Álgebra I

Curso 2021/22

Índice

Tema 1

El lenguaje de los conjuntos

Comenzamos el curso con una breve discusión de las nociones de teoría de conjuntos que jugarán un papel esencial en vuestra formación matemática.

> ***Su uso hoy día es fundamental para expresar de manera correcta los razonamientos y conceptos matemáticos.***

Fue Georg Ferdinand Ludwig Philipp Cantor (San Petersburgo, 1845 -1918) quien expuso originalmente la Teoría de Conjuntos, sobre la que David Hilbert (Königsberg, Prusia Oriental, 1862-1943) declara

> *"Cantor ha creado para los matemáticos un paraíso de pensamiento del cual ya nadie nos expulsará".*

Al tiempo, fijaremos el sentido de los símbolos matemáticos básicos, que seguro os son ya familiares: $\in$ (pertenece), $\forall$ (para todo), $\exists$ (existe), $|$ (tal que), $\vee$ (o), $\wedge$ (y), etc.

1.1 Sobre la teoría axiomática de conjuntos

La matemática es una ciencia totalmente abstracta. En contraposición con otras ciencias como pueden ser la física, la química o la biología, en matemáticas no hay forma de comprobar si un resultado es o no correcto. Esto hace que para realizar las matemáticas se establezca un contexto y en este contexto los matemáticos se pongan de acuerdo en que reglas o conceptos se dan por válidos.

Cantor propuso el contexto de "conjuntos" como el contexto básico en el que se establecen los axiomas y en el que se ha de desarrollar la matemática.

En el contexto de conjuntos hay dos nociones básicas:

- ***Conjunto***.
- ***Pertenece***.

Estas nociones básicas no se pueden definir pero si se deben entender. Además si aceptamos el contexto de conjuntos como aquel en el que vamos a desarrollar las matemáticas, sólo podremos hablar de conjuntos. Esto es: *Todo objeto matemático es un conjunto y cualquier enunciado debe estar basado en conjuntos y en la pertenencia.*

Una vez establecido el contexto en el que vamos a desarrollar las matemáticas, al ser esta una ciencia totalmente abstracta, necesitaremos establecer unas "*reglas del juego*" que nos permitan realizar nuestra ciencia.

Estas *reglas del juego* se conocen con el nombre de **Axiomas** y no tienen porqué ser aceptadas o estar fijadas de antemano. Los matemáticos tenemos que ponernos de acuerdo en los axiomas que vamos a aceptar. La única condición para aceptar estos axiomas será que ***no den lugar a contradicciones***.

Los matemáticos Ernst Friedrich Ferdinand Zermelo (Berlín, 1871-1953) y Abraham Halevi Fraenkel (Múnich 1891-1965) fijaron la axiomática más aceptada de teoría de conjuntos: *La axiomática de Zermelo-Fraenkel.*

Utilizaremos cualquier tipo de letra,

$$A, B, C, \cdots, X, Y, Z, \cdots a, b, c, \cdots, x, y, z, \cdots, \alpha, \beta, \gamma, \cdots$$

para expresar un conjunto.

Utilizaremos $\in$ para indicar pertenece. Así escribiremos por ejemplo:

Sea $x \in X$.

Cuyo significado será:

Sea x un elemento de X.

Y, por supuesto, tanto x como X, son conjuntos.

Comenzamos estableciendo un primer concepto: **El concepto de contenido:**

Diremos que el conjunto X está contenido en el conjunto Y, y lo indicaremos $X \subseteq Y$ si todo elemento que pertenece a X también pertenece a Y.

Simbólicamente escribiremos:

Definición 1.1.1. $X \subseteq Y \Leftrightarrow \forall x \in X, x \in Y$.

El concepto de contenido está perfectamente definido. No como ocurre con el concepto de pertenece, que es básico y espero entendáis aunque no lo hemos (no podemos) definido.

El segundo concepto que definimos es el de igualdad. Simbólicamente:

Definición 1.1.2. $X = Y \Leftrightarrow X \subseteq Y \wedge Y \subseteq X$.

Que leeremos: X es igual a Y si (y solo si) X está contenido en Y e Y está contenido en X.

Ya que estamos hablando de un concepto (el de conjunto) totalmente abstracto, no podemos probar la existencia de ningún conjunto. Con el primer axioma aceptaremos la existencia de un conjunto especial, aquel que no tiene elementos:

Axioma 1: $\exists X; \forall x, x \notin X$.

Hasta ahora tenemos dos definiciones (contenido e igualdad) y un axioma, con esto podemos dar nuestro primer teorema:

Teorema 1.1.3. *Si X es un conjunto que satisface el Axioma 1, entonces $X \subseteq Y$, para cualquier conjunto Y.*

La demostración de este axioma es algo especial y no siempre este tipo de demostraciones fue aceptado. Es una demostración *por reducción al absurdo.* Este tipo de demostraciones consiste en negar la hipótesis del teorema y llegar a una contradicción, es decir hemos de llegar a algo que contradiga nuestros axiomas (en nuestro caso sólo tenemos el Axioma 1).

Lo primero que tememos que saber es negar las hipótesis del Teorema 1.1.3.

Notemos que negar un enunciado del tipo:

$\forall Y$ se cumple bla, bla, bla.

Sería:

$\exists Y$ que no cumple bla,bla, bla.

Por tanto la negación de la hipótesis del Teorema 1.1.3 sería:

Si X es un conjunto que satisface el Axioma 1, entonces $\exists Y$ tal que $X \nsubseteq Y$.

Y la afirmación $X \nsubseteq Y$ nos diría que ha de existir un elemento $x \in X$ que no esté en Y. Lo que contradice la hipótesis de que X satisface el Axioma 1, ya que X no tiene elementos.

Una consecuencia (o corolario) inmediato de este Teorema 1.1.3 es que sólo existe un conjunto que satisfaga el Axioma 1. Que podemos enunciar como:

Corolario 1.1.4. *Existe un único conjunto que satisface el Axioma 1. Denotaremos a este conjunto como $\emptyset$ o también 0 y lo llamaremos conjunto vacío o cero.*

Demostración. Si X_1 y X_2 son dos conjuntos que satisfacen el Axioma 1. Como X_1 satisface el Axioma 1 el Teorema 1.1.3 implica $X_1 \subseteq X_2$. Por otro lado como X_2 también satisface el Axioma 1, el mismo teorema nos daría $X_2 \subseteq X_1$. De donde tenemos la igualdad. ∎

Hacer un estudio profundo de la axiomática de conjuntos en estos momentos sería muy arriesgado, habría muchas posibilidades de que no entendiéramos mucho y por otro lado este no es el objetivo del curso. Vamos entonce algunas reglas (de forma intuitiva) que me permitan trabajar o construir conjuntos, estás reglas están totalmente formalizadas en los axiomas de Zermelo-Fraenkel.

¿Cómo podemos dar un conjunto?

La axiomática nos permite dar un conjunto de dos formas distintas:

- Por extensión.
- Por comprensión.

