Lenguaje matemático, conjuntos y números

a

1 de diciembre de 2016

Índice general

1 Nociones de lógica

1.1. Conectores lógicos básicos

1.1.1. Negación

p	$\neg p$
0	1
1	0

Tabla 1.1: Negación

1.1.2. Disyunción

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Tabla 1.2: Disyunción

1.1.3. Conjunción

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Tabla 1.3: Conjunción

1.1.4. Condicional

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

Tabla 1.4: Disyunción

A la proposicional condicional se le asocian 3 nuevas proposiciones:

Condiconal recíproco $q \to p$.

Condiconal contrario $\neg p \to \neg q$.

Condiconal contrarrecíproco $\neg q \to \neg p$.

1.1.5. Bicondicional

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Tabla 1.5: Disyunción

1.2. Construcción de nuevas propociones

Contradicción Proposición que solo toma el valor 0, se denota como **0**.

Tautología Proposición que solo toma el valor 1, se denota como **1**.

1.3. Leyes lógicas

1.3.1. Leyes lógicas con una proposición

Doble negación

$$\neg\neg p \Leftrightarrow p$$

1.3.2. Simplificación

1. $p \vee p \Leftrightarrow p$
2. $p \wedge p \Leftrightarrow p$
3. $p \rightarrow p \Leftrightarrow p$
4. $p \leftrightarrow p \Leftrightarrow p$

Tercio exclusivo

$$p \vee \neg p \Leftrightarrow \mathbf{1}$$

Contradicción

$$p \wedge \neg p \Leftrightarrow \mathbf{0}$$

1.3.3. Leyes lógicas equivalentes con dos proposiciones

Identidad

1. $p \vee 0 \Leftrightarrow p$ y $p \vee 1 \Leftrightarrow 1$.

2. $p \wedge 1 \Leftrightarrow p$ y $p \wedge 0 \Leftrightarrow 0$.

3. $1 \rightarrow p \Leftrightarrow p$.

De Morgan

1. $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$.

2. $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$.

Del condicional

1. $p \rightarrow q \Leftrightarrow \neg p \vee q$.

2. $p \rightarrow q \Leftrightarrow \neg(p \wedge \neg q)$.

3. $p \rightarrow q \Leftrightarrow p \rightarrow (p \wedge q)$.

4. $p \rightarrow q \Leftrightarrow q \rightarrow (p \vee q)$.

Del bicondicional

$$p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$$

Reducción al absurdo

$$\neg p \rightarrow (q \wedge \neg q) \Leftrightarrow p$$

Transposición

1. $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$.

2. $p \leftrightarrow q \Leftrightarrow \neg p \leftrightarrow \neg q$.

1.3.4. Leyes lógicas equivalentes con tres proposiciones

Asociativas

1. $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$.
2. $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$.
3. $p \leftrightarrow (q \leftrightarrow r) \Leftrightarrow (p \leftrightarrow q) \leftrightarrow r$.
4. $p \rightarrow (q \vee r) \Leftrightarrow (p \rightarrow q) \vee (p \rightarrow q)$.
5. $p \rightarrow (q \wedge r) \Leftrightarrow (p \rightarrow q) \wedge (p \rightarrow q)$.

Distributivas

1. $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge q)$.
2. $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee q)$.
3. $p \rightarrow (q \vee r) \Leftrightarrow (p \rightarrow q) \vee (p \rightarrow q)$.
4. $p \rightarrow (q \wedge r) \Leftrightarrow (p \rightarrow q) \wedge (p \rightarrow q)$.

1.3.5. Leyes lógicas condicionales

Simplificación condicional

1. $p \wedge q \Rightarrow p$.
2. $p \Rightarrow p \vee q$

Inferencia

1. $\neg p \wedge (p \vee q) \Rightarrow q$.
2. $p \wedge (\neg p \vee \neg q) \Rightarrow \neg q$.

Ponendo ponens

$$(p \to q) \land p \Rightarrow q$$

Tollendo tollens

$$(p \to q) \land \neg q \Rightarrow \neg p$$

1.3.6. Validación de proposiciones

La validación de las proposiciones se puede realizar mediante:

- Construcción de la tabla de verdad.
- Refutación: Se aplica reducción al absurdo.

1.4. Forma clausulada

Proposición formada por la conjunción ($\land$) de disyunciones ($\lor$).

2 Conjuntos

2.1. Algunas ideas sobre conjuntos. Predicados

Un conjunto C está bien definido cuando se tiene un criterio que permite decidir si un determinado elemento b pertenece al conjunto C o no pertenece al conjunto C.

Un objeto no puede ser a la vez un conjunto y un elemento de ese conjunto. Este decir, la proposición $b \in b$ es falsa.

La colección de todos los conjuntos posibles no forman un conjunto.

2.1.1. Igualdad de conjuntos

Se dice que dos conjuntos A y B son iguales, y se escribe $A = B$, si y sólo si tiene los mismo elementos.

Cuando un conjunto se determina mediante una lista de todos sus elementos se dice que está **definido por extensión**.

2.1.2. Inclusión de conjuntos

$$A \subset B \Leftrightarrow x \in A \wedge x \in B$$

$$A = B \Leftrightarrow A \subset B \wedge B \subset A$$

2.1.3. Predicados

$$C_P = \{x \in C | P_x\}$$

P_x es un predicado que indica si el elemento x forma parte del conjunto o no. Los conjuntos así definidos se dice que está **definido por extensión**.

Al conjunto C se le conoce como **universo de predicado**.

Dos predicados son **equivalentes** sobre un universo C si definen el mismo subconjunto de C.

2.1.4. Conjunto vacío

$$\emptyset = \{x \in C | x \notin C\}$$

No tiene ningún elemento y es subconjunto de cualquier conjunto.

2.1.5. Principio de inducción

Si un predicado P se define sobre $\mathbb{N}$ tal que:

1. 0 satisface la propiedad P. Es decir, P_x es verdadero.

