MATEMÁTICA DISCRETA Y LÓGICA

Juan Diego Barrado Daganzo
1º de Carrera

3 de julio de 2021

LÓGICA ELEMENTAL

PROPOSICIONES

Las proposiciones son oraciones de sentido inequívoco que pueden ser ciertas o falsas. Usaremos habitualmente letras para referirnos a ellas: A, B, C, ...

- **Proposiciones compuestas**: solo pueden determinarse su veracidad por contraste con el mundo real
- **Proposiciones atómicas**:formadas por las anteriores, su veracidad se puede determinar a partir de la combinación de las de las proposiciones atómicas que las componen.

Operaciones con proposiciones

Negación

La proposición A puede ser falsa o verdadera, pero $\neg A$ siempre será lo contrario de lo que sea A.

A	$\neg A$
V	F
F	V

Conjunción

Es la ocurrencia de ambas proposiciones de forma simultánea, es decir, que ocurre tanto P como Q.

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

Disyunción

Es la ocurrencia de una, otra o ambas proposiciones de forma simultánea, es decir, que ocurre o P, o Q o tanto P como Q.

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

Implicación

Se suele expresar como si P, entonces Q o P implica Q. En este tipo de operaciones decimos que P es la hipótesis o premisa y Q la tesis o consecuencia[1].

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

Recíproco de implicación

Es la otra relación posible entre A y B y no es lo mismo puesto que las tablas de verdad son distintas.

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

Ej.: "Si un número es entero, entonces es racional". Ser racional es una condición necesaria para poder ser entero.

Equivalencia

"P es equivalente a Q" quiere decir que: $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. Se suele decir: "P si y solo si Q" o "P es necesario y suficiente". De este modo, P y Q vienen a decir lo mismo o a expresar lo mismo.

Q	P	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
F	F	V	V	V
F	V	F	V	F
V	F	V	F	F
V	V	V	V	V

Ej.: "Un número es par si y solo si es divisible por 2"

[1] ¡¡¡Terminología importante!!! Decimos que P es condición suficiente para Q (basta que se cumpla P para concluir Q) y también, decimos que Q es condición necesaria para P puesto que para que $P \Rightarrow Q$ sea cierto, ha de cumplirse necesariamente Q cuando P es cierto (cuando $P \Rightarrow Q$ es cierto y Q es falso, también P debe ser falso).

Tautologías

Una tautología es una proposición o afirmación que es cierta para cualquier caso que se plantee. Para afianzar el concepto veamos unos ejemplos:

$$\neg(\neg A) \Leftrightarrow A$$

A	$\neg A$	$\neg(\neg A)$	$\neg(\neg A) \Leftrightarrow A$
F	V	F	V
V	F	V	V

$$(A \Rightarrow B) \Leftrightarrow \neg(A \wedge \neg B)$$

A	B	$\neg B)$	$\neg(A \wedge \neg B)$	$A \Rightarrow B$	$(A \Rightarrow B) \Leftrightarrow \neg(A \wedge \neg B)$
F	F	V	V	V	V
F	V	F	V	V	V
V	F	V	F	F	V
V	V	F	V	V	V

Contraposición

La contraposición es una tautología que establece una equivalencia entre una implicación ya dada y su contrapuesta:

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$$

P : "$x > 3$"
Q : "$x > 2$"
$P \Rightarrow Q$: "$Six > 3, entoncesx > 2$"
$\neg Q \Rightarrow \neg P$: "$Six < 2, entoncesx < 3$"

LÓGICA DE PREDICADOS

Con frecuencia nuestros enunciados y razonamientos cotidianos aluden a elementos o individuos de un colectivo, pero la Lógica Proposicional no recoge propiedades sobre individuos ni generalidades ni relaciones entre individuos para poder formalizarlos adecuadamente.

Por ejemplo:

- "x es par",
- "Algunos mamíferos leen"
- "Todos los que leen disfrutan"

Es necesario extender la Lógica Proposicional con nuevos elementos, dando lugar a un nuevo lenguaje formal más adecuado para las matemáticas, el lenguaje de la **Lógica de Primer Orden o Lógica de Predicados (LPO)**, se compone de:

- **Dominio o universo de discurso**: colectivo de individuos sobre los que hablamos.

  Ej.: "x es par", su dominio podría ser N

- **Constantes**: nombres propios referidos a individuos.

  Ej.: 8, María, Juan.

- **Variables**: Denotan valores cualesquiera del dominio. Representan individuos anónimos, generales.

  Ej.: x, y, ...

- **Predicados**: Enunciados sobre individuos. Pueden expresar propiedades de un individuo.

  Ej.: $P(x) \equiv x$ es par, $M(y) \equiv y$ es mamífero

  También pueden expresar relaciones entre individuos.

  Ej.: $H(x, y) \equiv x$ e y son hermanos

- **Funciones**: Descripción de un individuo en función de otro o de otros.

  Ej.: $x + y, 3y, f(x) \ldots$.

Leyes de equivalencia

Dos proposiciones distintas w_1 y w_2 son equivalentes cuando sus valores de verdad son iguales en las mismas situaciones, es decir, las tablas de verdad son iguales.

Elemento neutro

$$(w_1 \wedge V) \equiv w_1$$

$$(w_1 \vee F) \equiv w_1$$

Leyes de dominación

$$(w_1 \vee V) \equiv V$$

$$(w_1 \wedge F) \equiv F$$

Ley de absorción

$$(w_1 \vee (w_1 \wedge w_2)) \equiv w_1$$

$$(w_1 \wedge (w_1 \vee w_2)) \equiv w_1$$

Ley de Idempotencia

$$(w_1 \vee w_1) \equiv (w_1 \wedge w_1) \equiv V$$

Doble negación

$$\neg\neg w_1 \equiv w_1$$

Ley de contradicción

$$(w_1 \wedge \neg w_1) \equiv F$$

Leyes de De Morgan

$$\neg(w_1 \vee w_2) \equiv \neg w_1 \wedge \neg w_2$$

$$\neg(w_1 \wedge w_2) \equiv \neg w_1 \vee \neg w_2$$

Ley del medio excluido

$$(w_1 \vee \neg w_1) \equiv V$$

Conmutatividad

$$w_1 \vee w_2 \equiv w_2 \vee w_1$$
$$w_1 \wedge w_2 \equiv w_2 \wedge w_1$$

Leyes distributivas

$$w_1 \vee (w_2 \wedge w_3) \equiv (w_1 \vee w_2) \wedge (w_1 \vee w_3)$$
$$w_1 \wedge (w_2 \vee w_3) \equiv (w_1 \wedge w_2) \vee (w_1 \wedge w_3)$$

Leyes asociativas

$$w_1 \vee w_2 \vee w_3 \equiv (w_1 \vee w_2) \vee w_3 \equiv w_1 \vee (w_2 \vee w_3)$$
$$w_1 \wedge w_2 \wedge w_3 \equiv (w_1 \wedge w_2) \wedge w_3 \equiv w_1 \wedge (w_2 \wedge w_3)$$

Contraposición

$$w_1 \Rightarrow w_2 \equiv \neg w_2 \Rightarrow \neg w_1$$

Definición de condicional

$$w_1 \Rightarrow w_2 \equiv \neg w_1 \vee w_2$$

Definición de equivalencia

$$w_1 \Leftrightarrow w_2 \equiv (w_1 \Rightarrow w_2) \wedge (w_2 \Rightarrow w_1)$$

Cuantificadores

Los cuantificadores: *existe*[2] y *para todo*[3], se refieren a una propiedad relativa a un objeto x o a todos los objetos de un cierto grupo.

Cuando queremos decir que existe un objeto x que cumple una cierta propiedad o proposición, escribimos:

$$\exists x : P(x)$$

(*)[4]

$$\text{Ej.: } \exists x \in \mathbb{R} : (x > 0) \wedge (\forall y \in \mathbb{N} : x \neq y)$$

Cuando queremos decir que todos los objetos de un cierto grupo tienen la propiedad $P(x)$:

$$\forall x : P(x)$$

$$\text{Ej.: } \forall x \in \mathbb{R} : x^2 \geq 0 \Rightarrow P(x)$$

Para referirse a que existe un ÚNICO x que cumpla cierta proposición se utiliza el símbolo: $\exists!$, que se puede definir como:

$$\exists! x : P(x) \Rightarrow \exists x : P(x) \wedge [\forall y : P(y) \Rightarrow y = x]$$

Para negar una proposición con cuantificadores, negamos todas sus partes:

$$\neg(\forall y : P(x)) \Leftrightarrow \exists x : \neg P(x)$$

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

Con varios cuantificadores y variables:

$$\neg(\forall x \exists y : P(x, y)) \Leftrightarrow \exists x \forall y : \neg P(x, y)$$

En general, los cuantificadores no conmutan:

$$\forall x \in D : (\exists y \in D : P(x)) \neq \exists y \in D : (\forall x \in D : P(x, y))$$

[2] Tras un existe se suele poner una CONJUNCIÓN.
[3] Después de un *para todo* SE DEBE ESCRIBIR UN PREDICADO (implicaciones, equivalencias...).
[4] Los dos puntos: significan *Tal que*.

MÉTODOS DE DEMOSTRACIÓN

Una **demostración matemática** es una argumentación lógica que establece la verdad de una proposición matemática.

Un **sistema matemático** es tanto los hechos matemáticos de los que partes como los procesos de deducción que dan nuevos hechos matemáticos en un cierto campo de las matemáticas. Los sistemas matemáticos están formados por:

- **Axiomas**: proposiciones matemáticas siempre ciertas
- **Definiciones**: permiten crear nuevos conceptos en base a los ya existentes
- **Términos primitivos**: definidos mediante acuerdos o postulados
- **Teoremas**: proposiciones matemáticas para las que se ha demostrado que son verdaderas
- **Lemas**: teoremas pequeños para demostrar un teorema posterior
- **Corolarios**: teoremas consecuencia de otros

La argumentación lógica es válida si la veracidad de las premisas de las que se parte conlleva necesariamente a la veracidad de la conclusión que se pretende demostrar, es decir, si no podemos concebir un escenario donde las premisas sean verdaderas y las conclusiones falsas.

$$\begin{cases} \varphi_1 \\ \varphi_2 \\ ... \\ \varphi_n \end{cases} \vdash \psi$$

Si una argumentación es válida, se dice que la conclusión se deduce lógicamente de las premisas, es decir, la proposición $\varphi_1 \wedge \varphi_2 \wedge ... \wedge \varphi_n \Rightarrow \psi$ debe ser verdadera y se denota como:

$$\{\varphi_1, \varphi_2, ..., \varphi_n\} \models \psi$$

Reglas de inferencia

Son las reglas empleadas en la argumentación, son válidas sencillas y permiten desarrollar la argumentación mediante su aplicación.

Modus Ponens

$$\{A \Rightarrow B, A\} \vdash B$$

Silogismo Disyuntivo

$$\{A \vee B, \neg B\} \vdash A$$

Modus Tollens

$$\{A \Rightarrow B, \neg B\} \vdash \neg A$$

Conjunción

$$\{A, B\} \vdash A \wedge B$$

Simplificación

$$\{A \wedge B\} \vdash A$$

Adición

$$\{A\} \vdash A \vee B$$

Demostración por casos

$$\{A \Rightarrow C, B \Rightarrow C\} \vdash (A \vee B) \Rightarrow C$$

Silogismo Hipotético

$$\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C$$

Para las proposiciones con cuantificadores y en el ámbito del manejo de los mismos en la lógica:

Particularización universal

Si $\forall x \in D : P(x)$ es cierto, entonces $P(a)$ también es cierto siendo a un elemento concreto de D

Particularización existencial

Si $\exists x \in D : P(x)$ es cierto, entonces es cierto que $\exists a \in D : P(a)$ siendo a un elemento concreto

Generalización universal

Si $P(x)$ se satisface para un x arbitrario, entonces $\forall x \in D : P(x)$

Generalización existencial

Si $P(x)$ se satisface para un x concreto de D, entonces $\exists x \in D : P(x)$

Demostración directa

Basada en la tautología Modus ponens:

$$[P \wedge (P \Rightarrow Q)] \Rightarrow Q$$

Lo que se puede traducir en:

$$[P \wedge (P \Rightarrow R)] \wedge (R \Rightarrow T) \wedge ... \wedge (... \Rightarrow Q)] \Rightarrow Q$$

Ej.: "El cociente de números racionales es racional"

$$a, b \in \mathbb{Q} \Rightarrow a = \frac{m}{n}, b = \frac{k}{l} : m, n, k, l \in \mathbb{Z} \wedge n, l \neq 0$$

$$\frac{a}{b} = \frac{\frac{m}{n}}{\frac{k}{l}} = \frac{ml}{nk} \Rightarrow ml, nk \in \mathbb{Z} \wedge b \neq 0 \Rightarrow k \neq 0 \Rightarrow nk \neq 0 \Rightarrow \frac{a}{b} \in \mathbb{Q}$$

Ej.: "La suma de los cuadrados de dos números impares (enteros) es un número par"

$$\begin{aligned} m &= 2k-1, k \in \mathbb{Z} \\ n &= 2l-1, l \in \mathbb{Z} \end{aligned}$$

$$\begin{aligned} m^2 + n^2 &= (2k-1)^2 + (2l-1)^2 \\ &= 4k^2 - 4k + 1 + 4l^2 + -4l + 1 \\ &= 4k^2 + 4l^2 - 4k - 4l + 2 \\ &= 2(2k^2 + 2l^2 - 2k - 2l + 1) \\ &= 2 \cdot \lambda \Rightarrow \text{ es par} \end{aligned}$$

Reducción al absurdo

Se basa en la tautología *Reductio ad absurdum*:

$$[(A \wedge \neg B) \Rightarrow F] \Leftrightarrow (A \Rightarrow B)$$

A	B	$[(A$	$\wedge$	$\neg B)$	$\Rightarrow$	$F]$	$\Leftrightarrow$	$(A$	$\Rightarrow$	$B)$
F	F	F	F	V	V	F	V	F	V	F
F	V	F	F	F	V	F	V	F	V	V
V	F	V	V	V	F	F	V	V	F	F
V	V	V	F	F	V	F	V	V	V	V

Para aplicar este método seguimos los siguientes pasos:

1. Considerar como cierto lo contrario de lo que queremos demostrar
2. Llegar a una contradicción
3. Como al considerar $(\neg B \Rightarrow F) \Rightarrow (B \Rightarrow V)$
4. Esto último es así por considerar como A: "se cumplen las reglas básicas de la aritmética"

Ej.: "Existen infinitos primos"

1. Consideramos que existe un número finito de primos tal que: $p_1 < p_2 < ... < p_n$
2. Ahora tomamos un $p = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$
3. ¿ Este número sería divisible por alguno de los primos que lo compone? Siempre daría resto 1 por el sumando del final, luego el propio p sería primo. #[5]
4. Queda demostrado que debe haber una cantidad infinita de primos

Ej.: "$3\sqrt{2} - 1$ es irracional" Suponemos que es racional:

$$3\sqrt{2} - 1 = r \in \mathbb{Q} \Leftrightarrow 3\sqrt{2} = r + 1 = q \in \mathbb{Q} \Leftrightarrow \sqrt{2} = \frac{q}{3} \in \mathbb{Q} \ \#$$

[5] El símbolo # significa contradicción, aunque también puedes encontrar un rayo con flecha o un ! para expresar esto mismo

Demostración por contrarrecíproco

Se trata de demostrar la siguiente expresión:

$$A \Rightarrow B \equiv \neg B \Rightarrow \neg A$$

Ej.: "Para todo numero natural n, si el cuadrado de n es impar entonces n es impar"

$$\forall n \in \mathbb{N}: \ impar(n^2) \Rightarrow impar(n), \text{ donde } impar(n) \equiv \exists k \in \mathbb{N} : n = 2k + 1$$

Razonamos demostrando el contrarrecíproco:

$\forall n \in \mathbb{N} : \neg impar(n) \Rightarrow \neg impar(n^2) \equiv \forall n \in \mathbb{N} : par(n) \Rightarrow par(n^2)$, donde $par(n) \equiv \exists k \in \mathbb{N} : n = 2k$

Consideramos n un numero natural par, por definición de par:

$$n = 2k, \text{con } k \in \mathbb{N}$$

Elevando al cuadrado obtengo:

$$n^2 = 4k^2 = 2 \cdot 2k^2 = 2 \cdot k', \text{ con } k' \in \mathbb{N}, \text{ pues } k \in \mathbb{N}$$

Por definición de par, n^2 es par.

Demostración por contraejemplo (refutación)

Consiste en dar un ejemplo concreto para el cual no se cumple la proposición del enunciado.

Ej.:"Para cualquier numero entero p, si p es primo entonces $2^p - 1$ es primo.

$$\forall p \in \mathbb{Z} : primo(p) \Rightarrow primo(2^p - 1), \text{ sin embargo, para } p = 67 \text{ no es cierto}$$

Ej.: Conjetura de Euler: "Ninguna n-ésima potencia con $n > 2$ puede ser la suma de menos de n n-ésimas potencias de números naturales."

$$\forall x_1, x_2, x_3, ..., x_n, n \in \mathbb{N} : \left((n > 2) \Rightarrow \left(\forall k \in \mathbb{N} : (k < n) \Rightarrow (x^n \neq \sum_{i=1}^{k} x_i^n) \right) \right)$$

Sin embargo, esta fórmula no es cierta, puesto que para $n = 5$ y $k = 4$, existen $x_1 = 27$, $x_2 = 84$, $x_3 = 110$, $x_4 = 133$ y $x = 144$:

$$144^5 = 27^5 + 84^5 + 110^5 + 133^5$$

Demostración por casos

Se basa en la regla de inferencia de silogismo hipotético

Ej.: "Para todo entero c impar no existe solución real de la ecuación: $n^2 + n + c = 0$"

$$\forall c \in \mathbb{Z} : impar\,(c) \Rightarrow \neg \left(\exists n \in \mathbb{Z} : n^2 + n - c = 0 \right)$$

Razonamos por el contrarreciproco:

$$\forall c \in \mathbb{Z} : \left(\exists n \in \mathbb{Z} : n^2 + n - c = 0 \right) \Rightarrow par(c)$$

Distingo ahora dos casos, el que n sea par o impar:

- Para n par:

$$n = 2k, k \in \mathbb{Z} \Rightarrow c = n^2 + n = (2k)^2 + 2k = 2 \cdot (2k^2 + k) = 2 \cdot \lambda, \ \lambda \in \mathbb{Z} \Rightarrow par(c)$$

- Para n impar:

$$n = 2k+1, k \in \mathbb{Z} \Rightarrow c = n^2+n = (2k+1)^2+2k+1 = 2\cdot(2k^2+3k+1) = 2\cdot\varphi, \ \varphi \in \mathbb{Z} \Rightarrow par(c)$$

Inducción matemática

Sea $P(n)$ una propiedad definida para un número natural n, para la cual se verifica que: $\forall n \in \mathbb{N} : P(n)$, aplicamos el **PRINCIPIO DE INDUCCIÓN MATEMÁTICA** sobre $n \in \mathbb{N}$:

$$\forall n \in \mathbb{N} : (P(0) \wedge (\forall k \geq 0 : P(k) \Rightarrow P(k+1))) \Rightarrow P(n)$$

Principio de Inducción

1. Consideremos una afirmación $P(n)$ relativa a los números naturales n.
2. Si es cierta $P(0)$ y para $n \in \mathbb{N}$ arbitrario $\rightarrow P(n) \Rightarrow P(n+1)$, entonces $\forall n \in \mathbb{N}, P(n)$ es cierto.

Terminología:

- $P(0)$ es la **base de inducción**.
- $P(n)$ es la **hipótesis de inducción**.
- $P(n) \Rightarrow P(n+1)$ es el **paso inductivo**.

