Conjuntos

José Cuevas Barrientos

19 de diciembre de 2022

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.

Introducción

La teoría de conjuntos emerge a finales del siglo 19 y principios del siglo 20 como una solución al problema de los fundamentos de las matemáticas, debe entenderse pues que la matemáticas sin conjuntos es posible y muy natural, pero que desde su aparición los conjuntos son universalmente empleados pues poseen una estructura lo suficientemente *amorfa* como para poder representar todo tópico en matemáticas. Ésto, como siempre, es un arma de doble filo: por un lado todo es un conjunto (o una clase en la teoría NBG), y por el otro lado la expresión «X es un conjunto» es en general extremadamente vacía.

0.1 Historia de la teoría de conjuntos

La teoría de conjuntos fue inventada por Georg Cantor en 1874 para resolver un problema de series trigonométricas mediante inducción transfinita. El tema de los conjuntos fue adoptado por Peano, Dedekind y Frege como un prototipo de fundamentos para las matemáticas, en particular, Frege propondría la primera teoría axiomática de conjuntos que luego sería contradecida mediante la paradoja de Burali-Forti, y más tarde por la paradoja de Russell, lo que obligó a replantearse la cuestión de las axiomatizaciones de conjuntos y surge así entre 1903 y 1923 la teoría ZFC con aportes adicionales de Skolem y Mirimanoff.

Volviendo a Cantor, al estudiar con detenimiento sus teorías de ordinales y cardinales, él optaría por dedicarse extensivamente a explorar el segundo por el resto de su vida, lo que resulta muy apropiado pues es también el más vasto de los campos de la teoría de conjuntos incluso hasta el presente. Uno de los principales aspectos de su trabajo fue estudiar la relación entre los números cardinales $\aleph_0$ del conjunto de números naturales y $\mathfrak{c} = 2^{\aleph_0}$ de los números reales, Cantor sospechaba que $\mathfrak{c} = \aleph_1$ lo que hoy se conoce como la hipótesis del continuo, dando paso a una generalización. El problema de clasificar números cardinales también está estrechamente relacionado al problema del axioma de elección, ésto se suma a otros problemas de cuestiones que parecen ser "indemostrables", de modo que la historía de la teoría de conjuntos es también la historía de la teoría de modelos. Aquí se destaca la figura de Gödel que revolucionó la perspectiva sobre ellos, y demostro la consistencia de $\mathsf{ZF} + \mathsf{AE}$; así como el famoso método de *forcing* de Cohen en 1963 que prueba la consistencia de $\mathsf{ZF} + \neg\mathsf{AE}$. El método de *forcing* se volvió popular porque mató varios pájaros de un tiro, entre los cuales se prueba la independencia de la existencia de los cardinales inaccesibles, los cuales surgen a partir de una duda de Hausdorff y más tarde fueron adoptados por Sierpiński y Tarski.

La gran importancia que adquiere la teoría de conjuntos es como un lenguaje universal para poder describir las matemáticas de maneras formales, el cuál sería principalmente el objetivo de una serie de charlas realizadas por David Hilbert en la universidad de Göttingen. La teoría de conjuntos desde su origen era visto como una ramificación del análisis, pues sus primeros objetivos tenían relación con él, la idea de considerar la teoría de conjuntos como un tópico o una rama aislada de las matemáticas vendría mucho después de la mano con la idea de la lógica matemática; en ese sentido se parece a lo sucedido con la topología que eventualmente también se disasocia del análisis, a pesar de ser imprescendible en y para él. La topología también emplea y se hace valer de varios teoremas de la teoría de conjuntos. Finalmente, tiempo después, se discutiría el tema de la teoría de categorías como una nueva y alternativa fundación de las matemáticas a la teoría de conjuntos, la diferencia es una que algunos categoristas plantean como la distinción entre unas matemáticas estáticas (conjuntos) y fluidas (categorías); el problema de la construcción de categorías sería parcialmente resuelta con los universos de Grothendieck que emplean los cardinales fuertemente inaccesibles en los universos de von Neumann, pero la mayoría de categoristas ignora los fundamentos formales para su construcción y recrean una axiomatización similar a la teoría de tipos de Russell, que es de hecho predecesora a los conjuntos. Originalmente, Cantor no hubiera esperado que la teoría básica de conjuntos se volviera conocimiento elemental del academicismo matemático, actualmente enseñado en los primeros años de universidad, y es probable que en unas decadas la teoría de categorías reemplace a los conjuntos.

Realicé la siguiente tabla sobre la historia de la teoría de conjuntos tomando en cuenta las anotaciones históricas de Jech [**4**] y la introducción de Andreas Blass [**13**].

Año	**Suceso**	**Fuente**
1874	$\mathbb{R}$ es no numerable [**17,** Teo. 1.44]. El conjunto de reales algebraícos es numerable.	Georg Cantor. *Ueber eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen.*
1878	Definición de equipotencia (§3.1). Formulación de la hipótesis del continuo (§3.6).	Georg Cantor. *Ein Beitrag zur Mannigfaltigkeitslehre.*
1904	Formulación del axioma de elección (AE) para probar el teorema del buen orden (§3.3).	Ernest Zermelo. *Beweis, dassjede Menge wohlgeordnet werden kann.*
1908	Primera formulación de ZFC (§1.2).	Ernest Zermelo. *Untersuchungen über die Grundlagen der Mengenlehre.*
1912	Investigación de los cardinales de Mahlo (§4.2.1). Primer ejemplo de cardinal inaccesible.	Paul Mahlo. *Zur Theorie und Anwendung der ρ_0-Zahlen.*
1920	Problema de las rectas de Suslin.	Mikhail Suslin. *Problème 3.*
1924	Descubrimiento de la paradoja de Banach-Tarski [**17,** §A.1.3] como consecuencia del AE.	Stefan Banach y Alfred Tarski. *Sur la d'ecomposition des ensembles de points in parties respectivement congruents.*
1925	Formulación del axioma de fundación (§2.4) y primera versión de la teoría NBG.	John von Neumann. *Eine Axiomatisierung der Mengenlehre.*
1930	Definición de cardinal inaccesibles (§3.5.3).	Wacław Sierpiński y Alfred Tarski. *Sur une propriété caracteristique des nombres inaccessibles.*
	Los cardinales medibles son inaccesibles.	Stanisław Ulam. *Zur Masstheorie in der allgemeinen Mengenlehre.*
1935	Construcción de los árboles de Aronszajn y de Kurepa. Equivalencia de árboles con el problema de Suslin.	Đ. Kurepa. *Ensembles ordonnés et ramifiés.*
1956	Notación flecha de combinatoria. Teorema de Erdős-Rado.	P. Erdős y R. Rado. *A partition calculus in set theory.*

Año	Suceso	Fuente
	Teorema de Fodor.	G. Fodor. *Eine Bemerkung zur Theorie der regressiven Funktionen.*
1962	Formulación del axioma de determinación (AD).	Jan Mycielski y Hugo Steinhaus. *A mathematical axiom contradicting the Axiom of Choice.*
1963	Invención del método de *forcing* para probar la independencia del HC.	Paul Cohen. *The independence of the continuum hypothesis.*

0.2 Historia de la teoría de categorías

La teoría de categorías se distancia bastante de la historia de la teoría de conjuntos, mientras que una se forja en conjunción con la lógica y el cuestionamiento a los fundamentos de las matemáticas, la otra tiene unos origenes prácticos que sientan las bases de la filosofía categorista. La cuestión es la siguiente: al encontrarse con objetos más complicados tanto en álgebra como en topología se vuelve tanto o más razonable el estudio desde un punto de vista de *cómo* interactúa el objeto respecto a sus funciones, que de *qué* está compuesto internamente.

El paso cero fueron las revoluciones en las definiciones formales de función según la escuela de Cantor y Dedekind, pero el primer rayo concreto de luz a ésta nueva teoría fue precisamente un artículo de la mano de dos topólogos algebristas en los años cuarenta: Eilenberg y Mac Lane. Mac Lane se encargaría durante años de difundir su propia obra y organizar la teoría que se mecía en su seno, lo que lo convirtió en uno de los filósofos de las matemáticas más distinguido del último siglo.

Una pregunta intermedia natural sería la siguiente: ¿si la teoría de categorías se consolida como siendo infinitamente más útil que la teoría elemental de conjuntos, por qué aún predomina la segunda en ambitos pedagógicos? En primer lugar, la teoría de conjuntos es más vieja y por ello goza de un mayor estándar; en segundo lugar, la teoría de categorías requiere un profundo cambio de paradigma que no es del todo necesario para disciplinas como análisis real o funcional, sino que adquiere tonalidades distintas cuando se pone en contexto de teorías algebraicas; en tercer lugar, predomina una buena metáfora que contrasta a ambas, los conjuntos comprenden una teoría *estática* o *rígida* de las matemáticas, mientras que las categorías comprenden una teoría *fluida*; lo que quiere decir que en general, el enfoque categorial es más complicado puesto que para poder decir algo útil de un objeto hay que ponerlo a actuar con otros, mientras que los conjuntos ya vienen con sus acciones más o menos bien descritas, aunque poco expresivas; y en cuarto lugar, porque si bien las categorías forman una base sólida de las matemáticas, se asienta sobre los pilares axiomáticos de los conjuntos (aunque varios categoristas ignoran los aspectos conjuntistas que permiten libertades sobre sus objetos, como los modelos y los cardinales inaccesibles).

En cualquier caso, los conjuntos ofrecen un panorama discreto de las matemáticas, mientras que los topólogos, algebristas y geómetras buscaban una entidad más conexa que abarcase sus teorías. Curiosamente, señala Mac Lane que la notación de las funciones mediante flechas ($f\colon X \to Y$) surgió antes de las categorías, y que de hecho inspiró el concepto original. La verdadera revolución de Eilenberg y Mac Lane fue declarar a las flechas como tan importantes como los espacios sobre los cuales actuaban.

En los años cincuenta, Mac Lane comenzó a mirar el álgebra mediante el nuevo prisma de las categorías y se topó con la curiosa simetría entre módulos y grupos abelianos, y se percató de que no residía en el hecho de que sus definiciones se parecieran, sino de que sus categorías se parecían. Así, Mac Lane buscó establecer los axiomas para una definición común aunque sin éxito, que luego fue sucedido por Buchsbaum también sin éxito, hasta la llegada de Grothendieck en 1957 en la que impuso un estándar con su noción de *categoría abeliana*, lo que impuso una revolución en el álgebra homológica.

A finales de los años cincuenta, Kan introdujo la pieza restante para el panorama de categorías puras: la adjunción. En los años sesenta, el texto de Freyd [**0**] se convirtió en un estándar y ordenó todas estas ideas, tratando de enfatizar todos los micro-hitos de la naciente disciplina. Grothendieck volvió a agitar las esferas de las matemáticas con la noción del *topos*, señalando que generalizaba la idea del espacio topológico. ...

Para la teoría de categorías, de haces y de topoi me basé en los artículos [**0**] y [**0**].

Año	**Suceso**	**Fuente**
1945	Definición de categoría (§**??**).	Samuel Eilenberg y Saunders Mac Lane. *General Theory of Natural Equivalences.*
1956	Definición de adjunción.	Daniel Kan. *Adjoint Functors.*
1957	Definición de categoría abeliana. Aplicaciones al álgebra homológica.	Alexander Grothendieck. *Sur quelques points d'algèbre homologique.*

Año	**Suceso**	**Fuente**
1960	Teorema de Watts-Eilenberg.	Charles E. Watts. *Intrinsic characterizations of some additive functors.* Samuel Eilenberg. *Abstract description of some basic functor.*
1964	Teorema y teorema especial del funtor adjunto.	Peter Freyd. *Abelian categories.*

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 las matemáticas modernas. 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).

Éste capítulo cubre bastante, en general todo aquello que suele constituir la teoría de conjuntos necesaria para casi todo libro, exceptuando por la cardinalidad que se estudia en el capítulo 3. El propósito que buscamos es una mezcla entre los fundamentos lógicos de la matemática (lenguajes formales y teorías axiomáticas de conjuntos), así como los fundamentos prácticos de ella (axiomas de Peano y construcción de $\mathbb{Z}$ y $\mathbb{Q}$). Además se aprovecha de dar una sección introductoria al lenguaje de la teoría de categorías que es universalmente empleado a lo largo de casi todas las ramas de las matemáticas.

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 $p, q, r, \dots$

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 *conectores 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 $\implies$, léase «si ... entonces ...») es aquel que es falso cuando el primero (llamado condición) es verdadero y el segundo (llamado deducción) es falso.

p	q	$p \implies q$
V	V	V
F	V	F
V	F	V
F	F	V

Coimplicador (denotado $\iff$, léase «si y sólo si») es aquel que es verdadero cuando ambas proposiciones comparten valor de verdad.

p	q	$p \iff q$
V	V	V
F	V	F
V	F	F
F	F	V

Se evita decir que éstos son «todos los conectores» porque teóricamente puedes construir infinitos conectores lógicos a partir de éstos.

Definición 1.2 (Tautología): Se dice que una proposición compuesta P que depende de otras $p, q, \dots$ es una *tautología* si es siempre cierta, independiente de los valores de verdad de $p, q, \dots$. 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. $\neg(p \lor q) \equiv \neg p \land \neg q$ (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. $p \iff q \equiv (p \implies q) \land (q \implies p)$ (caracterización del coimplicador).
17. $p \lor q \equiv \neg p \implies q$ (caracterización del disyuntor).
18. $p \implies q \equiv (p \land \neg q) \implies F$ (demostración por contradicción).

Una variable, usualmente denotada como x, y, z, etc.; es un símbolo que potencialmente refiere a un objeto del universo. Por ejemplo la conmutatividad de la suma usualmente se denota mediante la fórmula «$x + y = y + x$» que se traduce como que la expresión vale para cualquier x e y, sin importar los valores escogidos. Nótese sin embargo que una expresión como «$x + 2 = 4$» **no** es una proposición debido a que no hay una interpretación fija (es decir, un valor para x). Así tales expresiones se convierten en *predicados*, y para que tengan sentido se pueden emplear alguno de los tres cuantificadores:

Cuantificador universal (denotado $\forall$, léase «para todo») es aquel que es verdadero cuando $\phi(x)$ lo es para toda valoración de x.

Cuantificador existencial (denotado $\exists$, léase «existe») es aquel que es verdadero cuando $\phi(x)$ lo es para alguna valoración de x.