2. Si n satisface la propiedad P entonces el sucesor de n satisface también la propiedad P.

2.1.6. Cuantificadores

$$\neg(\forall x P_x) \Leftrightarrow \exists x \neg P_x$$
$$\neg(\exists x P_x) \Leftrightarrow \forall x \neg P_x$$

2.1.7. Complementario y partes de un conjunto

Complementario

$$\bar{A} = \{x \in U | x \notin A\} = \{x \in U | \neg P_x\}$$

Partes de un conjunto

$$\mathbb{P}(A) = \{B | B \subset A\}$$

2.2. Operaciones con conjuntos

2.2.1. Union

$$A \cup B = \{x | x \in A \vee x \in B\}$$

2.2.2. Intersección

$$A \cap B = \{x | x \in A \wedge x \in B\}$$

2.2.3. Familia de conjuntos

Si tenemos en cuenta un **conjunto de indices** no vacío I. A cada $i \in I$ le asociamos un conjunto F_i. La colección de todos esos conjuntos se denomina **familia de conjuntos** y se denota:

$$F = \{F_i | i \in I\}$$

Cuando todos los F_i son subconjuntos de un mismo conjunto U entonces F es un subconjunto de $P(U)$. Cualquier subconjunto G no vacío de $P(U)$ es una familia de conjuntos.

La unión e intersección se generaliza a familias arbitrarias:

$$\bigcup_{i\in I} = \{x|\exists i \in I, x\exists F_i\}$$
$$\bigcap_{i\in I} = \{x|\forall i \in I, x\exists F_i\}$$

Si la familia viene dada por $\emptyset \neq G \subset P(U)$:

$$\bigcup_{F\in G} = \{x|\exists F \in G, x\exists F_i\}$$
$$\bigcap_{F\in G} = \{x|\forall F \in G, x\exists F_i\}$$

2.2.4. Diferencia de conjuntos

$$A\backslash B = \{x|x \in A \wedge x \notin B\}$$

2.2.5. Diferencia simétrica

$$\begin{aligned} A\triangle B =&(A \cup B)\backslash(A \cap B) = \\ &\{x|x \in A \wedge x \notin B\} \cup \{x|x \notin A \wedge x \in B\} \end{aligned}$$

2.3. Algebra de conjuntos

2.4. Producto de conjuntos

Dado n conjuntos $A_1, A_2, \ldots, A_n$ se denomina producto de A_1, por A_2, por $\ldots$, por A_n al conjunto:

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n)|x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n\}$$

2.5. Relaciones entre conjuntos

Dados los conjuntos A y B, todo subconjunto $R \subset A \times B$ es una relación del conjunto A al conjunto B, relación entre A y B o correspondencia entre A y B.

$$R : A \longrightarrow B$$

Otra notación posible es:

$$xRy \Leftrightarrow (x, y) \in R \subset A \times B$$

A es el conjunto inicial, y B el conjunto final.

2.5.1. Conjunto original de la relación R

$$R^{-1}(B) = \{x \in A | \exists y \in B, xRy\}$$

2.5.2. Conjunto final de la relación R

$$R(A) = \{y \in B | \exists x \in A, xRy\}$$

2.5.3. Conjunto imagen de $x \in A$

$$R(x) = \{y \in B | (x, y) \in R\} = \{y \in B | xRy\}$$

2.5.4. Conjunto original de $y \in B$

$$R^{-1}(y) = \{x \in A | (x, y) \in R\} = \{x \in A | xRy\}$$

2.5.5. Composición de relaciones

Dadas las relaciones R entre los conjuntos A y B, y la relación S entre los conjuntos B y C, se define una relación entre los conjuntos A y C conocida como **composición de las relaciones R y S** o relación composición:

$$S \circ R = \{(x, z) \in A \times C | \exists y \in B, xRy \wedge ySz\}$$

3 Relaciones y aplicaciones entre conjuntos

3.1. Propiedades básicas

3.1.1. Reflexiva

R es reflexiva $\Leftrightarrow (x,x) \in R \Leftrightarrow \forall x \in U, xRx$

3.1.2. Simétrica

R es simétrica $\Leftrightarrow R^{-1} \subset R \Leftrightarrow \forall x, y \in U, xRy \Rightarrow yRx$.

3.1.3. Antisimétrica

R es antisimétrica $\Leftrightarrow R^{-1} \cap R = \{(x,x)|x \in U\} \Leftrightarrow \forall x, y \in U, xRy \wedge yRx \Rightarrow x = y$.

3.1.4. Transitiva

R es transtitiva $\Leftrightarrow R \circ R = R \Leftrightarrow \forall x, y, z \in U, xRy \wedge yRz \Rightarrow xRz$.

3.2. Relación de equivalencia

Una relación $\mathcal{E}$ en el conjunto U se denomina **relación de equivalencia** si posee las siguientes características:

1. Reflexiva.
2. Simétrica.
3. Transitiva.

3.2.1. Clase de equivalencia

Dada una relación de equivalencia $\mathcal{E}$ en el conjunto U, se denomina **clase de equivalencia** del elemento $x \in U$ al conjunto imagen de x:

$$x\mathcal{E} = [x] = \{y \in U | x\mathcal{E}y\}$$

- $x\mathcal{E}y \Rightarrow [x] = [y]$.
- Cualquier $y \in [x]$ es denominado **representante de la clase** $[x]$.
- $x \not\mathcal{E} y \Rightarrow [x] \cap [y] = \emptyset$

3.2.2. Conjunto cociente

Dada una relación de equivalencia $\mathcal{E}$ en el conjunto U, se denomina **conjunto cociente**, y se denota por $U/\mathcal{E}$, al conjunto de todas las clases que general la relación de equivalencia $\mathcal{E}$.

3.2.3. Partición de un conjunto

Una partición de un conjunto U es una familia P de subconjuntos no vacíos de U disjuntos dos a dos y cuya unión es el conjunto U. Es decir:

1. $\forall A, B \in P, A = B \vee A \cap B = \emptyset$.
2. $\bigcup_{A \in P} A = U$.