Ej.: "$\forall n \in \mathbb{N} : \sum_{k=0}^{n} = \frac{n \cdot (n+1)}{2}$"

Construimos la hipótesis de inducción

$$P(n) \equiv \sum_{k=0}^{n} k = \frac{n \cdot (n+1)}{2}$$

Comprobamos que la base de inducción es cierta

$$P(0) \equiv 0 = \frac{0 \cdot 1}{2} \Leftrightarrow 0 = 0$$

Demostramos que $P(n+1) \equiv \frac{(n+1) \cdot (n+2)}{2}$

$$\sum_{k=0}^{n+1} k = 0 + 1 + ... + n + (n+1) \overset{H.I.}{=} \frac{n \cdot (n+1)}{2} + (n+1) = \frac{(n+1) \cdot (n+2)}{2}$$

Con lo cual se cumple $\forall n \in \mathbb{N} : P(n)$

Ej.: "$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + ... + \frac{1}{\sqrt{n}} \geq \sqrt{n}$ "

Pruebo el que existe la base de inducción

$$P(1) \equiv \frac{1}{\sqrt{1}} \geq 1 \Leftrightarrow 1 \geq 1$$

Dada mi hipótesis de inducción: $P(n) \equiv \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + ... + \frac{1}{\sqrt{n}} \geq \sqrt{n}$, demuestro que se verifica $P(n+1) \equiv \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + ... + \frac{1}{\sqrt{n+1}} \geq \sqrt{n+1}$ (Paso inductivo):

$$P(n) \equiv \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + ... + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} \overset{H.I.}{\geq} \sqrt{n} + \frac{1}{\sqrt{n+1}} \overset{?}{\geq} \sqrt{n+1}$$

$$\sqrt{n} + \frac{1}{\sqrt{n+1}} \geq \sqrt{n+1} \Leftrightarrow \frac{1}{\sqrt{n+1}} \geq \sqrt{n+1} - \sqrt{n} = \frac{1}{\sqrt{n+1} + \sqrt{n}} \Leftrightarrow \frac{1}{\sqrt{n+1}} \geq \frac{1}{\sqrt{n+1} + \sqrt{n}}$$

Principio de Inducción Completa

En ocasiones la inducción completa no es suficiente para la demostración de ciertas proposiciones y se debe recurrir a un estadio superior de esta: la **Inducción Fuerte o Completa**.

La novedad en esta función es que ya no solo $P(k) \Rightarrow P(k+1)$ sino que todas las "fichas de dominó" anteriores sustentan la siguiente.

La diferencia fundamental está en:

- **Casos Base**: $n = m$, $n = m + 1$, $n = m + 2$, ..., $n = m + i$ (los que sean necesarios)
- **Paso inductivo**: $n > m + i$

  Suponiendo que se verifica la H.I.C. $\rightarrow \forall k > m + i : m \leq l < k : P(l)$, se trata de demostrar que se verifica $P(k)$.

Es decir, esto último indica que demostrados los casos base necesarios, todos los valores entre el primer caso base para el que se ha comprobado la hipótesis de inducción y el k que queremos probar son válidos para la proposición y gracias a ellos, a esos l podemos introducir la hipótesis inductiva para demostrar $P(k)$.

Ej.:

$$P(n) \equiv \exists a, b \in \mathbb{N} : n = 3a + 8b : \forall n \geq 14$$

Casos base:

$$P(14) \equiv \exists a, b \in \mathbb{N} : 14 = 3a + 8b, a = 2 \wedge b = 1$$

$$P(15) \equiv \exists a, b \in \mathbb{N} : 15 = 3a + 8b, a = 5 \wedge b = 0$$

$$P(16) \equiv \exists a, b \in \mathbb{N} : 16 = 3a + 8b, a = 0 \wedge b = 2$$

Paso inductivo:

$$\forall k \geq 17 : 14 \leq l < k : P(l) \equiv \exists a', b' \in \mathbb{N} : l = 3a' + 8b'$$

Probamos que se cumple $P(k)$:

$$k = k - 3 + 3 \overset{m \leq k-3 < k}{=} 3a' + 8b' - 3 = 3(a' - 1) + 8b' \Rightarrow a = a' - 1 \wedge b = b'$$

Luego $\forall n \in \mathbb{N} : \exists a, b \in \mathbb{N} : n = 3a + 8b$

Concretamente en este ejemplo decimos incluso que el $a_k = a_{k-3} - 1$ y que $b_k = b_{k-3}$

NÚMEROS, INDUCCIÓN Y RECURSIÓN

INTRODUCCIÓN A LOS CONJUNTOS NUMÉRICOS

Números naturales

Se define el conjunto $\mathbb{N} = \{0, 1, 2, ...\}$ de los números naturales mediante los 5 **Axiomas de Peano**:

- Existe un elemento de $\mathbb{N}$ al que llamamos 0 (primer natural)
- Existe una función sucesor; $\mathbb{N} \to \mathbb{N} : \forall n \in \mathbb{N} : s(n) \in \mathbb{N}$
- El 0 no es sucesor de ningún natural:

$$\forall n \in \mathbb{N} : s(n) \neq 0$$

- No existen dos números naturales distintos con el mismo sucesor:

$$\forall n \in \mathbb{N} : (s(n) = s(m)) \Rightarrow n = m$$

- Todo conjunto numérico A al que pertenece el 0 y donde cualquier elemento que pertenezca a él posee superior, necesariamente coincide con los naturales:

$$\forall A \subseteq \mathbb{N} : ((0 \in A) \wedge (\forall n \in A : s(n) \in A)) \Rightarrow A = \mathbb{N}$$

Llamamos segmento de $\mathbb{N}$ al subconjunto $N_m : m \in \mathbb{N}$

$$\mathbb{N} = \{m, m+1, m+2, ...\}$$

Números enteros

Son una extensión de los naturales incluyendo los negativos, sigue las mismas reglas de generación que el conjunto anterior, pero con la diferencia que de incluir la función predecesor para incluir los negativos, perdiendo la cualidad de *primer entero*.

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$$

Números racionales

Incluyen nuevamente a los anteriores y nacen ante la insuficiencia de estos para describir ciertos aspectos matemáticos

$$\mathbb{Q} = \left\{ \frac{a}{b} : (\forall a, b \in \mathbb{Z}) \wedge (b \neq 0) \right\}$$

Números reales

Están formados por los anteriores sumando el conjunto $\mathbb{I}$ de los irracionales. Nacen de la incompletitud de los anteriores para ciertas áreas de las matemáticas y completan la recta real, conformándola como una recta sin "huecos".

$$\mathbb{R} = \{-\infty, ..., +\infty\}$$

Números complejos

Estos por último surgen aunando los anteriores y los imaginarios, basados estos últimos en la unidad $i = \sqrt{-1}$. Terminan de completar los números necesarios para fundamentar la matemática más fundamental.

$$\mathbb{C} = \{\mathbb{R}, \sqrt{-1}, 3 + 23i, ...\}$$

DEFINICIONES RECURSIVAS

Una función $f : N_m \to B$ está definida recursivamente sobre N_m si para cada $n \in \mathbb{N}_m$:

- Está definida por un valor de $b \in B$ concreto **(Caso Base)**
- Se define el valor de n recurriendo a alguno de los anteriores valores de n **(Caso Recursivo)**

$$\text{Ej.: } \begin{cases} f(m) = b & \text{caso base} \\ f(n) = f(n-1) + f(n-2) & \text{caso recursivo} \end{cases}$$

Demostración de definiciones recursivas

Recursión simple

Para este tipo de casos es habitual recurrir a la demostración por **inducción simple** lo que implica que debemos seguir los pasos de la misma.

Ej.: "Demostrar que $fact(n) = n!$, donde $fact()$ es una función definida como:

$$\begin{array}{rccc} fact: & \mathbb{N} & \to & \mathbb{N} \\ & n & \longmapsto & fact(n) \end{array}$$

$$fact: \begin{cases} fact(0) = 1 \\ fact(n) = n \cdot fact(n-1) & n \geq 1 \end{cases}$$

Razonamos por inducción simple:

Caso Base$\to$ $fact(0) = 1 = n!$

Paso inductivo $n > 0$:

Mi hipótesis de inducción es: $fact(k) = k! : \forall k \geq 0$ por lo que debería ser: $fact(k+1) = (k+1)!$

$$fact(k+1) = (k+1) \cdot fact(k) \overset{H.I.}{=} (k+1) \cdot k! = (k+1)!$$

Como $k \geq 0 \Leftrightarrow k + 1 \geq 1 \Rightarrow n > 0$ y además $fact(k+1) = (k+1) \cdot fact(k)$ porque $k \geq 0$ por lo que a $k+1$ se le aplica el caso recursivo.

Recursión múltiple

Para estos casos es más habitual el empleo de la **Inducción Completa** porque cubre la magnitud de recursión propia de estas funciones al completo, en este caso tendremos más de un caso base.

Ej.: "Demostrar que la $fib(n) \leq n! : \forall n > 0$ Primero definimos la **función de fibonacci**:

$$\begin{aligned} fib : \mathbb{N} &\to \mathbb{N} \\ n &\longmapsto fib(n) \end{aligned}$$

$$fib : \begin{cases} fib(0) = 0 \\ fib(1) = 1 \\ fib(n) = fib(n-1) + fib(n-2) \quad n \geq 2 \end{cases}$$

Casos base:

$$fib(0) \overset{?}{\leq} 0! \Leftrightarrow 0 \leq 1$$

$$fib(1) \overset{?}{\leq} 1! \Leftrightarrow 1 \leq 1$$

Paso inductivo $\forall n > 2$:

Mi hipótesis de inducción es que $\forall k \geq 2 : fib(l) \leq l! : 0 \leq l < k$

Demostramos que se verifica $P(k) \equiv fib(k) \leq k! : \forall k \geq 2$

$fib(k) = fib(k-1) + fib(k-2) \overset{H.I.}{\leq} (k-1)! + (k-2)! = (k-1) \cdot (k-2)! + (k-2)! = (k-2)! \cdot k \Leftrightarrow$
$\Leftrightarrow fib(k) \leq (k-2)! \cdot k \Leftrightarrow fib(k) \cdot (k-1) \leq (k-1) \cdot (k-2)! \cdot k \Leftrightarrow fib(k) \cdot (k-1) \leq k! \Rightarrow fib(k) \leq k!$

TEORÍA DE NÚMEROS

Es la rama de las matemáticas que estudia las propiedades de los números, en particular de los enteros.

$$\mathbb{Z} = ..., -1, 0, 1, ...$$

División entera

Teorema de la división entera

Dados $a, b \in \mathbb{Z}$ con $a > 0, b > 0$ existen dos números enteros $c, r \in \mathbb{Z}$ tales que:

$$a = bc + r$$

Demostración:

1. **Existencia**

   Por inducción completa sobre $a \geq 0$:

   $$\exists c, r \in \mathbb{Z} : a = bc + r : 0 \leq r < b : \forall a \geq 0, b > 0$$

   Casos base: $a \leq b$

   $$\text{Si } a < b \Rightarrow a = b \cdot 0 + a : 0 \leq a < b \Rightarrow c = 0, r = a$$

   $$\text{Si } a = b \Rightarrow a = b \cdot 1 + 0 : 0 \leq 0 \leq b \Rightarrow c = 1, r = 0$$

Paso inductivo, probamos los casos $a > b$:

$$\text{H.I.} \rightarrow \forall a > b : \exists c', r' \in \mathbb{Z} : l = b \cdot c' + r' \wedge 0 \leq r' < b : 0 \leq l < a$$

Comenzamos diciendo que:

$$0 < a - b < a \Rightarrow a - b = b \cdot c' + r' \wedge 0 \leq r' < b$$

De aquí podemos operar que:

$$a - b = b \cdot c' + r' \Leftrightarrow a = bc' + b + r' \Rightarrow a = b(c' + 1) + r'$$

Luego existen ambos números

2. **Unicidad**

Razonamos por reducción al absurdo, suponiendo que existen más de uno:

$$a = bc_1 + r_1 = bc_2 + r_2$$

Con $c_1 \neq c_2$ y $0 \leq r_i < b$

Distinguimos dos casos:

- $c_1 > c_2$

$$a = bc_1 + r_1 = bc_1 + r_1 + bc_2 - bc_2 = bc_2 + b(c_1 - c_2) + r_1$$

Como $a = bc_2 + r_2 \Rightarrow r_2 = a - bc_2$ y sustituyendo la a de antes[6][7]

$$r_2 = bc_2 + b(c_1 - c_2) + r_1 - bc_2 = b(c_1 - c_2) + r_1 \overset{6.}{\geq} b + r_1 \overset{7.}{\geq} b \ \#$$

[8]

- $c_2 > c_1$ De forma análoga al caso anterior, llegamos a la contradicción $r_1 \geq$, en consecuencia se toma como cierto $c_1 = c_2$

Para demostrar la unicidad del resto, se recurre a $c_1 = c_2$:

$$r_1 = a - bc_1 = a - bc_2 = r_2$$

Corolarios

- Para $a, b \in \mathbb{Z} : b > 0, \exists! c, r \in \mathbb{Z}$ del mismo signo que $a : a = bc + r \wedge 0 \leq |r| < b$

[6] Porque $c_1 - c_2 \geq 1$
[7] Porque $r_1 \geq 0$
[8] Porque $0 \leq r_2 < b$

Demostración

Si $a \geq 0$ se cumple directamente por el **Teorema de la División Entera**. Si $\boldsymbol{a < 0}$ aplicamos el **Teorema de la División Entera** para $\boldsymbol{a' = -a}$, pues $a' \geq 0$ y $b > 0$: existen únicos $c', r' \in \mathbb{Z}$ tales que $a' = b \cdot c' + r'$ con $0 \leq r' < b$. Ahora bien:

$$\begin{array}{ll} a' = b \cdot c' + r' & \Longrightarrow \quad [\text{ Por definición } a' = -a \,] \\ -a = b \cdot c' + r' & \Longrightarrow \\ a = -b \cdot c' - r' & \Longrightarrow \\ a = b \cdot (-c') + (-r') & \Longrightarrow \\ a = b \cdot c + r & \end{array}$$

donde $\boldsymbol{c = -c'} \in \mathbb{Z}$, pues $c' \in \mathbb{Z}$, y $\boldsymbol{r = -r'} \in \mathbb{Z}$, pues $r' \in \mathbb{Z}$. Además:

$$\begin{array}{ll} 0 \leq r' < b & \Longrightarrow \quad [\text{ Como } r' \geq 0 \text{ se verifica que } |-r'| = r' \,] \\ 0 \leq |-r'| < b & \Longrightarrow \quad [\text{ Por definición } r = -r' \,] \\ 0 \leq |r| < b & \end{array}$$

Luego existen únicos $c, r \in \mathbb{Z}$ tales que $a = b \cdot c + r$ y $0 \leq |r| < b$. ■

- **Ejemplo**

  Para $a = -8$ y $b = 3$ se tiene que:

  $-8 = 3 \cdot (-1) + (-5)$ pero no se verifica $0 \leq |-5| < 3$.
  $-8 = 3 \cdot (-3) + 1$ pero no se verifica que r = 1 tenga el mismo signo que $a = -8$.
  $-8 = 3 \cdot (-\mathbf{2}) + (-\mathbf{2})$ se verifica que $0 \leq |-2| < 3$. Luego $c = -2$ y $r = -2$, con el mismo signo que $a = -8$.

- Para $a, b \in \mathbb{Z} : b > 0, \exists! c, r \in \mathbb{Z}$ que $a : a = bc + r \wedge 0 \leq r < b$

Demostración

Si $\boldsymbol{a \geq 0}$ se cumple directamente por el **Teorema de la División Entera**. Si $\boldsymbol{a < 0}$, por el **Corolario 1**: existen únicos $c', r' \in \mathbb{Z}$ tales que $a = b \cdot c' + r'$ con $c' < 0$, $\boldsymbol{r' \leq 0}$, y $0 \leq |r'| < b$.

Distinguimos casos: $r' = 0$ y $r' < 0$

- **Caso 1**: $\boldsymbol{r' = 0}$

  $a = b \cdot c' + r' = b \cdot c' + 0 = b \cdot c'$. Luego $\boldsymbol{c = c'}$ y $\boldsymbol{r = 0}$.

  $div(-8, 3) =^{\mathbf{C1}} (-2, -2)$
  $div(-8, 3) =^{\mathbf{C2}} (-3, 1)$

- **Caso 2**: $r' < 0$

  $$a = b \cdot c' + r' = b \cdot c' + r' - b + b = b \cdot c' - b + r' + b = b \cdot (c' - 1) + (r' + b) = b \cdot c + r$$

  donde $\boldsymbol{c = c' - 1} \in \mathbb{Z}$, pues $c' \in \mathbb{Z}$, y $\boldsymbol{r = r' + b} \in \mathbb{Z}$, pues $r', b \in \mathbb{Z}$. Además $0 \leq r < b$:

  Como $0 \leq |r'| < b$ significa que $-b < r' < b$, y además $r' < 0$, se cumple que $-b < r' < 0$.
  Entonces $b - b < r' + b < 0 + b$, es decir, $0 < r < b$. Luego se cumple $0 \leq r < b$. ■

Si $\boldsymbol{b < 0}$ entonces **se cambiaría $\boldsymbol{a}$ de signo** y se aplicaría el **Corolario 2** con $b > 0$.

- Para $a, b \in \mathbb{Z} : b \neq 0, \exists! c, r \in \mathbb{Z}$ que $a : a = bc + r \wedge 0 \leq r < b$

Múltiplos y divisores

Notación y propiedades

- Para decir que a **es divisor de** b: $a \mid b$
- Para decir que a **es múltiplo de** b: $a \dot{b}$
- Para decir que a no es divisor de b: $a \nmid b$

- $a \mid b$ y $a \mid n \Rightarrow a \mid (m+n)$ y $a \mid (m \cdot n)$
- $a \mid m \Rightarrow a \mid m \cdot k$
- $a \mid m \Rightarrow a \cdot k \mid m \cdot k$
- $a \mid m \Rightarrow \frac{a}{k} \mid \frac{m}{k}, \forall k \in \mathbb{Z}$

Casos especiales:

- $\frac{0}{0}$ no está definido
- $0 \mid 0$ porque $0 = 0 \cdot 0$
- $0 \nmid a$ con $a \neq 0$ pues no se cumple $a = 0 \cdot c$
- $\frac{a}{0}$ no está definido

Teorema de Euclides

Máximo común divisor

- $mcd(0,0)$ no existe
- $mcd(a,b) = mcd(b,a)$
- $mcd(a,b) = mcd(|a|,|b|)$
- $mcd(a,0) = mcd(0,a) = |a|$

Lema de Euclides

$$mcd(a,b) = mcd(b,r) : a \geq b > 0$$

Demostración:

- "$\subseteq$" Vamos a ver que todo divisor común de a y b también lo es de b y r. Sean $a = d \cdot c_1, b = d \cdot c_2$:
$$r = a - bc = d \cdot c_1 - d \cdot c_2 \cdot c = d(c_1 - c_2 - c) \Rightarrow d \mid r$$
- "$\supseteq$" Vamos a ver que todo divisor común de r y b también lo es de b y a. Sean $b = d \cdot c_1, r = d \cdot c_2$:
$$a = bc + r = d \cdot c_1 \cdot c - d \cdot c_2 = d(c_1 \cdot c + c_2) \Rightarrow d \mid a$$

De este razonamiento se desprende el que $mcd(a,b) = mcd(b,r)$

Teorema de Euclides

Dados $a, b \in \mathbb{Z} : a > b \geq 0 \Rightarrow \exists! mcd(a,b)$

Demostración:

1. Demostramos la **existencia** por inducción completa sobre $b \geq 0$:

   Caso base: $b = 0$

   $$mcd(a, b) = mcd(a, 0) = |a| = a$$

   Paso inductivo, probamos los valores $b > 0$:

   $$\text{H.I.} \rightarrow \forall b > 0 : \exists! mcd(a, l) : 0 \leq l < b \wedge a > l \geq 0$$

   $$a = bc + r$$

   Como $0 \leq r < b$ por el teorema de la división entera, podemos tomar como $l = r$ y entonces se verifica $mcd(b, r)$ que por el lema de euclides se extiende a $mcd(a, b)$

2. Demostramos ahora la unicidad, por reducción al absurdo: Supongamos que $d_1 = mcd(a, b)$ y $d_2 = mcd(a, b)$, con $d_1 \neq d_2$ y $d_1, d_2 > 0$. Por definición de máximo común divisor:

   $$\begin{cases} d_1 \mid d_2 \Leftrightarrow d_2 = c \cdot d_1 \\ d_2 \mid d_1 \Leftrightarrow d_1 = c' \cdot d_2 \end{cases} \Rightarrow d_1 = c' \cdot d_2 = c' \cdot c \cdot d_1 \Rightarrow c' \cdot c = 1 \Leftrightarrow c' = c = 1$$

   Luego $d_1 = c' \cdot d_2 = d_2$ y $d_2 = c \cdot d_1 = d_1$

Algoritmo de Euclides

Es el algoritmo cuyo objetivo es automatizar la búsqueda de un $mcd(a, b)$ tales que $a \geq b > 0$:

1. Comenzamos dividiendo ambos números:

   $$a = b \cdot a_1 + b_1$$

2. Suponemos dos casos:

   - $b_1 = 0$, por el Lema de Euclides:

     $$mcd(a, b) = mcd(a_1, b_1) = mcd(a_1, 0) = a_1$$

   - $b_1 > 0$, entonces tomamos como nuevos $a = a_1$ y $b = b_1$:

     $$a_1 = b_1 \cdot a_2 + b_2$$

     Y de nuevo llegamos a la tesitura de evaluar si $b_2 = 0$

3. Con lo cual, dividimos divisor y restos sucesivos, hasta llegar a un momento en el que: $b_i = 0$ que significará que:

   $$mcd(a, b) = mcd(a_i, b_i) = mcd(a_i, 0) = a_i$$

De este modo podemos calcular sin problemas el $mcd(a, b)$ mediante divisiones enteras sucesivas.