Cuantificador existencial con marca de unicidad (denotado $\exists!$, léase «existe un único») es aquel que es verdadero cuando $\phi(x)$ lo es para una única valoración de x.

Si $\phi(x)$ es una valoración, entonces $\forall x\ \phi(x)$ se lee «Para todo x se cumple $\phi(x)$». La ley de De Morgan da resultado a la siguiente tautología:

$$\neg(\forall x\ \phi(x)) \iff \exists x\ \neg\phi(x).$$

En general cuando uno escribe una fórmula con variables libres (que no estén ligadas por un cuantificador) se implicita un «para todo...». Los profesores emplean expresiones como «$x + 2 = 4$» para encontrar todas las valoraciones que hacen que la fórmula sea verdadera.

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 español como con lenguaje lógico.

El lenguaje de la teoría de conjuntos posee un relator $\in$ tal que $x \in y$ se lee «x pertenece o es un elemento de y».

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 más trivial que suene 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 fuese que sí, entonces es porque satisface la proposición $\phi(x) := x \notin x$, es decir, $R \notin R$ lo que es absurdo. Si la respuesta fuese que no, entonces como $R \notin R$ satisface 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.

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

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 $\mathcal{F}$.

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

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 $x_1, x_2, \dots, x_n$ existe un único conjunto y cuyos elementos son solamente los x_i al que denotamos:

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

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 $\{x_1, x_2, \dots, x_n\}$. La unicidad, como de costumbre, se deduce del axioma de extensionalidad. $\square$

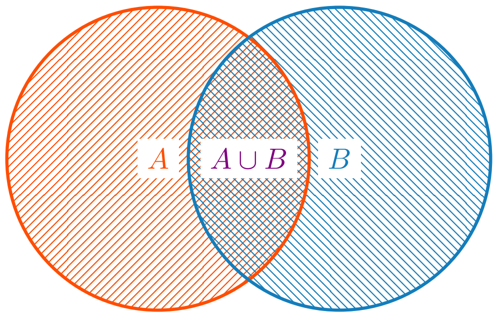


Figura 1.1. Diagrama de Venn de la unión.

§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.

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 $\bigcup \mathcal{A} \subseteq B$.

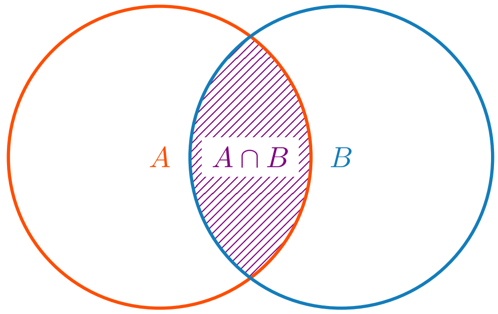


Figura 1.2. Diagrama de Venn de la intersección.

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.

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 $A \subseteq \bigcap \mathcal{B}$.

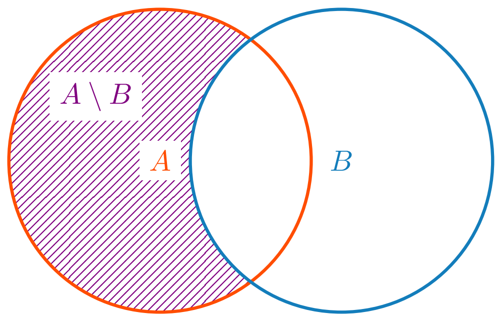


Figura 1.3. Diagrama de Venn de la diferencia.

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, vale decir

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

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).
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).

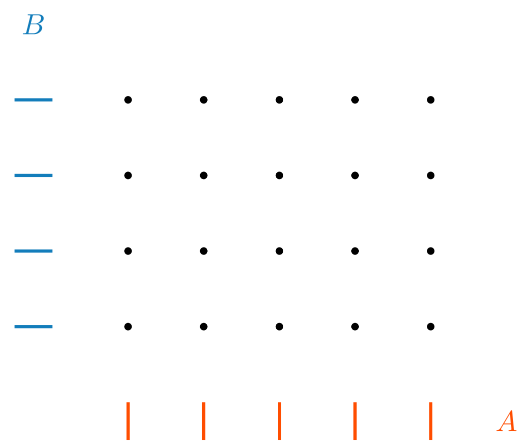


Figura 1.4. Diagrama del producto cartesiano.

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

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

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

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

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

Se define la imagen de un conjunto X general como

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

Se define la *composición* de dos relaciones como

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

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

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

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

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

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

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

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 $f \circ f^{-1} = \mathrm{Id}_A$ y $f^{-1} \circ f = \mathrm{Id}_B$.

Nótese que siempre existe f^{-1} como relación, el teorema anterior señala que si f es biyección, entonces f^{-1} es una función. En éste contexto es práctico definir lo siguiente:

Definición 1.27: Sea $f : A \to B$, dado $b \in B$ se dice que $f^{-1}[\{b\}]$ es la *fibra* según f de b.

Corolario 1.28: Una función $f : A \to B$ es una biyección syss todas las fibras son singulares.

Proposición 1.29: 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. 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 ι, 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 $A_1, \dots, A_n$ son conjuntos no vacíos y $(x_1, \dots, x_n) \in A_1 \times \cdots \times A_n$, 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 $\pi_i(x_1, \dots, x_n) = x_i$.

Proposición 1.30: 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:

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

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 1.31: 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 ϕ 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.

1.5 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 1.32 (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 1.33: 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 1.34 – *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 un conjunto P de todos los n's tales que si h, h' son aproximaciones definidas en n, entonces se cumpla que $h(n) = h'(n)$. 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. □

Teorema 1.35: Sean $(N, s, 0)$ y $(N', s', 0')$ sistemas de Peano. Entonces siempre existe una función $f : N \to N'$ biyectiva tal que $f(0) = 0'$.

PISTA: Basta construir tal función por recursión. □

Más adelante, en §?? veremos que éste enunciado se traduce en que de alguna manera todos los sistemas de Peano son el mismo, pero con distintos nombres.

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

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

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 1.37: 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 1.38: Para todo $n \in \mathbb{N}$ se cumple que $s(n)=n+1$.

Teorema 1.39: 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 1.40: Para todo $n \in \mathbb{N}$ se cumple

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

Teorema 1.41: Para todo $n, m \in \mathbb{N}$ se cumple que $n+m=m+n$ (conmutatividad).

Definición 1.42: 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 1.43: 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).

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

Teorema 1.44: 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 1.45: 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 1.46 – *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 1.47: 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 1.48: 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 1.49 – *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 1.50: 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 1.51: Fijada una categoría, la relación dada por "éstos objetos son isomorfos" corresponde a una relación de equivalencia.

Teorema 1.52: 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 1.53: 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 1.54: 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 1.55: 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 1.56: 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 1.57: 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. $\dfrac{af+be}{bf} = \dfrac{cf+de}{df}$.
2. $\dfrac{ae}{bf} = \dfrac{ce}{df}$.
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 1.58: 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 1.59: 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.

§1.5.4 Particiones y relaciones de equivalencia.

Definición 1.60 – *Partición*: Dado un conjunto X, una familia $\mathcal{F}$ de subconjuntos de X es un *cubrimiento* de X si

$$\bigcup \mathcal{F} = X.$$

Si, además, $\mathcal{F}$ es un cubrimiento de X cuyos elementos son disjuntos dos a dos,[a] entonces $\mathcal{F}$ se dice una *partición* de X.

[a] Es decir, que si $A, B \in \mathcal{F}$ son distintos, entonces A y B son disjuntos.

Ejemplos. Son particiones:

1. El conjunto de números pares y el de los impares de $\mathbb{N}$ o de $\mathbb{Z}$. Esto quiere decir: todo número natural o entero es o par o impar, nunca ambos.

2. $\{X\}$ es una partición de X.

3. Si X tiene al menos dos elementos, entonces si $x \in X$ se cumple que $\{\{x\}, X_{\neq x}\}$ es una partición de X.

Proposición 1.61: Sea $f : A \to B$, entonces las fibras son un cubrimiento de A. Es más, f es suprayectiva syss las fibras son una partición de A.

DEMOSTRACIÓN: Notar ésto es trivial, ya que lo único que puede suceder es que un elemento del codominio no tenga preimagen en cuyo caso su fibra sea vacía, ésto se resuelve exigiendo que f sea suprayectiva. □

Teorema 1.62: Sea $\sim$ una relación reflexiva sobre A, y defínase

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

entonces $\mathcal{F} := \{[a] : a \in A\}$ es una partición de A syss $\sim$ es una relación de equivalencia.

DEMOSTRACIÓN: $\Longleftarrow$. Es trivial, puesto que los conjuntos $[a]$ son las clases de equivalencia y hemos visto que: Todo $a \in A$ cumple que $a \in [a]$, de modo que son cubrimiento. Y que para todo $a, b \in A$ se cumplía uno solo: o $[a] = [b]$ o $[a] \cap [b] = \varnothing$, es decir, las clases de equivalencia son disjuntas dos a dos y luego son partición.

$\Longrightarrow$. En primer lugar son cubrimiento y no poseen clases vacías por ser relación reflexiva, veamos las otras condiciones:

i) <u>$\sim$ es simétrica:</u> Supongamos que $a \sim b$, luego $b \in [a]$ (por definición) y $b \in [b]$ (por ser reflexiva). Como son partición, entonces $[a] = [b]$ y $a \in [b]$, es decir, $b \sim a$.

ii) <u>$\sim$ es transitiva:</u> Sea $a \sim b$ y $b \sim c$. Por el razonamiento anterior $[a] = [b]$ y $[b] = [c]$, luego $c \in [c] = [a]$, por lo que $a \sim c$. $\square$

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, de modo que si existen les denotamos $\min B$, $\max B$, $\inf B$ y $\sup B$ resp.
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. $\square$

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:

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

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 $O_{<}(x)$.

Pista: 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, ahora probaremos que f es un isomorfismo entre segmentos iniciales:

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

2. $\operatorname{Dom} f = A$ 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 $x_0 \notin \operatorname{Dom} f$.

Finalmente, 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 α 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 α está bien ordenado por $\in$.

Denotamos por Ω_{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 α es un ordinal y $\beta \in \alpha$, entonces por transitividad, $\beta \subseteq \alpha$ luego es inmediato que β 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 α 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 α^+ es transitivo. Ahora basta ver que todo subconjunto x no vacío de α^+ no vacío posee $\in$-minimal: si $x = \{\alpha\}$, entonces es claro, de lo contrario $x \setminus \{\alpha\}$ es no vacío, luego es subconjunto de α 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 α está $\in$-bien fundado.
También es claro que α^+ es $\in$-conexo. □

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

DEMOSTRACIÓN: Como $\beta \setminus \alpha \subset \beta$ entonces posee un $\in$-mínimo γ. Se cumple que $\gamma \subseteq \alpha$ pues de lo contrario $\delta \in \gamma \setminus \alpha$ estaría en $\beta \setminus \alpha$ y sería menor que γ. Probaremos que $\alpha \subseteq \gamma$: Si $\delta \in \alpha$, entonces como $\delta, \gamma \in \beta$ y β 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 α, β son ordinales entonces $\alpha \cap \beta$ es un ordinal.

DEMOSTRACIÓN: Sea $\gamma := \alpha \cap \beta$, como $\gamma \subseteq \alpha$ entonces γ es $\in$-bien ordenado. Aún basta probar que γ 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 $\alpha, \beta \in \Omega_{\mathrm{Ord}}$ entonces $\alpha \in \beta, \alpha = \beta$ o $\beta \in \alpha$. En consecuente, $\alpha \subseteq \beta$ o $\beta \subseteq \alpha$

DEMOSTRACIÓN: Sea $\gamma := \alpha \cap \beta \in \Omega_{\mathrm{Ord}}$, 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*: Ω_{Ord} es un ordinal, por ende, es una clase propia.

DEMOSTRACIÓN: Ya hemos probado que Ω_{Ord} es transitivo y $\in$-conexo, aún falta ver que es bien fundado: Sea $X \subseteq \Omega_{\mathrm{Ord}}$ una clase no vacía y sea $\alpha \in X$ cualquiera. Si α 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 β en $\alpha \cap X$. Y $\varnothing = \beta \cap \alpha \cap X = \beta \cap X$ pues $\beta \subseteq \alpha$. □

La conclusión en ZF es que Ω_{Ord} no existe.

Corolario 2.24: Se cumple:

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

4. Para todo $\alpha \in \Omega_{\mathrm{Ord}}$, 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: Los números ordinales α se clasifican en:

Nulo Si $\alpha = 0$.

Sucesor Si $\alpha = \beta^+$ para algún $\beta \in \Omega_{\mathrm{Ord}}$.

Límite Si no es ni nulo, ni sucesor.

Finito Si para todo $\beta \leq \alpha$ se cumple que β es sucesor.

Infinito Si no es finito, es decir, si es mayor o igual a algún ordinal límite.

Se denota ω a la clase de ordinales finitos.

Corolario 2.26: Se cumple que:

1. ω es el primer ordinal infinito y también el primer ordinal límite.
2. α es infinito syss $\alpha \geq \omega$.

Teorema 2.27: Todo conjunto bien ordenado es isomorfo a un único ordinal.

Demostración: (**Nota:** Intente demostrarlo por sí solo.)
Sea A un conjunto bien ordenado y Ω_{Ord} que sabemos que está bien ordenado también. Luego alguno es isomorfo a un segmento inicial del otro, pero $A \not\cong \Omega_{\mathrm{Ord}}$ pues existiría una función $f : A \to \Omega_{\mathrm{Ord}}$ que es suprayectiva, pero entonces por axioma de reemplazo Ω_{Ord} sería un conjunto; un razonamiento análogo se aplica si Ω_{Ord} fuera isomorfo a un segmento inicial de A. Sólo nos queda que A es isomorfo a un segmento inicial de Ω_{Ord} que son los ordinales. □

Definición 2.28: Si $(A, \leq)$ es un conjunto bien ordenado, denotamos por $\operatorname{ord}(A, \leq)$ al único ordinal al que le es isomorfo.

Teorema 2.29 – *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 $C = \Omega_{\text{Ord}}$.

