# Conjuntos

José Cuevas Barrientos

30 de junio de 2021

# *Índice general*

# *Preámbulo*

**Pre-requisitos.** Este libro no presupone requisitos, al menos no desde el punto de vista formal. Me explico: éstos apuntes pretenden ser el primer acercamiento axiomático para un lector cualquiera, pero advierto que saltar desde el reino de las matemáticas intuitivas al de las matemáticas lógicas no es tan sencillo. Sí, el libro no utiliza ningún teorema que no esté demostrado en sí mismo, o en otro de mi autoría, pero avanza con una velocidad que asume familiaridad con ciertas definiciones básicas, por ejemplo, en el libro se construyen los números y las operaciones entre ellos (adición, producto y potencias), pero si usted no entiende bien conceptos elementales como la regla de signos en el producto de enteros, éste libro no lo va a aclarar.

**Métodos y objetivos.** El libro comienza con una explicación de las leyes lógicas fundamentales, seguido de una introducción axiomática a la teoría de conjuntos; hay varios libros mucho más sencillos que optan por evitar los sistemas axiomáticos, pero personalmente prefiero matar dos pájaros de un tiro con éste enfoque, además de que es más claro para mí. Luego se estudia el tema del buen orden que se relaciona a los números ordinales, que para ciertos contextos resultan un poco más abstracto, pero son elementales en la teoría de conjuntos.

**Orden y propósitos.** Aquí se explican a grandes rasgos los contenidos y objetivos de cada capítulo, así como sus relaciones entre sí:

1. **Teoría axiomática de conjuntos:** Se presentan dos modelos de axiomas conocidos, el de Zermelo-Fraenkel (ZF) y el de von Neumann-

Bernays-Gödel (NBG), mediante los cuáles se construyen las operaciones elementales (unión, intersección, diferencia, producto y complemento relativo). Luego se definen dos objetos fundamentales para toda rama matemática: las relaciones y las funciones, así como propiedades básicas que pueden o no poseer. Se define también el concepto de categoría que, si bien abstracto, es (implícita y) universalmente aplicado en un sinfín de contextos. Se termina por construir los números naturales mediante los axiomas de Dedekind-Peano, los números enteros y los números racionales a partir del concepto de relación de equivalencia, y también se discute la aritmética entre estos tres conjuntos.

2. **Orden y ordinales:** Se definen distintos tipos de ordenamientos, así como elementos especiales (cotas, elementos minimales, etc.). Se observa que los llamados conjuntos *bien ordenados* son "similares", con lo cual se busca definir unos representantes que son los llamados *números ordinales*. Se estudia la aritmética entre ordinales, así como tipos de funciones. Se termina por presentar el axioma de regularidad y su relación a los ordinales.

3. **Cardinalidad y elección:** Se define el concepto de *equipotencia* que era la forma en la que Cantor describía la cualidad de "tener la misma cantidad" entre conjuntos. Tras lo cuál, al igual que con el buen orden, se busca construir posibles representantes. Un subconjunto de los ordinales parece un buen candidato, pero ¿lo es? La respuesta, bastante profunda, se relaciona a una de las proposiciones más controversiales de las matemáticas, el axioma de elección (AE); con lo que se comienza a discutir las equivalencias y formas en las que se presenta. El capítulo continua discutiendo la aritmética entre cardinales (principalmente asumiendo formas del AE), que abren la puerta a varios tópicos del maravilloso y complicado mundo de la teoría de conjuntos intermedia.

Parte I.

# Teoría básica de conjuntos

# 1

# *Teoría de conjuntos axiomática*

En este capítulo se pretenden dar todos los fundamentos, definiciones y propiedades básicas que se emplean tanto a lo largo de todo el texto como a lo largo del resto de la literatura matemática. Para ello se emplea una metodología formal y sistemas axiomáticos, en particular, se discuten los dos sistemas más populares y útiles para el texto: la teoría de Zermelo-Fraenkel (ZF) y la de von Neumann-Bernays-Gödel (NBG).

## 1.1. Introducción a la lógica proposicional

> **Definición 1.1 – *Proposición*:** Se dice que una expresión es una *proposición* si posee un valor no-ambiguo de verdad (i.e., o es verdadero, o es falso). Se suelen denotar las proposiciones con las letras $p, q, r, \ldots$

Ejemplos de proposiciones son: "Isaac Newton nació el 25 de diciembre", "Amsterdam es una ciudad" y "las naranjas son verduras" (la última siendo falsa).

Nótese que si $p$ y $q$ son proposiciones, podemos usarlas para formar otras proposiciones, por ejemplo "Newton nació el 25 de diciembre o Amsterdam es una ciudad". A ésta clase de proposiciones les decimos *compuestas* y los símbolos que nos permiten componer proposiciones se llaman *signos lógicos*, los más populares son los siguientes:

**Negador** (denotado $\neg$, léase "no") es aquel que revierte el valor de verdad

de una proposición. Osea, si $p$ es verdadero, $\neg p$ es falso y viceversa; éste comportamiento se puede reducir en la siguiente tabla de verdad.

| $p$ | $\neg p$ |
|---|---|
| V | F |
| F | V |

**Conjuntor** (denotado $\wedge$, léase "y") es aquel que es verdadero siempre que sus partes lo sean.

| $p$ | $q$ | $p \wedge q$ |
|---|---|---|
| V | V | V |
| F | V | F |
| V | F | F |
| F | F | F |

**Disyuntor** (denotado $\vee$, léase "o") es aquel que es verdadero cuando alguna de sus partes lo sean.

| $p$ | $q$ | $p \vee q$ |
|---|---|---|
| V | V | V |
| F | V | V |
| V | F | V |
| F | F | F |

**Implicador** (denotado $\Longrightarrow$, léase "si ... entonces ...") es aquel que es falso cuando el primero (llamado condición) es verdadero y el segundo (llamado deducción) es falso.

| $p$ | $q$ | $p \Longrightarrow q$ |
|---|---|---|
| V | V | V |
| F | V | F |
| V | F | V |
| F | F | V |

**Coimplicador** (denotado $\Longleftrightarrow$, léase "si y sólo si") es aquel que es verdadero cuando ambas proposiciones comparten valor de verdad.

| $p$ | $q$ | $p \Longleftrightarrow q$ |
|---|---|---|
| V | V | V |
| F | V | F |
| V | F | F |
| F | F | V |

**Definición 1.2 – *Tautología*:** Se dice que una proposición compuesta $P$ que depende de otras $p, q, \ldots$ es una *tautología* si es siempre cierta, independiente de los valores de verdad de $p, q, \ldots$. Así mismo, $P$ es una *contradicción* si es siempre falsa.

Por ejemplo, "V" es una tautología y "F" una contradicción. Es obvio que si $P$ es una tautología, entonces $\neg P$ es una contradicción y viceversa. Un ejemplo de tautología es $p \vee \mathrm{V}$. En general denotaremos $P \equiv Q$ si $P \iff Q$ es una tautología, ésto se hace para no repetir tanto el " $\iff$ ".

Las siguientes tautologías, por su popularidad, se dicen *leyes lógicas*:

1. $p \wedge p \equiv p$ (idempotencia).
2. $p \vee p \equiv p$ (idempotencia).
3. $p \wedge q \equiv q \wedge p$ (conmutatividad).
4. $p \vee q \equiv q \vee p$ (conmutatividad).
5. $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ (asociatividad).
6. $(p \vee q) \vee r \equiv p \vee (q \vee r)$ (asociatividad).
7. $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ (distributividad).
8. $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$ (distributividad).
9. $p \wedge V \equiv p$ (neutro).
10. $p \vee F \equiv p$ (neutro).
11. $\neg(p \wedge q) \equiv \neg p \vee \neg q$ (ley de De Morgan).
12. $\neg(p \vee q) \equiv \neg p \wedge \neg q$ (ley de De Morgan).
13. $p \iff p$.
14. $p \iff q \equiv q \iff p$ (conmutatividad).
15. $(p \iff q) \iff r \equiv p \iff (q \iff r)$ (asociatividad).
16. $p \iff q \equiv (p \implies q) \wedge (q \implies p)$ (caracterización del coimplicador).
17. $p \vee q \equiv \neg p \implies q$ (caracterización del disyuntor).
18. $p \implies q \equiv (p \wedge \neg q) \implies F$ (demostración por contradicción).

De momento éste es el lenguaje básico de las matemáticas. En la teoría de modelos uno comienza a fundamentar y detallar éstos objetos, mediante varias definiciones que incluyen por ejemplo el concepto de *sentencia* que viene a ser algo así como una "oración formalmente formulada" (como $2+2=4$) que sustituye al de proposición, ya que una sentencia puede no tener valor de verdad, pero siempre se puede comprender; en este sentido las matemáticas pueden definirse como el estudio de las sentencias puesto que hasta encontrar una demostración (o un contraejemplo), éstas quedan como "preguntas abiertas".

## 1.2. Axiomas y el lenguaje de ZF

**Axiomas: ¿qué son y para qué sirven?** Como se apreció en la primera sección para poder demostrar que un teorema $Q$ es cierto, se requiere de algún teorema $P$ que sea cierto que haga cumplir $P \implies Q$, por ende, es aparente la necesidad de tener puntos de partida; a estas proposiciones básicas que se les asume como verdaderas sin previa demostración es a lo que llamamos *axiomas*. Una característica de los axiomas es que como son la base de todo nuestro conocimiento y van a ser los cimientos de toda la teoría que desarrollemos, estos deben ser sencillos de manera que sean accesibles para los nuevos científicos, y además tendremos discusiones sobre el por qué de su existencia. Estas discusiones serán particularmente extensas con el axioma de elección (y derivados) y el axioma de regularidad.

Algo que notar es que como estamos en una etapa tan temprana que hasta carece de elementos, no podemos siquiera definir objetos, sino que los axiomas sirven como descriptores de sus características. Para enfatizar la importancia de la lógica, los axiomas serán escritos tanto en castellano como con lenguaje lógico.

**Axioma de Extensionalidad:** Dos conjuntos se dicen iguales syss comparten todos sus elementos.

$$\forall xy\,(x = y \iff \forall z\,(z \in x \iff z \in y)).$$

Nótese que el axioma de extensionalidad nos da un criterio básico para describir a los conjuntos, sin embargo, nada nos dice que siquiera existan los conjuntos. Por eso, pese a que suene trivial, debemos introducir un axioma que nos diga que existe algún tipo de conjunto:

**Axioma del Conjunto Vacío:** Existe un conjunto que no posee

elementos.

$$\exists x \forall y \ (y \in x \iff y \neq y).$$

El axioma de extensionalidad nos dice que dicho conjunto es único, luego denotaremos a dicho conjunto como $\varnothing$ y le llamamos *conjunto vacío*.

**Definición 1.3 – *Sub-, superconjunto*:** Se escribe $x \subseteq y$ (léase "$x$ es subconjunto de $y$", "$x$ está contenido en $y$" o "$y$ es superconjunto de $x$") si todos los elementos de $x$ son también elementos de $y$, en lenguaje formal:

$$\forall xy \ (x \subseteq y \iff \forall z \ (z \in x \implies z \in y)).$$

Se le añade el sufijo *propio* si además los conjuntos son distintos y se denota como $x \subset y$, es decir

$$\forall xy \ (x \subset y \iff x \subseteq y \land x \neq y).$$

**Proposición 1.4:** Para todo $A, B, C$ se cumple:

1. $\varnothing \subseteq A$.
2. $A \subseteq A$ (reflexividad).
3. $A \subseteq B$ y $B \subseteq C$ implican $A \subseteq C$ (transitividad).
4. $A \subseteq B$ y $B \subseteq A$ implican $A = B$ (antisimetría).

**Axioma de Especificación:** Dado un predicado $\phi(z)$ y un conjunto $x$, existe otro $y$ cuyos elementos son los elementos de $x$ que hacen cumplir $\phi(x)$.

$$\forall x \exists y \forall z \ (z \in y \iff z \in x \land \phi(x)).$$

Notemos que por al axioma de extensionalidad, el conjunto formado es siempre único, en cuyo caso denotaremos a tal $y$ como

$$y := \{z \in x : \phi(z)\}.$$

El axioma de especificación nos dice que podemos formar cualquier tipo de subconjuntos que queramos, ¿pero por qué tiene que definir subconjuntos de otro fijo? ¿Por qué no se puede construir conjuntos arbitrarios dada una proposición formal? Originalmente, la teoría de Frege incluía al *axioma de*

*comprensión* que poseía dichas cualidades, pero pronto se mostró que dicha teoría era **inconsistente**, i.e., llegaba lógicamente a contradicciones, y una de las primeras pruebas de ello es la siguiente:

**Teorema 1.5 – *Antinomia de Russell*:** No existe un conjunto que contenga a todos los conjuntos que no se contienen a sí mismos, es decir, no existe un conjunto que satisfaga:

$$R := \{x : x \notin x\}.$$

Demostración: Lo probaremos por contradicción: Supongamos que $R$ existe y es conjunto. Luego, ¿$R \in R$? Si la respuesta es que sí, entonces es porque cumple con la proposición $\phi(x) := x \notin x$, es decir, $R \notin R$ lo que es absurdo. Si la respuesta es que no, entonces como $R \notin R$ cumple con la condición para ser elemento de $R$, luego $R \in R$. En ambos casos se llega a una contradicción, luego $R$ no puede existir. □

Como consecuencia se demuestra también:

**Teorema 1.6 (Antinomia de Cantor):** No existe un conjunto que contenga a todos los conjuntos, es decir, no existe un conjunto que satisfaga:

$$V := \{x : x = x\}.$$

Esto, seguido de otra serie de paradojas o antinomias conjuntistas, que repasaremos en este texto, forzaron la creación de sistemas más restrictivos, siendo la teoría de Zermelo la más popular entre ellas. Al final del capítulo al hablar de la teoría NBG veremos también como se proponen otras soluciones a este problema.

**Proposición 1.7:** Todo conjunto $x$ posee un subconjunto $R(x) \subseteq x$ tal que $R(x) \notin x$.

Demostración: Sea $R(x) := \{y \in x : y \notin y\}$. Por definición es subconjunto de $x$, pero veamos que si $R(x) \in x$ entonces entramos en el bucle de si $R(x) \in R(x)$, luego $R(x) \notin x$. □

**Corolario 1.8:** Para todo $x$ existe $y$ tal que $x \subset y$.

Demostración: Basta notar que $x \subset x \cup \{R(x)\}$. □

**Axioma del Par (Desordenado):** Para todo par de conjuntos $x, y$ existe un conjunto $z$ cuyos elementos son únicamente $x$ e $y$.

$$\forall xy \exists z \forall t \ (t \in z \iff t = x \vee t = y).$$

Por extensionalidad, $z$ es único y se denota $z := \{x, y\}$. También denotaremos $\{x\} := \{x, x\}$.

**Proposición 1.9:** Si $\{a, b\} = \{c, d\}$, entonces $a = c$ y $b = d$ o $a = d$ y $b = c$.

**Proposición 1.10:** Definiendo $(x, y) := \{\{x\}, \{x, y\}\}$, se cumple que $(a, b) = (c, d)$ syss $a = c$ y $b = d$.

Es por esto, que al conjunto $(x, y)$ le llamamos par ordenado. Este fue propuesto por Kuratowski, pero Wiener también propuso la definición de par ordenado como

$$(x, y) := \{\{\varnothing, \{x\}\}, \{\{y\}\}\}.$$

Ambas definiciones cumplen con la propiedad anterior, que es la que en esencia define el par ordenado.

En general notemos que como todos los elementos de nuestra teoría de conjuntos, naturalmente habrán ocasiones en las que queramos hablar de conjuntos cuyos miembros son, a su vez, conjuntos; en cuyo caso les diremos *familias* de conjuntos.

**Axioma de la Unión:** Dada una familia de conjuntos $\mathcal{F}$, existe un conjunto que contiene a todos los miembros de los miembros de $\mathcal{F}$.

$$\forall \mathcal{F} \exists x \forall y \ (y \in x \iff \exists S \ (S \in \mathcal{F} \wedge y \in S)).$$

En general denotamos que $y := \bigcup \mathcal{F} = \bigcup_{S \in \mathcal{F}} S$. También denotamos $x \cup y := \bigcup \{x, y\}$.

**Proposición 1.11:** Dados los conjuntos $x_1, x_2, \ldots, x_n$ existe un único conjunto $y$ cuyos elementos son solamente los $x_i$ al que denotamos:

$$y := \{x_1, x_2, \ldots, x_n\}$$

Demostración: Notemos que podemos formar una terna desordenada

$$\{x_1, x_2, x_3\} := \{x_1, x_2\} \cup \{x_1, x_3\}; \quad \{x_1, x_2, x_3, x_4\} := \{x_1, x_2, x_3\} \cup \{x_1, x_4\};$$

y así procedemos recursivamente hasta formar $\{x_1, x_2, \ldots, x_n\}$. La unicidad, como de costumbre, se deduce del axioma de extensionalidad. □

**§1.2.1 Operaciones y álgebra de conjuntos.** Entre conjuntos hay varios tipos de operaciones fundamentales que se suelen emplear a lo largo de toda la matemática contemporánea. Para ilustrar mejor el significado de éstas operaciones adjuntaremos los llamados diagramas de Venn, dos conjuntos serán representados como círculos y el área acharada corresponde a la operación.

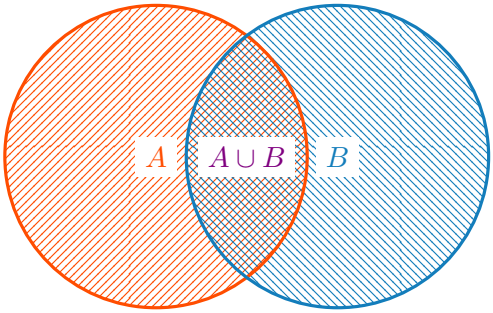



Figura 1.1. Diagrama de Venn de la unión.