Teorema de Bezout

Este teorema dice que elegidos dos números cuales quiera, su máximo común divisor se puede escribir como combinación lineal de cada número por una constante, llamamos a su $mcd(a, b) = d$:

$$d = m \cdot a + n \cdot b$$

Además estos u y v no tienen por qué ser únicos.

Demostración: Es suficiente con probarlo para $a \geq b > 0$, por que en los casos en los que haya negativos, se puede pasar ese signo a u o v. Para $a = b = 0 \Rightarrow \nexists d$, y para $a = b > 0 \Rightarrow d = a \Rightarrow a = a \cdot 1 + b \cdot 0$.

Razonamos por inducción completa sobre $b \geq 0$:

1. Caso base: $b = 0$

$$d = mcd(a, b) = mcd(a, 0) = a \Rightarrow u = 1, v = 0$$

2. Paso inductivo, razonamos para $b > 0$:

   H.I. $\rightarrow \forall b > 0 : 0 \leq l < b$ y que $a' > l \geq 0$, que si $d' = mcd(a', l) \Rightarrow \exists m', n' \in \mathbb{Z} : d' = m'a' + n'l$

   Podemos suponer por el teorema de la división entera que $a = bc + r$ y además por el lema de euclides que:

$$mcd(a, b) = mcd(b, r) \overset{H.I.}{=} m'b + n'r = m'b + n(a - bc) = n'a + m'b - n'bc = an' + b(m' - n'c) = am + bn$$

Algoritmo de Bezout

Para calcular los coeficientes mencionados antes que satisfacen la igualdad de Bezout, existe un algoritmo muy sencillo.

1. Consideramos los primeros $m_k = 0$ y $n_k = 0$, siendo este k el último paso del algoritmo de Euclides.

2. Tomamos el resto de pares como:

$$m_i = n_{i-1}$$

$$n_i = m_{i-1} - m_i \cdot c_i$$

   Donde c_i es el cociente de dicho paso

3. Los valores $m = m_0$ y $n = n_0$ son los correctos.

i	a_i	b_i	r_i	c_i	m_i	n_i
0	721	448	273	1	**23**	$-14 - 23 \cdot 1 = \mathbf{-37}$
1	448	273	175	1	-14	$9 - (-14) \cdot 1 = 23$
2	273	175	98	1	9	$-5 - 9 \cdot 1 = -14$
3	175	98	77	1	-5	$4 - (-5) \cdot 1 = 9$
4	98	77	21	1	4	$-1 - 4 \cdot 1 = -5$
5	77	21	14	3	-1	$1 - (-1) \cdot 3 = 4$
6	21	14	7	1	1	$0 - 1 \cdot 1 = -1$
7	14	7	0	2	0	$1 - 0 \cdot 2 = 1$
8	**7**	0	–	–	1	0

$mcd(721, 448) = \mathbf{7} = \mathbf{23} \cdot 721 + (\mathbf{-37}) \cdot 448$. Luego $m = 23$ y $n = -37$.

Mínimo común múltiplo

Dados $a, b \in \mathbb{Z}$ definimos el mínimo común múltiplo de a y b como el menor de los múltiplos comunes.

$$mcm(a, b) = m \Leftrightarrow \begin{cases} a \mid m \wedge b \mid m \\ \forall m' \in \mathbb{Z} : a \mid m' \wedge b \mid m' \Rightarrow m \mid m' \end{cases}$$

Propiedades:

- $mcm(0,0) = 0$
- $mcm(a,b) = mcm(|a|,|b|)$
- $mcm(a,b) = mcm(b,a)$
- $mcm(a,0) = 0$
- $mcd(a,b) \cdot mcm(a,b) = a \cdot b : \forall a,b > 0$

Números primos

Decimos que un número es primo cuando el único divisor además del 1 es sí mismo.

$$p \text{ primo} \Leftrightarrow \nexists d \in \mathbb{Z} : (0 < d < p) \wedge d \mid p \Rightarrow \forall d \in \mathbb{Z} : (d \mid p \Rightarrow d = 1 \vee d = p)$$

Los números que no son primos son compuestos[9] y se pueden expresar como producto de primos.

Algoritmo para el cálculo de números primos

Lo que hacemos es seguir el siguiente procedimiento:

1. Calcular la raíz cuadrada aproximada por truncamiento del número en cuestión.
2. Indicar todos los números primos menores o iguales que esa raíz aproximada. Es decir, busco $0 < p^2 \leq n$.
3. Si cada uno de los primos indicados anteriormente NO divide a n entonces ese n es primo.

   Ej.: $n = 467$ es primo?

   $$\sqrt{467} \simeq 21 \Rightarrow 0 < p \leq 21 \Rightarrow p = 2,3,5,7,11,13,17,19$$

   Como no hay ningún primo $p : p \mid 467 \Rightarrow 467$ es primo.

Teorema Fundamental de la Aritmética

Todo número entero se puede descomponer como producto de primos.

$$\forall n \in \mathbb{Z} : n = p_1 \cdot ... \cdot p_n : p_i \text{ es primo}$$

Demostración:

- Existencia: razonamos por reducción al absurdo.

  $$n = 1 \rightarrow 1 = p_1^{n_1} \cdot ... \cdot p_m^{n_m} : m = 0$$

  Demostrado el caso base suponemos para cualquier $k > 1$ que se cumple la proposición $P(k) \equiv \forall l \in \mathbb{N} : 1 \leq l < k$, l admite una descomposición en primos. Distinguimos ahora dos casos:

  - k es primo:

    $$k = k \cdot 1$$

[9] Por convenio, 0 y 1 no son primos

- k no es primo:

$$k = l_1 \cdot l_2 = p_1^{n_1} \cdot ... \cdot p_m^{n_m} \cdot q_1^{t_1} \cdot ... \cdot q_s^{t_s}$$

- Unicidad: por inducción sobre t:
  - Probamos los casos base: $t = 1 \Rightarrow p_1 = q_1$
  - Demostrados los casos $n \leq t - 1$, demostramos que:

    $p_1 \cdot p_2 \cdot ... \cdot p_t = q_1 \cdot q_2 \cdot ... \cdot q_s \Rightarrow p_1 \mid q_1 \cdot ... \cdot q_n \Rightarrow p_1 \mid q_i \Rightarrow q_1 = p_1 \cdot k \Rightarrow k = 1$ por ser primos

    Sustituyendo en la expresión inicial:

$$p_1 \cdot ... \cdot p_t = p_1 \cdot q_2 \cdot ... \cdot q_s \Rightarrow p_2 \cdot ... \cdot p_t = q_2 \cdot ... \cdot q_s$$

    En el primer lado de la igualdad hay $t - 1$ factores y en el lado derecho $s - 2$, con lo cual:

$$r - 1 = s - 1 \overset{H.I:}{\Rightarrow} r = s$$

Infinitud de los números primos

Existen infinitos números primos, aunque no los conozcamos todos.

Demostración:

Sean $p_1, p_2, ..., p_n$ los únicos números primos donde $n \in \mathbb{N}$, escojamos el número:

$$b = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$$

Como $b \notin P = \{p_i : p \text{ primo} \wedge i \in \mathbb{N}\}$, entonces $\exists p_i \in P : b = p_i \cdot c$. Por lo tanto:

$$b = p_1 \cdot p_2 \cdot ... \cdot p_i \cdot ... \cdot p_n + 1 \Leftrightarrow 1 = p_i \cdot (c - p_1 \cdot p_2, ..., p_n) \Rightarrow p_i \mid 1 \Rightarrow p_i = 1 \Rightarrow b \text{ primo } \#$$

TEORÍA DE CONJUNTOS

CONJUNTOS

Un conjunto es una colección de objetos que está definido de forma clara para saber si un elemento[10] pertenece o no a ese conjunto. A los elementos que pertenecen a un conjunto se les denomina **elementos**.

$$a \in A = \{a\}$$

Relaciones de pertenencia

- **Igualdad de conjuntos**: $A = B \Leftrightarrow x \in A \Leftrightarrow x \in B \Leftrightarrow A \subset B \wedge B \subset A$
- **Pertenencia o no a un conjunto**: $a \in A = \{x : P(x)\} \Leftrightarrow P(a) \equiv True$
- **Inclusión de conjuntos**: $A \subset B \Leftrightarrow \forall a \in A \Rightarrow \forall a \in B$

Es decir, si un conjunto contiene a otro, los elementos del primero están contenidos en el segundo y si un elemento pertenece a un conjunto, se encuentra entre sus elementos, **NO entre los elementos de un conjunto que sea elemento del conjunto mayor**.

Ej.:

Razona cuáles de las afirmaciones que siguen son verdaderas:

a) $1 \in \{1\}$,	*b*) $\{1\} \subseteq \{1\}$,	*c*) $\{1\} \in \{1\}$,
d) $\{1\} \subseteq \{\{1\}\}$,	*e*) $\{1\} \in \{\{1\}\}$,	*f*) $\emptyset \subseteq \emptyset$,
g) $\emptyset \subseteq \{1\}$,	*h*) $\emptyset \in \{1\}$,	*i*) $\{\emptyset\} = \emptyset$.

Solución:

a) $1 \in \{1\}$ es verdadero, ya que 1 es el único elemento del conjunto unitario $\{1\}$.

b) $\{1\} \subseteq \{1\}$ es verdadero, ya que cualquier conjunto está contenido en sí mismo.

c) $\{1\} \in \{1\}$ es falso, ya que el conjunto $\{1\}$ no es un elemento del conjunto unitario $\{1\}$ que sólo tiene por elemento el 1.

d) $\{1\} \subseteq \{\{1\}\}$ es falso, ya que $1 \in \{1\}$, pero $1 \notin \{\{1\}\}$, cuyo único elemento es $\{1\}$.

e) $\{1\} \in \{\{1\}\}$ es cierto ya que efectivamente $\{1\}$ es el único elemento del conjunto unitario $\{\{1\}\}$.

f) $\emptyset \subseteq \emptyset$ es verdadero, ya que cualquier conjunto está contenido en sí mismo.

g) $\emptyset \subseteq \{1\}$ es verdadero, ya que el conjunto vacío está contenido en cualquier conjunto.

h) $\emptyset \in \{1\}$ es falso, ya que el conjunto vacío no es un elemento de $\{1\}$, cuyo único elemento es el 1.

i) $\{\emptyset\} = \emptyset$ es falso, porque $\emptyset \in \{\emptyset\}$, pero $\emptyset \notin \{\emptyset\}$.

[10] El conjunto que contiene a todos los elementos es el **universal** U y el que no contiene a ninguno es el **vacío** $\emptyset$

Si $x \in \{\{y,z\},\{y\}\}$, ¿qué se puede asegurar?

(a) $x \in \{y\}$ (b) $y \in x$ (c) $\{y\} \in x$

Solución:

La expresión $x \in \{\{y,z\},\{y\}\}$ significa que x es un elemento del conjunto $\{\{y,z\},\{y\}\}$ que tiene exactamente dos elementos. Por tanto, x es o bien el primer elemento $\{y,z\}$ o el segundo elemento $\{y\}$. Ninguno de estos dos elementos es igual a y, por lo que ninguno de los dos pertenece al conjunto unitario $\{y\}$:

$$\{y,z\} \notin \{y\} \qquad \{y\} \notin \{y\}.$$

En consecuencia la respuesta (a) no es correcta.

En ninguno de los dos casos tenemos que $\{y\}$ sea un elemento de x:

$$\{y\} \notin \{y,z\} \qquad \{y\} \notin \{y\}.$$

Por tanto la respuesta (c) tampoco es correcta.

En cambio, el elemento y sí que pertenece a x en ambos casos:

$$y \in \{y,z\} \qquad y \in \{y\}.$$

Así la respuesta correcta es (b).

Axiomas de la teoría de conjuntos

Durante la historia ha habido conflictos lógicos en cuanto a la definición de conjuntos que desmoronaron los cimientos de las matemáticas como la **paradoja de Rusell**, por ello se fundamento la nueva teoría de conjuntos, **la axiomática** en lo que se conoce como los **AXIOMAS DE LA TEORÍA DE CONJUNTOS**:

- **Axioma de extensionalidad**: Dos clases A y B que poseen los mismos elementos son la misma clase.
- **Axioma del formador de clases**: Para cada fórmula $f(x)$ existe al menos una clase formada por todos los conjuntos que satisfacen la fórmula $f(x)$.
- **Axioma del par no ordenado**: El par formado por dos conjuntos es a su vez, otro conjunto.
- **Axioma de regularidad**: Para cada clase no vacía, siempre hay al menos un elemento que no contiene otros elementos de la clase, esto es , que es disjunto con ella.
- **Axioma de la gran union**: Si A es un conjunto, entonces $\bigcap_{a \in A} a$ es también un conjunto.
- **Axioma del conjunto vacío**: $\emptyset$ es el conjunto sin elementos.
- **Axioma de infinidad**: Existe un conjunto A con las siguientes propiedades: $\emptyset \in A$ y si $x \in A \Rightarrow x \cup \{x\} \in A$, lo que asegura la existencia de conjuntos infinitos.
- **Axioma funcional**: Sea A un conjunto y $f : A \to B$ una aplicación, entonces B es un conjunto, es decir, si el conjunto del dominio es un conjunto, el conjunto formado por los valores del codominio también lo es para poder establecer la relación entre ambos.
- **Axioma del conjunto de partes**: Para cada conjunto A existe un conjunto $P(A)$ formado por todos los subconjuntos de A.
- **Axioma de Elección**: Dada cualquier familia no vacía de conjuntos no vacíos, dos a dos disjuntos, existe, por lo menos, un conjunto que contiene un elemento y sólo uno de cada conjunto perteneciente a la familia.

Operaciones con conjuntos

- Inclusión: $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$
- Equivalencia: $A \equiv B \Leftrightarrow A \subset B \wedge B \subset A$
- Pertenencia: $x \in A \Leftrightarrow A = \{..., x, ...\}$
- Conjunto vacío: $\emptyset = \{\} : \forall x \in \emptyset$
- Intersección: $A \cap B = \{x : x \in A \wedge x \in B\}$
- Unión: $A \cup B = \{x : x \in A \vee x \in B\}$
- Complemento: $A \backslash B = \{x : x \in A \wedge x \notin B\}$
- Intersecciones múltiples: Sea I un conjunto de de índices y $\forall i \in I$

$$\bigcap_{i \in I} A_i = \{x : \forall i \in I : x \in A_i\}$$

- Uniones múltiples: Sea I un conjunto de de índices y $\forall i \in I$

$$\bigcup_{i \in I} A_i = \{x : \exists i \in I : x \in A_i\}$$

Familia de Conjuntos

Cuando a un conjunto no pertenece un elemento sino que más conjunto, decimos que este es una **familia de conjuntos**. Para este concepto definimos la unión y la intersección como:

$$\bigcup F = \{x : x \in C \text{ para algún } C \in F\}$$

$$\bigcap F = \{x : x \in C \text{ para todo } C \in F\}$$

Ej.: Sea $M_k = \{n \cdot k : n \in \mathbb{N}\}$ y $F\{M_k : k \geq 2\} = \{M_2, M_3, ...\}$ se define:

$$\bigcup F = \bigcup_{k \geq 2} M_k = \mathbb{N} \backslash \{1\}$$

$$\bigcap F = \bigcap_{k \geq 2} M_k = \{0\}$$

Partes de un Conjunto

Sea A un conjunto, se le llama *partes de A* o P(A) al conjunto formado por todos los subconjuntos de A:

$$\text{Ej.: } A = \{a, b, c\} \rightarrow P(A) = \{\{a\}, \{b\}, \{c\}, \emptyset, \{a, b\}, \{a, c\}, \{b, c\}, A\}$$

Producto Cartesiano

Sean A y B conjuntos no vacíos, llamamos par ordenado a una pareja donde $a \in A$ y $b \in B$:

$$(a, b) \neq (b, a) : a \in A \wedge b \in B$$

El producto cartesiano[11] de dos conjuntos es el conjunto:

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

[11] Es distributivo con respecto de la unión e intersección de conjuntos

Dada una colección arbitraria de conjuntos $A_1, A_2, ..., A_n$, llamaremos producto cartesiano de los mismos a las n-tuplas ordenadas $(a_1, a_2, ..., a_n)$, donde $a_i \in A_1 \leq i \leq n$:

$$\underbrace{A \times A \times ... \times A}_{n \text{ veces}} = \{(a_1, ..., a_n) : a_i \in A, 1 \leq i \leq n\}$$

Y se denota por A^n

Álgebra de Boole

Si T es un conjunto fijado y $A, B \subseteq T$ dos subconjuntos de T, tenemos que $A \cap B, A \cup B, A \backslash B$ y $T \backslash A$ son subconjuntos de T.

Si $A, B \in P(T)$, entonces como $A \cup B, A \cap B, T \backslash A \in P(T)$, podemos definir estos conjuntos como operaciones en $P(T)$.

Complementario de un Conjunto

Dado un conjunto $A \in T$, definimos el complementario como $T \backslash A$ y se denota como $\bar{A}$ o $\backslash A$

Leyes del Álgebra de Boole

$A \cup (B \cup C) = (A \cup B) \cup C$	Asociativa	$A \cap (B \cap C) = (A \cap B) \cap C$
$A \cup B = B \cup A$	Conmutativa	$A \cap B = B \cap A$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributiva	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$\backslash (A \cup B) = (\backslash A) \cap (\backslash B)$	De Morgan	$\backslash (A \cap B) = (\backslash A) \cup (\backslash B)$
$A \cup A = A$	Idempotencia	$A \cap A = A$
$\backslash \backslash A = A$	Doble complementación	
$A \cup (B \cap A)$ =A	Absorción	$A \cap (B \cup A)$ =A
$A \cup \varnothing = A$		$A \cap \varnothing = \varnothing$
$A \cup T = T$		$A \cap T = A$
$A \cup (\backslash A) = T$	Complementación	$A \cap (\backslash A) = \varnothing$

Además se le pueden aplicar a este tipo de conjuntos las Leyes de De Morgan vistas en el capítulo de LÓGICA DE PREDICADOS.

