~~Muy~~ breve introducción a la lógica, los conjuntos, los enteros y los temas que se vayan acumulando

Ilán A. Goldfeder

5 de julio de 2019

Las definiciones son importantes en matemáticas. Creo que para muchos problemas, cuya resolución puede parecer difícil a primera vista, basta con entender qué significan cada uno de los elementos involucrados para facilitar su respuesta.

Índice

1 Una introducción a la lógica **3**
- 1.1 Conectivos lógicos . . . 3
- 1.2 Tablas de verdad . . . 4
- 1.3 La implicación . . . 5
- 1.4 Otros elementos de la lógica . . . 6
  - 1.4.1 Relación entre cuantificadores universales y existenciales 9

2 Las pruebas **10**
- 2.1 ¿Qué significa que $P \Rightarrow Q$ sea verdadera? . . . 11
- 2.2 Tipos de pruebas . . . 12
  - 2.2.1 Pruebas directas . . . 12
  - 2.2.2 Pruebas por contraposición . . . 12
  - 2.2.3 Pruebas por reducción al absurdo o por contradicción . 12
  - 2.2.4 Pruebas por casos . . . 13

3 Los conjuntos **14**
3.1 Ejemplos 16
3.1.1 El conjunto vacío 16
3.1.2 Los conjuntos unitarios 16
3.1.3 Las parejas no ordenadas 16
3.1.4 Algunos conjuntos de números 17
3.2 Propiedades de los conjuntos 17
3.2.1 La igualdad de conjuntos 17
3.2.2 Orden y repetición de elementos en conjuntos 18
3.2.3 Los subconjuntos 18
3.2.4 El conjunto potencia 21
3.2.5 Diagramas de Venn 21
3.2.6 Operaciones de conjuntos: la unión 21
3.2.7 Operaciones de conjuntos: la intersección 24
3.2.8 Más propiedades sobre la unión y la intersección 25
3.2.9 Operaciones de conjuntos: diferencia y complemento . 27
3.2.10 Las leyes de De Morgan 28
3.3 Parejas ordenadas y el producto cartesiano 30
3.3.1 Relaciones binarias 31
3.3.2 Pruebas por vacuidad 32
3.3.3 Algunas propiedades de las relaciones 33
3.3.4 Algunos ejemplos 33

4 Funciones **34**
4.1 Ejemplos de funciones 39
4.2 Inyectiva, suprayectiva y biyectiva 40
4.3 Restricciones de las funciones 44
4.4 Composición de funciones 45
4.4.1 Propiedades de la composición de funciones 47
4.5 Funciones inversas 49
4.6 Cardinalidad 51

5 Propiedades de los números enteros **55**

6 Divisibilidad **59**
6.1 Propiedades de la divisibilidad 60

7 Algoritmo de la división **62**
7.1 Principio del Buen Orden 63
7.2 Números primos 65

1 Una introducción a la lógica

Una *proposición* o *enunciado* es una afirmación que **tiene un y sólo un valor de verdad**, es decir, es *verdadero* o *falso* (aunque puede que no lo conozcamos). Por ejemplo, «el 23 de febrero de 1997 cayó en lunes» necesariamente es verdadero o falso, aunque no lo sepas en el momento en que lees este texto[1]. Por otro lado, «¿qué hora es?» u «hoy es un día muy bonito» no son enunciados, el primero no tiene valor de verdad y el segundo está sujeto a quien lo interprete. Usualmente denotamos por letras mayúsculas como P, Q, R, etc. los enunciados.

1.1 Conectivos lógicos

Por medio de los *conectivos lógicos* podemos construir nuevos enunciados a partir de enunciados previos. Supongamos que P y Q son dos enunciados (esto significa que son verdaderos o falsos, pero no ambos ni ninguno). Los conectivos lógicos son:

1. **Disyunción.** $P \vee Q$: «P o Q». La disyunción tiene valor de verdad *verdadera* cuando al menos una de las dos proposiciones que la conforman es verdadera, pero cuando ambas son falsas, la disyunción es *falsa*.

2. **Conjunción.** $P \wedge Q$: «P y Q». La conjunción tiene el valor de verdad *verdadera* cuando **ambas** proposiciones son verdaderas, pero si **al menos una** de las dos es falsa, entonces la conjunción es *falsa*.

3. **Negación.** $\neg P$, $\sim P$: «no P». La negación tiene el valor de verdad contrario al de la proposición que califica.

4. **Implicación.** $P \Rightarrow Q$: «si P entonces Q». La implicación es posiblemente el conectivo lógico que resulta más difícil de entender, sólo es *falsa* cuando P es verdadera y Q es falsa; en otro caso, es siempre

[1] El enunciado es falso, ya que fue domingo.

verdadera. En una sección que viene más adelante, explicaremos con mayor detalle cómo funciona.

5. **Doble implicación.** $P \Leftrightarrow Q$: «P si y sólo si Q». La doble implicación es una abreviatura para $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. La doble implicación es *verdadera* cuando ambas proposiciones tienen el mismo valor de verdad, es decir, cuando ambas son verdaderas o cuando ambas son falsas y la doble implicación es *falsa* cuando una proposición es verdadera y la otra es falsa.

En computación, la conjunción también se suele denotar por «AND», la disyunción por «OR» y la negación por «NOT».

1.2 Tablas de verdad

Las tablas de verdad nos permiten *calcular* el valor de una proposición compuesta a partir de los valores de verdad de las proposiciones que las componen, considerando todas las posibilidades que éstas tengan. En los cuadros 1 al 5 se muestran los posibles valores de verdad de cada uno de los cinco conectivos lógicos.

P	**Q**	**P** $\vee$ **Q**
V	V	V
V	F	V
F	V	V
F	F	F

Cuadro 1: Disyunción

P	**Q**	**P** $\wedge$ **Q**
V	V	V
V	F	F
F	V	F
F	F	F

Cuadro 2: Conjunción

P	$\neg$**P**
V	F
F	V

Cuadro 3: Negación

P	**Q**	**P** $\Rightarrow$ **Q**
V	V	V
V	F	F
F	V	V
F	F	V

Cuadro 4: Implicación

P	**Q**	**P** $\Leftrightarrow$ **Q**
V	V	V
V	F	F
F	V	F
F	F	V

Cuadro 5: Doble implicación

1.3 La implicación

La implicación es posiblemente el conectivo lógico que resulta más difícil de entender. Consideremos un político P que haga campaña y durante ésta prometa que, de ser elegido, habrá más becas para estudiantes. Los demás contrincantes no prometieron nada al respecto. Después de las elecciones, hay dos posibilidades: P sí fue o no fue elegido. Si P no es elegido, la persona que fue elegida puede o no crear más becas; qué bueno si sí lo hace, pero si no, no pasa nada pues no lo prometió. Si P resulta elegido, esperaríamos que creara más becas, como prometió. Si sí lo hace, todo está bien; pero si no, nos quejaremos. En una implicación de la forma $P \Rightarrow Q$, P es el político y Q es que lleve a cabo su promesa; P es verdadera si sí es elegido y es falsa si no lo es, Q es verdadera si sí cumple su promesa y es falsa si no. El único caso en que el podríamos (y deberíamos) quejarnos es si P resultado elegido, pero no cumple su promesa. La implicación es igual: sólo es falsa cuando P es verdadera, pero Q es falsa; en cualquier otro caso, la implicación $P \Rightarrow Q$ es verdadera.

Que una implicación $P \Rightarrow Q$ sea verdadera, no nos dice mucho sobre la verdad o falsedad de P y Q (veremos que sí nos dice *algo*). Consideremos los siguientes ejemplos:

- P: «llueve» y
- Q: «hay nubes».

La implicación $P \Rightarrow Q$ se lee «si llueve entonces hay nubes», la cual es verdadera (puede que no veamos las nubes, pero ahí están, ya que la lluvia es vapor de agua de condensada y las nubes son vapor de agua). Aunque $P \Rightarrow Q$ sea verdadera, eso no nos dice que ahora está o no lloviendo ni tampoco nos dice que ahora hay o no nubes. Lo que no puede pasar es que llueva sin que haya ningún rastro de nubes (es decir, de vapor de agua).

En una implicación

$$P \Rightarrow Q,$$

«P» es el *antecedente* o *hipótesis* y Q es el *consecuente* o *conclusión*. Podemos pensar que, en el caso en $P \Rightarrow Q$ es verdadera, P es una *llave* que, cuando es verdadera, nos asegura que Q es verdadera.

Por otro lado, sólo hay un renglón en el cuadro 4 en el que $P \Rightarrow Q$ es falsa: cuando P es verdadera y Q es falsa (que ocurre cuando P sí es elegido, pero no cumple su promesa, en nuestro ejemplo previo).

1.4 Otros elementos de la lógica

Usamos *paréntesis* «(» y «)» para agrupar y así precisar nuestras expresiones. Consideremos las proposiciones:

- P: «hoy es lunes» y
- Q: $5 < 0$.

Las proposiciones siguientes se leen:

- $\neg(P \vee Q)$: «No es cierto que: hoy es lunes o $5 < 0$».
- $(\neg P) \vee Q$: «No es cierto que hoy es lunes o $5 < 0$».
- $P \vee (\neg Q)$: «Hoy es lunes o no es cierto que $5 < 0$».

Si comparáramos tablas de verdad de las cuatro proposiciones anteriores, veríamos que no coinciden.

Las *constantes extralógicas* son elementos de nuestro **universo de trabajo**. Por ejemplo, en la proposición «$\sqrt{b} = 2$», donde nuestro universo de trabajo son los números reales, «b» es una constante extralógica que vale cuatro y en la proposición «$\pi = 3$», donde nuestro universo de trabajo son los números reales, «π» es una constante extralógica igual al cociente del diámetro de un círculo entre su diámetro.

Las *variables*, que usualmente denotamos como x, y, z, etcétera, con o sin subíndices, no tienen un valor predeterminado. Cuando hacemos afirmaciones con una o varias variables, obtenemos un *predicado*: afirmaciones que no son enunciados hasta que especifiquemos los valores de las variables. Además, debemos señalar cuál es el conjunto sobre el cual «va a correr» la variable (es decir, de donde provienen los valores que tomará la variable), al cual llamamos el *conjunto de referencia* o *alcance de la variable*. Por ejemplo, si $P(x)$ es el predicado «x es un número par»,[2] donde el conjunto de referencia de x son todos los números enteros, para $x = 3$ tendríamos el enunciado $P(3)$: «3 es un número par», el cual es falso, y para $x = 0$ tendríamos el enunciado $P(0)$: «0 es un número par», el cual es verdadero.

Consideremos la proposición $P(x)$: «$2x$ es un número par», donde el alcance de la variable son todos los números enteros. No importa qué valor tome la variable x, $P(x)$ siempre será verdadero; dicho de otro modo: «para todo x, $P(x)$ es verdadero». Esto lo denotamos de la forma

$$\forall x P(x).$$

El símbolo «$\forall$» es el *cuantificador universal*. Es importante darnos cuenta que el valor de verdad de una proposición con un cuantificador depende del

[2]Un número x es par si existe un número entero k tal que $x = 2k$.

alcance de sus variables. Si para la misma proposición $P(x)$: «$2x$ es un número par», cambiamos el alcance de la variable por todos los números reales, $\forall x P(x)$ se vuelve falsa (por ejemplo, para $x = {}^1/_2$ tenemos que $P({}^1/_2)$ es falsa).

Consideremos de nuevo la proposición $P(x)$: «$2x$ es un número par». Para que la proposición $\forall x P(x)$ sea verdadera es necesario que $P(x)$ sea verdadera para **todos** los posibles valores que tome x; pero ¿qué pasa si para uno de esos valores, resulta que $P(x)$ no es verdadera? Entonces $\forall x P(x)$ no puede ser verdadera y, si no es verdadera, significa que es falsa. Así, para que $\forall x P(x)$ sea falsa **basta con que exista al menos un valor** de x en el que $P(x)$ sea falsa o, de otra forma, en el que $\neg P(x)$ sea verdadera. Esto lo denotamos como

$$\exists x(\neg P(x))$$

y se lee «existe x tal que $\neg P(x)$ es verdadera». El símbolo «$\exists$» es el *cuantificador existencial*, de la misma forma que para el cuantificar universal, debemos señalar cuál es el conjunto de referencia o alcance del cuantificador. Cuando $\forall x P(x)$ es falsa, $\neg(\forall x P(x))$ es verdadera.

Una *tautología* es una proposición que siempre es verdadera, por ejemplo, $P \vee \neg P$ (en lo que sigue, escribiremos $P \vee \neg P$ en vez de $P \vee (\neg P)$). Véase el cuadro 6. Lo contrario a una tautología es una *contradicción*: una proposición que siempre es falsa, por ejemplo, $P \wedge \neg P$. Véase el cuadro 7.

P	**¬P**	**P ∨ ¬P**
V	F	V
F	V	V

Cuadro 6: Tautología

P	**¬P**	**P ∧ ¬P**
V	F	F
F	V	F

Cuadro 7: Contradicción

Si P y Q son dos proposiciones tales que $P \Leftrightarrow Q$ es una tautología, decimos que P y Q son *tautológicamente equivalente*, *lógicamente equivalentes* o, simplemente, *equivalentes*. Lo anterior significa que P y Q tienen la misma tabla de verdad. Si nos dan dos proposiciones P y Q y resulta que tienen la misma tabla de verdad, significa que son lógicamente equivalentes.

Ejercicio 1. Da las tablas de verdad de las proposiciones $\neg(P \vee Q)$, $\neg(P \wedge Q)$, $\neg P \vee \neg Q$ y $\neg P \wedge \neg Q$. A partir de las tablas de verdad, determina cuáles de las proposiciones son lógicamente equivalentes entre sí.

Solución. Primero hagamos las tablas de verdad, éstas aparecen en los cuadros 8 a 11.

P	**Q**	$\mathbf{P} \vee \mathbf{Q}$	$\neg(\mathbf{P} \vee \mathbf{Q})$
V	V	V	F
V	F	V	F
F	V	V	F
F	F	F	V

Cuadro 8: Negación de «$\vee$»

P	**Q**	$\mathbf{P} \wedge \mathbf{Q}$	$\neg(\mathbf{P} \wedge \mathbf{Q})$
V	V	V	F
V	F	F	V
F	V	F	V
F	F	F	V

Cuadro 9: Negación de «$\wedge$»

P	**Q**	$\neg\mathbf{P}$	$\neg\mathbf{Q}$	$\neg\mathbf{P} \vee \neg\mathbf{Q}$
V	V	F	F	F
V	F	F	V	V
F	V	V	F	V
F	F	V	V	V

Cuadro 10: Conjunción de negaciones

P	**Q**	$\neg\mathbf{P}$	$\neg\mathbf{Q}$	$\neg\mathbf{P} \wedge \neg\mathbf{Q}$
V	V	F	F	F
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Cuadro 11: Disyunción de negaciones

Notemos que las tablas de verdad de $\neg(P \vee Q)$ y $\neg P \wedge \neg Q$ son iguales, así como las de $\neg(P \wedge Q)$ y $\neg P \vee \neg Q$; por lo tanto, son lógicamente equivalentes entre sí. Podemos verificarlo calculando las tablas de verdad de $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$ y $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$.

P	**Q**	$\neg(\mathbf{P} \vee \mathbf{Q})$	$\neg\mathbf{P} \wedge \neg\mathbf{Q}$	$\neg(\mathbf{P} \vee \mathbf{Q}) \Leftrightarrow (\neg\mathbf{P} \wedge \neg\mathbf{Q})$
V	V	F	F	V
V	F	F	F	V
F	V	F	F	V
F	F	V	V	V

Cuadro 12: Primera equivalencia

P	**Q**	$\neg(\mathbf{P} \wedge \mathbf{Q})$	$\neg\mathbf{P} \vee \neg\mathbf{Q}$	$\neg(\mathbf{P} \wedge \mathbf{Q}) \Leftrightarrow (\neg\mathbf{P} \vee \neg\mathbf{Q})$
V	V	F	F	V
V	F	V	V	V
F	V	V	V	V
F	F	V	V	V

Cuadro 13: Segunda equivalencia

Ejercicio 2. Determina las tablas de verdad de las siguientes proposiciones:

(a) $(P \vee Q) \Rightarrow R$ (b) $P \Rightarrow (Q \vee R)$

Solución. La respuesta aparece en las tablas 14 y 15.

$\mathbf{P}$	$\mathbf{Q}$	$\mathbf{R}$	$\mathbf{P} \vee \mathbf{Q}$	$(\mathbf{P} \vee \mathbf{Q}) \Rightarrow \mathbf{R}$
V	V	V	V	V
V	V	F	V	F
V	F	V	V	V
V	F	F	V	F
F	V	V	V	V
F	V	F	V	F
F	F	V	F	V
F	F	F	F	V

Cuadro 14: Tabla de verdad de $(P \vee Q) \Rightarrow R$

$\mathbf{P}$	$\mathbf{Q}$	$\mathbf{R}$	$\mathbf{Q} \wedge \mathbf{R}$	$\mathbf{P} \Rightarrow (\mathbf{Q} \vee \mathbf{R})$
V	V	V	V	V
V	V	F	F	F
V	F	V	F	F
V	F	F	F	F
F	V	V	V	V
F	V	F	F	V
F	F	V	F	V
F	F	F	F	V

Cuadro 15: Tabla de verdad de $P \Rightarrow (Q \vee R)$

1.4.1 Relación entre cuantificadores universales y existenciales

Supongamos que tenemos un predicado $P(x)$ tal que no es cierto que $\forall x P(x)$, eso significa que existe un x tal que $P(x)$ es falso, es decir, $\exists x(\neg P(x))$. Por lo tanto, tenemos la siguiente equivalencia tautológica:

$$\neg(\forall x P(x)) \Leftrightarrow \exists x(\neg P(x)).$$

De forma análoga, si no es cierto que $\exists x P(x)$, significa que para todo x, $P(x)$ es falso, es decir, $\neg P(x)$ es verdadero. Así, tenemos la siguiente

equivalencia:

$$\neg(\exists x P(x)) \Leftrightarrow \forall x(\neg P(x)).$$

2 Las pruebas

Las matemáticas que conocemos están basadas en la noción de *prueba* o *demostración*. ¿Qué pasa cuándo sumamos dos números enteros pares[3]? Si hacemos algunos ejemplos (por ejemplo, $2 + 4 = 6$, $0 + 8 = 8$, $-4 + 4 = 0$, etc.), veremos que en todos los casos el resultado también es un número par. Podríamos sospechar que la suma de **cualesquiera** dos números enteros pares siempre es par, pero ¿cómo estar seguros? Podría ser que exista un ejemplo que no conozcamos. Un posible camino sería que **chequemos todos los posibles valores** de la suma, pero no es posible hacerlo.