3.3. Relación de orden

Una relación $\mathcal{R}$ en el conjunto U se denomina **relación de orden** is posee las propiedades:

1. Reflexiva.
2. Antisimétrica.
3. Transitiva.

$\mathcal{R}$ es una **relación de orden total** $\Leftrightarrow \mathcal{R}^{-1} \cup \mathcal{R} = U \times U \Leftrightarrow \forall x, y \in U, x\mathcal{R}y \vee y\mathcal{R}x$. En cualquier otro caso es una **relación de orden parcial**.

3.3.1. Intervalos en un conjunto ordenado

Dados un conjunto ordenado $(U, \preceq)$, y $a, b \in U$ tales que $a \preccurlyeq b$, se denominan intervalos a cada uno de los siguientes conjuntos:

Intervalo abierto $(a, b) = \{x \in U | a \prec x \prec y\}$

Intervalo cerrado $[a, b] = \{x \in U | a \preceq x \preceq y\}$

Intervalo semiabiertos Pueden ser:

- $(a, b] = \{x \in U | a \prec x \preceq y\}$
- $[a, b) = \{x \in U | a \preceq x \prec y\}$

3.3.2. Intervalos iniciales y finales

Dado un conjunto ordenado $(U, \preceq)$, los siguientes conjuntos también se denominan intervalos:

Intervalo inicial abierto $(\leftarrow, a) = \{x \in U | x \prec a\}$.

Intervalo final abierto $(a, \leftarrow) = \{x \in U | a \prec x\}$.

Intervalo inicial cerrado $(\leftarrow, a] = \{x \in U | x \preceq a\}$.

Intervalo final cerrado $[a, \leftarrow) = \{x \in U | a \preceq x\}$.

3.3.3. Orden lexicográfico en $\mathbb{R}^2$

$$(a, b) \leq_L (c, d) \Leftrightarrow (a < c) \vee (a = c \wedge (b \leq d))$$

3.3.4. Orden producto en $\mathbb{R}^2$

$$(a, b) \leq_P (c, d) \Leftrightarrow a \leq c \wedge b \leq d$$

3.3.5. Conjunto acotado

Dados un conjunto ordenado $(U, \preceq)$ y un subconjunto $A \subset U$, se denomina:

Cota superior Cualquier elemento $u \in U$ que cumple que $\forall x \in A, x \preceq u$.

Cota inferior Cualquier elemento $u \in U$ que cumple que $\forall x \in A, u \preceq x$.

Conjunto A acotado superiormente Si existe una cota superior de A.

Conjunto A acotado inferiormente Si existe una cota inferior de A.

Conjunto A acotado Si existe tanto cota superior como inferior de A.

3.3.6. Máximo, mínimo, supremo e ínfimo

Máximo del conjunto A $\text{máx}(A) = m \in A$ tal que $\forall x \in A, x \preceq m$.

Mínimo del conjunto A $\text{mín}(A) = m \in A$ tal que $\forall x \in A, m \preceq x$.

Supremo del conjunto A Cota superior $\sup(A) = s \in U$ tal que $s \preceq u$ para toda cota superior u de A.

Ínfimo del conjunto A Cota inferior $\text{ínf}(A) = i \in U$ tal que $u \preceq i$ para toda cota inferior u de A.

El ínfimo es el máximo de las cotas inferiores. El supremo es el mínimo de las cotas superiores.

Si existe máximo entonces hay supremo y son iguales. Si existe mínimo entonces hay ínfimo y son iguales.

Dados un conjunto ordenado $(U, \preceq)$ y un subconjunto $A \subset U$, se tiene:

- Si existe máximo, mínimo, del conjunto A, entonces éste es único.
- Si existe supremo, ínfimo, del conjunto A, entonces éste es único.
- Si existe supremo s del conjunto A y $s \in A$, entonces s es el máximo de A.
- Si existe ínfimo i del conjunto A y $i \in A$, entonces i es el mínimo de A.

Propiedad del buen orden

Se dice que un conjunto $(U, \preceq)$ es un conjunto **bien ordenado**, o que la relación $\preceq$ es una buena ordenación, si cualquier subconjunto no vacío posee mínimo. El elemento mínimo de cada subconjunto A también se denomina primer elemento.

Propiedad del supremo

Se dice que un conjunto $(U, \preceq)$ cumple la propiedad del supremo si y sólo si cualquier subconjunto no vacío A acotado superiormente posee supremo.

3.3.7. Maximal y minimal

Dados un conjunto ordenado $(U, \preceq)$ y un subconjunto $A \subset U$ se define:

Maximal del conjunto A Es un elemento $m \in A$ tal que

$$\nexists x \in A, x \neq m, m \preceq x$$

Minimal del conjunto A Es un elemento $m \in A$ tal que

$$\nexists x \in A, x \neq m, x \preceq m$$

Si un conjunto tiene máximo (mínimo) entonces solo hay un maximal (minimal) que coincide con él.

3.4. Aplicaciones entre conjuntos

Una relación entre los conjuntos A y B se denomina **aplicación**, o **función**, entre A y B si y sólo si cualquier elemento del conjunto inicial A esta relacionado con un único elemento del conjunto final B.

- A es el conjunto **inicial, original o dominio de definición** de f, y se denota como $Orig(f), Dom(f)$.
- B es el conjunto **final** de f.
- $f(A) = Im(f) = \{y \in B | \exists x \in A, f(x) = y\} = \{f(x) | x \in A\}$ es el **conjunto imagen**.
- $f(x)$ es la imagen de x.
- $f^{-1}(y) = \{x \in A | f(x) = y\}$ se denomina **imagen inversa de y por f**.
- El conjunto de aplicaciones de A a B se denota por $\mathcal{F}(A, B), B^A, \mathcal{F}(A)$.

Una aplicación f es **constante** $\Leftrightarrow \forall x, x' \in A, f(x) = f(x')$.

Una relación de equivalencia $\mathcal{E}$ sobre un conjunto A define una aplicación f que asigna a cada elemento su clase de equivalencia. Se denomina **proyección canónica**.

