UNIDAD
DIDÁCTICA

2 RELACIONES, APLICACIONES Y FUNCIONES (RAF)

OBJETIVOS DE LA UNIDAD

Familiarizar al estudiante con conceptos fundamentales, relevantes y ubicuos, no solo para las matemáticas, sino también para la ciencia en general e incluso para la vida cotidiana. Estos conceptos son los siguientes:

- Relaciones y sus tipos: equivalencia y orden.
- Aplicaciones: sus tipos y operaciones.
- Funciones y morfismos (homomorfismos, isomorfismos, automorfismos y endomorfismos).
- Sistemas y estructuras algebraicas: operaciones internas y externas.

1. INTRODUCCIÓN

Durante la Segunda Guerra Mundial, en el momento álgido del poderío nazi, Hitler decidió invadir Inglaterra. Como paso previo, desencadenó masivos, violentos y continuados bombardeos aéreos en lo que se conoció como la batalla de Inglaterra. Frente a los más que superiores medios aéreos nazis, tanto en bombarderos como en cazas, los británicos solo pudieron oponer unas menguadas fuerzas aéreas, básicamente cazas Hurricane, en lo que era su Royal Air Force (RAF). Con todo salieron tan bien libradas de los combates que el desembarco y la consiguiente invasión del Reino Unido jamás se produjo. Ante el valor, la decisión, el coraje, la habilidad, etc., de la menguada RAF, Churchill pronunció una de las frases que hicieron historia: «Nunca tantos deben tanto a tan pocos».

Jugando con las iniciales de los conceptos que se van a abordar en esta Unidad didáctica, «relaciones», «aplicaciones» y «funciones», que también dan el acrónimo RAF, se puede parafrasear la famosa frase de Churchill diciendo que, en matemáticas, «nunca tantas realizaciones deben tanto a tan pocos conceptos». En efecto, los conceptos aquí abordados son tan fundamentales, prácticamente para todas las matemáticas, más aún, para toda la ciencia, incluso más, para infinidad de cosas de la vida cotidiana, que sin ellos la matemática, de existir, sería una caricatura de lo que es. La ciencia devendría prácticamente imposible. Y la vida sería, además de muy distinta, seguramente mucho peor. Pero es que, a mayores, solo son tres, o mejor dicho, uno: las «relaciones», pues las «aplicaciones» son un tipo especial de relaciones y las «funciones» una clase particular de las aplicaciones, de modo que $R \supset A \supset F$.

Unas palabras de advertencia. En los diferentes textos aparecen distintos enfoques, énfasis y terminología para tratar estas cuestiones, casi tantos como autores, incluso más, pues algún autor, al repetir o hacer nuevas ediciones de sus textos, cambia alguno a todos los elementos anteriores. Aquí se sigue un enfoque ecléctico y globalizador, usando, eso sí, una visión única, completando, en cada caso, lo que decía un autor con lo que decían otros, naturalmente cuando esto no era lo mismo. Por ejemplo, la inmensa mayoría de los textos, al hablar de las propiedades de las relaciones, se limitan a las cuatro necesarias para definir las relaciones binarias más importantes (equivalencia y orden), es decir, a la **reflexividad**, **simetría**, **antisimetría** y **transitividad**. Sin embargo, aquí se han ampliado dichas propiedades sustancialmente y se ha mantenido la terminología usada por cada autor para entrenar al estudiante en la lectura y aprendizaje de distintas formas de expresar lo mismo, pues así es como aparece en el mundo real.

2. RELACIONES

2.1. DEFINICIÓN

Una **relación** no es más que un subconjunto de un referencial o del producto cartesiano de dos o más conjuntos diferentes o idénticos.

2.2. TIPOS DE RELACIONES

2.2.1. Relaciones unarias o monarias

En un conjunto referencial U, cuyos elementos son susceptibles de verificar una propiedad p, el subconjunto R, o $R(p)$, constituido por los elementos que verifican p, define una **relación unaria**:

$$R \subset U$$

Entonces, se dice que los elementos de R verifican la relación o, mejor aún, están en la relación. Por ejemplo, la «criba de Eratóstenes» permite establecer, en una lista limitada de números pertenecientes a $\mathbb{N}$, los números de dicha lista que son primos. Pues bien, el subconjunto de los números primos obtenidos de esta forma no es otra cosa que una relación unaria.

2.2.2. Binarias

Si ahora en vez de un conjunto se tienen dos conjuntos, verbigracia A y B, se denomina **relación binaria** a un subconjunto del producto cartesiano de $A \times B$:

$$R \subset A \times B$$

El conjunto de pares ordenados que están en la relación constituye la lista de elementos de R.

2.2.3. N-arias

La noción de producto cartesiano, vista en la Unidad didáctica 1, para dos conjuntos puede ampliarse de varias formas; a saber:

- A conjuntos idénticos; verbigracia, $A \times A$.
- A conjuntos infinitos; por ejemplo, $\mathbb{N} \times \mathbb{N}$.
- A más de dos conjuntos, verbigracia, $A \times B \times C$. Entonces, en vez de pares ordenados se tienen ternas ordenadas.

Más aún, pues este concepto puede generalizarse a n conjuntos; por ejemplo, A, B, C, $\overset{n}{\ldots}$, N, teniéndose entonces una n-erna. En este caso, la relación recibe el nombre de «n-aria».

En resumen, una **relación n-aria** es un subconjunto de n-ernas ordenadas pertenecientes al producto cartesiano de n conjuntos iguales o distintos que están en la relación.

Las relaciones son útiles en informática por muchas razones; sin ir más lejos, todas las «bases de datos relacionales» utilizan relaciones n-arias para el almacenamiento y acceso de datos. Sin embargo, en esta Unidad, y por ser las más generales, solo se van a considerar las relaciones binarias. Naturalmente, todo lo que se diga de ellas es, *mutatis mutandis*, aplicable a relaciones de «aridad» superior.

En la tabla 1, se muestran sucintamente los tipos de relaciones con sus ejemplos asociados más habituales en la ciencia.

Tabla 1. **Relaciones más habituales en ciencia**

Tipo de relación	Descripción	Ejemplos
Taxonómica	Clasifica un concepto general en un número más específico de conceptos u objetos.	*A* es *B*. *A* puede clasificarse como un *B*, un *C* o un *D*.
Estructural	Describe cómo un concepto o un sistema de conceptos puede ser descompuesto en partes o subsistemas.	*A* está cerca de *B*. *A* está a la izquierda de *B*.
Topológica	Describe la distribución espacial de conceptos físicos y las interconexiones entre estos conceptos.	*A* está a la derecha de *B*. *A* está encima de *B*. *A* está debajo de *B*. *A* está dentro de *B*. *A* contiene a *B*. *A* intersecta a *B*. *A* está conectada a *B*. *A* está en contacto con *B*.

.../...

Tipo de relación	Descripción	Ejemplos
.../...		
Causal	Describe cómo ciertos estados o acciones inducen otros estados o acciones.	*A* causa *B*. *A* es causado por *B*.
Funcional	Describe las condiciones por las cuales pueden ocurrir acciones y las reacciones y consecuencias que pueden resultar de las acciones.	*A* permite *B*. *A* necesita *B*. *A* dispara *B*.
Cronológica	Describe la secuencia temporal en la que ocurren los eventos.	*A* sucede antes que *B*. *A* ocurre después que *B*. *A* y *B* suceden simultáneamente. *A* ocurre durante *B*. *A* comienza antes de que *B* finalice.
Similaridad	Establece la «igualdad» o analogía entre conceptos y en qué grado.	La válvula *A* está abierta=admite gasolina.
Condicional	Define las condiciones en las que tienen lugar ciertas cosas.	Cuando masas pequeñas se mueven a poca velocidad y mucha aceleración usar hipótesis cuántica.
Finalidad	Establece el porqué y para qué de los conceptos.	Los códigos los crearon los humanos para transmitir sus ideas.

2.3. DOMINIO, RECORRIDO Y CAMPO DE UNA RELACIÓN

En las relaciones, las siguientes definiciones son importantes:

- El **dominio** de una relación binaria *R*, que explícitamente se representa por «Dom» *R*, es el conjunto de todos los primeros miembros de los pares de *R*; es decir, «Dom» $R \triangleq \{x | \exists \text{ y} < x, y > \in R\}$.
- El **recorrido** o **contradominio** de una relación binaria *R*, que explícitamente se representa por «Rec» *R*, es el conjunto de todos los segundos miembros de los pares de *R*; esto es, «Rec» $R \triangleq \{x | \exists \text{ y} < y, x > \in R\}$.