Pista: Aplicar el buen orden de los ordinales. □

Teorema 2.30 – *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 α-aproximación si cumple con la última ecuación pero tiene dominio α. Por el buen ordenamiento de los ordinales se puede probar con facilidad que, si existen, las α-aproximaciones y la función deseada misma son únicas.

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

Definición 2.31: Una función $f : \alpha \to X$ cuyo dominio es un ordinal se dice una *sucesión* de largo α. Decimos que una α-sucesión es discretamente creciente si para todo β tal que $\beta^+ < \alpha$ se cumple que $f(\beta) < f(\beta^+)$. Si f es una sucesión discretamente 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 (discretamente) creciente es *continua* si para todo λ límite se cumple que $f(\lambda) = \lim_{\delta \to \lambda} f(\delta)$.

Una sucesión continua de codominio Ω_{Ord} que es discretamente creciente se dice una *función normal*.

Corolario 2.32: Una función estrictamente creciente es discretamente creciente.

Luego también veremos el converso, pero de momento es útil tenerlos como conceptos separados.

Teorema 2.33: Si $f : \alpha \to \Omega_{\text{Ord}}$ es normal, entonces para todo $\beta < \alpha$ se cumple que $\beta \leq f(\beta)$.

Demostración: Ésta es una aplicación por inducción transfinita:

1. Caso base: Trivial pues $f(0) \in \Omega_{\text{Ord}}$ y $0 = \min \Omega_{\text{Ord}}$, ergo $0 \leq f(0)$.
2. Caso sucesor: Sea β tal que $\beta^+ < \alpha$ y $\beta \leq f(\beta)$, luego como $f(\beta) < f(\beta^+)$ se cumple $\beta^+ \leq f(\beta)^+ \leq f(\beta^+)$.
3. Caso límite: Sea $\lambda < \alpha$ límite. Luego, por continuidad, $f(\lambda) = \sup\{f(\delta) : \delta < \lambda\}$. Es decir, para todo $\delta < \lambda$ se cumple que $\delta \leq f(\delta) \leq f(\lambda)$, es decir, $f(\lambda)$ es cota superior de $O_<(\lambda)$, y como λ es supremo de dicho conjunto se tiene que $\lambda \leq f(\lambda)$. □

Teorema 2.34: 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

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

Si g es estrictamente creciente, entonces f es normal.

2.3 Aritmética ordinal

Definición 2.35: Dado un ordinal α se definen las operaciones como las únicas sucesiones continuas tal que

$$\alpha + 0 := \alpha, \qquad \alpha + (\beta^+) := (\alpha + \beta)^+,$$

$$\alpha \cdot 0 := 0, \qquad \alpha \cdot (\beta^+) := \alpha \cdot \beta + \alpha,$$
$$\alpha^0 := 1, \qquad \alpha^{\beta^+} := \alpha^\beta \cdot \alpha.$$

Teorema 2.36: Para todo $\alpha, \beta, \gamma \in \Omega_{\text{Ord}}$ se cumple:

1. $\alpha^+ = \alpha + 1$.
2. $0 + \alpha = \alpha + 0 = \alpha$ (elemento neutro).
3. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ (asociatividad).
4. Las funciones de la forma $f(\alpha) = \beta + \alpha$ son normales.
5. $\alpha < \beta$ syss existe $\gamma > 0$ tal que $\beta = \alpha + \gamma$.
6. Una función normal es estrictamente creciente, en consecuencia, $\alpha < \beta$ syss $\gamma + \alpha < \gamma + \beta$.
7. $\gamma + \alpha = \gamma + \beta$ syss $\alpha = \beta$.
8. Si $\alpha \leq \beta$, entonces $\alpha + \gamma \leq \beta + \gamma$.

Demostración: La mayoría se demuestran por inducción transfinita. Vamos a ver algunas:

3. Lo haremos por inducción transfinita sobre γ:

   i) Caso base:

   $$\alpha + (\beta + 0) = \alpha + \beta = (\alpha + \beta) + 0.$$

   ii) Caso sucesor:

   $$\begin{aligned} \alpha + (\beta + (\gamma + 1)) &= \alpha + ((\beta + \gamma) + 1) = (\alpha + (\beta + \gamma)) + 1 \\ &= ((\alpha + \beta) + \gamma) + 1 = (\alpha + \beta) + (\gamma + 1). \end{aligned}$$

   iii) Caso límite:

   $$\begin{aligned} \alpha + (\beta + \lambda) &= \alpha + (\lim_{\delta \to \lambda} \beta + \delta) = \lim_{\delta \to \lambda} \alpha + (\beta + \delta) \\ &= \lim_{\delta \to \lambda} (\alpha + \beta) + \delta = (\alpha + \beta) + \lambda. \end{aligned}$$

4. Es discretamente creciente y continua por construcción.

5. Ambas implicancias son por inducción transfinita, recomendamos al lector intentarlo solo:

   $\Longrightarrow$. Vamos a construir las siguientes clases de ordinales:

$$B := \{\alpha + \gamma : 0 \neq \gamma \in \Omega_{\text{Ord}}\}, \quad C := O_{\leq}(\alpha) \cup B.$$

   Queremos ver que $C = \Omega_{\text{Ord}}$, en cuyo caso, claramente $\beta \in B$.
   Supongamos que $C \neq \Omega_{\text{Ord}}$, entonces por buen orden existe el mínimo $\lambda \notin C$. Claramente $\lambda > \alpha \geq 0$ y no puede ser un ordinal sucesor, pues si $\lambda = \delta + 1$, como $\delta = \alpha + \gamma$, entonces $\alpha + (\gamma + 1) = \lambda \in C$.
   Luego λ debe ser un ordinal límite, así que definamos $S := \{\delta : \alpha + \delta < \lambda\}$, claramente S es no vacío y una cota superior de S es el mismo λ, pues $\alpha + \lambda \geq \lambda$ por ser normal, ergo S posee un supremo γ. γ no es nulo, ni tampoco sucesor, porque si lo fuese entonces $\gamma = \epsilon + 1$ y $\alpha + \epsilon < \lambda \leq \alpha + \epsilon + 1$, ergo $\lambda = \alpha + \gamma$ lo cuál es contradictorio pues λ no es sucesor. Si γ fuese límite, entonces $\alpha + \gamma := \sup\{\alpha + \delta : \delta < \gamma\}$, entonces claramente $\lambda \geq \alpha + \gamma$, pero $\lambda \not> \alpha + \gamma$, pues entonces $\lambda = \alpha + \gamma + 1$ que es sucesor, en conclusión $\lambda = \alpha + \gamma$.

   $\Longleftarrow$. Sale por inducción sobre $\gamma > 0$.

8. Como $\alpha \leq \beta$, entonces $\beta = \alpha + \delta$ y $\alpha + \gamma \leq \alpha + \delta + \gamma$, es decir, basta probar que $\gamma \leq \delta + \gamma$, pero ésto es verdadero pues $(\delta+)$ es normal. □

Teorema 2.37: Si $f : \alpha \to \Omega_{\text{Ord}}$ es normal y $\lambda < \alpha$ es límite, entonces $f(\lambda)$ también es límite.

Demostración: Sea $\beta < f(\lambda)$, veremos que $\beta + 1 < f(\lambda)$. Luego $\beta < \sup_{\delta < \lambda} f(\delta)$, es decir, existe $\delta_0 < \lambda$ tal que $\beta \leq f(\delta_0)$ por definición de supremo, con lo que $\beta + 1 \leq f(\delta_0) + 1 \leq f(\delta_0 + 1) < f(\lambda)$. □

Teorema 2.38: Para todo $\alpha, \beta, \gamma \in \Omega_{\text{Ord}}$ se cumple:

1. $0 \cdot \alpha = \alpha \cdot 0 = 0$ (aniquilador).
2. $1 \cdot \alpha = \alpha \cdot 1 = \alpha$ (elemento neutro).
3. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ (distributividad por la derecha).
4. $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ (asociatividad).
5. $\alpha < \beta$ y $\gamma > 0$ syss $\gamma \cdot \alpha < \gamma \cdot \beta$, equivalentemente, el producto con $\gamma > 0$ fijo es una función normal.

6. Si $\gamma > 0$, entonces $\gamma \cdot \alpha = \gamma \cdot \beta$ syss $\alpha = \beta$.
7. Si $\alpha \leq \beta$, entonces $\alpha \cdot \gamma \leq \beta \cdot \gamma$.

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

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

de hecho $1 + \alpha = \alpha$ syss $\alpha \geq \omega$. Además

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

Y al igual es generalizable.

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 2.39: 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 2.40: 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 2.41: Si R es una relación sobre A y $B \subseteq A$, entonces:

1. B es R-cerrado syss $B = \operatorname{ct}_R(B)$.
2. $\operatorname{ct}_R(B)$ 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 2.42: 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

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

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

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

Corolario 2.43: Se cumple:

1. No hay $\in$-ciclos, i.e., una sucesión finita $(x_1, \dots, x_n)$ 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 $y := \{x_1, \dots, x_n\}$ 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 2.44 – *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 2.45: Se cumple:

1. Las clases de la forma V_α son conjuntos.
2. Para todo ordinal α 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_α 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 α 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 2.46: Una clase es propia syss contiene elementos de rango arbitrariamente grande.

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

Teorema 2.47: 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 $A \precsim B$ si existe $f : A \to B$

inyectiva, y que $A \lnsim B$ 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 $A \lnsim \mathcal{P}(A)$.

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 $I_n := \{1, 2, \dots, n\}$, 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 $A \precsim B$ y B es finito, entonces A también y $|A| \leq |B|$.
2. Si $A \precsim B$ 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 Cantor-Schröder-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 $A \precsim B$ y $B \precsim A$, 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 $\operatorname{Img}(f \upharpoonright z) = f[z]$ y $\operatorname{Img}(g \upharpoonright B \setminus f[z]) = A \setminus z$ ambas siendo biyectivas, luego

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

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 $\overline{\overline{y}}^{\overline{\overline{x}}} = \overline{\overline{\mathrm{Func}(x, y)}}$.

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_α son conjuntos y claramente para todo conjunto x se cumple que $[x] \subseteq V_{(\mathrm{rang}\, x)+1}$, 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 λ es *inicial* o un *cardinal de von Neumann* si para todo $\delta < \lambda$ se cumple que $\delta \not\approx \lambda$. Dado un ordinal α se denota $|\alpha| := \min\{\beta \in \Omega_{\text{Ord}} : \beta \approx \alpha\}$, es decir, $|\alpha|$ es el único ordinal inicial equipotente a α. Se denota por Ω_{Card} al conjunto de cardinales de von Neumann.

Lema 3.22 (Hartogs): Si x es un conjunto arbitrario existe un ordinal $\kappa < \Omega_{\text{Ord}}$ 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 α es tal que $\alpha \lesssim x$ syss existe $(y, R) \in P$ tal que $\alpha = \operatorname{ord}(y, R)$, luego si $\beta := \sup\{\operatorname{ord}(y, R) + 1 : (y, R) \in P\}$ entonces $\beta \not\lesssim x$ y β 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 α 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 $\aleph : \Omega_{\text{Ord}} \to \Omega_{\text{Ord}}$ 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 denotaremos ω_α 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, ni su producto, ni sus potencias.

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 κ 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 α: El caso inicial es trivial, pues para todo $(n, m) \in \omega^2$ hay finitos puntos menores que él. Sea α, 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 ω_α 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 κ, μ son ordinales iniciales y al menos uno es infinito, entonces

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

En el contexto de cardinales de von Neumann siempre denotamos $|X|$ al cardinal de X, en lugar de $\overline{\overline{X}}$.

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 distintos 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 α tal que $f(\alpha) = \infty$, sea γ 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 β es el mínimo ordinal tal que p_β 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. $\square$

Teorema 3.31: Son equivalentes:

1. **El axioma de elección**.
2. Si $\mathcal{F}$ es una familia de conjuntos no vacíos y disjuntos dos a dos, entonces posee una función de elección.
3. Las retracciones en la categoría Set son las funciones suprayectivas, es decir, toda función suprayectiva $f : A \to B$ posee inversa izquierda $g : B \to A$ tal que $g \circ f = \mathrm{Id}_B$.

Demostración: Claramente (1) $\implies$ (2) $\wedge$ (3).

(3) $\implies$ (2). Notemos que si $\mathcal{F}$ es una familia de conjuntos disjuntos dos a dos, entonces se define la función $f : \bigcup \mathcal{F} \to \mathcal{F}$ tal que $y \in f(y)$. Claramente f es suprayectiva, luego posee inversa izquierda $g : \mathcal{F} \to \bigcup \mathcal{F}$ tal que $g(x) \in f(g(x)) = x$, es decir, g es una función de elección.

(2) $\implies$ (1). Si $\mathcal{F}$ es una familia de conjuntos no vacíos, que no sean todos disjuntos dos a dos, entonces definimos

$$\mathcal{G} := \{x \times \{x\} : x \in \mathcal{F}\}$$

que es una familia de conjuntos no vacíos dos a dos, de modo que posee una función de elección que induce una función de elección sobre $\mathcal{F}$. □

Teorema 3.32: Son equivalentes:

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

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

Lema 3.33: 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

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

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 δ_{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 3.34: 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_δ es bien ordenable para todo $\delta < \lambda$, entonces $\kappa := \bigcup_{\delta<\lambda} |V_\delta|^+$. Como κ es por definición bien ordenable, entonces $\leq^*$ es un buen orden sobre $\mathcal{P}(\kappa)$.

Ahora construiremos unos buenos ordenes $\trianglelefteq_\alpha$ sobre V_α tal que para todo $\beta \leq \alpha$ se cumpla que V_β es un segmento inicial de V_α, lo haremos por recursión transfinita:
El caso base $\trianglelefteq_0 := \varnothing$.
Si $\trianglelefteq_\delta$ está definido, entonces sea φ_δ el isomorfismo de orden entre $(V_\delta, \trianglelefteq_\delta)$ y su tipo de orden α_δ. 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 ν 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 $\gamma := \max\{\operatorname{rang} x, \operatorname{rang} y\} + 1 < \lambda$, luego $x \trianglelefteq_\lambda y$ syss $x \trianglelefteq_\gamma y$. De modo que $\trianglelefteq_\lambda$ es un buen orden sobre V_λ 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 3.35: 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: $\implies$. 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. $\Box$

Teorema 3.36: Si $\mathfrak{p}$ es un cardinal y κ 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 α_x el primer ordinal tal que $(x, \alpha_x) \notin A$, luego $\{(x, \alpha_x) : x \in X\} \subseteq B$ y $\mathfrak{p} \leq \kappa$. $\Box$

Teorema 3.37: 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) $\Longrightarrow$ (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 κ 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 κ, cómo κ posee sucesor cardinal éste ha de ser κ^+ (¿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 3.38: 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 3.39: Se cumple:

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

Proposición (DE) 3.40: 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) 3.41: 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 $\mathbb{N} \precsim X$ y para ver que $X \precsim Y$ 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 $Y \precsim \mathbb{N}$. 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, $X \precsim Y \approx \mathbb{N}$. □

La elección fue necesaria al momento de elegir las biyecciones.