La **aplicación de identidad** asigna a cada $x \in A$ el mismo valor. Se denota como $I_A, 1_A, Id_A$.

3.4.1. Igualdad entre aplicaciones

Dos aplicaciones $f : A \longrightarrow B$ y $g : A' \longrightarrow B'$ son iguales:

$$f = g \Leftrightarrow \begin{cases} A = A' \\ B = B' \\ f(x) = g(x)\ \forall x \in A \end{cases}$$

3.4.2. Composición de aplicaciones

Dadas las aplicaciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$, se define la **composición de** f y g, o aplicación composición, a la aplicación de A a C, que denotamos como $g \circ f$, tal que:

$$(g \circ f)(x) = g(f(x)), \forall x \in A$$

3.4.3. Función característica de un conjunto

Dado un subconjunto $A \subset U$, se llama función característica de A, y se denota $\mathcal{X}_A$, a la función $\mathcal{X}_A : U \longrightarrow \mathbb{R}$ definida de la forma:

$$\mathcal{X}_A = \begin{cases} 1\ x \in A \\ 0\ x \notin A \end{cases}$$

3.4.4. Aplicación sobreyectiva o sobreyección

Es una aplicación tal que cualquier elemento del conjunto final está relacionado con alguno del conjunto inicial. Es decir, $f \in \mathcal{F}(A, B)$ tal que $Im(f) = B$, o lo que es lo mismo:

$$\forall y \in B, \exists x \in tal\ que\ Af(x) = y$$

3.4.5. Aplicación inyectiva o inyección

Es una aplicación tal que no hay dos elementos del conjunto inicial que tengan la misma imagen. Es decir, $f \in \mathcal{F}(A, B)$ tal que:

$$\forall x, x' \in A, f(x) = f(x') \Rightarrow x = x'$$

O lo que es lo mismo:

$$\forall x, x' \in A, x \neq x' \Rightarrow f(x) \neq f(x')$$

3.4.6. Composición de aplicaciones sobreyectivas e inyectivas

Dadas las aplicaciones $f \in \mathcal{F}(A, B)$, $g \in \mathcal{F}(B, C)$ y $g \circ f \in \mathcal{F}(A, B)$, se tiene:

1. Si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.

2. Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.

3.4.7. Aplicación biyectiva o biyección

Es una aplicación que es sobreyectvia o inyectiva al mismo tiempo, es decir, tal que cada elemento del conjunto final está relacionado cono un único elemento del conjunto inicial. Es decir, una aplicación $f \in \mathcal{F}(A, B)$ tal que:

$$\textit{para cada } y \in B \textit{ existe un unico elemento } x \in A \textit{ tal que } f(x) = y$$

Una aplicación $f \in \mathcal{F}(A, B)$ es biyectiva si y sólo si existe una aplicación $g \in \mathcal{F}(A, B)$ tal que $f \circ g = I_B$ y $g \circ f = I_A$.

Sean $f \in \mathcal{F}(A, B)$ y $g \in \mathcal{F}(B, C)$ aplicaciones biyectivas, entonces $g \circ f \in \mathcal{F}(A, C)$ es biyectiva, y su inversa es:

$$(g \circ f)^{-1}(x) = f^{-1}(x) \circ g^{-1}(x)$$

Sea una aplicación $f \in \mathcal{F}(A, B)$:

1. f es sobreyectiva si y sólo si existe una aplicación $h \in \mathcal{F}(B, A)$ tal que $f \circ h = I_B$.

2. f es inyectiva si y sólo si existe una aplicación $g \in \mathcal{F}(A, B)$ tal que $g \circ f = I_A$.

3.5. Equipotencia de conjuntos

Dos conjuntos A y B se dicen equipotentes si y sólo si existe una biyección entre ellos, y se denota $A \equiv B$.

3.5.1. Cardinal

Se denomina:

Cardinal 0 Es la colección de todos los conjuntos equipotentes con $\emptyset$, y se representa con el símbolo del número 0.

Cardinal n Es la colección de todos los conjuntos equipotentes con $1, \ldots, n \subset \mathbb{N}^*$, y se representa con el símbolo del número n.

Cardinal de $\mathbb{N}$ o $\mathfrak{N}_0$ Es la colección de todos los conjuntos equipotentes con $\mathbb{N}$, y se representa con el símbolo del número $\mathfrak{N}_0$.

Cardinal $\mathbb{R}$ o $\mathfrak{c}$ Es la colección de todos los conjuntos equipotentes con $\mathbb{R}$, y se representa con el símbolo del número $\mathfrak{c}$.

Decimos que el conjunto A tiene n elementos siendo $n \in \mathbb{N}^*$ si y sólo si:

$$card(A) = n$$

Se dice que un conjunto A es:

Finito Si existe $n \in \mathbb{N}$ tal que $card(A) = n$.

Infinito Si no es un conjunto finito.

Numerable Si existe una biyección de los números naturales al conjunto, y se indica escribiendo $card(A) = \mathfrak{N}_0$.

4 Operaciones internas y estructuras algebraicas

4.1. Operaciones internas

Sea E un conjunto. Una **operación interna**, o **ley de composición interna**, en E es una aplicación de $E \times E$ en E. Es decir, es una ley que asocia a todo par (a, b) de elemento de E un elemento único de E, que notaremos, $a \star b$.

4.1.1. Propiedades

Sea E un conjunto y $\star$ una operación interna definida en E:

Asociativa $\forall a, b, c \in E, a \star (b \star c) = (a \star b) \star c$.

Conmutativa $\forall a, b \in E, a \star b = b \star a$.

Elemento neutro $\exists e \in E, \forall a \in E, a \star e = e \star a = a$.

Elemento simétrico del elemento $a \in E$ a un elemento $a' \in E$ tal que $a \star a' = a' \star a = e$.

Sea $\star$ una operación interna en E, si existe elemento neutro de $\star$ en E este es único.

Sea $\star$ una operación asociativa interna en E con elemento neutro $e \in E$. Si $a \in E$ tiene elemento simétrico, este es único.

