento.

El valor absoluto de la diferencia de dos vectores tiene una interesante interpretación geométrica:

Proposición 2.72. *Sean $z_1, z_2 \in \mathbb{C}$ dos números complejos considerados como vectores en $\mathbb{R}^2$. Si $d(z_1, z_2)$ denota la distancia entre (los extremos de) los dos vectores en $\mathbb{R}^2$ (Véase la Figura 2.6). Entonces*

$$d(z_1, z_2) = |z_1 - z_2| = |z_2 - z_1|$$

Demostración. Sea $z_1 = x_1 + iy_1$ y $z_2 = x_2 + iy_2$. A partir de la geometría sabemos que $d(z_1, z_2) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$ y ésta es justamente la definición de los $|z_1 - z_2|$.

Ya que $(x_1 - x_2)^2 = (x_2 - x_1)^2$ y $(y_1 - y_2)^2 = (y_2 - y_1)^2$, también tenemos $|z_1 - z_2| = |z_2 - z_1|$. Simplemente dice que el vector desde z_1 hasta z_2 tiene la misma longitud que su inversa, el vector desde z_2 hasta z_1. □

La interpretación geométrica de los números complejos en forma de valor absoluto y argumento nos permite dar un significado al producto de complejos:

$$\begin{aligned}(x_1 + iy_1)(x_2 + iy_2) &= (r_1 \cos\theta_1 + ir_1 \operatorname{sen}\theta_1)(r_2 \cos\theta_2 + ir_2 \operatorname{sen}\theta_2) = \\ &= (r_1 r_2 \cos\theta_1 \cos\theta_2 - r_1 r_2 \operatorname{sen}\theta_1 \operatorname{sen}\theta_2) + \\ &\quad + i(r_1 r_2 \cos\theta_1 \operatorname{sen}\theta_2 + r_1 r_2 \operatorname{sen}\theta_1 \cos\theta_2) = \\ &= r_1 r_2 \left(\cos(\theta_1 + \theta_2) + i \operatorname{sen}(\theta_1 + \theta_2)\right).\end{aligned}$$

Observa que se usan las identidades trigonométricas del seno y coseno de la suma.

Por lo tanto el valor absoluto del producto es $r_1 r_2$ y su argumento es $\theta_1 + \theta_2$ (uno de ellos). Geométricamente, estamos multiplicando las longitudes de los dos vectores que representan los dos números complejos, y sumando sus ángulos medidos con respecto al eje x positivo.

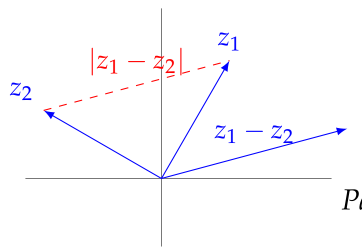


Figura 2.6: El valor absoluto de la diferencia mide la distancia entre dos complejos.

Teniendo en cuenta el cálculo anterior, en principio por abreviar, se introduce una nueva notación (conocida como *fórmula de Euler*)

$$e^{i\theta} = \cos\theta + i \operatorname{sen}\theta.$$

Veremos más adelante que tiene una íntima relación con la *función exponencial compleja*, pero de momento no es más que una notación.

Dejamos como ejercicio para los estudiantes la prueba de las siguientes propiedades

Ejercicio 2.73. *Para cualquier $\theta, \theta 1, \theta 2 \in \mathbb{R}$,*

1. $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$.
2. $\dfrac{1}{e^{i\theta}} = e^{-i\theta}$.
3. $e^{i(\theta+2k\pi)} = e^{i\theta}$.
4. $|e^{i\theta}| = 1$

Teniendo en cuenta la anterior notación diremos que *un número complejo está expresado en forma trigonométrica o forma polar* si se expresa a partir de su valor absoluto r y uno de sus argumentos θ de la siguiente forma $z = re^{i\theta}$.

Para pasar de forma rectangular de complejo $z = x + iy$, que no sea nulo, a su forma polar $z = re^{i\theta}$ y viceversa usamos las igualdades

Conocidos r, θ	Conocidos x, y
$x = r\cos\theta$ $y = r \operatorname{sen}\theta$	$r^2 = x^2 + y^2$ $\tan\theta = \dfrac{y}{x}$, si $x \neq 0$ $\theta = \dfrac{\pi}{2}$, si $x = 0$ e $y > 0$ $\theta = -\dfrac{\pi}{2}$, si $x = 0$ e $y < 0$

Basándose en lo anterior es de muy fácil demostración el siguiente resultado:

Proposición 2.74 (Fórmula de De Moivre)**.** *Para cualquier ángulo θ se tiene:*

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^n = \cos(n\theta) + i\,\mathrm{sen}(n\theta).$$

Ejercicio 2.75. *Utiliza los resultados del ejercicio 2.73 para obtener las fórmulas del ángulo triples:*

1. $\cos 3\theta = \cos^3\theta - 3\cos\theta\,\mathrm{sen}^2\,\theta.$
2. $\mathrm{sen}\,3\theta = 3\cos^2\theta\,\mathrm{sen}\,\theta - \mathrm{sen}^3\,\theta.$

Propiedades geométricas

El cuadrado del valor absoluto de un complejo tiene la buena propiedad

$$|x+iy|^2 = x^2 + y^2 = (x+iy)(x-iy).$$

Esta es una de las muchas razones para dar el proceso de pasar del complejo $z = x+iy$ a $x - iy$ el nombre especial de conjugar z.

Se denota el *complejo conjugado* como

$$\overline{x+iy} = x - iy.$$

Geométricamente, la conjugación z significa que se refleja el vector correspondiente a z con respecto a la eje real. El siguiente ejercicio recoge algunas propiedades básicas del conjugado.

Ejercicio 2.76. *Para cualesquiera $z, z_1, z_2 \in \mathbb{C}$,*

1. $\overline{z_1 \pm z_2} = \overline{z_1} \pm \overline{z_2}.$
2. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}.$
3. $\overline{\left(\dfrac{z_1}{z_2}\right)} = \dfrac{\overline{z_1}}{\overline{z_2}}.$
4. $\overline{\overline{z}} = z.$
5. $|\overline{z}| = |z|.$
6. $|z|^2 = z\,\overline{z}.$
7. $\mathrm{Re}\,z = \frac{1}{2}(z+\overline{z}),$
8. $\mathrm{Im}\,z = \frac{1}{2i}(z-\overline{z}).$
9. $\overline{e^{i\theta}} = e^{-i\theta}.$

El dibujo de la figura 2.7 nos da una idea de un número complejo y su conjugado, así como alguna propiedad de desigualdad geométrica

$$-|z| \leq \mathrm{Re}\,z \leq |z| \quad \text{y} \quad -|z| \leq \mathrm{Im}\,z \leq |z|$$

De la propiedad 6 del ejercicio 2.76 obtenemos una forma fácil para calcular la división de complejos.

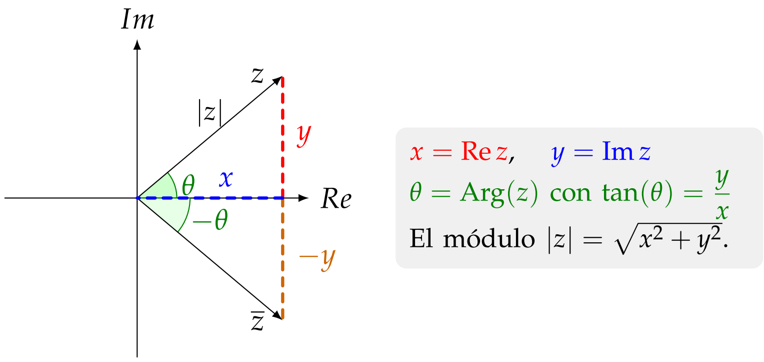


Figura 2.7: Un complejo y su conjugado.

$$\frac{z_1}{z_2} = \frac{1}{|z_2|^2} z_1\overline{z_2}.$$

Ejercicio 2.77. *Calcula la siguiente división compleja* $\dfrac{1+i}{i}$ *de dos formas distintas, en forma polar y usando la anterior propiedad. Expresa el resultado en forma rectangular y en forma polar.*

Y, por último, obtenemos las siguientes desigualdades clásicas:

Proposición 2.78. *Para* $z_1, z_2, \dots \in \mathbb{C}$*, tenemos las siguientes desigualdades:*

(a) La desigualdad triangular: $|z_1 + z_2| \leq |z_1| + |z_2|$.

(b) Forma general de la desigualdad triangular: $|\pm z_1 \pm z_2| \leq |z_1| + |z_2|$.

(c) La desigualdad triangular inversa: $|\pm z_1 \pm z_2| \geq |z_1| - |z_2|$.

(d) La desigualdad triangular para las sumas: $\left|\sum_{k=1}^{n} z_k\right| \leq \sum_{k=1}^{n} |z_k|$.

Demostración.