Daremos un conjunto X por **extensión** cuando especifiquemos todos los elementos de X. Por ejemplo, si ya conocemos otros conjuntos a, b, c, podremos dar un nuevo conjunto cuyos elementos son estos tres conjuntos. Indicaremos esto como:

$$X = \{a, b, c\}.$$

A partir del único conjunto que tenemos hasta ahora, el vacío $\emptyset$ o cero 0, podemos dar (por extensión) un nuevo conjunto:

$$1 = \{\emptyset\} = \{0\}.$$

Este conjunto tiene un sólo elemento que es el conjunto vacío. Ya disponemos de dos conjuntos $\emptyset$ y 1 y por tanto podemos dar (por extensión) otro nuevo conjunto, el que tiene a estos dos como elementos:

$$2 = \{0, 1\}.$$

Podemos ya construir infinitos conjuntos: $3 = \{0, 1, 2\}, 4 = \{01, 2, 3\}, \cdots$.

Sin embargo, **NO** podemos dar por extensión el conjunto

$$\mathbb{N} = \{0, 1, 2, 3, \cdots\},$$

Dar un conjunto por extensión significa dar o listar "*todos sus elementos*" es imposible listar todos los elementos de un conjunto infinito. No vale poner puntos suspensivos y quedarse tan pancho. Necesitaremos un nuevo axioma para poder hablar del conjunto de los números naturales.

Daremos un conjunto por **comprensión** cuanto tengamos una propiedad referente a los elementos de un conjunto ya dado X y nos quedemos con el conjunto de los elementos de X que tienen esa propiedad. Por ejemplo, suponer que hemos podido construir el conjunto $\mathbb{N}$ de los números naturales y que sabemos que significa que un número natural es par. Entonces podemos da por comprensión el conjunto P de los número naturales pares. Indicaremos esto de la siguiente forma:

$$P = \{x \in \mathbb{N}; x \text{ es par }\}.$$

El conjunto de las partes de un conjunto.

Si $A \subseteq S$ diremos que A es un subconjunto de S, de esta manera hemos indicado una propiedad:

Ser subconjunto.

La propiedad de ser subconjunto no está (en principio) referida a los elementos de un conjunto, la axiomática de conjuntos incluye un axioma que permite, dado un conjunto S, construir el conjunto de los subconjuntos de S. Este conjunto es llamado conjunto de las partes (o subconjuntos) de S y lo indicamos:

$$\mathcal{P}(S) = \{A; A \subseteq S\}.$$

Notemos que $\mathcal{P}(S)$ no está definido por comprensión ya que los elementos A en $\mathcal{P}(S)$ no son elementos de un conjunto ya definido. Esto es, para que pudiésemos dar $\mathcal{P}(S)$ por comprensión necesitaríamos un conjunto ?? (que no tenemos) de manera que

$$\mathcal{P}(S) = \{A \in ??; A \subseteq S\}.$$

Necesitamos un axioma que nos permita hablar del conjunto de las partes de un conjunto S.

Como consecuencia del Teorema 1.1.3 tenemos que:

$$\forall S, \emptyset \in \mathcal{P}(S),$$

por tanto $\mathcal{P}(S) \neq \emptyset$ ya que por lo menos tiene un elemento. Por otro lado siempre $S \subseteq S$ y por tanto también tenemos:

$$\forall S, S \in \mathcal{P}(S),$$

Así, podemos concluir que:

- $\forall S, \mathcal{P}(S) \neq \emptyset$ y
- si $S \neq \emptyset$ entonces $\mathcal{P}(S)$ tiene al menos dos elementos $\emptyset$ y S.

Operaciones con conjuntos.

Aunque la axiomática de conjuntos permite definir uniones e intersecciones de conjuntos cualesquiera, vamos a restringir (en un principio) estas construcciones a los subconjuntos de un conjunto dado.

Así A y B son subconjuntos de S, el subconjunto de S de elementos a tales que $a \in A$ y $a \in B$ es llamado la *intersección* de A y B. Lo denotamos por $A \cap B$. Este conjunto puede definirse por comprensión de la siguiente forma:

$$A \cap B = \{a \in S \mid a \in A \wedge a \in B\}.$$

Notar que hemos usado | en lugar de ; en la definición anterior, esta notación también es usual.

Si $A \cap B = \emptyset$, entonces A y B se dicen *disjuntos*.

La unión $A \cup B$ de A y B es el subconjunto de elementos a tales que $a \in A$ o $a \in B$:

$$A \cup B = \{a \in S \mid a \in A \vee a \in B\}.$$

Una importante propiedad que relaciona estas operaciones entre subconjunto de $\mathcal{P}(S)$ es la siguiente.

Proposición 1.1.5 (Propiedad distributiva)**.** *Para cualesquiera subconjuntos $A, B, C \subseteq S$,*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Demostración. Probamos la primera y dejamos la segunda como ejercicio. Sea $a \in A \cap (B \cup C)$. Como $a \in B \cup C$, será $a \in B \vee a \in C$, y como $a \in A$ bien $a \in A \cap B \vee a \in A \cap C$. Se deduce que $a \in (A \cap B) \cup (A \cap C)$. Ahora, sea $a \in (A \cap B) \cup (A \cap C)$. Será $a \in (A \cap B) \vee a \in (A \cap C)$. En cualquier caso $a \in A \wedge a \in B \vee a \in C$. Entonces $a \in A \wedge a \in B \cup C$, o sea que $a \in A \cap (B \cup C)$. ■

Intersecciones y uniones pueden ser definidas para un conjunto arbitrario de subconjuntos de un conjunto S. Sea $\Gamma \subseteq \mathcal{P}(S)$ un tal conjunto de subconjuntos. Entonces definimos su intersección

$$\bigcap_{A\in\Gamma} A = \{a \in S \mid a \in A \; \forall A \in \Gamma\}$$

y su unión

$$\bigcup_{A\in\Gamma} A = \{a \in S \mid \exists A \in \Gamma \mid a \in A\} \, .$$

Si Γ es finito, digamos $\Gamma = \{A_1, A_2, \ldots, A_n\}$, entonces escribimos también $\bigcap_{i=1}^n A_i$ o $A_1 \cap A_2 \cap \cdots \cap A_n$ para su intersección y, análogamente, $\bigcup_{i=1}^n A_i$ o $A_1 \cup A_2 \cup \cdots \cup A_n$ para su unión. Es fácil ver que las propiedades distributivas son válidas para intersecciones y uniones arbitrarias de subconjuntos: $B \cap \bigcup_{A\in\Gamma} A = \bigcup_{A\in\Gamma}(B \cap A)$, $B \cup \bigcap_{A\in\Gamma} A = \bigcap_{A\in\Gamma}(B \cup A)$.

Si $A \subseteq S$ es cualquier subconjunto, se define su *complementario* como

$$c(A) = \{a \in S \mid a \notin A\}.$$

(otras notaciones usuales para este son $\overline{A}$, $S - A$).

Algunas propiedades elementales son:

1. $c(\emptyset) = S$,
2. $c(S) = \emptyset$,
3. $A \cap c(A) = \emptyset$,
4. $A \cup c(A) = S$,
5. $c(c(A)) = A$.