**Proposición 1.12 (Propiedades de la unión):** Sean $A, B, C, D$ conjuntos, entonces:

1. $\bigcup \varnothing = \varnothing$.
2. $\bigcup \{x\} = x$.
3. $A \cup A = A$ (idempotencia).
4. $(A \cup B) \cup C = A \cup (B \cup C)$ (asociatividad).
5. $A \cup \varnothing = A$ (elemento neutro).
6. $A \cup B = B \cup A$ (conmutatividad).
7. $A \subseteq A \cup B$ y $B \subseteq A \cup B$.
8. $A \subseteq B$ syss $A \cup B = B$.
9. $A \subseteq C$ y $B \subseteq D$ implica $A \cup B \subseteq B \cup C \subseteq C \cup D$.
10. $A, B \subseteq C$ implica $A \cup B \subseteq C$.
11. Si para todo $A \in \mathcal{A}$ se cumple que $A \subseteq B$, entonces $\bigcup \mathcal{A} \subseteq B$.

**Definición 1.13 – *Intersección*:** Dada una familia de conjuntos $\mathcal{X}$, denotamos por $\bigcap \mathcal{X}$ al conjunto dado por los elementos que pertenezcan a todos los miembros de $\mathcal{X}$, i.e

$$\bigcap \mathcal{X} := \left\{ x \in \bigcup \mathcal{X} : \forall y \, (y \in \mathcal{X} \implies x \in y) \right\}.$$

Llamaremos intersección binaria entre $x$ e $y$ a $x \cap y := \bigcap \{x, y\}$, es decir, $x \cap y$ es el conjunto de los elementos de $x$ e $y$ que tienen en común. Diremos que dos conjuntos son *disjuntos* si su intersección es vacía.

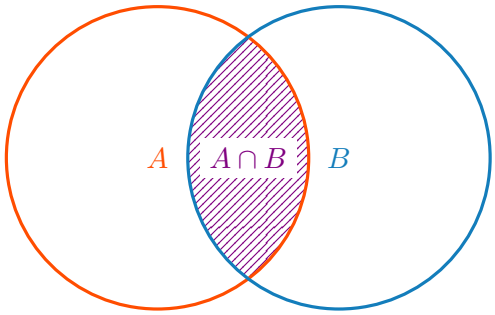



**Figura 1.2.** Diagrama de Venn de la intersección.

**Proposición 1.14 (Propiedades de la intersección):** Sean $A, B, C, D$ conjuntos, entonces:

1. $A \cap A = A$ (idempotencia).
2. $(A \cap B) \cap C = A \cap (B \cap C)$ (asociatividad).
3. $A \cap \varnothing = \varnothing$ (aniquilador).
4. $A \cap B = B \cap A$ (conmutatividad).
5. $A \cap B \subseteq A$ y $A \cap B \subseteq B$.
6. $A \subseteq B$ syss $A \cap B = A$.
7. $A \subseteq C$ y $B \subseteq D$ implica $A \cap B \subseteq B \cap C \subseteq C \cap D$.
8. $A \subseteq B, C$ implica $A \subseteq B \cap C$.

9. Si para todo $B \in \mathcal{B}$ se cumple que $A \subseteq B$, entonces $A \subseteq \bigcap \mathcal{B}$.
10. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributividad).
11. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributividad).

**Definición 1.15 – *Resta conjuntista*:** Siendo $A, B$ conjuntos se define $A \setminus B$ como los elementos de $A$ que no están en $B$, i.e.

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

Por notación abreviaremos $A_{\neq x} := A \setminus \{x\}$.

Por la paradoja de Cantor es claro que no podemos hablar de un conjunto universo absoluto, pero usualmente nos restringiremos a lo que diremos un universo *relativo* $U$, bajo el cuál definimos el complemento de un conjunto $A$ como los elementos de $U$ que le faltan, osea

$$A^c := \{x \in U : x \notin A\} = U \setminus A.$$

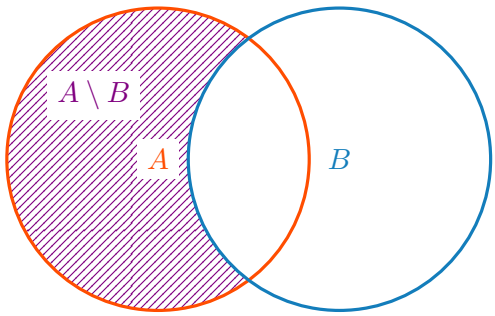



Figura 1.3. Diagrama de Venn de la diferencia.

**Proposición 1.16:** Sean $A, B, C$ conjuntos contenidos en un universo $U$, entonces:

1. $(A^c)^c = A$ (doble complemento).
2. $A \cup A^c = U$ y $A \cap A^c = \varnothing$.
3. $U^c = \varnothing$ y $\varnothing^c = U$.
4. $(A \cup B)^c = A^c \cap B^c$ (ley de De Morgan).

5. $(A \cap B)^c = A^c \cup B^c$ (ley de De Morgan).
6. $A \setminus B = A \cap B^c$.
7. $A \subseteq B$ syss $B^c \subseteq A^c$.
8. $A \setminus B = \varnothing$ syss $A \subseteq B$.
9. $A \cap B = \varnothing$ syss $A \subseteq B^c$.

**Axioma por Partes:** Para todo conjunto $x$, existe otro $y$ que contiene a todos los subconjuntos de $x$.

$$\forall x \exists y \forall z \ (z \in y \iff z \subseteq x).$$

El conjunto $y$ es único y se suele llamar *conjunto potencia* de $x$, usualmente denotado $\mathcal{P}(x)$ o $\mathrm{Sub}(x)$.

**Proposición 1.17:** Para todo $A, B, C$ se cumple:

1. $\varnothing, A \in \mathcal{P}(A)$.
2. $\mathcal{P}(\varnothing) = \{\varnothing\}$.
3. $\bigcup \mathcal{P}(A) = A$.
4. $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ syss $A \subseteq B$.
5. $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
6. $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$.
7. $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$ syss $A \subseteq B$ o $B \subseteq A$.

## 1.3. Relaciones y funciones

**Definición 1.18 – *Producto cartesiano y relaciones*:** Se define el producto cartesiano[a] entre $A$ y $B$ como el conjunto de todos los posibles pares ordenados con primera coordenada en $A$ y segunda en $B$, es decir

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

Podemos definir el producto cartesiano entre varios conjuntos de forma

recursiva como:

$$X_1 \times X_2 \times \cdots X_n \times X_{n+1} := (X_1 \times X_2 \times \cdots X_n) \times X_{n+1}.$$

Y denotamos

$$X^n := \underbrace{X \times X \times \cdots \times X}_{n \text{ veces}}.$$

Se dice que $R$ es una relación $n$-aria si sus elementos son $n$-tuplas ordenadas, es decir, si es el subconjunto de un producto cartesiano. Si $R$ es binaria y $(a, b) \in R$ entonces lo anotaremos como que $aRb$, de lo contrario, $a\not{R}b$. Si $R$ es binaria, también definimos:

**Dominio** El conjunto de los elementos que ocupan la primera coordenada.

$$\operatorname{Dom} R := \{x : \exists y \ (xRy)\}.$$

**Imagen o rango** El conjunto de los elementos que ocupan la segunda coordenada.

$$\operatorname{Img} R := \{y : \exists x \ (xRy)\}.$$

**Campo** El conjunto de los elementos que ocupan cualquier coordenada.

$$\operatorname{Fld} R := \operatorname{Dom} R \cup \operatorname{Img} R.$$

En general si $R$ es binaria, $\operatorname{Dom} R \subseteq A$ y $\operatorname{Img} R \subseteq B$ lo abreviaremos como $R : A \multimap B$. Si $\operatorname{Fld} R \subseteq A$, entonces diremos que $R$ es relación sobre $A$.

[a] la. *Renatus Cartesius*: René Descartes.

Queda al lector comprobar por qué el producto cartesiano siempre existe como conjunto (para ello utilice y recuerde la definición de par ordenado de Kuratowski). No hay una forma estándar de visualizar el producto cartesiano entre conjuntos con diagramas de Venn, pero un tipo de diagrama consiste en dibujar los elementos de los conjuntos como puntos y ver el producto como el plano formado.

**Proposición 1.19 (Propiedades del producto cartesiano):** Sean $A, B, C, D$ conjuntos, entonces:

1. $A \subseteq C$ y $B \subseteq D$ implican $A \times B \subseteq C \times D$ (isotonía).
2. $A \times \varnothing = \varnothing \times A = \varnothing$ (aniquilador).

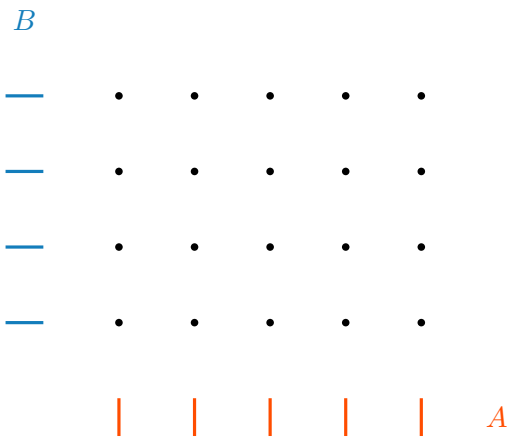



**Figura 1.4.** Diagrama del producto cartesiano.

3. $(A \cup B) \times C = (A \times C) \cup (B \times C)$ y $A \times (B \cup C) = (A \times B) \cup (A \times C)$ (distributividad).
4. $(A \cap B) \times C = (A \times C) \cap (B \times C)$ y $A \times (B \cap C) = (A \times B) \cap (A \times C)$ (distributividad).
5. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$ y $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$ (distributividad).

**Proposición 1.20 (Propiedades de las relaciones):** Si $R, S$ son relaciones:

1. $R \cup S$ es una relación y

$$\operatorname{Dom}(R \cup S) = \operatorname{Dom} R \cup \operatorname{Dom} S, \ \operatorname{Img}(R \cup S) = \operatorname{Img} R \cup \operatorname{Img} S.$$

2. $R \cap S$ es una relación y

$$\operatorname{Dom}(R \cap S) \subseteq \operatorname{Dom} R \cap \operatorname{Dom} S, \ \operatorname{Img}(R \cap S) \subseteq \operatorname{Img} R \cap \operatorname{Img} S.$$

3. $R \setminus S$ es una relación y

$$\operatorname{Dom} R \setminus \operatorname{Dom} S \subseteq \operatorname{Dom}(R \setminus S), \ \operatorname{Img} R \setminus \operatorname{Img} S \subseteq \operatorname{Img}(R \setminus S).$$

4. Si $R \subseteq S$, entonces

$$\operatorname{Dom} R \subseteq \operatorname{Dom} S, \qquad \operatorname{Img} R \subseteq \operatorname{Img} S.$$

5. Si $A$ es conjunto entonces $\mathrm{Id}_A := \{(a,a) \in A^2 : a \in A\}$ es una relación sobre $A$ llamada la *identidad* y cumple que $\mathrm{Dom}(\mathrm{Id}_A) = \mathrm{Img}(\mathrm{Id}_A) = \mathrm{Fld}(\mathrm{Id}_A) = A$.

6. $\varnothing$ es una relación con $\mathrm{Fld}\,\varnothing = \varnothing$ y es la única relación sobre $\varnothing$. Un dato curioso es que $\mathrm{Id}_\varnothing = \varnothing$.

7. Si $A, B$ son conjuntos, entonces $A \times B$ es relación sobre $A \cup B$. Si además son no vacíos entonces $\mathrm{Dom}(A \times B) = A$ e $\mathrm{Img}(A \times B) = B$.

**Definición 1.21:** Sea $R$ una relación binaria y sea $X$ arbitrario, entonces llamamos la restricción de $R$ a $X$ a la relación

$$R|_X = R \restriction X := \{(x,y) : (x,y) \in R \wedge x \in X\}.$$

Se define la imagen de un conjunto $X$ general como

$$R[X] := \mathrm{Img}(R|_X) = \{y : \exists x \in X\ (x,y) \in R\}$$

Se define la *composición* de dos relaciones como

$$R \circ S := \{(x,z) : \exists y\ ((x,y) \in R \wedge (y,z) \in S)\}$$

Y se define la relación *inversa* como

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

**Proposición 1.22:** Si $R, S, T$ son relaciones y $A, B$ conjuntos:

1. $\varnothing$ es una relación sobre $A$ y es la única sobre $\varnothing$.

2. $\mathrm{Id}_A := \{(a,a) : a \in A\}$ y $A^2$ son relaciones sobre $A$.

3. Si $R$ es relación sobre $B$, entonces $R|_A$ lo es sobre $A$.

4. Si $\mathrm{Dom}\,R \subseteq A$ entonces $R|_A = R$. En cambio, si $B \cap \mathrm{Dom}\,R = \varnothing$, entonces $R|_B = \varnothing$.

5. Si $A \subseteq B$ entonces $R[A] \subseteq R[B]$.

6. $\mathrm{Id}_{\mathrm{Dom}\,R} \subseteq R \circ R^{-1}$ e $\mathrm{Id}_{\mathrm{Img}\,R} \subseteq R^{-1} \circ R$.

7. $\mathrm{Dom}(R \circ S) \subseteq \mathrm{Dom}\,R$ e $\mathrm{Img}(R \circ S) \subseteq \mathrm{Img}\,S$.

8. $(R \circ S) \circ T = R \circ (S \circ T)$.

**Proposición 1.23 (Propiedades de la inversa):** Si $R, S$ son relaciones:

1. $\operatorname{Dom}(R^{-1}) = \operatorname{Img} R$ e $\operatorname{Img}(R^{-1}) = \operatorname{Dom} R$.
2. $(R^{-1})^{-1} = R$.
3. $(R \cup S)^{-1} = R^{-1} \cap S^{-1}$.
4. $(R \cap S)^{-1} = R^{-1} \cup S^{-1}$.
5. $(R \setminus S)^{-1} = R^{-1} \setminus S^{-1}$.
6. Si $R \subseteq S$ entonces $R^{-1} \subseteq S^{-1}$.
7. Si $A$ es conjunto, entonces $\operatorname{Id}_A^{-1} = \operatorname{Id}_A$ y, en particular, $\varnothing^{-1} = \varnothing$.
8. Si $A, B$ son conjuntos entonces $(A \times B)^{-1} = B \times A$.

**Definición 1.24 – *Propiedades de las relaciones*:** Dada una relación $R$ sobre $X$, se dice que posee alguna de las siguientes características si para todos $x, y, z \in X$ se cumple:

**Reflexividad** $xRx$.

**Irreflexividad** $\neg xRx$.

**Simetría** $xRy \implies yRx$.

**Asimetría** $xRy \implies \neg(yRx)$.

**Antisimetría** $xRy \wedge yRx \implies x = y$.

**Transitividad** $xRy \wedge yRz \implies xRz$.

**Conexión** $xRy \vee yRx$.

**Unívocidad** $xRy \wedge xRz \implies y = z$.

**Definición 1.25 – *Función*:** Se dice que $f : A \multimap B$ es una función o aplicación si es una relación unívoca tal que $\operatorname{Dom} f = A$, en cuyo caso de notaremos $f : A \to B$. En este contexto, a $B$ se le dice el *codominio* de la función. De darse ésto, entonces $(x, y) \in f$ lo denotaremos como $f(x) = y$ y se dice que $y$ es **la** imagen de $x$, y que $x$ es **una** preimagen de $y$. La univocidad nos dice que todo punto del dominio posee una única imagen. Además de ello, se dice que una función puede ser:

**Inyectiva** Si no hay puntos del dominio que compartan imagen,

$$\forall xy \in A\ (f(x) = f(y) \implies x = y).$$

**Supra- o epiyectiva** Si todo punto del codominio posee preimagen,

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

**Biyectiva** Si es inyectiva y biyectiva, osea, si todo punto del codominio posee una única preimagen,

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

Se denota por $\operatorname{Func}(A, B)$ al conjunto de funciones de dominio $A$ y codominio $B$. Se denota por $\operatorname{Sym}(A)$ al conjunto de biyecciones de dominio y codominio $A$.

Notemos que el concepto de *ser suprayectiva* es relativamente informal porque depende del codominio que es un superconjunto arbitrario de la imagen de la función, esta noción es más útil en contextos algebraicos donde queremos buscar un nexo entre dos conjuntos específicos. Otra nota es que personalmente utilizo la palabra *suprayectiva*, no obstante, la palabra *epiyectiva* puede ser útil para asociar los conceptos con las nomenclatura categórica.

**Teorema 1.26:** Si $f : A \to B$ es función, entonces $f^{-1}$ es función syss $f$ es biyectiva. En cuyo caso $f \circ f^{-1} = \operatorname{Id}_A$ y $f^{-1} \circ f = \operatorname{Id}_B$.

**Proposición 1.27:** Si $f : A \to B$, $g : B \to C$ y $h : C \to D$, entonces:

1. $f \circ g : A \to C$.
2. Si $f \circ g$ es suprayectiva entonces $g$ también lo es.
3. Si $f \circ g$ es inyectiva entonces $f$ también lo es.

4. $\mathrm{Id}_A$ es biyectiva, luego $\mathrm{Id}_A \in \mathrm{Sym}(A)$ y se cumple que $\mathrm{Sym}(A)$ es siempre no vacío.

5. Si $f, g$ son ambas inyectivas (suprayectivas o biyectivas), entonces $f \circ g$ también lo es

6. Si $f, g$ son biyectivas, entonces $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

**§1.3.1 Funciones canónicas y productos generalizados.** La palabra *canónico* proviene del sustantivo griego κανών significando "regla" o "estándar". Éstas funciones son ejemplos clásicos que ilustran mejor la teoría.

- Si $\varnothing \neq A \subseteq B$, entonces se le llama *inclusión* de $A$ en $B$, denotado por $\iota$, a la aplicación tal que $\iota(a) = a$.