- El **campo** de una relación R es el conjunto de todos los primeros y segundos, miembros de los pares de R; o sea, es la unión del dominio y el contradominio o recorrido:

$$\text{«Cam»}\ R \triangleq (\text{«Dom»}\ R \cup \text{«Rec»}\ R)$$

Así, si «Dom» $R = \{1, 3\}$, «Rec» $R = \{a, b\}$, «Cam» $R = \{1, 3, a, b\}$. Si, verbigracia, «Dom» $R = \{x|x$ es un varón y x es padre de alguna mujer$\}$, «Rec» $R =$ $= \{x|x$ es una mujer y algún varón es padre de $x\}$, «Cam» $R = \{x|x$ es un varón padre de alguna mujer, o x es una mujer que tiene por padre algún varón$\}$.

El símbolo $\triangleq$ significa igual por definición.

2.4. OPERACIONES ENTRE RELACIONES: RESTRICCIÓN; CONVERSA O INVERSA; PRODUCTO RELATIVO

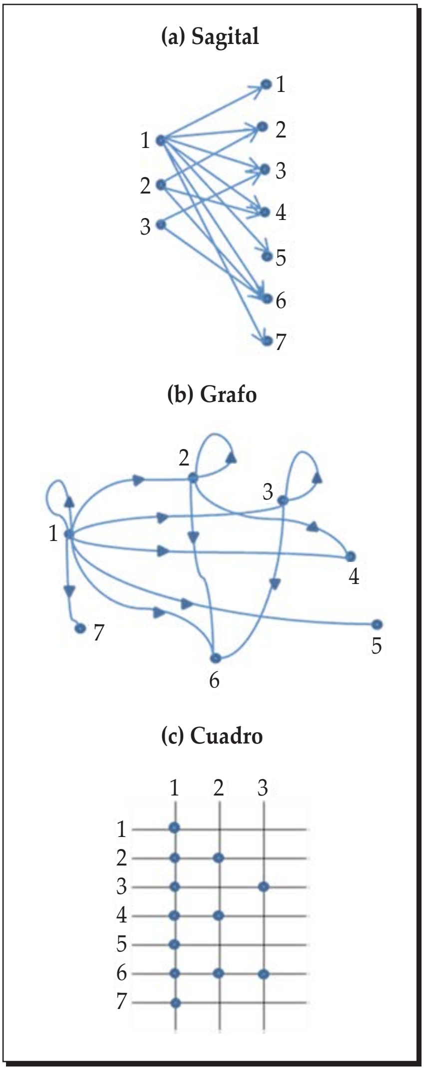
Las relaciones, como acaba de verse, son cierto tipo de conjuntos, concretamente conjuntos de pares, ternas, en general, «n-ernas», ordenadas. En tanto que conjuntos, obviamente a ellas se aplican las siguientes operaciones generales entre conjuntos, ya vistas en la Unidad didáctica 1: unión, intersección, complementación, etc. Pero además, en tanto que conjuntos de ernas, se pueden definir para ellas ciertas operaciones especiales; las más comunes y útiles son las siguientes, aunque para simplificar solo se van a considerar relaciones binarias:

- **Restricción.** Se denomina restricción de una relación R respecto a un conjunto cualquiera C, que se denota mediante R/C, a una nueva relación formada por los pares de R, cuyo primer miembro pertenece a C; es decir, $R/C \triangleq \{\langle x, y\rangle | \langle x|y\rangle \in R \wedge x \in C\}$.
- **Imagen.** Se denomina imagen de una relación R bajo un conjunto C, y se denota por $R[C]$ al conjunto de los segundos miembros de los pares de R cuyo primer miembro pertenece a C; o sea, el «recorrido» de R/C: $R[C] \triangleq$ $\triangleq \{y/\exists x|\langle x, y\rangle \in R \wedge x \in C\} =$ «Rec» R/C. Así, verbigracia, si $R = \{\langle x, y\rangle|x$ es un libro escrito por $y\}$ y $C = \{x|x$ es una novela policíaca$\}$, $R/C = \{\langle x, y\rangle|x$ es una novela policíaca escrita por $y\}$ y $R[C] = \{x|x$ ha escrito alguna novela policíaca$\}$.
- **Conversa o inversa.** La relación conversa o inversa, de una relación R que se denota por R^{-1}, es la relación R «dada la vuelta»; es decir, la relación cuyos pares son los pares de R «invertidos», intercambiando sus miembros; esto es, $R^{-1} \triangleq \{\langle x, y\rangle|\langle y, x\rangle \in R\}$. Así, para el ejemplo anterior $R^{-1} = \{\langle x, y\rangle|x$

ha escrito el libro y} y si R fuera la relación: $R = \{\langle x, y\rangle | x$ es progenitor de $y\}$, $R^{-1} = \{\langle x, y\rangle | x$ es hijo de $y\}$.

- **Producto relativo de las relaciones *R* y *S*.** Se denomina producto relativo de dos relaciones R y S, que se denota por «$R|S$», a la relación puente entre R y S. Es, por tanto, una nueva relación formada por los pares $\langle x, y\rangle$, tales que x es el primer miembro de un par de R, cuyo segundo miembro es el primer miembro de un par de S que tiene y como segundo miembro. Más coloquialmente, x tiene a su derecha en R algo que está a la izquierda de y en S. Por consiguiente, $R|S \triangleq \{\langle x, y\rangle | \exists Z | \langle x, z\rangle \in$ $\in R \wedge \langle z, y\rangle \in S\}$. Por ejemplo, si $R = \{\langle x, y\rangle | x$ es primo de $y\}$ y $S = \{x, y | x$ es hijo de $y\}$, entonces $R|S = \{\langle x, y\rangle | x$ es sobrino de $y\}$ y $S|T = \{\langle x, y\rangle | x$ es hijo de un primo de $y\}$.

Figura 1. **Distintas representaciones de una relación**



2.4.1. Representación de relaciones

Una relación puede representarse de distintas maneras, entre las que cabe destacar las siguientes: **grafo**, **sagital** o mediante un **cuadro**. Sean, verbigracia, los conjuntos

$$A = \{1, 2, 3\} \text{ y } B = \{1, 2, 3, 4, 5, 6, 7\}$$

Y sea la relación R dada por $x \in A$ divide a B, obteniéndose el conjunto C, tal que

$$C = ARB = \{(1, 1), (1, 2), (2, 2), (1, 3), (3, 3), (1, 4), (2, 4), (1, 5), (1, 6), (2, 6), (3, 6), (1, 7)\}$$

Entonces, las figuras 1 (a), (b) y (c) representan, respectivamente, esta relación con sus formas de grafo, sagital o en cuadro.

2.5. PROPIEDADES DE LAS RELACIONES

Las relaciones, en tanto que conjunto de pares, pueden tener propiedades, que pueden ser de cierto tipo, en función de qué les ocurra a sus pares conjuntamente considerados. Por ejemplo, una relación puede ser tal que siempre que tenga un par, tenga también un par opuesto (verbigracia, «ser hermano de»), o que no tenga nunca dos pares opuestos (verbigracia, «ser progenitor de») o que todo elemento del campo esté relacionado consigo mismo (verbigracia, «ser tan o más alto que») etc. Teniendo esto en cuenta, las propiedades más destacadas de las relaciones son las siguientes:

- **Reflexividad.** Se da cuando todo objeto del campo está relacionado consigo mismo. Formalmente, R es reflexiva $\stackrel{\triangle}{\leftrightarrow} \forall x\ (x \in «\text{Cam}»\ R \rightarrow \langle x, x\rangle \in R)$.
- **Irreflexividad.** En este caso, ningún objeto está relacionado consigo mismo. Formalmente, R es irreflexiva $\stackrel{\triangle}{\leftrightarrow} \forall x\ (x \in «\text{Cam}» \rightarrow \langle x, x\rangle \notin R)$.
- **Simetría.** Para todo par, el par converso está también en la relación. Formalmente, R es simétrica $\stackrel{\triangle}{\leftrightarrow} \forall x, y\ (\langle x, y\rangle \in R \rightarrow \langle y, x\rangle \in R)$.
- **Asimetría.** Cuando ningún par está invertido en la relación. Formalmente, R es asimétrica $\stackrel{\triangle}{\leftrightarrow} \forall x, y(\langle x, y\rangle \in R \rightarrow \langle y, x\rangle \notin R)$.
- **Antisimétrica.** Cuando los únicos pares conversos, caso de haber alguno, son los idénticos; es decir, con ambos miembros idénticos, o, dicho de otro modo, no hay dos pares «diferentes» invertidos. Formalmente, R es antisimétrica $\stackrel{\triangle}{\leftrightarrow} \forall x, y(\langle x, y\rangle \in R \wedge \langle y, x\rangle \in R \rightarrow x = y)$.
- **Transitividad.** La relación se «hereda»; es decir, siempre que un objeto esté relacionado con otro y este lo esté con un tercero, el primero también está relacionado con el tercero. Formalmente, R es transitiva $\stackrel{\triangle}{\leftrightarrow} \forall x, y, z(\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \rightarrow \langle x, z\rangle \in R)$.
- **Intransitividad.** No hay ninguna secuencia de pares transitivos. Formalmente, R es intransitiva $\stackrel{\triangle}{\leftrightarrow} \forall x, y, z(\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \rightarrow \langle x, z\rangle \notin R)$.
- **Conexión débil.** Cualesquiera dos objetos del «campo» diferentes están relacionados en un sentido u otro o en los dos. Formalmente, R es conexa $\stackrel{\triangle}{\leftrightarrow} \forall x, y(x \in \text{Cam}\ R \wedge y \in \text{Cam}\ R \wedge x \neq y \rightarrow \langle x, y\rangle \in R \vee \langle y, x\rangle \in R)$.
- **Conexión fuerte.** Cualesquiera dos objetos del campo están relacionados en un sentido u otro o en los dos. Formalmente, R es fuertemente conexa $\stackrel{\triangle}{\leftrightarrow} \forall x, y(x \in \text{Cam}\ R \wedge y \in \text{Cam}\ R \rightarrow \langle x, y\rangle \in R \vee \langle y, x\rangle \in R)$.