EL ÁLGEBRA DE LA LÓGICA DE GEORGE BOOLE

Sócrates es hombre
Todos los hombres son mortales

Luego Sócrates es mortal

podía ser representado formalmente de la siguiente manera matemática, donde x designa la «clase de los hombres», y representa la «clase que solo contiene a Sócrates» y z representa la clase de los seres mortales:

$$\begin{array}{l} y \,.\, x = y \\ x \,.\, z = x \\ \hline y \,.\, z = y \end{array}$$

SUMA	PRODUCTO
$x + (1 - x) = 1$	$x \,.\, (1 - x) = 0$
$0 + x = x$	$0 \,.\, x = 0$
$1 + x = 1$	$1 \,.\, x = x$
$x + x = x$	$x \,.\, x = x$
$x + y = y + x$	$x \,.\, y = y \,.\, x$
$x + (y + z) = (x + y) + z$	$x \,.\, (y \,.\, z) = (x \,.\, y) \,.\, z$
$x + (y \cdot z) = (x + y) \cdot (x + z)$	$x \,.\, (y + z) = x \,.\, y + x \,.\, z$

1. Multiplicando por la izquierda ambos miembros de la segunda ecuación $x \,.\, z = x$ por y:

$$x \,.\, z = x \Rightarrow y \,.\, (x \,.\, z) = y \,.\, x$$

2. Aplicando la ley de transitividad para la multiplicación entre clases (análoga a la de multiplicación entre números) al primer miembro de la ecuación:

$$y \,.\, (x \,.\, z) = y \,.\, x \Rightarrow (y \,.\, x) \,.\, z = y \,.\, x$$

3. Aplicando ahora la primera ecuación $y \,.\, x = z$, se sustituye finalmente $y \,.\, x$ por y:

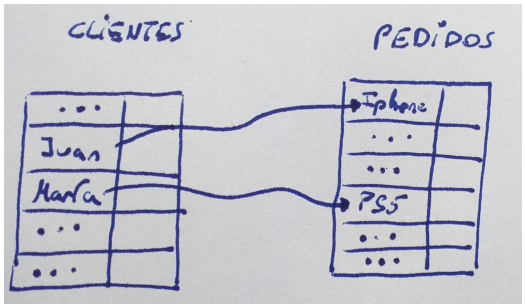
$$(y \,.\, x) \,.\, z = y \,.\, x \Rightarrow y \,.\, z = y$$

$$x \,.\, x = x$$

$$\begin{array}{ll} x \cdot x = x & \Rightarrow \\ x \cdot x - x = 0 & \Rightarrow \text{ sacando factor común} \\ x \cdot (x - 1) = 0 & \Rightarrow \\ x = 0, \text{ o bien } x = 1 & \end{array}$$

RELACIONES BINARIAS

Una relación binaria es una relación entre dos conjuntos, que a su vez es subconjunto del producto cartesiano de los conjuntos que relaciona.



$$R = \{(Juan, Iphone12), (Maria, PS5)\} \subseteq CLIENTES \times PEDIDOS$$

$$S = \{(Juan, Iphone12, 12000), (Maria, PS5, 3004)\} \subseteq CLIENTES \times PEDIDOS \times CUENTAS$$

Definimos el concepto de relación binaria entre los conjuntos A y B como un subconjunto R del producto cartesiano de ambos conjuntos:

$$R \subseteq A \times B$$

Si un par ordenado de los conjuntos de A y B pertenece al conjunto formado por la relación binaria, entonces decimos que xRy y en caso contrario decimos que $x \not R y$.

Definimos el dominio de la relación binaria como:

$$dom(R) = \{x \in A : xRy : \exists y \in B\}$$

Y definimos su imagen o rango como:

$$ran(R) = \{y \in B : xRy : \exists x \in A\}$$

Veamos algunos ejemplos de lo comentado anteriormente:

- Sea $A = \{3, 4, 5, 6\}$ y $B\{2, 3, 4, 5\}$ y $R \subseteq A \times B$

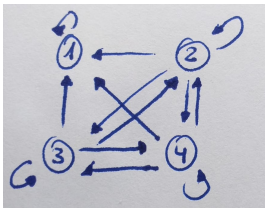
$$xRy \overset{Def.}{\Leftrightarrow} x \leq y : \forall x \in A \land \forall y \in B \Rightarrow R = \{(3,3), (3,4), (3,5), (4,4), (4,5), (5,5)\}$$

$$dom(R) = \{3, 4, 5\} \land ran(R) = \{3, 4, 5\}$$

- Sea $A = B = \{1, 2, 3, 4\}$ y $R \subseteq A^2$:

$$xRy \overset{Def.}{\Leftrightarrow} x^2 \geq y : \forall x, y \in A$$

Para este ejemplo nos podemos ayudar de un grafo que haga visibles las relaciones entre elementos a través de nodos y líneas de unión:



$$dom(R) = \{1, 2, 3, 4\} \land ran(R) = \{1, 2, 3, 4\}$$

- Sea $A = B = \{2, 3, 4, 6\}$ y $R \subseteq A^2$:

$$xRy \overset{Def.}{\Leftrightarrow} x \mid y : \forall x, y \in A$$

$$dom(R) = A \land ran(R) = A$$

- Sea $A = B = \mathbb{R}$ y $R \subseteq R^2$:

$$xRy \overset{Def.}{\Leftrightarrow} |x| + |y| = 1 : \forall x, y \in \mathbb{R}$$

$$dom(R) = [-1, 1] \land ran(R) = [-1, 1]$$

Propiedades de las relaciones binarias

Sea $R \subseteq A^2$, esta cumple las siguientes propiedades:

- **Reflexiva**: $\forall x \in A : xRx$
- **Antireflexiva**: $\nexists x \in A : xRx$
- **Simétrica**: $\forall x, y \in A : xRy \Rightarrow yRx$
- **Antisimétrica**: $\forall x, y \in A : (xRy \land yRx) \Rightarrow x = y$
- **Transitiva**: $\forall x, y, z \in A : (xRy \land yRz) \Rightarrow xRz$
- **Conexa**: $\forall x, y \in A : x \neq y \Rightarrow (xRy \lor yRx)$

Veamos algunos ejemplos:

- Sea $A = \mathbb{N}\backslash\{0\}$ y $R \subseteq A^2$

$$xRy \overset{Def.}{\Leftrightarrow} mcd(x, y) = 1 : \forall x, y \in A$$

1. reflexividad: $xRx : \forall x \in A$?

$$mcd(x,x) = 1 : \forall x \in A \Rightarrow \# \Rightarrow NO$$

2. antireflexividad: $\nexists x \in A : xRx$?

$$\nexists x \in A : mcd(x,x) = 1 \Rightarrow \# \Rightarrow NO$$

3. simetría: $\forall x, y \in A : mcd(x,y) = 1 \Rightarrow mcd(y,x) = 1$?

$$mcd(x,y) = mcd(y,x) = 1 \Rightarrow SI$$

4. antisimetría: $\forall x, y \in A : mcd(x,y) = mcd(y,x) = 1 \Rightarrow x = y$?

$$mcd(a,b) = mcd(b,a) = 1 : \text{a y b primos} \nRightarrow a = b \Rightarrow NO$$

5. transitividad: $\forall x, y, z \in A : mcd(x,y) = 1 = mcd(y,z) \Rightarrow mcd(x,z) = 1$?

$$mcd(4,7) = 1 = mcd(7,2) \text{ , pero } mcd(4,2) \neq 1 \Rightarrow NO$$

6. conexión: $\forall x, y \in A : x \neq y \Rightarrow mcd(x,y) = 1 \vee mcd(y,x) = 1$?

$$2 \neq 4, mcd(2,4) = 1 \wedge mcd(4,2) \neq 1 \Rightarrow NO$$

Operaciones entre relaciones binarias

Sean R y S dos relaciones tal que $R, S \subseteq A \times B$ y la relación binaria $T \subseteq B \times C$.

- **Relación Unión**: $R \cup S = \{(x,y) \in A \times B : xRy \vee xSy\}$
- **Relación Intersección**: $R \cap S = \{(x,y) \in A \times B : xRy \wedge xSy\}$
- **Relación Complemento**: $\overline{R} = \{(x,y) \in A \times B : xRtachadoy\}$
- **Relación Inversa**: $R^{-1} = \{(y,x) \in B \times A : xRy\}$
- **Relación Composición (o producto)**: $R \cdot S = \{(x,z) \in A \times C : \exists y \in B : xRy \wedge ySz\}$
- **Relación Identidad**: $id_A = \{(x,x) \in A \times A : x \in A\}$

Propiedad de las operaciones

Sean $R \subseteq A \times B$, $S \subseteq B \times C$ y $T \subseteq C \times D$

- **Asociatividad**: $R \cdot (S \cdot T) = (R \cdot S) \cdot T$
- **Elemento neutro**: $id_A \cdot R = R \cdot id_A = R$
- **Elemento inverso**[12]: $(R \cdot S)^{-1} = S^{-1} \cdot R^{-1}$

Demostración de la 3:

$z(R{\cdot}S)^{-1}x \Leftrightarrow x(R{\cdot}S)z \Leftrightarrow \exists y : xRy \wedge ySz \Leftrightarrow \exists y : yR^{-1}x \wedge zS^{-1}s \Leftrightarrow \exists y : zS^{-1}y \wedge yR^{-1}x \Leftrightarrow z(S^{-1}{\cdot}R^{-1})x$

[12] NO es conmutativo

FUNCIONES

Las funciones son relaciones binarias. Una relación binaria , $R \subseteq A \times B$, es una función si para todo $a \in A$ existe **a lo sumo** un $b \in B$ tal que aRb:

$$\forall a \in A : (\exists! b \in B : aRb) \vee (\nexists b \in B : aRb)$$

Por ejemplo, $R \subseteq Z \times Z : xRy \overset{def}{\Leftrightarrow} y = x^2$, sí es una función porque $\forall x \in \mathbb{Z} : \exists! y \in \mathbb{Z} : xRy$, pero la función inversa $xR^{-1}y \Leftrightarrow x = y^2 \Leftrightarrow y = \sqrt{x}$, no es función porque hay puntos del dominio que tienen más de una imagen.

Notación, dominio y rango y concepto de función total

Por **notación**, escribiremos $y = f(x)$, donde $f : A \to B$, para referirnos a la relación binaria a la que llamamos función e indicar los conjuntos que relaciona.

Al **dominio** y al **rango** los denotaremos como:

- $dom(f) = \{x \in A : \exists f(x)\} \subseteq A$
- $ran(f) = \{f(x) \in B : x \in dom(f)\} \subseteq B$

Una función $f : A \to B$ es **total** si $dom(f) = A$, por el contrario, $f : A \not\to B$ es **parcial**[13] si $dom(f) \subset A$.

Operaciones con funciones

Definimos las siguientes operaciones:

1. **Restricción de** $f : A \to B$ **a** $C \subseteq A$:
   - $f\mid_C : C \to B$
   - $f\mid_C (x) = f(x) : \forall x \in dom(f) \cap C$
2. **Composición de** $f : A \to B$ **y** $g : B \to C$:
   - $f \circ g : A \to C$
   - $f \circ g(x) = g(f(x)) \Rightarrow \begin{cases} dom(f \circ g) = \{x \in dom(f) : f(x) \in dom(g)\} \\ ran(f \circ g) = \{ran(g\mid_{dom(g) \cap ran(f)})\} \end{cases}$
3. Inversa de una función $f : A \to B$:
   - $f^{-1} = B \to A$
   - $f^{-1}(x) = y \Leftrightarrow f(y) = x$

Propiedades de las operaciones

Sean $f : A \to B$, $g : B \to C$ y $h : C \to D$:

- **Asociativa**: $(f \circ g) \circ h = f \circ (g \circ h)$

[13] También se usa la notación de $f : A \dashrightarrow B$

- **Elemento inverso**[14]: $f \circ f^{-1} = id_A$ ó $f^{-1} \circ f = id_B$
- **Elemento neutro**: $id_A \circ f = f \circ id_B = f$

Que como vemos le otorga a este conjunto junto con la operación composición estructura de cuerpo.

Propiedades de las funciones

Inyectividad

Sean A y B conjuntos y $f : A \to B$ una función, se dice que f es **inyectiva** cuando todo elemento de A posee una imagen distinta de la imagen de cualquier otro elemento de A:

$$\forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$

En la práctica, para calcular si una función es inyectiva o no, tomaremos $f(x_1) = f(x_2)$ y si eso resulta en $x_1 = x_2$ entonces es inyectiva, si no no.

Ej.: "$f(x) = x^2$"

$$f(x_1) = f(x_2) \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1^2 - x_2^2 = 0 \Rightarrow$$

$$\Rightarrow (x_1 - x_2)(x_1 + x_2) = 0 \Rightarrow \begin{cases} x_1 - x_2 = 0 \Rightarrow & x_1 = x_2 \\ x_1 + x_2 = 0 \Rightarrow & x_1 = -x_2 \end{cases} \Rightarrow \text{ no es inyectiva}$$

También se puede coger un elemento y que pertenezca a la imagen, despejar x de $y = f(x)$ y ver si para un mismo y hay varios valores de x:

Ej.: $f : \mathbb{R}^+ \to \mathbb{R}^+ : f(x) = \frac{x^2}{1+x}$

$$y \in im(f) \Rightarrow y = f(x) = \frac{x^2}{1+x} \Leftrightarrow x^2 - yx - y = 0$$

$$x = \frac{y \pm \sqrt{y^2 + 4y}}{2} \text{ pero como } \frac{y - \sqrt{y^2 + 4y}}{2} < 0 \Rightarrow x \notin \mathbb{R}^+ \Rightarrow inyectiva$$

Ej.: "$E = \{x \in \mathbb{R} : 1 \leq x \leq 2\}$, $G = \{y \in \mathbb{R} : 1 \leq y \leq 4\}$ y $f(x) = \frac{1}{x^2}$"

$$f(E)? \to 1 \leq x \leq 2 \Leftrightarrow 1 \leq x^2 \leq 4 \Leftrightarrow 1 \geq x \geq \frac{1}{4} = f(E)$$

$$f^{-1}(G)? \to 1 \leq y = f(x) = \frac{1}{x^2} \leq 4 \Leftrightarrow 1 \geq x^2 \geq \frac{1}{4} \Leftrightarrow 1 \geq |x| \geq \frac{1}{2} \begin{cases} 1 \geq x \geq \frac{1}{2} & \Rightarrow 1 \geq x \geq \frac{1}{2} \\ 1 \geq -x \geq \frac{1}{2} & \Rightarrow -1 \leq x \leq -\frac{1}{2} \end{cases}$$

Suprayectividad

Sean A y B conjuntos y $f : A \to B$ una función, se dice que f es **suprayectiva** o *sobre* cuando todo elemento de B es imagen[15] de algún elemento de A:

$$\forall b \in B : \exists a \in A : f(a) = b$$

En la práctica, para calcular si una función es inyectiva o no, tomaremos $y = f(x)$ y despejaremos x, si y toma como posibles valores los mismos que los valores del codominio, es suprayectiva.

Ej.: "$f(x) = x^2$"

$$y = x^2 \Rightarrow x = \sqrt{y} \Rightarrow y \in (0, \infty)$$

Luego no es suprayectiva porque $f : \mathbb{R} \to \mathbb{R}$

[14] $id_A : A \longrightarrow A : id_A(x) = x$ y análogo con id_B
[15] Lo que se traduce en que $im(f) = B$

Biyectividad

Sean A y B conjuntos y $f : A \to B$ una función, se dice que f es **biyectiva** cuando f es inyectiva y suprayectiva simultáneamente.

Que en el fondo también es decir que $\exists f^{-1}$

CARDINALIDAD

Un conjunto A es FINITO si $\exists n \in \mathbb{N}$ de manera que exista una biyección entre $\{0, 1, ..., n-1\}$ y el conjunto que queremos determinar como finito[16].

En este caso decimos que n es el **cardinal** de A y se representa como $|A|$.

Ej.: $A, B \subseteq \mathbb{N} : A, B$ son infinitos, selecciona la opción correcta:

1. $\mathbb{N} \backslash (A \cup B)$ es finito
2. $A \cap B$ es infinito
3. $A \cup B$ es infinito
4. Ninguna de las anteriores

Consideramos que $A = \{n \in \mathbb{N} : n \text{ es } \dot{3}\}$ y $B = \{n \in \mathbb{N} : n - 1 \text{ es } \dot{3}\}$, esto implica que $\mathbb{N} \backslash (A \cup B) = \{n \in \mathbb{N} : n - 2 \text{ es } \dot{3}\}$ que es infinito. $\Rightarrow 1)\#$

Es fácil ver que $A \cup B$ es infinito, luego $3) \Rightarrow Ok$

Propiedades de los cardinales

El concepto de cardinal que estamos tratando SÓLO es aplicable a CONJUNTOS FINITOS:

- $S \subseteq A \Rightarrow |S| \leq |A|$
- $|A \cup B| = |A| + |B| - |A \cap B|$
- $A \backslash B = |A| - |A \cap B|$
- $|A \times B| = |A| \cdot |B|$
- $|\{f \mid f : A \longrightarrow B\}| = VR^{|A|}_{|B|} = |B|^{|A|}$
- $|P(A)| = 2^{|A|}$

Principio del Palomar

Surge de la situación de meter palomas en huecos de un palomar, si tenemos que meter cada paloma en un hueco y vemos que hay más palomas en huecos, necesariamente algún hueco tendrá más de una paloma.

Volviendo a las matemáticas, lo que queremos decir es que si:

$$f : A \longrightarrow B \wedge |A| > |B| \Leftrightarrow \nexists f \text{ inyectiva}$$

[16] Los conjuntos infinitos son aquellos que no son finitos

Y además esto quiere decir que hay, al menos, $\frac{|A|}{|B|}$ aproximado al entero superior, número de palomas que comparten hueco.

Relaciones de Cardinalidad

Sean A y B dos conjuntos[17], entonces son:

- **Equipotentes**: $A \sim B \Leftrightarrow \exists f : A \longrightarrow B : f$ **biyectiva**, es decir, si son finitos, entonces: $|A| = |B|$.

  Esta relación entre ambos $\sim$ es una RELACIÓN DE EQUIVALENCIA.[18]

- **Dominación**: Se dice que A está dominado por B y se expresa como: $A \leq B \Leftrightarrow \exists f : A \longrightarrow B : f$ **inyectiva**, es decir, si A y B son finitos, entonces $|A| \leq |B|$.

  Esta relación entre ambos $\sim$ es una RELACIÓN DE ORDEN.[19]

  Teorema de Schröeder-Bernstein:

  $$A \leq B \wedge B \leq A \Rightarrow A \sim B$$

- **Dominación estricta**: A está estrictamente dominado por B y se expresa como $A < B$, si está dominado, pero no son equipotentes.

Conjuntos numerables y no numerables

Decimos que un conjunto es **numerable** cuando podemos establecer una biyección entre él y los números naturales, es decir, son equipotentes.[20].

$$A \text{ numerable} \Leftrightarrow A \text{ finito } \vee A \sim \mathbb{N}$$

Como ejemplos vemos que los naturales, los enteros, los racionales, los pares, los impares, los primos, $\mathbb{N}_m$... son numerables.

Propiedades:

Además, tenemos que si $A_i \sim \mathbb{N}$, entonces:

- $\bigcup_{i=1}^{m} A_i \sim \mathbb{N}$
- $\bigcup_{i \in \mathbb{N}} A_i \sim \mathbb{N}$
- $A_1 \times A_2 \times ... \times A_n \sim \mathbb{N}$

Decimos que un conjunto es **NO numerable** cuando no se cumplen las premisas de ser numerable.

$$A \text{ no numerable} \Leftrightarrow A \text{ no es finito } \wedge A \nsim \mathbb{N}$$

Ej.: Demostrar que $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$

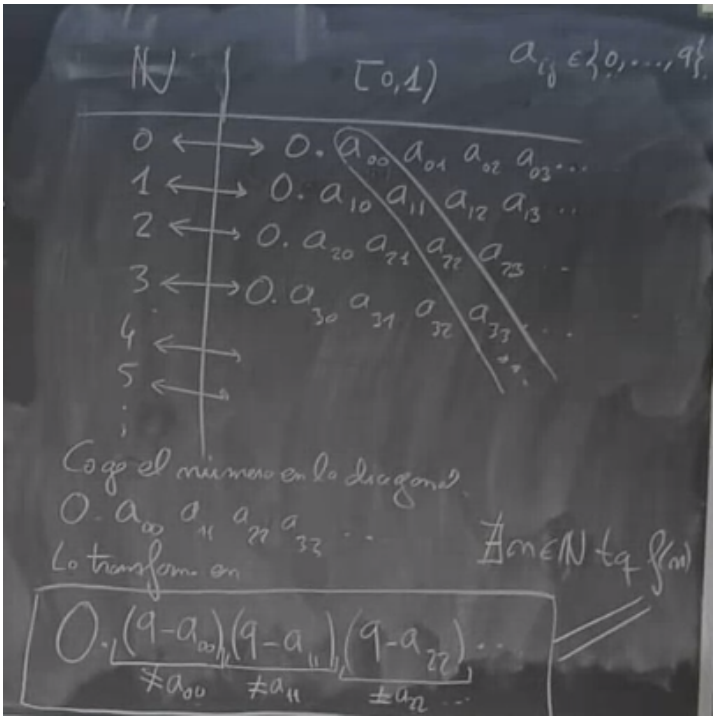
Para estas demostraciones es útil demostrar que uno es dominante sobre el otro y viceversa.Si tenemos que $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ podemos definir la función: $f((n, m)) = 2^n \cdot 3^m$ y vemos que claramente es inyectiva.