- A la inclusión de un conjunto sobre si mismo se le dice la función *identidad* y se denota por $\mathrm{Id}_A(a) = a$.

- Si $A_1, \ldots, A_n$ son conjuntos no vacíos y $(x_1, \ldots, x_n) \in A_1 \times \cdots \times A_n$, entonces se le llama *proyección sobre la $i$-ésima coordenada*, denotada por $\pi_i : A_1 \times \cdots \times A_n \to A_i$, a la aplicación tal que $\pi_i(x_1, \ldots, x_n) = x_i$.

**Proposición 1.28:** Se cumple:

1. La identidad es una biyección.

2. La inclusión es inyectiva.

3. La proyección (sobre cualquier coordenada) es suprayectiva.

**Productos y funciones.** En principio no es obvio, pero los productos pueden entenderse como funciones, simplemente basta notar que las tuplas pueden verse como funciones desde un conjunto de coordenadas a los otros: por ejemplo, un par $(x, y) \in A^2$ es equivalente a una función $f : \{1, 2\} \to A$ pues $(f(1), f(2)) \in A^2$.

Luego si $I$ es un conjunto no vacío cuyos elementos llamaremos *índices*, $\{X_i : i \in I\}$ es una familia de conjuntos no vacíos, entonces se puede entender:

$$\prod_{i \in I} X_i := \left\{ f : \left( f : I \to \bigcup_{i \in I} X_i \right) \wedge \forall i \in I \; f(i) \in X_i \right\}$$

Incluso si nuestra familia no tuviera un conjunto de índices, podemos tomar a cada conjunto de la familia como su propio índice, de modo que la definición anterior permite construir:

$$\prod_{x\in\mathcal{F}} x := \{f : f(x) \in x \in \mathcal{F}\}$$

Si nuestra familia está indexada, entonces también podemos conservar una proyección:

$$\boldsymbol{x} \in \prod_{i\in I} X_i \implies \pi_i(\boldsymbol{x}) := \boldsymbol{x}(i)$$

pues recordemos que $\boldsymbol{x}$ no es más que una función.

## 1.4. Tópicos opcionales

**§1.4.1 Clases y NBG.** En ZF vimos el axioma esquemático de especificación que nos permite construir conjuntos con propiedades pero que no son universales, sino que son parte de otro preexistente; la razón para esto yace en las paradojas de Russell y Cantor ya mencionadas, pero existe otro método para construir objetos más grandes sin producir contradicciones, la respuesta son las llamadas *clases propias* que forman parte de la teoría de von Neumann-Bernays-Gödel (NBG).

> **Definición 1.29:** Todo objeto de la teoría NBG es una clase. Una clase $A$ que es miembro de otra clase $B$ se dice un *conjunto*. Las clases que no son conjuntos se llaman *clases propias*.

Los axiomas de la teoría NBG son:

**Extensionalidad** Dos clases son iguales syss poseen los mismos miembros.

**Conjunto vacío** Existe un conjunto sin elementos.

**Par** Si $x, y$ son conjuntos, entonces $\{x, y\}$ es un conjunto.

**Unión** Si $\mathcal{F}$ es un conjunto cuyos miembros son conjuntos, entonces $\bigcup \mathcal{F}$ es un conjunto.

**Partes** Si $x$ es un conjunto, entonces $\mathcal{P}(x)$ es un conjunto.

**Comprensión** Dada una propiedad $\phi$ existe una clase $X$ cuyos miembros son los conjuntos $y$ que cumplen $\phi(y)$.

**Reemplazo** Si $F$ es una función y $x$ es un conjunto, entonces $F[x]$ es un conjunto.

Realmente los dos cambios significativos son los dos últimos axiomas que son los que dicen cosas acerca de las clases. Por el axioma de comprensión si podemos construir algo llamado la clase de Russell y la clase universo, pero en este caso las paradojas de Russell y Cantor se traducen en una demostración de que ambas son clases propias.

**§1.4.2 Teoría de categorías.** La teoría de categorías, más que una ser una teoría en si misma representa un lenguaje que varias ramas de las matemáticas, como el álgebra abstracta y la topología, emplean. Esto se debe a que por naturaleza, la teoría de categorías nos dirá acerca de una forma de equivalencia entre las relaciones de los elementos de dos o más conjuntos; mediante ella podremos describir formalmente una noción de equivalencia.

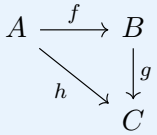
**Definición 1.30 – *Categoría*:** Una categoría $\mathsf{C}$ consta de:

1. Un conjunto $\mathrm{Obj}(\mathsf{C})$ de *objetos*.
2. Un conjunto $\mathrm{Morf}(\mathsf{C})$ de *morfismos* o *flechas*.
3. Un par de aplicaciones $\mathrm{Dom}, \mathrm{Cod} : \mathrm{Morf}(\mathsf{C}) \to \mathrm{Obj}(\mathsf{C})$. Si $f \in \mathrm{Morf}(\mathsf{C})$ cumple que $\mathrm{Dom}(f) = A$ y $\mathrm{Cod}(f) = B$, entonces abreviaremos todo esto como que $A \xrightarrow{f} B$. Se define

$$\mathrm{Hom}_{\mathsf{C}}(A, B) := \{f \in \mathrm{Morf}(\mathsf{C}) : A \xrightarrow{f} B\},$$
$$\mathrm{End}_{\mathsf{C}}(A) := \mathrm{Hom}_{\mathsf{C}}(A, A).$$

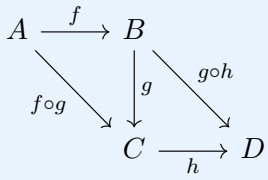
   (Se obviarán los subíndices cuando no haya ambigüedad sobre la categoría.)

4. Una operación $\circ$ tal que $A \xrightarrow{f} B$ y $B \xrightarrow{g} C$ cumpla que $A \xrightarrow{f \circ g} C$. Diremos que el siguiente diagrama:



conmuta syss $h = f \circ g$, o también cuando dos conjuntos de flechas que parten y terminan en los mismos lugares son iguales bajo composición.

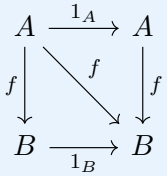
Otra condición para la composición es que sea asociativa, i.e., que el diagrama




conmute.

Se usaran flechas punteadas para indicar que existe un morfismo que hace que el diagrama conmute.

5. Una aplicación $1 : \mathrm{Obj}(\mathsf{C}) \to \mathrm{Morf}(\mathsf{C})$ tal que $1_A \in \mathrm{End}_{\mathsf{C}}(A)$, y que hace que el siguiente diagrama siempre conmute:

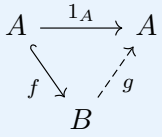



Dado eso podemos denotar $\mathsf{C} = (\mathrm{Obj}\,\mathsf{C}, \mathrm{Morf}\,\mathsf{C}, \mathrm{Dom}, \mathrm{Cod}, \circ, \mathrm{Id})$.
Se dice que una categoría es *pequeña* si $\mathrm{Obj}\,\mathsf{C}$ resulta ser un conjunto.

**Ejemplos.** En particular hay dos categorías que se usaran en este libro: la categoría $\mathsf{Set}_U = (U, \mathrm{Func}(U), \mathrm{Dom}, \mathrm{Img}, \circ, \mathrm{Id})$ y la categoría $\mathsf{Rel}_U := (U, \mathcal{P}(U^2), \mathrm{Dom}, \mathrm{Img}, \circ, \Delta)$. Notemos que éstas categorías no son pequeñas.

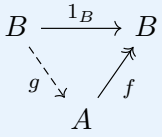
**Definición 1.31 – *Clasificación de morfismos*:** Fijada una categoría $\mathsf{C}$, se dice que un morfismo $A \xrightarrow{f} B$ es un:

**Monomorfismo** Si existe $B \xrightarrow{g} A$ tal que el siguiente diagrama conmuta:




Les denotaremos con la flecha $\hookrightarrow$.

**Epimorfismo** Si existe $B \xrightarrow{g} A$ tal que el siguiente diagrama conmuta:




Les denotaremos con la flecha $\twoheadrightarrow$.

**Isomorfismo** Si es un mono- y un epimorfismo al mismo tiempo. Les denotaremos con la flecha $\rightsquigarrow$ (algunos libros usan $\xrightarrow{\sim}$).

También fijada una categoría diremos que dos objetos de ella son *isomorfos* si existe un isomorfismo entre ellas. Claramente todo objeto de una categoría es isomorfo a sí mismo.

**Proposición 1.32:** Si $A \xrightarrow{f} B$ es un isomorfismo tal que $B \xrightarrow{g} A$ y $B \xrightarrow{h} A$ satisfacen que $f \circ g = 1_A$ y $h \circ f = 1_B$, entonces $g = h$.

Demostración: Basta notar que

$$g = 1_B \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ 1_A = h.$$

□

**Definición 1.33:** Si $A \xrightarrow{f} B$ es un isomorfismo, entonces llamaremos inversa, denotada $f^{-1}$, al único morfismo tal que $f \circ f^{-1} = 1_A$ y $f^{-1} \circ f = 1_B$.

Notemos que los isomorfismos de Set son las mismas aplicaciones biyectivas. Más adelante veremos que la noción de "isomorfismo" entre conjuntos se dice *equipotencia* en el capítulo 3.

**Definición 1.34 – *Funtor*:** Dadas dos categorías $\mathsf{A}$ y $\mathsf{B}$, se dice que una función $F$ es un *funtor* entre ambas si:

1. Para todo objeto $A$ de $\mathsf{A}$ se cumple que $F(A)$ es un objeto de $\mathsf{B}$.
2. Para todo morfismo $A \xrightarrow{f} B$ en $\mathsf{A}$ se cumple que $F(A) \xrightarrow{F(f)} F(B)$ en $\mathsf{B}$.
3. Si $A \xrightarrow{f} B$ y $B \xrightarrow{g} C$ en $\mathsf{A}$, entonces $F(f) \circ F(g) = F(f \circ g)$.
4. $F(1_A) = 1_{F(A)}$.

## 1.5. Sistemas numéricos

Para formalizar las nociones de los números se realizan una cadena de construcciones comenzando desde los naturales.

**§1.5.1 Los números naturales.** Para construir a los números naturales se utilizan los llamados axiomas de Dedekind-Peano. En éste texto primero definiremos un sistema de Peano como un conjunto cualquiera que cumple éstos axiomas, luego probaremos que en cierta forma todos éstos conjuntos tienen la misma forma, y finalmente discutiremos si existe algún sistema de Peano.

**Definición 1.35 – *Sistema de Peano*:** Se dice que una terna ordenada $(N, s, 0)$ es un *sistema de Peano* si $N$ es una clase, $0 \in N$ y $s : N \to N$ satisfacen:

1. No existe $n \in N$ tal que $s(n) = 0$.
2. $s$ es inyectiva, i.e., si $n, m \in N$ son tales que $s(n) = s(m)$, entonces $n = m$.
3. Si $A \subseteq N$ es tal que $0 \in A$ y para todo $n \in A$ se cumple que $s(n) \in A$, entonces $A = N$ (principio de inducción).

De no haber ambigüedad escribiremos que $N$ es un sistema de Peano a secas.

**Proposición 1.36:** Si $N$ es un sistema de Peano, para todo $n \in N$ distinto del 0, existe $m \in N$ tal que $s(m) = n$.

Demostración: Sea $A$ el conjunto formado por todos los elementos que hacen cumplir el enunciado, incluyendo al 0, luego probaremos que $A = n$ mediante el principio de inducción:
Por construcción $0 \in A$. Si $n \in A$, entonces claramente $s(n) \in A$. En conclusión $A = N$, y todo elemento distinto del 0 cumple lo pedido. □

**Teorema 1.37 – *Principio de recursión*:** Si $N$ es un sistema de Peano, $a \in A$ y $g : N \times A \to A$, entonces existe una única función $f : N \to A$ tal que para todo $n \in N$ se cumple:

$$f(0) = a, \quad f(s(n)) = g(n, f(n)).$$

Demostración: Antes de considerar la función $f$ como tal, diremos que una función $h : X \to A$ es una *aproximación* si:

1. $X \subseteq N$, $0 \in X$ y para todo $n \in X_{\neq 0}$ se cumple que existe un $m \in X$ tal que $n = s(m)$.

2. $h$ hace cumplir el enunciado (al menos respecto de los elementos que posee).

Ahora probaremos que las aproximaciones concuerdan en los valores: En concreto construyendo:

$$P := \{n \in N : \forall h : X \to A, h' : Y \to A \text{ aprox.}(n \in X \cap Y \implies h(n) = h'(n))\}$$

probaremos por inducción que $P = N$.
Claramente $0 \in P$, pues todas las aproximaciones toman $a$ en el valor 0. Si $h, h'$ son aproximaciones definidas en $s(n)$, entonces también están definidas en $n$ (pues su dominio incluye los antecesores de todos) y cómo $n \in P$ entonces se concluye que $h(n) = h'(n)$ (por definición de $P$), luego $h(s(n)) = g(n, h(h)) = g(n, h'(n)) = h'(s(n))$, como se quería probar.
Ahora hemos de probar que existen aproximaciones definidas para cualquier elemento de $N$, lo cual también se hace por inducción (ejercicio para el lector).

Finalmente $f$ se define para todo $n \in N$ como el valor que toma cualquier aproximación definida en $n$.

Por último queda la unicidad, que se hace también por inducción y es análogo a cómo se demuestra que las aproximaciones concuerdan en los valores. □

Podemos usar los sistemas de Peano para construir una categoría: Sus objetos son los sistemas de Peano y si $(N, s, 0)$ y $(N', s', 0')$ son sistemas de Peano, diremos que una función $f : N \to N'$ es un morfismo si

$$f(0) = f(0'), \quad \forall n \in \mathbb{N}\ f(s(n)) = s'(f(n)).$$

**Teorema 1.38:** Todo morfismo entre dos sistemas de Peano es de hecho un isomorfismo. Además entre todo par de sistemas de Peano existe un morfismo. En consecuencia, todos los sistemas de Peano son isomorfos.

Hint: Basta construir tal función por recursión. □

La teoría de categorías nos dice pues que en cierta forma los sistemas de Peano son únicos, éste no suele ser el caso con otros sistemas matemáticos (como los grupos), pero es porque en buscabamos unicidad en los números naturales.

**Un sistema de Peano conveniente...** Gracias a la última proposición hemos probado que de algún modo todos los sistemas de Peano "se parecen", luego no importa cómo se construya un sistema en particular, así que hemos de construir uno:

**Definición 1.39:** Sea $\mathbb{N}$ el sistema de Peano tal que $0 := \varnothing$ y $s(n) := n \cup \{n\}$. De este modo:

$$\begin{aligned}
1 &:= s(0) = \{0\} & 5 &:= s(4) = \{0,1,2,3,4\}\\
2 &:= s(1) = \{0,1\} & 6 &:= s(5) = \{0,1,2,3,4,5\}\\
3 &:= s(2) = \{0,1,2\} & 7 &:= s(6) = \{0,1,2,3,4,5,6\}\\
4 &:= s(3) = \{0,1,2,3\} & 8 &:= s(7) = \{0,1,2,3,4,5,6,7\}\\
& & &\vdots
\end{aligned}$$

A los elementos de esta clase les llamamos *números naturales*.

Un problema es que en NBG no sabemos si $\mathbb{N}$ es una clase propia o un conjunto, lo que se traduce que en ZF no sepamos si existe siquiera, para ello hace falta el siguiente axioma:

**Axioma de Infinitud:** Los sistemas de Peano existen y son conjuntos. En particular $\mathbb{N}$ es un conjunto.

Notemos que en NBG el axioma de infinitud implica que todo sistema de Peano es un conjunto, pues ya probamos que existe una función desde uno a otro.

**Aritmética natural.**

**Definición 1.40:** Dado un natural $m$ se define por recursión la función $(m+) : \mathbb{N} \to \mathbb{N}$ tal que

$$(m+)(0) = m, \quad (m+)(s(n)) = s((m+)(n))$$

En la práctica se escribe $(m+)(n) = m + n$.

Por ejemplo

$$2+2 = 2+s(1) = s(2+1) = s(2+s(0)) = s(s(2+0)) = s(s(2)) = s(3) = 4.$$

**Proposición 1.41:** Para todo $n \in \mathbb{N}$ se cumple que $s(n) = n + 1$.

**Teorema 1.42:** Para todo $n, m, p \in \mathbb{N}$ se cumple que $(n + m) + p = n + (m + p)$ (asociatividad).

Demostración: Se realiza por inducción sobre $p$:
Si $p = 0$:

$$(n + m) + 0 = n + m = n + (m + 0).$$

Si se cumple para $p$, entonces

$$\begin{aligned}(n + m) + (p + 1) &= ((n + m) + p) + 1 = (n + (m + p)) + 1 \\ &= n + ((m + p) + 1) = n + (m + (p + 1)).\end{aligned}$$

□

En general todas las demostraciones respecto de propiedades de la adición se hacen por medio de inducción.

**Lema 1.43:** Para todo $n \in \mathbb{N}$ se cumple

$$n + 0 = 0 + n = n, \quad 1 + n = n + 1.$$

**Teorema 1.44:** Para todo $n, m \in \mathbb{N}$ se cumple que $n + m = m + n$ (conmutatividad).

**Definición 1.45:** Dado un natural $m$ se define por recursión la función $(m\cdot) : \mathbb{N} \to \mathbb{N}$ tal que

$$(m\cdot)(0) = 0, \quad (m\cdot)(n+1) = (m\cdot)(n) + m.$$

Al igual que con la suma, escribimos $(m\cdot)(n) = m \cdot n$. En algunos casos incluso obviamos el "$\cdot$" y escribimos $mn = m \cdot n$

**Teorema 1.46:** Para todo $n, m, p \in \mathbb{N}$ se cumple:

1. $n(m+p) = nm + np$ (distributividad por la izquierda).
2. $(n+m)p = np + mp$ (distributividad por la derecha).
3. $n(mp) = (nm)p$ (asociatividad).
4. $n \cdot 0 = 0 \cdot n = 0$ y $n \cdot 1 = 1 \cdot n = n$.
5. $nm = mn$ (conmutatividad).