Un problema similar presenta el diseño de 'hardware' y 'software', cuando diseñamos un procesador o preparamos un programa, esperamos que bajo ciertas entradas, el procesador o el programa dé cierto resultado, pero por lo general las posibles entradas son demasiadas para verificar que el diseño es apropiado (y, por otro lado, uno diseña un procesador o prepara un programa para ahorrarse precisamente ese trabajo). ¿Cómo asegurar que las cosas funcionan apropiadamente?

En el caso de las matemáticas, la respuesta a este planteamiento es la **prueba** o **demostración**, intuitivamente, una argumentación que no deje lugar a dudas. Veamos cómo sería en la pregunta que nos planteamos, tenemos que x y y son números enteros pares y queremos probar que $x + y$ es un número par.

$x = 2p$, donde p es un número entero	*Por la definición de número par*
$y = 2q$, donde q es un número entero	*Por la definición de número par*
$x + y = 2p + 2q$	*Por propiedades de la igualdad*
$= 2(p + q)$	*Por la propiedad distributiva*
$= 2r$, con $r = p + q$	*La suma de números enteros es un número entero*

[3] ¿Qué significa que un número entero sea «par»? Recordemos que **definimos** que un número entero n es *par* si existe otro número entero, digamos k, tal que tenemos que $n = 2k$, es decir, podemos expresar n como dos por otro número entero. De forma similar, un número entero n es *impar* si existe otro número entero, digamos k, tal que tenemos que $n = 2k + 1$.

> Concluimos que $x + y = 2r$, es decir, expresamos la suma como dos por un número entero. Por la definición de número par, $x+y$ es un número par.

Notemos que cada paso está justificado ya sea porque sea hipótesis, sea un resultado anterior o porque se deduzca de una de las premisas previas.

Si consideramos las proposiciones

- P: «x y y son números enteros pares» y
- Q: «$x + y$ es un número entero par»

hemos probado/demostrado que $P \Rightarrow Q$ es verdadera.

¿Por qué partimos suponiendo que P es verdadera? Cuando queremos probar que $P \Rightarrow Q$ es verdadera, tenemos dos casos: P es verdadera o es falsa. Si es verdadera, para que $P \Rightarrow Q$ sea verdadera, Q tiene que ser verdadera. Pero cuando P es falsa, $P \Rightarrow Q$ es automáticamente verdadera.

2.1 ¿Qué significa que $P \Rightarrow Q$ sea verdadera?

Recordemos que hay un único caso en el que $P \Rightarrow Q$ es falsa: cuando P es verdadera y Q es falsa. Para cualquier otra combinación de valores de verdad de P y Q, tenemos que $P \Rightarrow Q$ resulta ser verdadera.

- Supongamos que $x = 2$ y $y = 3$. En este caso, P es falsa y Q también es falsa.
- Supongamos que $x = 5$ y $y = 3$. En este caso, P es falsa, pero ¡Q es verdadera!
- Supongamos que $x = 2$ y $y = 4$. En este caso, P es verdadera y ¡Q también es verdadera!

Los tres casos anteriores se siguen de que $P \Rightarrow Q$ sea verdadera. Como dijimos, el único caso que no puede darse es que P sea verdadera y Q sea falsa.

Por lo anterior, siempre que nos digan que la proposiciones P y $P \Rightarrow Q$, siempre concluiremos que Q también es verdadera. A esta regla se le conoce como *modus ponendo ponens* o *modus ponens* (su nombre en latín) y frecuentemente la veremos como:

$$\begin{array}{l} P \\ P \Rightarrow Q \\ \hline \therefore\ Q \end{array}$$

2.2 Tipos de pruebas

2.2.1 Pruebas directas

Frecuentemente, no hay una forma directa de mostrar que $P \Rightarrow Q$ es verdadera, pero en cambio, podemos mostrar que existen proposiciones P_1, P_2, $\ldots$, P_k tales que

$$\begin{array}{rcl} P & \Rightarrow & P_1 \\ P_1 & \Rightarrow & P_2 \\ P_2 & \Rightarrow & P_3 \\ & \vdots & \\ P_{k-1} & \Rightarrow & P_k \\ P_k & \Rightarrow & Q \end{array}$$

Si supiésemos que P también es verdadera, del primer renglón deducimos que P_1 es verdadera. Ya que P_1 es verdadera, del segundo renglón deducimos que P_2 es verdadera. Y seguimos así hasta tener que P_{k-1} es verdadera, por el penúltimo renglón, se sigue que P_k es verdadera. Del último renglón, se sigue que Q es verdadera. Por lo tanto, de la lista de implicaciones anteriores, se sigue que $P \Rightarrow Q$ es verdadera.

2.2.2 Pruebas por contraposición

Del ejercicio 1.1, sabemos (eventualmente, tal vez) que $P \Rightarrow Q$ y $\neg Q \Rightarrow \neg P$ son tautológicamente equivalentes. A la segunda proposición se la llama la *contraposición* de la primera y, ya que son tautológicamente equivalentes, si probamos que $\neg Q \Rightarrow \neg P$ es verdadera, también tendremos que $P \Rightarrow Q$ es verdadera, que es lo que queríamos probar.

2.2.3 Pruebas por reducción al absurdo o por contradicción

Esta es uno de los métodos de prueba más difícil de entender, pero es posiblemente el más poderoso. Supongamos que queremos demostrar que $P \Rightarrow Q$, la prueba *por reducción al absurdo* o *por contradicción* consiste en suponer que P es verdadera y que Q es falsa (es decir, que las hipótesis son verdaderas, pero la conclusión es falsa) y, de lo anterior, llegar a una contradicción. En símbolos lógicos, estamos probando que

$$(P \wedge \neg Q) \Rightarrow (R \wedge \neg R)$$

es verdadera. El consecuente es $R \wedge \neg R$, que vimos que siempre es falso, *i. e.*, es una contradicción. No sabemos quién es R en principio, sólo que llegaremos a una contradicción (o absurdo, de ahí el nombre). La única forma en que una implicación sea verdadera pero el consecuente sea falso es cuando el antecedente es falso (la última línea en el cuadro 4). Por lo tanto, $P \wedge \neg Q$ es falso y $\neg(P \wedge \neg Q)$ es verdadero; más aún, tenemos que

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

Con lo que concluimos que $P \Rightarrow Q$, que es lo que queríamos demostrar.

2.2.4 Pruebas por casos

Cuando queremos demostrar una implicación del tipo $(P_1 \vee P_2) \Rightarrow Q$, podemos probar por separado que tanto $P_1 \Rightarrow Q$ como $P_2 \Rightarrow Q$ son verdaderas, ya que del ejercicio 1.1 tenemos que

$$[(P_1 \vee P_2) \Rightarrow Q] \Leftrightarrow [(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q)]$$

Veamos el ejemplo siguiente; consideremos dos números enteros x y y junto con las proposiciones siguentes:

- P_1: «x es un número par».
- P_2: «y es un número par».
- Q: «xy es un número par».

Deseamos probar que $(P_1 \vee P_2) \Rightarrow Q$, pero probaremos que $P_1 \Rightarrow Q$ y $P_2 \Rightarrow Q$ son verdaderas. Primero probemos que $P_1 \Rightarrow Q$; si x es un número par entonces podemos escribirlo de la forma $x = 2p$, donde p es un número entero. Por lo tanto, $xy = (2p)y = 2(py)$; ya que py es un número entero, xy es un número par. Ahora probemos que $P_2 \Rightarrow Q$; si y es un número par entonces podemos escribirlo de la forma $y = 2q$, donde q es un número entero. Por lo tanto, $xy = x(2q) = 2(xq)$; ya que xq es un número entero, xy es un número par. Por lo tanto, hemos probado que $(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q)$, que es equivalente a $(P_1 \vee P_2) \Rightarrow Q$, lo que queríamos probar.

Ejercicios

1.1 Prueba que las siguientes proposiciones son tautológicamente equivalentes.

(a) $P \Rightarrow Q$ y $\neg Q \Rightarrow \neg P$

(b) $P \Rightarrow Q$ y $\neg P \vee Q$

(c) P y $\neg(\neg P)$

(d) $P \vee Q$ y $Q \vee P$

(e) $P \wedge Q$ y $Q \wedge P$

(f) $P \wedge \neg P$ y $\neg(P \vee \neg P)$

(g) $\neg(P \vee Q)$ y $\neg P \wedge \neg Q$

(h) $\neg(P \wedge Q)$ y $\neg P \vee \neg Q$

(i) $(P_1 \vee P_2) \Rightarrow Q$ y $(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q)$

3 Los conjuntos

Los conjuntos fueron un elemento crucial en la formalización de las matemáticas durante los siglos XIX y XX y, en su momento, fueron muy cuestionados, incluso entre los propios matemáticos[4].

Intuitivamente, nos parece claro *qué es* un conjunto. Pero si tratamos de definirlos de forma más formal (valga la redundancia), nos enfrentaremos con un problema; podríamos tal vez definir conjunto como una «colección», pero ¿qué es una *colección*? Una colección es una «familia», ¿pero qué es una familia? Y así podríamos seguir. En la lengua es común encontrar ese tipo de ejemplos. Por ejemplo, si hojeamos el *Diccionario de la Real Academia Española*, encontraremos que define 'soberbia' como 'altivez' y 'altivez' como 'soberbia'. Sin embargo, ni en Matemáticas ni en Computación podemos darnos el lujo de tener definiciones cíclicas. Por otro lado, no todo es definible; si no aceptamos definiciones cíclicas, nos toparemos con una lista infinita de definiciones, lo cual ciertamente no es posible.

¿Un callejón sin salida? No necesariamente; resulta que para trabajar con los conjuntos no es necesario saber *qué son*, sino *cómo funcionan*. Y lo más importante sobre los conjuntos es saber cuándo alguien **es** o **no es** elemento en un conjunto dado.

Dado un conjunto A, si x es un *elemento* de A lo denotamos por

$$x \in A$$

y si x *no es elemento* de A, lo denotamos por

$$x \notin A.$$

[4] A George Cantor se lo reconoce como *el padre de la Teoría de los Conjuntos* y fue tan controversial en su época que Leopold Kronecker, que fue profesor suyo, lo llamó públicamente «charlatán científico», «renegado» y «corruptor de la juventud».

A esto se le conoce como *relación de pertenencia*. Si nos dan un supuesto conjunto B en el que no sea posible saber si x pertenece o no a B, entonces B no es un conjunto.

¿Cómo damos un conjunto? Existen dos formas usuales para describir conjuntos. La primera forma consiste en dar todos los elementos del conjunto, por ejemplo:

$$A = \{2, 4, 6\}.$$

A esta forma la llamaremos *por extensión*. La segunda forma consiste en dar una propiedad que satisfagan los elementos del conjunto y sólo la satisfagan los elementos del conjunto, por ejemplo:

$$A = \{x\colon x \text{ es un número entero par y } 1 \leq x \leq 7\},$$

que se lee

> «A es el conjunto de todas las x tales que x es un número entero par y $1 \leq x \leq 7$».

A esta forma la llamamos *por comprensión*. Esta propiedad es un predicado, como los que vimos previamente. Si tomamos:

- $P(x)$: «x es un número entero par y $1 \leq x \leq 7$»,

podemos reescribir A como

$$A = \{x\colon P(x)\}.$$

Notemos que $P(2)$, $P(4)$ y $P(6)$ son verdaderos, pero para cualquier otra x, digamos $x = 5$, tenemos que $P(5)$ es falso. Cuando para $x = b$, $P(b)$ es verdadera, significa que $b \in A$, pero si $P(b)$ es falsa, significa que $b \notin A$. Es importante que la propiedad sea sólo verdadera con los elementos que sí están en el conjunto. Por ejemplo, si tomamos:

- $Q(x)$: «x es un número entero y $1 \leq x \leq 7$»

y definimos $B = \{x\colon Q(x)\}$, tenemos que

$$B = \{1, 2, 3, 4, 5, 6, 7\}.$$

3.1 Ejemplos

3.1.1 El conjunto vacío

Aunque pueda sonar extraño, existe un conjunto **que no tiene elementos**, el *conjunto vacío*, que se denota por el símbolo $\varnothing$. De forma extensiva, escribiríamos

$$\varnothing = \{\ \}$$

y de forma comprensiva

$$\varnothing = \{x\colon x \neq x\}.$$

Para cualquier x, claramente la propiedad $x \neq x$ es falsa.

Observemos que la siguiente es una tautología

$$\forall x(x \notin \varnothing)$$

y, por lo tanto, la siguiente es una contradicción

$$\exists x(x \in \varnothing).$$

3.1.2 Los conjuntos unitarios

Para cada objeto a, existe un conjunto que sólo contiene a a: *el conjunto unitario de* a,

$$\{a\}.$$

También podemos escribirlo de forma comprensiva como

$$\{x\colon x = a\}.$$

Algunos le llaman «singulete», que es una suerte de transliteración del inglés 'singleton'. Sin embargo, lo apropiado en español es «unitario».

3.1.3 Las parejas no ordenadas

Si tenemos dos objetos, digamos a y b, tales que $a \neq b$, existe un conjunto que los contiene a ambos, pero no contiene ningún objeto más: *la pareja no ordenada*

$$\{a, b\}.$$

De forma comprensiva, podemos escribir

$$\{x\colon x = a \vee x = b\}.$$

3.1.4 Algunos conjuntos de números

También tenemos los diferentes conjuntos de números (aunque no los definiremos formalmente, los daremos por conocidos).

- El *conjunto de los (números) naturales* $\mathbb{N} = \{0, 1, 2, \dots, \}$.

  Es necesario mencionar que hay diferentes posturas sobre si el cero es o no un número natural (es decir, sobre cuál de $0 \in \mathbb{N}$ o $0 \notin \mathbb{N}$ es verdadera), nosotros supondremos que sí lo es. Cuando tengas dudas sobre cuál sea caso, especifícalo en donde lo vayas a utilizar.

- El *conjunto de los (números) enteros* $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. El conjunto de los (números) enteros *positivos* $\mathbb{Z}^+ = \{0, 1, 2, 3, \dots\}$ y el conjunto de los (números) enteros *negativos* $\mathbb{Z}^- = \{-1, -2, -3, \dots\}$.

- El *conjunto de los (números) racionales* $\mathbb{Q} = \{{}^{p}/_{q} : p, q \in \mathbb{Z}, q \neq 0\}$.

- El *conjunto de los (números) reales* $\mathbb{R}$.

3.2 Propiedades de los conjuntos

Lo importante para nosotros es *¿qué podemos hacer con los conjuntos?*

3.2.1 La igualdad de conjuntos

Si A y B son dos conjuntos, ¿cuándo son iguales? Definimos que dos conjuntos A y B son *iguales* (y lo denotamos como $A = B$) si y sólo si tienen los mismos elementos. Es decir, para todo $x \in A$, se tiene que $b \in B$ y para todo $x \in B$, se tiene que $x \in A$. Dicho de otra forma,

$$A = B \underset{\text{definición}}{\Longleftrightarrow} \forall x(x \in A \Leftrightarrow x \in B).$$

> Para probar que dos conjuntos A y B son **iguales**, debemos tomar cada elemento x que esté en A y verificar que también es elemento de B y viceversa, tomar cada elemento x que esté en B y verificar que es elemento de A.

3.2.2 Orden y repetición de elementos en conjuntos

Consideremos los conjuntos $A = \{a, b\}$ y $B = \{b, a, a\}$, ¿son iguales A y B? Para demostrarlo, tenemos que verificar que cada elemento de A también lo sea de B y viceversa. En A vemos dos elementos, a y b, y ambos son elementos de B. Por otro, en B vemos tres elementos, b, a y a, y los tres también están en B. Por lo tanto, $A = B$.

Lo anterior es un ejemplo de que en los conjuntos no importa ni el **orden** ni si aparecen elementos **repetidos**, tan sólo nos importa si un elemento **está o no está**.

3.2.3 Los subconjuntos

A veces querremos hacer referencia a una parte de un conjunto, a esas partes las llamamos subconjuntos. Dados dos conjuntos A y B, decimos que A es *subconjunto* de B (y lo denotamos como $A \subseteq B$) si para todo elemento x de A, se tiene que x es también elemento de B. En notación de lógica,

$$A \subseteq B \underset{\text{definición}}{\Longleftrightarrow} \forall x(x \in A \Rightarrow x \in B). \tag{3.1}$$

Cuando $A \subseteq B$, también lo denotamos por $B \supseteq A$ y decimos que B es *superconjunto* de A.

Notemos que para cualquier conjunto A, tenemos que $A \subseteq A$ (porque la proposición

$$\forall x(x \in A \Rightarrow x \in A)$$

siempre es verdadera). Si $A = B$, tendremos que $A \subseteq B$ y $B \subseteq A$. Y resulta que al revés, también es cierto.

Teorema 3. *Considérense dos conjuntos A y B, $A = B$ si y sólo si $A \subseteq B$ y $B \subseteq A$*

Demostración. Recordemos que una doble implicación «P si y sólo si Q» es «$P \Leftrightarrow Q$», cuando nos piden probar una doble implicación, debemos probar dos implicaciones: $P \Rightarrow Q$ y $Q \Rightarrow P$.

Primera implicación: Si $A = B$ entonces $A \subseteq B$ y $B \subseteq A$. Para probar una implicación, suponemos el antecedente y debemos llegar al consecuente, así supongamos que $A = B$. Eso significa que

$$\forall x(x \in A \Leftrightarrow x \in B),$$

que es lo mismo que

$$\forall x[(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)].$$

Por lo tanto, tenemos que tanto

$$\forall x(x \in A \Rightarrow x \in B).$$

como

$$\forall x(x \in B \Rightarrow x \in A)$$

son verdaderas. Por la definición de subconjunto, se sigue que $A \subseteq B$ y $B \subseteq A$.

Segunda implicación: Si $A \subseteq B$ **y** $B \subseteq A$ **entonces** $A = B$. Así, supongamos que $A \subseteq B$ y $B \subseteq A$; por definición de subconjunto tenemos que

$$\forall x(x \in A \Rightarrow x \in B) \text{ y } \forall x(x \in B \Rightarrow x \in A).$$

Se sigue que

$$\forall x[(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)],$$

que es $\forall x(x \in A \Leftrightarrow x \in B)$. Así, $A = B$. □

El símbolo «□» se suele utilizar en matemáticas para indicar el fin de una prueba.