4.2. Grupos

Sean G un conjunto y $\star$ una **operación interna** en G. Se dice que el par $(G, \star)$ tiene estructura de grupo, o que $(G, \star)$ es un **grupo**, si se satisfacen las siguientes propieda-

des:

1. $\star$ es **asociativa**.
2. Existe **elemento neutro** de $\star$ en G.
3. Para todo elemento $a \in G$, existe en G el **elemento simétrico** de a respecto de $\star$.

Si ademas la operación $\star$ es conmutativa se dice que el grupo es **conmutativo** o **abeliano**.

4.2.1. Propiedades de un grupo

Sea $(G, \star)$ un grupo. Se tiene:

1. $\forall a, b \in G, a \star b = a \star c \Rightarrow b = c$ (Propiedad cancelativa).
2. Para todo $a, b \in G$, existe un único $x \in G$, tal que $a \star x = b$.
3. Si a^{-1} y b^{-1} son los simétricos de a y b respectivamente, entonces $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

4.2.2. Subgrupos

Dados $(G, \star)$ y $H \subset G$, se dice que H es un subgrupo de G si $(H, \star)$ tiene a su vez estructura de grupo. En particular, el subconjunto $\{e\}$ y el propio G son subgrupos de G.

Sean un grupo $(G, \star)$ y H un subconjunto no vacío de G, $(H, \star)$ es un subgrupo de G si y sólo si $\forall a, b \in H, a \star b^{-1} \in H$.

4.2.3. Congruencia modulo

Sea $(G, \star)$ un **grupo abeliano** y sea $(H, \star)$ un subgrupo. La relación $\mathcal{R}_H$ en G definida:

$$\forall a, b \in G, a\mathcal{R}_H \Leftrightarrow a \star b^{-1} \in H$$

es una relación de equivalencia, que se denomina **congruencia modulo H**.

4.3. Anillos

Sea A un conjunto y sean $+$ y $\cdot$ dos operaciones internas definidas en A. Diremos que $(A, \star)$ es un **anillo** si se satisface:

1. $(A, +)$ es un grupo conmutativo.

2. La operación $\cdot$ es asociativa.

3. La operación $\cdot$ es distributiva respecto de la operación $+$, esto es,

$$a(b+c) = ab + ac$$
$$(b+c)a = ba + ca$$

Si además la operación $\cdot$ es conmutativa, se dice que $(A, +, \cdot)$ es una **anillo conmutativo**.

Si $(A, +, \cdot)$ tiene elemento neutro para $\cdot$, siendo este distinto del elemento neutro de $\star$, se dice que $(A, +, \cdot)$ es una **anillo unitario**.

4.3.1. Propiedades de un anillo

Sea $(A, +, \cdot)$ un anillo. Se tiene:

1. $\forall a \in A, A \cdot 0 = 0 \cdot A = 0$, se dice que 0 es absorbente para el producto.

2. $\forall a, b \in A, (-a)b = a(-b) = -(ab)$ y $(-a)(-b) = ab$.

3. Si además el $(A, +, \cdot)$ es una anillo conmutativo se satisfacen las siguientes igualdades:

$$(a+b)^2 = a^2 + b^2 + 2ab$$
$$(a+b)(a-b) = a^2 - b^2$$
$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

Divisores de cero

En un anillo $(A, +, \cdot)$ se dice que el elemento $a \in A, a \neq 0$, es un divisor si existe $b \in A, b \neq 0$, tal que $ab = 0$.

4.3.2. Subanillos. Ideales

Sea $(A, +, \cdot)$ un anillo y H un subconjunto no vació de G. Se dice que H es un **subanillo** de A si $(H, +, \cdot)$ es a su vez una anillo. Los subconjuntos $\{1\}$ y el propio A son subanillos de A.

Sean $(A, +, \cdot)$ un anillo y H un subconjunto no vacío de A. H es un **subanillo** de A si y sólo si $\forall a, b \in H$ se cumple:

1. $a - b \in H$.

2. $ab \in H$.

Sean $(A, +, \cdot)$ un **anillo conmutativo** e I un subconjunto no vacío de A. Se dice que I es un **ideal** de A si cumple:

1. $a - b \in I, \forall a, b \in I$.

2. $ac \in I, \forall a \in I, \forall c \in A$.

Si $(A, +, \cdot)$ un **anillo conmutativo** y $a \in A$ es un elemento fijo, el conjunto

$$aA = (a) = \{ak | k \in A\}$$

es un ideal de A que se denomina **ideal principal** generado por a.

4.4. Cuerpos

Sea $\mathbb{K}$ un conjunto y seán $+$ y $\cdot$ dos operaciones internas definidas en $\mathbb{K}$. $(\mathbb{K}, +, \cdot)$ es un **cuerpo** si se satisfacen las siguientes propiedades:

1. Las operaciones $+$ y $\cdot$ son asociativas en $\mathbb{K}$.

2. Las operaciones $+$ y $\cdot$ son conmutativas en $\mathbb{K}$.

3. La operación $\cdot$ es distributiva respecto la operación $+$ en $\mathbb{K}$.

4. Existen dos elementos distintos en $\mathbb{K}$ que se designan por $0, 1$ que son elementos neutros de la suma y del producto respectivamente.

5. Existencia de opuesto: para todo a en $\mathbb{K}$ existe el simétrico de a respecto de la suma que se designa por $-a$.

6. Existencia de inverso: para todo elemento $a \neq 0$ de $\mathbb{K}$ existe el simétrico de a para el producto que se designa por a^{-1}.

O lo que es lo mismo:

1. $(\mathbb{K}, +)$ es un grupo conmutativo.

2. $(\mathbb{K}, \cdot)$ es un grupo conmutativo.

3. La operación $\cdot$ es distributiva respecto de la operación $+$ en $\mathbb{K}$.

4.4.1. Subcuerpos

Sea $(\mathbb{K}, +, \cdot)$ un cuerpo y sea H un subconjunto no vacío de $\mathbb{K}$ donde consideramos las restricciones de las operaciones en $\mathbb{K}$. Se dice que H es un **subcuerpo** de $\mathbb{K}$ si $(H, +, \cdot)$ es su vez un cuerpo.