Hint: Todas las demostraciones son por inducción y/o utilizan propiedades anteriores. □

**Teorema 1.47:** Si $n, m \in \mathbb{N}$ son tales que existe $p \in \mathbb{N}$ tal que $n + p = m + p$, entonces $n = m$ (cancelación).

**Teorema 1.48:** Se cumple:

1. Si $n + m = 0$, entonces $n = m = 0$.
2. Si $nm = 0$, entonces o $n = 0$ o $m = 0$

Demostración:

1. Supongamos que $n \neq 0$, luego posee antecesor $p$ tal que $n = p+1$, luego $n+m = (p+m)+1$, pero como 0 no es el sucesor de nadie, entonces $n + m \neq 0$.
2. Supongamos que $n = n' + 1$ y $m = m' + 1$, entonces

$$nm = (n'+1)m = n'm + m = (n'm + m') + 1 \neq 0.$$

□

**Definición 1.49 – *Relación de orden lineal*:** Se dice que una relación $\leq$ sobre un conjunto $A$ es de *orden lineal* si es reflexiva, antisimétrica, transitiva y conexa.

**Teorema 1.50:** Se dice que un natural $n$ es menor o igual que otro $m$, denotado $n \leq m$, si existe un $p \in \mathbb{N}$ tal que $n + p = m$. $\leq$ es una relación de orden lineal.

Demostración: Con $p = 0$ es claro que $\leq$ es reflexiva, la asociatividad comprueba que $\leq$ es transitiva. Si $n \leq m$ y $m \leq n$, entonces existen $p, q \in \mathbb{N}$ tales que $n + p = m$ y $m + q = n$, luego

$$n + 0 = n = m + q = n + (p + q),$$

luego por cancelación se cumple que $p+q = 0$, con lo que $p = q = 0$ y $n = m$, probando que $\leq$ es antisimétrica.

La conexión de $\leq$ se deduce por inducción. □

**Definición 1.51:** Si $n \leq m$ son naturales, entonces existe $p \in \mathbb{N}$ tal que $n + p = m$ y por cancelación dicho $p$ es único, luego denotamos $p := m - n$. A esta operación la llamamos *resta*.

Sin embargo observe que la resta no está definida sobre todos los naturales.

**§1.5.2 Números enteros.** Aquí introduciremos el concepto de relación de equivalencia para extender los números naturales y algunas de sus propiedades, comenzando por un conjunto que generaliza la resta.

**Definición 1.52 – *Relación de equivalencia*:** Dado un conjunto no vacío $A$, una relación $\sim$ sobre $A$ es de *equivalencia* si es reflexiva, simétrica y transitiva.

Si $\sim$ es una relación de equivalencia sobre $A$ y $a \in A$ entonces se denota

$$[a]_\sim := \{b \in A : a \sim b\}$$

a los conjuntos de dicha forma se dicen *clases de equivalencia*. Se le llama *conjunto cociente*, denotado por $A/\sim$, al conjunto formado por las clases de equivalencia de $A$.

Si $\sim$ es de equivalencia se le llama *proyección*, denotado por $\pi_\sim : A \to A/\sim$, a la función tal que $\pi_\sim(a) = [a]_\sim$. Cabe destacar que

para cualquier relación de equivalencia se cumple que la proyección es suprayectiva.
De no haber ambigüedad sobre los signos se puede obviar el signo $\sim$ en las clases de equivalencia y en la proyección.

**Proposición 1.53:** Si $\sim$ es de equivalencia sobre $A$, entonces para todo $a, b \in A$ se da que: si $a \sim b$ entonces $[a] = [b]$, y de lo contrario $[a] \cap [b] = \varnothing$.

**Proposición 1.54:** Fijada una categoría, la relación dada por "éstos objetos son isomorfos" corresponde a una relación de equivalencia.

**Proposición 1.55:** La relación $\sim$ sobre $\mathbb{N} \times \mathbb{N}$ dada por

$$(a, b) \sim (c, d) \iff a + d = b + c$$

es de equivalencia. Se denota por $\mathbb{Z}$ al conjunto cociente, cuyos elementos llamamos *números enteros*.

Demostración: Claramente es reflexiva y simétrica, por ende queda probar que es transitiva:
Sean $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$, por definición

$$a + d = b + c, \quad c + f = d + e,$$

luego, sumando los mismos lados de la misma ecuación se obtiene

$$a + f + (c + d) = b + e + (c + d)$$

por ende $(a, b) \sim (e, f)$. □

La idea sobre los números enteros es que los pares $(a, b)$ representan la cantidad "$a - b$", pero dado que no es posible definirla universalmente hacemos un reordenamiento de términos, pero el lector debe recordar esta idea internamente para facilitar las definiciones.

**Lema 1.56:** Si $[a, b] = [c, d]$ y $[e, f] \in \mathbb{Z}$, entonces:

1. $[a + e, b + f] = [c + e, d + f]$.
2. $[ae + bf, af + be] = [ce + df, cf + de]$.
3. $a + f \leq b + e$ syss $c + f \leq d + e$.

**Definición 1.57:** En $\mathbb{Z}$ se denota $+n := [n, 0]$, $-n := [0, n]$, y se definen las operaciones

$$[a, b] + [c, d] = [a + c, b + d], \quad [a, b] \cdot [c, d] = [ac + bd, bc + ad].$$

Además también se define la relación $\leq$ que se lee como "menor o igual":

$$[a, b] \leq [c, d] \iff a + d \leq b + c.$$

**Teorema 1.58:** Se cumple:

1. Todo elemento de $\mathbb{Z}$ es de la forma $+n$ o $-n$, y el único que se puede escribir de ambas formas es $+0 = -0 = 0$.
2. La suma en $\mathbb{Z}$ es asociativa y conmutativa.
3. Si $n, m \in \mathbb{N}$, entonces $(+n) + (+m) = +(n + m)$, $(-n) + (-m) = -(n + m)$, $(\pm n) + 0 = 0 + (\pm n) = \pm n$, y $n + (-n) = (-n) + n = 0$.
4. Si $n, m \in \mathbb{N}$ y $n \geq m$, entonces $(+n) + (-m) = +(n - m)$ y si $n \leq m$, entonces $(+n) + (-m) = -(m - n)$
5. Si $x \in \mathbb{Z}$ existe $x' \in \mathbb{Z}$ tal que $x + x' = 0$.
6. Si $x, y, z \in \mathbb{Z}$ cumplen que $x + y = x + z$, entonces $y = z$. En consecuencia el $x'$ anterior es único y podemos denotarlo como $(-x)$. De aquí admitimos que $x - y := x + (-y)$.
7. Si $n \in \mathbb{N}$, entonces $-(+n) = -n$ y $-(-n) = +n$. Más generalmente si $x \in \mathbb{Z}$, entonces $-(-x) = x$.
8. El producto en $\mathbb{Z}$ es conmutativo, asociativo y distributivo respecto a la suma (por ambos lados).
9. Para todo $x \in \mathbb{Z}$ se cumple que $(+1) \cdot x = x$, $0 \cdot x = 0$ y $(-1) \cdot x = -x$.
10. Para todo $x, y \in \mathbb{Z}$ se cumple
$$x(-y) = (-x)y = -(xy), \quad (-x)(-y) = xy.$$
11. $\leq$ es una relación de orden lineal.
12. Para todo $x, y \in \mathbb{Z}$ se cumple que $x \leq y$ syss $0 \leq y - x$.
13. Para todo $x, y, z \in \mathbb{Z}$ se cumple: Si $z > 0$, entonces $x < y$ syss $xz < yz$. Si $z < 0$, entonces $x < y$ syss $xz > yz$.

**§1.5.3 Números racionales.** Al igual que con los enteros comenzamos por una relación de equivalencia que viene a representar la división.

**Proposición 1.59:** La relación $\sim$ sobre $\mathbb{Z} \times \mathbb{Z}_{\neq 0}$ dada por

$$(a, b) \sim (c, d) \iff ad = bc,$$

es de equivalencia. Se denota por $\mathbb{Q}$ al conjunto cociente, cuyos elementos llamamos *números racionales*.

Para mayor facilidad incluso, vamos a denotar las clases de equivalencia como $\frac{a}{b} := [a, b]$.

**Lema 1.60:** Para todo $a, b, c, d, e, f \in \mathbb{Z}$ (con $0 \notin \{b, d, f\}$), tales que $\frac{a}{b} = \frac{c}{d}$ se cumple:

1. $\frac{af+be}{bf} = \frac{cf+de}{df}$.
2. $\frac{ae}{bf} = \frac{ce}{df}$.
3. Existen $n \in \mathbb{Z}$ y $m \in \mathbb{N}$ tales que $\frac{a}{b} = \frac{n}{m}$.
4. Si $b, d, f > 0$, entonces $af \leq be$ syss $cf \leq de$.

**Definición 1.61:** En $\mathbb{Q}$ se denota $n := \frac{n}{1}$ con $n \in \mathbb{Z}$. Y se definen las operaciones:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Y la relación

$$\frac{a}{b} \leq \frac{c}{d} \iff ad \leq bc.$$

**Teorema 1.62:** Se cumple:

1. La suma en $\mathbb{Q}$ es conmutativa y asociativa.
2. Si $x \in \mathbb{Q}$, entonces $x + 0 = x$. Si $a, b \in \mathbb{Z}$, entonces $\frac{a}{b} + \frac{-a}{b} = 0$.
3. El producto en $\mathbb{Q}$ es conmutativo, asociativo y distributivo respecto de la suma (por ambos lados).
4. Si $x \in \mathbb{Q}$, entonces $1 \cdot x = x$, $(-1) \cdot x = -x$, $0 \cdot x = 0$.

5. Si $a, b \in \mathbb{Z}$ y $a \neq 0$, entonces $\frac{a}{b} \cdot \frac{b}{a} = 1$. Se denota $\left(\frac{a}{b}\right)^{-1} := \frac{b}{a}$.
6. Si $x, y, z \in \mathbb{Q}$ con $z \neq 0$, entonces $xz = yz$ syss $x = y$.
7. $\leq$ es una relación de orden lineal.
8. $\frac{a}{b} \geq 0$ syss $a$ y $b$ tienen el mismo signo, o $a$ es nulo.
9. Para todo $x, y \in \mathbb{Q}$ se cumple que $x \leq y$ syss $0 \leq y - x$.

Varias de las propiedades de $\mathbb{Q}$ y $\mathbb{Z}$ pueden simplificarse mediante la llamada teoría de grupos, anillos y cuerpos que se puede encontrar en cualquier libro de álgebra. Luego de los números racionales viene la inclusión de los irracionales en el conjunto de números reales, sin embargo, su construcción es todo un tema distinto y preferí incluirlo como el primer capítulo de mi libro de análisis y topología.

# 2

# *Orden y números ordinales*

## 2.1. Orden parcial, lineal y buen orden

**Definición 2.1:** Se dice que una relación $\leq$ es de:

**Preorden** Si es reflexiva y transitiva.

**Orden** Si es de preorden y es antisimétrica.

**Orden total o lineal** Si es de orden y es conexa.

Un par $(A, \leq)$ donde $\leq$ es una relación de orden sobre $A$, se dice un *conjunto parcialmente ordenado*. Si $\leq$ es de orden total se dice que $(A, \leq)$ es un *conjunto linealmente ordenado*. Si $\leq$ es de preorden, denotamos $<$ a la relación dada por $x < y$ syss $x \leq y$ y $x \neq y$.

**Proposición 2.2:** Se cumple:

1. Si $A$ es un conjunto arbitrario entonces $(\mathcal{P}(A), \subseteq)$ es un conjunto parcialmente ordenado.

2. Si $(A, \leq)$ es parcialmente (resp. linealmente) ordenado y $B \subseteq A$, entonces $(B, \leq|_B)$ es parcialmente (resp. linealmente) ordenado.

**Definición 2.3:** Si $(A, \leq)$ es parcialmente ordenado y $B \subseteq A$, entonces se dice que $a \in A$ es:

**Minimal (resp. maximal) de $B$** Si $a \in B$ y para todo $b \in B$ se cumple que $b \not\leq a$ (resp. $b \not\geq a$).

**Cota inferior (resp. superior) de $B$** Si para todo $b \in B$ se cumple que $b \geq a$ ($b \leq a$).

**Mínimo (resp. máximo) de $B$** Si es cota inferior (resp. superior) de $B$ y $a \in B$.

**Ínfimo (resp. supremo) de $B$** Si es la máxima (resp. mínima) cota inferior (resp. superior) de $B$.

$B$ se dice *inferiormente (resp. superiormente) acotado* si posee una cota inferior (resp. superior). $B$ se dice *acotado* (a secas) si es inferior y superiormente acotado.

**Proposición 2.4:** Dado un subconjunto $B$ de un conjunto parcialmente ordenado $A$ se cumple:

1. Si $B$ posee mínimo, máximo, ínfimo o supremo; éste es único.
2. Si $B$ posee mínimo (resp. máximo), entonces es su único minimal (resp. maximal).
3. El ínfimo (resp. supremo) de $B$ es el mínimo (resp. máximo) syss pertenece a $B$.
4. Una cota inferior (resp. superior) de $B$ contenida en $B$ es el ínfimo (resp. supremo), y por consecuente es el mínimo (resp. máximo).
5. Si $A$ es linealmente acotado, entonces un elemento es minimal (resp. maximal) de $B$ syss es su mínimo (resp. máximo).

**Definición 2.5:** Un conjunto parcialmente ordenado se dice:

**Completo** Si todo conjunto inferiormente acotado tiene ínfimo.

**Bien fundado** Si todo conjunto posee minimal.

**Bien ordenado** Si todo conjunto posee mínimo.

En el último caso también se dice que $\leq$ es un buen orden.

**Proposición 2.6:** Si $A$ es parcialmente ordenado, entonces:

1. Todo subconjunto de un conjunto bien fundado (resp. bien ordenado) está bien fundado (resp. bien ordenado).

2. Todo subconjunto inferiormente acotado de $A$ tiene ínfimo syss todo subconjunto superiormente acotado de $A$ tiene supremo.

3. Si $A$ es bien fundado, entonces es bien ordenado syss es linealmente ordenado.

4. Si $A$ es bien ordenado entonces es completo.

Demostración: Sólo probaremos la segunda, de la cual haremos una implicancia pues la otra es análoga: $\Longrightarrow$ . Sea $B$ no vacío y acotado superiormente, entonces llamamos a $S$ el conjunto de cotas superiores de $B$. Evidentemente todo elemento de $b$ es una cota inferior de $S$, luego como $A$ es completo, se cumple que $S$ posee ínfimo $m$. Y como $m$ es máximo de las cotas inferiores de $S$ y todo elemento de $B$ es cota inferior de $S$, entonces $m$ es cota superior de $B$, luego $m \in S$, pero como es cota inferior de $S$ se cumple que $m$ es mínimo de $S$, i.e., $m$ es supremo de $B$. □

**Definición 2.7:** Si $(A, \leq), (B, \preceq)$ son parcialmente ordenados, entonces los morfismos $f : A \to B$ son las aplicaciones que preservan el orden, es decir tales que para todo $x, y \in A$ se cumple que

$$x \leq y \implies f(x) \preceq f(y).$$

También se dice que $f$ es *creciente*. $f$ es *estrictamente creciente* si $x < y$ implica $f(x) \prec f(y)$. Una biyección $f$ tal que $f$ y $f^{-1}$ son crecientes se dice un *isomorfismo*.

**Proposición 2.8:** Toda biyección creciente entre conjuntos linealmente ordenados es un isomorfismo.

**Lema 2.9:** Si $A$ está bien ordenado, entonces toda función estrictamente creciente $f : A \to A$ cumple que $x \leq f(x)$.

Demostración: Supongamos que fuese falso, entonces sea $F$ el conjunto de los elementos de $A$ para los que no se cumple el enunciado. Como $A$ está bien ordenado sea $m := \min F$, luego, por definición, $f(m) < m$, pero entonces $f(f(m)) < f(m)$, luego $f(m) \in F$ lo que contradice la minimalidad de $m$. □

**Corolario 2.10:** El único automorfismo de un conjunto bien ordenado es la identidad.

**Corolario 2.11:** Si dos conjuntos bien ordenados son isomorfos, entonces el isomorfismo es único.

**Definición 2.12:** Un subconjunto $S$ de un conjunto parcialmente ordenado $A$ se dice un *segmento inicial* si para todo $a \in A$ tal que existe $s \in S$ tal que $a \leq s$ se cumple que $a \in S$. Se dice que un segmento inicial es propio si es distinto $A$.

Si $x \in A$ se define:

$$O_{\leq}(x) := \{a \in A : a \leq x\}, \quad O_{\geq}(x) := \{a \in A : a \geq x\},$$
$$O_{<}(x) := \{a \in A : a < x\}, \quad O_{>}(x) := \{a \in A : a > x\}.$$

Si no hay ambigüedad sobre los signos abreviaremos $O_{<}(x)$ como $O(x)$.

**Proposición 2.13:** Se cumple:

1. Para todo $x \in A$ se cumple que $O_{<}(x)$ y $O_{\leq}(x)$ son segmentos iniciales.

2. Si $A$ es linealmente ordenado y completo, entonces todo segmento inicial propio es de la forma $O_{<}(x)$ o $O_{\leq}(x)$.