Así, por ejemplo: $R = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle, \langle 1, 3\rangle, \langle 3, 3\rangle\}$ es reflexiva, antisimétrica, transitiva, conexa y fuertemente conexa. $S = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle\}$ es irreflexiva, simétrica e intransitiva. $T = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 1, 3\rangle\}$ es irreflexiva, asimétrica, antisimétrica, transitiva y conexa. $U = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle\}$ no tiene ninguna de estas propiedades. Ø tiene todas las propiedades, pues hace falso el antecedente de todos los definientes. $V = \{\langle 1, 2\rangle\}$ es irreflexiva, asimétrica, antisimétrica, transitiva, intransitiva y conexa; en este caso, la transitividad e intransitividad se cumplen ambas porque se cumplen vacuamente. $W = \{\langle 1, 1\rangle\}$ es reflexiva, simétrica, transitiva, conexa y fuertemente conexa. $Q = \{\langle x, y\rangle | x$ e y tienen los mismos progenitores$\}$ es reflexiva, simétrica y transitiva. $P = \{\langle x, y\rangle | x$ es más alto que $y\}$ es irreflexiva, asimétrica, antisimétrica y transitiva. $O = \{\langle x, y\rangle | x$ ama $a\}$ no tiene ninguna de estas propiedades.

Entre estas propiedades se dan las implicaciones siguientes: simetría más transitividad implican reflexividad; asimetría implica tanto irreflexividad como antisimetría; y conexión débil más reflexividad implican conexión fuerte.

Teniendo en cuenta los grafos de las relaciones, una relación es **reflexiva** si y solo si su grafo, tal y como se muestra en la figura 2, tiene un bucle en cada uno de sus puntos; en caso contrario, recibe el nombre de **antirreflexiva**.

Una relación es **simétrica** si, tal y como se muestra en la figura 3, cada vez que su grafo tiene una flecha que va de a hacia b, también hay un arco que va de b hacia a; si esta simultaneidad no existe, la relación es **antisimétrica**. Es decir, R, simétrica $\Leftrightarrow R = R^{-1}$.

Una relación es **transitiva** si su grafo, tal y como se muestra en la figura 4, satisface a la condición: «si» una flecha va de a hacia b

Figura 2. **Representación de la reflexividad**

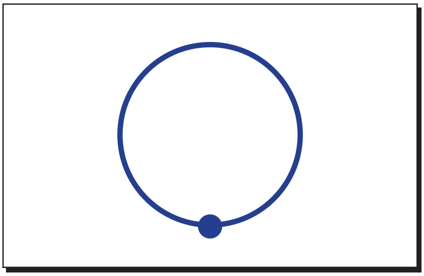


Figura 3. **Representación de simetría**

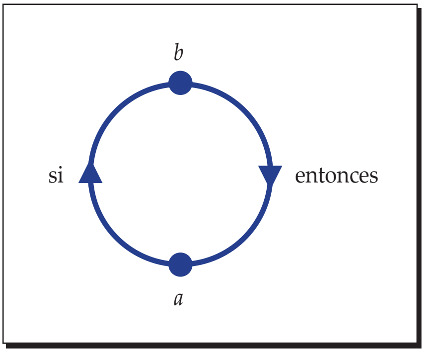
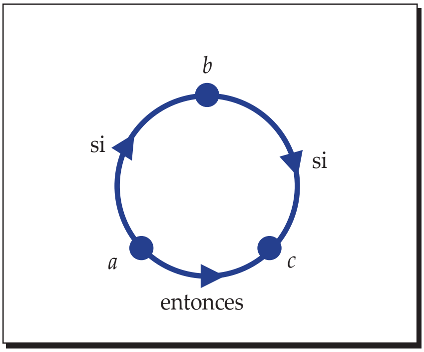
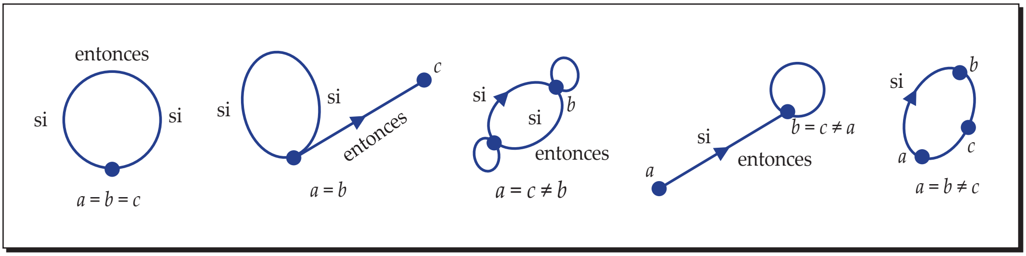


Figura 4. **Representación de la transitividad**



y otra flecha va de b hacia c, «entonces» una flecha va de a hacia c, y esto cualquiera que sean los puntos a, b, c distintos o no. En este caso, se tienen las diversas relaciones que se muestran en la figura 5.

Figura 5. **Diversas formas de transitividad**



2.6. COMPOSICIÓN DE RELACIONES

La relación $M \circ P$ se llama compuesta de las relaciones P y M. En general $M \circ P \neq P \circ M$. Si a y b son relaciones, se tiene la fórmula dada por la figura 6: $(B \circ A)^{-1} = A^{-1} \circ B^{-1}$.

La composición de relaciones es «asociativa»; es decir, se cumple $C \circ (B \circ A) = (C \circ B) \circ A$, tal y como se muestra en la figura 7.

Por ejemplo, si $\perp$ es una relación de perpendicularidad definida en un conjunto C de rectas del plano π, y $\|$ es una relación de paralelismo definida en un conjunto C de rectas del plano π, entonces se demuestra fácilmente que:

- $\perp^2 = \perp \circ \perp = \|$.
- $\perp \circ \| = \| \circ \perp = \perp$.
- $\| \circ \| = \|$.

$\forall\ a, b, c$ resulta: $(a/b$ y $b/c) \Rightarrow a/c$.

Figura 6. **Representación de la composición de relaciones**

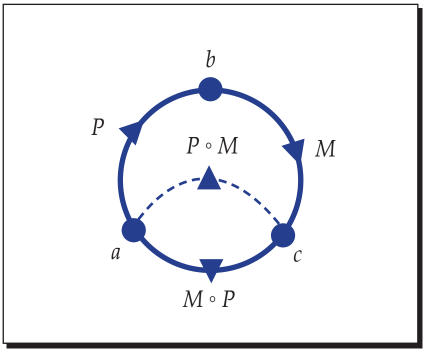
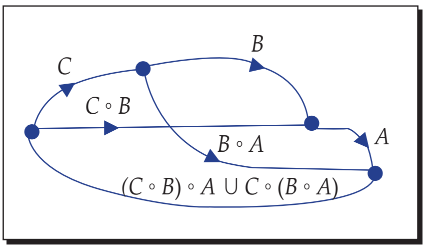


Figura 7. **Asociatividad de la composición de relaciones**



2.7. RELACIÓN DE EQUIVALENCIA

- Una relación binaria R en un conjunto A es de equivalencia si es reflexiva, simétrica y transitiva. En otros términos, una relación binaria $\mathcal{R}$ se denomina **relación de equivalencia** si es a la vez reflexiva, simétrica y transitiva. Esto significa que para todo x se tiene que $x \mathcal{R} x$, y que $x \mathcal{R} y$ implica que $y \mathcal{R} x$ y que $x \mathcal{R} y$ e $y \mathcal{R} z$ implican que $x \mathcal{R} z$. La igualdad, el paralelismo de vectores y la semejanza de triángulos son relaciones de equivalencia. Para subrayar que una relación ε es de equivalencia, a veces, se emplea la notación específica $x \equiv y$ (mód ε), que se lee «x es congruente con y módulo ε», y también «x es equivalente a y módulo ε». Si no hay confusión posible, se dirá «x es equivalente a y».