Algo menos evidentes son las siguientes:

Proposición 1.1.6 (Morgan)**.**

$$c(\bigcap_{A\in\Gamma} A) = \bigcup_{A\in\Gamma} c(A), \tag{1.1}$$

$$c(\bigcup_{A\in\Gamma} A) = \bigcap_{A\in\Gamma} c(A). \tag{1.2}$$

Demostración. Probamos la primera. Sea $a \in c(\bigcap_{A\in\Gamma} A)$. Entonces $a \notin \bigcap_{A\in\Gamma} A$ y, por tanto, $\exists A \in \Gamma \mid a \notin A$ o, lo que es lo mismo, $\exists A \in \Gamma \mid a \in c(A)$. Por tanto, $a \in \bigcup_{A\in\Gamma} c(A)$. Supongamos ahora $a \in \bigcup_{A\in\Gamma} c(A)$. Entonces $\exists A \in \Gamma \mid a \in c(A)$ o, lo que es lo mismo, $\exists A \in \Gamma \mid a \notin A$. Pero entonces $a \notin \bigcap_{A\in\Gamma} A$ y, por tanto, $a \in c(\bigcap_{A\in\Gamma} A)$. ■

También se cumple:

Proposición 1.1.7. *Para cualesquiera dos subconjuntos $A, B \in \mathcal{P}(S)$,*

$$A \subseteq B \Leftrightarrow c(B) \subseteq c(A).$$

Demostración. Si $A \subseteq B$, y $a \notin B$, entonces $a \notin A$, luego $c(B) \subseteq c(A)$. Y recíprocamente, si $c(B) \subseteq c(A)$, entonces $A = cc(A) \subseteq cc(B) = B$. ■

Para subconjuntos $A, B \in \mathcal{P}(X)$, es usual también construir el subconjunto

$$A \backslash B = \{a \in A \mid a \notin B\} = A \cap c(B).$$

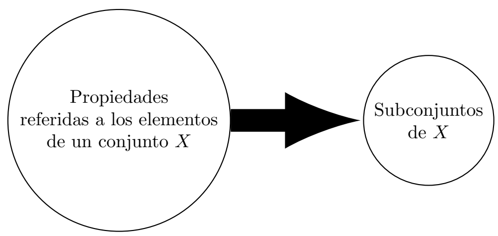
1.1.1 Proposiciones y Demostraciones.

Hemos aceptado que si tenemos una propiedad P referida a los elementos de un conjunto X podemos dar, por comprensión, el subconjunto de los elementos de X que tienen la propiedad P:

$$X_P = \{a \in X \mid a \text{ satisface } P\}.$$

Por ejemplo, si $\mathbb{Z}$ es el conjunto de los números enteros, entonces $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$ es el conjunto de los números naturales, o enteros no negativos.

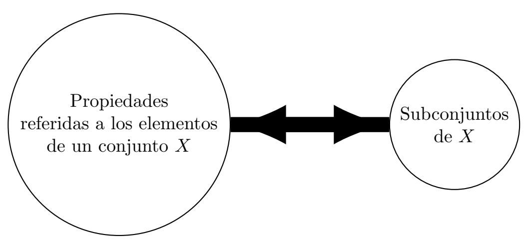
De esta manera podemos asociar a cada propiedad referida a los elementos de un conjunto X un elemento de $\mathcal{P}(X)$:



También podemos ir en sentido contrario. Esto es, a cada subconjunto $A \subseteq X$ le podemos asociar la propiedad referida a los elementos de X:

$P_A =$"ser elemento de A".

De manera que tenemos una equivalencia entre las propiedades referidas a los elementos de X y los subconjuntos de X.



Esta equivalencia nos permite trasladar conceptos de un contexto a otro. De manera que los operadores lógicos corresponden a operaciones en conjuntos. Así por ejemplo:

Si P y Q son propiedades referidas a los elementos de un conjunto X, la propiedad $P \wedge Q$, leída como *"P y Q"*, es aquella que es satisfecha exactamente por los elementos que satisfacen tanto P como Q. De manera que:

$$X_{P \wedge Q} = \{x \in X \mid x \in X_P \wedge x \in X_Q\} = X_P \cap X.Q$$

Decimos entonces que el conectivo lógico $\wedge$ equivale a la operación $\cap$.

Análogamente, la propiedad $P \vee Q$, leída como *"P o Q"*, se define como aquella que satisfacen exactamente los que satisfacen P o satisfacen Q. De forma que

$$X_{P \vee Q} = \{x \in X \mid x \in X_P \vee x \in X_Q\} = X_P \cup X_Q.$$

La propiedad que es verificada por aquellos elementos sobre los que una propiedad P es falsa, es denotada por $\neg P$, y leída como *"no P"*. Así que

$$X_{\neg P} = \{x \in X \mid x \notin X_P\} = c(X_P).$$

Operador lógico		Operación en conjuntos	
y	$\wedge$	$\cap$	intersección
o	$\vee$	$\cup$	unión
no	$\neg$	c	complementario

Table 1.1: Correspondencia operador lógico vs operación conjuntista

Podemos sintetizar esto en la siguiente Tabla 1.1.1:

Una *proposición matemática* es una relación entre dos propiedades P, Q referidas a los elementos de un conjunto X, del tipo $P \Rightarrow Q$, que leemos *"P implica Q"*, y significa que si un elemento de X satisface la propiedad P entonces ese elemento también satisface la propiedad Q.

Esto es:

La proposición $P \Rightarrow Q$ será verdad si $X_P \subseteq X_Q$.

Demostrar una proposición $P \Rightarrow Q$ consistirá precisamente en probar la inclusión $X_P \subseteq X_Q$.

La negación de este hecho que escribimos $P \not\Rightarrow Q$, significa entonces que $X_P \nsubseteq X_Q$, esto es que:

$$\exists a \in X_P;\ a \notin X_Q.$$

Así:

La falsedad de una proposición, se demuestra con un *contraejemplo.*

Una propiedad fundamental en el manejo de las proposiciones es la siguiente

Proposición 1.1.8 (Transitividad)**.** *Sean P, Q y R propiedades referidas a los elementos de un conjunto X. Si $P \Rightarrow Q$ y $Q \Rightarrow R$, entonces $P \Rightarrow R$.*

Demostración. Si $X_P \subseteq X_Q \subseteq X_R$, entonces $X_P \subseteq X_R$. ∎

Cuando se satisface $P \Rightarrow Q$ y $Q \Rightarrow P$, decimos que las propiedades P y Q son*equivalentes*. Será por que $X_P = X_Q$.

Expresamos este hecho simbólicamente por $P \Leftrightarrow Q$, leído como:

Un elemento satisface P si y solo si satisface Q, o *P se satisface cuando y solo cuando Q lo hace.*

El siguiente hecho es un recurso muy utilizado en demostraciones.