3. Si $A$ es bien ordenado, entonces todo segmento inicial propio es de la forma $O_{<}(x)$.

Hint: Si $S$ es un segmento inicial considere $x := \sup S$ en la segunda. Si $O_{\leq}(x)$ es un segmento inicial considere $y := \min(O_{>}(x))$ en la tercera. □

**Lema 2.14:** Un conjunto bien ordenado no es isomorfo a ningún segmento inicial propio.

Demostración: Si $f$ fuera estrictamente creciente y existiera $u \in A$ tal que $\operatorname{Img} f = O_<(u)$, entonces $f(u) < u$ □

**Teorema 2.15:** Si $(A, \leq), (B, \preceq)$ son conjuntos bien ordenados, entonces solo una de las siguientes condiciones se cumple:

1. $A$ y $B$ son isomorfos.
2. $A$ es isomorfo a un segmento inicial de $B$.
3. $B$ es isomorfo a un segmento inicial de $A$.

Demostración: En esta demostración denotaremos que "$x$ es isomorfo en orden a $y$" como $x \cong y$:

$$f := \{(x, y) \in A \times B : O_<(x) \cong O_\prec(y)\},$$

bajo esta definición es claro que $f$ es función creciente e inyectiva.

$\operatorname{Img} f$ **es un segmento inicial de** $B$**.** Si $y_1 \prec y_2$ e $y_2 \in \operatorname{Img} f$ entonces existe $x_2 \in A$ tal que $O(x_2) \cong O(y_2)$ sea $g : A_{x_2} \to A_{y_2}$ el isomorfismo de orden, entonces sea $x_1 := g^{-1}(y_1)$ luego es fácil notar que $g[O(x_1)] = O(y_1)$ y que su restricción es un isomorfismo, luego $y_1 \in \operatorname{Img} f$. Análogamente se razona que $\operatorname{Dom} f$ es segmento inicial de $A$.

$\operatorname{Dom} f = A$ **o** $\operatorname{Img} f = B$**.** Sin perdida de generalidad supongamos que $\operatorname{Img} f \neq B$, entonces sea $y_0 := \min(B \setminus \operatorname{Img} f)$, luego $\operatorname{Img} f = O(y_0)$. Supongamos por contradicción que $\operatorname{Dom} f \neq A$, entonces sea $x_0 := \min(A \setminus \operatorname{Dom} f)$, luego $\operatorname{Dom} f = O(x_0)$, pero entonces $(x_0, y_0) \in f$ lo que contradice que $x_0 \notin \operatorname{Dom} f$.

El lema rellena detalles incluido el que los tres casos son mutuamente exclusivos. □

## 2.2. Números ordinales

El último teorema es una parte fundamental de la teoría de los conjuntos bien ordenados, dice que tienen una estructura bastante sencilla, luego nos gustaría poder tener una especie de representante, ese es el rol que van a jugar los ordinales. Más adelante veremos que los ordinales tienen además una forma de aritmética entre ellos que les otorga la cualidad de "ser números", además los ordinales darán luz a dos de los últimos axiomas que comprenden nuestra teoría elemental[1].

[1]Por supuesto hay muchos otros axiomas, pero no se consideran al mismo nivel de relevancia que el axioma de fundación y AE.

**Definición 2.16:** Se dice que una clase $\alpha$ es un *ordinal* si:

1. Para todo $u \in v$ y $v \in \alpha$ se cumple que $u \in \alpha$ (transitividad).
2. Todo subconjunto $x \subseteq \alpha$ tiene un $\in$-minimal, i.e., existe un $z \in x$ tal que para todo $y \in x$ se cumple que $y \notin u$, osea, un $z \in x$ tal que $z \cap x = \varnothing$ (bien fundado).
3. Para todo $u, v \in \alpha$ se cumple que $u \in v$, $u = v$ o $v \in u$ ($\in$-conexo).

Las últimas dos condiciones pueden reemplazarse diciendo que $\alpha$ está bien ordenado por $\in$.

Denotamos por $\Omega_{\text{Ord}}$ a la clase que contiene a todos los conjuntos que sean ordinales.

**Teorema 2.17:** Si $x$ es $\in$-bien fundado entonces $x \notin x$.

Demostración: Si $x \in x$ entonces $\{x\} \subseteq x$, luego posee $\in$-minimal que sólo puede ser $x$, sin embargo $x \cap \{x\} = x \neq \varnothing$. □

**Teorema 2.18:** Todo elemento de un ordinal es también un ordinal.

Demostración: Si $\alpha$ es un ordinal y $\beta \in \alpha$, entonces por transitividad, $\beta \subseteq \alpha$ luego es inmediato que $\beta$ es $\in$-bien ordenado, basta probar que es transitivo.

Sea $u \in v$ y $v \in \beta$, por transitividad, $v \in \alpha$ y $u \in \alpha$. Luego como $\alpha$ está $\in$-bien ordenado el conjunto $\{u, v, \beta\}$ tiene un $\in$-mínimo, luego ha de ser $u$ (¿por qué?), pero entonces $u \in \beta$ como se quería probar. □

**Proposición 2.19:** Se cumple:

1. $\varnothing$ es un ordinal.
2. Si $\alpha \in \Omega_{\text{Ord}}$, entonces $\alpha^+ := \alpha \cup \{\alpha\} \in \Omega_{\text{Ord}}$.

Demostración: Es claro que $\varnothing$ es un ordinal.

Es fácil ver que $\alpha^+$ es transitivo. Ahora basta ver que todo subconjunto $x$ no vacío de $\alpha^+$ no vacío posee $\in$-minimal: si $x = \{\alpha\}$, entonces es claro, de lo contrario $x \setminus \{\alpha\}$ es no vacío, luego es subconjunto de $\alpha$ por lo que tiene un $\in$-minimal $u$, basta ver que $u \cap \{\alpha\} = \varnothing$. De lo contrario $\alpha \in u \in \alpha$,

luego $\alpha \in \alpha$ lo que contradice que $\alpha$ está $\in$-bien fundado.
También es claro que $\alpha^+$ es $\in$-conexo. □

**Lema 2.20:** Si $\alpha, \beta$ son ordinales y $\alpha \subset \beta$ entonces $\alpha \in \beta$.

Demostración: Como $\beta \setminus \alpha \subset \beta$ entonces posee un $\in$-mínimo $\gamma$. Se cumple que $\gamma \subseteq \alpha$ pues de lo contrario $\delta \in \gamma \setminus \alpha$ estaría en $\beta \setminus \alpha$ y sería menor que $\gamma$. Probaremos que $\alpha \subseteq \gamma$: Si $\delta \in \alpha$, entonces como $\delta, \gamma \in \beta$ y $\beta$ es $\in$-conexo se cumple que $\delta \in \gamma$, $\delta = \gamma$ o $\gamma \in \delta$; pero las últimas dos son falsas pues por transitividad $\gamma \in \alpha$ con lo que $\gamma \notin \beta \setminus \alpha$, lo que es absurdo. □

**Lema 2.21:** Si $\alpha, \beta$ son ordinales entonces $\alpha \cap \beta$ es un ordinal.

Demostración: Sea $\gamma := \alpha \cap \beta$, como $\gamma \subseteq \alpha$ entonces $\gamma$ es $\in$-bien ordenado. Aún basta probar que $\gamma$ es transitivo: Si $u \in \gamma$ entonces $u \in \alpha, \beta$, y de hecho, $u \subseteq \alpha, \beta$, ergo $u \subseteq \gamma$. □

**Teorema 2.22:** Si $\alpha, \beta \in \Omega_{\text{Ord}}$ entonces $\alpha \in \beta, \alpha = \beta$ o $\beta \in \alpha$. En consecuente, $\alpha \subseteq \beta$ o $\beta \subseteq \alpha$

Demostración: Sea $\gamma := \alpha \cap \beta \in \Omega_{\text{Ord}}$, si $\alpha \neq \gamma \neq \beta$, entonces $\gamma \in \alpha$ y $\gamma \in \beta$, ergo, $\gamma \in \alpha \cap \beta$, pero eso no es posible pues es $\in$-bien fundado. □

**Teorema 2.23 – *Antinomia de Burtali-Forti*:** $\Omega_{\text{Ord}}$ es un ordinal, por ende, es una clase propia.

Demostración: Ya hemos probado que $\Omega_{\text{Ord}}$ es transitivo y $\in$-conexo, aún falta ver que es bien fundado: Sea $X \subseteq \Omega_{\text{Ord}}$ una clase no vacía y sea $\alpha \in X$ cualquiera. Si $\alpha$ es un $\in$-minimal, entonces no hay nada que probar; de lo contrario, $\varnothing \neq \alpha \cap X \subseteq \alpha$ luego existe un $\in$-minimal $\beta$ en $\alpha \cap X$. Y $\varnothing = \beta \cap \alpha \cap X = \beta \cap X$ pues $\beta \subseteq \alpha$. □

La conclusión en ZF es que $\Omega_{\text{Ord}}$ no existe.

**Corolario 2.24:** Se cumple:

1. $\Omega_{\text{Ord}}$ está $\subseteq$-bien ordenado, por lo cual vamos a denotar $\leq \equiv \subseteq$
2. $0 := \varnothing$ es el mínimo ordinal.
3. $\alpha^+$ es el mínimo ordinal estrictamente mayor que $\alpha$.

4. Para todo $\alpha \in \Omega_{\text{Ord}}$, se cumple que $\alpha = O_<(\alpha)$.
5. Si $A$ es una clase de ordinales, entonces $\min A = \bigcap A$ y $\sup A = \bigcup A$.

**Definición 2.25:** Se dice que un ordinal $\alpha$ es:

**Sucesor** Si $\alpha = 0$ o existe $\beta \in \Omega_{\text{Ord}}$ tal que $\alpha = \beta^+$. De lo contrario se dice que es un ordinal *límite*.

**Finito** Si para todo $\beta \leq \alpha$ se cumple que $\beta$ es sucesor. Se dice que es infinito de lo contrario.

Se denota $\omega$ a la clase de ordinales finitos.

**Teorema 2.26:** Todo conjunto bien ordenado es isomorfo a un único ordinal.

Demostración: (**Nota:** Intente demostrarlo por sí solo.)

Sea $A$ un conjunto bien ordenado y $\Omega_{\text{Ord}}$ que sabemos que está bien ordenado también. Luego alguno es isomorfo a un segmento inicial del otro, pero $A \ncong \Omega_{\text{Ord}}$ pues existiría una función $f : A \to \Omega_{\text{Ord}}$ que es suprayectiva, pero entonces por axioma de reemplazo $\Omega_{\text{Ord}}$ sería un conjunto; un razonamiento análogo se aplica si $\Omega_{\text{Ord}}$ fuera isomorfo a un segmento inicial de $A$. Sólo nos queda que $A$ es isomorfo a un segmento inicial de $\Omega_{\text{Ord}}$ que son los ordinales. □

**Definición 2.27:** Si $(A, \leq)$ es un conjunto bien ordenado, denotamos por $\text{ord}(A, \leq)$ al único ordinal al que le es isomorfo.

**Teorema 2.28 – *Inducción transfinita*:** Sea $C$ una clase de ordinales, tal que:

- $0 \in C$.
- Si $\alpha \in C$, entonces $\alpha^+ \in C$.
- Si para todo $\delta < \lambda$ se cumple que $\delta \in C$, entonces $\lambda \in C$.

Entonces $C = \Omega_{\text{Ord}}$.

Hint: Aplicar el buen orden de los ordinales. □

**Teorema 2.29 – *Recursión transfinita*:** Sea $A$ una clase arbitraria con

$$\mathcal{F} := \bigcup_{\alpha \in \Omega_{\text{Ord}}} \text{Func}(\alpha; A),$$

y sea $G : \mathcal{F} \to A$, entonces existe una única función $F : \Omega_{\text{Ord}} \to A$ tal que para todo $\alpha \in \Omega_{\text{Ord}}$ se cumple

$$F(\alpha) := G(F|_\alpha).$$

Demostración: Vamos a decir que una función es una $\alpha$-aproximación si cumple con la última ecuación pero tiene dominio $\alpha$. Por el buen ordenamiento de los ordinales se puede probar con facilidad que, si existen, las $\alpha$-aproximaciones y la función deseada misma son únicas.

Luego sigue probar la existencia de $\alpha$-aproximaciones arbitrarias encajadas, lo cual se puede hacer por inducción transfinita y, finalmente, si se denota por $f_\alpha$ a la única $\alpha$-aproximación, entonces se define $F(\alpha) := G(f_\alpha)$. □

**Definición 2.30:** Una función $f : \alpha \to X$ cuyo dominio es un ordinal se dice una *sucesión* de largo $\alpha$. Si $f$ es una sucesión creciente y $\lambda \in \text{Dom}\, f$ es un ordinal límite, entonces se denota

$$\lim_{\delta \to \lambda} f(\delta) := \sup_{\delta < \lambda} f(\delta),$$

Se dice que una sucesión creciente es *continua* si para todo $\lambda$ límite se cumple que $f(\lambda) = \lim_{\delta \to \lambda} f(\delta)$.

Una sucesión continua de codominio $\Omega_{\text{Ord}}$ que es estrictamente creciente se dice una *función normal*.

**Teorema 2.31:** Para todo $g : \Omega_{\text{Ord}} \times \Omega_{\text{Ord}} \to \Omega_{\text{Ord}}$ y $\beta \in \Omega_{\text{Ord}}$, existe una única sucesión continua $f : \Omega_{\text{Ord}} \to \Omega_{\text{Ord}}$ tal que

$$f(0) = \beta, \quad f(\alpha^+) = g(\alpha, f(\alpha)).$$

## 2.3. Aritmética ordinal

**Definición 2.32:** Dado un ordinal $\alpha$ se definen las operaciones como

las únicas sucesiones continuas tal que

$$\begin{aligned} \alpha + 0 &:= \alpha, & \alpha + (\beta^+) &:= (\alpha + \beta)^+, \\ \alpha \cdot 0 &:= 0, & \alpha \cdot (\beta^+) &:= \alpha \cdot \beta + \alpha, \\ \alpha^0 &:= 1, & \alpha^{\beta^+} &:= \alpha^\beta \cdot \alpha. \end{aligned}$$

**Proposición 2.33:** Para todo $\alpha, \beta, \gamma \in \Omega_{\text{Ord}}$ se cumple:

1. $\alpha^+ = \alpha + 1$.
2. $0 + \alpha = \alpha + 0 = \alpha$.
3. $\alpha < \beta$ syss $\gamma + \alpha < \gamma + \beta$, equivalentemente, la suma con $\gamma$ fijo es una función normal.
4. $\gamma + \alpha = \gamma + \beta$ syss $\alpha = \beta$.
5. Si $\alpha \leq \beta$, entonces $\alpha + \gamma \leq \beta + \gamma$.

Hint: La mayoría se demuestran por inducción transfinita. □

**Proposición 2.34:** Para todo $\alpha, \beta, \gamma \in \Omega_{\text{Ord}}$ se cumple:

1. $0 \cdot \alpha = \alpha \cdot 0 = 0$ y $1 \cdot \alpha = \alpha \cdot 1 = \alpha$.
2. $\alpha < \beta$ y $\gamma > 0$ syss $\gamma \cdot \alpha < \gamma \cdot \beta$, equivalentemente, el producto con $\gamma > 0$ fijo es una función normal.
3. Si $\gamma > 0$, entonces $\gamma \cdot \alpha = \gamma \cdot \beta$ syss $\alpha = \beta$.
4. Si $\alpha \leq \beta$, entonces $\alpha \cdot \gamma \leq \beta \cdot \gamma$.

**Teorema 2.35:** La suma y el producto ordinal son asociativos, i.e., para todo $\alpha, \beta, \gamma \in \Omega_{\text{Ord}}$ se cumple:

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma, \qquad \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma.$$

Sin embargo, las reglas sobre los números naturales no se extienden a los números ordinales, por ejemplo

$$1 + \omega := \lim_{n \to \omega} 1 + n = \omega < \omega + 1$$

Además

$$2 \cdot \omega := \lim_{n \to \omega} 2n = \omega < \omega \cdot 2.$$

## 2.4. Relaciones bien fundadas

Si $R$ es una relación, entonces se denota $R^2 := R \circ R$ y por recursión, $R^{n+1} := R^n \circ R$.

**Proposición 2.36:** Si $R$ es una relación sobre $A$, entonces:

1. $R \cup \mathrm{Id}_A$ es reflexiva sobre $A$.
2. $R^* := \bigcup_{n=1}^{\infty} R^n$ es transitiva sobre $A$.
3. $R^*$ es la mínima (por inclusión) relación transitiva sobre $A$ que contiene a $R$.
4. $\bar{R} := R^* \cup \mathrm{Id}_A$ es un preorden sobre $A$.
5. $\bar{R}$ es el mínimo (por inclusión) preorden sobre $A$ que contiene a $R$.

**Definición 2.37:** Si $R$ es una relación sobre $A$, se dice que una subclase $B$ de $A$ es *$R$-cerrada* si para todo $x, y \in A$ tales que $xRy$ e $y \in B$ se da que $x \in B$.
También se le llama *$R$-clausura* de $B$, denotado $\mathrm{ct}_R(B)$, a la clase

$$\mathrm{ct}_R(B) := B \cup \bigcup_{b \in B} O_{R^*}(b).$$

**Proposición 2.38:** Si $R$ es una relación sobre $A$ y $B \subseteq A$, entonces:

1. $B$ es $R$-cerrado syss $B = \mathrm{ct}_R(B)$.
2. $\mathrm{ct}_R(B)$ es el mínimo $R$-cerrado (bajo inclusión) que contiene a $B$.
3. $B$ es $R^*$-cerrado syss $R$-cerrado.
4. $A$ y $\varnothing$ son $R$-cerrados.

**Definición 2.39:** Se dice que una relación $\prec$ sobre una clase $A$ es *reducida* si para todo $x \in A$ se cumple que $O_{\prec}(x)$ es un conjunto.
Si $\preceq$ es parcialmente ordenada, bien fundada y reducida sobre $A$, entonces para todo $x \in A$ se define por recursión transfinita

$$\mathrm{rang}_{\preceq} x := \sup\{\mathrm{rang}_{\preceq} y + 1 : y \prec x\},$$

donde se asume que $\operatorname{rang}_{\preceq} x = 0$ si $x$ es minimal.