Teorema (AEN) 3.42: Toda clase infinita contiene una subclase numerable (que es, por ende, un conjunto). Equivalentemente, X infinito syss $\mathbb{N} \precsim X$.

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 $[X]^n$. □

§3.3.3 Finitud de Dedekind.

Definición 3.43: Se dice que un conjunto X es *Dedekind-infinito* (o D-infinito para abreviar) si posee un subconjunto propio $Y \subset X$ tal que $X \approx Y$. De lo contrario se dice Dedekind-finito (o D-finito).

Corolario 3.44: Todo conjunto finito es D-finito, y conversamente, todo conjunto D-infinito es infinito.

Pista: Ésto es equivalente al principio del palomar. □

Proposición 3.45: Son equivalentes:

1. X es Dedekind-infinito.
2. $\overline{\overline{X}} = \overline{\overline{X}} + 1$.

3. $\aleph_0 \leq \overline{\overline{X}}$.

Demostración: (3) $\implies$ (2). Sea $f : \mathbb{N} \to X$ inyectiva. Sea $\infty \notin X$, de modo que $\overline{\overline{X}} + 1 = \overline{\overline{X \cup \{\infty\}}}$. Luego definamos $g : X \to X \cup \{\infty\}$ así:

$$g(x) := \begin{cases} \infty, & x = f(0) \\ f(n), & x = f(n+1) \\ x, & x \notin \operatorname{Img} f \end{cases}$$

que resulta ser una biyección.

(2) $\implies$ (1). Sea $f : X \to X \cup \{\infty\}$ biyectiva. Luego $f^{-1} : X \cup \{\infty\} \to X$ también lo es, y en particular, $f^{-1} \restriction X$ es una función inyectiva a un subconjunto propio de X.

(1) $\implies$ (3). Sea $f : X \to X$ inyectiva pero no suprayectiva, de modo que existe un $y \in X \setminus \operatorname{Img} f$. Luego definamos $g : \mathbb{N} \to X$ por recursión:

$$g(0) = y, \qquad g(n+1) = f(g(n)),$$

lo que resulta ser inyectiva (¿por qué?). □

Corolario 3.46: Son equivalentes:

1. Todo conjunto es D-finito syss es finito.
2. Todo cardinal es $\leq$-comparable a $\aleph_0$, es decir, si $\mathfrak{p}$ es cardinal entonces $\aleph_0 \leq \mathfrak{p}$ o $\mathfrak{p} \leq \aleph_0$.

Lema 3.47: Son equivalentes:

1. Existe $f : X \to \mathbb{N}$ suprayectiva.
2. $\mathcal{P}(X)$ es D-infinito.

Demostración: (1) $\implies$ (2). Sea $f : X \to \mathbb{N}$ suprayectiva, entonces $g : \mathbb{N} \to \mathcal{P}(X)$ definida por $g(n) := f^{-1}[\{n\}]$ es una inyección.

(2) $\implies$ (1). Sea $f : \mathbb{N} \to \mathcal{P}(X)$ inyectiva, queremos construir $g : \mathbb{N} \to \mathcal{P}(X)$ inyectiva y cuyas imágenes sean no vacías y disjuntas dos a dos, para ello también definiremos en simultáneo la función $G(n) := \bigcup_{m<n} g(m)$ pues exigir que los $g(n)$ sean disjuntos dos a dos implica que $G(n)$ y $g(n)$ lo sean para todo $n \in \mathbb{N}$: Supongamos que para todo $m < n$ los $g(m)$s están definidos de modo que el conjunto $\{f(k) \setminus G(n) : k \geq n\}$ sea infinito, luego definimos

$$n^* := \min\{k : k \geq n \wedge f(k) \setminus G(n) \neq \varnothing \neq (X \setminus f(k)) \setminus G(n)\}$$

y luego definimos $g(n) := f(n^*) \setminus G(n)$ si $\{f(k) \setminus (f(n^*) \cup G(n)) : k \geq n\}$ es infinito o $g(n) := X \setminus (f(n^*) \setminus G(n))$ de lo contrario.
Finalmente definimos $h : X \to \mathbb{N}$ así

$$h(x) := \begin{cases} n, & x \in g(n) \\ 0, & x \notin \bigcup_{n\in\mathbb{N}} g(n) \end{cases}$$

y es claro que la función es suprayectiva. □

Teorema 3.48: Son equivalentes:

1. Un conjunto es D-finito syss es finito.
2. La unión de D-finitos conjuntos D-finitos es D-finitos.
3. La imagen de conjuntos D-finitos es D-finita.
4. El conjunto potencia de un conjunto D-finito es D-finito.

Más aún, todos son consecuencia del AEN.

Demostración: (1) $\implies$ (2). El enunciado se traduce a ver que la unión finita de finitos es finita, lo que ya vimos en la primera sección.

(2) $\implies$ (3). Sea $f : X \to Y$ suprayectiva con X D-finito, entonces $Y = \bigcup \big\{\{f(x)\} : x \in X\big\}$ donde el conjunto de la derecha es D-finito y sus elementos son finitos (y por tanto D-finitos).

(3) $\implies$ (4). Lo haremos por contrarrecíproca: Si $\mathcal{P}(X)$ es D-infinito, por el lema existe $f : X \to \mathbb{N}$ suprayectiva, como $\mathbb{N}$ es D-infinito, entonces por (3) X también.

(4) $\implies$ (1). Basta probar que todo conjunto infinito es D-infinito. Sea X un conjunto infinito, entonces definamos $f : \mathbb{N} \to \mathcal{PP}(X)$ así $f(n) := [X]^n$ y resulta ser inyectiva, de modo que $\mathcal{PP}(X)$ es D-infinito, luego por (4), $\mathcal{P}(X)$ también y X también. □

En particular la proposición: "Todo conjunto infinito es D-infinito" es una forma débil del AE, más débil que AEN.

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 3.49: 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 3.50: 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 3.51: 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 3.52: Se cumplen:

1. $\sum_{i\in I} \kappa = |I|\,\kappa$ y $\prod_{i\in I} \kappa = \kappa^{|I|}$.
2. $\nu \sum_{i\in i} \kappa_i = \sum_{i\in i} \nu\kappa_i$ y $\prod_{i\in I} \kappa_i^\nu = \left(\prod_{i\in I} \kappa_i\right)^\nu$.
3. Si para todo $i \in I$ se cumple que $\kappa_i \leq \mu_i$, entonces $\sum_{i\in I} \kappa_i \leq \sum_{i\in I} \mu_i$ y $\prod_{i\in I} \kappa_i \leq \prod_{i\in I} \mu_i$.
4. $\prod_{i\in I} \kappa^{\mu_i} = \kappa^{\sum_{i\in I} \mu_i}$.
5. Si I_j con $j \in J$ es partición estricta de I, entonces
$$\sum_{i\in I} \kappa_i = \sum_{j\in J} \sum_{i\in I_j} \kappa_i, \quad \prod_{i\in I} \kappa_i = \prod_{j\in J} \prod_{i\in I_j} \kappa_i.$$
6. Si $(\kappa_\alpha)_{\alpha<\mu}$ es una sucesión creciente de cardinales no nulos tal que μ es infinito o algún κ_α lo es, entonces
$$\sum_{\alpha<\mu} \kappa_\alpha = \mu \lim_{\alpha\to\mu} \kappa_\alpha, \quad \prod_{\alpha<\mu} \kappa_\alpha = \left(\lim_{\alpha\to\mu} \kappa_\alpha\right)^\mu.$$

Demostración: Sólo probaremos la última: Llamemos $\kappa := \lim_{\alpha\to\mu}\kappa_\alpha$. En primer lugar como $\kappa_\alpha \geq 1$ se tiene que $S := \sum_{\alpha<\mu}\kappa_\alpha \geq \mu$. Y además como $\bigcup_{\alpha<\mu}\kappa_\alpha = \kappa \leq S$, se concluye que $S \geq \mu\kappa$. Así mismo, como $\kappa_\alpha \geq \kappa$, entonces $S \leq \sum_{\alpha<\mu}\kappa = \mu\kappa$, comprobando la igualdad.

Para el caso del producto, es fácil ver que $P := \prod_{\alpha<\mu}\kappa_\alpha \leq \kappa^\mu$. Supongamos que μ es infinito (pues el caso finito es trivial), luego existe $f : \mu\times\mu \to \mu$ biyectiva y podemos particionar el conjunto en $I_\alpha := f[\mu\times\{\alpha\}]$, de modo que $\mu = \bigcup_{\alpha<\mu} I_\alpha$. Además todos los I_α deben de ser no acotados, pues de lo contrario tendrían cardinal estrictamente menor que μ. Luego $\lim_{\beta\in I_\alpha}\kappa_\beta = \kappa$ porque I_α no está acotado y es claro que $\kappa_\beta \leq \prod_{\beta\in I_\alpha}\kappa_\beta$, de modo que $\lim_{\beta\in I_\alpha}\kappa_\beta = \kappa \leq \prod_{\beta\in I_\alpha}\kappa_\beta$. En consecuente:

$$P = \prod_{\alpha<\mu}\prod_{\beta\in I_\alpha}\kappa_\beta \geq \prod_{\alpha<\mu}\lim_{\beta\in I_\alpha}\kappa_\beta = \prod_{\alpha<\mu}\kappa = \kappa^\mu. \qquad \square$$

Lema 3.53: Si $2 \leq \kappa_i$ para todo $i \in I$, entonces $\sum_{i\in I}\kappa_i \leq \prod_{i\in I}\kappa_i$.

Demostración: Como sabemos, $\sum_{i\in I}\kappa_i \leq |I|\sup_{i\in I}\kappa_i$. Nótese que $\prod_{i\in I}\kappa_i \geq \prod_{i\in I} 2 = 2^{|I|} \geq |I|$. Y $\kappa_i \leq \prod_{i\in I}\kappa_i$ para todo $i \in I$, ergo, $\sup_{i\in I}\kappa_i \leq \prod_{i\in I}\kappa_i$, y por ende se cumple el enunciado. $\square$

Teorema 3.54 – *Teorema de König*: Si $\kappa_i < \mu_i$ para todo $i \in I$, entonces

$$\sum_{i\in I}\kappa_i < \prod_{i\in I}\mu_i.$$

Demostración: Si $I = \varnothing$, entonces $0 < 1$. Si no, entonces definamos $I' := \{i \in I : \kappa_i \geq 1\}$, con lo que $\mu_i \geq 2$ para todo $i \in I'$, ergo

$$\sum_{i\in I}\kappa_i = \sum_{i\in I'}\kappa_i \leq \prod_{i\in I'}\mu_i \leq \prod_{i\in I}\mu_i.$$

Prosigamos por contradicción: si los cardinales fuesen iguales, entonces existiría $f : \coprod_{i\in I}\kappa_i \to \prod_{i\in I}\mu_i$ que fuese biyectiva que induce a $f_i : \kappa_i \to \mu_i$ definida por $f_i(\alpha) = \pi_i(f(\alpha, i))$. Como $\kappa_i < \mu_i$, entonces f_i no es suprayectiva y existe $\alpha_i \in \mu_i \setminus \operatorname{Img} f_i$, y mediante AE definimos $\boldsymbol{\alpha} := (\alpha_i)_{i\in I} \in \prod_{i\in I}\mu_i$. Sea $(\beta, j) := f^{-1}(\boldsymbol{\alpha})$, luego $\beta \in \kappa_j$, pero $f_j(\beta) = \pi_j[f(\beta, j)] = \alpha_j \notin f_j[\kappa_j]$, contradicción. $\square$

Nótese que por la naturaleza del capítulo, el teorema de König depende del AE. El teorema de Cantor que dice que $\kappa < 2^\kappa$ es un corolario del teorema de König.

Una aplicación breve y útil de la aritmética cardinal:

Teorema 3.55: Sea $(A, \leq)$ un conjunto linealmente ordenado tal que para todo $a \in A$ se cumple que $|O_{\leq}(a)| < \kappa$, entonces $|A| \leq \kappa$.

DEMOSTRACIÓN: Primero nótese que $\hbar(A) \leq \kappa$, pues de lo contrario, $\kappa < \hbar(A)$ y existe una inyección $\kappa \to A$. ... Empleando elección construyamos una sucesión $x_{-} : \mu \to A$ por recursión transfinita que es estrictamente creciente y no acotada con $\mu \leq \hbar(A)$, la cual existe pues sabemos que $|\hbar(A)| \not\leq |A|$. □

3.5 Cofinalidad

Definición 3.56 – *Cofinalidad*: Sea $\lambda \in \Omega_{\mathrm{Ord}}$ límite, se dice que una sucesión $f : \alpha \to \lambda$ es cofinal si $f[\alpha]$ no está acotado en λ. se define $\operatorname{cf} \lambda$ como el mínimo ordinal α tal que existe una α-sucesión cofinal.

Se dice que un ordinal es *regular* si $\lambda = \operatorname{cf} \lambda$, de lo contrario se dice que es *singular*.

Proposición 3.57: Se cumplen las siguientes para todo ordinal límite λ:

1. $\omega \leq \operatorname{cf} \lambda \leq \lambda$.
2. Existe $f : \operatorname{cf} \lambda \to \lambda$ cofinal y normal.
3. $\operatorname{cf} \lambda = \operatorname{cf} |\lambda|$.
4. $\operatorname{cf}(\operatorname{cf} \lambda) = \operatorname{cf} \lambda$, en consecuencia, $\operatorname{cf} \lambda$ es un cardinal regular.
5. $\operatorname{cf} \lambda$ es el mínimo cardinal tal que existe $X \subseteq \lambda$ de tamaño $\operatorname{cf} \lambda$ tal que $\sup X = \lambda$.