Proposición 1.1.9. *Sean P_1, ..., P_n, una lista de propiedades referidas a los elementos de un conjunto X. Si se satisface que $P_1 \Rightarrow P_2$, $P_2 \Rightarrow P_3$, ..., $P_{n-1} \Rightarrow P_n$ y $P_n \Rightarrow P_1$, entonces $P_i \Leftrightarrow P_j$ para todo i, j.*

Demostración. Es consecuencia de la transitividad: Si $i < j$, tenemos que $P_i \Rightarrow P_j$ y también $P_j \Rightarrow P_1 \Rightarrow P_i$. ∎

Proposición 1.1.10. *Para cualesquiera dos subconjuntos $A, B \in \mathcal{P}(X)$,*

$$A \subseteq B \Leftrightarrow c(B) \subseteq c(A).$$

Demostración. Si $A \subseteq B$, y $a \notin B$, entonces $a \notin A$, luego $c(B) \subseteq c(A)$. Y recíprocamente, si $c(B) \subseteq c(A)$, entonces $A = cc(A) \subseteq cc(B) = B$. ∎

El siguiente hecho también es un recurso muy utilizado en demostraciones.

Proposición 1.1.11. *Sean P y Q propiedades referidas a elementos de un con junto X. Las siguientes proposiciones son equivalentes (en el sentido de que se satisface una si y solo si se satisface la otra, por tanto demostrar una es equivalente a demostrar la otra):*
(i) $P \Rightarrow Q$.
(ii) $\neg Q \Rightarrow \neg P$.

Demostración. $X_P \subseteq X_Q$ equivale a que $c(X_Q) \subseteq c(X_P)$. ∎

Cuando uno demuestra $\neg Q \Rightarrow \neg P$ para probar $P \Rightarrow Q$, se dice que razonamos el ***contrarecíproco*** de la proposición original.

También se suele decir que demostramos $P \Rightarrow Q$ *por reducción al absurdo*: Supongamos que un elemento verifica P pero no Q. Entonces verifica $\neg Q$ y, por tanto, $\neg P$. Es decir, que no verifica P en contradicción a la hipótesis.

Ejercicios

En los siguientes enunciados, $A, B, C, \ldots$ refieren a subconjuntos arbitrarios de un conjunto dado X, y se pide demostrar la veracidad de las equivalencias o igualdades propuestas.

1. $A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

2. $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$.

3. (a) $A \cap B = \emptyset \Leftrightarrow A \subseteq c(B) \Leftrightarrow B \subseteq c(A)$.
   (b) $A \cup B = X \Leftrightarrow c(A) \subseteq B \Leftrightarrow c(B) \subseteq A$.

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

5. (a) $A - B = A \Leftrightarrow A \cap B = \emptyset$.
   (b) $A \cap (B - C) = (A \cap B) - (A \cap C)$.

6. Siendo la "*diferencia simétrica*" $A \triangle B$ de A y B el subconjunto
$$A \triangle B = (A - B) \cup (B - A),$$
   (a) $A \triangle B = (A \cup B) - (A \cap B)$.
   (b) $A \triangle B = B \triangle C$.
   (c) $A \triangle \emptyset = A$.
   (d) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
   (e) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

7. Si A y B son finitos, $|A \cup B| + |A \cap B| = |A| + |B|$.

8. Si A, B, y C son finitos,

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

En los siguientes enunciados, $P, Q, R, ...$ refieren a propiedades que pueden ser satisfechas, o no, por los elementos de un conjunto X. Se pide demostrar la veracidad de las proposiciones o propuestas siguientes.

9. (a) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$.
   (b) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$.

10. Las siguientes proposiciones son equivalentes:
    (a) $P \Rightarrow Q$.
    (b) $P \vee Q \Leftrightarrow Q$.
    (c) $P \wedge Q \Leftrightarrow P$.

11. (a) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$.
    (b) $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$.

12. $(P \vee \neg Q) \vee (P \vee \neg R) \Leftrightarrow P \vee \neg(Q \wedge R)$.

13. $P \vee Q \vee \neg Q \Leftrightarrow P \vee Q \vee \neg(P \vee R)$.

14. $(P \vee \neg Q) \wedge (Q \vee \neg P) \Leftrightarrow (P \wedge Q) \vee \neg(P \vee Q)$.

1.2 El conjunto producto cartesiano. Aplicaciones

Si S y T son conjuntos, su *producto cartesiano*, denotado $X \times Y$, es el conjunto de todos los pares ordenados (x, y) con $x \in S$ e $y \in T$:

$$S \times T = \{(x, y) \mid x \in S,\ y \in T\}.$$

En este conjunto, los elementos (x, y) y (x', y') son considerados iguales si y solo si $x = x'$ e $y = y'$. Así, si $|S| = m$ y $|T| = n$, entonces $|S \times T| = mn = |S|\,|T|$. Los conjuntos S y T no tienen que ser distintos. Cuando $S = T$, escribimos también S^2 en lugar de $S \times S$.

Más generalmente, desde n conjuntos dados listados en un cierto orden, S_1, ..., S_n, podemos formar el producto

$$S_1 \times S_2 \times \cdots \times S_n = \prod_{i=1}^{n} S_i = \{(x_1, x_2, \cdots, x_n) \mid x_i \in S_i\ \forall\, i = 1, \ldots, n\};$$

cuando $S_1 = S_2 = \cdots = S_n = S$ uno también escribe S^n en lugar de $S_1 \times S_2 \times \cdots \times S_n$.

Definición 1.2.1. *Una "aplicación" es una terna de datos (S, T, f), donde S es un conjunto, llamado el "dominio" de la aplicación, T es otro conjunto, llamado el "rango" de la aplicación, y $f \subseteq S \times T$ es un subconjunto del producto cartesiano, llamado su "grafo" , tal que las siguientes dos propiedades se verifican.*

1. *Para cualquier $x \in S$ existe un $y \in T$ tal que $(x, y) \in f$.*

2. *Si $(x, y), (x', y') \in f$, entonces $x = x' \Rightarrow y = y'$.*

Dos aplicaciones son consideradas iguales si y solo si tienen el mismo dominio, el mismo rango y los mismos grafos.

La notación usual para una tal aplicación es escribir $f : S \to T$ o $S \xrightarrow{f} T$, y uno se refiere a ella como *la aplicación f del conjunto S en el conjunto T* Las condiciones anteriores establecen que para cualquier elemento x del dominio hay un único elemento y del rango tal que (x, y) pertenece al grafo. La notación usual para ese elemento es $f(x)$, al que uno se refiere como la *imagen de x por f*, o *el elemento de T que corresponde a x por f*.

Para conocer una aplicación $f : S \to T$ es suficiente especificar la imagen $f(x)$ en T de cada elemento x de S. Usualmente, esto se hace proponiendo una fórmula que determina, para cada $x \in S$, su imagen $f(x) \in T$. Pero hay que ser cuidadoso en esto: Es necesario garantizarse que cada elemento de S tiene "bien definida su imagen" $f(x)$, esto es, que cada elemento S tiene una imagen y solo una.

EJEMPLOS.

1. Sea $\mathbb{N} = \{0, 1, 2, \ldots, \}$ el conjunto de los números naturales. No existe una aplicación $f : \mathbb{N} \to \mathbb{N}$ tal que la imagen de cada natural x venga dada por la fórmula $f(x) = x - 1$, pues el 0 no tiene asignado imagen. Esa fórmula, sin embargo si define una aplicación $f : \mathbb{Z} \to \mathbb{Z}$.