La anterior es una muestra de una prueba formal. Pero para nuestros fines, no es necesaria tanta formalidad. Podemos reescribirla de la siguiente forma.

Demostración. $\Rightarrow$] Supongamos que $A = B$, por demostrar que $A \subseteq B$ y $B \subseteq A$. Sabemos que $A \subseteq A$ y como $A = B$, al cambiar cada una de las A obtenemos que $A \subseteq B$ y $B \subseteq A$.

$\Leftarrow$] Supongamos que $A \subseteq B$ y $B \subseteq A$. Tenemos que probar que $A = B$ y es por definición (es decir, tomamos un elemento x en A y verificamos que está en B y viceversa). Sea $x \in A$, como $A \subseteq B$, entonces $x \in B$ y sea $x \in B$, como $B \subseteq A$, entonces $x \in A$; por lo tanto, $A = B$. □

Teorema 4. *El conjunto vacío es único.*

Que el conjunto vacío sea *único* significa que si A y B son dos conjuntos vacíos, entonces $A = B$; estamos mostrando que no pueden haber dos conjuntos vacíos diferentes.

Demostración. Sean A y B dos conjuntos vacíos. Esto significa que satisfacen la siguiente propiedad

$$\forall x(x \notin A) \text{ y } \forall x(x \notin B).$$

Para mostrar que $A = B$, tenemos que mostrar que todo elemento de A también es elemento de B y viceversa.

A $\subseteq$ B]. Tenemos que probar que $\forall x(x \in A \Rightarrow x \in B)$, pero ya que $x \in A$ es falso para cualquier x, el antecedente es falso y, por lo tanto, la implicación es verdadera. Por lo tanto, $A \subseteq B$.

B $\subseteq$ A]. Tenemos que probar que $\forall x(x \in B \Rightarrow x \in A)$, pero ya que $x \in B$ es falso para cualquier x, el antecedente es falso y, por lo tanto, la implicación es verdadera. Por lo tanto, $B \subseteq A$.

Por lo tanto, $A = B$. □

Cuando $A \subseteq B$ pero $A \neq B$, decimos que A es *subconjunto propio* de B y lo dentomos por $A \subsetneq B$. Formalmente,

$$A \subsetneq B \underset{\text{definición}}{\Longleftrightarrow} \forall x(x \in A \Rightarrow x \in B) \wedge \exists x(x \notin A \wedge x \in B). \tag{3.2}$$

¿Cuándo un conjunto A **no es subconjunto** de otro conjunto B? La definición de ser subconjunto es que todo elemento de A también es elemento de B, que no se cumpla significaría que hay un elemento en A que no sea elemento de B. Lo denotamos como $A \nsubseteq B$. Formalmente, no se cumpliría la propiedad de ser subconjunto (la ecua-ción 3.1), es decir, sería falsa. Y, por lo tanto, su negación será verdadera:

$$\neg[\forall x(x \in A \Rightarrow x \in B)] \Leftrightarrow [\exists x \neg(x \in A \Rightarrow x \in B)].$$

Recordemos que $P \Rightarrow Q$ es tautológicamente equivalente a $\neg P \vee Q$, así:

$$(\exists x \neg(x \in A \Rightarrow x \in B) \Leftrightarrow (\exists x \neg(\neg(x \in A) \vee x \in B)) \Leftrightarrow (\exists x(x \in A \wedge x \notin B)),$$

¡que justamente dice que existe un elemento en A que no está en B!

Finalmente, resulta que el conjunto vacío es subconjunto de **cualquier otro conjunto**.

Teorema 5. *Para todo conjunto A, se satisface*[5] *que $\varnothing \subseteq A$.*

Demostración. Debemos probar que para todo x, si $x \in \varnothing$ entonces $x \in A$. Pero la hipótesis es siempre falsa y, por lo tanto, la implicación es siempre verdadera. Se sigue que $\varnothing \subseteq A$. □

3.2.4 El conjunto potencia

3.2.5 Representación gráfica de los conjuntos: diagramas de Venn

Los diagramas de Venn son una representación gráfica de los conjuntos que nos ayuda a entender cómo se comportan las operaciones entre conjuntos. Un gran rectángulo suele representar el *universo*, el conjunto en el que viven todos los elementos de los conjuntos con los que trabajamos. Y cada conjunto lo solemos representar como un círculo dentro del rectángulo (véase la figura 1).

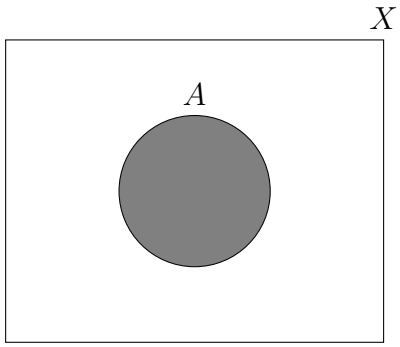


Figura 1: Un digrama de Venn

3.2.6 Operaciones de conjuntos: la unión

Dados dos conjuntos A y B existe un tercer conjunto que contiene los elementos tanto de A como de B, pero ningún otro, a dicho conjunto se lo llama

[5]Usamos «se satisface» como sinónimo de «es verdadero».

la *unión* de A y B y lo denotamos como $A \cup B$. Otra forma de decirlo es:

$$A \cup B = \{x \colon x \in A \vee x \in B\}.$$

Formalmente,

$$x \in A \cup B \underset{\text{definición}}{\Longleftrightarrow} (x \in A \vee x \in B).$$

La unión está asociada con el colectivo lógico «o». En términos de diagramas de Venn, puede consultarse la figura 5.

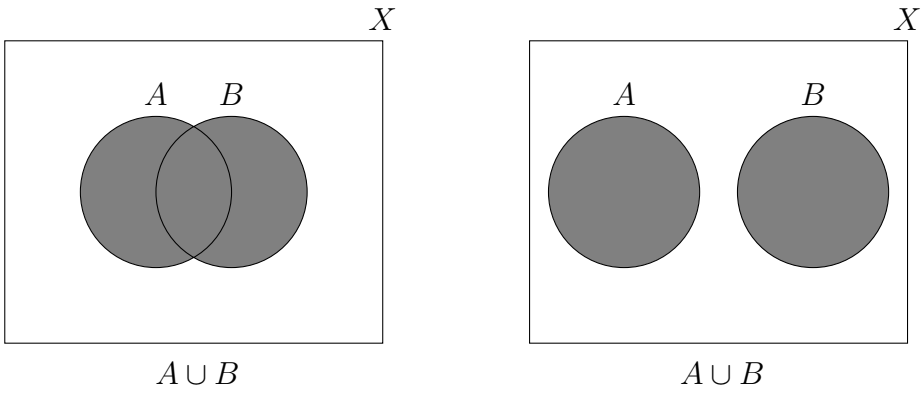


Figura 2: Unión de conjuntos

Ejemplo 1. Consideremos los conjuntos $A = \{1, 2, \bigstar, \square\}$, $B = \{\&, 2, 3\}$ y $C = \{\bigstar, 1\}$. Determínese $A \cup B$, $B \cup C$ y $A \cup C$.

Tenemos que:

- $A \cup B = \{1, 2, 3, \&, \bigstar, \square\}$
- $A \cup C = \{1, 2, \bigstar, \square\}$
- $B \cup C = \{1, 2, 3, \&, \bigstar\}$

Teorema 6 (Propiedades de la unión)**.** *Sean A, B y C tres conjuntos arbitrarios. Se cumplen las siguientes propiedades:*

(a) $A \subseteq A \cup B$ *y* $B \subseteq A \cup B$

(b) $A \cup A = A$ *y* $A \cup \varnothing = A$

(c) $A \cup (B \cup C) = (A \cup B) \cup C$

(d) $A \cup B = B \cup A$

(e) $A \cup B = A$ *si y sólo si* $B \subseteq A$

Probaremos todas las afirmaciones excepto la cuarta, que se quedará como ejercicio.

Demostración. Probemos (a). Probemos primero que $A \subseteq A \cup B$; para ello, tomemos cualquier elemento $x \in A$. Debemos mostrar que $x \in A \cup B$, pero, por definición, $A \cup B = \{x \colon x \in A \vee x \in B\}$. Así, es claro que $x \in A \cup B$, de donde $A \subseteq A \cup B$. La prueba de la segunda proposición es análoga.

Probemos (b). Probemos primeros que $A \cup A = A$. Tenemos que probar que $A \cup A \subseteq A$ y $A \subseteq A \cup A$. Por la definición de unión, si $a \in A \cup A$ entonces $x \in A$ o $x \in A$, por lo tanto $A \cup A \subseteq A$. La otra contención se sigue del inciso previo. Por lo tanto, $A \cup A = A$. Ahora probemos que $A \cup \varnothing = A$. De forma análoga, debemos mostrar dos contenciones: $A \cup \varnothing \subseteq A$ y $A \subseteq A \cup \varnothing$. Si $x \in A \cup \varnothing$, se sigue que $x \in A$ (ya que $\forall x(x \notin \varnothing)$); por lo tanto, $A \cup \varnothing \subseteq A$. La otra contención se sigue del inciso (a). Por lo tanto, $A \cup \varnothing = A$.

Probemos (c). Resulta un poco más complicado, de la misma forma, tenemos que mostrar dos contenciones:

$$A \cup (B \cup C) \subseteq (A \cup B) \cup C$$

y

$$(A \cup B) \cup C \subseteq A \cup (B \cup C).$$

Ambas pruebas son engorrosas, pero parecidas, por lo que sólo probaremos la primera. Debemos tomar $x \in A \cup (B \cup C)$ y probar que $x \in (A \cup B) \cup C$. Ya que es una unión, $x \in A$ o $x \in B \cup C$ (es una prueba por casos). **Caso 1.** Si $x \in A$, se sigue que $x \in A \cup B$ y, por lo tanto, $x \in (A \cup B) \cup C$ (aplicamos dos veces el inciso (a)). **Caso 2.** Si $x \in B \cup C$, hay dos posibilidades: $x \in B$ o $x \in C$. **Caso 2.1.** Si $x \in B$ entonces $x \in B \cup C$ y, así, $x \in A \cup (B \cup C)$. **Caso 2.2.** Si $x \in C$ entonces $x \in B \cup C$ y, así, $x \in A \cup (B \cup C)$. En todos los casos concluimos que $x \in A \cup (B \cup C)$ y, por lo tanto, $A \cup (B \cup C) \subseteq (A \cup B) \cup C$. La otra contención es similar.

Finalmente, probemos el inciso (e). Como es una doble implicación, debemos probar los dos sentidos de la implicación. Primero probemos que si $A \cup B = A$ entonces $B \subseteq A$. Supongamos que $A \cup B = A$. Por el inciso (a), $B \subseteq A \cup B = A$, por lo tanto, $B \subseteq A$, con lo que terminamos. Ahora probemos el otro sentido, es decir, si $B \subseteq A$ entonces $A \cup B = A$. Supongamos que $A \subseteq$, para probar que $A \cup B = A$ tenemos que mostrar ambas contenciones: $A \cup B \subseteq A$ y $A \subseteq A \cup B$. Probemos primero que $A \cup B \subseteq A$, para ello tomemos $x \in A \cup B$; así, hay dos casos: $x \in A$ o $x \in B$. **Caso 1.** Si $x \in A$

entonces $x \in A$. **Caso 2.** Si $x \in B$, por hipótesis, $B \subseteq A$ y, por lo tanto, $x \in A$. De ambos casos, se sigue que $A \cup B \subseteq A$, por lo tanto, si $B \subseteq A$ entonces $A \cup B = A$. Al juntar ambas implicaciones, tenemos (e). □

3.2.7 Operaciones de conjuntos: la intersección

Dados dos conjuntos A y B existe un tercer conjunto que contiene sólo aquellos elementos que son elementos tanto de A como de B, pero ningún otro, a dicho conjunto se lo llama la *intersección* de A y B y lo denotamos como $A \cap B$. Otra forma de decirlo es:

$$A \cap B = \{x \colon x \in A \wedge x \in B\}.$$

Formalmente,

$$x \in A \cap B \underset{\text{definición}}{\Longleftrightarrow} (x \in A \wedge x \in B).$$

La intersección está asociada con el colectivo lógico «y».

Ejemplo 2. Consideremos los conjuntos $A = \{1, 2, \bigstar, \square\}$, $B = \{\&, 2, 3\}$ y $C = \{\bigstar, 1\}$. Determínese $A \cap B$, $B \cap C$ y $A \cap C$.

Tenemos que:

- $A \cap B = \{2\}$
- $A \cap C = \{\bigstar, 1\}$
- $B \cap C = \{\ \}$

Cuando pasa que, dados dos conjuntos A y B se tiene que $A \cap B = \varnothing$, decimos que A y B son conjuntos *ajenos*[6].

Teorema 7 (Propiedades de la intersección)**.** *Sean A, B y C tres conjuntos arbitrarios. Se cumplen las siguientes propiedades:*

(a) $A \cap B \subseteq A$ *y* $A \cap B \subseteq B$

(b) $A \cap A = A$ *y* $A \cap \varnothing = \varnothing$

(c) $A \cap (B \cap C) = (A \cap B) \cap C$

(d) $A \cap B = B \cap A$

(e) $A \cap B = A$ *si y sólo si* $A \subseteq B$

Probaremos algunas de las afirmaciones, el restos se quedarán como ejercicios.

[6]También se utiliza el término «disjuntos», que deriva del término en inglés 'disjoint'. Sin embargo, es preferible «ajenos».

Demostración. Probemos (a). Primero probemos que $A \cap B \subseteq A$, para ello, debemos tomar cualquier elemento en $A \cap B$ y verificar que también es elemento de A. Si $x \in A \cap B$ entonces $x \in A$ y $x \in B$, por lo tanto, $x \in A$ y tenemos que $A \cap B \subseteq A$. La otra contención es similar.

Probemos la segunda afirmación de (b). Debemos mostrar dos contenciones: $A \cap \varnothing \subseteq \varnothing$ y $\varnothing \subseteq A \cap \varnothing$. **Caso 1.** Probemos que $A \cap \varnothing \subseteq \varnothing$. Para ello, tomemos $x \in A \cap \varnothing$, es decir, $x \in A$ y $x \in \varnothing$. Pero $x \in \varnothing$ siempre es falsa, por lo tanto, $x \in A$ y $x \in \varnothing$ implica $x \in \varnothing$ es verdadera, que es lo que queríamos probar. **Caso 2.** Probemos que $\varnothing \subseteq A \cap \varnothing$, pero anteriormente mostramos que el conjunto vacío es subconjunto de cualquier conjunto. De ambos casos, concluimos que $A \cap \varnothing = \varnothing$.

Finalmente, probemos (d). Debemos probar que $A \cap B \subseteq B \cap A$ y que $B \cap A \subseteq A \cap B$. Probemos primero que $A \cap B \subseteq B \cap A$, consideremos $x \in A \cap B$, es decir, $x \in A$ y $x \in B$. Ya que las conjunciones conmutan (es decir, $P \wedge Q$ y $Q \wedge P$ son tautológicamente equivalentes), se sigue que $x \in B$ y $x \in A$ y, por lo tanto, $x \in B \cap A$. Por lo tanto, $A \cap B \subseteq B \subseteq A$. La otra contención es muy parecida. De ambas, se tiene que $A \cap B = B \cap A$. □

3.2.8 Más propiedades sobre la unión y la intersección

Teorema 8. *Sean A, B y C tres conjuntos arbitrarios. Se cumplen las siguientes propiedades:*

(a) Si $A \subseteq B$ entonces $A \cup C \subseteq B \cup C$.

(b) Si $A \subseteq B$ entonces $A \cap C \subseteq B \cap C$.

(c) Si $A \subseteq C$ y $B \subseteq C$ entonces $A \cup B \subseteq C$.

(d) Si $C \subseteq A$ y $C \subseteq B$ entonces $C \subseteq A \cap B$.

Probaremos algunas de las afirmaciones, el restos se quedarán como ejercicios.

Demostración. Primero probaremos (a). Suponemos que $A \subseteq B$ y debemos probar que $A \cup C \subseteq B \cup C$; para ello, tomemos $x \in A \cup C$. Por la definición de la unión, $x \in A$ o $x \in C$, por lo que tenemos dos casos. **Caso 1.** Supongamos que $x \in A$, por hipótesis $A \subseteq B$ y, así, $x \in B$; por el inciso (a) del teorema 6, tenemos que $x \in B \cup C$. **Caso 2.** Supongamos que $x \in C$, por el inciso

(a) del teorema 6, tenemos que $x \in B \cup C$. De ambos casos se sigue que $A \cup C \subseteq B \cup C$.

Finalmente probaremos (c). Supondremos que $A \subseteq C$ y $B \subseteq C$, debemos mostrar que $A \cup B \subseteq C$. Tomemos $x \in A \cup B$, por definición de la unión $x \in A$ o $x \in B$, así tenemos dos casos. **Caso 1.** $x \in A$, por hipótesis $A \subseteq C$, por lo tanto se sigue que $x \in C$. **Caso 2.** $x \in B$, por hipótesis $B \subseteq C$, por lo tanto se sigue que $x \in C$. De los dos casos, se sigue que $A \cup B \subseteq C$. □

Teorema 9. *Sean A, B y C tres conjuntos arbitrarios. Se cumplen las siguientes propiedades:*

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

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

Demostración. Sólo probaremos el inciso (a); debemos mostrar dos contenciones: $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ y $A \cup (B \cap C) \supseteq (A \cup B) \cap (A \cup C)$.

$\subseteq$] Tomemos $x \in A \cup (B \cap C)$, por la definición de unión, se tiene que $x \in A$ o $x \in B \cap C$, es decir, tenemos dos casos. **Caso 1.** $x \in A$. Por el inciso (a) del teorema 6, $x \in A \cup B$ y $x \in A \cup C$. Por la definición de intersección, se sigue que $x \in (A \cup B) \cap (A \cup C)$. **Caso 2.** $x \in B \cap C$, por la definición de intersección, se tiene que $x \in B$ y $x \in C$. Usando dos veces el inciso (a) del teorema 6, se sigue que $x \in A \cup B$ y $x \in A \cup C$. Por la definición de intersección, tenemos que $x \in (A \cup B) \cap (A \cup C)$. En ambos casos, hemos llegado a la conclusión que queríamos.