En el otro sentido, si tenemos que $g : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ siendo $g(n) = (n, 0)$, vemos claramente que es inyectiva y, en consecuencia, podemos decir que ambos se dominan el uno al otro, lo que implica que son equipotentes.

[17] No necesariamente finitos
[18] Las características de la relación son reflexividad, simetría y transitividad
[19] Las características de la relación son reflexividad, .ªntisimetríaz transitividad
[20] En esta asignatura los conjuntos finitos también los consideramos numerables

Demostración de la NO numerabilidad de los $\mathbb{R}$

Vamos a demostrar que $[0,1) \nsim \mathbb{N}$ y en consecuencia $\mathbb{R} \nsim \mathbb{N}$. Razonamos por reducción al absurdo: supongamos que $[0,1) \sim \mathbb{N} \Rightarrow \exists f : [0,1) \longrightarrow \mathbb{N} : f$ biyectiva



Vemos que si podemos establecer una biyección, entonces a cada natural le puede corresponder un número en el intervalo $[0,1)$. Como son reales, tienen infinitos decimales por lo que yo puedo escribirlos como en la imagen siendo $a_{ij} \in \{0,...,9\}$ y se relación con los naturales como se muestra en la imagen.

Posteriormente, si cogemos la diagonal principal como está rodeada, tenemos que el número formado es el número que se muestra abajo. Si ese número lo transformas de forma que quede la parte encuadrada abajo (que es completamente válido porque sigue siendo un real del intervalo), entonces vemos que este número siempre se diferencia de cada número de la tabla por lo menos en algunas de las cifras. En consecuencia, ya no puede estar emparejado con ninguno de los naturales.

RELACIONES DE EQUIVALENCIA Y ORDEN

RELACIONES DE EQUIVALENCIA

Una relación de binaria $R \subset A \times A$ sobre un conjunto A cualquiera es una relación de equivalencia si es:

- Reflexiva
- Simétrica
- Transitiva

Y en ese caso escribimos $X \sim Y$ en lugar de xRy.

Las relaciones de equivalencia establecen una partición sobre el cuerpo en el que están definidas, dividiendo el mismo en clases de equivalencia y, en consecuencia, haciendo que todos los elemento del cuerpo pertenezcan a una y solo una de las clases de equivalencia definidas.

Clases de equivalencias

Dada una relación de equivalencia "$\sim$" sobre un conjunto A y un elemento $x \in A$ perteneciente al mismo, se define como la **clase de equivalencia** de x como:

$$[x] = \{y \in A : x \sim y\}$$

Propiedades

Definidas las clases de equivalencia, es fácil ver las siguientes propiedades referidas a las mismas:

- $x \in [x]$
- $x \sim y \Leftrightarrow [x] = [y]$
- $x \nsim y \Rightarrow [x] \neq [y] \Rightarrow [x] \cap [y] = \emptyset$

Ej.: En $\mathbb{Z}$, consideramos $xRy \Leftrightarrow x + 3y = \dot{4}$.:

- Reflexiva: $xRx \Leftrightarrow x + 3x = 4 \div 4$
- Simetrica: $xRy \Rightarrow x + 3y = 4k \Rightarrow 4 \mid x \wedge 4 \mid y \Rightarrow y + 3x = 4k + 3 \cdot 4 \cdot k = 4(k + 3k) \Rightarrow yRx$

- Transitiva: fácil de demostrar

Con lo cual, la clase de equivalencia $[4] = \{y \in \mathbb{Z} : 4Ry\} = \{y \in \mathbb{Z} : 4 - 3y = 4k\} \Rightarrow y = \dot{4}$

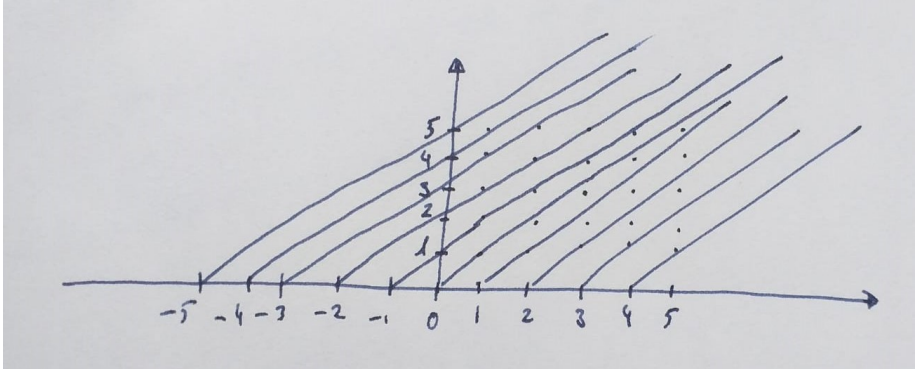
Conjunto cociente

Definimos el conjunto cociente denotado por $A/\sim$ como el conjunto de todas las clases que forman los elementos de A con respecto a esa clase de equivalencia.

$$A/\sim \quad = \{[x] : x \in A\}$$

Por ejemplo, tenemos en las relaciones de congruencia $\mathbb{Z}/n$ donde $\mathbb{Z}/n = \{[0], [1], ..., [n-1]\}$.

Ej.: En $\mathbb{N} \times \mathbb{N}$ definimos $(a, b)R(c, d) \Leftrightarrow a + d = b + c$. Vemos que $(0, 0)R(1, 1)$, $(0, 0)R(2, 2)R...$, también tenemos que $(1, 0)R(2, 1)$.



Es fácil comprobar que es una relación de equivalencia. Entonces, vemos que si prolongamos dichas rectas, cada clase de equivalencia que corresponde a cada una de las rectas. Se puede definir que $\mathbb{N} \times \mathbb{N}/R \sim \mathbb{Z}$; construyendo así los números enteros.

RELACIONES DE ORDEN

Conjuntos ordenados y relación usual de orden

Una relación binaria $R \subset A \times A$ sobre un conjunto A es una **RELACIÓN DE ORDEN**[21] si es:

- Reflexiva
- Antisimétrica
- Transitiva

Además, decimos que se trata de una relación de **ORDEN TOTAL o lineal** si además es:

- Conexa

[21] Ordinario o parcial representado por: $\sqsubseteq$

Llamamos **CONJUNTO ORDENADO** al par $(A, \sqsubseteq)$ formado por el conjunto A sobre el que está definida la relación de orden $\sqsubseteq$ y la propia relación de orden.

- Ej.: $(A, \leq)$, siendo A cualquier conjunto contenido en $\mathbb{R}$ es un conjunto ordenado porque "$\leq$" cumple las premisas de relación de orden. Además, constituye un orden total.
- Ej.: $(\mathbb{N}_1, |)$ también cumple las premisas de conjunto ordenado.
- $(P(A), \subseteq)$ para cualquier conjunto A y la relación de inclusión usual.

Relación de orden estricto

Si tenemos una relación binaria $R \subset A \times A$ sobre un conjunto A, decimos que es un **ORDEN ESTRICTO**[22] si cumple las propiedades:

- Antireflexiva
- Transitiva

Además, decimos que se trata de una relación de **ORDEN ESTRICTO TOTAL o lineal** si además es:

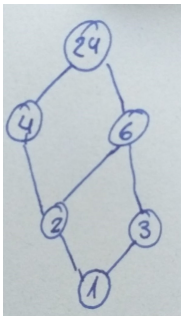
- Conexa

Diagramas de Hasse

Sirven para representar gráficamente[23] conjuntos ordenados. Dado un conjunto ordenado $(A, \sqsubseteq)$ su *diagrama de Hasse* se obtiene mediante el siguiente algoritmo:

- Cada elemento del conjunto A se representa en un vértice
- Se dibuja una linea en dirección ascendente entre los vértices x e y si $x \sqsubseteq y$ y además no hay ningún elemento entre medias de ellos, es decir, $\nexists z \in A : x \sqsubseteq z \sqsubseteq y$

Ej.: Si $A = \{1, 2, 3, 4, 6, 24\}$ y $\sqsubseteq \sim |$, entonces tenemos un conjunto ordenado y su diagrama de Hasse es:



[22] Representado por $\sqsubset$

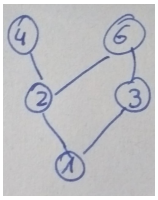
[23] Son útiles para estructuras de datos discretos, por lo que son útiles para conjunto finitos e infinitos numerables porque su representación para conjuntos de mayor cardinal es demasiado compleja y se usan otras estructuras

Elementos especiales de los conjuntos ordenados

Sea $(A, \sqsubseteq)$ un conjunto ordenado y $S \subseteq A$:

- **ELEMENTOS EXTREMOS**:
  - $x \in S$ es el **máximo** de S si $y \sqsubseteq x : \forall y \in S$
  - $x \in S$ es el **mínimo** de S si $x \sqsubseteq y : \forall y \in S$
- **ELEMENTOS EXTREMALES**:
  - $x \in S$ es el **maximal** en S si $\nexists y \in S : x \neq y : x \sqsubseteq y$
  - $x \in S$ es el **minimal** en S si $\nexists y \in S : x \neq y : y \sqsubseteq x$.

Ej.: Consideramos el conjunto ordenado $(A, |)$, donde $A = \{1, 2, 3, 4, 6\}$. Su diagrama de Hasse es:



Sea $S = A$, entonces tenemos que 4 y 6 son maximales, pero sin embargo no existe el máximo porque ningún elemento es mayor que TODOS. El único minimal que existe es el 1, que en este caso coincide con el mínimo. Si solo nos fijamos en el segundo nivel, es decir, $S = \{2, 3\}$, entonces tenemos que existen dos maximales, ningún maximo y dos minimales, pero ningún mínimo.

Del mismo modo, si $(A, \sqsubseteq)$ un conjunto ordenado y $S \subset A$:

- **COTAS**:
  - $x \in A$ es **cota superior** de S si $u \sqsubseteq x : \forall u \in S$. Al conjunto de todas las cotas superiores de un conjunto se le denota por:
    $$Sup(S) = \{x \in A : x \text{ es cota superior de } S\}$$
  - $x \in A$ es **cota inferior** de S si $x \sqsubseteq u : \forall u \in S$. Al conjunto de todas las cotas inferiores de un conjunto se le denota por:
    $$Inf(S) = \{x \in A : x \text{ es cota inferior de } S\}$$
- **SUPREMOS E ÍNFIMOS**:
  - $x \in A$ es **supremo** de S si es el mínimo en la relación de orden "$\sqsubseteq$" definida del conjunto $Sup(S)$:
    $$\bigsqcup S = \text{mín}\, Sup(S)$$
  - $x \in A$ es **ínfimo** de S si es el máximo en la relación de orden "$\sqsubseteq$" definida del conjunto $Inf(S)$:
    $$\bigsqcap S = \text{máx}\, Inf(S)$$

Funciones que conservan el orden

Funciones monótonas

Las funciones que respetan el orden de los elementos a los que se les aplica se llaman **funciones monótonas**, es decir, sean $(A, \sqsubseteq_A)$ y $(B, \sqsubseteq_B)$ dos conjuntos ordenados y la función $f : A \to B$:

$$f \text{ es monótona} \Leftrightarrow \forall x, y \in A : x \sqsubseteq_A y \Rightarrow f(x) \sqsubseteq_B f(y)$$

Funciones que preservan el orden

Son funciones monótonas en las que si se cumple el recíproco de la propiedad que definía el concepto de función monótona.

$$f \text{ conserva el orden} \Leftrightarrow \forall x, y \in A : x \sqsubseteq_A y \Leftrightarrow f(x) \sqsubseteq_B f(y)$$

Isomorfismo y automorfismo de orden

Decimos que una función es un **isomorfimo de orden** si es una función que conserva el orden y además es biyectiva.

Decimos que una función es un **automorfismo** de orden cuando es un isomorfimo y además el conjunto de llegada y de partida es el mismo.

Teorema

Sean $(A, \sqsubseteq_A)$ y $(B, \sqsubseteq_B)$ dos conjuntos ordenados y la función $f : A \to B$ un isomorfismo de orden, entonces:

- $x = \text{máx}\, A \Leftrightarrow f(x) = \text{máx}\, B$
- $x =$ maximal en $A \Leftrightarrow f(x) =$ maximal en B
- $x = \text{mín}\, A \Leftrightarrow f(x) = \text{mín}\, B$
- $x =$ minimal en $A \Leftrightarrow f(x) =$ minimal en B

TEORÍA DE GRAFOS

CONCEPTO DE GRAFO Y TIPOS

Tipos de grafos

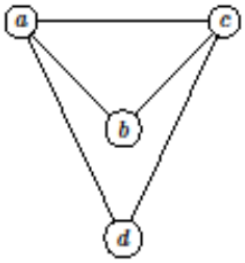
Grafo no dirigido

Un **grafo no dirigido** es un elemento matemático formado por los siguientes elementos:

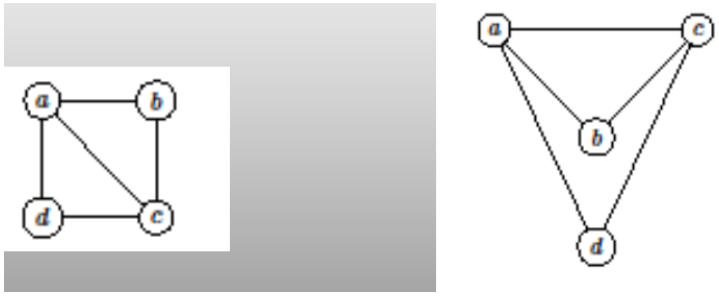
- Conjunto de vértices: $V = \{v_1, ..., v_n\}$ Es el conjunto **finito** formado por todos los elementos que denominamos **vértices**.

- Conjunto de aristas: $E = \{e_1, ..., e_m\}$ es un conjunto finito formado por los subconjuntos de V cuyo cardinal es dos, es decir, cada $e_k = \{v_i, v_j\}$ donde $v_i, v_j \in V : v_i \neq v_j$.

El conjunto formado por los vértices no puede ser el conjunto vacío, pero en cambio el conjunto formado por las aristas sí. Cuando las aristas llevan asignadas un valor o etiqueta decimos que estamos ante un grado valorado.



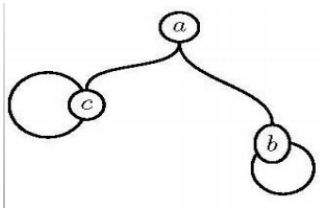
Un mismo grafo puede tener distintas representaciones, pero representar la misma información. En ese caso, decimos que son isomorfos.



Es fácil destacar que para referirnos a una arista en este tipo de grados es indiferente el orden en el que nombre los vértices que conecta puesto que al tratarse de un grafo no dirigido, hemos definido cada arista como un subconjunto de cardinal dos, así pues $\{v_i, v_j\} = \{v_j, v_i\}$.

Pseudografos

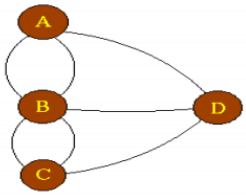
Cumplen la definición ordinaria que se ha dado de grafo, a excepción de que en este caso se permiten las **autoaristas**, es decir, que suprimimos la condición de que $v_i \neq v_j$ para la autoarista $e = \{v_i, v_j\}$.



A estas aristas se las conoce como lazos o bucles.

Multigrafos

Reúnen todas las condiciones anteriores, con la única excepción de que entre dos vértices puede haber más de una arista.



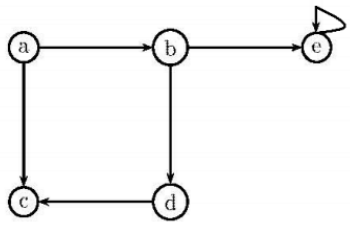
Es decir, a pesar de que las aristas unen mismos vértices hay que llamarlas de forma distinta porque representan caminos distintos entre ambos puntos.

Grafo dirigido

Los grafos dirigidos reúnen las mismas características y peculiaridades de los grafos no dirigidos, a excepción de que en este caso las aristas poseen dirección y pasan a llamarse **arcos**. Con lo cual podemos decir que poseen los siguientes elementos:

- Conjunto de vértices: $V = \{v_1, ..., v_n\}$
- Conjunto de arcos: $A = \{(v_i, v_j), ...\}$

  Es decir, en este caso los arcos representan la relación de adyacencia entre dos vértices. Cuando uAv decimos que el arco está orientado desde el origen u hasta el destino v y que el destino v es adyacente al origen u. Como relación que es, ahora en vez de ser subcojuntos de V son **pares** de V.



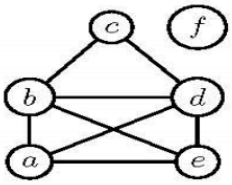
Grado de un vértice: adyacencia

Decimos que dos vértices son adyacentes o vecinos si existe una arista que los une. En ese caso los vértices son los extremos[24] de la arista.

$$uAv \Leftrightarrow \exists a = \{u, v\} \in E$$

El **grado de un vértice** es el número de aristas[25] que inciden sobre él. Cuando un vértice posee grado 0 se le llama aislado y en los **GRAFOS NO DIRIGIDOS** el grado es sinónimo del número de vértices adyacentes.

En los grafos dirigidos, distinguimos entre **grado de entrada** ($gr^-(v)$): número de aristas de las que es origen el vértice y **grado de salida**($gr^+(v)$): número de aristas de las que es destino.



gr(a) = gr(e) = 3
gr(b) = gr(d)= 4
gr(f) = 0 (vértice aislado)
gr(c) = 2

Teorema de los apretones de manos

Sea G un grafo, entonces se tiene que el sumatorio de los grados es el doble del número de aristas:

$$\sum_{v \in V} gr(v) = 2|E|$$

Demostración:

La demostración es sencilla, puesto que si una arista conecta dos vértices y el grado de un vértice es el número de aristas que inciden sobre él, se tiene que al sumar los grados de cada vértices, las aristas que unen dos se cuentan dos veces.

Corolario:

[24] Si v es extremo de la arista a se dice que a incide en él
[25] En los pseudografos, las autoaristas cuentan dos veces como arista incidente

Es evidente de forma inmediata que cualquier grafo dirigido tiene un número par de vértices de grado impar.

Teorema

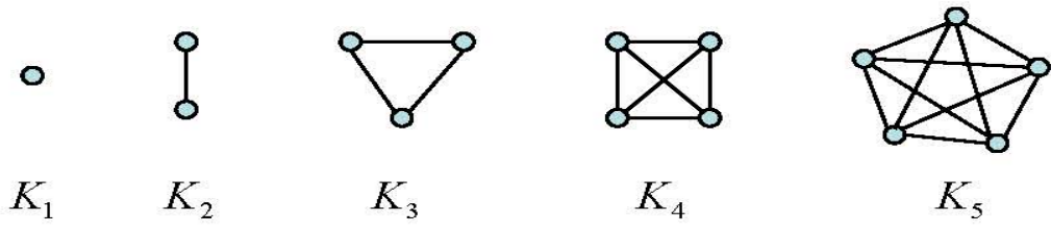
El mismo teorema pero para grafos dirigidos nos dice que:

$$\sum_{v \in V} gr^{+}(v) + \sum_{v \in V} gr^{-}v = |A|$$

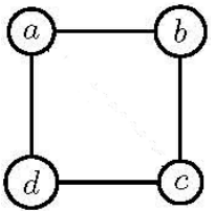
Que se ve de forma evidente que entendiendo la demostración del anterior, este es cierto.

Grafo completo y regular

Para un número de vértices mayor que 1, se dice que un **grafo es completo de orden** n si cada par de vértices escogidos son adyacentes.

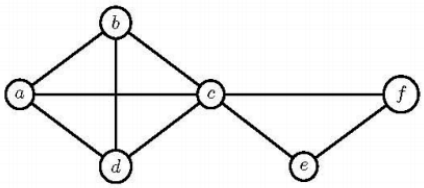


Se llama **grafo regular de grado** $K \geq 0$ o grafo $K-$regular a los grafos cuyos vértices poseen todos grado K.



Matriz de Adyacencia

Para representar las relaciones que existen en un grafo entre los distintos vértices del mismo se puede utilizar lo que denominamos **matriz de adyacencia**.



$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

En esta matriz, las filas y las columnas son los vértices (en el mismo orden) y un uno en cierta coordenada significa que los vértices columna y fila están relacionados por medio de una arista.

Es fácil observar que las matrices en **grados no dirigidos** serán simétricas y su diagonal será 0 (si no se permiten los pseudografos). No ocurre esto con los grafos dirigidos, en los que por convenio se tiene que las filas representan los vértices origen y las columnas los vértices destino, por lo que ya no se guarda esta relación de simetría entre ambos.