  Desde un punto de vista formal, y como ya se comentó, toda relación de equivalencia ε generaliza, pues, las propiedades de igualdad. Recíprocamente, la igualdad aparece con frecuencia, como «contracción» de una equivalencia. Ya que no son «idénticos» los símbolos 2/3, 4/6, 6/9, no son «iguales», pero sí lo son los números racionales que representan $0,\hat{6}$, puesto que los símbolos son equivalentes según se desprende de la conocida regla «producto de medios igual a producto de extremos». Esta noción de equivalencia no es exclusiva, ni mucho menos, de las matemáticas. Por ejemplo, la «fonología» de una lengua considera como equivalentes dos sonidos que el «fonético» reconoce como diferentes, con tal de que estos sonidos no se hallen jamás en oposición y que la sustitución de uno por el otro sea indiferente en la comunicación de dos personas que hablan. La clase de equivalencia es el «fonema».

- Una clase de equivalencia de un elemento $a \in A$ es el conjunto $[a] = \{x \in A / /xRa\}$, y verifica las propiedades siguientes:

  – $\forall a \in A, [a] \neq \emptyset$.

  – $[a] = [b] \Leftrightarrow aRb$.

  – Si $[a] \neq [b]$, entonces $[a] \cap [b] \neq \emptyset$.

- Una partición o conjunto cociente de un conjunto no vacío A es una colección de subconjuntos no vacíos $A_1, A_2, \ldots A_i \ldots$ de A tales que:

  – $A_i \cap A_j = \emptyset$, si $i \neq j$.

  – $A \cup_{i \in I} A_i$; es decir, $\forall a \in A, \exists i$ tal que $a \in A_i$.

Los subconjuntos A_i se denominan **bloques de la partición** o **clases**. Una relación de equivalencia en un conjunto produce una partición del conjunto, y, recíprocamente, una partición de un conjunto determina una relación de equivalencia en el conjunto.

Teorema

Si R es una relación de equivalencia en A, entonces $A/R = \{[a]/a \in A\}$ es una partición de A.

(La demostración del teorema aparece en la bibliografía).

Teorema

Sea $\{A_1, A_2, \ldots, A_i, \ldots\}$ una partición de A; entonces la relación R definida en A por $aRb \Leftrightarrow \exists i \in I$, tal que $a, b \in A_i$, es una relación de equivalencia en A.

(La demostración del teorema aparece en la bibliografía).

Por ejemplo, sea A igual que antes:

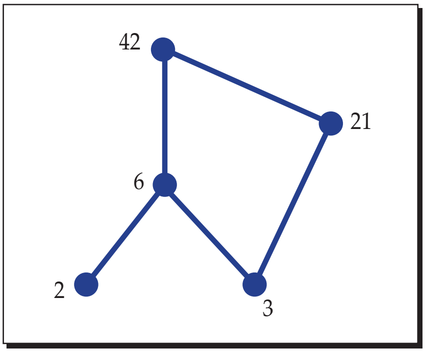
$A = \{1, 2, 3, 4, 5\}$ y una partición de A dada por $P = \{\{1, 2\},\{3, 5\},\{4\}\}$, entonces la relación $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 5), (5, 3), (5, 5), (4, 4)\}$ es una relación de equivalencia en A, cuyo conjunto cociente es $A/R = \{[1], [3], [4]\}$.

2.8. RELACIONES DE ORDEN: MAYORANTES, MINORANTES. LÍMITES. CARDINALES Y ORDINALES

Una relación binaria $\mathcal{R}$ se dice que es una relación de orden si es reflexiva, antisimétrica y transitiva. En otros términos: para todo x se verifica $x \mathcal{R} x$, $x \mathcal{R} y$ e $y \mathcal{R} x$ implican $x = y$; finalmente, $x \mathcal{R} y$ e $y \mathcal{R} z$ implican $x \mathcal{R} z$. Por ejemplo, sobre el conjunto de los números enteros, la relación $x \leq y$ es una relación de orden. Dicha relación, al admitir la igualdad, caracteriza un orden en sentido amplio o no estricto. De ahí que la relación $<$ podría denominarse relación de orden estricto. Aquí, uno se va a atener a la costumbre que tiende a reservar el nombre de relación de orden para las relaciones reflexivas.

Sobre el conjunto de los enteros iguales o superiores a 1, la relación x/y, es decir, x divide a y, es también una relación de orden. Sin embargo, debe observarse la diferencia

Figura 8. **Diagrama de relación** $/$



siguiente: dos elementos a y b son siempre «comparables» mediante la relación $\leq$, ya que siempre se tendrá $a \leq b$ o bien $b \leq a$, e incluso las dos si $a = b$, mientras que dos elementos como 7 y 36 «no son comparables» mediante la relación $/$. El hecho de que 7 no divida a 36 no implica que 36 divida a 7. Así pues, la relación $\leq$ es una relación de **orden total**, en tanto que $/$ es una relación de **orden parcial**.

Muchas veces conviene representar por un diagrama un conjunto ordenado mediante una relación de orden total o parcial. Para ello, los elementos se simbolizan con puntos $(\cdot)$ o circulitos $(\circ)$, dos elementos comparables se unen por una línea, y, si $a \mathcal{R} b$, se coloca b encima de a. La figura 8 representa el conjunto $\{2, 3, 6, 21, 42\}$ ordenado por $/$.

La relación «a es un ascendiente de b» es una de esas relaciones que pueden denominarse de **orden estricto**. Su diagrama está compuesto de árboles genealógicos. El orden es parcial.

La relación $\subseteq$, definida en el conjunto de las partes de un referencial, es una relación de orden parcial, quizás la más primitiva de todas.

- **Mayorantes y minorantes.** Límites superior e inferior. Sea A un conjunto dotado con una relación de orden $\mathcal{R}$. Si el orden es total, se empleará el signo $\leq$, que se lee «inferior o igual a»; si el orden es parcial, se utilizará el símbolo $\wp$, que se leerá «precede» o «es anterior a».

  Si $a \leq b$, o si $a \wp b$, se dice también que b es un «mayorante» para a. Si A' es una parte de A tal que para todo $a \in A'$, se verifica que $a \leq b$ o $a \wp b$, se dice que b es un «mayorante» de A'.

  En el caso del orden total, si el conjunto de todos los mayorantes de A' contiene un elemento β menor que todos los restantes, se demuestra fácilmente, por reducción al absurdo, que β es único y se denomina «el» límite superior de A'. Las nociones de «minorante» y «límite inferior» se deducen de las anteriores invirtiendo el orden.

  En el conjunto de los enteros, todo subconjunto finito admite un límite superior y otro inferior que pertenecen al subconjunto. En el conjunto de los enteros naturales, todo subconjunto admite un límite inferior y lo contiene. En el conjunto de los racionales, el subconjunto A' de elementos de la forma $1 - 1/n$ con n entero y positivo admite el 1 como límite superior, pero no lo contiene; es «abierto». Añadiéndole el 1 se obtiene el conjunto cerrado $\bar{A}'$. El conjunto de los números «racionales» x, tales que $x^2 < 2$ admite como mayorantes 1,5 o 1,42 o 1,415…, pero se demuestra que tal conjunto no tiene límite superior en el conjunto de los números racionales.

- **Cardinales.** Sea $\mathcal{F}$ un conjunto de conjuntos, mejor llamado **familia** de conjuntos: $\mathcal{F} = \{A, A', A'', \ldots\}$ finito o infinito. Se escribirá $A \equiv A'$ si y solo si existe una biyección de A en A'. Entonces, $\in$ es una relación de equivalencia sobre $\mathcal{F}$. Cada clase se denomina **número cardinal** o simplemente **cardinal**, y se dirá que dos conjuntos de una misma clase tienen la misma «potencia». Verbigracia, los días de la semana y las maravillas del mundo antiguo tienen la misma potencia: 7.

  Cuando un conjunto es aplicable biunívocamente sobre el conjunto $\aleph^*$ de los números enteros naturales, se dice que es **numerable** o que su cardinal es $\aleph_0$, alef de índice 0. El conjunto de los pares, el de los cuadrados perfectos y el de los números primos son conjuntos numerables. De lo anterior, se deduce que un conjunto infinito puede tener la misma potencia que una de sus partes propias.

- **Ordinales.** Sea $\mathfrak{D} = \{B, B', B'', \ldots\}$ una familia de conjuntos totalmente ordenados. Se escribirá $T \equiv T'$ si y solo si existe una aplicación biunívoca de T sobre T' que conserve el orden; es decir, que si $a \leq b$, se deberá tener $a' \leq b'$ para las imágenes. Se demuestra, con relativa facilidad, que $\equiv$ es una relación de equivalencia. A cada clase se le denomina un **tipo de orden**. Un conjunto se dice **bien ordenado** si todo subconjunto no vacío admite un primer elemento. $\mathbb{N}$, ordenado naturalmente, está bien ordenado. La clase de un conjunto bien ordenado es un «tipo de buen orden» o un «ordinal». La clase de $\mathbb{N}^*$ es el primer «ordinal transfinito» que se designa por W.