Sea $(\mathbb{K}, +, \cdot)$ un cuerpo y sea H un subconjunto con al menos dos elementos distintos. H es un subcuerpo de $\mathbb{K}$ si y sólo si se cumple:

1. $a - b \in \mathbb{K}$ para todo $a, b \in H$.

2. $ab^{-1} \in H$ para todo $a, b \in H* = H\backslash\{0\}$.

4.5. Orden y operaciones

4.5.1. Grupo ordenado

Sea una una relación de orden $\preceq$ definida sobre un grupo conmutativo $(G, +)$, se dice que $(G, +, \preceq)$ es un **grupo ordenado** si la relación de orden es compatible con la suma,

es decir:

$$\forall a, b, c \in G, a \preceq b \Rightarrow a + c \preceq b + c$$

En un grupo ordenado $(G, +, \preceq)$ se satisfacen las siguientes propiedades:

1. $a \preceq b \Leftrightarrow b + (-a) \in G_+$.
2. $a \preceq b \wedge a' \preceq b' \Rightarrow a + a' \preceq b + b'$.
3. $a \preceq b \Rightarrow -b \preceq -a$.

4.5.2. Anillo ordenado

Sea una una relación de orden $\preceq$ definida sobre un grupo conmutativo $(A, +, \cdot)$, se dice que $(A, +, \cdot, \preceq)$ es un **anillo ordenado** si se cumple:

1. $\forall a, b, c \in A, a \preceq b \Rightarrow a + c \preceq b + c$.
2. $\forall a, b \in A, 0 \preceq a \wedge 0 \preceq b \Rightarrow 0 \preceq ab$.

Si la relación de orden es total, se dice que el anillo es una **anillo totalmente ordenado**. Si además, es un cuerpo hablaremos de **cuerpo ordenado**.

En un anillo totalmente ordenado se define el **valor absoluto** de $a \in A$ mediante:

$$[a] = \begin{cases} a & si \quad 0 \preceq a \\ -a & si \quad a \prec a \end{cases}$$

En un anillo totalmente ordenado $(A, +, \cdot, \preceq)$ se satisfacen las siguientes propiedades:

1. $a \preceq b \Leftrightarrow b - a \in A$.
2. $a \preceq b \wedge a' \preceq b' \Rightarrow a + a' \preceq b + b'$.
3. $a \preceq b \Rightarrow -b \preceq -a$.
4. $a \preceq b \wedge 0 \preceq c \Rightarrow ac \preceq bc$.
5. $a \preceq b \wedge c \preceq 0 \Rightarrow bc \preceq ac$.
6. $\forall a \in A, 0 \preceq a^2$.

7. Si A es un anillo unitario entonces $0 \prec 1$.

8. $|a| \succeq 0, \forall a \in A$ y $|a| = 0 \Leftrightarrow a = 0$.

9. $|ab| = |a||b|, \forall a, b \in A$.

10. $|a + b| \preceq |a| + |b|, \forall a, b \in A$.

Si además $(A, +, \cdot)$ es un cuerpo también se cumple:

1. $a \succ b \Rightarrow a^{-1} \succ 0$.

2. $0 \prec a \preceq b \Rightarrow b^{-1} \preceq a^{-1}$.

3. $a \preceq b \prec 0 \Rightarrow b^{-1} \preceq a^{-1}$.

4.6. Homomorfismos

Sean G y G' dos conjuntos donde se tiene respectivamente definida una operación interna $+$. Sea $f : G \longrightarrow G'$ una aplicación. Se dice que f es un **homomorfismo** si se cumple que:

$$\forall a, b \in G, f(a + b) = f(a) + f(b)$$

Si $G = G'$ se denomina **endomorfismo**. Si el homomorfismo es biyectivo hablaremos de **isomorfismo** y todo endomorfismo biyectivo se denomina **automorfismo**.

4.6.1. Propiedades de un homomorfismo

1. Si $f : G \longrightarrow G'$ es un homomorfismo entonces la operación de G' es una operación interna cuando se restringe al conjunto imagen $f(G)$.

2. Si $f : G \longrightarrow G'$ y $g : G' \longrightarrow G''$ son homomorfismo entonces la composición $g \circ f : G \longrightarrow G'$ es un homomorfismo.

3. Si $f : G \longrightarrow G'$ es un isomorfismo entonces la aplicación inversa $f^{-1} : G' \longrightarrow G$ es un isomorfismo.

La existencia de un isomorfismo entre dos conjuntos define una relación de equivalencia, ya que es reflexiva, simétrica y transitiva.

4.6.2. Homomorfismo de grupo

Sean $(G,+)$ y $(G',+)$ dos grupos tales que sus elementos neutros son respectivamente 0_G y $0_{G'}$, y $-a$ y $-a'$ los elementos simétricos de $a \in G$ y $a' \in G'$. Sea $f : G \longrightarrow G'$. Se tiene:

1. $f(0_G) = 0_{G'}$.
2. $f(-a) = -f(a), \forall a \in G$.
3. Si H es un subgrupo de G entonces,

   $$f(H) = \{a' \in G' | \exists a \in H, f(a) = a'\}$$

   es un subgrupo de G'.
4. Si H' es un subgrupo de G' entonces,

   $$f^{-1}(H') = \{a \in G | a \in G, f(a) \in H'\}$$

   es un subgrupo de G.

Sean $(G,+)$ y $(G',+)$ dos grupos y $f : G \longrightarrow G'$ es un homomorfismo. Se tiene:

1. Imf es un subgrupo de G'.
2. $Kerf$ es un subgrupo de G.
3. f es inyectivo si y sólo si $Kerf = \{0_G\}$.
4. f es sobreyectivo si y sólo si $Imf = G'$

4.6.3. Homomorfismo de anillos y cuerpos

Si $(A,+,\cdot)$ y $(A',+,\cdot)$ son dos anillos, un **homomorfismo de anillos** es una aplicación $f : A \longrightarrow A'$ tal que para todo $a, b \in A$ se cumple:

1. $f(a+b) = f(a) + f(b)$.
2. $f(ab) = f(a)f(b)$.