(a) Usamos algunas propiedades vistas en el Ejercicio 2.76.

$$\begin{aligned}
|z_1 + z_2|^2 &= (z_1+z_2)\overline{(z_1+z_2)} = (z_1+z_2)(\overline{z_1}+\overline{z_2}) = \\
&= |z_1|^2 + z_1\overline{z_2} + \overline{z_1\overline{z_2}} + |z_2|^2 = \\
&= |z_1|^2 + 2\mathrm{Re}\,(z_1\overline{z_2}) + |z_2|^2 \leq \\
&\leq |z_1|^2 + 2|z_1|\,|z_2| + |z_2|^2 = \\
&= (|z_1| + |z_2|)^2
\end{aligned}$$

(b) Se obtiene de la anterior, con más que considerar que $|\pm z| = |z|$.

(c) $|z_1| = |z_1 - z_2 + z_2| \leq |z_1 - z_2| + |z_2|$ de donde se obtiene que

$$|z_1 - z_2| \geq |z_1| - |z_2|.$$

Las restantes desigualdades se obtienen a partir de ésta con más que considerar $|\pm z| = |z|$.

(d) Procedemos por inducción.

- Para $n = 2$ no es más que la desigualdad triangular (a).
- Hipóteisis de inducción:
  Suponemos $\left|\sum_{k=1}^{r} z_k\right| \leq \sum_{k=1}^{r} |z_k|$ para $2 \leq r < n$.
- Para $n > 2$, tenemos (usando nuevamente (a))

$$\left|\sum_{k=1}^{n} z_k\right| = \left|\sum_{k=1}^{n-1} z_k + z_n\right| \leq \left|\sum_{k=1}^{n-1} z_k\right| + |z_n| \leq \sum_{k=1}^{n-1} |z_k| + |z_n| = \sum_{k=1}^{n} |z_k|.$$

□

Proposición 2.79. *Sea $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ un polinomio con todos sus coeficientes a_i números reales. Si $z \in \mathbb{C}$ es una raíz de $p(x)$, entonces su conjugado $\overline{z}$ es también raíz.*

Demostración. Si $z = re^{i\theta}$, entonces

$$p(z) = a_0 + a_1 r e^{i\theta} + a_2 r^2 e^{i2\theta} + \cdots + a_n r^n e^{in\theta} = 0 \tag{2.7}$$

Además

$$p(\overline{z}) = a_0 + a_1 r e^{-i\theta} + a_2 r^2 e^{-i2\theta} + \cdots + a_n r^n e^{-in\theta} = b \in \mathbb{C}. \tag{2.8}$$

Sumando y restando (2.7) y (2.8) nos da, respectivamente

$$b = 2a_0 + 2a_1 r \cos\theta + 2a_2 r^2 \cos(2\theta) + \ldots 2a_n r^n \cos(n\theta) \text{ (que es real)}$$
$$b = -i\big(2a_1 r \operatorname{sen}\theta + 2a_2 r^2 \operatorname{sen}(2\theta) + \ldots 2a_n r^n \operatorname{sen}(n\theta)\big) \text{ (que es imaginario)}$$

por tanto, $b = 0$, que prueba que $\overline{z}$ es también raíz. □

2.5.3. Función exponencial

Damos por conocida la función exponencial real y, sobre todo, sus propiedades. Nuestro objetivo es extender esta función a una nueva definida en los complejos (con imagen compleja) que extienda a la real ya conocida, a la que añadimos que sea compatible con la fórmula de Euler, ya definida,

$$e^{iy} = \cos y + i \operatorname{sen} y.$$

Definición 2.80. La función exponencial (compleja) se define para cualquier complejo $z = x + iy$ como

$$\boxed{\exp z = \exp(x + iy) = e^x e^{iy} = e^x(\cos y + i \operatorname{sen} y).}$$

Efectivamente, esta definición extiende a la de los reales.

$$\exp(x) = \exp(x + i0) = e^x(\cos 0 + i \operatorname{sen} 0) = e^x.$$

Además la fórmula de Euler es un caso particular de la exponencial compleja

$$\exp(ix) = e^{ix}$$

Las propiedades ya conocidas de la exponencial real se extienden a la compleja (y algunas otras nuevas)

Proposición 2.81. *Por todo $z, z_1, z_2 \in \mathbb{C}$,*

1. $\exp z_1 \exp z_2 = \exp(z_1 + z_2)$.
2. $\dfrac{1}{\exp z} = \exp(-z)$.
3. $\dfrac{\exp z_1}{\exp z_2} = \exp(z_1 - z_2)$.
4. $\exp(z + 2\pi i) = \exp z$.
5. $|\exp z| = \exp(\operatorname{Re} z)$.
6. $\exp z \neq 0$ *para cada* $z \in \mathbb{C}$.
7. $\exp' z = \exp z$.