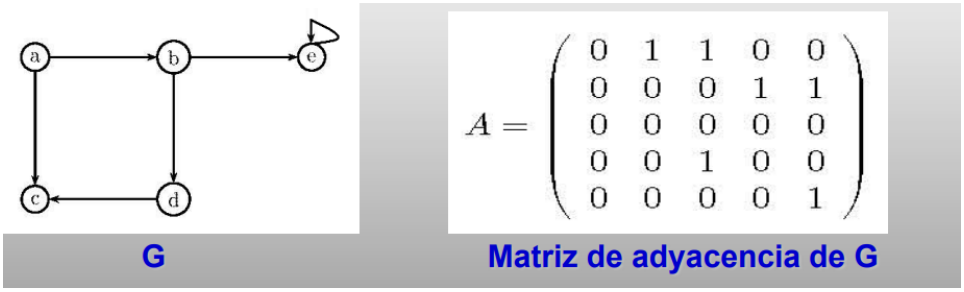
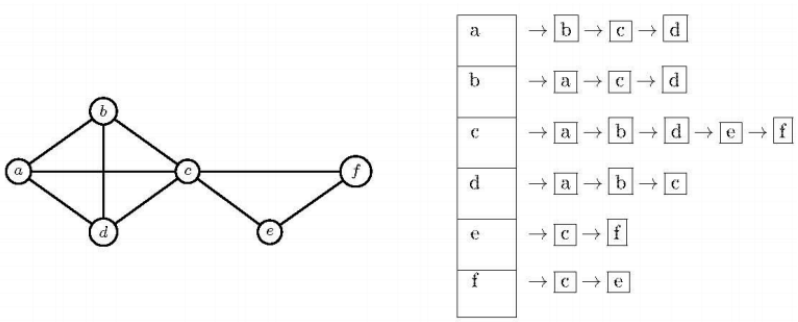
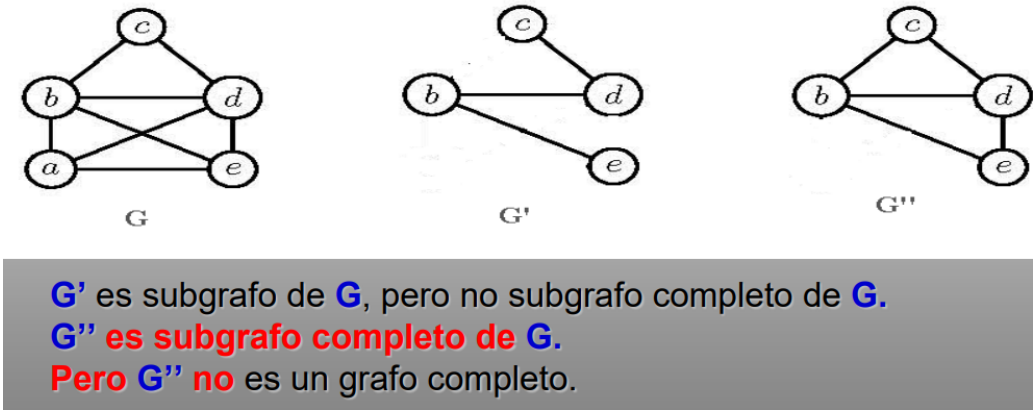


Tabla de adyacencia



Subgrafos

Dado un grafo $G = (V, E)$ y otro $G' = (V', E')$ se dice que G' es un subgrafo de G si $V' \subset V$ y $E' \subset E$, es decir, si es un subconjunto del grafo principal.



Además se llama subgrafo completo si el subgrafo posee todas las aristas que conectan los vértices del subgrafo en el grafo principal.

CAMINOS Y CONECTIVIDAD

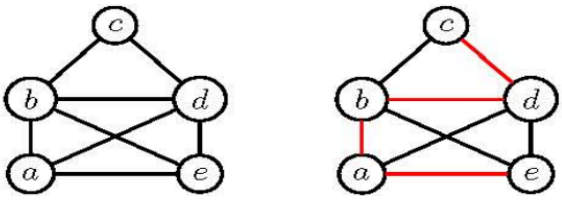
Movimientos por el grafo

Recorridos y circuitos

Un **recorrido**[26] es una sucesión de vértices del grafo que **permite la repetición de vértices y aristas**:

$$R = \{v_0, ..., v_n\} : \{v_i, v_{i+1}\} \in E$$

Decimos entonces que el recorrido conecta el vértice inicial con el final, que su longitud es n y cabe destacar que aunque el recorrido vaya por el mismo "sendero" no es lo mismo ir de c a e que al revés, es decir, son recorridos distintos.



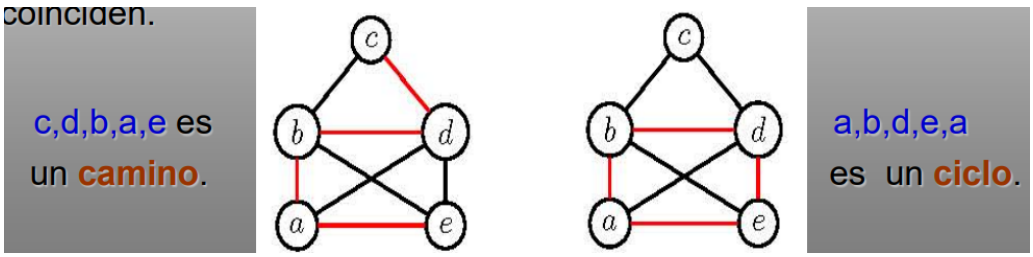
Por otro lado, cuando un **recorrido comienza y termina en el mismo sitio** se le llama **circuito**.

Caminos y ciclos

Un **camino** es un recorrido que no permite repetir ni vértices ni aristas (salvo el primero y el último):

$$C = \{v_0, ..., v_n\} : v_i \neq v_j : \forall 0 < i < j < n$$

Cuando un **camino comienza y termina en el mismo vértice**se le conoce como **ciclo**.



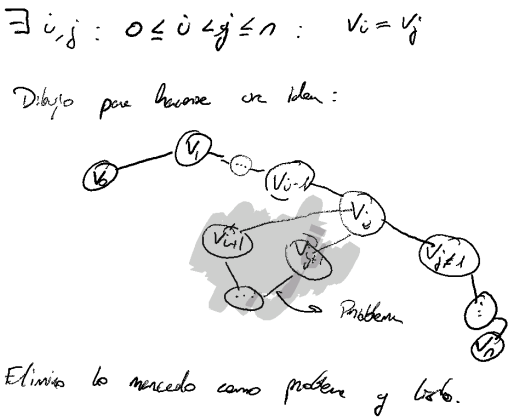
Teorema: de cualquier recorrido se puede extraer un camino:

$$\forall x, y \in V : \exists R = \{x, ..., y\} \Leftrightarrow \exists C = \{x, ..., y\}$$

Demostración:

Si directamente tenemos el camino ya hemos acabado, en caso contrario lo que ocurre es que hay vértices se repiten más de una vez, con lo cual podemos simplificar el problema al siguiente dibujo:

[26] Los conceptos explicados en este apartado son aplicables a los grafos dirigidos teniendo en cuenta que las aristas ahora poseen dirección

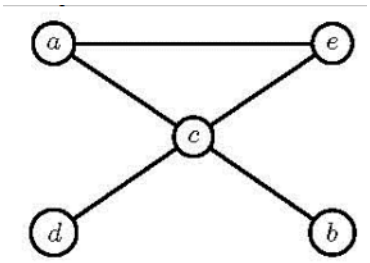


La implicación de derecha a izquierda es trivial por la propia definición de camino, para la otra implicación la idea es que se puedan "cortar" esos flecos del dibujo para poder extraer el recorrido limpio.

Grafo Conexo

Si definimos la relación $C \subset V^2$, en un grafo no dirigido, de manera que dos vértices están conectados si y sólo si existe un camino entre ambos, esto define una relación de equivalencia[27] en V:

- Reflexiva:
$$aCa \Leftrightarrow C = \{\emptyset\}$$
- Simétrica:
$$aCb \Rightarrow C_1 = \{a, ..., b\} \Rightarrow C_2 = \{b, ..., a\} \Rightarrow bCa$$
- Transitividad:
$$\begin{cases} xCy \Rightarrow \exists C_1 = \{x, ..., y\} \\ yCz \Rightarrow C_2 = \{y, ..., z\} \end{cases} \Rightarrow \exists R = \{x, ..., y, ..., z\} \overset{Teorema}{\Rightarrow} \exists C = \{x, ..., y, ..., z\}$$



Decimos entonces que un **grafo es conexo** si y solo si para cada par de vértices del grafo siempre existe un **camino entre ambos**, es decir, que el conjunto cociente tiene sólo un elemento. Una buena forma de demostrar esta propiedad en un grafo es construir un recorrido que pase por todos los vértices y por el teorema de la parte de caminos, siempre podremos extraer un camino entre dos vértices.

Proposición:

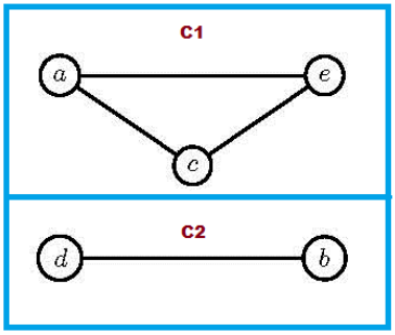
Una consecuencia es que si un grafo es conexo entonces si tiene n vértices tiene como mínimo $n-1$ aristas.

[27] En general en los grafos dirigidos no forma una relación de equivalencia

Componentes conexas, puntos de corte y aristas puente

Componentes conexas:

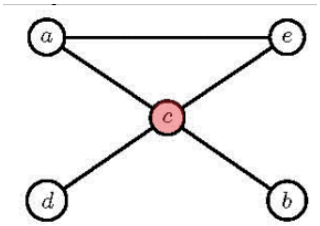
Cada clase de equivalencia del conjunto cociente definido se denomina **componente conexa**, es decir, son los mayores subgrafos conexos del grafo principal.



Si el grafo es conexo solo existe una clase de equivalencia y en consecuencia una componente conexa, pero si no lo es entonces existirán más componentes conexas[28].

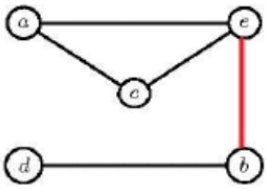
Puntos de corte:

Denominamos puntos de corte a aquellos puntos que tras ser eliminados junto con las aristas que inciden en él, divide al grafo en más componentes conexas.



Aristas puentes

Definimos las aristas puente como las aristas que si se eliminan descomponen el grafo en más componentes conexas, o dicho de otra manera, en dos subgrafos no conectados entre ellos.



Lemas de caracterización

En un grafo conexo, $v \in V$ es un **punto de corte** si existen dos puntos para los que cualquier camino que escoja y que conecte a ambos contiene necesariamente al punto de corte:

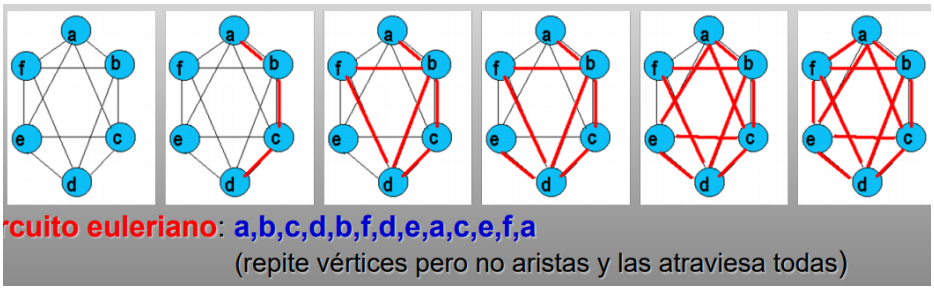
$$\exists x, y \in V : \forall C = \{x, ..., y\} : v \in C$$

[28] A los vértices aislados se les llama componentes conexas triviales

En un grafo conexo, $e \in E$ es una **arista puente** si y sólo si no se encuentra contenida en ningún ciclo posible del grafo.

Grafos eurelianos

Cuando un circuito pasa por todas las aristas de un grafo sin repetir ninguna se lo conoce como **circuito eureliano**. A los grafos que los contienen se los denomina **grafos eurelianos**.



Cuando lo que se consigue no es un circuito sino un recorrido eureliano se dice que el grafo es un **grafo semieureliano** y es condición excluyente de ser eureliano, es decir, o se es eureliano o se es semieureliano pero uno no es un caso particular del otro.

Teorema de Euler

Un grafo es eureliano si y solo si es conexo y todos su vértices son de grado par:

$$eureliano \Leftrightarrow \text{conexo} \ \wedge \forall v \in V : gr(v) = 2k : k \in \mathbb{N}$$

Un grafo es semieureliano si y solo si es conexo y todos sus vértices son de grado par salvo únicamente dos de grado impar:

$$semieureliano \Leftrightarrow \text{conexo} \ \wedge \forall v \in V \backslash \{v_i, v_j\} : gr(v) = 2k : gr(v_i) \neq 2k \neq gr(v_j)$$

Demostración:

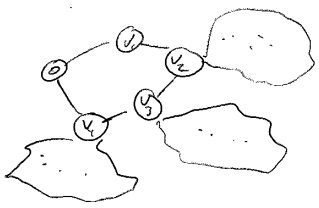
Se pueden usar métodos algebraicos pero en el fondo es liar la demostración. Si pensamos que este tipo de circuitos no pueden repetir aristas, cada vez que entramos por una arista en un vértice tiene que existir otra por la que se pueda salir para no usar por la que se ha venido, es decir, que el grado de todos los vértices tiene que ser par. En caso de que solo halla dos vértices que sean de grado impar, quiere decir que en uno de ellos se comienza y en el otro se termina pues esa arista de más es para empezar el recorrido o para terminarlo.

Búsqueda de circuitos eurelianos

Aunque la caracterización de un grafo eureliano es simple, la búsqueda de dicho recorrido puede ser tediosa, por lo que se presenta el siguiente algoritmo:

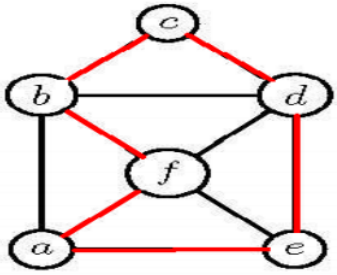
1. Escogemos un circuito cualquiera
2. Borramos las aristas de ese circuito del grafo y nos queda otro subgrafo que estará dividido en varias componentes conexas.
3. Dentro de estas componentes buscamos circuitos eurelianos y si son muy complejas lo tratamos como si fuese otro grafo volviendo al punto 1

4. Cuando hemos encontrado los pequeños circuitos eurelianos en cada componente y solo se usan las aristas de esa componente, podemos "pinchar" esos circuitos en el circuito del inicio sin que haya ningún problema.



Grafos Hamiltonianos

Cuando un ciclo pasa por todos los vértices de un grafo sin repetir ninguno se lo conoce como **ciclo hamiltoniano**. A los grafos que los contienen se los denomina **grafos hamiltonianos**.



Condiciones necesarias y suficientes

Sin embargo, para este problema no se conoce ningún teorema que caracterice a este tipo de grafos como ocurre con los eurelianos. Pero si que existen una serie de condiciones que son necesarias o suficientes para poder descartar casos.

Condiciones necesarias

- Conexo.
- No puede tener vértices de grado 1. Si tiene más de un vértice, todos sus vértices son de grado ≥ 2.
- No puede tener puntos de corte.
- No puede tener aristas puente.

Condiciones suficientes

- Teorema de Dirac:

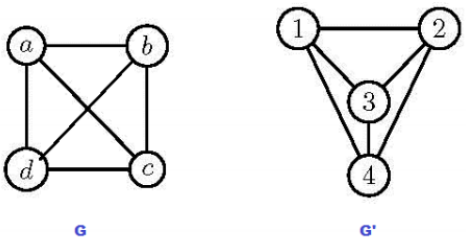
$$|V| \geq 3 : \forall v \in V : gr(v) \geq \frac{n}{2} \Rightarrow HAMILTONIANO$$

- Teorema de Ore:

$$|V| \geq 3 : \forall u, v \in V : \nexists e = \{u, v\} \in E : gr(u) + gr(v) \geq n \Rightarrow HAMILTONIANO$$

Isomorfismo de grafos

Decimos que dos grafos son isomorfos cuando existe una función biyectiva entre los vértices que preserve la adyacencia.



Es decir, que si tirásemos de los vértices, como si se hubiesen liado las aristas, hasta colocar los vértices de la misma forma resultaría que salvo los nombres ambos serían el mismo grafo.

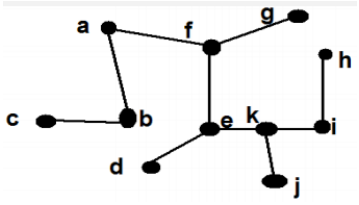
Condiciones necesarias

Lamentablemente, no existe ningún teorema que caracterice a estos grafos por lo que solo basta con conformarse con una serie de condiciones que descartan casos que comprobar:

- Mismo número de vértices.
- Mismo número de aristas.
- Mismo número de vértices con un mismo grado n.
- Si uno de los grafos tiene como subgrafo a K_n (salvo renombramiento de vértices), lo mismo debe suceder en el otro grafo.
- Si uno de los grafos es euleriano o hamiltoniano o conexo el otro también ha de serlo.
- Si en uno de los grafos hay un ciclo de longitud n, lo mismo debe suceder en el otro grafo.
- En general, no diferir en alguna propiedad que preservan las biyecciones que preservan la adyacencia.

Árboles

Un árbol es un grafo no dirigido y conexo sin ciclos no triviales (que no sean de longitud 0). Cuando destacamos un vértice sobre los demás, llamamos a este raíz.



Propiedades

Cualquier árbol tal y como lo hemos definido cumple las siguientes propiedades:

- Entre cada par de vértices de T hay un camino único
- Toda arista de T es una arista puente. Al eliminar cualquier arista de T se desconecta el árbol es dos componentes conexas que son a su vez árboles.
- $|E| = |V| - 1$

Además si un árbol tiene raíz podemos distinguir en él las siguientes partes:

- A los vértices se les llaman habitualmente **nodos**.
- El **nivel** de un nodo es la longitud del camino desde la raíz del árbol a dicho nodo. Por tanto el nivel de la raíz es 0.
- Se llaman **hijos** de un nodo x de nivel i a los nodos de nivel $i + 1$ adyacentes a x.
- Todo nodo es **padre de sus hijos**.
- Los hijos de un mismo padre son **hermanos**.
- La raíz es el único nodo que no tiene padre.
- Se llaman **hojas a los nodos sin hijos**. Se llaman **nodos internos** a los demás.
- Las **ramas** del árbol son los caminos desde su raíz a las hojas.
- La **altura (o talla)** del árbol es la longitud de su rama más larga.

COMBINATORIA

En este tema vamos a estudiar la combinatorio, entre cuyas aplicaciones está el determinar de forma precisa el cardinal de un conjunto determinado. Por lo que consiste básicamente en métodos de conteos de distintas cosas.

MÉTODOS DE CONTEO

Principios elementales del conteo

El método general para el recuento concreto de casos será:

- Definir un conjunto S que contendrá a todas las posibilidades.
- Calcular $|S|$ utilizando los métodos de conteo.

Para realizar estas labores de cuantificación, podemos tener en cuenta las siguientes reglas aplicadas para conjuntos FINITOS:

- **Inclusión**:
$$S \subset A \Rightarrow |S| \leq |A|$$
- **Principio de inclusión-exclusión**
$$|A \cup B| = |A| + |B| - |A \cap B|$$
- **Exclusión**:
$$|A \backslash B| = |A| - |A \cap B|$$
- **Regla del Producto**:
$$|A \times B| = |A| \cdot |B|$$
- **Asignaciones posibles**:
$$|(A \to B)| = |B|^{|A|}$$
- **Biyección**:
$$\exists f : A \to B \text{ biyectiva} \Rightarrow |A| = |B|$$
- **Conjunto de Partes**:
$$|P(A)| = 2^{|A|}$$

Recuento por filas y columnas

En ocasiones, será conveniente representar el conjunto del que queremos hallar el cardinal como una relación binaria sobre dos subconjuntos del mismo, es decir, $R \subset X \times Y$. Definimos ahora:

$$x_0 \in X : y_0 \in Y \Rightarrow \begin{cases} F_{x_0} = R \cap (\{x_0\} \times Y) \\ C_{y_0} = R \cap (X \times \{y_0\}) \end{cases}$$

Es decir[29], para cada coordenada de la fila definimos el conjunto F_{x_0} que representa el número de pares que tienen a x_0 por primera coordenada y de forma análoga con y_0 y C_{y_0}.