Para la $+$ se cumplen las todas propiedades del homomorfismo de grupo, y para $\cdot$ las propiedades del último grupo.

Si Si $(A, +, \cdot)$ y $(A', +, \cdot)$ son cuerpos estaríamos ante un **homomorfismo de cuerpos**.

4.6.4. Homomorfismo de conjuntos ordenados

Si tenemos dos conjuntos ordenados $(U, \preceq)$ y $(V, \preccurlyeq)$ una aplicación $f : U \longrightarrow V$ se denomina **homomorfismo de estructuras ordenadas** si es creciente, es decir:

$$\forall a, b \in U, a \preceq b \Rightarrow f(a) \preceq f(b)$$

Si f es biyectiva estaremos ante un **isomorfirmos de estructuras ordenadas**.

5 Los números naturales y los números enteros

5.1. Los números naturales

Los números naturales se definen mediante los axiomas de Peano:

1. El elemento 0 es un número natural.
2. Todo elemento natural n tiene un único elemento sucesor que tambien es un número natural.
3. 0 no es el sucesor de ningún número natural.
4. Dos números naturales cuyos sucesores sean iguales, son iguales.
5. Si un conjunto de número naturales incluye al 0 y a todos los sucesores de cada uno de los elementos, incluye a todos los números naturales.

Se denotan de la siguiente manera, teniendo en cuenta si incluyen al 0 o no:

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

En resumen:

- Todo número natural $n \neq 0$ es sucesor de algún número natural.
- Para todo $n \in \mathbb{N}, n \neq s(n)$.

5.1.1. Suma

Se define mediante recursión sobre n la suma $m + n$ mediante:

1. $m + 0 = n$ para todo $m \in \mathbb{N}$.

2. $m + s(n) = s(m + n)$ para todo $m, n \in \mathbb{N}$.

La suma de números naturales es una operación interna en $\mathbb{N}$ que satisface, cualesquiera que sean $m, n, p \in \mathbb{N}$, las siguientes propiedades:

1. Existencia de elemento neutro: $m + 0 = 0 + m = m$.

2. Asociativa: $(m + n) + p = m + (n + p)$.

3. Conmutativa: $m + n = n + m$.

4. Cancelativa: $m + p = n + p \Rightarrow m = n$.

5.1.2. Producto

Se define por recurrencia sobre n el producto, que designamos por $m \cdot n$ o mn, de los numeros naturales m y n mediante:

1. $m \cdot 0 = 0$ para todo $n \in \mathbb{N}$.

2. $m \cdot s(n) = m \cdot n + m$ para todo $m, n \in \mathbb{N}$.

El producto de números naturales es una operación interna en $\mathbb{N}$ que satisface, cualesquiera que sean $m, n, p \in \mathbb{N}$, las siguientes propiedades:

1. Existencia de elemento neutro: $m \cdot 1 = 1 \cdot m = m$.

2. Distributiva: $m(n + p) = mn + mp$ y $(n + p)m = nm + pm$.

3. Asociativa: $(m \cdot n) \cdot p = m \cdot (n \cdot p)$.

4. Conmutativa: $m \cdot n = n \cdot m$.

5. Cancelativa: $mp = np \wedge p \neq 0 \Longrightarrow m = n$.

Se define la potencia n-ésima de a, a^n, mediante:

1. $0^n = 0$ para todo $n \in \mathbb{N}*$.
2. $a^0 = 1$ para todo $a \in \mathbb{N}*$.
3. $a^{n+1} = aa^n$ para todo $a \in \mathbb{N}*$ y $n \in \mathbb{N}$.

5.1.3. Ordenación de números naturales

Dados $m, n \in \mathbb{N}$ se define la relación *menor o igual*, $\leq$, mediante:

$$\exists p \in \mathbb{N}, m + p = n \Rightarrow m \leq n$$

Se define *estrictamente menor*,$<$ como:

$$m \leq n \wedge m \neq n \Rightarrow m < n$$

Además, se obtiene la siguiente relación:

$$m < n \Leftrightarrow m + 1 \leq n$$

Las relaciones *mayor o igual*, $\geq$, y *estrictamente mayor*, $<$, se definen como:

$$m \geq n \Leftrightarrow n < m$$
$$m < n \Leftrightarrow n \leq m$$

La relación $\leq$ es una *relación de orden* total en $\mathbb{N}$, compatible con la suma y producto de número naturales, es decir para todo $m, n, p \in \mathbb{N}$ se tiene:

$$m \leq n \Rightarrow \begin{cases} m + p \leq n + p \\ mp \leq np \end{cases}$$

El intervalo abierto $(n, n + 1)_{\mathbb{N}}$ es vacío, para todo $n \in \mathbb{N}$.

El conjunto $\mathbb{N}$ con la relación $\leq$ es un conjunto bien ordenado.

En $\mathbb{N}$, todo subconjunto no vacío y acotado superiormente, tiene máximo.

5.2. Conjuntos finitos

Un conjunto A es **finito** si es vacío o si existe una biyección de A sobre un listado cerrado $[1, n]_{\mathbb{N}}$, con $n \neq 0$. En caso contrario, se dice que el conjunto es **infinito**.

Los intervalos cerrados tienen las siguientes propiedades:

- Si $n, m \in \mathbb{N}$ y existe una aplicación inyectiva $f : [1, n]_{(\mathbb{N})} \longrightarrow [1, m]_{(\mathbb{N})}$ entonces $n \leq m$.
- Si $n, m \in \mathbb{N}$ y existe un biyección $f : [1, n]_{(\mathbb{N})} \longrightarrow [1, m]_{(\mathbb{N})}$ entonces $n = m$.

Sea A un conjunto finito no vacío. Existe un único número natural n, no nulo, tal que A y $[1, n]_{\mathbb{N}}$ son equipotentes. Se dice entonces que $card(A) = n$.