DEMOSTRACIÓN: Casí todas son inmediatas, pero veamos la 2: Sea $g : \operatorname{cf} \lambda \to \lambda$ una función cofinal cualquiera, construimos f normal por recursión donde $f(0) := g(0)$ y $f(\alpha + 1) := \max\{g(\alpha), f(\alpha) + 1\}$. □

Lema 3.58: Sean $f : \alpha \to \beta$ y $g : \beta \to \lambda$ cofinales, con g creciente; entonces $f \circ g : \alpha \to \lambda$ es cofinal.

DEMOSTRACIÓN: Sea $\gamma < \lambda$. Como g es cofinal, existe $\delta < \beta$ tal que $g(\delta) \geq \gamma$. Como f es cofinal, existe $\eta < \alpha$ tal que $f(\eta) \geq \delta$, y como g es creciente se cumple que

$$(f \circ g)(\eta) = g(f(\eta)) \geq g(\delta) \geq \gamma. \qquad \square$$

Teorema 3.59: Si $f : \lambda \to \eta$ es cofinal y creciente, entonces $\operatorname{cf} \lambda = \operatorname{cf} \eta$.

Demostración: Por el lema anterior si $g : \operatorname{cf} \lambda \to \lambda$ es cofinal, entonces $g \circ f : \operatorname{cf} \lambda \to \eta$ es cofinal y $\operatorname{cf} \eta \leq \operatorname{cf} \lambda$.

Sea $h : \operatorname{cf} \eta \to \eta$ cofinal, luego queremos construir $r : \operatorname{cf} \eta \to \lambda$ cofinal, y lo hacemos así: $r(\alpha) := \min\{\beta < \lambda : h(\alpha) \leq f(\beta)\}$ que está bien definido por cofinalidad de f. Vamos a probar que r es cofinal: Sea $\gamma < \lambda$, entonces $f(\gamma) < \eta$, luego por cofinalidad de h existe $\delta < \operatorname{cf} \eta$ tal que $f(\gamma) \leq h(\delta)$ y por definición $f(r(\delta)) \geq h(\delta)$, y por monotonía de f se tiene que $\gamma \leq r(\delta)$ lo que completa la prueba.
Finalmente $\operatorname{cf} \lambda \leq \operatorname{cf} \eta$ y por antisimetría se cumple la igualdad. $\square$

Definición 3.60: Se dice que un álef κ es:

Límite Si para todo $\mu < \kappa$ se cumple que $\mu^+ < \kappa$.

Sucesor Si existe $\mu < \kappa$ tal que $\kappa = \mu^+$.

Límite fuerte Si para todo cardinal $\mu < \kappa$ se cumple que $2^\mu < \kappa$.

Corolario 3.61: Un álef de la forma $\aleph_\alpha$ con $\alpha > 0$ es límite o sucesor syss α lo es.

Proposición (AE) 3.62: Sea κ un álef. $\mu := \operatorname{cf} \kappa$ es el mínimo cardinal tal que existe una μ-sucesión de cardinales $(\nu_\alpha)_{\alpha<\mu}$ menores que κ y tales que

$$\sum_{\alpha<\mu} \nu_\alpha = \kappa.$$

Demostración: Debemos probar que dicha sucesión existe y que si μ satisface el enunciado, entonces $\mu \geq \operatorname{cf} \kappa$:

- Sea $f : \operatorname{cf} \kappa \to \kappa$ cofinal. Luego $\nu_\alpha := |f(\alpha)|$ satisface que

$$\kappa = \left| \bigcup_{\alpha<\mu} f(\alpha) \right| \leq \sum_{\alpha<\mu} \nu_\alpha \leq \kappa \cdot \operatorname{cf} \kappa = \kappa.$$

- Supongamos que $\mu < \operatorname{cf}\kappa$ y sea $(\nu_\alpha)_{\alpha<\mu}$ una μ-sucesión de cardinales con $\nu_\alpha < \kappa$, luego $\nu : \mu \to \kappa$ no puede ser cofinal por definición, ergo, tiene supremo λ y
$$\sum_{\alpha<\mu} \nu_\alpha = \mu \cdot \lambda < \kappa. \qquad \square$$

Teorema 3.63: Se cumplen:

1. $\aleph_0$ es regular.
2. Si λ es ordinal límite, entonces $\operatorname{cf}\aleph_\lambda = \operatorname{cf}\lambda$.
3. (AE) Los álefs sucesores son regulares.

Demostración: La 1 es trivial y la 2 sale de ver que $(\aleph_\delta)_{\delta<\lambda}$ es una sucesión no acotada en $\aleph_\lambda$.

La 3 sale de aplicar la proposición anterior, pues si $\mu := \operatorname{cf}\aleph_{\beta+1} \leq \aleph_\beta$, entonces una μ-sucesión de cardinales $\nu_\alpha \leq \aleph_\beta$ y

$$\sum_{\alpha<\mu} \nu_\alpha \leq \sum_{\alpha<\mu} \aleph_\beta = \aleph_\beta \cdot \mu = \aleph_\beta < \aleph_{\beta+1}. \qquad \square$$

§3.5.1 Puntos fijos de funciones normales.

Definición 3.64: Sea $f : \lambda \to \lambda$ una función normal con $\operatorname{cf}\lambda > \aleph_0$, denotamos $f^\omega(\alpha) := \sup_{n<\omega} f^n(\alpha)$.

Teorema 3.65 – *Teorema del punto fijo de funciones normales*: Sea $f : \lambda \to \lambda$ una función normal con $\operatorname{cf}\lambda > \aleph_0$, entonces para todo $\alpha < \lambda$ se cumple que $\beta := f^\omega(\alpha)$ satisface que es el menor punto fijo de f mayor o igual a α.

Demostración: Veamos que cumple todas las propiedades exigidas:

1. Como $f^0(\alpha) = \alpha$, claramente $\beta \geq \alpha$.
2. Primero, por normalidad de f se cumple que $\beta \leq f(\beta)$. Luego veamos que clase de ordinal es β:
   - Si fuese nulo, entonces $\alpha = 0$ y $f(\alpha) \leq \beta = 0$, ergo $\alpha = \beta = 0$ es punto fijo.

- Si $\beta = \gamma + 1$, entonces como $\gamma < \beta$ se tiene que existe un n tal que $\gamma < f^n(\alpha)$, luego, en consecuencia

$$f(\beta) = f(\gamma + 1) \leq f(f^n(\alpha)) = f^{n+1}(\alpha) \leq \beta.$$

- Si β es límite, entonces considerando el que para todo $\delta < \beta$ existe $f^N(\alpha) \geq \delta$ se da que

$$f(\beta) = \lim_{\delta \to \beta} f(\delta) \leq \lim_{n \to \omega} f(f^n(\alpha)) = \lim_{n \to \omega} f^{n+1}(\alpha) = \beta.$$

3. Supongamos que $\gamma \geq \alpha$ es un punto fijo de f. Luego $f(\gamma) = \gamma \geq f(\alpha)$ y una simple inducción concluye que $\gamma \geq f^n(\alpha)$, de modo que γ es cota superior de $\{f^n(\alpha) : n \in \mathbb{N}\}$, pero como β es el supremo, entonces necesariamente $\beta \leq \gamma$. □

Definición 3.66 (Función derivada): Dada $f : \lambda \to \lambda$ normal con $\operatorname{cf} \lambda > \aleph_0$ se define su función derivada $g : \lambda \to \lambda$ como la siguiente función normal por recursión:

$$g(0) := f^\omega(0), \quad g(\alpha + 1) := f^\omega(g(\alpha) + 1),$$

en este caso denotamos $g = f'$.

Corolario 3.67: Dada $f : \lambda \to \lambda$ normal con $\operatorname{cf} \lambda > \aleph_0$, entonces su función derivada es la única función normal cuya imagen corresponde a todos los puntos fijos de f.

Proposición 3.68: Se cumplen las siguientes:

1. $\mathrm{Id}' = \mathrm{Id}$.
2. Para $n > 0$ natural, $(n + \,)' = (\omega + \,)$.
3. $(\omega + \,)' = (\omega^2 + \,)$ y más generalmente $(\omega^n + \,)' = (\omega^{n+1} + \,)$ para $n \in \mathbb{N}$.
4. $(\omega \cdot \,)' = (\omega^\omega \cdot \,)$ y más generalmente $(\omega^{\omega^n} \cdot \,)' = (\omega^{\omega^{n+1}} \cdot \,)$ para $n \in \mathbb{N}$.

Aquí vimos varios ejemplos de funciones normales conocidos, pero no hemos visto la exponencial: Notemos que por el teorema $\omega^{()}$ también tiene puntos fijos, así que denotamos ε_0 al primero de ellos. Dicho de otro modo $\varepsilon_0 = \omega^{\omega^{\omega^{\cdots}}} = \omega^{\varepsilon_0}$.

Interesantemente podemos repetir el proceso y definir $f'' := (f')'$ y generalmente:

$$f^{(0)}(\beta) := f(\beta), \quad f^{(\alpha+1)}(\beta) := (f^{(\alpha)})'(\beta), \quad f^{(\lambda)}(\beta) := \lim_{\delta\to\lambda} f^{(\delta)}(\beta).$$

Y de hecho podemos admitir la notación para funciones que no sean normales, sólo que hay que recordar un par de datos:

- Si f es estrictamente creciente, entonces sus derivadas también, pese a que no sepamos siempre como calcularlas, o que puedan cambiar los dominios, por ejemplo.
- Si f es estrictamente creciente, entonces $f(\alpha) \geq \alpha$ para todo α, y así con sus derivadas.
- Si f es estrictamente creciente, entonces $\alpha \mapsto f^{(\alpha)}(\beta)$ es una función normal, de modo que $f^{(\alpha)}(\beta) \geq \max\{\alpha, \beta\}$. De hecho, lo mejor que puede suceder a un ordinal α es que $f^{(\alpha)}(0) = \alpha$, pues $\min\{f^{(\alpha+1)}(0), f^{(\alpha)}(1)\} > \alpha$.

§3.5.2 Exponenciación cardinal. Aquí hay que tener particular ojo en que la exponenciación cardinal difiere de la exponenciación ordinal. Un ejemplo es que $\aleph_0^{\aleph_0} = 2^{\aleph_0} > \aleph_0$, ergo $2^{\aleph_0} \geq \omega_1$ como ordinales. Mientras que ω^ω es un punto fijo de la $\aleph_0$-sucesión $\omega^n < \omega_1$, de modo que $\omega^\omega < \omega_1 \leq \aleph_0^{\aleph_0}$.

Teorema 3.69: Si $2 \leq \kappa \leq \mu$ y μ es un álef, entonces $\kappa^\mu = 2^\mu$.

Demostración: $2^\mu \leq \kappa^\mu \leq \mu^\mu \leq (2^\mu)^\mu = 2^\mu$. □

Teorema (AE) 3.70 – *Fórmula de Hausdorff*: Para todo $\alpha, \beta \in \Omega_{\mathrm{Ord}}$ se cumple:

$$\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}.$$

Demostración: Si $\alpha+1 \leq \beta$, entonces $\aleph_{\alpha+1} \leq \aleph_\beta$ y por el teorema anterior

$$\aleph_{\alpha+1}^{\aleph_\beta} = 2^{\aleph_\beta} = 2^{\aleph_\beta}\aleph_{\alpha+1} = \aleph_\alpha^{\aleph_\beta}\aleph_{\alpha+1}.$$

Si $\alpha + 1 > \beta$, entonces como $\aleph_{\alpha+1}$ es regular se tiene que

$$\mathrm{Func}(\omega_{\alpha+1}, \omega_\beta) \approx \mathrm{Func}\left(\coprod_{\delta<\omega_{\alpha+1}} \delta; \omega_\beta\right) = \coprod_{\delta<\omega_{\alpha+1}} \mathrm{Func}(\delta; \omega_\beta),$$

de modo

$$\aleph_{\alpha+1}^{\aleph_\beta} = |\operatorname{Func}(\omega_{\alpha+1}, \omega_\beta)| = \sum_{\delta<\omega_{\alpha+1}} |\delta|^{\aleph_\beta} \leq \sum_{\delta<\omega_{\alpha+1}} \aleph_\alpha^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta}\aleph_{\alpha+1}. \qquad \square$$

Ahora veamos un par de consecuencias del teorema de König:

Teorema (AE) 3.71: Para κ álef se cumple:

1. $\kappa < \kappa^{\operatorname{cf}\kappa}$.
2. $\kappa < \operatorname{cf}(2^\kappa)$.
3. Para $2 \leq \mu \in \Omega_{\mathrm{Card}}$ se cumple $\kappa < \operatorname{cf}(\mu^\kappa)$.

Demostración:

1. Sea $(\nu_\alpha)_{\alpha<\operatorname{cf}\kappa}$ una sucesión cofinal de cardinales, entonces
$$\kappa = \sum_{\alpha<\operatorname{cf}\kappa} \nu_\alpha < \prod_{\alpha<\operatorname{cf}\kappa} \kappa = \kappa^{\operatorname{cf}\kappa}.$$
2. Si $\mu := \operatorname{cf}(2^\kappa) \leq \kappa$, entonces se cumpliría que $(2^\kappa)^\mu \leq (2^\kappa)^\kappa = 2^\kappa$ lo que contradice el item 1.
3. Análogo al anterior. $\square$

Corolario (AE) 3.72: El cardinal del continuo $\mathfrak{c} := 2^{\aleph_0}$ no tiene cofinalidad $\aleph_0$. Luego, por ejemplo, $\mathfrak{c} \neq \aleph_\omega$.

§3.5.3 Cardinales inaccesibles.

Definición 3.73: Un cardinal es *débilmente inaccesible* (resp. inaccesible) si es mayor estricto que $\aleph_0$, es regular y es un cardinal límite (resp. límite fuerte).

Corolario 3.74: Todo cardinal inaccesible es débilmente inaccesible.

Corolario 3.75: Si κ es débilmente inaccesible entonces $\kappa = \aleph_\kappa$.