Demostración. Ejercicios. □

Hacemos las siguientes observaciones:

1. La cuarta identidad es muy especial y no tiene equivalente en el caso real. Se dice que la función exponencial compleja es periódica con período $2\pi i$. Esto tiene muchas consecuencias interesantes, entre ellas que la función exponencial compleja no es inyectiva.

2. La última igualdad hace referencia a la derivada de la función exponencial compleja. Aunque está fuera de los contenidos de este curso, lo mostramos por remarcar los "parecidos" y las "diferencias" entre la exponencial real y la compleja.

Figura 2.8: La función exponencial compleja transforma rectas horizontales en semirectas radiales desde el origen.

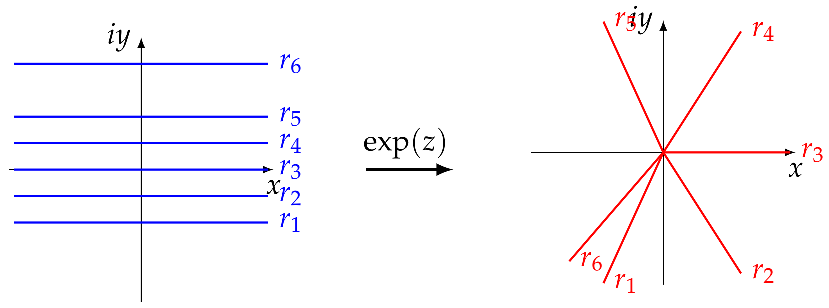
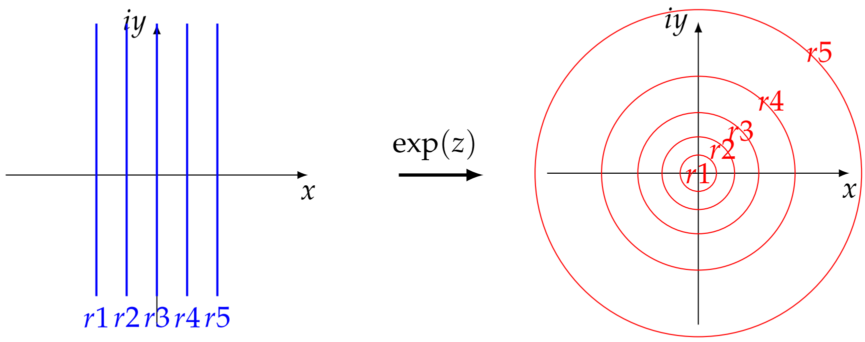


Figura 2.9: La función exponencial compleja transforma rectas verticales en circunferencias concéntricas al origen.



3. Las figuras 2.8 y 2.9 muestan como la exponencial compleja transforma rectas del plano complejo horizontales y verticales en otros subconjuntos de puntos de los complejos.

Ejercicio 2.82. *Describe las imágenes de los siguientes conjuntos bajo la función exponencial* $\exp z$*:*

a) *el segmento definido por* $z = iy$, $0 \leq y \leq 2\pi$.

b) *el segmento definido por* $z = 1 + iy$, $0 \leq y \leq 2\pi$.

c) *el rectángulo* $\{z = x + iy \in \mathbb{C} : 0 \leq x \leq 1,\ 0 \leq y \leq 2\pi\}$.

2.5.4. Funciones trigonométricas y trigonométricas hiperbólicas

Las funciones trigonométricas reales seno, coseno, tangente, cotangente, etc. tienen sus análogas complejas, aunque no juegan el mismo papel prominente como en el caso real. De hecho, podemos definirlos como simplemente ser combinaciones especiales de la función exponencial.

Definición 2.83. El seno y coseno (complejo) se definen como

$$\operatorname{sen} z = \frac{1}{2i}\left(\exp(iz) - \exp(-iz)\right)$$
$$\cos z = \frac{1}{2}\left(\exp(iz) + \exp(-iz)\right).$$

Las funciones tangente y cotangente se definen

$$\tan z = \frac{\operatorname{sen} z}{\cos z} = -i\,\frac{\exp(2iz) - 1}{\exp(2iz) + 1}$$
$$\cot z = \frac{\cos z}{\operatorname{sen} z} = i\,\frac{\exp(2iz) + 1}{\exp(2iz) - 1},$$

respectivamente.

Ejercicio 2.84. *Prueba las igualdades anteriores referidas a la tangente y cotagente. Para ello usa la igualdad* $(\exp z)(\exp(-z)) = e^0 = 1$.

Prueba, igualmente, que las funciones trigonométricas definidas extienden a las funciones trigonométricas reales.