$\supseteq$] Tomemos $x \in (A \cup B) \cap (A \cup C)$, por la definición de intersección, se tiene que $x \in A \cup B$ y $x \in A \cup C$. Como cada unión implica dos casos y tenemos dos uniones, en total tenemos cuatro casos posibles. **Caso 1.** $x \in A$ y $x \in A$. Por el inciso (a) del teorema 6 concluimos que $x \in A \cup (B \cap C)$. **Caso 2.** $x \in A$ y $x \in C$. La prueba es idéntica que en el caso 1. **Caso 3.** $x \in B$ y $x \in A$. La prueba es idéntica que en el caso 1. **Caso 4.** $x \in B$ y $x \in C$. Por lo tanto, $x \in B \cap C$. Por el inciso (a) del teorema 6, tenemos que $x \in A \cup (B \cap C)$. De todos los casos, concluimos que $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$, que es lo que queríamos probar. □

3.2.9 Operaciones de conjuntos: la diferencia de conjuntos y el complemento de un conjunto

Dados dos conjuntos A y B, la *diferencia de conjuntos* $A \setminus B$ son todos los elementos de A que **no están** en B. Es decir,

$$A \setminus B = \{x \colon x \in A \wedge x \notin B\}.$$

O, de otra forma,

$$x \in A \setminus B \underset{\text{definición}}{\Longleftrightarrow} (x \in A \wedge x \notin B).$$

Cuando todos los elementos de los conjuntos con los que estamos trabajando están contenidos en un conjunto acordado X (al cual llamamos nuestro *universo* (de trabajo)), podemos definir el *complemento* de un conjunto dado A como todos los elementos del universo X que no están en A y se lo suele denotar por $\overline{A}$ o A^c. Es decir,

$$\overline{A} = X \setminus A.$$

Proposición 10. *Sean A y B. Se cumplen las siguientes propiedades:*

(a) $A \setminus A = \varnothing$ *y* $A \setminus \varnothing = A$

(b) $A \setminus B \subseteq A$

(c) $A \setminus B = A$ *si y sólo si* $A \cap B = \varnothing$

Demostración. Sólo demostraremos el inciso (c). Como es una doble implicación, debemos mostrar ambos sentidos.

$\Rightarrow$] Queremos demostrar que si $A \setminus B = A$ entonces $A \cap B = \varnothing$. En este caso, lo más fácil es demostrar la contraposición, *i. e.*, si $A \cap B \neq \varnothing$ entonces $A \setminus B \neq A$. Supongamos que $A \cap B \neq \varnothing$, es decir, existe un elemento x tal que $x \in A \cap B$. Por la definición de diferencia de conjuntos, $x \notin A \setminus B$. Pero $x \in A$, por lo tanto, $A \setminus B \neq A$, que es lo queríamos probar. Por lo tanto, si $A \setminus B = A$ entonces $A \cap B = \varnothing$.

$\Leftarrow$] Queremos demostrar que si $A \cap B = \varnothing$ entonces $A \setminus B = A$. Por el inciso (b) sabemos que $A \setminus B \subseteq A$, por lo que sólo faltaría por probar que $A \subseteq A \setminus B$. Tomemos $x \in A$. Por hipótesis, $x \notin B$ (pues son conjuntos ajenos). Por lo tanto, $x \in A \setminus B$ (recordemos que $A \setminus B$ son todos los elementos de A que no están en B). Por lo tanto, si $A \cap B = \varnothing$ entonces $A \setminus B = A$. □

Notemos que $\overline{\overline{A}} = A$. Si X es el universo, tenemos que $\overline{X} = \varnothing$ y $\overline{\varnothing} = X$.

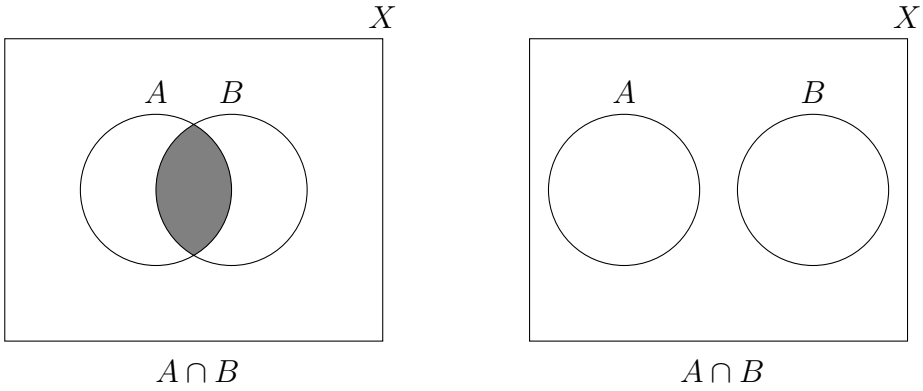


Figura 3: Intersección de conjuntos

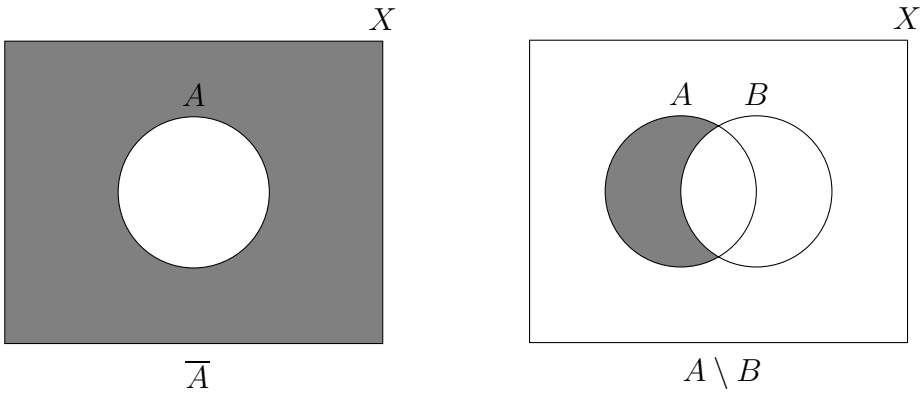


Figura 4: Complemento y diferencia de conjuntos

3.2.10 Las leyes de De Morgan

¿Cuándo un elemento x *no está* en $A \cup B$? Si x estuviese en A o x estuviese en B entonces x estuviera en $A \cup B$, por lo tanto, x no puede estar ni en A ni en B (es decir, x no está en A y x no está en B). Así, si $x \notin A \cup B$ entonces $x \notin A$ **y** $x \notin B$.

¿Cuándo un elemento x *no está* en $A \cap B$? Si x estuviese en A y x estuviese en B entonces x estuviera en $A \cup B$, por lo tanto, x no puede no estar en A o puede no estar en B. Es decir, si $x \notin A \cap B$ entonces $x \notin A$ **o** $x \notin B$.

Teorema 11. *Sean A, B y C tres conjuntos arbitrarios. Se cumplen las siguientes propiedades:*

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

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

Demostración. Probaremos el inciso (a). Debemos mostrar dos contenciones: $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$ y $A \setminus (B \cup C) \supseteq (A \setminus B) \cap (A \setminus C)$.

$\subseteq$] Consideremos $x \in A \setminus (B \cup C)$, es decir, x está en A y x no está en $B \cup C$. Por lo tanto, «x está en A y "x no está en B y x no está en C"» (uso las comillas solamente para señalar el orden de los enunciados). Por lo tanto[7], tenemos que «"x está en A y x no está en B" y "x está en A y x no está en C"»; de aquí que $x \in (A \setminus B) \cap (A \setminus C)$.

$\supseteq$] Consideremos $x \in (A \setminus B) \cap (A \setminus C)$. Por definición de intersección, tenemos que $x \in A \setminus B$ y $x \in A \setminus C$. Así, «"x está en A y x no está en B" y "x está en A y x no está en C"». Por la misma propiedad que el inciso previo, es equivalente a «"x está en A" y "x no está en B y x no está en C"». Por lo tanto, x está en A y x no está en $B \cup C$, es decir, $x \in A \setminus (B \cup C)$. □

Si consideramos que X es el *universo* en el que viven tanto los elementos de B como de C, podemos reescribir el teorema de la siguiente forma (que es la forma habitual de las leyes de De Morgan).

Teorema 12. *Sean B y C dos conjuntos arbitrarios. Se cumplen las siguientes propiedades:*

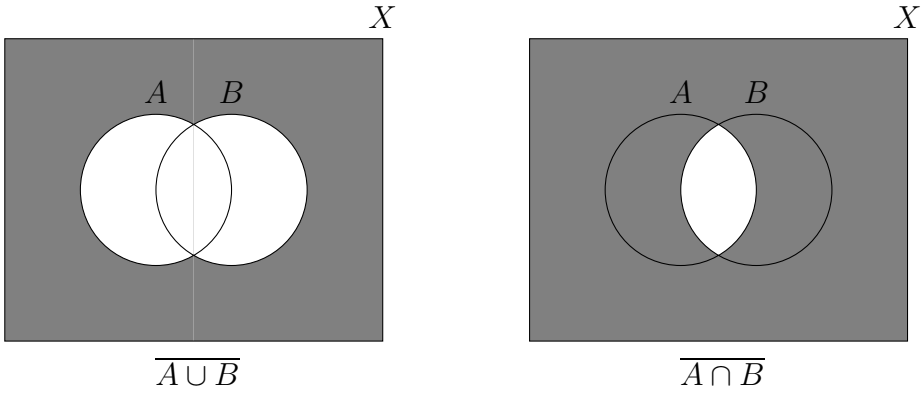
(a) $\overline{B \cup C} = \overline{B} \cap \overline{C}$

(b) $\overline{B \cap C} = \overline{B} \cup \overline{C}$

Notemos que tan sólo es la versión de conjuntos de «la negación de la conjunción es la disyunción y la negación de la disyunción es la conjunción»:

$$\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q) \text{ y } \neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$$

[7]Notemos que dados tres enunciados P, Q y R, se tiene que $P \wedge (Q \wedge R)$ es tautológicamente equivalente a $(P \wedge Q) \wedge (P \wedge R)$.



$\overline{A \cup B}$ $\overline{A \cap B}$

Figura 5: Complementos de la unión y la intersección

3.3 Parejas ordenadas y el producto cartesiano

Previamente vimos las parejas no ordenadas, ahora veremos las **parejas ordenadas**. Dados dos elementos, a y b, llamamos a $(a,\ b)$ una *pareja ordenada* con *primera entrada* a y *segunda entrada* b. Lo importante en las parejas ordenadas es precisamente el **orden**. Si tenemos dos parejas ordenadas $(a,\ b)$ y $(c,\ d)$, tenemos que

$$(a, b) = (c, d) \text{ si y sólo si } a = c \text{ y } b = d.$$

Es importante pensar en cuándo **no es cierto** que dos parejas $(a,\ b)$ y $(c,\ d)$ son iguales (es decir, cuándo son diferentes), que es simplemente negar ambos lados del enunciado previo.

$$(a, b) \neq (c, d) \text{ si y sólo si } a \neq c \text{ o } b \neq d.$$

Para que dos parejas ordenadas sean **iguales**, debe pasar que **son iguales entrada a entrada** (en todas las entradas) mientras que para que dos parejas ordenadas sean **diferentes**, debe pasar que **son diferentes en *al menos* una entrada**.

Dados dos conjuntos A y B, el *producto cartesiano* de A y B, que denotamos por $A \times B$, es el conjunto de todas las parejas ordenadas cuyas primeras entradas están en A y cuyas segundas entradas están en B. Es decir,

$$A \times B = \{(x, y) \colon x \in A \wedge y \in B\}$$

o, de dicho de otra forma,

$$(x, y) \in A \times B \underset{\text{definición}}{\Longleftrightarrow} (x \in A \wedge y \in B).$$

Teorema 13. *Dados dos conjuntos A y B, se tiene que $A \times B \neq \varnothing$ si y sólo si $A \neq \varnothing$ y $B \neq \varnothing$.*

Demostración. Como es una doble implicación, debemos probar ambos sentidos.

$\Rightarrow$] Debemos probar que si $A \times B \neq \varnothing$ entonces $A \neq \varnothing$ y $B \neq \varnothing$. Como es una implicación, debemos suponer el antecedente y llegar, a través de deducciones lógicas, a la consecuencia. Así, supongamos que $A \times B \neq \varnothing$; esto significa que hay una pareja ordenada en el producto cartesiano, es decir, podemos tomar $(x, y) \in A \times B$. Por la definición del producto cartesiano, sabemos que $x \in A$ y $x \in B$. ¡Pero esto significa que $A \neq \varnothing$ y $B \neq \varnothing$!

$\Leftarrow$] Debemos probar que si $A \neq \varnothing$ y $B \neq \varnothing$ entonces $A \times B \neq \varnothing$. Como $A \neq \varnothing$ y $B \neq \varnothing$, existen x y y tales que $x \in A$ y $y \in B$. Tenemos que (x, y) es una pareja ordenada y, por definición de producto cartesiano, $(x, y) \in A \times B$. Por lo tanto, $A \times B \neq \varnothing$. □

Pregunta. ¿Qué dice la contraposición del teorema 13?

Ejemplo 3. Consideremos los conjuntos $A = \{\&, 2, 3\}$ y $B = \{\bigstar, 1\}$. Determínese $A \times B$, $B \times A$, $A \times A$ y $B \times B$.

Tenemos que:

- $A \times B = \{(\&, \bigstar), (\&, 1), (2, \bigstar), (2, 1), (3, \bigstar), (3, 1)\}$
- $B \times A = \{(\bigstar, \&), (\bigstar, 2), (\bigstar, 3), (1, \&), (1, 2), (1, 3)\}$
- $A \times A = \{(\&, \&), (\&, 2), (\&, 3), (2, \&), (2, 2), (2, 3), (3, \&), (3, 2), (3, 3)\}$
- $B \times B = \{(\bigstar, \bigstar), (\bigstar, 1), (1, \bigstar), (1, 1)\}$

Observemos que $(\&, \bigstar) \neq (\bigstar, \&)$ (pues $\& \neq \bigstar$). Por ello, $(\&, \bigstar) \in A \times B$ pero $(\&, \bigstar) \notin B \times A$. Por lo tanto, concluimos que, en general, $A \times B \neq B \times A$. Es decir, a diferencia de la unión y la intersección, el producto cartesiano **no es conmutativo**.

3.3.1 Relaciones binarias

Desde al menos la educación básica, conocemos algunas relaciones binarias, como por ejemplo el «menor que», «mayor que», «igual a» «menor que o

igual a», «mayor que o igual a», etcétera. Pensemos, por ejemplo, en la relación «menor que» en los números enteros. Por ejemplo, tenemos que

$$-9 < -8,\ \ -3 < 3,\ \ 9 < 13,\ \ -5 < 0,\ \ -1000 < 500.$$

Dado que involucran dos números (y el orden ciertamente importa porque no podemos escribir $-8 < -9$), podemos reescribir dichas relaciones en forma de parejas ordenadas:

$$(-9, -8),\ (-3, 3),\ (9, 13),\ (-5, 0),\ (-1000, 500).$$

En general, podemos escribir que la relación de ser *menor que* en los números enteros es el conjunto

$$\{(m, n) \colon (m, n) \in \mathbb{Z} \text{ y } n - m \text{ es un entero positivo}\}.$$

La relación de *igualdad* en los números enteros quedaría dada por el conjunto de parejas ordenadas

$$\{(m, n) \colon m, n \in \mathbb{Z} \text{ y } m = n\}.$$

Ambos conjuntos son subconjuntos de $\mathbb{Z} \times \mathbb{Z}$.

En general, dado un conjunto X, una *relación (binaria)* R sobre X es cualquier subconjunto del producto cartesiano $X \times X$. Por ejemplo, si $X = \{1, 2, 3, 4\}$, $R = \{(1, 1), (1, 3), (1, 4), (2, 3)\}$ es una relación sobre X.

Si R es una relación sobre un conjunto X y $(x, y) \in R$, muchas veces lo encontraremos denotado como $x\mathrm{R}y$, que es precisamente la notación que usamos en $>, <, =, \geq, \leq$.

Notemos que, para cualquier conjunto X, el conjunto $\varnothing$ es un subconjunto de $X \times X$ (recordemos que el vacío es subconjunto de cualquier conjunto) y, por lo tanto, es una relación sobre X, se la llama la *relación vacía*. Otra relación relevante es $X \times X$, que es subconjunto de sí mismo.

3.3.2 Pruebas por vacuidad

Una relación sobre X es un «conjunto de parejas ordenadas de elementos en X» y acabamos de afirmar que el vacío es una relación, por lo tanto, es un conjunto de parejas ordendas; pero, ¿cómo puede ser un conjunto de parejas ordenadas si no tiene elementos? Que un conjunto R sea un «conjunto de parejas ordenadas» significa que la siguiente proposición es verdadera

$$\forall x \in R (x \text{ es una pareja ordenada}). \tag{3.3}$$

Si R no fuese un conjunto de parejas ordenadas, entonces el enunciado 3.3 sería falso y, por lo tanto, su negación es verdadera:

$$\exists x \in R(x \textbf{ no} \text{ es una pareja ordenada}), \tag{3.4}$$

pero para el conjunto vacío, el enunciado anterior es falso. Por lo tanto, para el vacío el enunciado 3.3 es verdadero y, por lo tanto, el vacío es un conjunto de parejas ordenadas.

3.3.3 Algunas propiedades de las relaciones

En esta sección, consideremos una relación R sobre un conjunto X (es decir, $R \subseteq X \times X$).

- R es *reflexiva* si para todo $x \in X$, se tiene que $(x, x) \in R$ o, equivalentemente, $x\mathrm{R}x$.
- R es *simétrica* si para toda $(x, y) \in R$, también tenemos que $(y, x) \in R$. De otra forma, si $x\mathrm{R}y$ entonces $y\mathrm{R}x$.
- R es *transitiva* si siempre que (x, y), $(y, z) \in R$ entonces $(x, z) \in R$. De otra forma, si $x\mathrm{R}y$ y $y\mathrm{R}z$ entonces $x\mathrm{R}z$.
- R es *antisimétrica* si siempre que (x, y), $(y, x) \in R$ entonces $x = y$. De otra forma, si $x\mathrm{R}y$ y $y\mathrm{R}x$ entonces $x = y$.

3.3.4 Algunos ejemplos

- La relación «menor que» en $\mathbb{Z}$ es transitiva, pero no es reflexiva ni simétrica.

  Por ejemplo, tenemos que $-10 < 3$, $3 < 10$ y, ciertamente, $-10 < 10$.