Demostración: Basta notar que si $\kappa = \aleph_\lambda$ con λ límite, entonces

$$\kappa = \aleph_\lambda = \operatorname{cf}(\aleph_\lambda) = \operatorname{cf}(\lambda) = \lambda \qquad \square$$

Veamos la razón tras su nombre: Por el corolario vimos que κ debe ser un punto fijo de la sucesión $\aleph$ lo que ya revela ser bastante problemático, más aún, no nos podemos acercar con sucesiones a κ y tampoco lo podemos empleando exponenciación de cardinales. De hecho, está probado que la existencia (o no) de los cardinales inaccesibles es independiente a ZFC. Ésto no es nada nuevo, de hecho podemos ver que con los axiomas comunes y corrientes podemos construir todos los ordinales naturales, pero necesitamos un axioma especial para decir que $\aleph_0$, el primer cardinal límite-regular, es constructible.

Los cardinales que son mayores o iguales al primer cardinal débilmente inaccesible se llaman *cardinales grandes*.

De momento no sabemos si existen o no cardinales inaccesibles, pero es útil dar la siguiente definición:

Definición 3.76: Denotamos por $\daleth$ a la sucesión que enumera los cardinales débilmente inaccesibles, de modo que el menor de ellos es $\daleth_0$, el siguiente es $\daleth_1$ y así. Para los cardinales fuertemente inaccesibles empleamos $\dot{\daleth}_\alpha$.

Corolario 3.77: Ni $\daleth$, ni $\dot{\daleth}$ son normales, pese a que son estrictamente crecientes.

Los cardinales grandes son principalmente una herramienta filosófica, pero que puede tener ciertas aplicaciones, siendo una de ellas un fundamento a la teoría de categorías: En lugar de pensar en la categoría de grupos cualesquiera podemos considerar todos los grupos de cardinalidad $< \dot{\daleth}_0$ y así con todas las categorías; de modo que si luego construimos una categoría de éstas categorías sabremos que su clase de objetos será un conjunto de cardinalidad $\leq \dot{\daleth}_0$, y así podemos justificar la existencia o construcción de categorías entre categorías entre categorías *(ad infinitum)*. Ésto es, sin embargo, difícil de explicar para alumnos que no posean trasfondo en teoría de conjuntos, por lo cual los categoristas suelen evitar el problema.

Definición 3.78: Sea κ un álef se dice que κ es:

0-débilmente inaccesible	syss	es regular.
$\alpha+1$-débilmente inaccesible	syss	es α-débilmente inaccesible y es límite de α-débilmente inaccesibles.
λ-débilmente inaccesible	syss	es δ-débilmente inaccesible para todo $\delta < \lambda$.

En particular, los cardinales débilmente inaccesibles son los 1-débilmente inaccesibles bajo ésta definición.

Corolario 3.79: Un cardinal κ es 2-débilmente inaccesible syss $\kappa = \daleth_\kappa$, es decir, $\kappa = \daleth'_\alpha$. En general, los cardinales de la forma $\daleth_\beta^{(\alpha)}$ son exactamente los $(1+\alpha)$-débilmente inaccesibles.[1] En particular, un cardinal κ es a lo más κ-débilmente inaccesible.

Demostración: Nótese que si κ es 2-débilmente inaccesible, entonces es débilmente inaccesible y de la forma $\daleth_\beta$. Además, la sucesión $(\daleth_\alpha)_{\alpha<\beta}$ es cofinal en κ, de modo que $\kappa = \daleth_\kappa$. □

De éste modo podemos también decir que un cardinal es $(1+\alpha)$-inaccesible si es de la forma $\dot{\daleth}_\beta^{(\alpha)}$. Sin embargo, recordemos que ni $\daleth$ ni $\dot{\daleth}$ son normales, de modo que nuestro teorema no sirve para encontrar sus derivadas si es que existen.

3.6 Dos hipótesis de cardinalidad (HCG y HCS)

Definición 3.80: Dado un álef κ, decimos que se cumple:

HGC(κ) Si $2^\kappa = \kappa^+$.

HCS(κ) Si $2^{\operatorname{cf}\kappa} < \kappa \implies \kappa^{\operatorname{cf}\kappa} = \kappa^+$.

Se consideran los posibles siguientes axiomas:

Hipótesis del continuo (abreviado HC) Si HGC($\aleph_0$).

Hipótesis del continuo generalizada (abreviado HCG) Si para todo cardinal infinto $\mathfrak{p}$ no existe otro $\mathfrak{q}$ tal que

$$\mathfrak{p} < \mathfrak{q} < 2^{\mathfrak{p}}.$$

Hipótesis de los cardinales singulares (abreviado HCS) Si para todo álef κ se cumple que HCS(κ).

[1] Aquí el $(1+\alpha)$ se emplea para notar que si α es natural entonces le sumamos 1, pero si $\alpha \geq \omega$, entonces la concordancia es igual.

Si se asume AE, entonces

$$\mathrm{HGC} \iff \forall \kappa \in \Omega_{\mathrm{Card}} \; (\kappa \geq \aleph_0 \implies \mathrm{HGC}(\kappa))$$

§3.6.1 HCG implica AE. Ésta demostración está contenida en [**14**].

Lema 3.81: Si $\mathfrak{p} \geq \aleph_0$, entonces $2^{\mathfrak{p}} + \mathfrak{p} = 2^{\mathfrak{p}}$.

DEMOSTRACIÓN: Si $\mathfrak{p} \geq \aleph_0$, entonces $\mathfrak{p} = \mathfrak{p} + 1$, de modo que

$$2^{\mathfrak{p}} \leq 2^{\mathfrak{p}} + \mathfrak{p} \leq 2^{\mathfrak{p}} + 2^{\mathfrak{p}} = 2 \cdot 2^{\mathfrak{p}} = 2^{1+\mathfrak{p}} = 2^{\mathfrak{p}}. \qquad \square$$

Lema 3.82: Si $2\mathfrak{p} = \mathfrak{p}$ y $\mathfrak{q} + \mathfrak{p} = 2^{\mathfrak{p}}$, entonces $\mathfrak{q} \geq 2^{\mathfrak{p}}$.

DEMOSTRACIÓN: Sea A un conjunto de cardinalidad $\mathfrak{q}$ y B de cardinalidad $\mathfrak{p}$. Luego, la hipótesis se reduce a que $A \amalg B \approx \mathcal{P}(B) \approx \mathcal{P}(B \times \mathbf{2})$ con $\mathbf{2} := \{0, 1\}$, por ende, existe $f : A \amalg B \to \mathcal{P}(B \times \mathbf{2})$ biyección. Sea $E \subseteq B \times \{1\}$ de modo que $E \in \mathcal{P}(B \times \mathbf{2})$, entonces definamos

$$g(E) := E \cup \{x \in B : (x, 0) \notin f(x)\} \in \mathcal{P}(B \times \mathbf{2}).$$

Luego notemos que si $g(E) = f(x)$ con $x \in B$, entonces $(x, 0) \in g(E)$ syss $(x, 0) \notin f(x) = g(E)$, de modo que $g(E) = f(y)$ con $y \in A$. Nótese que luego $g \circ f^{-1}$ es una aplicación inyectiva desde $\mathcal{P}(B \times \{1\}) \approx \mathcal{P}(B)$ cuya imagen es un subconjunto de A, es decir $2^{\mathfrak{p}} = |\mathcal{P}(B)| \leq |A| = \mathfrak{q}$. $\square$

Teorema 3.83: Se cumple que

$$\mathrm{HCG} \implies \mathrm{AE}.$$

DEMOSTRACIÓN: Para ello vamos a comenzar por considerar un cardinal $\mathfrak{p} \geq \aleph_0$ y llamamos $\kappa := \hbar(\mathfrak{p})$ luego definir por recursión:

$$\mathfrak{p}_0 := \mathfrak{p}, \qquad \mathfrak{p}_{n+1} := 2^{\mathfrak{p}_n}.$$

Ahora, probaremos que si $\kappa \leq \mathfrak{p}_n$ entonces: o $\mathfrak{p}$ es un álef o $\kappa \leq \mathfrak{p}_{n-1}$.

Dos observaciones principales son que los $\mathfrak{p}_n$ forman una $\leq$-cadena, de modo que si alguno es un álef, entonces $\mathfrak{p}_0$ también; y la otra observación es que $\kappa \leq \mathfrak{p}_3$ así que basta seguir el proceso recursivamente, para tener que o $\mathfrak{p}_0$ es un álef o $\hbar(\mathfrak{p}) \leq \mathfrak{p}$ lo que es absurdo por lema de Hartogs.

Nótese que

$$\mathfrak{p}_{n-1} \leq \kappa + \mathfrak{p}_{n-1} \leq \mathfrak{p}_n + \mathfrak{p}_n = \mathfrak{p}_n = 2^{\mathfrak{p}_{n-1}},$$

de modo que $\kappa + \mathfrak{p}_{n-1}$ está entre $\mathfrak{p}_{n-1}$ y $2^{\mathfrak{p}_{n-1}}$, por lo que, por HCG se cumple que

$$\kappa + \mathfrak{p}_{n-1} \in \{\mathfrak{p}_{n-1}, \mathfrak{p}_n\}$$

Es decir, o $\kappa \leq \mathfrak{p}_{n-1}$ o $\kappa + \mathfrak{p}_{n-1} = 2^{\mathfrak{p}_{n-1}}$. En el segundo caso, veamos que por el lema (reemplazando $\mathfrak{q} = \kappa$ y $\mathfrak{p} = \mathfrak{p}_{n-1}$) nos queda que $2^{\mathfrak{p}_{n-1}} \leq \kappa$, de modo que por la observación se tiene que $\mathfrak{p}$ es un álef.

Finalmente corrijamos un detalle: ¿qué sucede si $\mathfrak{p}$ es infinito, pero $\mathfrak{p} \not\geq \aleph_0$? Pues basta notar que $\mathfrak{p}' := \mathfrak{p} + \aleph_0$ cumple las condiciones, luego es un álef que contiene a $\mathfrak{p}$ y listo. □

4

Conjuntos estacionarios y álgebras booleanas

Dado que ya hemos visto la definición de un cardinal inaccesible, veremos aquí como los cardinales surgen naturalmente en una serie de problemas interdisciplinarios como en topología y el análisis. Además estudiaremos las álgebras booleanas y su relación a los conjuntos con la representación de Stone.

4.1 Álgebras booleanas

Definición 4.1 – *Álgebra booleana*: Es una séxtupla $(A, +, \cdot, -, 0, 1)$ donde $+, \cdot : A^2 \to A$ y $- : A \to A$ son tales que para todo $u, v, w \in A$:

1. $u + v = v + u$ y $u \cdot v = v \cdot u$ (conmutatividad).
2. $(u + v) + w = u + (v + w)$ y $(u \cdot v) \cdot w = u \cdot (v \cdot w)$ (asociatividad).
3. $u \cdot (v + w) = u \cdot v + u \cdot w$ y $u + (v \cdot w) = (u + v) \cdot (u + w)$ (distributividad).
4. $u + (u \cdot v) = u$ y $u \cdot (u + v) = u$ (absorción).
5. $u + (-u) = 1$ y $u \cdot (-u) = 0$ (complementos).

Cuando no haya ambigüedad en los signos denotaremos que «A es un álgebra booleana» sin especificar las operaciones.

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.

Ejemplos. Son álgebras booleanas:

- Aquella que consiste de un único elemento $0 = 1$, denotada $\mathbf{1}$.
- Aquella que sólo consiste de los elementos $\{0, 1\}$, denotada $\mathbf{2}$.
- Si $A \neq \varnothing$, denotamos por $\mathbf{Sub}(A) := (\mathcal{P}(A), \cup, \cap, {}^c, \varnothing, A)$ al álgebra booleana. Éste tipo de álgebras se dicen *conjuntistas*.
- Si $A \neq \varnothing$, entonces el álgebra dado por las operaciones conjuntistas sobre el conjunto de elementos

$$\mathbf{FC}(A) := \{B \subseteq A : |B| < \aleph_0 \vee |B^c| < \aleph_0\}$$

  que son los subconjuntos finitos o de complemento finito de A forman un álgebra booleana.

Proposición 4.2: Dada un álgebra booleana $(A, +, \cdot, -, 0, 1)$, para todo $u, v \in A$ se cumple:

1. $1 = -0$ y $0 = -1$.
2. $-(-u) = u$ (doble negación).
3. $u \cdot 1 = u + 0 = u$ (elementos neutro).
4. $u \cdot 0 = 0$ y $u + 1 = u$ (aniquiladores).
5. $u \cdot u = u + u = u$ (idempotencia).
6. $-(u + v) = -u \cdot -v$ y $-(u \cdot v) = -u + -v$ (leyes de De Morgan).

Definición 4.3 – *Subálgebra*: Dada un álgebra booleana A, se dice que B es un subálgebra, denotado $B \leq A$, si:

1. $0, 1 \in B$.

2. $u, v \in B$ implican que $u+v, uv, (-u) \in B$.

Luego si $A \neq \mathbf{1}$, entonces $\mathbf{2} \leq A$.

Proposición 4.4 (Criterio de subálgebras): Si A es un álgebra booleana y $B \subseteq A$, entonces $B \leq A$ syss:

1. $0 \in B$.
2. Si $u, v \in B$, entonces $u + -v \in B$.

Demostración: Sea $u \in B$, luego $0 + -u = -u \in B$, de modo que $-0 = 1 \in B$. Si $u, v \in B$, entonces $u + -(-v) = u + v \in B$. Además si $u, v \in B$, entonces $uv = -(-(uv)) = -(-u + -v) \in B$. □

Lema 4.5: La intersección de subálgebras es un subálgebra.

Demostración: Sea $\mathcal{F}$ una familia de subálgebras de A, y sea $B := \bigcap \mathcal{F}$, para probar que $B \leq A$ aplicaremos el criterio anterior:

1. Para todo $C \in \mathcal{F}$ se cumple que $C \leq A$ por construcción; de modo que $0 \in C$ y en conclusión $0 \in B$.
2. Si $u \in B$, entonces $u \in C$ para todo $C \in \mathcal{F}$, luego $-u \in C$ por ser subálgebra, y $-u \in B$.
3. Si $u, v \in B$, entonces $u, v \in C$ para todo $C \in \mathcal{F}$, luego $u + v \in C$ por ser subálgebra, y $u + v \in B$. □

Definición 4.6: Dado $S \subseteq A$, se denota $B := \langle S \rangle$ al mínimo subálgebra $B \leq A$ tal que $S \subseteq B$. Se construye $\langle S \rangle$ como la intersección de todos los subálgebras que le contienen.