3. APLICACIONES

3.1. DEFINICIÓN

Dados dos conjuntos A y B, se define una **aplicación**, en inglés *mapping*, de A en B dando un «criterio» transformación o «regla» que permita hacer corresponder a todo elemento de A un elemento bien determinado de B. Esta «regla» se considera como un «operador», que se designa por la letra f, g, T, … Si $a \in A$, $f(a)$ designa el «aplicado» o transformado de a y representa, por consiguiente, un elemento de B. Se describe $a \xrightarrow{f} f(a)$, y se dice que a se aplica sobre $f(a)$.

Es importante distinguir claramente los tres elementos que intervienen en una aplicación. El elemento $a \in A$, f, el operador, y $f(a) \in B$. Con frecuencia es cómodo designar con otra letra, verbigracia, b, al elemento de B denotado por $f(a)$. En tal caso se escribe $a \to b$: $f(a)$, pero esto no es más que un convenio de escritura que interesa separar de la noción de aplicación.

Al elemento $f(a)$ se le denomina **imagen** de a. Recíprocamente, a es el antecedente de $f(a)$. A se denomina **conjunto inicial**, **origen** o **de partida** o aun **dominio**, y B, **conjunto final**, **llegada** o **codominio de la aplicación**.

Con frecuencia, se encuentran aplicaciones de un conjunto A en sí mismo; es decir, $A = B$. En estas condiciones, existe una aplicación particular tal que, a todo $a \in A$, asocia el mismo elemento a. Es la «aplicación idéntica», generalmente denotada por I.

3.2. RESTRICCIÓN DE UNA APLICACIÓN

Sea A_1 un subconjunto cualquiera de A. Toda aplicación de A en B determina una aplicación de A_1 en B, en la que la imagen de un elemento de A_1 queda definida en virtud de pertenecer a A. Esta aplicación se llama **restricción** de f a A_1.

3.3. GRAFO DE UNA APLICACIÓN

Recibe este nombre el subconjunto del conjunto producto $A \times B$, constituido por los pares $[a, f(a)]$ asociados en la aplicación. Así, por ejemplo, en la teoría ordinaria de funciones, el grafo de la aplicación $x \to f(x)$ está constituido por el conjunto de los puntos (x, y) del plano, tales que $y = f(x)$.

3.4. TIPOS DE APLICACIONES

Sea f una aplicación de A en B, y A_1 un subconjunto cualquiera de A. En la aplicación f, el conjunto de las imágenes de los elementos de A_1 constituye un subconjunto de B, que se escribe con la notación $f(A_1)$ y que se denomina **imagen** del subconjunto A_1. Si A_1 es vacío, se establece además que $f(\varnothing) = \varnothing$. En general, se tendrá $f(A_1) \subseteq B$.

Si A_1 se reduce a un solo elemento, su imagen queda igualmente reducida a un elemento, de acuerdo con la definición de la aplicación. Si $A_1 = A$, el subconjunto obtenido $f(A)$ se llama **subconjunto «imagen» de la aplicación**. En cualquier caso, se tiene que $f(A) \subseteq B$.

- Aplicación suprayectiva o sobre. Si se verifica que $f(A) = B$, de modo que el conjunto de las imágenes recubre totalmente a B, la aplicación se denomina **sobre** o **suprayectiva** y se dice que es una **suprayección**. Se emplea también la expresión «aplicación de A sobre B», reemplazando la preposición «en», utilizada en el caso general, por la preposición «sobre». Por definición de $f(A)$, la aplicación de A en $f(A)$ es, evidentemente, suprayectiva.

Considérese ahora una parte B_1 de B. Se denomina «imagen recíproca» de B_1 por f al subconjunto de todos los $a \in A$, tales que $f(a) \in B_1$. Se denotará por $f^{-1}(B_1)$ esta parte de B, conviniendo además que $f^{-1}(\varnothing) = \varnothing$. Adviértase que si f no es «suprayectiva», se puede tener $f^{-1}(B_1) = \varnothing$, incluso siendo $B_1 \neq \varnothing$. Para ello es suficiente que B_1 y el subconjunto imagen sean distintos.

- Se dice que una aplicación de A en B es **inyectiva** o también que es una **inyección**, cuando dos elementos distintos de A tienen imágenes distintas en B. Por consiguiente, todo elemento de B puede tener como máximo un antecedente; es decir, la imagen recíproca de todo punto será, o bien vacía, o bien estará reducida a un punto.
- Aplicación biyectiva. Una aplicación f de A en B que sea a la vez «suprayectiva» e «inyectiva» se denomina **biyectiva**. También se dice que es una **biyección**. En tal aplicación, todo $b \in B$ admite un antecedente y solo uno en A, lo que define una aplicación de B en A. Esta nueva aplicación es suprayectiva, ya que todo elemento a de A es antecedente del elemento $f(a)$ de B. Es también inyectiva, ya que dos elementos diferentes de B no pueden tener el mismo antecedente en A. Se ha obtenido, pues, una biyección de B en A, llamada **biyección recíproca** de f, o las dos igualdades equivalentes siguientes: $b = f(a)$ o $a = f^{-1}(b)$.

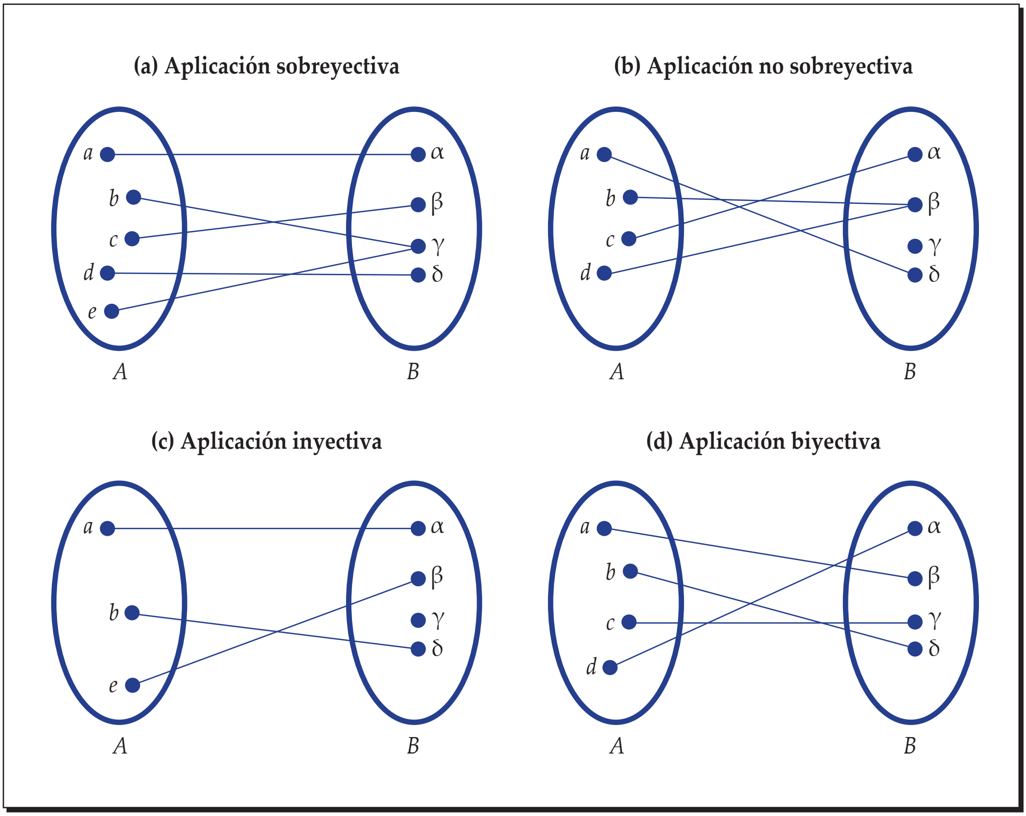
  Dos conjuntos entre los cuales es posible establecer una biyección se denominarán **equipotentes**; se dice, asimismo, que tienen la misma potencia.

Dicho lo anterior, es de señalar lo siguiente. En primer lugar, si se considera una aplicación inyectiva en la que $f(A)$ es el subconjunto imagen, la aplicación de A sobre $f(A)$ es biyectiva, pero, en general, no es una biyección de A sobre B. Al hablar de aplicación inyectiva se ha empleado el símbolo $f^{-1}(B_1)$ para designar la imagen recíproca de una parte de B, y, en este caso, f^{-1} no designa una aplicación de B en A. Sin embargo, hay que hacer constar que si se trata de una biyección, la imagen recíproca de un subconjunto reducido a un elemento, $f^{-1}(\{b\})$, coincide con el transformado $f^{-1}(b)$ en la biyección recíproca. Por lo tanto, no hay contradicción en los dos usos del signo f^{-1}.