Ahora si llamamos $\mathbb{R} = \{R : R \subset X \times Y\}$ al conjunto de todas las posibles relaciones binarias de ese conjunto, las aplicaciones:

$$\begin{cases} f_{x_0} : \mathbb{R} \to \mathbb{N} & \text{donde } f_{x_0}(R) = |F_{x_0}(R)| \\ c_{y_0} : \mathbb{R} \to \mathbb{N} & \text{donde } c_{y_0}(R) = |C_{y_0}(R)| \end{cases}$$

Asignan a cada relación binaria y a cada elemento de cada conjunto, el cardinal de su fila o de su columna respectivamente (es decir, es lo mismo que lo explicado arriba pero asignando el valor en función de la relación definida).

De este modo es trivial que:

$$|R| = \sum_{x_0 \in X} f_{x_0}(R) = \sum_{y_0 \in Y} c_{y_0}(R)$$

Y a modo de corolario, si $\forall x_0 \in X : f_{x_0}(R) = \lambda$ y $\forall y_0 \in Y : c_{y_0}(R) = \varphi$, entonces:

$$|R| = \lambda|X| = \varphi|Y|$$

CÁLCULO DE AGRUPACIONES

Variaciones, combinaciones, permutaciones...

Cuando escogiendo elementos de un conjunto hacemos grupos en determinadas condiciones, surge la pregunta de: ¿Cuántos grupos distintos podré formar? Para poder responder adecuadamente esta pregunta hace falta tener en cuenta las condiciones en las que se forman esos grupos y qué se considera distinto en cada caso.

Variaciones sin repetición

Llamamos **variaciones sin repetición** de n elementos tomados de m en m y lo denotamos por V_m^n a los distintos grupos que se pueden hacer SIN REPETIR LOS ELEMENTOS DEL CONJUNTO A REPARTIR, tomándolos de m en m y teniendo en cuenta que para mismos elementos en un grupo pero órdenes distintos, las asociaciones son distintas, es decir, $abc \neq bca$ aunque posean los mismos elementos.

Para dar respuesta a este problema, nos preguntamos cuál es el cardinal del conjunto de las funciones inyectivas que van de un conjunto $|N| = n$ a otro $|M| = m$:

$$V_m^n = |m \hookrightarrow n| = \prod_{i=1}^{m}(n - i + 1) = \frac{n!}{(n-m)!}$$

Por convenio tenemos que $n < m \Rightarrow V_m^n = 0$ y que $m = 0 \Rightarrow V_m^n = 1$.

[29] De forma gráfica se puede ver como el número de puntos que hay (pares) en la vertical de un punto del eje x

Permutaciones sin repetición

Las **permutaciones sin repetición** son un caso concreto de las variaciones sin repetición donde $m = n$, es decir, la única diferencia es en qué orden se encuentran los elementos puesto que todos los conjuntos poseen a todos los posibles elementos. En este caso y aplicando la fórmula de antes:

$$V_n^n = \frac{n!}{(n-n)!} = n!$$

Variaciones con repetición

Llamamos **variaciones con repetición** de n elementos tomados de m en m y lo denotaremos por VR_m^n a los distintos grupos que podemos formar agrupando n elementos de m en m PUDIENDO SELECCIONAR EL MISMO ELEMENTOS MÁS DE UNA VEZ pero distinguiendo agrupaciones distintas para órdenes distintos.

En este caso la pregunta es ¿cuántas funciones totales hay de un conjunto $|N| = n$ a otro $|M| = m$?

$$VR_m^n| = (m \hookrightarrow n)| = n^m$$

Combinaciones sin repetición

Las combinaciones son variaciones en las que no importa el orden de los elementos escogidos, es decir, nos preguntamos por el número de subconjuntos del conjunto de índices a escoger cuyo cardinal es el especificado. Concretamente, las **combinaciones sin repetición** son aquellas en las que NO SE PUEDE ESCOGER AL MISMO INDIVIDUO MÁS DE UNA VEZ Y SE DEBEN FORMAR GRUPOS DEL CARDINAL ESPECIFICADO.

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

Propiedades:

1. $\forall n, m \in \mathbb{N} : n < m \Rightarrow \binom{n}{m} = 0$
2. $\forall n \geq 0 : \binom{n}{0} = \binom{n}{n} = 1$
3. $\forall n \geq 0 : \binom{n}{1} = n$
4. $\forall n, m \in \mathbb{N} : \binom{n}{m} = \binom{n}{n-m}$
5. $\forall n, m \in \mathbb{N} : \binom{n-1}{m-1} + \binom{n-1}{m}$
6. $\sum_{m=0}^{n} \binom{n}{m} = 2^n$
7. $\sum_{m=0}^{n} (-1)^m \binom{n}{m} = 0$

Combinaciones con repetición

De nuevo, hablamos de variaciones en las que no importa el orden de los elementos escogido, pero con la novedad de que en las **combinaciones con repetición** SE PUEDE ESCOGER EL MISMO INDIVIDUO MÁS DE UNA VEZ.

$$\left[\begin{matrix} n \\ m \end{matrix}\right] = \binom{n+m-1}{m}$$

Demostración:

La demostración de dicho resultado es porque podemos considerar cada posible combinación como una palabra binaria (formada por 0 y 1) de la siguiente forma:

$$\overbrace{111\cdots1}^{k_1}\ 0\ \overbrace{11\cdots1}^{k_2}\ 0\cdots0\ \overbrace{11\cdots1}^{k_n}$$

Donde cada k_i es el número de veces que se repite cada elemento y cada 0 es un separador de elementos; los 1 corresponden al elemento que se repite k_i veces. De este modo, el problema queda reducido al cálculo del número de palabras binarias de longitud $n+m-1$ porque tenemos m elementos útiles y $n-1$ separadores.

Teorema Binomial

Más conocido como el binomio de Newton afirma que:

$$\forall n \in \mathbb{N} : (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

Es decir, que podemos calcular la potencia enésima de cualquier suma gracias a esta fórmula. La demostración es sencilla por inducción.

Principio de Inclusión-Exclusión

A pesar de que se ha visto la forma simplificada para 2 conjuntos anteriormente, este es una generalización para n conjuntos:

Sean $A_0, A_1, \ldots, A_{n-1}$ conjuntos finitos, podemos definir α_i como la suma de los cardinales de todas las intersecciones de i conjuntos de los n que hay, es decir:

$$\alpha_i = \sum_{I \subseteq n : |I| = i} |\bigcap_{j \in I} A_j|$$

De este modo, para calcular el cardinal de la unión de todos los conjuntos basta con atenerse a:

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} (-1)^{i-1} \alpha_i$$

Es decir, que tenemos que sumar o restar las sucesivas intersecciones 2 a 2, 3 a 3, 4 a 4, etc. al total.

Teorema Multinomial

Repartos ponderados

Dados $X = \{a_1, a_2, \cdots, a_n\}$ y $k \in \mathbb{N} \setminus \{0\}$ se define el reparto ponderado como el reparto de los n elementos del conjunto X en k subconjuntos $C_i \subseteq X : |C_i| = m_i,\ 1 \leq i \leq k$ de forma que la suma de los cardinales de todos sea el cardinal total, es decir, $\sum_{i=1}^{k} m_i = n$.

Permutaciones circulares

LÓGICA PROPOSICIONAL

DEFINICIÓN Y LENGUAJE DE LA LÓGICA

La lógica estudia la fundamentación del concepto de certeza y todo lo que esta involucra, además estudia las reglas del pensamiento y de la argumentación válida para poder discernir cuando es o no un pensamiento correcto y cuando es cierta la deducción de unas conclusiones a partir de ciertas premisas.

Sintaxis de la lógica proposicional

Alfabeto de la lógica proposicional

En primer lugar, hemos de hacer una distinción entre el lenguaje natural (que admite ambigüedades) y el lenguaje de la lógica (que no las admite) por lo que será necesario disponer de una serie de símbolos que no dejen espacio a la interpretación, es decir, nuestro lenguaje va a estar formado por:

- **Símbolos lógicos**: $\{\bot, \top, \neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$
  - **Constantes lógicas**: $\{\bot, \top\}$: Indican la falsedad o veracidad respectivamente.
  - **Conectivas unarias**: $\{\neg\}$: Define la relación de negación vista en el apartado de lógica elemental visto en este libro.
  - **Conectivas binarias**: $\{\wedge, \vee, \rightarrow, \leftrightarrow\}$: Definen las relaciones de "y", "o", implicación y equivalencia vistas en el apartado de lógica elemental de este libro.
- **Símbolos auxiliares**: $\{(,)\}$

  Son símbolos que denotan la precedencia de operaciones
- **Signatura**: $\{\Sigma\}$

  Denota al conjunto de símbolos de proposición. La base del estudio de la lógica proposicional son las **proposiciones**. Estas son oraciones declarativas que o bien es cierta o bien es falsa, pero que no admite ambigüedades. Dentro de las proposiciones podemos distinguir:
  - **Proposiciones atómicas**:

    Las denotamos por letras minúsculas y no se pueden descomponer en otras más simples, p. ej., $p =$"Mario compró un coche" es una proposición atómica.
  - **Proposiciones compuestas**:

    Estas proposiciones son las que están formadas por proposiciones atómicas y por las relaciones que podamos establecer entre ellas a través de conectivas lógicas.

Con lo cual, definimos el alfabeto sobre el que vamos a trabajar como:

$$A_\Sigma = \Sigma \cup \{\bot, \top, \neg, \wedge, \vee, \rightarrow, \leftrightarrow\} \cup \{(,)\}$$

De modo análogo, definimos el conjunto de todas las posibles palabras que podemos formar sobre este alfabeto como:

$$A_\Sigma^*$$

Lenguaje de la lógica proposicional

Sin embargo, no todas las palabras que formemos sobre el alfabeto definido como A_Σ tienen sentido. Como sabemos que lo único que tiene algún sentido y está bien construido son las proposiciones atómicas, hay que definir de alguna forma unas **reglas de formación** que permitan determinar qué palabras tienen sentido, a las que llamaremos fórmulas:

- Las proposiciones atómicas y las constantes lógicas son fórmulas.
- Si φ es una fórmula, entonces $\neq \varphi$ es una fórmula
- Si φ_1 y φ_2 son fórmulas, entonces $\varphi_1 \wedge \varphi_2$ es una fórmula.
-
- Si φ_1 y φ_2 son fórmulas, entonces $\varphi_1 \vee \varphi_2$ es una fórmula.
- Si φ_1 y φ_2 son fórmulas, entonces $\varphi_1 \rightarrow \varphi_2$ es una fórmula.
- Si φ_1 y φ_2 son fórmulas, entonces $\varphi_1 \leftrightarrow \varphi_2$ es una fórmula.

De este modo, dada una signatura Σ concreta, queda determinado por completo el lenguaje válido con el que vamos a trabajar y que vamos a denotar por L_Σ: el conjunto de todas las fórmulas con signatura Σ. A estas fórmulas válidas las denotamos por letras griegas usualmente $\varphi, \psi, \xi, ...$

Principio de Inducción Estructural

Dada una propiedad P concreta, la demostración de que esa propiedad se atiene a todas las fórmulas definidas en nuestro lenguaje de la lógica es correcta si verificamos:

- **Caso base**

  Toda fórmula atómica tiene la propiedad P
- **Pasos inductivos**
  - **Negación** $(\neg\varphi)$: sabiendo que la fórmula φ posee la propiedad P, demostrar que $\neg\varphi$ también tiene dicha propiedad.
  - **Conectiva** $(\varphi_1 \square \varphi_2)$: sabiendo que φ_1 y φ_2 la poseen, demostrar que $\varphi = \varphi_1 \square \varphi_2$ la posee también.

Principio de Unicidad Estructural

Podemos determinar de modo único el proceso de construcción que ha seguido una fórmula hasta llegar hasta la expresión sintáctica que la representa. Esto permite definir una biyección entre la estructura sintáctica asignada y el significado de la fórmula.

Toda fórmula φ cae dentro de uno de los siguientes casos:

- Es atómica.
- Es la negación de otra fórmula $\varphi = \neg\varphi_1$.
- Es la composición por medio de una conectiva de otras dos fórmulas $\varphi = \varphi_1 \square \varphi_2$.

Principio de Recursión Estructural

Dado un conjunto A y una función $f : L_\Sigma \to A$ permite definir de modo único el valor de una fórmula a partir de sus proposiciones atómicas.

- **Caso base**

  Si φ es atómica entonces $f(\varphi) =$ valor dependiendo de f

- **Pasos inductivos**

  - **Negación ($\neg\varphi$)**: siempre que una fórmula sea negación de otra se tiene que $f(\neg\varphi) =$ valor dependiendo de $f(\varphi)$
  - **Conectiva ($\varphi_1 \square \varphi_2$)**: siempre que una fórmula sea la unión por medio de una conectiva de otras se tiene que $f(\varphi) =$ valor dependiendo de $f(\varphi_1)$ y $f(\varphi_2)$

Semántica de la lógica proposicional

Valor veritativo de una fórmula

Definidos ya los símbolos y el lenguaje que vamos a utilizar, tiene sentido definir cuando una fórmula es o no cierta y que símbolo y significado tiene eso en nuestro lenguaje.

Definimos el **valor veritativo de** φ como cualquier aplicación:

$$v : \Sigma \to \{0, 1\}$$

Es decir, dada una fórmula a cada proposición de la signatura que la compone se le asigna un valor binario, correspondiendo el 0 a la falsedad y el 1 a la veracidad. De esto se deduce que si trabajamos con una signatura de cardinal $|\Sigma| = n$, entonces el número de valoraciones posibles para una fórmula formada por las mismas es de $|v| = 2^n$

Además, es necesario atribuir un valor veritativo a cada conectiva lógica, puesto que estas cambian el significado de las proposiciones de la signatura cuando son empleadas, luego:

$$v_\neg : \{0, 1\} \to \{0, 1\}$$

$$v_\square : \{0, 1\} \times \{0, 1\} \to \{0, 1\}$$

De forma que en función de la conectiva que se sustituya en el $\square$ se tendrá una tabla de verdad u otra.

Por último, es necesario definir cual es el valor veritativo de una fórmula compuesta por la combinación de varias proposiciones y conectivas lógicas. Para ello definimos, finalmente, la siguiente función recursiva para determinar el valor de cualquier fórmula dentro del lenguaje, dadas $\varphi \in L_\Sigma, v : \Sigma \to \{0, 1\}$ definimos la función valoración como:

$$[\cdot]^v : L_\Sigma \to \{0, 1\} \text{ de forma que } \begin{cases} [\top]^v = 1 & \text{caso base} \\ [\bot]^v = 0 & \text{caso base} \\ [p]^v = v(p) : \forall p \in \Sigma & \text{caso base} \\ [\neg\varphi]^v = v_\neg([\varphi]^v) & \text{caso recursivo} \\ [\varphi_1 \square \varphi_2]^v = v_\square([\varphi_1]^v, [\varphi_2]^v) & \text{caso recursivo} \end{cases}$$

Satisfacibilidad

Cuando tenemos una fórmula concreta $\varphi \in L_\Sigma$ y una función valoración $v : \Sigma \to \{0, 1\}$, pueden ocurrir dos cosas:

- Si $[\varphi]^v = 1$, entonces decimos que v satisface φ o que v es modelo de φ y lo denotamos por $v \models \varphi$ o $v \in Mod(\varphi)$.
- Si $[\varphi]^v = 0$, entonces decimos que v no satisface φ o que no es modelo de φ y lo denotamos por $v \not\models \varphi$

Cuando al menos existe alguna valoración que es modelo de la fórmula, decimos que esta es satisfactible y cuando no existe ninguna decimos que es insatisfactible.

Del mismo modo, cuando tenemos un conjunto $\Phi = \{\varphi_1, \varphi_2, \cdots, \varphi_n\} \subset L_\Sigma$ de fórmulas podemos decir que ese conjunto es satisfactible si existe al menos una valoración que haga ciertas todas las fórmulas del conjunto:

$$\exists v : \Sigma \to \{0,1\} : v \in Mod(\varphi_i) : \forall i = 1, \cdots, n \Rightarrow \Phi \text{ satisfactible}$$

El conjunto es insatisfactible cuando no existe ninguna valoración que haga ciertas todas las fórmulas del conjunto de forma simultánea:

$$\forall v : \Sigma \to \{0,1\} : v \notin Mod(\varphi_i) : \exists i = 1, \cdots, n \Rightarrow \Phi \text{ insatisfactible}$$

Tipos de fórmulas según su satisfacibilidad:

- Decimos que una fórmula es una **tautología** si es cierta para cualquier valoración:

$$\forall v : \Sigma \to \{0,1\} : v \in Mod(\varphi)$$

- Decimos que una fórmula es contradicción si es falsa para cualquier valoración:

$$\forall v : \Sigma \to \{0,1\} : v \notin Mod(\varphi)$$

- Decimos que una fórmula es contingencia cuando posee tanto valoraciones falsas como ciertas:

$$\exists v, w : \Sigma \to \{0,1\} : v \in Mod(\varphi) \wedge w \notin Mod(\varphi)$$

Caso particular

En primer lugar, definimos el vocabulario de φ como $voc(\varphi)$ y compone el conjunto de proposiciones atómicas $p_i \in \Sigma$ que componen a la fórmula φ.

Sabiendo lo anterior, dada una fórmula $\chi \in L_\Sigma$ cuyo vocabulario está formado por m proposiciones atómicas. Si tenemos m fórmulas $\varphi_1, \varphi_2, \cdots \in L_\Sigma$ definimos un caso particular como:

$$\chi' = [p_1 \mid \varphi_1, \cdots, p_m \mid \varphi_m]$$

Donde la fórmula χ' final es el resultado de sustituir cada φ_i por la proposición p_i en cada una de sus apariciones en χ.

MÉTODOS DE DEDUCCIÓN Y ARGUMENTACIÓN

Validez de la argumentación lógica

Una vez que tenemos claro todos los conceptos anteriores, parece coherente querer valerse de esta definición de la lógica en un lenguaje formal para decidir si una cierta argumentación es válida o no, es decir, si realmente tienen una fundamentación lógica las demostraciones, teoremas y deducciones que uno pueda hacer.

Consecuencia lógica

Dado un conjunto de fórmulas $\Phi \subset L_\Sigma$, que denominaremos **conjunto de premisas**, y una fórmula ψ, que denominaremos **consecuencia**, decimos que ψ es consecuencia lógica de Φ si cualquier modelo de Φ lo es de ψ (pero no es necesario que los de ψ lo sean de Φ).

$$\forall v : \Sigma \to \{0,1\} : v \in Mod(\Phi) \Rightarrow v \in Mod(\psi) \Leftrightarrow \Phi \models \psi$$

Es decir, que un razonamiento es consecuencia de las premisas cuando cualquier valoración que haga cierta las premisas hace cierta la consecuencia.

Teorema de la deducción

Si tenemos un conjunto de premisas Φ y un conjunto de fórmulas $\varphi, \psi, \varphi_1, \ldots, \varphi_n \in L_\Sigma$, entonces:

- $\Phi \models (\varphi \to \psi) \Leftrightarrow \Phi \cup \{\varphi\} \models \psi$
- $\Phi \models (\varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n) \to \psi \Leftrightarrow \Phi \cup \{\varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n\} \models \psi$
- $\varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n \to \psi$ es tautología $\Leftrightarrow \varphi_1, \varphi_2, \cdots, \varphi_n \models \psi$

Es decir, en definitiva todo se resume a que si una fórmula es consecuencia lógica de un conjunto de premisas, entonces esta se puede incorporar al conjunto de premisas como una nueva para poder seguir haciendo más deducciones lógicas.

Si encuentras esto difícil entonces no eres inteligente o no lo has trabajado.
Lo has trabajado y eres inteligente luego no lo encontrarás difícil.