**Axioma de Fundación:** Todas las clases son $\in$-bien fundadas.

**Corolario 2.40:** Se cumple:

1. No hay $\in$-ciclos, i.e., una sucesión finita $(x_1, \ldots, x_n)$ tal que $x_1 \in x_2 \in \cdots \in x_n \in x_1$.
2. No hay $\in$-sucesiones decrecientes, i.e., tales que $x_1 \ni x_2 \ni x_3 \ni \cdots$.

Demostración: Supongamos que sí la hubiera, luego $y := \{x_1, \ldots, x_n\}$ es $\in$-bien fundado por lo que posee $\in$-minimal. Sin embargo, $x_1$ no lo es pues $x_n \in x_1 \cap y$, y para otro $i$ tampoco pues $x_{i-1} \in x_i \cap y$.
Del mismo modo se prueba el inciso restante. □

**§2.4.1 La jerarquía de von Neumann.** Dado que vimos que todo conjunto es bien fundado, todo conjunto ha de tener rango (bajo $\in$), luego hay una forma de construir conjuntos en base a dicha noción:

**Definición 2.41 – *Universo de von Neumann*:** Se define por inducción transfinita las clases

$$V_0 := \varnothing, \quad V_{\alpha+1} := \mathcal{P}(V_\alpha), \quad V_\lambda := \bigcup_{\delta<\lambda} V_\delta.$$

**Teorema 2.42:** Se cumple:

1. Las clases de la forma $V_\alpha$ son conjuntos.
2. Para todo ordinal $\alpha$ se cumple que $V_\alpha = \{x : \operatorname{rang} x < \alpha\}$.
3. Si $\alpha \leq \beta$ son ordinales, entonces $V_\alpha \subseteq V_\beta$.
4. $\operatorname{rang} V_\alpha = \alpha$.
5. Los conjuntos de la forma $V_\alpha$ son transitivos.

Demostración: 1. Se demuestra por inducción fuerte. En caso de que sea un ordinal sucesor, entonces basta aplicar el axioma por partes. En caso de que sea un ordinal límite, se utiliza el hecho de que tal ordinal es conjunto y luego una función biyectiva para probar que $\{V_\alpha : \alpha < \lambda\}$ es un conjunto, luego su unión lo es también.

2. Lo probaremos por inducción transfinita: El caso base $\alpha = 0$, y el caso en que $\alpha$ es límite son triviales.
   Si $x \subseteq V_\alpha$, entonces

$$\operatorname{rang} x = \sup\{\operatorname{rang} y + 1 : y \in x\} \leq \alpha < \alpha + 1.$$

   Así mismo, si $\operatorname{rang} x < \alpha + 1$, entonces para todo $y \in x$ se cumple que $\operatorname{rang} y + 1 \leq \operatorname{rang} x < \alpha + 1$, luego $\operatorname{rang} y < \alpha$ y $x \subseteq V_\alpha$, i.e., $x \in V_{\alpha+1}$.

3. Es corolario del inciso anterior.

4. Es trivial.

5. Queda de ejercicio al lector.

□

**Corolario 2.43:** Una clase es propia syss contiene elementos de rango arbitrariamente grande.

Demostración: Si una clase $A$ contiene a elementos de rango, digamos menor que $\beta$, entonces $A \in V_{\beta+1}$. □

**Teorema 2.44:** Son equivalentes:

1. **El axioma de fundación:** Todos los conjuntos son $\in$-bien fundados.

2. $V = \bigcup_{\alpha \in \Omega_{\mathrm{Ord}}} V_\alpha$.

# 3

# *Cardinalidad*

## 3.1. Definiciones elementales y cardinalidad finita

La cardinalidad es la idea de "tener la misma cantidad", luego una técnica sería contar la cantidad en ambos conjuntos y compararlos, pero inmediatamente se vuelve obsoleta al introducir conjuntos infinitos que deriva naturalmente del axioma de infinitud ya introducido en el primer capítulo. Así que Cantor propuso una idea que puede ser explicada mediante la siguiente analogía: Si queremos saber si en un autobús hay tantos asientos como pasajeros basta pedirles a todos los pasajeros que se sienten y ver que no hayan puestos vacíos (admitiendo que no existe la posibilidad de que dos o más personas ocupen un mismo asiento, o de que gente vaya parada dado que hay asientos vacíos). Esta idea de asignar un único asiento a un único pasajero viene a ser sustituida por una función biyectiva entre dos conjuntos.

Otra explicación es que se desea establecer una especie de equivalencia en el lenguaje de la categoría de conjuntos, eso nos otorga la definición de equipotencia de manera natural, pues sólo exige que existan $f, g$ tales que su composición sea la identidad, luego se concluye que las funciones son biyecciones y que una es la inversa de la otra.

**Definición 3.1 – *Equipotencia*:** Se dice que dos clases $A, B$ son *equipotentes*, denotado $A \approx B$, si existe una función biyectiva de dominio $A$ y rango $B$. También denotamos que $A \lesssim B$ si existe $f : A \to B$

inyectiva, y que $A \lesssim B$ si $A \lesssim B$ pero $A \not\approx B$.

Nótese que la equipotencia es de hecho la cualidad de ser isomorfos en la categoría de los conjuntos.

**Proposición 3.2:** Para todas clases $A, B, C, D$ se cumple:

1. $A \approx A$.
2. $A \approx B$ syss $B \approx A$.
3. $A \approx B$ y $B \approx C$ implican $A \approx C$. En consecuencia, la equipotencia es una relación de equivalencia entre clases.
4. $A \approx B$ implica $A \lesssim B$. En particular $A \lesssim A$.
5. $A \lesssim B$ y $B \lesssim C$ implican $A \lesssim C$.
6. Si $A \approx B$, $C \approx D$ y $A \lesssim C$, entonces $B \lesssim D$.

**Teorema 3.3 – *Teorema de Cantor*:** Para todo conjunto $A$, se cumple que $A \lesssim \mathcal{P}(A)$.

Demostración: La inyección es clara: para todo $a \in A$ se cumple que $f(a) := \{a\} \in \mathcal{P}(A)$.

Veamos que no existe una función suprayectiva desde $A$ a $\mathcal{P}(A)$: Sea $f : A \to \mathcal{P}(A)$, definamos $B := \{a \in A : a \notin f(a)\}$, si existiese $b \in A$ tal que $f(b) = B$, entonces nos preguntamos: ¿$b \in f(b)$? Si la respuesta es afirmativa, entonces por construcción $b \notin B$. Si la respuesta es negativa, entonces $b \notin f(b)$, luego $b \in B$. Luego concluimos que no puede existir una preimagen de $B$, ergo, no hay función suprayectiva de $A$ a $\mathcal{P}(A)$; luego en particular no hay tal biyección. □

**Lema 3.4:** Si $I_n := \{1, 2, \ldots, n\}$, entonces no existe un subconjunto propio equipotente a $I_n$.

Demostración: Lo haremos por inducción sobre $n$. El caso $n = 0$ es trivial, ya que $\varnothing$ no posee subconjuntos propios. Supongamos que se cumple para $n$, probaremos que lo hace para $n + 1$: Por contradicción sea $X \subset I_{n+1}$ tal que $X \approx I_{n+1}$ y sea $f : I_{n+1} \to X$ biyectiva. Si $n + 1 \notin X$, entonces $X_{\neq f(n+1)}$ es subconjunto propio equipotente a $I_n$. Si $n + 1 \in X$, entonces

sea $k := f^{-1}(n+1)$, si $k = n+1$ entonces el argumento anterior aplica, sino definimos $g : I_n \to I_n$ como

$$g(i) := \begin{cases} f(i), & i \neq k \\ f(n+1), & i = k \end{cases}$$

que resulta inyectiva y no suprayectiva, lo que es absurdo. □

**Corolario 3.5:** Si $A \approx I_n$ y $A \approx I_m$, entonces $n = m$.

**Definición 3.6:** Se dice que una clase $A$ es *finita* si existe $n \in \mathbb{N}$ tal que $A \approx I_n$, en dicho caso denotamos $|A| = n$.

El axioma de reemplazo nos dice que toda clase finita es un conjunto.

**Teorema 3.7:** Se cumple:

1. Si $A \lesssim B$ y $B$ es finito, entonces $A$ también y $|A| \leq |B|$.
2. Si $A \lesssim B$ y $A$ es infinito, entonces $B$ también.

**Proposición 3.8 (Principio del palomar):** Si $|A| < |B|$ y son ambos finitos, entonces toda función $f : B \to A$ no es inyectiva, es decir, siempre existe un $a \in A$ con más de una preimagen.

**§3.1.1 Aritmética cardinal finita.** Un análisis de la cardinalidad finita respecto a las clásicas operaciones conjuntistas genera una buena intuición para lo que en el siguiente capítulo consideraremos como principios básicos para un modelo de *números cardinales*. No otorgaremos las demostraciones a estos teoremas pues quedan al lector y todas derivan de una aplicación de inducción natural.

**Teorema 3.9 – *Principio de inclusión-exclusión*:** Si $A, B$ son finitos, entonces su unión e intersección también y de hecho

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

**Teorema 3.10:** Si $A, B$ son finitos, entonces su producto también y

$$|A \times B| = |A| \cdot |B|.$$

**Proposición 3.11:** Si $A, B$ son finitos, entonces $\operatorname{Func}(A, B)$ también y

$$|\operatorname{Func}(A, B)| = |B|^{|A|}.$$

**Definición 3.12:** Si $A$ es una clase cualquiera, denotaremos $[A]^n$ a la clase de las subclases de $A$ de cardinal $n$, formalmente:

$$[A]^n := \{B \in \mathcal{P}(A) : |B| = n\}.$$

**Proposición 3.13:** Si $A$ es finito de cardinal $n$ y $m \leq n$, entonces

$$\left|[A]^m\right| = \binom{m}{n}.$$

**Teorema 3.14:** Si $A$ es finito de cardinal $n$, entonces $\mathcal{P}(A)$ también y

$$|\mathcal{P}(A)| = 2^n.$$

**Proposición 3.15:** Si $A$ es finito de cardinal $n$, entonces

$$|\operatorname{Sym}(A)| = n!$$

**§3.1.2 El teorema de Schröder-Cantor-Bernstein.** Éste teorema nos permite caracterizar mejor la equipotencia, hay una demostración bastante sencilla de él si se asume que lo más adelante indicaremos como el axioma de elección, pero el caso que prescinde de él es más complicado.

**Teorema 3.16 (punto fijo de Knaster-Tarski):** Si $(P, \leq)$ es un conjunto parcialmente ordenado completo acotado y $f : P \to P$ creciente, entonces $f$ posee un punto fijo.

Demostración: Como $P$ es acotado posee un máximo $M$, entonces $f(M) \leq M$, luego $A := \{x \in P : f(x) \leq x\}$ es no vacío y acotado inferiormente, por lo que, por completitud de $P$ posee ínfimo $p$.

Para todo $x \in A$ se cumple que $p \leq x$, luego $f(p) \leq f(x) \leq x$, por ende $f(p)$ es cota inferior de $A$, ergo $f(p) \leq p$. Pero por la monotonía se cumple que $f(f(p)) \leq f(p)$, luego $f(p) \in A$ y como $p$ es cota inferior de $A$, entonces $p \leq f(p)$. En conclusión y por antisimetría $p = f(p)$. □

**Teorema 3.17 – *Teorema de Cantor-Schröder-Bernstein*:** Si $A \lesssim B$ y $B \lesssim A$, entonces $A \approx B$.

Demostración: Sean $f : A \to B$ y $g : A \to B$ inyectivas, entonces definimos $F : \mathcal{P}(A) \to \mathcal{P}(A)$ tal que $F(x) := A \setminus g\big[B \setminus f[x]\big]$, veremos que $F$ es creciente:

$$\begin{aligned} x \subseteq y &\implies f[x] \subseteq f[y] \implies B \setminus f[y] \subseteq B \setminus f[x] \\ &\implies g\big[B \setminus f[y]\big] \subseteq g\big[B \setminus f[x]\big] \\ &\implies A \setminus g\big[B \setminus f[x]\big] \subseteq A \setminus g\big[B \setminus f[y]\big]. \end{aligned}$$

Y $(\mathcal{P}(A), \subseteq)$ es un conjunto parcialmente ordenado completo y acotado, por lo que aplicando el teorema del punto fijo de Knaster-Tarski se concluye que existe $z \subseteq A$ punto fijo de $F$.

Ahora notemos que $A \setminus z = g\big[B \setminus f[z]\big]$, de modo que $\operatorname{Img}(f \restriction z) = f[z]$ y $\operatorname{Img}(g \restriction B \setminus f[z]) = A \setminus z$ ambas siendo biyectivas, luego

$$h := (f \restriction z) \cup \big(g \restriction (B \setminus f[z])\big)^{-1}$$

es una biyección. □

## 3.2. Números cardinales

Al contrario de con los cardinales entre conjuntos finitos, el concepto de un *número cardinal* no es claro entre la literatura matemática, por eso, otorgaremos condiciones básicas para una definición de números cardinales y luego presentaremos tres modelos.

**Lema 3.18:** Si $A \approx B$ y $C \approx D$, entonces:

1. $A \amalg C \approx B \amalg D$.
2. $A \times C \approx B \times D$.
3. $\operatorname{Func}(A, C) \approx \operatorname{Func}(B, D)$.

**Definición 3.19:** Se dice que una tupla $(\mathfrak{C}, , +, \times, ()^{()})$ es un modelo de números cardinales, si:

1. $\overline{\overline{=}} : V \to \mathfrak{C}$ es función suprayectiva tal que $x \approx y$ syss $\overline{\overline{x}} = \overline{\overline{y}}$.
2. $+ : \mathfrak{C}^2 \to \mathfrak{C}$ es tal que $\overline{\overline{x}} + \overline{\overline{y}} = \overline{\overline{x \amalg y}}$.

3. $\cdot : \mathfrak{C}^2 \to \mathfrak{C}$ es tal que $\overline{\overline{x}} \cdot \overline{\overline{y}} = \overline{\overline{x \times y}}$.

4. $()^{()} : \mathfrak{C}^2 \to \mathfrak{C}$ es tal que $\overline{\overline{x}}^{\overline{\overline{y}}} = \overline{\overline{\mathrm{Func}(x, y)}}$.

Los elementos de $\mathfrak{C}$ se denotan con las letras góticas (i.e, $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$) y se dicen *números cardinales*. Mantendremos la notación de $n$ para el número cardinal de $I_n$.

Se define $\leq$ sobre $\mathfrak{C}$ como que $\overline{\overline{x}} \leq \overline{\overline{y}}$ syss $x \lesssim y$. El teorema de Cantor-Schröder-Bernstein dice que $\leq$ es un orden parcial sobre $\mathfrak{C}$.

**Proposición 3.20:** Para todo $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \mathfrak{s} \in \mathfrak{C}$:

1. $+, \cdot$ son conmutativos y asociativos.

2. $\mathfrak{p} \cdot (\mathfrak{q} + \mathfrak{r}) = \mathfrak{p}\mathfrak{q} + \mathfrak{p}\mathfrak{r}$.

3. $\underbrace{\mathfrak{p} + \mathfrak{p} + \cdots + \mathfrak{p}}_{n} = n\mathfrak{p}$ y $\underbrace{\mathfrak{p} \cdot \mathfrak{p} \cdots \mathfrak{p}}_{n} = \mathfrak{p}^n$.

4. $1^{\mathfrak{p}} = \mathfrak{p}^0 = 0^0 = 1$ y $0^{\mathfrak{q}} = 0$ con $\mathfrak{q} > 0$.

5. Si $\overline{\overline{x}} = \mathfrak{p}$, entonces $\overline{\overline{\mathcal{P}(x)}} = 2^{\mathfrak{p}}$.

6. Si $\mathfrak{p} \leq \mathfrak{r}$ y $\mathfrak{q} \leq \mathfrak{s}$, entonces $\mathfrak{p} + \mathfrak{q} \leq \mathfrak{r} + \mathfrak{s}$, $\mathfrak{p}\mathfrak{q} \leq \mathfrak{r}\mathfrak{s}$ y si $0 < \mathfrak{p}, \mathfrak{q}$ entonces $\mathfrak{p}^{\mathfrak{q}} \leq \mathfrak{r}^{\mathfrak{s}}$. En particular, $\mathfrak{p} \leq \mathfrak{p} + \mathfrak{q}$.

7. $\overline{\overline{x}} + \overline{\overline{y}} = \overline{\overline{x \cap y}} + \overline{\overline{x \cup y}}$, en particular, $\overline{\overline{x \cup y}} \leq \overline{\overline{x}} + \overline{\overline{y}}$.

8. Si $\mathfrak{q} \geq 1$, entonces $\mathfrak{p} \leq \mathfrak{p}\mathfrak{q}$ y $\mathfrak{p} \leq \mathfrak{p}^{\mathfrak{q}}$.

**Cardinales de Frege.** Sea $x$ un conjunto arbitrario, se define:

$$\overline{\overline{x}} := \{y : x \approx y\},$$

claramente las clases de la forma $\overline{\overline{x}}$ cumplen los requisitos para ser números cardinales, sin embargo, queda como ejercicio para el lector probar que todos los cardinales, exceptuando $\overline{\overline{\varnothing}}$ son clases propias.

**El truco de Scott.** Sea $\sim$ una relación de equivalencia universal, es decir, que se aplique para todos los conjuntos en el universo. Si queremos formar clases de equivalencia que sean conjuntos podemos hacer lo siguiente, definamos $[x]$ como la clase formada por los conjuntos $y$ tales que $x \sim y$ y que $y$ sean de rango mínimo. Dado que las clases $V_\alpha$ son conjuntos y claramente para todo conjunto $x$ se cumple que $[x] \subseteq V_{(\operatorname{rang} x)+1}$, entonces

los $[x]$ son conjuntos. Como aplicación del truco de Scott podemos utilizar la equipotencia, que claramente es una relación de equivalencia universal, para formar números cardinales que sean conjuntos.