2. No existe una aplicación $f : \mathbb{N} \to \mathbb{N}$ tal que la imagen $f(x)$ de cada natural x venga dada por la fórmula

$$f(x) = \begin{cases} x & \text{si} \quad x \text{ no es múltiplo de 2 ni de 3} \\ x/2 & si \quad x \text{ es un múltiplo de 2,} \\ x/3 & si \quad x \text{ es un múltiplo de 3,} \end{cases}$$

pues hay naturales que corresponden a más de uno (es decir, con más de una imagen): $f(6) = 6/2 = 3$ y $f(6) = 6/3 = 2$. Esto es, los elementos $(6,2)$ y $(6,3)$ pertenecerían al grafo!.

3. Hay una aplicación $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $(m,n) \mapsto m+n$.

4. La correspondencia $x \mapsto f(x) = \frac{x^2+1}{x-1}$ define una aplicación $f : (0,1) \to \mathbb{R}$, pero no una aplicación $f : [0,1] \to \mathbb{R}$.

Usualmente, el subconjunto de todas las imágenes de una aplicación $f : S \to T$

$$Im(f) = \{y \in T \mid y = f(x) \text{ para algún } x \in S\} = \{f(x) \mid x \in S\}$$

es llamado la *imagen* de la aplicación.

La aplicación es llamada *sobreyectiva* is $Im(f) = T$, esto es, cuando todo elemento del rango es imagen de algún elemento del dominio.

La aplicación es llamada *inyectiva* si distintos elementos del dominio tienen distintas imágenes, esto es, si $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.

Si la aplicación f es simultáneamente inyectiva y sobreyectiva, entonces es llamada una *biyección*. Así, una aplicación $f : S \to T$ es una biyección cuando y solo cuando $\forall y \in T, \exists! x \in S \mid f(x) = y$. Si es posible establecer una biyección $f : S \to T$, se dice que S es biyectivo con T, y se expresa escribiendo $S \cong T$.

Ejemplos. Sea $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ el conjunto de los números enteros.

1. La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ tal que $f(x) = x^2$, no es inyectiva ni sobreyectiva.

2. La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ tal que $f(x) = 2x$, es injectiva pero no sobreyectiva.

3. La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ tal que $f(x) = x + 2$ es biyectiva.

4. Denotemos por $\mathbf{2} = \{0,1\}$ al conjunto con dos elementos, y sea $\mathbf{2}^S$ al conjunto de todas las aplicaciones $f : S \to \mathbf{2}$. Si $A \in \mathcal{P}(S)$, se define su *aplicación característica* $\chi_A : S \to \mathbf{2}$ por
$$\chi_A(x) = \begin{cases} 1 & \text{si} \quad x \in A, \\ 0 & \text{si} \quad x \notin A. \end{cases}$$
La correspondencia $A \mapsto \chi_A$, nos define una aplicación biyectiva $\chi : \mathcal{P}(S) \cong \mathbf{2}^S$: Si $\chi_A = \chi_B$, entonces $A = \{x \in S \mid \chi_A(x) = 1\} = \{x \in S \mid \chi_B(x) = 1\} = B$, por tanto χ is inyectiva. Para ver que es sobreyectiva, supongamos $f : S \to \mathbf{2}$ cualquier aplicación. Sea $A = \{x \in S \mid f(x) = 1\}$. Entonces $\chi_A = f$, pues dado cualquier $x \in S$, si $f(x) = 1$ entonces $x \in A$ y $\chi_A(x) = 1$, y si $f(x) = 0$, entonces $x \notin A$ y también $\chi_A(x) = 0$.

Sean $S \xrightarrow{f} T$ y $T \xrightarrow{g} U$ dos aplicaciones, donde el rango de f coincide con el dominio de g, de manera que se pueden escribir consecutivamente como $S \xrightarrow{f} T \xrightarrow{g} U$. Se define su *composición* como la aplicación $S \xrightarrow{gf} U$, cuyo dominio es S, el rango es U y, para cualquier $x \in S$,
$$(gf)(x) = g(f(x)).$$

La composición de aplicaciones satisface la *ley asociativa*: Si $S \xrightarrow{f} T \xrightarrow{g} U \xrightarrow{h} V$ son aplicaciones, entonces $h(gf) = (hg)f$. En efecto, ambas tienen el mismo dominio S, el mismo rango T y, para cualquier $x \in S$,

$$\begin{aligned}(h(gf))(x) = h((gf)(x)) = h(g(h(x))),\\ ((hg)f)(x) = (hg)(f(x)) = h(g(f(x))),\end{aligned}$$

por tanto que son la misma aplicación. Es usual escribir simplemente hgf para designarla.

Si $S \xrightarrow{f} T \xrightarrow{g} U$ son aplicaciones componibles y $h : S \to U$ es una aplicación, es usual indicar la igualdad $h = gf$ diciendo que el triángulo

$$\begin{tikzcd} & T \arrow[dr, "g"] & \\ S \arrow[ur, "f"] \arrow[rr, "h"] & & U \end{tikzcd}$$

es conmutativo, o que $h \neq gf$, diciendo que el triángulo no es conmutativo. Análogamente, un rectángulo de aplicaciones

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[d, "f'"'] & T \arrow[d, "g"] \\ T' \arrow[r, "g'"] & U \end{tikzcd}$$

es conmutativo, si $gf = g'f'$. En general, la conmutatividad de un diagrama de aplicaciones, cuando tiene sentido, significa que las aplicaciones obtenidas por composición desde un vértice inicial hasta uno terminal según las diferentes rutas son la mismas. Por ejemplo, la conmutatividad del diagrama

$$\begin{tikzcd} & & B \arrow[ddr, "g"] & \\ & A \arrow[ur, "f"] \arrow[drr, "h"] \arrow[dl, "i"'] & & \\ E \arrow[dr, "j"] & & & C \\ & D \arrow[urr, "k"'] & & \end{tikzcd}$$

significa que $gf = h = kji$.

Para cualquier conjunto S, se define la aplicación *identidad* en S, $id_S : S \to S$ (o 1_S, o 1 si S es claro por el contexto) como la aplicación tal que $id_S(x) = x$, para todo $x \in S$. Es la aplicación de S en si mismo cuyo grafo es la *diagonal* $\Delta = \{(x, x) \mid x \in S\}$. Si $f : S \to T$ es cualquier aplicación, uno verifica inmediatamente que $id_T f = f = f\, id_S$.

Lema 1.2.2. *Si $S \xrightarrow{f} T$ y $T \xrightarrow{g} S$ son dos aplicaciones tal que $gf = id_S$, es decir, tal que el triángulo*

$$\begin{tikzcd} & T \arrow[dr, "g"] & \\ S \arrow[ur, "f"] \arrow[rr, "id_S"] & & S \end{tikzcd}$$

conmuta, entonces f es inyectiva y g es sobreyectiva.