Las principales propiedades de las funciones trigonométricas reales también se cumplen para funciones trigonométricas complejas, como se ve en este lema,

Lema 2.85. *Pora todo complejo* $z, z_1, z_2 \in \mathbb{C}$,

1. $\sin(-z) = -\operatorname{sen} z$
2. $\cos(-z) = \cos z$
3. $\operatorname{sen}(z + 2\pi) = \operatorname{sen} z$
4. $\cos(z + 2\pi) = \cos z$
5. $\tan(z + \pi) = \tan z$
6. $\cot(z + \pi) = \cot z$
7. $\operatorname{sen}(z + \pi/2) = \cos z$
8. $\cos(z + \pi/2) = -\operatorname{sen} z$
9. $\operatorname{sen}(z_1 + z_2) = \operatorname{sen} z_1 \cos z_2 + \cos z_1 \operatorname{sen} z_2$
10. $\cos(z_1 + z_2) = \cos z_1 \cos z_2 - \operatorname{sen} z_1 \operatorname{sen} z_2$
11. $\operatorname{sen}^2 z + \cos^2 z = 1$
12. $\cos^2 z - \operatorname{sen}^2 z = \cos(2z)$
13. $\operatorname{sen}' z = \cos z$
14. $\cos' z = -\operatorname{sen} z$

Demostración. Ejercicio (prueba algunas). □

Obsérvese que las funciones trigonométricas seno y coseno son periódicas de periodo 2π al igual que las funciones trigonométricas reales. Igualmente las funciones complejas $\tan z$ y $\cot z$ son periódicas de periodo π.

En cambio la propiedad de ser acotada que tiene las funciones reales seno y coseno ($|\operatorname{sen} x| \leq 1$ y $|\cos x| \leq 1$) no es verdad para las funciones complejas $\operatorname{sen} z$ y $\cos z$ (por ejemplo, $|\operatorname{sen}(iy)| \to \infty$ cuando $y \to \pm\infty$).

Definición 2.86. Definimos las funciones trigonométricas hiperbólicas (seno, coseno, tangente y cotagente hiperbólicas), como

$$\begin{aligned}
\operatorname{senh} z &= \frac{1}{2}\left(\exp z - \exp(-z)\right) \\
\cosh z &= \frac{1}{2}\left(\exp z + \exp(-z)\right) \\
\tanh z &= \frac{\sinh z}{\cosh z} = \frac{\exp(2z) - 1}{\exp(2z) + 1} \\
\coth z &= \frac{\cosh z}{\operatorname{senh} z} = \frac{\exp(2z) + 1}{\exp(2z) - 1}
\end{aligned}$$

respectivamente. Como es habitual estas funciones complejas extienden a sus homónimas reales.

Ejercicio 2.87. *Prueba las siguientes igualdades*

a) $\cosh^2 z - \operatorname{senh}^2 z = 1$. *b)* $\cosh(iz) = \cos z$. *c)* $\operatorname{senh}(iz) = i \operatorname{sen} z$.

2.5.5. Logaritmos y exponenciales de base

El logaritmo complejo es una función que vamos a que es de un carácter un tanto complicado. Está motivada por ser la función inversa de la función exponencial, es decir, que estamos buscando una función de registro de manera que

$$\exp(\log z) = z = \log(\exp z). \tag{2.9}$$

Como veremos en breve, esto es esperar demasiado. Vamos a escribir, como de habitual, Sea $z = re^{i\theta}$ siendo $z \neq 0$, y supongamos que $\log z = u(z) + iv(z)$. Tenemos entonces que

$$\exp(\log z) = e^u e^{iv} = re^{i\theta}$$

de donde obtenemos que $u = \ln r = \ln |z|$, que está definido como un logaritmo neperiano de un número positivo. Por otro lado, v coincidiría con el argumento de z, pero sabemos que este no es único, por tanto, podemos definir la *multifunción logaritmo* del siguiente modo

$$\log z = \ln|z| + i\arg z.$$

Podemos interpretar esta función logaritmo como muchas funciones distintas y a cada una se le llama *rama logarítmica* y cualquiera de estas ramas verifican la condición de inversa que pedíamos en 2.9. Entre todas estas ramas se suele destacar la llamada el *logaritmo principal* escrito con la primera letra mayúscula

$$\operatorname{Log} z = \ln|z| + i\operatorname{Arg} z.$$

Dicho de otro modo, el logaritmo principal de un complejo es la rama cuya parte imaginaria está en el intervalo $(-\pi, \pi]$.

Como viene siendo habitual, el logaritmo principal extiende al logaritmo (neperiano) real, puesto que el argumento principal de un real positivo es cero.