Observe que el único requisito para formar los cardinales de Scott es asumir el axioma de fundación, el cual ya hemos discutido.

**Cardinales de von Neumann.** Sin embargo, lo más natural, y lo más útil sería utilizar a los ordinales como herramienta, esto requiere que todo conjunto sea equipotente a algún ordinal, pero podemos desarrollar nuestra teoría restringida exclusivamente a conjuntos que cumplan dicha descripción, en primer lugar admitamos una definición:

**Definición 3.21 – *Ordinales iniciales*:** Se dice que un ordinal $\lambda$ es *inicial* o un *cardinal de von Neumann* si para todo $\delta < \lambda$ se cumple que $\delta \not\approx \lambda$. Dado un ordinal $\alpha$ se denota $\overline{\alpha} := \min\{\beta \in \Omega_{\mathrm{Ord}} : \beta \approx \alpha\}$, es decir, $\overline{\alpha}$ es el único ordinal inicial equipotente a $\alpha$. Se denota por $\Omega_{\mathrm{Card}}$ al conjunto de cardinales de von Neumann.

**Lema 3.22 (Hartogs):** Si $x$ es un conjunto arbitrario existe un ordinal $\kappa < \Omega_{\mathrm{Ord}}$ tal que $\kappa \not\lesssim x$.

Demostración: Sea $P$ el subconjunto de $\mathcal{P}(x) \times \mathcal{P}(x^2)$ donde $(y, R) \in P$ si $R$ es un buen orden sobre $y$. Un ordinal $\alpha$ es tal que $\alpha \lesssim x$ syss existe $(y, R) \in P$ tal que $\alpha = \mathrm{ord}(y, R)$, luego si $\beta := \sup\{\mathrm{ord}(y, R) + 1 : (y, R) \in P\}$ entonces $\beta \not\lesssim x$ y $\beta$ es conjunto (¿por qué?). □

**Definición 3.23:** Dado $x$ un conjunto arbitrario se define el *número de Hartogs* de $x$, denotado por $\hbar(x)$, como el mínimo ordinal $\alpha$ tal que $\alpha \not\lesssim x$.

**Proposición 3.24:** Para todo conjunto $x$, $\hbar(x)$ es un conjunto y un ordinal inicial.

**Definición 3.25:** Se define $\aleph : \Omega_{\mathrm{Ord}} \to \Omega_{\mathrm{Ord}}$ como prosigue:

$$\aleph_0 := \omega, \quad \aleph_{\alpha+1} := \hbar(\aleph_\alpha), \quad \aleph_\lambda := \lim_{\delta<\lambda} \aleph_\delta.$$

Los ordinales que pertenecen al rango de la función $\aleph$ se dicen *álefs*. Cuando queramos utilizar las propiedades como ordinal de un álef de-

notaremos $\omega_\alpha$ a $\aleph_\alpha$.

Ojo que como los cardinales de von Neumann pretenden ser un modelo de cardinales la suma no es la misma que su suma como ordinales.

**Proposición 3.26:** Se cumple:

1. $\aleph$ es una función normal.
2. Todo ordinal infinito es inicial syss es un álef.
3. Los álefs son ordinales límite.

**Teorema 3.27:** Si $\kappa$ es un álef, entonces $\kappa^2 = \kappa$.

Demostración: Comenzaremos por definir el orden canónico de $(\Omega_{\mathrm{Ord}})^2$: $(\alpha, \beta) < (\gamma, \delta)$ syss $\max\{\alpha, \beta\} < \max\{\gamma, \delta\}$ o $\max\{\alpha, \beta\} = \max\{\gamma, \delta\}$ y $\alpha < \gamma$, o $\max\{\alpha, \beta\} = \max\{\gamma, \delta\}$, $\alpha = \gamma$ y $\beta < \delta$. Es fácil probar que éste es un buen orden. Luego se define $\Gamma : (\Omega_{\mathrm{Ord}})^2 \to \Omega_{\mathrm{Ord}}$ como el único isomorfismo de orden.

Por definición existe un único $\alpha \in \Omega_{\mathrm{Ord}}$ tal que $\kappa = \aleph_\alpha$, probaremos el teorema por inducción transfinita sobre $\alpha$: El caso inicial es trivial, pues para todo $(n, m) \in \omega^2$ hay finitos puntos menores que él. Sea $\alpha$, por contradicción, el primer ordinal tal que $\Gamma[\omega_\alpha^2] \neq \omega_\alpha$. Luego sean $\beta, \gamma < \omega_\alpha$ tales que $\Gamma(\beta, \gamma)$, como $\omega_\alpha$ es límite, existe $\max\{\beta, \gamma\} < \delta < \omega_\alpha$, por ende $\Gamma[\delta^2] \supseteq \omega_\alpha$, ergo, $|\delta^2| = |\delta|^2 > \omega_\alpha$, pero por minimalidad se cumple que $|\delta|^2 = |\delta| > \omega_\alpha$ lo que es absurdo. □

**Corolario 3.28:** Si $\kappa, \mu$ son ordinales iniciales y al menos uno es infinito, entonces

$$\kappa + \mu = \kappa \cdot \mu = \max\{\kappa, \mu\}.$$

## 3.3. El axioma de elección

Si tenemos un conjunto $A$ no vacío, la lógica nos permite extraer un $a \in A$ al azar. De forma similar, si $A$ es infinito se nos permite extraer cualquier tupla finita de $A$, sin embargo, no es capaz de explicarnos si podemos extraer un subconjunto infinito de elementos al azar. Esto último corresponde al axioma de elección y sus usos abarcan todas las ramas de las matemáticas, no obstante, tal como el axioma de elección puede utilizarse como una herramienta adicional para realizar demostraciones, también tiene consecuencias

"catastróficas" en ciertos contextos, es por ello que algunos matemáticos prefieren usar restricciones al axioma de elección, las cuales discutiremos (a grandes rasgos) en esta sección.

**Axioma de Elección (AE):** Dada una familia $\mathcal{F}$ de conjuntos no vacíos, existe una función $f : \mathcal{F} \to \bigcup \mathcal{F}$ tal que para todo $x \in \mathcal{F}$ se cumple que $f(x) \in x$.

Dichas funciones son apropiadamente llamadas *funciones de elección*, en esencia eligen un miembro al azar de un conjunto.

**Definición 3.29:** Si $(X, \leq)$ es un conjunto preordenado, entonces se dice que dos elementos $x, y \in X$ son *comparables* si $x \leq y$ o $y \leq x$. Un conjunto linealmente ordenado es un conjunto parcialmente ordenado en donde todo par de elementos son comparables.

Si $X$ es preordenado, entonces un subconjunto $A \subseteq X$ se dice:

**Cadena** Si todo par de elementos son comparables.

**Anticadena** Si todo par de elementos no son comparables.

**Teorema 3.30:** Son equivalentes:

1. **Axioma de elección** Toda familia de conjuntos no vacíos posee una función de elección.
2. **Teorema del buen orden de Zermelo** Todo conjunto puede ser bien ordenado.
3. **Lema de Zorn** Si en un conjunto parcialmente ordenado toda cadena está superiormente acotada, entonces dicho conjunto posee un elemento maximal.
4. **Lema de Teichmüller-Turkey** Si toda subfamilia no vacía $\mathcal{F}$ de $\mathcal{P}(X)$ de carácter finito[a] tiene un elemento maximal respecto de la inclusión.
5. Todo conjunto preordenado posee una anticadena maximal.

[a] Esto quiere decir que $A \in \mathcal{F}$ syss todo subconjunto finito de $A$ está en $\mathcal{F}$.

Demostración: (1) $\implies$ (2). El teorema del buen orden equivale claramente a que todo conjunto es equipotente a un ordinal: Sea $X$ un conjunto

arbitrario, sea $\infty \notin X$ un conjunto y sea $\sigma : \mathcal{P}(X) \setminus \{\varnothing\} \to X$ una función de elección. Primero, definamos $\bar{\sigma} : \mathcal{P}(X) \to X \cup \{\infty\}$ tal que $\bar{\sigma}(\varnothing) = \infty$ y $\bar{\sigma}(y) = \sigma(y)$ en otro caso. Vamos a definir por recursión transfinita una función $f : \hbar(X) \to X$ así: $f(0) := \sigma(X)$ y $f(\alpha) := \sigma(X \setminus \{f(\beta) : \beta < \alpha\})$. Por el lema de Hartogs se cumple que $f$ no puede ser inyectiva, es decir, ha de haber algún índice $\alpha$ tal que $f(\alpha) = \infty$, sea $\gamma$ el mínimo de ellos, luego $f|_\gamma$ es una biyección como se quería probar.

(2) $\implies$ (3). Sea $P$ dicho conjunto, por teorema del buen orden, existe $p : \gamma \to P$ biyectiva, luego se construye la siguiente sucesión por recursión transfinita la sucesión $c : \hbar(P) + 1 \to P$ así: $c_0 := p_0$ y $c_\alpha := p_\beta$ donde $\beta$ es el mínimo ordinal tal que $p_\beta$ es cota superior de $\{c_\delta : \delta < \alpha\}$ y de no existir tal elemento se repite tal elemento. Por lema de Hartogs, $c$ no puede ser inyectiva y por inducción transfinita, $\operatorname{Dom} c$ es una cadena, luego $c_{\hbar(P)}$ ha de ser un maximal.

(3) $\implies$ (4). Basta notar que toda cadena de una familia de carácter finito está acotada por su unión, luego por el lema de Zorn la familia tiene un elemento maximal.

(4) $\implies$ (5). Basta notar que el conjunto de anticadenas es una familia de carácter finito.

(5) $\implies$ (1). Sea $\mathcal{F}$ una familia de conjuntos no vacíos, entonces se define una relación $\leq$ sobre $\mathcal{F} \times \bigcup \mathcal{F}$ de modo que $(X, x) \leq (Y, y)$ syss $x \in X$, $y \in Y$ y $X = Y$. Es fácil notar que es de preorden, luego una anticadena maximal es necesariamente una función de elección. □

**Teorema 3.31:** Son equivalentes:

1. **El axioma de elección**.
2. **Principio maximal de Hausdorff:** Todo conjunto parcialmente ordenado posee una cadena maximal.

Hint: Relacione el principio de Hausdorff con los otros dos principios de maximalidad (de Zorn y de Teichmüller-Turkey). □

**Lema 3.32:** Si $A$ es bien ordenable, entonces existe un orden lineal sobre $\mathcal{P}(A)$.

Demostración: Sin perdida de generalidad, sea $A = \alpha$ un ordinal. Luego si $x \neq y \subseteq \alpha$, entonces

$$\delta_{xy} := \text{mín}(x \Delta y)$$

luego se define $x \leq y$ syss $x = y$ o $\delta_{xy} \in x$.
Claramente $\leq$ es reflexiva y conexa, probaremos que $<$ es transitiva: Si $x < y$ e $y < z$, probaremos que $x < z$. En primer lugar $\delta_{xy} \neq \delta_{yz}$, por lo que se debe dar alguna posibilidad: Si $\delta_{xy} < \delta_{yz}$, entonces $\delta_{xy} \notin z$, pues de lo contrario $\delta_{xy} \in y\Delta z$ contradiciendo la minimalidad de $\delta_{yz}$, por ende, $\delta_{xy} \in x\Delta z$. Si $\alpha \in x\Delta z$, puede darse que $\alpha \notin y$, en cuyo caso $\alpha \in x\Delta y$ o $\alpha \in y\Delta z$. Si $\alpha \in y \setminus x$, entonces $\alpha \in x\Delta y$, por lo que $\alpha \geq \delta_{xy}$. Si $\alpha \in y \setminus z$, entonces $\alpha \in y\Delta z$ y $\alpha \geq \delta_{yz} > \delta_{xz}$. En conclusión, $\delta_{xy} = \delta_{xz}$.
Si $\delta_{yz} < \delta_{xy}$, entonces $\delta_{yz} \in x$, luego análogamente se comprueba que $\delta_{yz} = \delta_{xz}$. □

**Teorema 3.33:** Son equivalentes:

1. **El axioma de elección**.
2. **El axioma de elecciones múltiples:** Para toda familia de conjuntos no vacíos $\{X_i : i \in I\}$ existe otra familia de conjuntos no vacíos $\{F_i : i \in I\}$ tales que $F_i$ es finito y $F_i \subseteq X_i$.
3. **Principio de Kurepa:** Todo conjunto parcialmente ordenado posee una anticadena maximal.
4. Todo conjunto linealmente ordenado puede ser bien ordenado.
5. El conjunto potencia de un conjunto bien ordenado puede ser bien ordenado.

Demostración: (1) $\implies$ (2). Trivial.

(2) $\implies$ (3). Sea $X$ parcialmente ordenado. Sea $f : \mathcal{P}(X) \setminus \{\varnothing\} \to \mathcal{P}_{\text{fin}}(X) \setminus \{\varnothing\}$ una función de elección múltiple tal que para todo $A \subseteq X$ no vacío, $f(A) \subseteq A$ finito. Luego sea $g(A)$ el subconjunto de elementos minimales de $g(A)$ que tiene la propiedad de que para todo $A$, $g(A)$ es una anticadena.
Si $K$ es una anticadena, definiremos

$$H(K) := \{x \in X \setminus K : K \cup \{x\} \text{ anticadena}\}$$

procedemos por contradicción, si $X$ no tuviese una anticadena maximal, para toda anticadena $K$ se cumpliría que $H(K)$ es no vacío, luego sea $\sigma : \hbar(\mathcal{P}(X)) \to \mathcal{P}(X)$ definido por inducción transfinita tal que

$$\sigma(\alpha) := \bigcup_{\beta<\alpha} \sigma(\beta) \cup g\left(H\left(\bigcup_{\beta<\alpha} \sigma(\beta)\right)\right),$$

pero es claramente inyectiva lo que contradice la definición de número de Hartogs.

(3) $\implies$ (4). Si $(X, \leq)$ es linealmente ordenado, entonces con

$$Y := \{(A, a) : a \in A \subseteq X\},$$

se define $\preceq$ sobre $Y$ como $(A, a) \preceq (B, b)$ syss $A = B$ y $a \leq y$. Es fácil notar que $\preceq$ es parcialmente ordenado, luego por el principio de Kurepa posee una anticadena maximal, pero ésto corresponde a una función de elección sobre $X$, luego $X$ es bien ordenable.

(4) $\implies$ (5). Basta aplicar el lema anterior.

(5) $\implies$ (1). Asumiendo el axioma de fundación, basta probar que los universos de von Neumann son bien ordenables. El caso base y el caso sucesor son triviales, pero el caso límite es más delicado: Si $V_\delta$ es bien ordenable para todo $\delta < \lambda$, entonces $\kappa := \bigcup_{\delta<\lambda} |V_\delta|^+$. Como $\kappa$ es por definición bien ordenable, entonces $\leq^*$ es un buen orden sobre $\mathcal{P}(\kappa)$.

Ahora construiremos unos buenos ordenes $\trianglelefteq_\alpha$ sobre $V_\alpha$ tal que para todo $\beta \leq \alpha$ se cumpla que $V_\beta$ es un segmento inicial de $V_\alpha$, lo haremos por recursión transfinita:
El caso base $\trianglelefteq_0 := \varnothing$.
Si $\trianglelefteq_\delta$ está definido, entonces sea $\varphi_\delta$ el isomorfismo de orden entre $(V_\delta, \trianglelefteq_\delta)$ y su tipo de orden $\alpha_\delta$. Claramente $\alpha_\delta < \kappa$, luego $\mathcal{P}\alpha_\delta \subseteq \mathcal{P}\kappa$ con lo que $\leq^*$ se restringe a un buen orden sobre $\mathcal{P}\alpha_\delta$ que induce un buen orden $\trianglelefteq^*_{\delta+1}$ en $\mathcal{P}(V_\delta) = V_{\delta+1}$. Finalmente definimos

$$x \trianglelefteq_{\delta+1} y \iff \begin{cases} x \trianglelefteq_\delta y, & \operatorname{rang} x < \delta > \operatorname{rang} y \\ x = x, & \operatorname{rang} x < \delta = \operatorname{rang} y \\ x \trianglelefteq^*_{\delta+1} y, & \operatorname{rang} x = \delta = \operatorname{rang} y \end{cases}$$

Si $\nu$ es límite y $\{\trianglelefteq_\delta\}_{\delta<\nu}$ está definido, entonces $\trianglelefteq_\nu := \bigcup_{\delta<\nu} \trianglelefteq_\delta$ y es fácil notar que es, en efecto, un buen orden.

Finalmente si $x, y \in V_\lambda$, entonces $\gamma := \text{máx}\{\operatorname{rang} x, \operatorname{rang} y\}+1 < \lambda$, luego $x \trianglelefteq_\lambda y$ syss $x \trianglelefteq_\gamma y$. De modo que $\trianglelefteq_\lambda$ es un buen orden sobre $V_\lambda$ cómo se quería probar. □

**§3.3.1 Equivalencias en la aritmética cardinal.** El teorema del buen ordenamiento de Zermelo, entre otras cosas, dice que todo cardinal es de hecho un cardinal de von Neumann lo que nos da una inmensa ventaja a la hora de hacer aritmética cardinal, pero veremos que otras condiciones aparentemente más débiles tienen de hecho el mismo efecto.

**Teorema 3.34:** Son equivalentes:

1. **El axioma de elección**.
2. Para todo par de conjuntos $x, y$ se cumple que $x \lesssim y$ o $y \lesssim x$ ($\lesssim$-comparabilidad).

Demostración: $\Longrightarrow$. El AE es equivalente a que todo conjunto es equipotente a un ordinal y es claro que los ordinales son $\lesssim$-comparables.

$\Longleftarrow$. Si todos los conjuntos son $\lesssim$-comparables, entonces basta considerar un conjunto $x$ y su número de Hartogs $\hbar(x)$, para concluir que $x$ es equipotente a un ordinal. □

**Teorema 3.35:** Si $\mathfrak{p}$ es un cardinal y $\kappa$ un álef tales que $\mathfrak{p} + \kappa = \mathfrak{p}\kappa$, entonces $\mathfrak{p} \leq \kappa$ o $\kappa \leq \mathfrak{p}$.