Demostración. Supongamos que $f(x) = f(y)$, para ciertos $x, y \in S$. Entonces $x = id_S(x) = gf(x) = gf(y) = id_S(y) = y$. Así que f es inyectiva. Dado cualquier $x \in S$, como $x = id_S(x) = gf(x) = g(f(x)$, es $x \in Im(g)$, luego g es sobreyectiva. ■

Supongamos ahora que $S \xrightarrow{f} T$ tal que existe una otra $T \xrightarrow{g} S$ tal que $gf = id_S$ y $fg = id_T$. Entonces f es inyectiva y sobreyectiva, por el lema, y por tanto una biyección. Recíprocamente, si f es biyectiva, entonces podemos encontrar una aplicación $g : T \to S$ tal que $gf = id_S$ y $fg = id_T$: Para cada $y \in T$, sea $g(y) \in S$ el único elemento de S tal que $f(g(y)) = y$. Esto define una tal aplicación g, claramente verificando que $fg = id_T$. Además, para cualquier $x \in S$, como obviamente $x \mapsto f(x)$, es $g(f(x)) = x$, así que $gf = id_S$. Esto prueba que

Proposición 1.2.3. *Una aplicación $f : S \to T$ es biyectiva si y solo si existe una aplicación $g : Y \to X$ tal que $gf = id_S$ y $fg = id_T$.*

Para $f : S \to T$ una biyección, solo existe una aplicación $g : T \to S$ tal que $gf = id_S$ y $fg = id_T$: Si $g' : T \to S$ es otra con $g'f = id_S$ y $fg' = id_T$, entonces

$$g' = g' id_T = g' fg = id_S g = g.$$

Esa única g es llamada la *inversa* de f y es denotada por f^{-1}. Si $f : S \to T$ es biyectiva, entonces su inversa $f^{-1} : T \to S$ es la única aplicación tal que $f^{-1}f = id_T$ y $ff^{-1} = id_T$. Observar que f^{-1} también es biyectiva y $(f^{-1})^{-1} = f$.

Como una primera aplicación del criterio de biyectividad anterior, podemos dar una demostración del hecho (bastante obvio) de que la composición de dos aplicaciones biyectivas es biyectiva: Sean $f : S \to T$ y $g : T \to U$ biyecciones, y consideremos su composición $gf : S \to U$. Entonces, tenemos sus inversas $g^{-1} : U \to T$ y $f^{-1} : T \to S$, y su compuesta $f^{-1}g^{-1} : U \to S$. Además

$$\begin{aligned}
(f^{-1}g^{-1})(gf) &= f^{-1}(g^{-1}(gf)) = f^{-1}((g^{-1}g)f) = f^{-1}(id_T f) = f^{-1}f = id_S, \\
(gf)(f^{-1}g^{-1}) &= g(f(f^{-1}g^{-1})) = g((ff^{-1})g^{-1}) = g(id_T g^{-1}) = gg^{-1} = id_U.
\end{aligned}$$

Así que gf es biyectiva, con inversa

$$(gf)^{-1} = g^{-1}f^{-1}.$$

La siguiente observación para conjuntos finitos es útil en muchas ocasiones

Lema 1.2.4. *Sea S un conjunto finito. Las siguientes propiedades para $f : S \to S$ son equivalentes:*

1. *f es biyectiva.*

2. *f es inyectiva.*

3. *f es sobreyectiva.*

Demostración. Supongamos que $|S| = n$. Si f es inyectiva, entonces $|Im(f)| = n$, luego $Im(f) = S$ y f es sobreyectiva. Recíprocamente, si f no es inyectiva, entonces $|Im(f)| < n$, luego f no es sobreyectiva. ■

1.2.1 Imágenes directas e inversas

Toda aplicación $f : S \to T$ determina otras

$$f_* : \mathcal{P}(S) \to \mathcal{P}(T), \quad f^* : \mathcal{P}(T) \to \mathcal{P}(S),$$

llamadas las aplicaciones *imagen* e *imagen inversas* por f, respectivamente, que están definidas, para cada $A \subseteq S$ y $X \subseteq T$, por

$$f_*(A) = \{f(a) \mid a \in A\}, \quad f^*(X) = \{a \in S \mid f(a) \in X\}.$$

Dejaremos como ejercicios las siguientes propiedades de las imágenes directas o inversas. Dada una aplicación $f : S \to T$, $A, B \subseteq S$ subconjuntos de S y $X, Y \subseteq T$ son subconjuntos de T.

1. Probar que $f^*(X \cup Y) = f^*(X) \cup f^*(Y)$ y $f_*(A \cup B) = f_*(A) \cup f_*(B)$.
2. Probar que $f^*(X \cap Y) = f^*(X) \cap f^*(Y)$ y $f_*(A \cap B) \subseteq f_*(A) \cap f_*(B)$.
3. Demostrar que si f es inyectiva, entonces $f_*(A \cap B) = f_*(A) \cap f_*(B)$.
4. Demostrar con el siguiente ejemplo que, en general, $f_*(A \cap B) \neq f_*(A) \cap f_*(B)$: Sea $f = |\ | : \mathbb{R} \to \mathbb{R}$ la aplicación "valor absoluto", $A = (0, 1)$ y $B = (-1, 0)$.
5. $f_*(f^*(X)) \subseteq X$, y se da la igualdad si f es sobreyectiva.
6. $A \subseteq f^*(f_*(A))$, y se da la igualdad si f es inyectiva.
7. Probar que, si f es una biyección entonces las aplicaciones $f_* : \mathcal{P}(S) \to \mathcal{P}(T)$ y $f^* : \mathcal{P}(T) \to \mathcal{P}(S)$ son biyectivas e inversas una de la otra.

EJERCICIOS

1. Sean $f : S \to T$ y $g : T \to U$ aplicaciones.
   (a) Probar que si ambas son inyectivas, entonces su composición $gf : S \to U$ es también inyectiva.
   (b) Probar que si ambas son sobreyectivas, entonces su composición $gf : S \to U$ es también es sobreyectiva.
   (c) Si su compuesta $gf : S \to U$ es inyectiva o sobreyectiva ¿qué podemos decir sobre f y g?
2. Sea $f : S \to T$ una aplicación.
   (a) Probar que f es inyectiva si y solo si tiene una *inversa por la izquierda*, es decir, existe una aplicación $g : T \to S$ tal que $gf = id_S$.
   (b) Dar un ejemplo de una aplicación inyectiva con dos diferentes inversas por la izquierda.
   (c) Probar que f es sobreyectiva si y solo si tiene una *inversa por la derecha*, es decir, existe una aplicación $g : T \to S$ tal que $fg = id_T$.
   (d) Dar un ejemplo de una aplicación sobreyectiva con dos diferentes inversas por la derecha.

3. En los siguientes ejercicios S y T son dos conjuntos arbitrarios, A, A' son subconjuntos de S y B, B' son subconjuntos de T.

   (a) i. Probar $A \times B$ es un subconjunto de $S \times T$.

       ii. Probar, con el siguiente ejemplo, que no todo subconjunto X de $S \times T$ es de la forma $X = A \times B$: $S = T = \{0, 1\}$, $X = \{(0, 0), (1, 1)\} \subseteq S \times T$.