Definición 4.7: Si A es subálgebra, entonces denotamos

$$u - v := u \cdot (-v).$$

Se dice que u, v son *disjuntos* si $u \cdot v = 0$. Se denota que $u \leq v$ si $u - v = 0$.

Proposición 4.8: Se cumple que:

1. $u \leq v$ syss $u + v = v$ syss $u \cdot v = u$ syss $-u + v = 1$.

2. $\leq$ es una relación de orden parcial sobre A.
3. 0 es el mínimo de $(A, \leq)$ y 1 su máximo.
4. $u \cdot v = \inf\{u, v\}$ y $u + v = \sup\{u, v\}$.

Demostración:

1. Se da lo siguiente:

$$\begin{aligned} u \leq v &\iff u \cdot (-v) = 0 \\ &\implies v = v + 0 = v + (u \cdot (-v)) = (v + u) \cdot (v + -v) \\ &\qquad = (v + u) \cdot 1 = v + u \\ &\implies u = u \cdot (u + v) = u \cdot v \\ &\implies 0 = u \cdot (-u) = u \cdot -(u \cdot v) = u \cdot (-u + -v) \\ &\qquad = u \cdot -u + u \cdot -v = u \cdot (-v). \end{aligned}$$

   También notemos que $1 = -u + v$ syss $0 = -(-u + v) = u \cdot (-v) = u - v$.

2. Claramente $u \cdot (-u) = 0$, ergo $u \leq u$.
   Si $u + v = v$ y $v + w = w$, entonces $u + w = u + (v + w) = (u + v) + w = v + w = w$.
   Si $u + v = v$ y $v + u = u$, entonces $u = v + u = u + v = v$.

3. Ejercicio para el lector.

4. Claramente $u + v$ es cota superior de $\{u, v\}$. Supongamos que w también lo es, entonces $u + w = w$ y $v + w = w$, ergo

$$(u + v) + w = u + (v + w) = u + w = w,$$

   es decir $u + v \leq w$. El otro es análogo. $\square$

Definición 4.9 (Morfismos): Dadas dos álgebras booleanas A, B, una aplicación $\varphi : A \to B$ es un *homomorfismo* de álgebras booleanas, si cumple que

1. $\varphi(0) = 0$ y $\varphi(1) = 1$.
2. $\varphi(u + v) = \varphi(u) + \varphi(v)$.
3. $\varphi(u \cdot v) = \varphi(u) \cdot \varphi(v)$.

4. $\varphi(-u) = -\varphi(u)$.

Naturalmente, ésto permite que las álgebras booleanas formen una categoría denotada Bool.

Corolario 4.10: $\mathbf{1}$ es un objeto final y $\mathbf{2}$ es un objeto inicial de Bool. Es decir, para todo álgebra booleana A, se cumple que existe un único morfismo $\mathbf{2} \xrightarrow{f} A$ y un único morfismo $A \xrightarrow{g} \mathbf{1}$. Si $A \neq \mathbf{1}$, entonces f es de hecho un monomorfismo.

Definición 4.11 – *Filtros, ideales*: Dado un álgebra booleana A, se dice que $F \subseteq A$ es un *filtro* si:

1. $0 \notin F, 1 \in F$.
2. Si $u, v \in F$, entonces $u \cdot v \in F$.
3. Si $u \leq v$ y $u \in F$, entonces $v \in F$.

Se dice que I es un *ideal* si:

1. $0 \in I, 1 \notin I$.
2. Si $u, v \in I$, entonces $u + v \in I$.
3. Si $u \leq v$ y $v \in I$, entonces $v \in I$.

Claramente, F es un filtro syss $I := \{-u : u \in F\}$ es un ideal, en este caso se dice que F e I son duales. Si X es un conjunto, un filtro o ideal de X lo es del álgebra booleana $\mathbf{Sub}(X)$.

Un filtro F tal que para todo $u \in A$ se cumple que $u \in F$ o $-u \in F$ se dice un *ultrafiltro*. El dual de un ultrafiltro se dice un *ideal primo*.

Ejemplos: Se cumple que:

- $\{0\}$ y $\{1\}$ son un ideal y un filtro resp., llamados los *triviales*.
- Si $u \notin \{0, 1\}$, se dice que $I_u := \{v : v \leq u\}$ y $F_u := \{v : v \geq u\}$ son un ideal y un filtro resp., llamados los *principales*.
- Si X es un conjunto infinito, entonces $I := [X]^{<\aleph_0}$ es un ideal, cuyo filtro dual es llamado el *filtro de Fréchet* de X. Cabe destacar que el filtro de Fréchet no es principal en estas condiciones.

Proposición 4.12: Un ideal (resp. filtro) es un ideal primo (resp. ultrafiltro) sobre A syss es la preimagen de $f^{-1}[\{0\}]$ (resp., $f^{-1}[\{1\}]$), donde f es un morfismo de A a $\mathbf{2}$.

Lema 4.13: Un ideal (resp. filtro) sobre A es primo (resp. ultrafiltro) syss es maximal respecto de la inclusión.

DEMOSTRACIÓN: $\Longrightarrow$. Es trivial.

$\Longleftarrow$. Lo probaremos por contrarrecíproca: Si I no es primo, entonces hay algún $u \in A$ tal que $u \notin I$ y $-u \notin I$. Notemos que $u + v = 1$ syss $-u \leq v$, y como $-u \notin I$ entonces $u + v \neq 1$ para todo $v \in I$. Luego sea

$$J := \{w \in A : w \leq u + v, \quad v \in I\}.$$

Veamos que J es ideal: claramente si $v \leq w$ y $w \in J$, entonces $v \in J$, y si $v, w \in J$, entonces existen $\bar{v}, \bar{w} \in I$ tales que $v \leq u + \bar{v}$ y $w \leq u + \bar{w}$, de modo que

$$v + w = \sup\{v, w\} \leq \sup\{u + \bar{v}, u + \bar{w}\} = (u + \bar{v}) + (u + \bar{w}) = u + (\bar{v} + \bar{w})$$

donde $\bar{v} + \bar{w} \in I$ por ser ideal, de modo que $v + w \in J$ por definición. En conclusión $J \supset I$, e I no es maximal. □

Definición 4.14: Se dice que $S \subseteq A$ tiene la *propiedad de intersecciones finitas* (o, PIF para acortar) si para todo $u_1, \dots, u_n \in S$ se cumple que $\prod_{i=1}^{n} u_i \neq 0$. Se le dice así, por que en el caso de conjuntos, en lugar del producto general se tiene que la intersección de finitos subconjuntos es no vacía.

Proposición 4.15: Se cumplen las siguientes:

1. Todo filtro posee la PIF.
2. La intersección arbitraria de filtros (resp. ideales) es un filtro (resp. ideal).
3. Si $\mathcal{F}$ es una $\subseteq$-cadena de filtros (resp. ideales), entonces $\bigcup \mathcal{F}$ es un filtro (resp. ideal).
4. Si $S \subseteq A$ posee la PIF, entonces existe un filtro tal que $S \subseteq F$.

DEMOSTRACIÓN:

1. Trivial de la definición de filtro.

2. Sea $\mathcal{F}$ la familia de filtros y sea $F := \bigcap \mathcal{F}$. Claramente $0 \notin F, 1 \in F$ pues se aplica para todo $F' \in \mathcal{F}$.
   Si $u, v \in F$, entonces $u, v \in F'$ para todo $F' \in \mathcal{F}$, de modo que $u \cdot v \in F'$ y en conclusión $u \cdot v \in F$.
   Si $u \leq v$ y $u \in F$, entonces $u \in F'$ para todo $F' \in \mathcal{F}$ y por definición $v \in F'$, en conclusión, $v \in F$.

3. Similar al anterior denotemos $F := \bigcup \mathcal{F}$, y veamos que es filtro:

   a) Claramente $0 \notin F, 1 \in F$ pues al menos un filtro de $\mathcal{F}$ posee al 1, y ninguno al 0.

   b) Sea $u, v \in F$, luego existen $G, H \in \mathcal{F}$ tal que $u \in G, v \in H$, pero como $\mathcal{F}$ está linealmente ordenado por $\subseteq$, entonces o $G \subseteq H$ o $H \subseteq G$; asumamos el primero, luego $u, v \in H$ y $u \cdot v \in H \subseteq F$.

   c) Sea $u \leq v$ con $u \in F$, luego existe $G \in \mathcal{F}$ tal que $u \in G$ y por lo tanto $v \in G \subseteq F$.

4. Sea S como exigimos, queremos formar un filtro a partir de S, así que vamos a hacerlo de la siguiente manera:

$$F := \left\{ u \in A : u \geq \prod_{i=1}^{n} v_i,\ v_i \in S \right\},$$

   es decir, los elementos de F son aquellos que son mayores que cualquier intersección finita; veamos que es un filtro: Claramente $0 \notin F$ y $1 \in F$, y además claramente si $u \leq v$ con $u \in F$ se cumple que $v \in F$. El producto es más interesante, si $u, v \in F$, entonces se cumple que $\prod_{i=1}^{n} \bar{u}_i \leq u$ y $\prod_{i=1}^{m} \bar{v}_i \leq v$ para algunos $\bar{u}_i, \bar{v}_i \in S$, pero entonces

$$u \cdot v \geq \left(\prod_{i=1}^{n} \bar{u}_i \right) \left(\prod_{i=1}^{m} \bar{v}_i \right) = \prod_{i=1}^{n+m} w_i$$

   donde $w_i = \bar{u}_i$ si $i \leq n$ y $w_i = \bar{v}_{i-n}$ si $i > n$; como $w_i \in S$, entonces $u \cdot v \in F$. □

Teorema 4.16: Son equivalentes:

Teorema de los ideales primos Todo álgebra booleana posee al menos un ideal primo.

Teorema del ultrafiltro (TUF) Todo filtro de un conjunto está contenido en un ultrafiltro.

Teorema de representación de Stone Toda álgebra booleana es isomorfa a una álgebra conjuntista.

Más aún, todos son consecuencia del AE.

Demostración: TIP $\iff$ TUF. Ver [**17,** Teo. 3.37].

AE $\implies$ TUF. Sea F un filtro que no es ultrafiltro, de modo que como no es maximal existe $G \supseteq F$ que es filtro y luego la familia

$$\mathcal{F} := \{G : G \supseteq F \wedge G \text{ es filtro}\}$$

es no vacía y satisface que toda $\subseteq$-cadena está acotada superiormente, por lo que por lema de Zorn posee un elemento maximal que es un ultrafiltro que contiene a F.

TIP $\implies$ Stone. ... □

Es decir, con ésto vemos que sin AE no sabemos siquiera si ciertas álgebras booleanas poseen ultrafiltros o no. Hagamos el siguiente ejercicio, supongamos que A es un álgebra booleana de cardinal infinito κ, de modo que posee 2^κ subconjuntos y como la familia de ultrafiltros es una subfamilia de $\mathcal{P}(A)$, entonces posee a lo más 2^{2^κ} elementos. De momento no sabemos si quiera si posee 1 elemento, pero recuerde que el máximo es 2^{2^κ}.

Definición 4.17: Se dice que un ultrafiltro D de un conjunto A es *uniforme* si para todo $X \in D$ se cumple que $|X| = |A|$.

Definición 4.18: Se dice que una familia $\mathcal{F}$ de subconjuntos de κ (como conjunto) es *independiente*, si para todo $X_1, \dots, X_n; Y_1, \dots, Y_m \in \mathcal{F}$ donde son todos distintos, se cumple que

$$|X_1 \cap \cdots \cap X_n \cap Y_1^c \cap \cdots \cap Y_m^c| = \kappa.$$

Lema 4.19: Cafa álef κ posee una familia independiente de cardinal 2^κ.

Demostración: Sea P el conjunto de pares ordenados $(F, \mathcal{F})$ donde F es subconjunto finito de κ y $\mathcal{F}$ es subconjunto finito de $[\kappa]^{<\omega}$, i.e., llamando $\mathcal{B} := [\kappa]^{<\omega}$ se tiene que $P := \mathcal{B} \times [\mathcal{B}]^{<\omega}$, como $|\mathcal{B}| = \kappa$, entonces $|P| = \kappa$. Luego el enunciado es equivalente a encontrar una familia independiente $\mathcal{A}$ de P de cardinal 2^κ.

Sea $A \subseteq \kappa$, entonces

$$X_A := \{(F, \mathcal{F}) \in P : F \cap A \in \mathcal{F}\}$$

y sea $\mathcal{A} := \{X_A : A \subseteq \kappa\}$. Veamos que $X : \mathcal{P}(\kappa) \to \mathcal{A}$ es una biyección: Claramente es suprayectiva y si $A \neq B$, entonces sin perdida de generalidad existe $\alpha \in A \setminus B$, de modo que con $F := \{\alpha\}$ y $\mathcal{F} := \{F\}$ notamos que $(F, \mathcal{F}) \in X_A$ pero $(F, \mathcal{F}) \notin X_B$. En conclusión $|\mathcal{A}| = 2^\kappa$.

Veamos que $\mathcal{A}$ es una familia independiente: Sean $A_1, \dots, A_n; B_1, \dots, B_m$ distintos subconjuntos de κ. Luego, para cada i, j se cumple que existe $\alpha_{i,j} \in A_i \Delta B_j$ [diferencia simétrica]. De modo que fijamos un conjunto finito F que contenga a todos los $\alpha_{i,j}$ (notar que hay κ conjuntos así). Notar que $F \cap A_i \neq F \cap B_j$ para todo i, j, de modo que si definimos $\mathcal{F} := \{F \cap A_i : 1 \leq i \leq n\}$, entonces se cumple que $(F, \mathcal{F}) \in X_{A_i}$ para todo i, mientras que $(F, \mathcal{F}) \notin X_{B_j}$ para todo j, por ende

$$(F, \mathcal{F}) \in X_{A_1} \cap \cdots X_{A_n} \cap X^c_{B_1} \cap \cdots \cap X^c_{B_m}$$

y luego, dicha intersección tiene κ elementos que es lo que se quería probar. □

Teorema (TUF) 4.20 (Pospíšil): Cada álef κ (como conjunto) posee 2^{2^κ} ultrafiltros uniformes.