- La relación de «ser igual» en $\mathbb{Z}$ es reflexiva, simétrica y transitiva. Por ejemplo, si $4 \cdot 2 = 8$ y $8 = 16/2$ entonces $4 \cdot 2 = 16/2$.

- La relación «mayor que o igual a» es antisimétrica, si $a \leq 7$ y $a \geq 7$ entonces $a = 7$.

4 Funciones

Un caso más general de las relaciones es cuando, en vez de considerar un sólo conjunto X, consideremos dos conjuntos X y Y. Decimos que R es una *relación de X en Y* si $R \subseteq X \times Y$. Y caso particular de estas relaciones son las funciones.

Dados dos conjuntos X y Y, una función f de X en Y es una **correspondencia** (que es un caso particular de una relación) tal que, a cada elemento x en X, le asigna **un y sólo un** elemento y en Y. Usualmente la denotamos como $f\colon X \to Y$. Al conjunto X se lo llama el *dominio* de la función, al conjunto Y, el *contradominio* o *codominio* de la función, a la forma de asignarle a cada $x \in X$ su $y \in Y$, se la llama la *regla de correspondencia* y decimos que $y = f(x)$ es la *imagen* bajo f de x.

Algunos ejemplos de funciones. Ejemplos intuitivos hay muchos y son muy comunes.

- A cada persona le corresponde su edad, todos tienen una edad y es única. En este caso, el dominio sería el conjunto de todas las personas y el contradominio el conjunto de todos los enteros no negativos.

- En una ciudad dada, cada día del año tiene una temperatura máxima. En este caso, el dominio son todos los días del año y el contradominio son los números reales.

- A cada estudiante de la UAM le corresponde una y sólo una matrícula. El dominio es el conjunto de todos los estudiantes de la UAM y el contradominio el conjunto de las posibles matrículas.

- A cada persona le corresponde su dirección de correo electrónico. ¿O no? Pues no, no es función, porque una persona podría tener más de una dirección de correo electrónico o incluso no tener.

En la figura 6 aparece la función $f\colon A \to B$, donde el dominio es el conjunto

$$A = \{\text{Miguel}, \text{Mariana}, \text{Alicia}, \text{Luis}\}$$

y el contradominio es el conjunto

$$B = \{21, 22, 23, 24, 25\}.$$

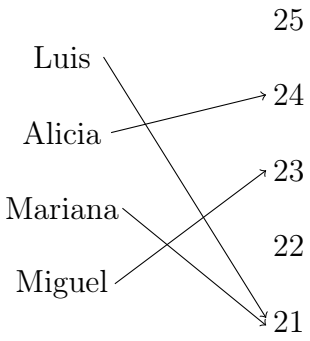


Figura 6: Una función f, donde la columna de la izquierda es el dominio y la de la derecha, el contradominio de f

Una forma de representar f es haciendo uso de las parejas ordenadas, de la forma siguiente:

$$f = \{(\text{Luis}, 21), (\text{Alicia}, 24), (\text{Mariana}, 21), (\text{Miguel}, 23)\}.$$

Tenemos que $f \subseteq A \times B$. En la definición de función pedimos que:

> «[...] a cada elemento x en A, le asigna **un y sólo un** elemento y en B [...]»

por lo que debe cumplirse que

- para cada $x \in A$, existe $y \in B$ tal que $(x, y) \in f$ y
- la y que asignamos es única, es decir, *no puede haber dos diferentes*, esto lo decimos de la forma siguiente: si $(x, y_1), (x, y_2) \in f$, como las segundas entradas no pueden ser diferentes, entonces

$$y_1 = y_2.$$

Definición 14 (Función)**.** Dados dos conjuntos A y B, una función f es un subconjunto de $A \times B$ que satisface las siguientes dos condiciones:

- para todo $x \in A$, existe $y \in B$ tal que $(x, y) \in f$ y
- si $(x, y_1), (x, y_1) \in f$ entonces $y_1 = y_2$.

¡Advertencia!

La figura 6 define formalmente una función, ya que nos dice quién es el

dominio, quién el contradominio y cuál es la regla de correspondencia. Para que algo sea función, no necesariamente tiene que estar presentada de la forma $f\colon A \to B$ con $y = f(x)$.

Dada una función f, por $\mathrm{Dom}(f)$ denotamos el dominio de la función f y por $\mathrm{Cod}(f)$ el contradominio de la función f.

Al igual que en lógica vimos cuándo dos proposiciones son *lógicamente equivalentes* y cuándo dos conjuntos son *iguales*, ahora veremos cuando dos funciones son iguales. Para tener una función, requerimos de tres cosas: el dominio, el contradominio y la regla de correspondencia (que no son más que las parejas ordenadas). Dos funciones $f\colon A \to B$ y $g\colon C \to D$ son *iguales* si y sólo si tienen el mismo dominio, el mismo contradominio y la misma regla de correspondencia, es decir,

$$A = C,\ B = D \text{ y } f = g.$$

Recordemos que, dadas una función $f\colon A \to B$ y $x \in A$, la $y \in B$ que le corresponde a x es la imagen de x bajo f y lo denotamos como $f(x) = y$. Por ejemplo, en la función f que aparece en la figura 6, el dominio es el conjunto $A = \{\text{Luis, Alicia, Mariana, Miguel}\}$ y el contradominio es el conjunto $B = \{21, 22, 23, 24, 25\}$. La imagen bajo f de Luis es 21, de Alicia es 24, de Mariana es 21 y de Miguel es 23. También podemos considerar la imagen no de sólo un elemento sino de un subconjunto del dominio. Por ejemplo, la imagen de $\{\text{Miguel, Luis}\}$ bajo f es $\{21, 23\}$ que es un subconjunto del contradominio. En general, si $C \subseteq A$, la *imagen directa de C bajo f* se denota por $f[C]$ y se define como

$$f[C] = \{f(x)\colon x \in C\}.$$

La *imagen (o rango) de la función f* es el conjunto $f[A]$, que es subconjunto de B y se la denota por $\mathrm{Im}(f)$. Por otro lado, si queremos saber de qué elementos en el dominio es imagen el 23, podemos ver que es Miguel, ya que $f(\text{Miguel}) = 23$; de quién es imagen $\{23, 24\}$, es $\{\text{Alicia, Miguel}\}$ y de quién es imagen 22, es $\varnothing$. Formalmente, dado $D \subseteq B$, la *imagen inversa de D bajo f* se denota por $f^{-1}[D]$ y se define como

$$f^{-1}[D] = \{x\colon f(x) \in D\}.$$

Observemos que siempre pasa que $f^{-1}[B] = A$, ¿por qué?

Ejemplos

1. Consideremos la función $f\colon \mathbb{Z} \to \mathbb{Z}$ tal que

$$f(x) = \begin{cases} 1 & \text{si } x \text{ es impar y} \\ 0 & \text{si } x \text{ es par.} \end{cases}$$

   Determina:

   (a) La imagen de -3, 0 y $^1/_2$.
   (b) La imagen directa de B, donde B es el conjunto de todos los números enteros pares.
   (c) La imagen de f.
   (d) La imagen inversa de 1.
   (e) La imagen inversa de $\{3, 4, 5\}$.

   Solución.

   (a) $f(-3) = 1$, $f(0) = 0$ y $f(^1/_2)$ no está definida porque $^1/_2$ no está en el dominio de la función.
   (b) $f[B] = \{0\}$.
   (c) $\text{Im}(f) = \{0, 1\}$.
   (d) $f^{-1}[\{1\}]$ es el conjunto de todos los números enteros impares.
   (e) $f^{-1}[\{3, 4, 5\}] = \varnothing$, porque ningún elemento del dominio tiene como imagen los números 3, 4 o 5.

2. Considera la función *valor absoluto*, $g\colon \mathbb{Z} \to \mathbb{Z}$, con $g(x) = |x|$. Determina lo siguiente:

   (a) Las imágenes de -2, 0 y 2.
   (b) La imagen directa de $\{-1, 2, -3, 4, -5\}$.
   (c) La imagen de f.
   (d) La imagen inversa de $\{3, 2, 1\}$.
   (e) La imagen inversa de $\{-3, -2, -1\}$.
   (f) La imagen inversa de $\{2\}$ y $\{-2\}$.

   Solución.

   (a) $g(-2) = 2$, $g(0) = 0$ y $g(2) = 2$.
   (b) $g[\{-1, 2, -3, 4, -5\}] = \{1, 2, 3, 4, 5\}$.
   (c) $\text{Im}(g) = \mathbb{Z}^+ \cup \{0\}$.
   (d) $g^{-1}[\{-3, -2, -1\}] = \{-3, -2, -1, 1, 2, 3\}$.
   (e) $g^{-1}[\{-3, -2, -1\}] = \varnothing$.

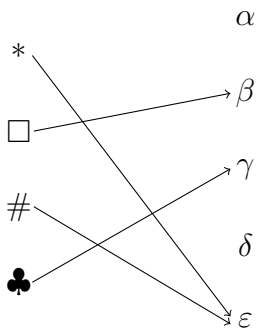


Figura 7: La función h, donde la columna de la izquierda es el dominio y la de la derecha, el contradominio de h

(f) $g^{-1}[\{2\}] = \{-2, 2\}$ y $g^{-1}[\{-2\}] = \varnothing$.

3. Considera la función h que aparece en la figura 7. Determina lo siguiente:

   (a) El dominio y el contradominio de h.
   (b) La imagen de h.
   (c) La imagen directa de $\{\clubsuit, \square\}$.
   (d) La imagen inversa de $\{\alpha\}$, $\{\alpha, \varepsilon\}$ y $\{\varepsilon\}$.

   Solución.

   (a) $\mathrm{Dom}(h) = \{*, \square, \#, \clubsuit\}$ y $\mathrm{Cod}(h) = \{\alpha, \beta, \gamma, \delta, \varepsilon\}$.
   (b) $\mathrm{Im}(h) = \{\beta, \gamma, \varepsilon\}$
   (c) $h[\{\clubsuit, \square\}] = \{\beta, \gamma\}$
   (d) $h^{-1}[\{\alpha\}] = \varnothing$, $h^{-1}[\{\alpha, \varepsilon\}] = \{*, \#\}$ y $h^{-1}[\{\varepsilon\}] = \{*, \#\}$.

4. Considera la función $j\colon \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2 + 2x - 3$. Determina lo siguiente:

   (a) La imagen -3, -1 y 1
   (b) La imagen directa de $[0, \infty)$.
   (c) La imagen de j.
   (d) La imagen inversa de $\{0\}$, $(-\infty, -3)$ y $[-3, \infty)$.

   Solución.

   (a) $j(-3) = 0$, $j(-1) = -4$ y $j(1) = 0$.
   (b) $j[[0, \infty)] = [-3, \infty)$.

(c) $\mathrm{Im}(j) = [-3, \infty)$
(d) $j^{-1}[\{0\}] = \{-3, 1\}$, $j^{-1}[(-\infty, -3)] = \varnothing$ y $j^{-1}[[-3, \infty)] = \mathbb{R}$.

4.1 Ejemplos de funciones

4.1.1 Dado cualquier conjunto X, la *función identidad* es $1_X \colon X \to X$ y está dada por

$$1_X(x) = x,$$

para todo $x \in X$.

4.1.2 Dado cualquier conjunto X, existe una única *función vacía* $f \colon \varnothing \to X$, donde la regla de correspondencia es el conjunto vacío.

Recuerda que una función es un conjunto de parejas ordenadas, en concreto, en un subconjunto del producto del cartesiano $\mathrm{Dom}(f) \times \mathrm{Im}(f)$; en el caso de las funciones vacías, $\mathrm{Dom}(f) = \varnothing$, y así $\mathrm{Dom}(f) \times \mathrm{Im}(f) = \varnothing$ (véase el teorema 13). Pero el único subconjunto del vacío es el vacío.

4.1.3 Si $X \neq \varnothing$, no existe ninguna función $f \colon X \to \varnothing$, porque para cualquier $x \in X$, tendríamos que $f(x) \in \varnothing$.

4.1.4 La función *valor absoluto* $|\cdot| \colon \mathbb{R} \to \mathbb{R}$, para todo $x \in \mathbb{R}$ se define como

$$|x| = \begin{cases} x & \text{si } x \geq 0 \text{ o} \\ -x & \text{si } x < 0. \end{cases}$$

Por ejemplo, en para $x = 3$, como $x \geq 0$, tenemos que $|3| = 3$. Si, por otro lado $x = -3$, ya que tenemos que $x < 0$ y así $|-3| = -(-3) = 3$.

4.1.5 La función *parte entera* o *función piso* $\lfloor \quad \rfloor \colon \mathbb{R} \to \mathbb{Z}$ se define, para $x \in \mathbb{R}$, como

$$\lfloor x \rfloor = \text{ el mayor entero menor que o igual a } x,$$

es decir, $\lfloor x \rfloor$ es el entero inmediato a la izquierda de x en la recta real.

Por ejemplo, $\lfloor \sqrt{5} \rfloor = 2$, $\lfloor 0 \rfloor = 0$, $\lfloor 5/3 \rfloor = 1$ y $\lfloor -5/3 \rfloor = -2$.

4.1.6 La función *función techo* $\lceil \quad \rceil \colon \mathbb{R} \to \mathbb{Z}$ se define, para $x \in \mathbb{R}$, como

$$\lceil x \rceil = \text{ el menor entero mayor que o igual a } x,$$

es decir, $\lceil x \rceil$ es el entero inmediato a la derecha de x en la recta real.

Por ejemplo, $\lceil \sqrt{5} \rceil = 3$, $\lceil 0 \rceil = 0$, $\lceil {}^{5}/_{3} \rceil = 2$ y $\lceil -{}^{5}/_{3} \rceil = -1$.

4.1.7 Considera la función $g\colon \mathbb{N} \to \mathbb{Z}$, con $0 \in \mathbb{N}$, definida para $x \in \mathbb{N}$ como

$$g(x) = \begin{cases} {}^{x}/_{2} & \text{si } x \text{ es par} \\ -\lceil {}^{x}/_{2} \rceil & \text{si } x \text{ es impar.} \end{cases}$$

4.1.8 Dado un conjunto X, consideremos una familia[8] $\mathcal{A}$ de conjuntos de X. Definamos la 'función' $f\colon \mathcal{A} \to X$, tal que para $A \in \mathcal{A}$,

$$f(A) = a,$$

para todo $a \in A$.

Por lo general, f **no es** una función. Si $X = \{1, 2, 3\}$ y $\mathcal{A} = \{\{1, 2\}, \{1, 2, 3\}, \varnothing\}$ tendríamos que:

(a) $f(\{1, 2\}) = 1$ y $f(\{1, 2\}) = 2$. Para que f sea función, a cada elemento en el dominio le debe corresponder **un único** elemento en el contradominio, en este caso le corresponden dos.

(b) $f(\varnothing) = ?$ Para que f sea función, a cada elemento en el dominio le debe corresponder un elemento en el contradominio, en este caso no le corresponde ninguno.

4.2 Inyectiva, suprayectiva y biyectiva

Una función $f\colon A \to B$ es *inyectiva* (o *uno-a-uno*) si cualesquiera dos elementos diferentes en el dominio siempre van a dar a elementos diferentes en el contradomino. Es decir,

$$\forall x_1 \forall x_2 (x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)). \tag{4.1}$$

La contraposición dice que

$$\forall x_1 \forall x_2 (f(x_1) = f(x_2) \Rightarrow x_1 = x_2). \tag{4.2}$$

Intuitivamente, la función «no pega» cosas. Por ejemplo, no hay dos estudiantes de la UAM que puedan tener la misma matrícula. Las funciones

[8] *Familia* es un sinónimo de conjunto.

'hash' nos gustaría que fueran inyectivas, aunque no puedan serlo (si no sabes que es una función 'hash', búscalo en Wikipedia).

Una función $f\colon A \to B$ es *suprayectiva* (o *sobre*) si para cada elemento $y \in B$, existe un elemento $x \in A$ tal que $f(x) = y$. Es decir,

$$\forall y \in B \exists x \in A(f(x) = y). \tag{4.3}$$

Una función $f\colon A \to B$ es *biyectiva* si es tanto inyectiva como suprayectiva. También se suele decir que f es una *correspondencia biunívoca* entre A y B.

Consideremos una función $f\colon A \to B$ inyectiva, pero no suprayectiva. ¿Qué le falta a f para ser biyectiva? No cumple que sea suprayectiva (y no hay forma que, con el dominio y el contradominio dados, lo haga), pero podríamos modificar el contradominio al considerar $\mathrm{Im}(f)$. Definamos la función $f^*\colon A \to \mathrm{Im}(f)$ con la misma regla de correspondencia, es decir, $f^*(x) = f(x)$. Por la definición de la imagen de f, tenemos que f^* es una función biyectiva. Frecuentemente se escribe $f\colon A \to \mathrm{Im}(f)$ aunque sea un abuso de notación.

Ejemplos

1. La función identidad $1_X\colon X \to X$ es tanto inyectiva como suprayectiva, es decir, es biyectiva.

2. Consideremos la función valor absoluto $f\colon \mathbb{R} \to \mathbb{R}$ dada por $f(x) = |x|$. Demuestra que la función f no es inyectiva ni suprayectiva.

   Solución. Para mostrar que f no es inyectiva, debemos mostrar que alguna de las proposiciones 4.1 o 4.2 (que son la definición de ser inyectiva) es falsa. Eso significa que sus negaciones[9] son verdaderas, es decir, que

   $$\exists x_1 \exists x_2(x_1 \neq x_2 \wedge f(x_1) = f(x_2)) \tag{4.4}$$

   o

   $$\exists x_1 \exists x_2(f(x_1) = f(x_2) \wedge x_1 \neq x_2) \tag{4.5}$$

   es verdadera. Es decir, para mostrar que una función **no es inyectiva**, debemos encontrar dos elementos diferentes en el dominio tal que sus

[9] Recuerda que

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

imágenes sean iguales. Por ejemplo, 2 y -2, ya que $f(2) = |2| = 2$ y $f(-2) = |-2| = 2$. Así, $f(2) = f(-2)$ y, por lo tanto, f no es inyectiva.

Para mostrar que f no es suprayectiva, debemos mostrar que la proposición 4.3 es falsa. Eso significa que su negación es verdadera, es decir, que

$$\exists y \in B \forall x \in A(f(x) \neq y).$$

El contradominio de la función f son todos los reales, en particular, -1 está ahí. Y ya que $f(x) = |x| \geq 0$ para todo x, no existe ninguna $x \in \mathbb{R}$ tal que $f(x) = -1$. Esto muestra que f no es suprayectiva.