Ejercicio 2.88. *Comprueba que el logaritmo principal de un número negativo $x = -|x|$ es el siguiente*

$$\operatorname{Log} x = \ln|x| + i\pi$$

Ejercicio 2.89. *¿Se siguen verificando las propiedades clásicas del logaritmo neperiano en el logaritmo principal? Por ejemplo, ¿es cierto que $\operatorname{Log}(z^2) = 2\operatorname{Log} z$?*

Estudia si otras propiedades clásicas se siguen verificando.

Exponenciales de base.

Dado un número complejo $a \in \mathbb{C}^*$ definimos la exponencial compleja de base a como

$$a^z = \exp(z \log a)$$

que, evidentemente, es una multifunción por serlo $\log a$. Llamamos *valor principal de a^z* $= \exp(z \operatorname{Log} a)$, es decir, el obtenido usando el logaritmo principal. Salvo que se diga lo contrario, se entiende por a^z el valor principal de la exponencial de base a.

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = \sum_{k\geq 0}\frac{1}{k!}.$$

Notemos que, si usamos el número e de Euler como base, el valor principal de su exponencial es justamente la función exponencial compleja, veamos:

$$e^z = \exp(z \operatorname{Log} e) = \exp(z(\ln e + i0)) = \exp z.$$

Ejercicios Propuestos

Conjuntos, Relaciones, Funciones

Ej. 2.1 — Sea $U = \{1, 2, 3, ..., 10\}$ el conjunto universal en el que se definen los siguientes conjuntos: $A = \{1, 4, 7, 10\}$, $B = \{1, 2, 3, 4, 5\}$ y $C = \{2, 4, 6, 8\}$. Escribe los siguientes conjuntos:

a) $\overline{A} \cap (C - A)$ *b)* $A \cap (B \cup C)$ *c)* $\overline{(A \cap B)} \cup \overline{C}$ *d)* $(A \times A) \cap (B \times B)$

Ej. 2.2 — Para cada $i \in \mathbb{N}$, consideremos $A_i = \left\{ x \in \mathbb{R} \mid 0 \leq x < \frac{1}{i+1} \right\}$. Calcular $\bigcup_{i \in \mathbb{N}} A_i$ y $\bigcap_{i \in \mathbb{N}} A_i$.

Ej. 2.3 — Si el conjunto X tiene 10 elementos ¿cuántos subconjuntos propios de X hay en $\mathcal{P}(X)$?

Ej. 2.4 — Dado $A = \{a, b, c\}$, si $\mathcal{P}(A)$ representa el conjunto de las partes de A, indica cuáles de las siguientes afirmaciones son ciertas:

a) $\emptyset \subseteq A$ *c)* $a \subseteq A$ *e)* $\{a\} \subseteq \mathcal{P}(A)$ *g)* $\emptyset \subseteq \mathcal{P}(A)$
b) $\emptyset \in A$ *d)* $a \in \mathcal{P}(A)$ *f)* $\{a\} \in \mathcal{P}(A)$ *h)* $\emptyset \in \mathcal{P}(A)$

Ej. 2.5 — De los 100 alumnos de una clase 60 han aprobado física, 48 matemáticas y 30 las dos. Halla el número de alumnos que no han aprobado ninguna de las dos.

Ej. 2.6 — Dados los conjuntos $X = \{2, 3, 4\}$ e $Y = \{3, 4, 5, 6, 7\}$ definimos la relación de X en Y: "*$x \mathcal{R} y$ si y sólo si x divide a y*". Escribe los elementos del grafo de la relación y una representación gráfica de la misma.

Ej. 2.7 — Verificar si las siguientes relaciones definidas sobre el conjunto de los números enteros cumplen las propiedades reflexiva, simétrica, antisimétrica o transitiva.

1. $a \mathcal{R}_1 b \Leftrightarrow a = b^2$
2. $a \mathcal{R}_2 b \Leftrightarrow a > b$
3. $a \mathcal{R}_3 b \Leftrightarrow$ 3 divide a $a - b$

Ej. 2.8 — (Feb. 2012) Dado el conjunto $A = \{1, 2, 3, 4, 5, 6\}$, se considera la relación $\mathcal{R}$ sobre A, tal que, para todo $a, b \in A$, $a \mathcal{R} b$ si, y sólo si, $a + b$ es divisible por 6.

1. Calcula los pares de la relación $\mathcal{R}$. Justifica por qué $\mathcal{R}$ no es una relación de equivalencia.
2. Añade los pares necesarios para que sea una relación de equivalencia.
3. Define el conjunto cociente.