Finalmente, indicar que, a veces, se dice de una aplicación que es **biunívoca**. Si no se añade nada más, esto significa que por tener todo elemento de A una imagen, toda «imagen» tiene solo un antecedente; por consiguiente, la transformación es inyectiva. Pero si se precisa que la transformación sea biunívoca entre A y B, se debe entender que, al tener todo elemento de B un antecedente y uno solo, existe una biyección de A sobre B, con su biyección recíproca de B sobre A.

La figura 9 muestra gráficamente los distintos tipos de aplicaciones considerados:

Figura 9. **Tipos de aplicaciones**



3.5. COMPOSICIÓN DE APLICACIONES

Existen varios tipos de composición de aplicaciones. Las más importantes son el producto y la autoaplicación que se consideran a continuación:

- **Producto de dos aplicaciones.** Sean tres conjuntos cualesquiera A, B, C, y considérese una aplicación f de A en B y una aplicación g de B en C. Si $a \in A$, f da una imagen $b = f(a)$, y g da de b una imagen $c = g(b)$. El paso directo de a a c define una aplicación h de A en C, tal que $c = h(a) = g[f(a)]$. Por definición, h se denomina **compuesta** o **producto** de las aplicaciones f y g. Simbolizando esta ley de composición por el signo $\circ$, se escribe $h = g \circ f$ y se lee g «compuesto, producto o círculo» f.

  Para respetar la notación funcional se está obligado a escribir las sucesivas aplicaciones de derecha a izquierda. Es interesante señalar que el producto $\circ$ la composición definida de esta manera no es una ley de composición en el sentido dado a ese término anteriormente. En efecto, f, g y h no son elementos de un mismo conjunto.

  La composición $\circ$ producto de aplicaciones es asociativa. Sean cuatro conjuntos A, B, C y D, y sea f una aplicación de A en B, g una aplicación de B en C y h una aplicación de C en D. La asociatividad se expresa por la fórmula $h \circ (g \circ f)a = (h \circ g) \circ f$, que resulta de la definición del producto; en efecto, para $a \in A$, el primer miembro da $[h \circ (g \circ f)]a = h[g \circ f(a)] =$ $= h(g[f(a)])$ y el segundo $[(h \circ g) \circ f]a = (h \circ g)f(a) = h(g[f(a)])$. Que manifiesta la identidad de los resultados, cualquiera que sea el elemento de A considerado.

- **Aplicación de un conjunto en sí mismo.** Considérese el caso particular de que los conjuntos B y C se confunden con A. Entonces, las aplicaciones f y g pertenecen al mismo conjunto: el de las aplicaciones de A en A. Este conjunto está bien definido, caracterizándose en él la igualdad por $f = f'$ si $f(a) =$ $= f'(a)$ para todo $a \in A$. Esta definición asocia a las aplicaciones f y g tomadas en este orden una aplicación producto, $g \circ f$, que pertenece igualmente al conjunto considerado. Se tiene, pues, una ley de composición sobre este conjunto y, según la propiedad precedente en (A), esta ley es asociativa. En general, no es conmutativa $g \circ f \neq f \circ g$, por lo que deberá respectarse el orden de los factores.

  El estudio de las transformaciones geométricas clásicas como simetría, rotación, homotecia, traslación, satisface la definición anterior, siendo A el conjunto de puntos en todo el espacio o en uno de sus planos.

- **Propiedades de la ley.** La ley de composición que acaba de definirse presenta las propiedades siguientes:
  - *Elemento neutro.* La ley admite un elemento neutro: la aplicación idéntica i que para todo $a \in A$ asocia $i(a) = a$. Se comprueba, en efecto, que para cualquier f: $i \circ f = f \circ i = f$.
  - *Simétrico.* Toda aplicación f de A en sí misma admite una aplicación simétrica o inversa con condiciones dadas por el teorema siguiente:

Teorema

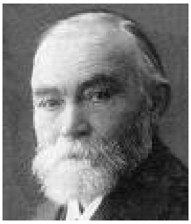
Una aplicación f de A en sí misma admite una aplicación simétrica, inversa, para la ley $\circ$ si y solo si es biyectiva.

(La demostración de este teorema aparece en la bibliografía).

4. FUNCIONES

4.1. GENERALIDADES

La noción de **función**, en principio no difiere del concepto de «aplicación». Precisamente hablando, solo se diferencia en que se usa el término «función» cuando A y B son conjuntos de números. También se adoptan para este caso algunas variantes de terminología. En efecto, a es entonces la variable, generalmente designada por x; A es el dominio de definición, y B, el dominio de valores.



Gottlob Frege. Nacido en Wismar (actual Alemania) en 1848.

En 1879 publicó su revolucionaria obra *Conceptografía* (*Begriffsschrift*), en la que sentó las bases de la lógica matemática moderna iniciando una nueva era en esta disciplina, que había permanecido prácticamente inalterada desde Aristóteles.

Frege fue el que dio contenido lógico al concepto de «función».

Muere en Bad Kleinen hacia 1925.

Conviene evitar una confusión demasiado frecuente entre f, que designa la función, o el operador, y $f(x)$, que es su valor para el elemento x. Corrientemente, se dice, verbigracia, «la función sen x», cuando debería decirse «la función sen». La notación de las aplicaciones $x \rightarrow \text{sen } x$ evita dicha confusión. También se puede decir: la función f definida por $f(x) = \text{sen } x$.

El término «función» proviene del latín *function*, que se deriva del verbo *fungi*, y significa cumplir. El concepto de «función» es fundamental en todas las ciencias y, naturalmente, en matemáticas. De hecho, en toda teoría matemática hay que determinar cuáles son los conjuntos, las relaciones y las funciones relevantes de la misma. Por ejemplo, el álgebra lineal considera espacios vectoriales y funciones lineales; en la teoría de grupos de los conjuntos, los grupos y las funciones son los homomorfismos, que conservan las operaciones; en topología, son, respectivamente, los conjuntos abiertos y las funciones continuas, etc.

Un ejemplo conspicuo son los polinomios y las funciones algebraicas, tales como $y = x^3 - 2x + 4$. Si en ella se sustituye x por, verbigracia, el número 3, se obtiene el valor $y = 25$. En tanto que si se hace $x = -3$, resulta $y = -17$. Se dice que 25 y – 17 son los valores que toma la función en $x = 3$ y $x = -3$.

Evidentemente, la composición de funciones sigue las reglas de la composición de aplicaciones.

4.2. DESCRIPCIÓN DE CONJUNTOS

Las funciones también sirven para describir conjuntos. En efecto, sea, verbigracia, el conjunto C la circunferencia unidad en el plano. Entonces, un conjunto C puede describirse de alguna(s) o incluso de todas las formas siguientes:

- **Implícita.** O como un conjunto de nivel; es decir, como antes:

$$C = f^{-1}(1) = \{(x, y) \neq \mathbb{R}^2 | x^2 + y^2 = 1\}, \text{ donde } f(x, y) = x^2 + y^2$$

- **Paramétrica.** Como una imagen: $C = \{(\cos t, \operatorname{sen} t) | 0 \leq t < 2\pi\}$. En efecto, si se considera la función cuyo dominio es el intervalo $[0, 2\pi]$ dada por $f(t) = (\cos t, \operatorname{sen} t)$, resulta que $f([0, 2\pi]) = \operatorname{Img}(f) = C$.
- **Explícita.** En este caso, un conjunto es la gráfica de una función. Por ejemplo, la semicircunferencia $C^+ = \{(x, y) | x^2 + y^2 = 1, \text{y} \geq 0\}$ es la gráfica de la función f: $[-1, 1] \to \mathbb{R}$, $i = f(x) = \sqrt{1 - x^2}$.

4.3. EJEMPLO DEL USO DE FUNCIONES: EL CALENDARIO UNIVERSAL

La medición del tiempo, no atmosférico, siempre ha estado vinculada al conocimiento de los movimientos de los astros; en particular, de la Luna y, sobre todo, del Sol. 1 año es el tiempo que la Tierra tarda en describir su órbita solar y es igual a 365 días más un exceso próximo a 6 horas. En tiempos del emperador romano Julio César, se instauró un calendario con 1 año de 365 días, más una corrección de 1 día más cada 4 años, para compensar las casi 6 horas perdidas, dando lugar a los años bisiestos. Sin embargo, como el tiempo real que tarda la Tierra en recorrer su órbita es un poco menor, al cabo de los siglos, el error convertido, no despreciable en absoluto, dio lugar a un cierto adelanto del calendario. Hacia 1582, en tiempos del papa Gregorio XIII, este error se cifró en 10 días. La manera de corregir esa acumulación de pequeños adelantos originó el calendario «gregoriano», el actualmente vigente. En este calendario siguen existiendo bisiestos; esto es, febrero tiene 29 días los años múltiplos de 4, excepto los últimos años de cada siglo, que solo lo serían si, además, fueran divisibles por 400. Es decir, 1700, 1800 y 1900 no fueron bisiestos, mientras que 1600 y 2000 sí lo fueron.