Demostración: Sea $X$ tal que $\overline{\overline{X}} = \mathfrak{p}$, entonces existen $A, B$ tales que $\overline{\overline{A}} = \mathfrak{p}$, $\overline{\overline{B}} = \kappa$ y que $X \times \kappa = A \cup B$.

Para todo $x \in X$ sea $s_x := \{x\} \times \kappa$, si existe algún $x \in X$ tal que $s_x \subseteq A$, entonces $\kappa \leq \mathfrak{p}$. De lo contrario, sea $\alpha_x$ el primer ordinal tal que $(x, \alpha_x) \notin A$, luego $\{(x, \alpha_x) : x \in X\} \subseteq B$ y $\mathfrak{p} \leq \kappa$. □

**Teorema 3.36:** Son equivalentes:

1. **El axioma de elección**.
2. Para todo $\mathfrak{p}, \mathfrak{q}$ infinitos se cumple que $\mathfrak{p} + \mathfrak{q} = \mathfrak{p}\mathfrak{q}$.
3. Para todo $\mathfrak{p}$ infinito se cumple que $\mathfrak{p}^2 = \mathfrak{p}$.
4. Para todo $\mathfrak{p}, \mathfrak{q}$ se cumple que $\mathfrak{p}^2 = \mathfrak{q}^2$ implica $\mathfrak{p} = \mathfrak{q}$.
5. **Sucesores cardinales:** Sea $\mathfrak{p}$, existe $\mathfrak{q} > \mathfrak{p}$ tal que para todo $\mathfrak{r} > \mathfrak{p}$ se cumple que $\mathfrak{q} \leq \mathfrak{r}$.

Demostración: (1) $\Longrightarrow$ (2) $\wedge$ (3) $\wedge$ (4) $\wedge$ (5). Trivial.

(2) $\Longrightarrow$ (1). Basta aplicar el teorema anterior con $\hbar(\mathfrak{p})$ para obtener que $\mathfrak{p}$ es un álef.

(3) $\Longrightarrow$ (2). Sea $\kappa := \hbar(\mathfrak{p})$, entonces es claro que $\mathfrak{p}\kappa \geq \mathfrak{p} + \kappa$, por ende basta probar la otra desigualdad:

$$\mathfrak{p} + \kappa = (\mathfrak{p} + \kappa)^2 = \mathfrak{p}^2 + 2\mathfrak{p}\kappa + \kappa^2 \geq \mathfrak{p}\kappa.$$

(4) $\implies$ (2). Sea $\mathfrak{p}$ infinito, entonces se define $\kappa := \mathfrak{p}^{\aleph_0}$ e inmediatamente $\kappa^2 = \kappa$. Luego

$$(\kappa \cdot \hbar(\kappa))^2 = \kappa \cdot \hbar(\kappa),$$

y probaremos que

$$(\kappa + \hbar(\kappa))^2 = \kappa \cdot \hbar(\kappa).$$

Notemos que

$$(\kappa + \hbar(\kappa))^2 = \kappa^2 + 2\kappa\hbar(\kappa) + \hbar(\kappa)^2 \geq \kappa \cdot \hbar(\kappa)$$

$$\begin{aligned}(\kappa + \hbar(\kappa))^2 &= \kappa^2 + 2\kappa\hbar(\kappa) + \hbar(\kappa)^2 \\ &= \kappa + \kappa\hbar(\kappa) + \hbar(\kappa) \\ &\leq \kappa\hbar(\kappa) + \kappa\hbar(\kappa) = \kappa \cdot \hbar(\kappa).\end{aligned}$$

Con lo que $\kappa$ es un álef, y claramente $\mathfrak{p} \leq \kappa$, luego $\mathfrak{p}$ es un álef.

(5) $\implies$ (1). Sea $A \approx \mathfrak{p}$, con $\mathfrak{p}$ un cardinal infinito cualquiera cuyo número de Hartogs es $\kappa$, cómo $\kappa$ posee sucesor cardinal éste ha de ser $\kappa^+$ (¿por qué?) y cómo $\kappa \leq \mathfrak{p} + \kappa$, entonces o $\mathfrak{p} + \kappa \geq \kappa^+$ o $\mathfrak{p} + \kappa = \kappa$.
Veamos por qué no puede darse el primer caso: Claramente $\mathfrak{p} + \kappa \approx A \amalg \kappa$. Si $\kappa^+ \leq \mathfrak{p} + \kappa$, entonces $\kappa^+ \approx B \subseteq A \amalg \kappa$, luego $B_- := B \cap (\{1\} \times \kappa)$ y $B_+ := B \cap (\{0\} \times A)$, al ser subconjuntos de un conjunto bien ordenable, ambos también lo son y claramente $B_- \lesssim \kappa$, luego $\kappa^+ \approx B_+ \lesssim A$, lo que es absurdo.
Finalmente, cómo $\mathfrak{p} \leq \mathfrak{p} + \kappa = \kappa$, entonces $\mathfrak{p}$ es un álef. □

**§3.3.2 Formas débiles de elección.** Debido a la inmensa potencia del AE, se definen versiones restringidas de él que son también útiles y menos catastróficas.

**Definición 3.37:** Se definen:

**Axioma de elecciones dependientes (DE)** Si $(X, R)$ son tales que para todo $x \in X$ el conjunto $\{y : xRy\}$ es no vacío. Entonces existe una sucesión $s : \mathbb{N} \to X$ tal que $s_i R s_{i+1}$ para todo $i \in \mathbb{N}$.

**Axioma de elecciones numerables (AEN)** Si $\mathcal{F}$ es una familia numerable de conjuntos no vacíos, entonces posee una función de elección.

**Teorema 3.38:** Se cumple:

$$\text{AE} \implies \text{DE} \implies \text{AEN}.$$

**Proposición (DE) 3.39:** Se cumple:

1. Si $(A, \leq)$ es linealmente ordenado, entonces es un buen orden syss no existe una sucesión estrictamente decreciente infinita.

2. Una relación binaria $R$ sobre $A$ está bien fundada syss no existe una sucesión $(a_n)_{n\in\mathbb{N}}$ en $A$ tal que para todo $n \in \mathbb{N}$

$$a_{n+1}\ R\ a_n.$$

**Teorema (AEN) 3.40:** La unión numerable de conjuntos numerables es numerable.

Demostración: Sean $\{X_i\}_{i\in\mathbb{N}}$ una sucesión de conjuntos numerables, se define $X := \bigcup_{i\in\mathbb{N}} X_i$ e $Y := \bigcup_{i\in\mathbb{N}} \{i\} \times X_i$. Como $X_0 \subseteq X$, entonces $\mathbb{N} \lesssim X$ y para ver que $X \lesssim Y$ se define $f : X \to Y$ tal que $f(x) = (n, x)$ donde $n$ es el mínimo índice tal que $x \in X_n$. Por Cantor-Schröder-Bernstein basta probar que $Y \lesssim \mathbb{N}$. Es claro que $Y$ es la unión disjunta de conjuntos numerables, luego para todo $X_i$ sea $x_i : \mathbb{N} \to X_i$ una biyección de modo que $x_i^n := x_i(n)$. Luego $Y \approx \mathbb{N}^2$, y, por ser un álef, se cumple que $\mathbb{N}^2 \approx \mathbb{N}$, ergo, $X \lesssim Y \approx \mathbb{N}$. □

La elección fue necesaria al momento de elegir las biyecciones.

**Teorema (AEN) 3.41:** Toda clase infinita contiene una subclase numerable (que es, por ende, un conjunto). Equivalentemente, $X$ infinito syss $\mathbb{N} \lesssim X$.

Demostración: Sea $X$ un conjunto infinito, $\mathcal{F} := \{[X]^n : n \in \mathbb{N}\}$ y sea $\sigma : \mathbb{N} \to \mathcal{F}$ una función de elección sobre $\mathcal{F}$, evidentemente $Y := \bigcup_{n\in\mathbb{N}} \sigma(n) \subseteq X$ y por el teorema anterior $Y \approx \mathbb{N}$ como se quería probar.

Si $X$ es una clase propia, se puede utilizar el truco de Scott para poder construir subconjuntos de los $[X]^n$. □

## 3.4. Aritmética cardinal

Toda ésta sección depende del axioma de elección, empezando por el lema que permite que las expresiones estén bien fundamentadas.

**Lema 3.42:** Si $\{A_i\}_{i\in I}$ y $\{B_i\}_{i\in I}$ son familias de conjuntos tales que $A_i \approx B_i$ para todo $i \in I$, entonces

$$\coprod_{i\in I} A_i \approx \coprod_{i\in I} B_i, \quad \prod_{i\in I} A_i \approx \prod_{i\in I} B_i.$$

**Definición 3.43:** Si $\{X_i : i \in I\}$ es una familia de conjuntos, entonces se define:

$$\sum_{i\in I} |X_i| := \left|\coprod_{i\in I} X_i\right|, \quad \prod_{i\in I} |X_i| := \left|\prod_{i\in I} X_i\right|.$$

En general, la suma y producto requieren de aplicaciones del AE para quedar bien definidos, sin embargo, por lo general en ésta sección utilizaremos a los cardinales de von Neumann mismos los cuales tienen una estructura bien definida. Por ejemplo, no se requiere de AE para probar que el producto de cardinales no vacíos es no vacío, ya que todos contienen al 0.

**Teorema 3.44:** Si $\{X_i : i \in I\}$ es una familia de conjuntos, entonces:

$$\left|\bigcup_{i\in I} X_i\right| \leq \sum_{i\in I} |X_i|.$$

**Teorema 3.45:** Si $\kappa := \sup\{\kappa_i : i \in I\}$ e $|I| = \mu$, entonces se cumple:

1. $\sum_{i\in I} \kappa_i = |I| \sup\{\kappa_i : i \in I\}$.
2. $\prod_{i\in I} \kappa_i^{\nu} = \left(\prod_{i\in I} \kappa_i\right)^{\nu}$.

# 4

# *Álgebras booleanas*

## 4.1. Álgebras booleanas

**Definición 4.1 – *Álgebra booleana*:** Es una séxtupla $(A, \vee, \wedge, \neg, 0, 1)$ donde $\vee, \wedge : A^2 \to A$ y $\neg : A \to A$ son tales que para todo $p, q, r \in A$:

1. $\neg(\neg p) = p$ (doble negación).
2. $1 = \neg 0$ y $0 = \neg 1$.
3. $p \wedge 1 = p \vee 0 = p$.
4. $p \wedge \neg p = 0$ y $p \vee \neg p = 1$.
5. $p \wedge p = p \vee p = p$ (idempotencia).
6. $p \wedge q = q \wedge p$ y $p \vee q = q \vee p$ (conmutatividad).
7. $(p \wedge q) \wedge r = p \wedge (q \wedge r)$ y $p \vee (q \vee r) = (p \vee q) \vee r$ (asociatividad).
8. $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$ y $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ (distributividad).
9. $p \vee (p \wedge q) = p$ y $p \wedge (p \vee q) = p$ (absorción).
10. $p \wedge 0 = 0$ y $p \vee 1 = 1$ (complementación).

11. $\neg(p \wedge q) = \neg p \vee \neg q$ y $\neg(p \vee q) = \neg p \wedge \neg q$ (leyes de De Morgan).

Se dice que un subconjunto es una *subálgebra* de $A$ si es no vacío y cumple ser un álgebra booleana.

Los axiomas para un álgebra booleana son muchos, pero en realidad éste es el enfoque de gran parte de los libros, fácilmente el lector notará que gran parte de las propiedades pueden simplificarse.

**Proposición 4.2:** Para que una séxtupla $(A, \vee, \wedge, \neg, 0, 1)$ sea un álgebra booleana basta con que satisfaga las leyes de conmutatividad, asociatividad, distributividad, absorción y complementación.

**Ejemplo.** Si $A$ es una clase no vacía, entonces $(\mathcal{P}(A), \cup, \cap, ^c, \varnothing, \mathcal{P}(A))$ es un álgebra booleana. A esta clase de álgebras booleanas se les dice *conjuntistas*.

# 5

# *Introducción a la teoría de modelos*

**Definición 5.1 – *Lenguaje, modelo*:** Un *lenguaje* $\mathcal{L}$ es simplemente una clase de símbolos separados en tres tipos:

1. Un conjunto de símbolos $\mathcal{C}$, denominados *constantes*.
2. Un conjunto de símbolos $\mathcal{F}$, denominados *funtores* donde a cada elemento le corresponde un único número natural.
3. Un conjunto de símbolos $\mathcal{R}$, denominados *relatores* donde a cada elemento le corresponde un único número natural.

Se dice que $\mathcal{M}$ es una $\mathcal{L}$-estructura si consta de:

- Una clase $M$ llamada *universo* de $\mathcal{M}$.
- Una función $f^{\mathcal{M}} : M^{n_f} \to M$ a todo funtor $f$ de $\mathcal{L}$.
- Una subclase $R^{\mathcal{M}} \subseteq M^{n_R}$ a todo relator $R$ de $\mathcal{L}$.
- Un elemento $c^{\mathcal{M}} \in M$ a toda constante de $\mathcal{L}$.

A $f^{\mathcal{M}}, R^{\mathcal{M}}$ y $c^{\mathcal{M}}$ se les dicen *interpretaciones* de $\mathcal{M}$ a $\mathcal{L}$.

**Ejemplo (lenguaje y modelo de Peano).** Primero establezcamos un lenguaje $\mathcal{L}$ de única constante $\spadesuit$, con un funtor monádico $S$, un funtor diádico $\oplus$ y un relator diádico $\sim$. Luego podemos considerar $\mathbb{N}$ como $\mathcal{L}$-modelo donde

$\spadesuit^{\mathbb{N}} \equiv 0$, $S(t) \equiv t^{\mathbb{N}} + 1$, $\oplus(a, b) \equiv a^{\mathbb{N}} + b^{\mathbb{N}}$ y $\sim \equiv =$. De modo que por ejemplo, el número 2 se denota $SS\spadesuit$ y el clásico teorema $2 + 2 = 4$ se denota

$$\sim \oplus SS\spadesuit SS\spadesuit SSSS\spadesuit$$

recordemos que ésto no es más que notación, en la práctica nunca ocuparemos ésta clase de notaciones.

# *Índice de notación*

| | |
|---|---|
| $\varnothing$ | Conjunto vacío, p. 7. |
| $A \subseteq B, A \subset B$ | $A$ es subconjunto, o subconjunto propio resp. de $B$, p. 7. |
| $(x, y)$ | Par ordenado de $x$ e $y$, p. 9. |
| $\bigcup \mathcal{A}, A \cup B$ | Unión de todos los miembros de $\mathcal{A}$, unión de $A$ y $B$ resp., p. 9. |
| $\bigcap \mathcal{A}, A \cap B$ | Intersección de todos los miembros de $\mathcal{A}$, intersección de $A$ y $B$ resp., p. 11. |
| $\mathcal{P}(A)$ | Conjunto potencia de $A$, p. 13. |
| $A \times B$ | Producto cartesiano de $A$ con $B$, p. 13. |
| $\operatorname{Dom} R, \operatorname{Img} R$ | Dominio e imagen de una relación $R$ resp., p. 14. |
| $\operatorname{Fld} R$ | Campo de una relación $R$, p. 14. |
| $R : A \multimap B$ | $R$ es relación desde $A$ hasta $B$, p. 14. |
| $f : A \to B$ | $f$ es una aplicación desde $A$ a $B$, p. 18. |
| $\operatorname{Func}(A, B)$ | El conjunto de funciones de dominio $A$ y codominio $B$, p. 18. |
| $\operatorname{Sym}(A)$ | El conjunto de biyecciones de dominio y codominio $A$, p. 18. |
| $\operatorname{Obj} \mathsf{C}, \operatorname{Morf} \mathsf{C}$ | Objetos, morfismos de la categoría $\mathsf{C}$, resp., p. 21. |

| | |
|---|---|
| $\mathrm{Hom}_{\mathsf{C}}(A, B)$ | Morfismos de $\mathsf{C}$ con dominio en $A$ y codominio en $B$, p. 21. |
| $\mathrm{End}_{\mathsf{C}}(A)$ | Endomorfismos de $\mathsf{C}$ sobre $A$, p. 21. |
| $\mathbb{N}$ | Conjunto de números naturales, p. 26. |
| $\mathbb{Z}$ | Conjunto de números enteros, p. 30. |
| $\omega$ | La clase de ordinales finitos, p. 42. |
| $V_\alpha$ | Conjunto formado por los conjuntos de rango $< \alpha$, p. 46. |
| $A \approx B$ | $A, B$ son equipotentes, p. 49. |
| $\hbar(A)$ | Número de Hartogs de un conjunto $A$, p. 55. |
| AE | Axioma de elección, p. 57. |
| AEN, DE | Axioma de elecciones numerables y dependientes, resp., p. 62. |

# *Índice alfabético*

# *Bibliografía*

## Teoría de conjuntos


1. Castillo, C. I. *Teoría de Conjuntos* `https://www.uv.es/ivorra/Libros/TC.pdf` (2019).
2. Hernández, F. H. *Teoría de Conjuntos. Una Introducción* (Sociedad Matemática Mexicana, 2003).
3. Jech, T. *Set Theory* (Springer-Verlag Berlin Heidelberg, 1978).
4. Lévy, A. *Basic Set Theory* (Dover Publications, Inc., 1979).
5. Vidal, J. C. *Teoría de Conjuntos* `https://www.uv.es/~jkliment/Documentos/SetTheory.pc.pdf` (2010).
6. Winfried Just, M. W. *Discovering Modern Set Theory* (American Mathematical Society, 1991).


## Teoría de modelos


7. Takeuti, G. *Proof Theory* (Elsevier Science, 1975).