3. Consideremos la función valor absoluto $g\colon \mathbb{R} \to [0, \infty)$ dada por $g(x) = |x|$. Demuestra que la función g no es inyectiva, pero sí es suprayectiva.

   Solución. Para mostrar que g no es inyectiva, procedemos igual que en el ejercicio previo, debemos encontrar dos elementos diferentes en el dominio tal que sus imágenes sean iguales. Por ejemplo, 2 y -2, ya que $g(2) = |2| = 2$ y $g(-2) = |-2| = 2$. Así, $g(2) = g(-2)$ y, por lo tanto, g no es inyectiva.

   Para mostrar que g es suprayectiva, debemos mostrar que

   $$\forall y \in [0, \infty) \exists x \in \mathbb{R}(g(x) = y).$$

   Si $y \in [0, \infty)$, ya que $y \geq 0$ se tiene que $|y| = y$. En este caso en particular, la x que buscamos es $x = y$, ya que $g(x) = g(y) = y$. Eso se cumple para toda $y \in [0, \infty)$. Por lo tanto, g es una función suprayectiva.

4. Consideremos la función valor absoluto $h\colon [0, \infty) \to \mathbb{R}$ dada por $h(x) = |x|$. Demuestra que la función h no es suprayectiva, pero sí es inyectiva.

   Solución. Para mostrar que h no es suprayectiva, procedemos igual que en el primer ejercicio, El contradominio de la función f son todos los reales, en particular, -1 está ahí. Y ya que $h(x) = |x| \geq 0$ para todo x, no existe ninguna $x \in \mathbb{R}$ tal que $h(x) = -1$. Esto muestra que h no es suprayectiva.

   Para mostrar que g es inyectiva, debemos mostrar que

   $$\forall x_1 \forall x_2 (x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)).$$

Consideremos x_1, $x_2 \in [0, \infty)$ tal que $x_1 \neq x_2$. Podemos suponer que $x_1 < x_2$, **sin pérdida de generalidad**[10]. Y ambos son no negativos, por lo que se tiene que $0 \leq x_1 < x_2$. Por la definición de valor absoluto, $h(x_1) = |x_1| = x_1$ y $h(x_2) = |x_2| = x_2$, por lo tanto, $h(x_1) < h(x_2)$ y así $h(x_1) \neq h(x_2)$. Por lo tanto, h es una función inyectiva.

5. Consideremos la función valor absoluto $j\colon [0, \infty) \to [0, \infty)$ dada por $j(x) = |x|$. Demuestra que la función j es biyectiva.

   Solución. Para mostrar que j es biyectiva, hay que probar que es inyectiva y que es suprayectiva. La prueba de que es suprayectiva es igual a la segunda parte del segundo problema y la prueba de que es inyectiva es igual a la segunda parte del tercer problema.

Notemos que en los tres ejemplos anteriores, las cuatro funciones f, g, h y j tienen la misma regla de correspondencia, pero la primera no es inyectiva ni suprayectiva, la segunda es suprayectiva, pero no inyectiva, la tercera es inyectiva, pero no suprayectiva y la cuarta es inyectiva y suprayectiva. La diferencia está en los dominios y contradominios de las funciones, de aquí que no basta con conocer la regla de correspondencia para determinar si una función es o no inyectiva o suprayectiva.

¡Advertencia!

Depende de qué es lo que queramos probar qué será lo que busquemos. Si deseamos probar que una función **sí es inyectiva**, debemos verificar que alguna de las proposiciones 4.1 o 4.2 es verdadera, como aparecen «para todos», tenemos que verificarlo **para todos** los elementos del dominio. Si, por otro lado, deseamos probar que una función **no es inyectiva**, debemos verificar que la proposición 4.4 es verdadera, como aparecen «existen», basta con **mostrar** dos elementos en el dominio que hagan verdadera la proposición.

[10] *Sin pérdida de generalidad* es una frase que encontraremos habitualmente en matemáticas. En este caso, ya que x_1 y x_2 son números reales distintos, necesariamente uno es más que chico que el otro, es decir, pasa que $x_1 < x_2$ o que $x_2 < x_1$. La única distinción recae en los subíndices, pero la prueba para ambos casos (es una prueba por casos) es idéntica, por lo que basta con hacerlo para una de las dos posibilidades.

4.3 Restricciones de las funciones

Dada una función $f\colon A \to B$, a veces nos interesa fijarnos en esa función pero sólo **en algunos** elementos del dominio, es decir, en un subconjunto $A' \subseteq A$. Por ejemplo, en la función f dada en la figura 6, queremos fijarnos en la función pero sólo en el subconjunto {Mariana, Miguel} del dominio. La idea es «borrar» la parte del dominio que no nos interesa y quedarnos con la que sí nos interesa. Véase la figura 8.

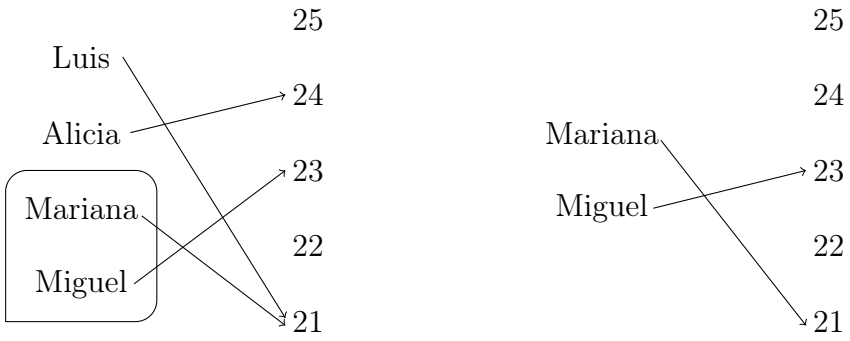


Figura 8: En la función f de la izquierda señalamos el subconjunto del dominio que nos interesa y en la de la derecha aparece la *restricción* de f al subconjunto deseado

Formalmente, dada una función $f\colon A \to B$ y un subconjunto $A' \subseteq A$, la *restricción de f a A'* es la función

$$f\restriction_{A'}\colon A' \to B$$

donde la regla de correspondencia, para $x \in A'$, es

$$f\restriction_{A'}(x) = f(x).$$

La función de la izquierda es la que estamos definiendo, la de la derecha ya nos la dieron y está bien definida porque ya que $x \in A'$ y $A' \subseteq A$, tenemos que $x \in A$, que es el dominio de la f.

De los ejemplos de la subsección 4.2, la función h es la restricción de la función f a $[0, \infty)$, pero ni g ni j son restricciones de la función f.

Ejemplos

1. Dado cualquier conjunto X, $1_X\colon X \to X$ es la función identidad de X en X. Si X' es cualquier subconjunto de X, la restricción de 1_X al

subconjunto X' es la *función inclusión de X' en X*

$$1_X\restriction_{X'}: X' \to X.$$

A veces se la denota como

$$1_X\restriction_{X'}: X' \hookrightarrow X.$$

Siempre es inyectiva (ya que la identidad es biyectiva) y si además X' es subconjunto propio de X, no será suprayectiva.

4.4 Composición de funciones

Consideremos las funciones f y g que aparecen en la figura 9 (donde la columna de la izquierda representa el dominio y la de la derecha, el contradominio). La función f le asigna a cada una de las cuatro personas del conjunto {Miguel, Mariana, Alicia, Luis} su edad y la función g asigna a cada edad, el año de nacimiento. Si quisieramos saber en qué año nació Miguel, primero aplicamos la función f, es decir, $f(\text{Miguel}) = 23$ y al resultado le aplicamos g, es decir, $g(23) = 1996$; Miguel nació en 1996. Para simplificar, podemos escribir $g(f(\text{Miguel})) = g(23) = 1996$. A esto se le conoce como la composición de funciones, observemos que para que esto haya tenido sentido, $f(x)$ debe ser elemento del dominio de g, para cualquier $x \in \text{Dom}(f)$ y, por otro lado, recordemos que $f(x) \in \text{Im}(f)$; de esto que debe pasar que $\text{Im}(f) \subseteq \text{Dom}(g)$.

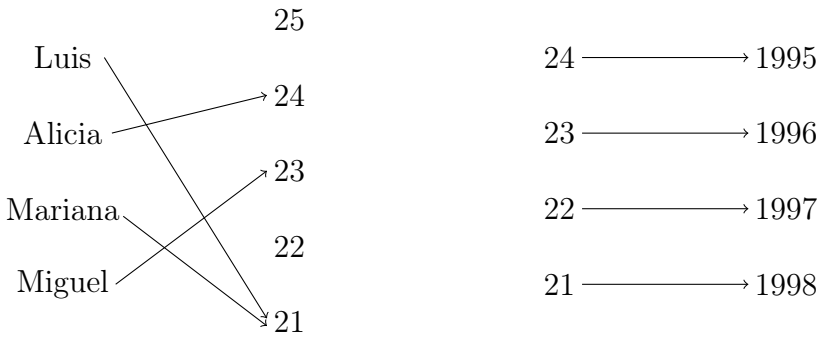


Figura 9: A la izquierda aparece la función f, que asigna a cada persona su edad, y a la derecha, la función g, que asigna a cada edad, el año de nacimiento

Formalmente, dadas dos funciones $f\colon A \to B$ y $g\colon C \to D$ tales que $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$, la *composición g 'bolita' f*, denotada[11] como $g \circ f$, es la función

$$g \circ f\colon A \to D,$$

dada por $g(f(x))$, para todo $x \in A$. Es decir,

$$(g \circ f)(x) = g(f(x)).$$

En particular, si $f\colon A \to B$ y $g\colon B \to C$ entonces claramente existe la composición $g \circ f\colon A \to C$ porque $\mathrm{Im}(f) \subseteq \mathrm{Cod}(f) = \mathrm{Dom}(g)$.

Ejemplos

1. Considera las funciones $f\colon \mathbb{R} \to \mathbb{R}$ y $g\colon [0, \infty) \to \mathbb{R}$ dadas por

   $$f(x) = x^2 \text{ y } g(x) = \sqrt{x},$$

   donde en cada caso la x pertenece al dominio que le corresponde. ¿Existe alguna de las composiciones $f \circ g$ o $g \circ f$? En caso afirmativo, determina cuál es su dominio, su contradominio y su regla de correspondencia.

   Solución. Para que la composición $f \circ g$ exista, debe pasar que $\mathrm{Im}(g) \subseteq \mathrm{Dom}(f)$. ¿Cuál es la imagen de la función g? Tenemos que $\mathrm{Im}(g) = [0, \infty)$, que ciertamente es subconjunto del dominio de f, que $\mathbb{R}$. Por lo tanto, la composición sí está definida y tenemos que

   $$f \circ g\colon [0, \infty) \to \mathbb{R}$$

   y

   $$(f \circ g)(x) = f(g(x)) = f(\sqrt{x}) = (\sqrt{x})^2.$$

   Ya que el dominio de $f \circ g$ es $[0, \infty)$, tenemos que $(\sqrt{x})^2) = x$. El dominio de $f \circ g$ **no puede ser** $\mathbb{R}$, porque al tomar un x negativo en $\mathbb{R}$, digamos $x = -1$, tenemos que $\sqrt{-1} \notin \mathbb{R}$.

   Para que la composición $g \circ f$ exista, debe pasar que $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$. ¿Cuál es la imagen de la función f? Tenemos que $\mathrm{Im}(f) = [0, \infty)$,

[11] Me parece que no se ha establecido una convención sobre si $g \circ f$ se lee como «la composición de f con g», «la composición de g con f», «la composición de f y g» o «la composición de g y f; por ello, prefiero denotarlo tal cual se lee con símbolos, para evitar confusiones.

que ciertamente es subconjunto del dominio de g, que $[0, \infty)$ (en este caso, $\text{Im}(f) = \text{Dom}(g)$. Por lo tanto, la composición sí está definida y tenemos que

$$g \circ f \colon \mathbb{R} \to \mathbb{R}$$

y

$$(g \circ f)(x) = g(f(x)) = g(x^2) = \sqrt{x^2}.$$

Esta función no es otra que el valor absoluto, es decir, $\sqrt{x^2} = |x|$.

4.4.1 Propiedades de la composición de funciones

Teorema 15. *Consideremos dos funciones biyectivas $f \colon A \to B$ y $g \colon B \to C$. La composición $g \circ f$ es biyectiva.*

Demostración. Debemos probar que $g \circ f$ es tanto inyectiva (enunciados 4.1 o 4.2) como suprayectiva (enunciado 4.3). Sabemos que tanto g como f son inyectivas y suprayectivas. Probaremos que

$$\forall x_1 \forall x_2 (x_1 \neq x_2 \Rightarrow (g \circ f)(x_1) \neq (g \circ f)(x_2)).$$

Recordemos que el dominio de $g \circ f$ es A y su contradominio es C. Consideremos x_1, $x_2 \in A$ tal que $x_1 \neq x_2$. Ya que f es una función inyectiva, se sigue que $f(x_1) \neq f(x_2)$. Notemos que $f(x_1)$, $f(x_2 \in \text{Im}(f) \subseteq \text{Dom(g)}$. Como g es una función inyectiva, tenemos que $g(f(x_1)) \neq g(f(x_2))$, que es lo que queríamos probar, ya que es lo mismo que $(g \circ f)(x_1) \neq (g \circ f)(x_2)$ Por lo tanto, $g \circ f$ es una función inyectiva.

Ahora probemos que $g \circ f$ es suprayectiva, es decir, debemos probar que:

$$\forall y \in C \exists x \in A((g \circ f)(x) = y).$$

Tomamos $y \in C$. Ya que g es una función suprayectiva, existe $z \in B$ tal que $g(z) = y$. Como f es una función suprayectiva, existe $x \in A$ tal que $f(x) = z$. Por lo tanto,

$$y = g(z) = g(f(x)) = (g \circ f)(x).$$

Por lo tanto, la composición $g \circ f$ es una función biyectiva. □

Podríamos preguntarnos (al menos, los matemáticos en algún momento lo hacemos), ¿el regreso es verdadero? El regreso dice: dadas dos funciones

$f\colon A \to B$ y $g\colon B \to C$, ¿si $g \circ f$ es biyectiva entonces g y f son funciones biyectivas? Resulta que es falso. Consideremos los conjuntos $A = \{\square, \blacksquare\}$ y $B = \{1, 2, 3\}$ y las funciones $f\colon A \to B$ y $g\colon B \to A$ como están dadas en la figura 10. La composición $g \circ f$ (véase la figura 4.4.1) es igual a la función identidad sobre A, es decir, $g \circ f = 1_A$. Por lo tanto, la composición $g \circ f$ si es biyectiva, pero f no es biyectiva porque no es suprayectiva y g no es biyectiva porque no es inyectiva.

Figura 10: Las funciones $f\colon A \to B$ y $g\colon B \to A$

La composición $g \circ f$ es biyectiva. Si reexaminamos la figura 4.4.1, para que $g \circ f$ sea suprayectiva, necesariamente la función que está a la derecha, g, tiene que ser suprayectiva y para que $g \circ f$ sea inyectiva, necesariamente la función que está a la izquierda, f, tiene que ser inyectiva. Así, tenemos los dos siguientes teoremas.

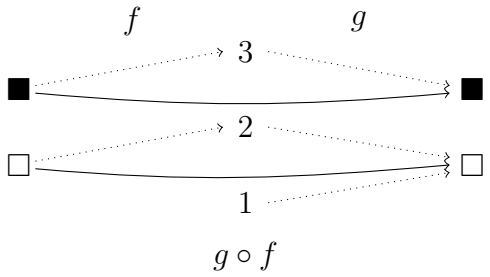


Figura 11: La composición resultante $g \circ f$

Teorema 16. *Sean $f\colon A \to B$ y $g\colon B \to C$ dos funciones. Si $g \circ f$ es suprayectiva entonces g es suprayectiva.*

Teorema 17. *Sean $f\colon A \to B$ y $g\colon B \to C$ dos funciones. Si $g \circ f$ es inyectiva entonces g es inyectiva.*

Prueba del teorema 16. Recordemos que A es el dominio y C es el contradominio de la función $g \circ f$. Por la definición de ser suprayectiva, tenemos que

$$\forall y \in C \exists x \in A((g \circ f)(x) = y)$$

y debemos mostrar que para todo $y \in C$, existe $z \in B$ tal que $g(z) = y$.

Así pues, tomemos $y \in C$. Por hipótesis, existe $x \in A$ tal que $y = (g \circ f)(x) = g(f(x))$. Pero $f(x) \in B$, así, el elemento que buscamos en el dominio de g es $f(x)$. □

La prueba del teorema 17 se deja como ejercicio.

4.5 Funciones inversas

Recordemos la función $h\colon A \to B$ que aparece en la figura 7, donde $A = \{*, \square, \#, \clubsuit\}$, $B = \{\alpha, \beta, \gamma, \delta, \varepsilon\}$, $h = \{(*, \varepsilon), (\square, \beta), (\#, \varepsilon), (\clubsuit, \gamma)\}$ y $h \subseteq A \times B$. ¿Qué pasa si volteamos las parejas de h? Obtendremos el siguiente conjunto de parejas ordenadas

$$h^* = \{(\varepsilon, *), (\beta, \square), (\varepsilon, \#), (\gamma, \clubsuit)\}$$

y tenemos que $h^* \subseteq B \times A$. ¿h^* es una función de B en A? En la figura 12 podemos ver la función h a la izquierda y la relación h^* a la derecha; claramente, h^* no es función. ¿Por qué h^* no es función? Falla en las condiciones

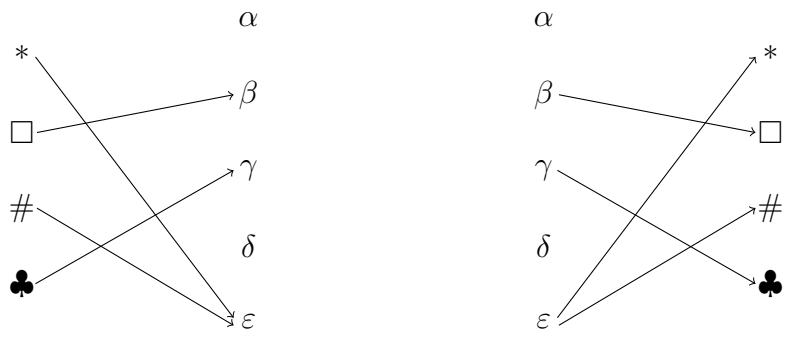


Figura 12: A la izquierda aparece la función h y a la derecha la relación *inversa* h^*

para ser función: hay elementos en B a los que no les corresponde ningún

elemento en A (en concreto, α y δ) y hay elementos en B a los que les corresponde dos elementos en A (al elemento ε le corresponde tanto $*$ como $\#$).