Ej. 2.9 — En el conjunto $A = \{1, 2, 3, 4\}$ se define la relación binaria:

$$\mathcal{R} = \{(1, 1), (2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4), (4, 2), (4, 3), (4, 4)\}.$$

Justifica que $\mathcal{R}$ es una relación binaria de equivalencia y halla el conjunto cociente. Dibuja una representación gráfica de la relación.

Ej. 2.10 — Demuestra que la relación de divisibilidad en $\mathbb{N} - \{0\}$:

$$a \mid b \text{ si y sólo si } b = na \text{ para algún } n \in \mathbb{N}$$

es una relación de orden e indica si es total o parcial. Representa gráficamente la relación restringida al subconjunto $\{1, 2, 3, 4, 6, 12\}$.

Ej. 2.11 — En $\mathbb{Z}$ se define la relación "$x \,\mathcal{R}\, y$ si y sólo si $x^2 - y^2 = x - y$" ¿es $\mathcal{R}$ una relación de equivalencia? En caso afirmativo, calcular los elementos de la clase $[a]$.

Ej. 2.12 — (Sept. 2012) Dados los conjuntos $A = \{1, 2, 3, 4, 5\}$ y $B = \{6, 7, 8, 9\}$, encuentra, si es posible, elementos $a, d \in A$ y $b, c \in B$ tales que la relación $\mathcal{R}_f = \{(1, 8), (2, 6), (2, b), (4, 7), (a, c), (d, 8)\} \subseteq A \times B$ cumpla que:

1. $\mathcal{R}_f$ no sea una función.
2. $\mathcal{R}_f$ sea una función inyectiva.
3. $\mathcal{R}_f$ sea una función, pero no sea sobreyectiva.

Ej. 2.13 — (Dic. 2012)

1. Considérese $\leq$ una relación de orden parcial en un conjunto A. Definimos una nueva relación binaria $\sim$ en el mismo conjunto A del siguiente modo:
$$a \sim b \iff a = b \text{ o bien } (a \not\leq b \text{ y } b \not\leq a)$$
Comprueba las propiedades de $\sim$ como relación: reflexiva, simétrica, antisimétrica y transitiva, probando las que son ciertas y poniendo un contraejemplo en las que no son ciertas. ¿Es $\sim$ una relación de equivalencia?

2. Pon, si es posible, un ejemplo de una función de $\mathbb{R} \to \mathbb{R}$ (reales de variable real) en cada uno de los siguientes casos:
   a) Inyectiva pero no sobreyectiva.
   b) Sobreyectiva pero no inyectiva.
   c) Ni inyectiva ni sobreyectiva.

Ej. 2.14 — Representa gráficamente, en un sistema cartesiano, las siguientes relaciones. Calcula su dominio e imagen. Indica cuáles son funciones en su dominio.

a) $\mathcal{R}_1 = \{(1,3),(2,2),(1,5),(3,5)\} \subseteq E \times F$, siendo $E = \{1,2,3\}$ y $F = \{2,3,4,5\}$.

b) $\mathcal{R}_2 = \{(x,y) \in \mathbb{R}^2 \mid y = \cos x\}$.

c) $\mathcal{R}_3 = \{(x,y) \in \mathbb{R}^2 \mid y^2 - x = 1\}$.

d) $\mathcal{R}_4 = \{(x,y) \in \mathbb{R}^2 \mid x - y^2 = 1\}$.

e) $\mathcal{R}_5 = \{(x,y) \in \mathbb{R}^2 \mid y^2 + x^2 = 4\}$.

f) $\mathcal{R}_6 = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 4\}$.

g) $\mathcal{R}_7 = \{(x,y) \in \mathbb{R}^2 \mid y + x = 2\}$.

Ej. 2.15 — Si consideramos las funciones de $\mathbb{R}$ en $\mathbb{R}$ cuyas gráficas sean rectas, ¿son todas aplicaciones biyectivas?

Ej. 2.16 — Prueba que la función $f\colon [0,\infty) \to (0,1]$ definida $f(x) = \frac{1}{x+1}$ es inyectiva. ¿Es sobreyectiva?

Ej. 2.17 — Clasifica por el tipo las siguientes funciones:

a) $f : \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$, definida $f(x) = |x-1|$.

b) $g : \mathbb{C} \to \mathbb{C}$, definida $f(z) = \overline{z}$.

c) $h : \mathbb{C} \to \mathbb{R}$, definida $f(z) = z\overline{z}$.

d) $t : \mathbb{N} \to \mathbb{Z}$, definida
$$t(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ par} \\ -\frac{n+1}{2} & \text{si } n \text{ impar} \end{cases}$$

Estructuras algebraicas

Ej. 2.18 — En el conjunto de los números naturales se definen las siguientes leyes de composición. Determina si son leyes de composición interna y en el caso que lo sean estudiar si cumplen la propiedad asociativa, conmutativa y poseen elemento neutro.