Premisas $\begin{cases} (p \to (\neg q \vee \neg r)) \\ (r \wedge q) \end{cases}$

Conclusión $\therefore \neg p$

p :Encuentras esto difícil
q :Eres inteligente
r :Lo has trabajado

p	q	r	¬ q	¬ r	(¬ q ∨ ¬ r)	((p → (¬ q ∨ ¬ r))	(r ∧ q)	¬ p
0	0	0	1	1	1	1	0	1
0	0	1	1	0	1	1	0	1
0	1	0	0	1	1	1	0	1
0	1	1	0	0	0	1	1	1
1	0	0	1	1	1	1	0	0
1	0	1	1	0	1	1	0	0
1	1	0	0	1	1	1	0	0
1	1	1	0	0	0	0	1	0

Regla de inferencia: (p → (¬ q ∨ ¬ r)) , (r ∧ q) ⊨ ¬ p

Teorema de Reducción al Absurdo

Si tenemos un conjunto de premisas $\Phi \subset L_\Sigma$ y una serie de fórmulas $\varphi, \psi, \varphi_1, \cdots, \varphi_n \in L_\Sigma$, entonces:

$$\Phi \models \psi \Leftrightarrow \Phi \cup \{\neg\psi\} \text{ instatisfactible}$$

O dicho de otro modo, si $\varphi_1, \varphi_2, \cdots, \varphi_n \models \psi \Rightarrow \varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n \wedge \neg\psi$ es contradicción.

Es decir, lo que estamos afirmando es que no hay ninguna valoración que haga ciertas las premisas y la negación de la conclusión simultáneamente, osea que si ocurren las premisas la conclusión debe darse. En caso de que esto no ocurra, la valoración o valoraciones que hacen satisfactible el nuevo conjunto se llaman **valoraciones contraejemplo**.

Ej.: Refuta $(p \to q) \models q$ mediante una valoración contraejemplo.

Valoración contraejemplo: $v : \Sigma \to \{0,1\}, \quad v(p) = v(q) = 0$

$$\begin{aligned}[[(p \to q) \wedge \neg q]]^v &= v_\wedge(v_\to(v(p), v(q)), v_\neg(v(q))) \\ &= v_\wedge(v_\to(0,0), v_\neg(0)) \\ &= v_\wedge(1,1) = 1\end{aligned}$$

Equivalencia lógica

No es difícil ver que si el número de proposiciones en el vocabulario de la fórmula crece, el crecimiento del número de valoraciones es exponencial, más concretamente 2^n donde n es el número de proposiciones atómicas. Por ello, es necesario encontrar un método para hallar el valor veritativo de una fórmula o al menos simplificarla para calcularlo sobre una más sencilla.

Equivalencia de fórmulas

Dadas $\varphi, \psi \in L_\Sigma$ decimos que ambas son lógicamente equivalentes cuando el conjunto de modelos de ambas coincide:

$$\varphi \sim \psi \Leftrightarrow Mod(\varphi) = Mod(\psi) \Leftrightarrow \forall v : \Sigma \to \{0,1\},\ [\varphi]^v = [\psi]^v$$

La siguiente definición implica que $\varphi \leftrightarrow \psi$ es una tautología y conlleva las siguientes propiedades:

- La relación $\sim \subseteq L_\Sigma \times L_\Sigma$ es una relación de equivalencia.
- Se tiene que $\varphi \models \psi$ y $\psi \models \varphi$
- Una fórmula es tautología si y solo si $\varphi \sim \top$
- Una fórmula es contradicción si y solo si $\varphi \sim \bot$
- Si tenemos una fórmula χ en la que aparece φ, es decir, $\chi(\varphi)$, entonces el sustituir φ por ψ en alguna o en todas las apariciones de la misma no influye en la valoración ni significado de la fórmula.

Un buen método para poder simplificar por equivalencia lógica estas fórmulas es tener en cuenta las leyes algebraicas de Boole que se pueden aplicar en este caso por formar junto con la función valoración un retículo de Boole:

$(\varphi \vee \psi) \vee \chi \sim \varphi \vee (\psi \vee \chi)$ $(\varphi \wedge \psi) \wedge \chi \sim \varphi \wedge (\psi \wedge \chi)$	Leyes de asociatividad
$\varphi \vee \psi \sim \psi \vee \varphi$ $\varphi \wedge \psi \sim \psi \wedge \varphi$	Leyes de conmutatividad
$\varphi \vee (\psi \wedge \chi) \sim (\varphi \vee \psi) \wedge (\varphi \vee \chi)$ $\varphi \wedge (\psi \vee \chi) \sim (\varphi \wedge \psi) \vee (\varphi \wedge \chi)$	Leyes de distributividad
$\neg(\varphi \vee \psi) \sim \neg\varphi \wedge \neg\psi$ $\neg(\varphi \wedge \psi) \sim \neg\varphi \vee \neg\psi$	Leyes de De Morgan
$\varphi \vee \varphi \sim \varphi$ $\varphi \wedge \varphi \sim \varphi$	Leyes de idempotencia
$\varphi \vee (\varphi \wedge \psi) \sim \varphi$ $\varphi \wedge (\varphi \vee \psi) \sim \varphi$	Leyes de absorción
$\varphi \vee \bot \sim \varphi$ $\varphi \wedge \top \sim \varphi$	Elemento neutro.Leyes de identidad
$\varphi \vee \top \sim \top$ $\varphi \wedge \bot \sim \bot$	Elemento nulo.Leyes de dominación
$\neg\top \sim \bot$ $\neg\bot \sim \top$ $\neg\neg\varphi \sim \varphi$ (Doble negación) $\varphi \vee \neg\varphi \sim \top$ (Tercio excluído) $\varphi \wedge \neg\varphi \sim \bot$ (Contradicción)	Leyes de negación

Forma normal conjuntiva y disyuntiva

Relacionado con el concepto anterior de equivalencia lógica, vamos a ver dos formas canónicas a las que se puede convertir cualquier fórmula del lenguaje de la lógica definido. Para ello definimos el concepto de **literal** como una fórmula del tipo φ o $\neg\varphi$, pero no se permiten otras conectivas lógicas entre ellas.

- **Forma Normal Disyuntiva (FND)**

  Se trata de una forma canónica en la que tenemos una serie de cláusulas conjuntivas, esto es, literales unidos entre ellos por conjunciones, unidas por disyunciones entre ellas, es decir:

$$FND \to (\varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n) \vee (\psi_1 \wedge \cdots \wedge \psi_m) \vee \cdots \vee (\chi_1 \wedge \cdots \wedge \chi_s)$$

- **Forma Normal Conjuntiva (FNC)**

  Se trata de una forma canónica en la que tenemos una serie de cláusulas disyuntivas, esto es, literales unidos entre ellos por disyunciones, unidas por conjunciones entre ellas, es decir:

$$FNC \to (\varphi_1 \vee \varphi_2 \vee \cdots \vee \varphi_n) \wedge (\psi_1 \vee \cdots \vee \psi_m) \wedge \cdots \wedge (\chi_1 \vee \cdots \vee \chi_s)$$

Teniendo en cuenta estos dos conceptos podemos asegurar la siguiente afirmación:

$$\forall \varphi \in L_\Sigma : \exists \psi(FND), \chi(FND) : \varphi \sim \psi \sim \chi$$

Puesto que si tenemos una fórmula φ sabemos que posee unas ciertas valoraciones que son modelos (o ninguna y en ese caso sería $\sim \perp$), de este modo la fórmula es cierta si y solo si son ciertas las condiciones de valoración de los literales de alguno de sus modelos, luego:

$$[\varphi]^v = 1 \Leftrightarrow [v_1 \vee v_2 \vee \cdots \vee v_n]^v = 1 \Rightarrow \exists \chi(FND) \in L_\Sigma : \psi \sim \varphi$$

Es decir, que pensando en la tabla de verdad de la fórmula, para cada línea que haga 1 la fórmula hay una combinación de 0 y 1 de los literales que identifican dicha línea, por tanto, esos literales van con una conjunción entre ellos y negados o no negados en función de si deben valer 0 o 1 y además todos los modelos van unidos entre ellos por disyunciones puesto que solo es necesario que al menos alguno de ellos sea cierto para que la fórmula sea cierta.

Para ahora obtener la FNC, hallamos la FND de la negación de la fórmula. Como esta FND y $\neg\varphi$ son equivalentes, si la negamos obtenemos de nuevo φ por las leyes algebraicas de Boole, pero la negación de una serie de cláusulas conjuntivas unidas por disyunciones es de nuevo por Boole una serie de cláusulas disyuntivas unidas por conjunciones, que además es equivalente a φ; luego tenemos ya nuestra FNC.

Leyes de equivalencia lógica para simplificación de fórmulas en forma normal.

$$(DIS) \quad (\varphi \wedge \psi) \vee (\varphi \wedge \neg\psi) \sim \varphi$$

$$(CON) \quad (\varphi \vee \psi) \wedge (\varphi \vee \neg\psi) \sim \varphi$$

y en ambos casos se dice que las dos cláusulas asocian con respecto a ψ

Tableaux semánticos

Este método consiste en un algoritmo muy preciso para poder determinar cuando a partir de unas hipótesis algo es consecuencia lógica o no sin necesidad de hacer a mano todas las tablas de verdad y comparar modelos, decidir si un conjunto de fórmulas es satisfactible, saber si algo es tautología y calcular las formas normales.

Demostración de la consecuencia lógica

Para poder demostrar que de un conjunto Φ de premisas una fórmula φ es consecuencia lógica demostramos que $\Phi \cup \{\neg\varphi\}$ es insatisfactible, es decir, refutamos la idea de que las premisas puedan ser ciertas siendo las condiciones falsas.

El procedimiento general parte de la base de ir simplificando y dividiendo en trozos cada una de las fórmulas que componen el conjunto en base a la siguiente clasificación:

Fórmulas simplificables: $\sigma \sim \sigma_1$		Fórmulas conjuntivas: $\alpha \sim \alpha_1 \wedge \alpha_2$			Fórmulas disyuntivas: $\beta \sim \beta_1 \vee \beta_2$		
σ	σ_1	α	α_1	α_2	β	β_1	β_2
$\neg\top$	$\bot$	$\varphi \wedge \psi$	φ	ψ	$\varphi \vee \psi$	φ	ψ
$\neg\bot$	$\top$	$\neg(\varphi \vee \psi)$	$\neg\varphi$	$\neg\psi$	$\neg(\varphi \wedge \psi)$	$\neg\varphi$	$\neg\psi$
$\neg\neg\varphi$	φ	$\neg(\varphi \rightarrow \psi)$	φ	$\neg\psi$	$(\varphi \rightarrow \psi)$	$\neg\varphi$	ψ
		$\varphi \leftrightarrow \psi$	$\varphi \rightarrow \psi$	$\psi \rightarrow \varphi$	$\neg(\varphi \leftrightarrow \psi)$	$\neg(\varphi \rightarrow \psi)$	$\neg(\psi \rightarrow \varphi)$

En sí, un tableaux va abriendo los distintos caminos o posibilidades que hacen ciertas a las fórmulas que componen el conjunto. Se trata de construir un árbol (grafo) a partir del tronco formado por las fórmulas iniciales e irlo prolongando en ramas según los escenarios que vayan surgiendo, para ello se siguen las siguientes reglas de formación:

- $[R_{ini}]$: Para poder comenzar, formamos el tronco del árbol con las fórmulas correspondientes al conjunto y esta será nuestra primera rama.
- $[R_\sigma]$: Si θ es una rama abierta de T con un nodo etiquetado con una fórmula simplificable σ, se obtiene T' **alargando** la rama θ con su simplificación σ_1.
- $[R_\alpha]$: Si θ es una rama abierta de T con un nodo etiquetado con una fórmula conjuntiva α, se obtiene T' **alargando** la rama θ con dos nodos nuevos etiquetados con las componentes de la conjunción α_1 y α_2.
- $[R_\beta]$: Si θ es una rama abierta de T con un nodo etiquetado con una fórmula disyuntiva β, se obtiene T' **dividiendo** a la rama θ en otras dos y usando como hijos las componentes β_1 y β_2.

Nuestro objetivo es aplicar de forma sucesiva todas estas reglas hasta llegar a un tableaux equivalente simplificado que no pueda reducirse más, en ese caso decimos que el tableaux queda terminado.

Cuando en uno de los caminos (recorridos desde el tronco hasta el final de una rama, **pero no entre ramas**) encontramos una fórmula φ y su negada $\neg\varphi$, entonces decimos que esa rama está cerrada, puesto que hemos llegado a un escenario imposible. **En consecuencia, si algo es consecuencia lógica de un conjunto de premisas, entonces al incorporarlo negado al mismo el tableaux correspondiente será cerrado en todas sus ramas**.

Satisfacibilidad de un conjunto de fórmulas

En el proceso de demostración de una deducción lógica hemos refutado que $\Phi \cup \{\neg\varphi\}$ sea satisfactible, por lo que ya sabemos como probar la satisfacibilidad de un conjunto de fórmulas; basta con ver que el tableaux que podemos construir con ellas es cerrado en todas sus ramas.

Si un tableaux que ha sido terminado todavía posee ramas abiertas, podemos asociar ese caso particular la valoración que hace que el conjunto no sea insatisfactible, dicha valoración quedará definida de la siguiente forma:

$$v_\theta = \{v_\theta(p_1), \cdots, v_\theta(p_n)\} : v_\theta(p_i) = \begin{cases} 1 & \text{si p aparece en } \theta \\ 0 & \text{si } \neg p \text{ aparece en } \theta \\ \text{arbitrario} & \text{si no aparece en } \theta \end{cases}$$

Para el caso de la deducción lógica, esta valoración v_θ es una valoración contraejemplo.

Cálculo de formas normales

Dada una fórmula $\varphi \in L_\Sigma$ podemos determinar su FND construyendo el tableaux asociado a dicha fórmula y podemos encontrarnos dos escenarios:

- Tableaux cerrado: en cuyo caso $FND(\varphi) = \bot$
- Tableaux abierto: en cuyo caso se construye una conjunción de todos los literales que aparezcan en la rama, es decir, que se escribe cada término p_i de la valoración v_θ con el símbolo $\neg$ delante o no en función de si la valoración particular de ese término es 1 o 0.

Para obtener la FNC se realizan las conversiones pertinentes explicadas en su capítulo.

LÓGICA DE PREDICADOS

Es claro que para la lógica desarrollada hasta ahora, a pesar de ser correcta, se tienen ciertas insuficiencias que no permiten desarrollar razonamientos más complejos con le lenguaje definido. Por ejemplo, nuestros razonamiento con frecuencia aluden a individuos como elementos de un colectivo y no como individuos y eso hace que enunciados como (poner ejemplo) no sean capaces de ser procesados por la lógica proposicional.

Para poder extender la lógica proposicional a un ámbito mucho más general y que permita desarrollar razonamientos más complejos necesitamos hacer una **extensión** de la misma, es decir, vamos a agregar los siguientes elementos:

- **Dominio o universo del discurso**: denota el colectivo de individuos sobre el que razonamos.
- **Constantes**: denotan los nombres propios que hacen referencia a individuos concretos del conjunto.
- **Variables**: denotan los valores cualesquiera del universo y permiten referirse a un individuo cualquiera de forma anónima.
- **Predicados**: son los enunciados sobre los individuos y hay de dos tipos:
  - Monádicos: que hacen referencia a propiedades de un individuo y le atribuye alguna propiedad.
  - Poliádicos: que hacen referencia a propiedades de las relaciones entre individuos.
- **Funciones**: son enunciados que describen un individuo en función de otro.
- **Símbolo de igualdad**: expresa la relación de igualdad entre dos términos.
- **Cuantificadores**: redefinen los predicados indicando la frecuencia con la que ocurre una afirmación.
  - Cuantificador universal: indica que algo es cierto para todos los individuos del colectivo.
  - Cuantificador existencial: indica que algo es cierto para al menos alguno de los individuos del colectivo.

En definitiva, este nuevo concepto de lógica permite profundizar mucho más allá en los razonamientos vistos y no prescinde de la lógica anterior, sino que la incorpora y la mejora.

DEFINICIÓN Y LENGUAJE DE LA LÓGICA

Sintaxis de la lógica de 1º orden

Alfabeto de símbolos primitivos

De nuevo, para poder definir cualquier lenguaje, en este caso el de la lógica de primer orden, necesitamos definir un alfabeto sobre el cual no haya interpretaciones posibles sobre el significado que le queremos atribuir a un enunciado concreto. Para ello, vamos a incorporar al alfabeto que teníamos en la lógica proposicional una serie de cambios y además redefinir en parte algunos conceptos:

- **Símbolos lógicos**: $\{\bot, \top, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists, =\}$
  - **Conectivas proposicionales**: $\{\bot, \top, \neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$.
  - **Cuantificadores**: $\{\forall, \exists\}$ denotando universal y existencial respectivamente.
  - **Signo de igualdad**: $\{=\}$ denotando igualdad entre términos.
- **Símbolos auxiliares**: $\{(,),\ ,\}$

  Son símbolos que denotan la precedencia de operadores o el radio de alcance de los cuantificadores.
- **Conjunto de Variables**: $V = \{x, y, z, w, t, \cdots\}$

  Es un conjunto infinito numerable de símbolos que denotan variables.
- **Signatura**: Σ

  Denotamos por Σ al conjunto de símbolos de función y predicado con sus respectivas aridades[30] asociadas, por tanto, podemos considerar:

  $$\Sigma = F_\Sigma \cup P_\Sigma : \begin{cases} F_\Sigma = \{f \text{ función }\} \\ P_\Sigma = \{P \text{ predicado}\} \end{cases}$$

  Además, si queremos especificar la aridad asociada a cada conjunto denotamos:

  $$F_\Sigma^n = \{f \in F_\Sigma : ar(f) = n\} \qquad P_\Sigma^n = \{P \in P_\Sigma : ar(P) = n\}$$

  Por último, consideramos a las funciones de aridad 0 como **constantes** y las denotaremos por letras minúsculas $a, b, c, d, \cdots$ y consideraremos los predicados de aridad 0 como **proposiciones** denotándolas por letras minúsculas $p, q, r, \cdots$

Por tanto, tras describir todos los símbolos que van a ser empleados y dotarlos de una función inequívoca, nos queda el siguiente alfabeto:

$$A_\Sigma = \Sigma \cup \{(,),\ ,\} \cup \{\bot, \top, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists, =\} \cup V$$

Lenguaje de la lógica de 1º orden

Una vez construido el alfabeto sobre el que se basará nuestro lenguaje, es necesario establecer unas normas para determinar qué palabras sobre ese alfabeto son válidas o no. En primer lugar, en este tipo de lógica se pueden construir 2 expresiones:

- **Términos** (T_Σ): designan individuos del universo del discurso.
- **Fórmulas** (L_Σ): representan enunciados sobre términos concretos.

Con cual para poder construir las distintas expresiones hay que ceñirse al siguiente conjunto de normas:

Reglas de formación de términos:

Denotamos al conjunto de términos sobre la signatura Σ como T_Σ y el conjunto lo forman las palabras construidas sobre el alfabeto A_Σ conforme al siguiente conjunto de normas:

[30] Número de argumentos

- Las variables son términos atómicos
- Las constantes son términos atómicos
- Si tenemos $t_1, \cdots, t_n \in T_\Sigma$ y $f \in F^n_\Sigma$, entonces $f(t_1, \cdots, t_n)$ es un término

Reglas de formación de fórmulas:

Denotamos al conjunto de fórmulas sobre la signatura Σ como L_Σ y el conjunto lo forman las palabras construidas sobre el alfabeto A_Σ conforme al siguiente conjunto de normas:

- Las construcciones que hemos calificado como proposiciones son fórmulas atómicas.
- Si $s, t \in T_\Sigma$, es decir, son términos, entonces $s = t$ es una fórmula atómica.
- Si $t_1, \cdots, t_n \in T_\Sigma$ y $P \in P^n_\Sigma$, entonces $P(t_1, \cdots, t_n)$ es una fórmula atómica.
- Si $\varphi \in L_\Sigma$, entonces $\neg\varphi$ es una fórmula compuesta.
- Si $\varphi_1, \varphi_2 \in L_\Sigma$, entonces $\varphi_1 \square \varphi_2$ es una fórmula compuesta (siendo $\square$ alguna conectiva lógica binaria).
- Si $\varphi \in L_\Sigma$ y $x \in V$, entonces $\forall x,\ \varphi$ es una fórmula compuesta llamada cuantificación universal.
- Si $\varphi \in L_\Sigma$ y $x \in V$, entonces $\exists x,\ \varphi$ es una fórmula compuesta llamada cuantificación existencial.