La anterior es una operación sobre las relaciones, si $R \subseteq A \times B$, la *relación inversa* R^{-1} se define como

$$R^{-1} = \{(y, x) \colon (x, y) \in R\}.$$

Como toda función es una relación, siempre podemos pensar en la inversa de una función, pero como explicamos arriba, no siempre es una función. ¿Cuándo sí lo es? Cuando f es una función biyectiva.

Teorema 18. *Si $f \colon A \to B$ es una función biyectiva, entonces $f^{-1} \colon B \to A$ es también una función biyectiva que satisface que*

$$f^{-1} \circ f = 1_A \text{ y } f \circ f^{-1} = 1_B,$$

a la cual llamamos la inversa *de f.*

Demostración. Ya que f es una función de A en B, donde para cada $x \in A$, existe un único $y \in B$ tal que $f(x) = y$ y cada una de las parejas $(x,\ y)$ son los elementos de f. La inversa será

$$f^{-1} = \{(y, x) \colon (x, y) \in f\} = \{(y, x) \colon y = f(x)\}.$$

Es decir, para $y \in B$, $f^{-1}(y) = x$ si y sólo si $f(x) = y$.

Como f es una función, tenemos que para cada $x \in A$, existe un único $y \in B$ tal que $f(x) = y$. Como f es biyectiva, también tenemos que

- si x_1, $x_1 \in A$ tales que $x_1 \neq x_2$ entonces $f(x_1) \neq f(x_2)$ y
- para todo $y \in B$ existe $x \in A$ tal que $f(x) = y$.

Observemos que, para todo $y \in B$, $f^{-1}[\{y\}]$ es un conjunto unitario: hay al menos un elemento porque f es suprayectiva y hay exactamente uno porque f es inyectiva, es decir, $f^{-1}[\{y\}] = \{x\}$.

Debemos probar que f^{-1} es una función biyectiva y se tiene que $f^{-1} \circ f = 1_A$ y $f \circ f^{-1} = 1_B$. Primero probemos que f^{-1} es una función, es decir, que para cada $y \in B$, existe un único $x \in A$ tal que $f^{-1}(y) = x$. ¿Qué x es ése? El único elemento que está en $f^{-1}(y)$, que como argumentamos previamente, es un conjunto unitario; esto asegura que existe y que es único. También debemos mostrar que f^{-1} es inyectiva y suprayectiva. Si no fuese inyectiva, existirían dos y_1, $y_2 \in B$ tales que $f^{-1}(y_1) = f^{-1}(y_1)$ □

4.6 Cardinalidad

La cardinalidad de los conjuntos nos permite dar una idea del tamaño de los conjuntos y compararlos entre sí. En un salón de clases, si quisiéramos saber si hay más estudiantes o bancas o si son del mismo tamaño basta con sentar a todos los estudiantes posibles y echar un ojo: si quedan estudiantes de pie, hay más estudiantes; si quedan bancas vacías, hay más bancas y si no pasa ni lo uno ni lo otro, tienen el mismo tamaño. No tuvimos que efectuar ningún cálculo, porque al sentar a los estudiantes estamos estableciendo una correspondencia entre los estudiantes y las bancas. Decimos que dos conjuntos son *equipotentes* (es decir, que tienen el mismo tamaño) si existe una función biyectiva entre ellos y lo denotamos como $A \approx B$.

Para cada $n \in \mathbb{N}$ (donde $0 \in \mathbb{N}$), definimos:

- si $n = 0$, $\mathcal{I}_0 = \varnothing$ y
- si $n > 0$, $\mathcal{I}_n = \{0, 1, \ldots, n-1\}$.

Así, tenemos que $\mathcal{I}_1 = \{0\}$, $\mathcal{I}_2 = \{0, 1\}$, $\mathcal{I}_3 = \{0, 1, 2\}$, etcétera y observemos que $\mathcal{I}_0$ no tiene elementos, $\mathcal{I}_1$ tiene un elemento, $\mathcal{I}_2$ tiene dos elementos, $\mathcal{I}_3$ tiene tres elementos, etcétera. Si m, $n \in \mathbb{N}$ y $m \leq n$ entonces tenemos que $\mathcal{I}_m \subseteq \mathcal{I}_n$ y si $m < n$ entonces $\mathcal{I}_m \subsetneq \mathcal{I}_n$.

Dado un conjunto A, decimos que A es *finito* si existe un número natural $n \in \mathbb{N}$ tal que $A \approx \mathcal{I}_n$; en otro caso (es decir, cuando para toda $n \in \mathbb{N}$ se tiene que A y $\mathcal{I}_n$ no son equipotentes), decimos que A es *infinito*.

Si A es un conjunto finito, su *cardinalidad* es n si y sólo si $A \approx \mathcal{I}_n$, esto lo denotamos como $|A| = n$. Por ejemplo, tenemos $|\varnothing| = 0$ y $|\{a\}| = 1$. Si $a \neq b$ entonces $|\{a, b\}| = 2$ (observa que si $a = b$ entonces $|\{a, b\}| = 1$).

Como podemos esperar:

Teorema 19. *Dados dos conjuntos A y B, se tiene que A y B tienen la misma cardinalidad si y sólo son equipotentes.*

Demostración. Probaremos sólo la ida. Supongamos que A y B tienen la misma cardinalidad, probaremos que $A \approx B$, es decir, debemos probar que existe una función biyectiva $f\colon A \to B$.

Ya que A y B tienen la misma cardinalidad, significa que existe un número natural n tal que

$$|A| = |B| = n.$$

Así, existen dos funciones biyectivas

$$g_1\colon A \to \mathcal{I}_n \text{ y } g_2\colon B \to \mathcal{I}_n.$$

Como g_2 es una función biyectiva, existe su inversa

$$g_2^{-1}\colon \mathcal{I}_n \to B.$$

Por lo tanto, la composición es una función biyectiva de A en B:

$$g_2^{-1} \circ g_1\colon A \to B$$

y, así, $A \approx B$. □

Los siguientes dos teoremas resultan muy importantes, pero sus demostraciones exceden son un poco más elaboradas (ya sea por medio de una prueba por inducción matemática o por contradicción).

Teorema 20. *Dados dos conjuntos finitos A y B, si $f\colon A \to B$ es una función inyectiva entonces $|A| \leq |B|$.*

Teorema 21. *Dados dos conjuntos finitos A y B, si $f\colon A \to B$ es una función suprayectiva entonces $|A| \geq |B|$.*

La idea del primero de estos dos teoremas es que si una función envía cada elementos del dominio a un elemento diferente en el contradominio, en el contradominio deben haber al menos tantos elementos como en el dominio, es decir, $|A| \leq |B|$. La idea del segundo es que si cada elemento en el contradominio proviene de al menos un elemento en el dominio, entonces el dominio debe tener al menos tanto elementos como el contradominio, es decir, $|A| \geq |B|$.

Así, si $f\colon A \to B$ es una función biyectiva, como es inyectiva tenemos que $|A| \leq |B|$ y como es biyectiva tenemos que $|A| \geq |B|$, por lo tanto $|A| = |B|$.

Ahora analizaremos cómo se comparta la cardinalidad con respecto a la unión de conjuntos. Si A y B son dos conjuntos ajenos (es decir, no tienen elementos en común o $A \cap B = \varnothing$, la cardinalidad de su unión debería de ser igual a la suma de las cardinalidades de cada uno de los conjuntos conjuntos. Y así pasa.

Teorema 22. *Si A y B son dos conjuntos finitos ajenos entonces*

$$|A \cup B| = |A| + |B|.$$

Demostración. Es decir, si $|A| = m$ y $|B| = n$ entonces debemos probar que $|A \cup B| = m+n$. Por hipótesis, sabemos que existen dos funciones biyectivas f_1 y f_2 tales que

$$f_1 \colon A \to \mathcal{I}_m \text{ y } f_2 \colon B \to \mathcal{I}_n.$$

Debemos mostrar que existe una función biyectiva

$$f_3 \colon A \cup B \to \mathcal{I}_{m+n}$$

Tal vez la primera aproximación podría ser definir la función de la siguiente forma:

$$f_3(x) = \begin{cases} f_1(x) & \text{si } x \in A \text{ o} \\ f_2(x) & \text{si } x \in B. \end{cases}$$

Si A o B es vacío, entonces sí funciona; pero si ambos son no vacíos, existirán $a \in A$ y $b \in B$ tales que $f_1(a) = 0$ y $f_2(b) = 0$, y así $f_3(a) = f_3(b)$, por lo que f_3 no sería biyectiva.

Recordemos que $\mathcal{I}_{m+n} = \{0,\ 1,\ \ldots,\ m-1,\ m,\ m+1,\ \ldots,\ m+n-1,\ m+n\}$, en $\{0,\ 1,\ \ldots,\ m-1\}$ hay exactamente m elementos y en $\{m,\ m+1,\ \ldots,\ m+n-1,\ m+n\}$ hay exactamente n elementos, podemos hacer corresponder los primeros a los elementos de A y los segundos, a los de B de la forma siguiente:

$$f_3(x) = \begin{cases} f_1(x) & \text{si } x \in A \text{ o} \\ f_2(x) + m & \text{si } x \in B. \end{cases}$$

Se dejará como ejercicio probar que f_3 efectivamente es una función biyectiva, con lo que tendríamos el resultado. □

Ahora daremos una versión más general del teorema previo al retirar la condición de que los conjuntos sean ajenos. Pero primero, veamos un caso en concreto: supongamos que $A = \{a,\ b,\ c\}$ y $B = \{b,\ c,\ d,\ e\}$. Tenemos que $|A| = 3$ y $|B| = 4$, se sigue que $|A| + |B| = 7$. Por otro lado, $A \cup B = \{a,\ b,\ c,\ d,\ e\}$ y $|A \cup B| = 5$. Claramente, $7 \neq 5$ y, por lo tanto, $|A| + |B| \neq |A \cup B|$. ¿Por qué falla? Los elementos a y b (que están en la intersección) los estamos contando dos veces, una cuando pertenecen a A y otra cuando pertenecen a B. ¿Cómo lo arreglamos? Quitamos una vez la cardinalidad de la intersección.

Pero requeriremos de un resultado previo, que es un corolario del teorema anterior.

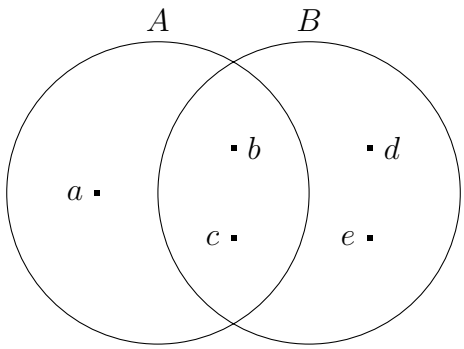


Figura 13: La cardinalidad de la unión de conjuntos

Corolario 23. *Si $B \subseteq A$ entonces $|A \setminus B| = |A| - |B|$.*

Teorema 24. *Para cualesquiera dos conjuntos finitos A y B, se tiene que*

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

Demostración. Para la prueba, usaremos el teorema anterior (el teorema 22). Sin embargo, para ocuparlo necesitamos tener conjuntos ajenos y éste no es necesariamente el caso. Observemos que

$$A = (A \setminus (A \cap B)) \cup (A \cap B) \text{ y } (A \setminus (A \cap B)) \cap (A \cap B) = \varnothing,$$

es decir, $A \setminus (A \cap B)$ y $A \cap B$ son conjuntos ajenos. Análogamente,

$$B = (B \setminus (A \cap B)) \cup (A \cap B) \text{ y } (B \setminus (A \cap B)) \cap (A \cap B) = \varnothing.$$

Por el teorema 22, se sigue que

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

y por el corolario 23, tenemos que

$$|A \setminus (A \cap B)| = |A| - |(A \cap B)|$$
$$|B \setminus (A \cap B)| = |B| - |(A \cap B)|$$

Finalmente, basta con observar que

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

donde los últimos tres conjuntos son mutuamente ajenos. □

5 Propiedades de los números enteros

A partir de los conjuntos es posible construir todos los números. Primero se construyen los naturales.[12] En los números enteros tenemos dos operaciones: la suma ($+$) y el producto ($\cdot$), que tienen las propiedades siguientes.

Teorema 25 (Propiedades de la suma)**.** *Dados (cualesquiera) tres números enteros a, b y c, se cumplen las siguiente propiedades.*

(a) ***Propiedades asociativa:*** $(a+b)+c = a+(b+c)$

(b) ***Propiedades conmutativa:*** $a+b = b+a$

(c) ***Existencia de neutro aditivo:*** $a+0 = 0+a = 0$

(d) ***Existencia del inverso aditivo:*** *Existe $a' \in \mathbb{Z}$ tal que $a+a' = 0$. Al número a' se lo suele denotar como $-a$ y quedaría $a+(-a) = 0$.*

El neutro y el inverso aditivos son únicos, es decir, siempre que tengamos que $a+c = a$, forzosamente $c = 0$, y si $a+b = 0$ entonces $b = -a$.

De lo anterior, la *resta* no es propiamente una operación diferente, sino la suma de un inverso aditivo. Formalmente, $a-b = a+(-b)$.

Teorema 26 (Propiedades del producto)**.** *Dados (cualesquiera) tres números enteros a, b y c, se cumplen las siguiente propiedades.*

(a) ***Propiedades asociativa:*** $(a\cdot b)\cdot c = a\cdot(b\cdot c)$

[12] *La siguiente es sólo una nota cultural, pueden omitirla sin consecuencias.* Es interesante, ya que su construcción es recursiva por medio de la *operación sucesor*, dado un conjunto A, el *sucesor* de A, se denota y define como

$$\sigma(A) = A \cup \{A\}.$$

El número cero corresponde al conjunto vacío, $\varnothing$; el número uno corresponde al sucesor del cero, $\varnothing \cup \{\varnothing\} = \{\varnothing\}$; el número dos corresponde al sucesor del uno, $\{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}$; el número del tres corresponde al sucesor del dos, $\{\varnothing, \{\varnothing\}\} \cup \{\{\varnothing, \{\varnothing\}\}\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, etcétera. Observa que sólo utilizamos operaciones de conjuntos y partimos de un sólo conjunto, el vacío. Este es un tipo de construcciones muy importantes en matemáticas, las construcciones *recursivas*. Con base en esto, se pueden definir formalmente las operaciones usuales de suma y producto.

A partir de los naturales, se pueden definir los números enteros como parejas de números naturales y también se pueden definir las operaciones en los números enteros a partir de las operaciones en los números naturales.

(b) ***Propiedades conmutativa:*** $a \cdot b = b \cdot a$

(c) ***Existencia de neutro multiplicativo:*** $a \cdot 1 = 1 \cdot a = a$

(d) ***Distributividad del producto sobre la suma:*** $a \cdot (b+c) = a \cdot b + a \cdot c$

El neutro multiplicativo es único, es decir, siempre que $a \cdot b = a$ *entonces* $b = 1$.

Teorema 27 (Ley de la cancelación para la suma)**.** *Si* a*,* b *y* c *son tres números enteros tales que* $a + c = b + c$ *entonces* $a = b$*. Análogamente, si tenemos que* $c + a = c + b$.

Demostración. Simplemente sumamos de ambos lados el inverso aditivo de c, así tenemos que

$$\begin{aligned} a + c &= b + c \\ (a + c) + (-c) &= (b + c) + (-c) \\ a + (c + (-c)) &= b + (c + (-c)) \\ a + 0 &= b + 0 \\ a &= b. \end{aligned}$$

□

Proposición 28. *Dado un número entero* a*, el inverso aditivo del inverso aditivo de* a *es igual a* a*, es decir,* $-(-a) = a$.

Lo anterior nos podría parecer 'evidente', sin embargo no lo es.

Demostración. Sabemos que $a + (-a) = 0$ y $(-a) + (-(-a)) = 0$, así:

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

□

Proposición 29. *Dado cualquier número entero a, se tiene que $a \cdot 0 = 0 \cdot a = 0$.*

Demostración. Ya que el producto es conmutativo, basta con probar que $a \cdot 0 = 0$. Tenemos que $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Por lo tanto, $a \cdot 0 = a \cdot 0 + a \cdot 0$, sumando de ambos lados el inverso aditivo de $a \cdot 0$, llegamos a que $0 = a \cdot 0$. □

Teorema 30. *Si a y b son dos números enteros tales que $a \cdot b = 0$ entonces $a = 0$ o $b = 0$.*

Para probar este resultado se necesita de una técnica de demostración que aún no hemos visto: la demostración por inducción matemática.

Teorema 31 (Ley de la cancelación para el producto)**.** *Si a, b y c son tres números enteros tales que $c \neq 0$ y $a \cdot c = b \cdot c$ entonces $a = b$. Análogamente, si tenemos que $c \cdot a = c \cdot b$.*

En el caso de los números enteros, no disponemos del inverso multiplicativo, ya que por lo general éste no es un número entero. Por ejemplo, el inverso multiplicativo del 2 sería $^1/_2$, pero $^1/_2$ no es un número entero.

Demostración.

$$\begin{aligned} a \cdot c &= b \cdot c \\ a \cdot c + (-(b \cdot c)) &= b \cdot c + (-(b \cdot c)) \\ a \cdot c - b \cdot c &= 0 \\ (a - b) \cdot c &= 0. \end{aligned}$$

Partimos de la igualdad que tenemos como hipótesis. Al sumar lo mismo de ambos lados, seguimos teniendo una igualdad, pero elegimos sumar el inverso aditivo de $b \cdot c$ y, por lo tanto, nos quedará un cero a la derecha (en el tercer renglón). Por el teorema 30, tenemos que $a - b = 0$ o $c = 0$. Por hipótesis, la última igualdad es falsa, se sigue que $a - b = 0$. Al sumar b de ambos lados, obtenemos que $a = b$. □

Ahora le daremos un orden a los números enteros. Como ya vimos previamente, un orden es un tipo particular de relación. Dados dos números enteros a y b, diremos que a *es menor que* b (y lo denotaremos como $a < b$)

si existe un número natural r, diferente del cero, tal que $a + r = b$, también se lo llama *menor estricto*. Si lo pensamos en la recta numérica, simplemente estamos diciendo que el número a está a la izquierda de b. Decimos que a *es menor que o igual a* b (y lo denotamos por $a \leq b$) si $a < b$ o $a = b$. Al conjunto junto con el orden también se lo llama *orden*; en los números enteros, tenemos los órdenes $(\mathbb{Z}, <)$ y $(\mathbb{Z}, \leq)$.