   (b) Probar las siguientes igualdades:

       i. $c(A \times B) = c(A) \times T \cup S \times c(B)$.

       ii. $(A \cup A') \times B = (A \times B) \cup (A' \times B)$.

       iii. $(A \cap A') \times B = (A \times B) \cap (A' \times B)$.

       iv. $(A \cap A') \times (B \cap B') = (A \times B) \cap (A' \times B')$.

       v. $(A \cup A') \times (B \cup B') = (A \times B) \cup (A' \times B) \cup (A \times B') \cup (A' \times B')$.

4. Se consideran los subconjuntos de $\mathbb{R}$, $S = [-1, 1]$, $T = [-3, 4]$. Describir en dibujo los siguientes recintos de $\mathbb{R}^2$: $S \times T$, $T \times S$, $(S \times T) \cup (T \times S)$, $(S \times T) \cap (T \times S)$, $(S \times T) - (T \times S)$, $(T \times S) - (S \times T)$.

1.3 Relaciones de equivalencia. Conjuntos cocientes.

Definimos una *relación* (binaria) entre los elementos de un conjunto S (o, simplemente, en S) como un subconjunto $R \subseteq S \times S$.

Si $(a, b) \in R$, se dice que *a está relacionado con b por la relación R*, y se escribe aRb. Muchas relaciones tienen una o más de las siguientes propiedades:

- **Reflexiva**. $\forall a \in S$, aRa,.
- **Simétrica**. $\forall a, b \in S$, si aRb, entonces bRa.
- **Transitiva**. $\forall a, b, c \in S$, si aRb y bRc, entonces aRc.

Por ejemplo:

1. La relación "a es padre de b" referida al conjunto de los humanos, no tiene ninguna de estas propiedades.

2. La relación"a tiene los mismos parientes que b" tiene las tres.

3. La relación "a es antecesor de b" es transitiva.

4. La relación "a es hermano de b" es simétrica.

Una relación R en un conjunto S que es reflexiva, simétrica y transitiva es llamada una *relación de equivalencia* sobre S.

Una relación de equivalencia separa los elementos del conjunto S en *bloques* o *clases de equivalencia* donde se agrupan todos los elementos que se relacionan entre sí por la relación dada. Si $a \in S$ es cualquier elemento, definimos "*su clase de equivalencia*" o "*la clase de equivalencia que representa* a", denotada por $\bar{a}$ (o $[a]$), como el subconjunto de S

$$\bar{a} = \{x \in S \mid xRa\},$$

donde se reúnen todos los elementos equivalentes a a. Cada uno de estos subconjuntos es no vacío, pues por la reflexividad $a \in \bar{a}$, y se verifica que cualesquiera dos bloques $\bar{a}$, $\bar{b}$ bien son disjuntos o coinciden:

Proposición 1.3.1. *Para cualesquiera $a, b \in S$, son equivalentes*

1. $\bar{a} \cap \bar{b} \neq \emptyset$.

2. aRb.

3. $\bar{a} = \bar{b}$.

Demostración. (1) $\Rightarrow$ (2): Supongamos que $\exists c \in \bar{a} \cap \bar{b}$. Como cRa y cRb, por la simetría, tenemos aRc y cRb, y entonces, por la transitividad, aRb.

(2) $\Rightarrow$ (3): Si $x \in \bar{a}$, entonces $xRa \wedge aRb \Rightarrow xRb \Rightarrow x \in \bar{b}$, así que $\bar{a} \subseteq \bar{b}$. Un argumento similar prueba que $\bar{b} \subseteq \bar{a}$ y por tanto $\bar{a} = \bar{b}$.

(3) $\Rightarrow$ (1) Es obvio. ■

Resulta así que las diferentes clases de equivalencia proporcionan una descomposición S en subconjuntos no vacíos dos cualesquiera de ellos son disjuntos. Esto es lo que se llama una *partición* de S.

Por ejemplo, si R es la relación "a tiene los mismos parientes que b" entre los españoles, que es claramente de equivalencia, agrupa a los españoles en bloques conformados por las familias.

Si R es la relación entre los puntos del plano $\mathbb{R}^2$ estableciendo que pRq si p y q están a la misma distancia del origen, los bloques son las circunferencias $C_r = \bar{r}$ centradas en el origen y radio r, con $r \geq 0$.

Similarmente, si R es la relación "a da el mismo resto que b al dividirlo por 2" sobre el conjunto $\mathbb{N} = \{0, 1, \dots\}$ de los números naturales, esta relación parte el conjunto de naturales en dos subconjuntos disjuntos, de una parte el conjunto de los números pares, $\overline{[0]}$, y de otra el conjunto de los impares, $\bar{1}$.

Dada una relación de equivalencia R sobre un conjunto S, se define el *conjunto cociente de S por la relación R*, denotado S/R, como el conjunto cuyos elementos son los diferentes bloques o clases de equivalencia para tal relación:

$$S/R = \{\bar{a} \in \mathcal{P}(S) \mid a \in S\}.$$

En tal descripción, es muy importante tener claro que, aunque los elementos de S/R están parametrizados por los elementos a de S, tal parametrización no es unívoca pues tenemos que tener muy presente que

$$\bar{a} = \bar{b} \Leftrightarrow aRb.$$

Desde esa observación, puede pensarse en el conjunto cociente S/R como el *que se obtiene a considerar iguales (el mismo, identificados) todos los elementos de S que son equivalentes entre sí por la relación dada.*

Así, por ejemplo, para la relación R sobre $\mathbb{N}$ donde dos números son equivalentes si dan el mismo resto al dividirlos por 2, el conjunto cociente tiene exactamente dos elementos

$$S/R = \{\bar{0}, \bar{1}\},$$

puesto que para cualquier natural n, $\bar{n} = \bar{0}$ si n es par, y $\bar{n} = \bar{1}$ si n es impar.

Análogamente, Si R es la relación entre los puntos del plano $\mathbb{R}^2$ estableciendo que dos puntos p y q son equivalentes si están a la misma distancia del origen, el conjunto cociente

$$\mathbb{R}^2/R = \{C_r \mid r \in \mathbb{R}, r \geq 0\}$$

es el conjunto de las diferentes circunferencias centradas en el origen del plano $\mathbb{R}^2$ (¡sus elementos son circunferencias, no puntos!).

La proyección canónica. Dada una relación de equivalencia R en un conjunto S se tiene una aplicación que llamaremos la proyección canónica $p : S \to S/R$ y que lleva un elemento $x \in S$ en su clase de equivalencia, $p(x) = \bar{x}$. Esta aplicación es claramentee sobreyectiva.

La relación núcleo de una aplicación. Toda aplicación $f : S \to T$ da lugar a una relación de equivalencia R_f en su dominio S, definida por $xR_f y \Leftrightarrow f(x) = f(y), \forall x, y \in S$. Esta relación es llamada la relación núcleo de f.

Notación. A la relación úcleo de una aplicación f también la denotaremos como $\sim_f$.