Si $n \in \mathbb{N}$ entonces toda aplicación inyectiva $f : [1, n]_{(\mathbb{N})} \longrightarrow [1, n]_{(\mathbb{N})}$ es biyectiva.

Sea A un subconjunto no vacío de $\mathbb{N}$. A es un conjunto finito si y sólo si A es un conjunto acotado superiormente.

Esta propiedad presenta los siguientes corolarios:

- $\mathbb{N}$ es un conjunto finito.
- Todo subconjunto de un subconjunto finito de $\mathbb{N}$ es finito.
- La unión de dos subconjuntos finitos de $\mathbb{N}$ es un subconjunto finito.
- El complementario de un subconjunto finito de $\mathbb{N}$ es un conjunto infinito.

Sea A un subconjunto de un conjunto finito de B y $A \neq B$. Entonces A es un conjunto finito y $card(A) < card(B)$.

Sea A un conjunto finito y f una aplicación de A en cualquier conjunto B. Entonces $f(A)$ es un conjunto finito y

$$card(f(A)) \leq card(A)$$

Además, $card(f(A)) = card(A)$ si y sólo si f es inyectiva.

Si f es una aplicación sobreyectiva de un conjunto finito A en un conjunto B, entonces:

$$card(B) \leq card(A)$$

Además, se tiene la igualdad $card(A) = card(B)$ si y sólo si f es una aplicación biyectiva.

Sean A y B dos conjuntos finitos de igual cardinal y sea una aplicación $f : A \longrightarrow B$. Son equivalentes:

1. f es inyectiva.
2. f es biyectiva.
3. f es sobreyectiva.

Sean A y B dos conjuntos finitos disjuntos. Entonces $A \cup B$ es un conjunto finito y:

$$card(A \cup B) = card(A) + card(B)$$

Sean A y B dos conjuntos finitos. Entonces $A \cup B$ y $A \cap B$ son conjuntos finitos y

$$card(A \cup B) + card(A \cap B) = card(A) + card(B)$$

Sean A y B dos conjuntos finitos. Entonces, $A \times B$ es un conjunto finito y

$$card(A \times B) = card(A) \cdot card(B)$$

Sean A y B dos conjuntos finitos. Supongamos que $a = card(A) \neq 0$ y $b = card(B) \neq 0$. Entonces

$$card(\mathcal{F}(A, B)) = card(B^A) = b^a$$

Sea A un conjunto finito. Entonces

$$card(\mathcal{P}(A)) = 2^{card(A)}$$

Sea A y B dos conjuntos finitos cuyos cardinales son $card(A) = n \neq 0$ y $card(B) = m \neq 0$. Entonces el número de aplicación inyectivas de A en B es

$$card(\mathcal{I}(A, B))) = m(m-1)\cdots(m-n+1)$$

El número anterior se conoce como **variaciones de** m **sobre** n $V_{m,n}$:

$$V_{m,n} = m(m-1)\cdots(m-n+1) = \frac{m!}{(m-n)!}$$

Sea A y B dos conjuntos finitos cuyos cardinales son $card(A) = card(B) = n$. Entonces el número de aplicaciones biyectivas de A en B es:

$$card(\mathcal{B}(A, B)) = n!$$

Sea A un conjunto finito tal que $card(A) = m$. Sea $0 \leq n \leq m$. El número de subconjuntos de A que poseen exactamente n elementos es

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

Es número se lee *msobren* y se denomina **coeficiente binomial**, **número combinatorio** o **combinaciones de m sobre en** $C_{m,n}$.

5.3. Conjuntos infinitos

Sea A un conjunto cualquiera. Entonces el conjunto $\mathcal{P}(A)$ y el conjunto A no son equipotentes.

Un conjunto A se considera **numerable** si es equipotente con $\mathbb{N}$. El cardinal de los conjuntos numerables se denota como *aleph sub zero* $\aleph_0$.

Sea A un subconjunto de $\mathbb{N}$. Entonces A es un conjunto finito o A es un conjunto numerable.

El conjunto $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ es numerable.

Se satisfacen las siguientes propiedades:

1. Todo subconjunto de un conjunto numerable es finito o numerable.

2. El producto de conjuntos numerables es numerable.

3. La unión de dos conjuntos numerables es numerables.

4. La unión numerable de conjuntos numerables es numerable.

5.4. Los números enteros

En $\mathbb{N} \times \mathbb{N}$ se define la relación de equivalencia $\mathcal{E}$:

$$(a, b)\mathcal{E}(a', b') \Leftrightarrow a + b' = a' + b$$

El **representante canónico del número entero** α es el par (m, n) donde al menos una de sus componentes es nula.

5.4.1. Operaciones en $\mathbb{Z}$

Sean $\alpha, \beta \in \mathbb{Z}$ y sean $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ sendos representantes. Se define:

$$\alpha + \beta = (a + c, b + d)$$
$$\alpha\beta = (ac + bd, bc + ad)$$

$\mathbb{Z}$ es una anillo conmutativo unitario.

$$\alpha \cdot 0 = 0 \cdot \alpha = 0$$
$$\alpha, \beta \in \mathbb{Z}, \alpha\beta = 0 \Rightarrow \alpha = 0 \vee \beta = 0$$

5.4.2. Orden en $\mathbb{Z}$

Dados $\alpha, \beta \in \mathbb{Z}$:

$$\alpha \leq \beta \Leftrightarrow \beta - \alpha \in \mathbb{Z}_+$$

$(\mathbb{Z}, +, \cdot, \leqslant)$ es un anillo totalmente ordenado.

5.4.3. Identificación de $\mathbb{N}$ con $\mathbb{Z}_+$

Todo subconjunto de $\mathbb{Z}$ no vacío y acotado

1. superiormente tiene máximo.
2. inferiormente tiene mínimo.

Propiedad arquimediana de $\mathbb{Z}$

Dados $\alpha, \beta \in \mathbb{Z}$ si $\alpha > 0$ entonces existe $n \in \mathbb{N}$ tal que $n\alpha \geq \beta$.