Para dos números enteros a y b, las expresiones $a > b$ y $a \geq b$ significan, respectivamente, $b < a$ y $b \leq a$. La expresión $a \not< b$ se lee «a no es menor que b» y eso significa que $a \geq b$. Análogalmente, la expresión $a \not\leq b$ se lee «a no es menor que o igual a b» y eso significa que $a > b$.

Teorema 32. *Los números enteros con el orden menor estricto, es decir,* $(\mathbb{Z}, <)$*, es un* orden parcial*, esto quiere decir que es una relación* irreflexiva

$$\forall x(x \not< x)$$

y es transitiva

$$\forall x \forall y \forall z((x < y \wedge y < z) \Rightarrow x < z)$$

Recordemos que la fórmula $\forall x(x \not< x)$ se lee «para todo x en $\mathbb{Z}$, se tiene que $x \not< x$» y la fórmula $\forall x \forall y \forall z((x < y \wedge y < z) \Rightarrow x < z)$ se lee «para cualesquiera enteros x, y y z en $\mathbb{Z}$, si $x < y$ y $y < z$ entonces se tiene que $x < z$».

Demostración. Para la irreflexividad, procedamos por contradicción. Supongamos que no es cierto que $\forall x(x \not< x)$, es decir, $\exists x(x < x)$. Por la definición de «menor que», se sigue existe un número natural r, diferente de cero, tal que $x + r = x$; sin embargo, esto implica que $r = 0$, lo que es una contradicción.

Para la transitividad, ya que $x < y$ y $y < z$, por definición existen dos números naturales, diferentes del cero, r_1 y r_2 tales que

$$\begin{aligned} x + r_1 &= y \\ y + r_2 &= z. \end{aligned}$$

Despejamos y de la segunda ecuación y la substituimos en la primera,

$$\begin{aligned} x + r_1 &= z + (-r_2) \\ x + (r_1 + r_2) &= z. \end{aligned}$$

Ya que r_1 y r_2 son números naturales diferentes de cero, $r_1 + r_2$ es un número natural diferente de cero y, por la definición de «menor que», se sigue que

$$x < z.$$

□

Teorema 33 (Propiedades del orden)**.** *(a) Dados tres números enteros a, b y c, si $a < b$ y $c > 0$ entonces $a \cdot c < b \cdot c$.*

(b) Dados tres números enteros a, b y c, si $a < b$ y $c < 0$ entonces $a \cdot c > b \cdot c$.

Demostración. **Inciso (a).** Ya que $a < b$, existe un número natural r tal que $a + r = b$. Al multiplicar ambos términos por c y aplicar la ley distributiva, se sigue que $a \cdot c + r \cdot c = b \cdot c$.

□

6 Divisibilidad

Ahora estudiaremos una relación muy importante sobre los números enteros: la divisibilidad. Dados dos números enteros a y b, decimos que a *divide a* b si y sólo si existe un entero k tal que

$$b = a \cdot k.$$

Lo denotamos por $a \mid b$. Los siguiente enunciados son formas equivalentes de decir $a \mid b$:

- a divide a b,
- a es divisor de b,
- a es factor de b,
- b es divisible entre a y
- b es múltiplo de a.

En caso de que a **no divida** a b (es decir, que *para todo*[13] entero k, siempre pasa que $b \neq a \cdot k$), lo denotamos por $a \nmid b$.

[13]Recuerda que, cuando negamos una proposición con un cuantificador existencial, obtenemos una proposición con un cuantificador universal y en la definición de divisibilidad aparece un cuantificador existencial.

Ejemplos

1. $3 \mid 12$, ya que para $k = 4$, tenemos que $12 = 3 \cdot 4$.
2. $5 \mid -35$, ya que para $k = -7$, tenemos que $-35 = 5 \cdot (-7)$.
3. $1 \mid -1$, ya que para $k = -1$, tenemos que $-1 = 1 \cdot (-1)$.
4. $-1 \mid 1$, ya que para $k = -1$, tenemos que $1 = (-1) \cdot (-1) = 1$.
5. $7 \mid 0$, ya que para $k = 0$, tenemos que $0 = 7 \cdot 0$.
6. $5 \nmid 7$, ya que para todo entero k, tenemos que $1 \cdot k \neq 7$.

Es muy importante observar que $a \mid b$ y a/b representan cosas completamente diferentes. La primera es una **relación** (puede ser que sea verdadera o falsa) y la segunda es una **operación** que nos arroja un valor. Por ejemplo, $0 \mid 0$ es verdadera, ya que para cualquier número entero k, se tiene que $0 = 0 \cdot k$ y, por otro lado, $0/0$ no está definido.

6.1 Propiedades de la divisibilidad

Teorema 34. *Consideremos tres números enteros a, b y c, se satisfacen las propiedades siguientes.*

(a) $a \mid a$ *(a esta propiedad se la conoce como* reflexividad*). En particular,* $0 \mid 0$.

(b) $a \mid 0$ *(todo número es divisor de cero).*

(c) Si $a \mid b$ *entonces también se tiene que* $a \mid -b$, $-a \mid b$ *y* $-a \mid -b$.

(d) $1 \mid a$ *y* $-1 \mid a$ *(el* 1 *y el* -1 *son divisores de cualquier número).*

(e) Si $0 \mid a$ *entonces* $a = 0$ *(el único número que tiene como divisor al cero es el cero).*

(f) Si $a \mid b$ *y* $b \mid c$ *entonces* $a \mid c$ *(a esta propiedad se la conoce como* transitividad*).*

(g) Si $a \mid b$ *entonces* $a \mid b \cdot c$.

(h) Si $a \mid b$ *entonces* $a \cdot c \mid b \cdot c$.

(i) Si $a \mid b$ *y* $a \mid c$ *entonces* $a \mid b + c$.

(j) Si $a \mid b$ y $a \mid c$ entonces $a \mid x \cdot b + y \cdot c$, para cualesquiera enteros x y y.

Demostración. (a) Para $k = 1$, tenemos que $a = a \cdot 1$. En particular, $0 = 0 \cdot 1$.

(b) Para $k = 0$, tenemos que $0 = a \cdot 0$.

(c) Sabemos que $a \mid b$, es decir, existe un entero k tal que $b = ak$.

- Para $a \mid -b$, si tomamos $k_1 = -k$, tenemos que $a \cdot k_1 = a \cdot (-k) = -(a \cdot k) = -b$.
- Para $-a \mid b$, si tomamos $k_2 = -k$, tenemos que $(-a) \cdot k_2 = (-a) \cdot (-k) = a \cdot k = b$.
- Para $-a \mid -b$, si tomamos $k_3 = k$, tenemos que $(-a) \cdot k_3 = (-a) \cdot k = -(a \cdot k) = -b$.

(d) Con $k = a$, $a = 1 \cdot k$ y con $k = -a$, $a = (-1) \cdot k$.

(e) Supongamos que $a \mid 0$; es decir, existe un número entero k tal que $0 = a \cdot k$. □

Teorema 35. *La divisibilidad satisface las propiedades siguientes.*

(a) Es una relación reflexiva, es decir, para todo número entero a, se tiene que $a \mid a$.

(b) Es una relación transitiva, es decir, para cualesquiera tres números enteros a, b y c, si $a \mid b$ y $b \mid c$ entonces $a \mid c$.

(c) Para todo número entero a, se tiene que $a \mid 0$. En particular, $0 \mid 0$.

(d) Para todo número entero a, se tiene que $1 \mid a$.

(e) Si a es un entero tal que $0 \mid a$ entonces $a = 0$.

(f) Dados dos enteros a y b, si $a \mid b$ entonces también se tiene que $-a \mid b$, $a \mid -b$ y $-a \mid -b$.

(g) Para dos números enteros a y b, si $a \mid b$ y $b \mid a$ entonces $|a| = |b|$.

Con $k = a$, tenemos que $a = 1 \cdot a$ y con $k = -a$, tenemos que $a = (-1) \cdot (-a) = 1 \cdot a$.

Demostración. **Inciso (a).** Para $r = 1$ tenemos que $a \cdot 1 = a$ y con $r' = -1$ tenemos $a \cdot (-1) = -a$.

Inciso (b). Ya que $a \mid b$ y $b \mid c$, existen dos números enteros r_1 y r_2 tales que

$$a \cdot r_1 = b$$
$$b \cdot r_2 = c$$

Al substituir, obtenemos que

$$(a \cdot r_1) \cdot r_2 = a \cdot (r_1 \cdot r_2) = c,$$

pero sabemos que $r_1 \cdot r_2$ es un entero. Por lo tanto, $a \mid c$.

Inciso (e). Si $a \mid b$ entonces existe un número entero r tal que $a \cdot r = b$. Basta con cambiar adecuadamente el signo de r para obtener las tres igualdades que muestran que $-a \mid b$, $a \mid -b$ y $-a \mid -b$.

Inciso (d). Ya que $a \mid b$ y $b \mid a$, existen dos números enteros r_1 y $r_2$tales que

$$a \cdot r_1 = b \text{ y } b \cdot r_2 = a.$$

Al substituir una ecuación en la otra, obtendremos

$$(a \cdot r_1) \cdot r_2 = a$$
$$a \cdot (r_1 \cdot r_2) = a.$$

Por la unicidad del neutro multiplicativo (teorema 26), tenemos que $r_1 \cdot r_2 = 1$. □

7 Algoritmo de la división

¿Cuántas veces cabe el dos en el número siete? Pensémoslo en la recta real, así tendríamos en principio la figura 14. Al menos, cabe un dos dentro de siete, véase la figura 15. Y podemos repetir dos veces más el mismo procedimiento, como se muestra en la figura 16.

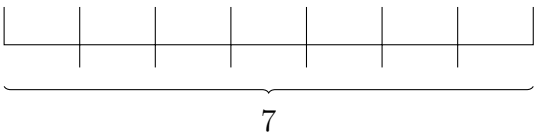


Figura 14: Siete en la recta real

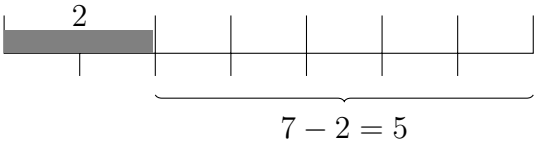


Figura 15: $7 - 2$ en la recta real

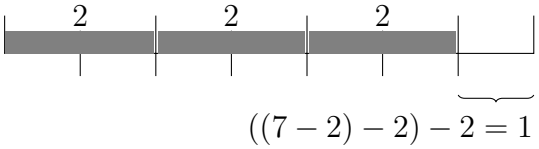


Figura 16: $((7 - 2) - 2) - 2$ en la recta real

7.1 Principio del Buen Orden

Recordemos que el conjunto de los números naturales $\mathbb{N}$ (en nuestro caso, el cero sí es un número natural) está ordenado, es decir, para cualesquiera dos números naturales n y m sólo pueda darse uno de los siguientes:

$$n < m \text{ o } n > m \text{ o } n = m.$$

Así, si tomamos un conjunto de números naturales, por ejemplo $A = \{978, 5, 34, 121\}$ o $B = \{x\colon x \text{ es un número impar}\}$, existe un elemento que es **menor que o igual a** a todos los elementos del conjunto. En el caso del conjunto A, el elemento menor es 5 y en el caso del conjunto B, el elemento menor es 1.

Definición 36. Consideremos un conjunto ordenado A. Dado un subconjunto X de A, si existe un elemento $a \in X$ que satisface que

$$\text{para todo } x \in X \text{ se tiene que } a \leq x,$$

decimos que a es un *mínimo* o *primer elemento* de X y se lo denota por $\text{mín}(X)$.

No todo subconjunto de un conjunto ordenado tiene un primer elemento. Por ejemplo, sí existe mín($\mathbb{N}$), pero no mín($\mathbb{Z}$), mín($\varnothing$) o mín($\{\frac{1}{n}\colon n \in \mathbb{N} \setminus \{0\}\}$). Aunque es un enunciado que pudiera parecer bastante evidente, en matemáticas no lo es (por motivos que exceden el presente texto); es por esto que tenemos el siguiente principio (el cual no se puede probar, es algo que tomamos por cierto).

Principio 37 (Principio del Buen Orden)**.** *Todo conjunto no-vacío de números naturales posee un primer elemento.*

Teorema 38 (Teorema del cociente/residuo)**.** *Dados dos números enteros a y d, donde d es positivo, existen dos únicos enteros q y r que satisfacen que*

$$a = qd + r \quad y \quad 0 \leq r < d, \tag{7.1}$$

donde q es el cociente *de a entre d y r es el* residuo *de a entre d.*

Que los números q y r sean **únicos** significa que si existen (otros) dos números q' y r' que satisfacen lo mismo, es decir, que

$$a = q'd + r' \quad \text{y} \quad 0 \leq r' < d,$$

entonces son los que ya teníamos, es decir,

$$r' = r \quad \text{y} \quad q' = q.$$

Demostración. Por el momento, sólo probaremos la existencia. Dados dos enteros a y d, donde d es positivo, demostraremos que existen dos enteros q y r tales que $a = qd + r$ y $0 \leq r \leq d$. Si $a = 0$, entonces para $q = r = 0$ tenemos que $0 = 0 \cdot d + 0$. Así pues, podemos suponer que $a \neq 0$. Ahora, consideraremos el conjunto

$$S = \{a - td\colon t \in \mathbb{Z} \text{ y } a - td \geq 0\}.$$

Probaremos que S es un conjunto no-vacío, para ello hay que exhibir algún elemento que pertenezca a S y consideraremos dos casos, dependiendo de si a es positivo o negativo.

Caso 1. a es positivo. Para $t = 0$, tenemos que $a - td = a - 0 \cdot d = a$ y como $a > 0$, se sigue que $a \in S$.

Caso 2. a es negativo. Para $t = a$, tenemos que $a - td = a - ad = a(1 - d)$ y como d es positivo, tenemos que $1 - d \leq 0$; se sigue que $a(1 - d) \geq 0$. Por lo tanto, $a(1 - d) \in S$.

Por lo tanto, S es un conjunto diferente del vacío y cuyos elementos son números naturales. Por el principio del Buen Orden, S tiene un primer elemento, sea $a - t_0 d$ el primer elemento de S, para algún $t_0 \in \mathbb{Z}$. Probaremos que $q = t_0$ y $r = a - t_0 d$ son los valores que buscamos. Al substituir, tenemos que

$$\begin{aligned} a &= qd + r \\ &= t_0 d + a - t_0 d \\ &= a. \end{aligned}$$

Ahora, nos falta probar que $0 \geq a - t_0 d < d$. La primera desigualdad se sigue por la forma en cómo definimos S (es conjunto de números no-negativos) y la segunda la probaremos por contradicción, es decir, supondremos que no es cierto: $a - t_0 d \geq d$. Pero entonces tendríamos que:

$$a - (t_0 - 1)d \geq 0,$$

y para $q' = t_0 - 1$ y $r' = a - (t_0 - 1)d$ se cumple la primera de las condiciones 7.1. En particular, tenemos que $a - (t_0 - 1)d \in S$. Pero resulta que $a - (t_0 - 1)d$ **es menor que** $a - t_0 d$, lo que es una contradicción porque escogimos $a - t_0 d$ como el menor elemento de S. Se sigue lo que queríamos probar, que

$$0 \leq a - t_0 d < 0.$$

□

7.2 Números primos

Un número entero p, con $p > 1$, es *primo* si sus únicos divisores positivos son él mismo y el uno. Consideremos un número entero n que no sea primo, eso significa que existe un entero d mayor que uno y menor que n (es decir, $1 < d < n$) tal que $d \mid n$. De la definición de divisibilidad, existe un número entero k tal que $n = dk$. Notemos que $d \neq 1$ y $d \neq n$, por lo tanto, $1 < k < n$. Así, si n no es primo entonces

$$n = dk,$$

con $1 < d, k < n$. Por esto, a los números primos se los suele llamar *compuestos*. Más aún, tenemos que:

Proposición 39. *Dado un número entero n mayor que uno, si n no es primo entonces existen dos enteros d y k tales que*

$$1 < d, k < n \quad y \quad n = dk.$$

Teorema 40. *Todo número entero mayor que uno tiene un divisor primo.*

El teorema anterior dice que para todo números entero n, con $n > 1$, existe un número primo tal que $p \mid n$. En algunos casos es claro, por ejemplo, para 2, 3 u 11, ya que todo número divide a sí mismo, ellos mismos son el número primo que buscamos. Si n no es primo, entonces, por la proposición 39, existen dos enteros d y k tales que $1 < d, k < n$ y $n = dk$. Si d es primo, ya terminamos, pues $d \mid n$. En otro caso, volvemos a descomponer d y repetimos el proceso.

Demostración. Sea n un número entero mayor que uno. Tenemos dos posibilidades: n es o no es primo. Si n es primo, entonces n es un divisor primo de n, con lo que habremos termino. Así pues, supongamos que n no es primo. Por la proposición 39, existen dos enteros d_1 y k_1 tales que

$$n = d_1 k_1 \quad \text{y} \quad 1 < d_1, k_1 < n.$$

De nuevo, tenemos dos posibilidades: d_1 es o no primo. Si d_1 es primo, ya terminamos porque $d_1 \mid n$ y, por lo tanto, d_1 es un divisor primo de n. En otro caso, tendríamos que d_1 es compuesto. Así, existen dos enteros d_2 y k_2 tales que

$$d_1 = d_2 k_2 \quad \text{y} \quad 1 < d_2, k_2 < d_1.$$

Otra vez, tenemos dos posibilidades: d_2 es o no primo. Si d_2 es primo, tenemos que $d_2 \mid d_1$ y ya sabíamos que $d_1 \mid n$, por lo tanto (por el teorema 35), tenemos que $d_2 \mid n$, es decir, d_2 es un divisor primo de n. En otro caso, d_2 es compuesto y repetimos el procedimiento. De esta forma, obtendremos un conjunto de enteros $d_1, d_2, \ldots, d_{r-1}, d_r$ tales que

$$0 < d_r < d_{r-1} < \cdots < d_2 < d_1 < n,$$

para algún entero positivo r.

□