Notemos que la relación de equivalencia asociada a la proyección canónica $p : S \to S/R$ es precisamente R, i.e. $R_p = R$.

La siguiente observación es muy útil para definir aplicaciones desde un conjunto cociente.

Proposición 1.3.2. *Sea R una relación de equivalencia sobre un conjunto S. Sea $f : S \to T$ una aplicación con la propiedad*

$$\forall a, b \in S, \text{ si } aRb \text{ entonces se verifica que } f(a) = f(b).$$

Entonces hay una aplicación $\bar{f} : S/R \to T$ *definida por la fórmula*

$$\bar{f}(\bar{a}) = f(a), \forall \bar{a} \in S/R.$$

Se verifica que $Im(\bar{f}) = Im(f)$*, por tanto que* $\bar{f}$ *es sobreyectiva si y solo si* f *lo es. Además* $\bar{f}$ *es inyectiva si y solo si se verifica que*

$$\forall a, b \in S, \ \text{si } f(a) = f(b), \ \text{entonces } aRb.$$

Demostración. Hemos de comprobar que la correspondencia $\bar{a} \mapsto f(a)$ define una aplicación de S/R en T. La primera condición de aplicación es clara, pues $\forall \bar{a} \in S/R$ tenemos que $(\bar{a}, f(a)) \in f$, esto es, todo elemento tiene asignada una imagen. Para ver la segunda, esto es que cada elemento tiene asignada una única imagen, supongamos que $(\bar{a}, f(a)), (\bar{b}, f(b)) \in S/R$, y que $\bar{a} = \bar{b}$. Entonces aRb y, por hipótesis, $f(a) = f(b)$. Luego, efectivamente, tenemos una aplicación bien definida.

La afirmación $Im(\bar{f}) = Im(f)$, y su consecuencia sobre la sobreyectividad, es inmediata. Para estudiar la inyectividad de $\bar{f}$, notemos que $\bar{f}(\bar{a}) = \bar{f}(\bar{b}) \Leftrightarrow f(a) = f(b)$. Par tanto, $\bar{f}$ será inyectiva si y solo si $f(a) = f(b) \Rightarrow \bar{a} = \bar{b}$ o, equivalentemente, $f(a) = f(b) \Rightarrow aRb$. ■

La aplicación $\bar{f} : S/R \to T$ es llamada la *inducida por* f *en el cociente*. Esta asigna a cada clase de equivalencia el valor que f asigna a cualquiera de sus representantes lo que, lógicamente, explica la condición de que f sea constante sobre elementos relacionados.

Ejemplo. Consideremos $[0, 1] \subseteq \mathbb{R}$, el intervalo cerrado de la recta real formado por los números t tales que $0 \leq t \leq 1$. Definamos en él la relación de equivalencia R por la que identificamos los puntos 0 y 1, y solo estos. Más precisamente, decimos que

$$tRu \Leftrightarrow \begin{cases} \text{si } t, u \in \{0, 1\} \\ t = u \text{ en otro caso} \end{cases}$$

De manera que el conjunto cociente $[0, 1]/R$ consiste del bloque $\bar{0} = \bar{1} = \{0, 1\}$ y de los bloques unitarios $\bar{t} = \{t\}$ con $0 < t < 1$.

Consideremos ahora la aplicación $f : [0, 1] \to C_1$, donde $C_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ es la circunferencia del plano real con radio 1 y centrada en el origen, definida por

$$f(t) = (cos(2\pi t), sen(2\pi t)), \quad 0 \leq t \leq 1.$$

Puesto que f es sobreyectiva y $f(t) = f(u) \Leftrightarrow tRu$, tenemos una biyección inducida

$$[0, 1]/R \cong C_1$$

que permite pensar a la circunferencia como el resultado de identificar los extremos del intervalo $[0, 1]$.

Como consecuencia inmediata de la Proposición 1.3.2 tenemos el siguiente

Teorema 1.3.3 (Descomposición canónica de una aplicación.)**.** *Dada una aplicación* $f : S \to T$ *existe un isomorfismo* $b : S/R_f \xrightarrow{\cong} Im(f)$ *que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[d, "p"'] & T \\ S/R_f \arrow[r, "\cong", "b"'] & Im(f) \arrow[u, hook, "i"'] \end{tikzcd}$$

donde p *es la proyección canónica e* i *es la inclusión.*

Demostración. Ya que, por definición $xR_fy \Leftrightarrow f(x) = f(y)$, la Proposición 1.3.2 nos permite definir $\bar{f} : S/R_f \to T$ como $\bar{f}(\bar{x}) = f(x)$ que además será inyectiva y cumple $fp(x) = f(x)$. Definimos entonces $b : S/R_f \to Im(f)$ como $b(\bar{x}) = \bar{f}(\bar{x}) = f(x)$ y tenemos el teorema. ∎

EJERCICIOS

1. Sea $\mathbb{N} = \{0, 1, 2 \ldots, \}$ el conjunto de los números naturales, Sobre $\mathbb{N}^2 = \mathbb{N}\times\mathbb{N}$ definimos $(a, b) \sim (c, d)$ si $a + d = b + c$.
   (a) Verificar que $\sim$ es una relación de equivalencia.
   (b) Sea $f : \mathbb{N}^2 \to \mathbb{Z}$ la aplicación definida por $f(a, b) = a - b$. Verificar que f induce una biyección $\mathbb{N}^2/\!\sim\, \cong \mathbb{Z}$.

2. ¿Qué está mal en la siguiente demostración de que toda relación R sobre S que es simétrica y transitiva es reflexiva? Para $a, b \in S$, aRb, implica bRa (por simetría) y entonces (por transitividad) aRa.

3. Sea $f : S \to T$ una aplicación. Probar que, si f es sobreyectiva, induce una biyección $S/R_f \cong T$.

4. Sea $Y \subseteq X$ un subconjunto. Sea $f : \mathcal{P}(X) \to \mathcal{P}(Y)$ la aplicación tal que $f(A) = A\cap Y$, para cada $A \in \mathcal{P}(X)$.
   (a) Probar que f es una sobreyección.
   (b) Describir la relación R_f, núcleo de f.
   (c) Probar que f induce una biyección $\mathcal{P}(X)/R_f \cong \mathcal{P}(Y)$.

5. Sea R una relación de equivalencia sobre el conjunto S. La aplicación $p : S \to S/R$ definida por $p(a) = \bar{a}$ es llamada la *proyección canónica* de S sobre el cociente ¿Qué relación hay entre R y R_p?

6. Un subconjunto $P \subseteq \mathcal{P}(S)$, recordar, es llamado una *partición del conjunto* S si
   (a) $\forall A \in P,\ A \neq \emptyset$.
   (b) $\bigcup_{A\in P} A = S$.
   (c) Para cualesquiera $A, B \in P$, $A \neq B$, se verifica que $A \cap B = \emptyset$.

   Así, por ejemplo, el conjunto cociente S/R, para R una relación de equivalencia sobre S, es una partición.

   Sea P una partición de S. Definimos la aplicación $p : S \to P$ por $p(a) = A$ si $a \in A$. ¿Qué relación hay entre P y S/R_p?