Teniendo esto en cuenta, si se quisiera saber, verbigracia, qué día de la semana fue el 12 de enero de 1910, se procedería de acuerdo con el príncipe de las matemáticas, Gauss, quien ideó una sencilla fórmula que permite responder al tipo de cuestiones que exponemos a continuación.

$S = D + M + Z + W$, siendo S el día pedido; D, el número del día, en el ejemplo $D = 12$; M es una función que solo depende del mes, en particular M (enero) = 0 (dicha función se explicita en la tabla 2); Z es otra función, que aparece descrita en la tabla 3, y depende del número de centenas del año, en este caso $Z(19) = 1$; finalmente, W es otra función, cuya descripción aparece en la tabla 4, y solo depende de las dos últimas cifras del año, en este caso $W(10) = 5$. Por último, se divide S por el número de días de la semana (7) y se obtiene el resto, que buscado en la tabla 5, da como resultado «miércoles», es decir, el día 12 de enero de 1910 fue miércoles.

Tabla 2. **Valores de la función *M***

M(enero) = 0	M(abril) = 6	M(julio) = 6	M(octubre) = 0
M(febrero) = 3	M(mayo) = 1	M(agosto) = 2	M(noviembre) = 3
M(marzo) = 3	M(junio) = 4	M(septiembre) = 5	M(diciembre) = 5

Tabla 3. **Valores de la función *Z***

Número de centenas	Z	Número de centenas	Z
15, 19	1	17, 21	3
16, 20	2	18, 22	4

Tabla 4. **Valores de la función *W***

Últimas cifras del año									***W***
00	06		17	23	28	34		45	0
01	07	12	18		29	35	40	46	1
02		13	19	24	30		41	47	2
03	08	14		25	31	36	42		3
	09	15	20	26		37	43	48	4
04	10		21	27	32	38		49	5
05	11	16	22		33	39	44	50	6
51	56	62		73	79	84	90		0
	57	63	68	74		85	91	96	1
52	58		69	75	80	86		97	2
53	59	64	70		81	87	92	98	3
54		65	71	76	82		93	99	4
55	60	66		77	83	88	94		5
	61	67	72	78		89	95		6

Tabla 5. **Correspondencia del resto con el día de la semana**

Domingo	0	Jueves	4
Lunes	1	Viernes	5
Martes	2	Sábado	6
Miércoles	3		

¿Por qué funciona la fórmula de Gauss? En primer lugar, no es extraño que el resto que da un número al dividirlo por 7 desempeñe un papel tan crucial; después de todo en cada semana hay exactamente 7 días. Por ejemplo, considérese la función M y hágase M(enero) = 0. Ahora bien, enero tiene 31 días; es decir, $31 = 4 \times 7 + 3$, que son 4 semanas justas y sobran, en este caso, 3 días; por eso, M(febrero) = 3. Esto es, si enero empieza en domingo, entonces febrero empieza en martes; si enero empieza en lunes, entonces febrero empieza en miércoles, y así sucesivamente.

Por otra parte, salvo los bisiestos, febrero tiene 28 días, que son 4 semanas justas, luego marzo comienza el mismo día de la semana que febrero: M(marzo) = M(febrero) = = 3. Por el contrario, marzo tiene 31 días, de nuevo $4 \times 7 + 3$, lo que hace que M(abril) = = M(marzo) + 3 = 6. Mayo, por un razonamiento similar, al tener solo 30, da M(mayo) = = abril + 2 módulo 7; o sea, M(mayo) = 1, que es el resto de dividir 8 por 7, y así sucesivamente.

Finalmente, las funciones Z y W introducen las correcciones debidas a los años bisiestos.

Naturalmente, este ejemplo también podría utilizarse en la aritmética modular. Se pide como ejercicio decir por qué.

4.4. FUNCIONES DE DISPERSIÓN: FUNCIONES «HASH»

Una de las aplicaciones más importantes en informática de las funciones son las funciones de dispersión o funciones «Hash», que, entre otras cosas, sirven para almacenar datos. Para ello, si se conocen los datos de entrada, se construye una función H: $Z \rightarrow Z_m$, que asigna a cada clave k un número, $H(k)$, de 1 a m. Este número sirve de índice para seleccionar una posición en una tabla formada por m registros de memoria.

Supóngase, verbigracia, que se tienen 2.000 personas y se dispone de 5.000 posiciones de memoria. En lugar de guardar los 2.000 números de DNI (documento nacional de identidad), se toma $m = 5.000$, o un número primo próximo a 5.000, y se utiliza entonces una función «Hash» $H(k) = (k \text{ mód } m)$ y se almacena en $H(k)$.

Por ejemplo, para guardar el número n se puede considerar como primera opción para la posición al número n(mód 11). La función de dispersión es $H(n) = n(\text{mod } 11)$. El resultado de guardar los números 15, 558, 32, 132, 102 y 5, en ese orden, en unas celdas originalmente vacías se muestra en la tabla 6.

Tabla 6. **Valores y módulos del ejemplo**

Valores	132			102	15	5				558	32
Módulos	0	1	2	3	4	5	6	7	8	9	10

Si ahora se quiere guardar, verbigracia, 257, como $H(257) = 4$, entonces se tendría que guardar 257 en la celda 4. Ahora bien, como puede verse, la celda 4 ya está ocupada por el 15; entonces, se dice que se produce una colisión: $H(x) = H(y)$ con $x \neq y$. Una forma de resolver las colisiones consiste en asignar la siguiente celda mayor vacía. En este caso ocuparía la posición 6.

Si se quisiera, ahora, localizar un valor ya guardado n, se calcula $m = H(n)$ y se comienza a buscar en la posición m. Si n no está en esa posición, se pasa a la siguiente mayor, y así sucesivamente. Si se llega a una celda vacía o se regresa a la posición inicial, entonces n no está presente.

5. MORFISMOS

Este concepto, junto con el de «ducción» (abducción, deducción, inducción y retroducción) son quizás las dos ideas más poderosas, fructíferas y ubicuas del método científico, por eso se tratan aquí los morfismos con alguna amplitud y profundidad.

- **Isomorfismo.** La noción de isomorfismo es uno de los conceptos básicos del álgebra moderna. Sean dos conjuntos C y C', y f, una biyección de C sobre C'. Supónganse definidas sobre C' una ley de composición, denotada por $*$, y otra sobre C' simbolizada por $*'$. La biyección se llama «regular» respecto a las leyes $*$, y $*'$ si la igualdad $a * b = c$, supuesta verificada en C, implica para las imágenes $f(a)$, $f(b)$ y $f(c)$ la igualdad: $f(a) *' f(b) =$ $= f(c)$, que se verifica sobre C'. Esto equivale a decir que el transformado del compuesto sobre A de dos elementos es el compuesto sobre C' de los transformados de estos elementos.

  De ello resulta que a toda igualdad entre diversos elementos de C compuestos por la ley $*$ corresponde una igualdad entre sus imágenes en C', compuestas de la misma manera según la ley $*'$. Por consiguiente, toda propiedad de la ley $*$ (asociatividad, conmutividad, elementos neutro e inverso, etc.) pertenece igualmente a la ley $*'$ de C'. Los dos conjuntos poseen, pues, propiedades algebraicas idénticas. Son isomorfos, del griego *isos*, esto es, «igual», y *morfé*, es decir, «forma», y pueden considerarse como dos realizaciones concretas de la misma estructura algebraica.

Esta noción se extiende además a estructuras más ricas. Sobre C y C' puede existir un mismo número de leyes de composición; a toda ley de C debe corresponder una ley de C', tal que f sea regular para cada par. Cabe también que existan relaciones binarias: $\mathcal{R}$ sobre C, $\mathcal{R}'$ sobre E'; la biyección f se denomina regular respecto a $\mathcal{R}$ y $\mathcal{R}'$ si $a\mathcal{R}b'$ implica $f(a)\mathcal{R}'f(b)$. Entonces, las relaciones $\mathcal{R}$ y $\mathcal{R}'$ gozan de las mismas propiedades. Los dos conjuntos C y C' se dicen isomorfos para las estructuras definidas por las leyes y relaciones consideradas. Algunos ejemplos aclararán lo anterior:

– Los símbolos 0, 1, 10, 11, 100, …, empleados en la numeración binaria, y los símbolos 0, 1, 2, 3, 4, 5, …, del sistema decimal, forman dos conjuntos isomorfos para las leyes de composición interna +, la relación <, etc. Estos dos conjuntos «concretos» son isomorfos con el conjunto «abstracto» de los enteros, del que dan dos representaciones.