1. $a * b = a^b$
2. $a * b = a$

Ej. 2.19 — Sea $E = \{a,b,c,d\}$ y $\mathcal{P}(E)$ el conjunto de las partes de E. Determina los elementos regulares de $\mathcal{P}(E)$ respecto de la operación unión $\cup$. Igual respecto de la intersección $\cap$.

Ej. 2.20 — En el conjunto $E = \{(x,y) \in \mathbb{R}^2 : x \neq 0\}$ se define la operación:

$$(a,b) * (c,d) = (ac, ad + bc)$$

Comprueba que $(E,*)$ es un grupo.

Ej. 2.21 — Encuentra los inversos de cada uno de los elementos del grupo multiplicativo $\mathbb{Z}_{11}{}^*$.

Ej. 2.22 — Resuelve en el cuerpo $\mathbb{Z}_{11}$ el siguiente sistemas de ecuaciones:

$$\left.\begin{array}{l} 2x-7y=1 \\ 3x+y=9 \end{array}\right\}$$

Nota: Todos los números pertenecen al cuerpo $\mathbb{Z}_{11}$.

Ej. 2.23 — Comprobar que el subconjunto de las matrices 3×3 siguiente

$$R=\left\{\begin{pmatrix} a & 0 & b \\ 0 & a & c \\ 0 & 0 & a \end{pmatrix} \mid a,b,c\in\mathbb{R}\right\}$$

es un anillo unitario. ¿Es conmutativo? ¿Es cuerpo?

Números complejos

Ej. 2.24 — Prueba que las raíces n-simas de la unidad (complejas), es decir, las soluciones de la ecuación $z^n=1$, con $z\in\mathbb{C}$, forman un grupo abeliano con la operación producto.

Ej. 2.25 — Escribe en forma polar:

a) $2i$.
b) $1+i$.
c) $-3+\sqrt{3}i$.
d) $-i$.
e) $(2-i)^2$.
f) $|3-4i|$.
g) $\sqrt{5}-i$.
h) $\left(\dfrac{1-i}{\sqrt{3}}\right)^4$.

Ej. 2.26 — Encuentra todas las soluciones (en forma rectangular) de las ecuaciones:

a) $z^6=1$.
b) $z^4=-16$.
c) $z^6=-9$.
d) $z^6-z^3-2=0$.

Ej. 2.27 — Dibuja los siguientes conjuntos en el plano complejo:

1. $\{z\in\mathbb{C} : |z-1+i|=2\}$.
2. $\{z\in\mathbb{C} : |z-1+i|\leq 2\}$.
3. $\{z\in\mathbb{C} : \mathrm{Re}(z+2-2i)=3\}$.
4. $\{z\in\mathbb{C} : \mathrm{Img}(z+2-2i)=3\}$.
5. $\{z\in\mathbb{C} : |z-i|+|z+i|=3\}$.
6. $\{z\in\mathbb{C} : |z|=|z+1|\}$.

Ej. 2.28 — Prueba que $\overline{\operatorname{sen} z}=\operatorname{sen}(\overline{z})$ y $\overline{\cos z}=\cos(\overline{z})$.

Ej. 2.29 — Sea $z=x+iy$. Prueba que

1. $\operatorname{sen} z=\operatorname{sen} x\cosh y+i\cos x\operatorname{senh} y$.

2. $\cos z = \cos x \cosh y - i \operatorname{sen} x \operatorname{senh} y$.

Ej. 2.30 — Determina la imagen de la cinta $\{z \in \mathbb{C} : -\pi/2 < \operatorname{Re} z < \pi/2\}$ bajo la función $f(z) = \operatorname{sen} z$.

Ej. 2.31 — ¿Hay alguna diferecia entre $\log\left(z^2\right)$ y $2 \log z$?

Ej. 2.32 — Halla la imagen del anillo $1 < |z| < e$ bajo el logaritmo principal.

Ej. 2.33 — Encuentra los valores principales de

a) $\log i$. *b)* $(-1)^i$. *c)* $\log(1+i)$.

Ej. 2.34 — Prueba que $|a^z| = a^{\operatorname{Re} z}$ si a es una constante real positiva.

Ej. 2.35 — Encuentra todas las soluciones de las siguientes ecuaciones:

a) $\operatorname{Log}(z) = \dfrac{\pi}{2} i$. *b)* $\exp(z) = \pi i$. *c)* $z^{1/2} = 1 + i$.