– En matemáticas elementales uno se familiariza, en un espíritu eminentemente práctico, con el isomorfismo que liga el conjunto de los números estrictamente positivos al conjunto de todos los números relativos, isomorfismo cuyo «léxico» es la tabla de logaritmos y cuya gramática tiene las reglas siguientes:

  - $\times$ corresponde a $+$.
  - : corresponde a –.
  - Elevar a la potencia de n corresponde a multiplicar por n.
  - Extraer raíz n-ésima corresponde a dividir por n.
  - $\leq$ corresponde a $\leq$.

  Para definir los números negativos se introducen a veces dos clases de números, afectando de un signo calificativo, + o –, a los números hasta entonces en uso. Termina la teoría identificando los números positivos con los números ordinarios. Para evitar que este procedimiento parezca un juego de prestidigitación, conviene señalar lo siguiente:

- Que un número afectado de un signo no es ya un número ordinario.
- Que el conjunto de números precedido del signo + es isomorfo con el de los números ordinarios.
- Que la asimilación es un convenio, cuya posibilidad se basa en dicho isomorfismo.

La construcción de los números racionales da lugar a una observación análoga para los símbolos n/L.

Una observación adicional es pertinente sobre lo dicho. Supóngase que existe una biyección f entre dos conjuntos A y A'. Si A posee ciertas leyes de composición, es posible definir leyes correspondientes sobre A'. A toda ley $*$ sobre A se asocia una ley $*'$ sobre A' definiendo el compuesto $c' = a' *' b'$ de los elementos $a' = f(a)$, y $b' = f(b)$ por $c' = f(c)$, siendo $c = a * b$. De este modo, los dos conjuntos resultan isomorfos. Se dice, entonces, que las operaciones sobre A' se han definido por isomorfismo.

- **Automorfismo.** Un caso particular es el automorfismo. Sea A un conjunto sobre el que está definida una ley *. Si f es una biyección en sí misma, regular para esta ley, entonces, como los conjuntos A y A' se confunden, el isomorfismo correspondiente recibe el nombre de «automorfismo». Por ejemplo, en geometría euclideana, la simetría con relación a un plano es un automorfismo del conjunto de los vectores libres del espacio dotado de la ley clásica de adición.
- **Homomorfismo.** Considérense dos conjuntos C y C' dotados respectivamente de leyes de composición $*$ y $*'$. Supóngase, además, que existe una aplicación suprayectiva f de C en C', tal que la imagen del compuesto de a por b mediante $*$ se superpone sobre el compuesto de a' por b' mediante $*'$. De forma más precisa: $a \to a'$ y $b \to b'$ y $a * b = c$ y $a' * b' = c'$ implican $c \to c'$.

  Se dice entonces que C' es una «imagen homorfa» de C, dando a f el nombre de «homomorfismo». Resulta obvio que en el caso de que f sea una biyección, este concepto se confunde con el de «isomorfismo».

  El concepto de «homomorfismo» es fundamental en la construcción de modelos.

  Se sabe que la aplicación f de C sobre C' da origen sobre C a una equivalencia asociada ε en la que los elementos $a, a_1, a_2, \ldots$ de una clase $C(a)$ son los que tienen la misma imagen a', de suerte que el conjunto cociente C/ε se aplica biunívocamente sobre el conjunto imagen C' por la regla $C(a) \Leftrightarrow a'$.

Por otra parte, ε induce sobre $\overline{C} = C/\varepsilon$ una ley $\overline{*}$, y decir que $C(a) \overline{*} C(b) = C(c)$ o que $a' * b' = c'$ equivale evidentemente a traducir el mismo contenido matemático en términos ligeramente diferentes. De manera rigurosa, el conjunto $\overline{C}$ dotado de la ley $\overline{*}$ es isomorfo con C' dotado de $*'$.

Si existe un elemento neutro e tal que $a * e = e * a = a$ cualquiera que sea a, su imagen e' da $a' * e' = e' * a' = a'$ cualquiera que sea a', ya que todo a' es imagen. Es decir, la imagen del elemento neutro es neutro, y en C/ε corresponde a una clase neutra $C(e)$.

Teorema

Sea C un conjunto dotado de una ley de composición $*$. Si C' es una imagen homomorfa de C por la aplicación f, la equivalencia ε asociada a f determina un conjunto cociente C/ε que es isomorfo con E' dotado de la ley $*'$.

- **Endomorfismo.** Si el conjunto C' es una parte de C, el homomorfismo recibe el nombre de «endomorfismo».

CONCEPTOS BÁSICOS A RETENER

- Relación: relación de equivalencia y orden.
- Aplicaciones y funciones diferenciales.
- Tipos de aplicaciones y funciones: inyectivas, sobreyectivas y biyectivas.
- Morfismos y sus tipos.

EJERCICIOS VOLUNTARIOS

Tras el estudio de esta Unidad didáctica, el estudiante puede hacer, por su cuenta, una serie de ejercicios voluntarios, como los siguientes:

1. Dé algunos ejemplos de relaciones monarias, ternarias y cuaternarias.

2. Además de las propiedades de las relaciones dadas en la Unidad, hay otras también interesantes. Identifíquelas y defínalas.

3. Dado el conjunto $\mathbb{Z}^*$ de los enteros positivos:

- Ver si es o no ordenado, y, si es ordenado, qué tipo de orden es.
- Dado el subconjunto $S=\{1, 2, 4, 5, 10\}$, calcular sus cotas superior o mayorante e inferior o minorante, su supremo e ínfimo, su maximal, minimal, mínimo; es decir, sus elementos extremales, si existen.

4. Al definir las aplicaciones, se identifican los tipos que habitualmente aparecen en todos los textos: inyectiva, sobreyectiva, biyectiva, de los que se dio su representación sagital; sin embargo, hay otros dos, muy importantes, de los que casi nunca se da su representante sagital. Identifíquelos, defínalos y dé su representación sagital.

5. Poner al menos un ejemplo de la restricción de una función y definir y dar un ejemplo de su recíproca, una ampliación de una función.

6. Considérese el conjunto de los divisores de 60. Represéntelos gráficamente y calcule si existen sus elementos extremales.

7. Considérese ahora los números primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, … Sea $\pi(x)$ el número de primos menores o iguales que x: $\pi(1) = 0$, $\pi(7) = 4$, $\pi(20) =$ $= 8$, … Como ejercicio:

- Calcular los valores $\pi(27)$, $\pi(40)$ y $\pi(200)$.
- Elaborar, por computador, una tabla de números primos hasta 1.000 y comprobar con ella la propiedad $\pi(2x) - \pi(x) \geq 1$, si $x \geq 1$.

8. Si a cada entero positivo n se le asigna $d(n)$ el número de sus divisores positivos: $d(1) = 1$, $d(2) = 2$, $d(3) = 3$, $d(4) = 3$, $d(10) = 4$, $d(30) = 8$, …, ¿cómo se denominan los números cuya imagen dada por esa función es 2? Describir los números n tales que $d(n) = 4$.

9. Responder a las siguientes cuestiones: ¿es inyectiva la función $f(x) =$ Lugar de nacimiento de x? Considérese la función número de divisores de un número, $d(n)$, cuyo dominio son los enteros positivos $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, y cuyo conjunto de llegada es también $\mathbb{Z}^+$. ¿Es inyectiva?

10. Para cada función de dispersión (Hash), mostrar en los casos a), b), c) y d) la forma en que se insertan los datos, en el orden dado, en celdas inicialmente vacías, con:

a) $H(x) = x$ (mód 11).

Celdas: del 0 al 10.

b) $H(x) = x^2$ (mód 11).

Datos: 53, 13, 281, 743, 377, 20, 10 y 796.

c) $H(x) = x$ (mód 17).

Celdas: del 0 al 16.

d) $H(x) = (x^2 + x)$ (mód 17).

Datos: 714, 631, 26, 373, 775, 906, 509, 2.032, 42, 4, 136, 1.028.

11. En el conjunto de los enteros relativos, las leyes + y · son estables respecto de la equivalencia ($a \cdot b$) = mult · 2. Demostrar que las operaciones inducidas son

$$\text{par} + \text{par} = \text{par}, \quad \text{par} + \text{impar} = \text{impar}, \quad \text{impar} + \text{impar} = \text{par}; \quad \text{y}$$

$$\text{par} \cdot \text{par} = \text{par}, \quad \text{par} \cdot \text{impar} = \text{par}, \quad \text{impar} \cdot \text{impar} = \text{impar}.$$

REFERENCIAS BIBLIOGRÁFICAS

BREUER, J.: *Iniciación a la teoría de conjuntos*, Madrid, Paraninfo, 1970.

GARCÍA MERAYO, F.: *Matemática discreta*, Madrid, Thomson, Paraninfo, SA, 2005.

LIPSCHUTZ, S.: *Teoría de conjuntos. 530 Problemas resueltos*, Serie de Compendios Schaum, Nueva York, McGraw-Hill, 1963.