Demostración: Para cada aplicación $f : \mathcal{A} \to \{0, 1\}$ se define

$$G_f := \{X \subseteq \kappa : |X^c| < \kappa\} \cup \{X : f(X) = 0\} \cup \{X^c : f(X) = 1\}$$

que es una familia con la PIF (¿por qué?), de modo que está contenido en un ultrafiltro D_f. Es claro que si $f \neq g$, entonces $D_f \neq D_g$, y también de que D_f es uniforme, por lo que hay al menos $|\{0, 1\}|^{|\mathcal{A}|} = 2^{2^\kappa}$ ultrafiltros uniformes. □

Definición 4.21: Se dice que un filtro (resp. ideal) es κ-completo para algún álef κ si se cumple que todo subconjunto suyo S con $|S| < \kappa$ posee ínfimo (resp. supremo) en el mismo filtro (resp. ideal). Decimos que un filtro es *completo* (a secas) si lo es para todo cardinal. Para ahorrar notación, denotamos σ-completo en lugar de $\aleph_1$-completo.

Nótese que por definición, todo filtro o ideal es $\aleph_0$-completo, de manera que ésta expresión es redundante. Claramente, los filtros principales sobre un conjunto son siempre completos. También, notemos que el filtro de Fréchet sobre $\mathbb{N}$ no puede ser σ-completo, pues $\{\mathbb{N} \setminus \{n\} : n \in \mathbb{N}\}$ es una subfamilia numerable del filtro de Fréchet cuya intersección es vacía; por el mismo argumento, el filtro de Fréchet sobre un álef κ no es (κ^+)-completo.

4.2 Conjuntos cerrados no acotados

Como los ordinales forman conjuntos ordenados, entonces poseen una topología estándar que ya hemos implicitado en el concepto de *sucesión continua*, pues la continuidad es exactamente la inducida por la topología del orden. Y así, podemos hablar de conjuntos abiertos o cerrados en un ordinal.

Definición 4.22: Tomando un ordinal λ como conjunto, se dice que $C \subseteq \lambda$ es cerrado si para todo ordinal límite $\gamma < \lambda$ tal que $C \cap \gamma$ no está acotado en γ se cumple que $\gamma \in C$. En general, si λ es límite podemos hablar de conjuntos cerrados no acotados (abreviados c.n.a.).

Un subconjunto S de λ es *estacionario* si para todo C c.n.a., se cumple que $C \cap S \neq \varnothing$.

En ésta sección trabajaremos sobre todo en ordinales λ que sean límites y tales que $\operatorname{cf} \lambda > \aleph_0$. Ésto se debe a que una de las primeras particularidades que veremos de los c.n.a.'s es que su intersección finita es un c.n.a., pero ésto es falso si permitimos que λ tenga cofinalidad numerable: Sea $(\alpha_n)_{n<\omega}$ una sucesión normal y cofinal en λ, entonces los conjuntos $\{\alpha_{2n} : n \in \mathbb{N}\}$ y $\{\alpha_{2n+1} : n \in \mathbb{N}\}$ son c.n.a.'s y disjuntos.

Intuitivamente los conjuntos estacionarios deben contener una buena dosis de puntos de acumulación.

Proposición 4.23: Un subconjunto $C \subseteq \lambda$ es cerrado syss es orden-completo, es decir, todo subconjunto de C acotado superiormente posee supremo.

Proposición 4.24: Sea κ un álef regular no numerable. Un subconjunto $C \subseteq \kappa$ es c.n.a. syss es la imagen de una endofunción normal de κ.

Teorema 4.25: Sea λ de $\operatorname{cf} \lambda > \aleph_0$. Sea $(C_\alpha)_{\alpha<\beta}$ una familia de conjuntos c.n.a. con $\beta < \operatorname{cf} \lambda$, entonces $\bigcap_{\alpha<\beta} C_\alpha$ es c.n.a.

Demostración: La intersección arbitraria de cerrados es cerrados, así que basta probar que es no acotado:

Sea $\gamma < \lambda$, entonces como cada C_α es no acotado se puede definir $f_\alpha(\gamma) := \min\{\delta \in C_\alpha : \delta > \gamma\}$. Luego, sea $g(\gamma) := \sup_{\alpha<\beta} f_\alpha(\gamma) > \gamma$, el cual está bien definido en λ pues $\beta < \operatorname{cf}\lambda$. Finalmente consideremos $g^\omega(\gamma)$ y veamos que es de hecho un ordinal límite: En efecto, si $\delta < g^\omega(\gamma)$, entonces $\delta \in \bigcup_{n<\omega} g^n(\gamma)$, ergo $\delta \in g^n(\gamma)$ para algún n finito, y por lo tanto

$$\delta + 1 < g^n(\gamma) + 1 \leq g(g^n(\gamma)) \leq g^\omega(\gamma).$$

Ahora, veamos que $g^\omega(\gamma) \cap C_\alpha$ no está acotado para ningún α: Sea $\delta < g^\omega(\gamma)$, luego $\delta < g^n(\gamma)$ para algún n y $\delta < f_\alpha(g^n(\gamma)) \in C_\alpha$ y $f_\alpha(g^n(\gamma)) \leq g(g^n(\gamma)) < g^\omega(\gamma)$, es decir, $\delta < f_\alpha(g^n(\gamma)) \in C_\alpha \cap g^\omega(\gamma)$.

Para concluir, como los C_α's son cerrados, vemos que todos incluyen a $g^\omega(\gamma) > \gamma$, de modo que su intersección no está acotada. □

Corolario 4.26: Sea λ de $\operatorname{cf}\lambda > \aleph_0$. La familia de los c.n.a.'s posee la PIF.

Definición 4.27: Sea λ de $\operatorname{cf}\lambda > \aleph_0$. Podemos definir el filtro generado por los c.n.a.'s, al que denotamos por $\mathbf{cna}(\lambda)$; así $S \in \mathbf{cna}(\lambda)$ syss S contiene a un c.n.a.

Corolario (AE) 4.28: Sea λ de $\operatorname{cf}\lambda > \aleph_0$. El filtro $\mathbf{cna}(\lambda)$ es $(\operatorname{cf}\lambda)$-completo.

Proposición 4.29: Sobre λ de $\operatorname{cf}\lambda > \aleph_0$ se cumplen:

1. Todo c.n.a. es estacionario.
2. E es estacionario en λ syss $E^c \notin \mathbf{cna}(\lambda)$. En consecuencia, si U es un ultrafiltro que extiende a $\mathbf{cna}(\lambda)$ entonces contiene a todos los conjuntos estacionarios.
3. Todo conjunto estacionario no está acotado.
4. La intersección entre un c.n.a. y un conjunto estacionario da un conjunto estacionario.

Proposición 4.30: Sea λ de $\operatorname{cf}\lambda > \aleph_0$. Si $\kappa < \operatorname{cf}\lambda$ es un álef regular, entonces

$$E_\kappa^\lambda := \{\alpha < \lambda : \operatorname{cf}\alpha = \kappa\}$$

es estacionario.

Consideremos el ordinal ω_2 que por AE es regular, entonces $E^{\omega_2}_{\aleph_0}$ y $E^{\omega_2}_{\aleph_1}$ son conjuntos estacionarios disjuntos, es decir, la intersección de estacionarios puede no ser estacionaria.

Naturalmente si $\lambda = \kappa$ es un álef regular no numerable, entonces deducimos que la intersección de a-lo-más κ c.n.a.'s es c.n.a. Ésta condición puede ser mejorada, con una nueva definición:

Definición 4.31: Sea $(C_\alpha)_{\alpha<\kappa}$ una sucesión de subconjuntos de κ, entonces se define su *intersección diagonal* como

$$\bigtriangleup_{\alpha<\kappa} C_\alpha := \left\{\gamma < \kappa : \gamma \in \bigcap_{\alpha<\gamma} C_\alpha\right\}.$$

Teorema 4.32: Si κ es un álef regular no-numerable y $(C_\alpha)_{\alpha<\kappa}$ es una sucesión de c.n.a.'s de κ, entonces $\bigtriangleup_{\alpha<\kappa} C_\alpha$ es c.n.a.

Demostración: Si definimos $D_\alpha := \bigcap_{\beta\leq\alpha} C_\beta$, entonces tenemos que $(D_\alpha)_{\alpha<\kappa}$ es una sucesión decreciente de c.n.a.s y que satisface que $C := \bigtriangleup_{\alpha<\kappa} C_\alpha = \operatorname{diag}_{\alpha<\kappa} D_\alpha$. Veamos que C es c.n.a.:

i) <u>C es cerrado:</u> Sea λ tal que $C \cap \lambda$ no está acotado, queremos ver que $\lambda \in C$, es decir, que $\lambda \in \bigcap_{\alpha<\lambda} D_\alpha$. Sea $\delta \in C$ menor a λ, entonces $X := \{\gamma \in C : \delta < \gamma < \lambda\}$, nótese que si $\gamma \in X$, entonces $\gamma \in D_\delta$, es decir, $X \subseteq D_\delta$ y luego $\sup D_\delta = \lambda \in D_\delta$.

ii) <u>C no está acotado:</u> Para ello veremos que si $(\beta_n)_{n<\omega}$ es una sucesión estrictamente creciente con $\beta_{i+1} \in D_{\beta_i}$, entonces $\beta := \lim_{n\to\omega} \beta_n \in C$; ésto es útil pues si $\alpha < \kappa$, entonces existe $\beta_0 \geq \alpha$ en D_0 por ser c.n.a. y automáticamente se concluye que C no está acotado.

Sea $\gamma < \beta$, entonces existe $n < \omega$ con $\beta_n > \gamma$, luego como $\beta_n \in D_{\beta_n} \subseteq D_\gamma$. Notemos que para todo $k \geq 0$ se cumple, por definición, que $\beta_{n+k} \in D_{\beta_n}$, de modo que $\beta \in D_{\beta_n} \subseteq D_\gamma$. Finalmente $\beta \in \bigcap_{\gamma<\beta} D_\gamma$, i.e., $\beta \in C$. □

Definición 4.33 – *Función regresiva*: Dado $S \subseteq \Omega_{\mathrm{Ord}}$, se dice que

$f: S \to \Omega_{\mathrm{Ord}}$ es una *función regresiva* si para todo $\alpha \in S_{\neq 0}$ se cumple que $f(\alpha) < \alpha$.

Teorema (AE) 4.34 – *Teorema de Fodor*: Sea κ un álef regular no numerable. Si E es estacionario en κ y $f: E \to \kappa$ es regresiva, entonces alguna fibra de f es estacionaria, es decir, $f^{-1}[\{\gamma\}]$ es estacionario para algún $\gamma < \kappa$.

Demostración: Por contradicción supongamos que todas las fibras no son estacionarias, es decir, $f^{-1}[\{\gamma\}] \cap C_\gamma = \varnothing$ para algún C_γ c.n.a., que satisface que para todo $\alpha \in E \cap C_\gamma$ se cumpla que $f(\alpha) \neq \gamma$. Definamos $C := \Delta_{\gamma<\kappa} C_\gamma$, que resulta ser c.n.a. por el teorema anterior. Definamos $C := \Delta_{\gamma<\kappa} C_\gamma$, que resulta ser c.n.a. por el teorema anterior. Luego $E \cap C$ no es vacío y contiene a algún α, notemos que por definición, $\alpha \in \bigcap_{\gamma<\alpha} E \cap C_\gamma$, es decir, $f(\alpha) \neq \gamma$ para todo $\gamma < \alpha$, luego $f(\alpha) \geq \alpha$ lo que es absurdo. □

Ejemplo (AE) 1 (Un estacionario de complemento estacionario): Sea $\kappa = \aleph_1$ y sea E el conjunto de los ordinales límite $\lambda < \aleph_1$. Claramente E es estacionario. Para cada $\lambda \in E$ se cumple que $\operatorname{cf} \lambda = \aleph_0$, por lo que existe una sucesión $x_{\lambda,n}$ creciente y cofinal en λ. Para cada $n \in \mathbb{N}$ definamos $f_n: E \to \kappa$ dado por $f_n(\lambda) := x_{\lambda,n}$.

Nótese que $f_n(\lambda) < \lambda$ para todo $\lambda \in E$. Luego por el teorema de Fodor existe un γ_n tal que la fibra $S_n := f_n^{-1}[\{\gamma_n\}]$ es estacionaria. Veamos que algún S_n tiene complemento estacionario: De lo contrario, existe un $C \cap S_n^c = \varnothing$, es decir, cada S_n contiene a algún c.n.a. Luego $\bigcap_{n\in\mathbb{N}} S_n$ también contiene a un c.n.a., luego contiene a un ordinal límite λ tal que $\gamma_n = f_n(\lambda) < \lambda$, y tal que $\lambda > \lim_{n\to\omega} \gamma_n$ (pues no está acotado). Pero $\lim_{n\to\omega} \gamma_n = \lim_{n\to\omega} f_n(\lambda) = \lambda$, lo que es absurdo.

Nótese que para la construcción de éste ejemplo fue necesario el uso del AE.

Lema 4.35: Sea κ un álef regular no numerable y sea E estacionario en κ. Entonces

$$T := \{\lambda \in E : \operatorname{cf} \lambda = \aleph_0 \vee (\operatorname{cf} \lambda > \aleph_0 \wedge E \cap \lambda \text{ no es estacionario en } \lambda)\}$$

es estacionario.

Demostración: Sea C un c.n.a. Sabemos que C es la imagen de una endofunción normal f, y podemos definir $g : \kappa \to \kappa$ como la función normal que pasa por todos los ordinales límite (como ejercicio, hágalo con funciones derivadas) de modo que $h := g \circ f$ es normal y $C' := \operatorname{Img} h$ es c.n.a. contenido en C, cuyos elementos son todos ordinales límite. Luego $E \cap C'$ es no vacío y posee un mínimo $\lambda = h(\alpha)$. Si $\operatorname{cf} \lambda = \aleph_0$, entonces $\lambda \in T$, así que supondremos que $\operatorname{cf} \lambda > \aleph_0$.

i) <u>$C \cap \lambda$ no está acotado en λ:</u> En primer lugar, nótese que $\lambda = f(g(\alpha))$ donde $g(\alpha)$ es límite, de modo que $\{f(\delta) : \delta < g(\alpha)\} = C \cap \lambda$ no está acotado en λ.

ii) <u>$C' \cap \lambda$ no está acotado en λ:</u> Sea $\ell : \lambda \to \lambda$ la función tal que $\ell(\alpha) := \min(C \cap \lambda \cap O_{\geq}(\alpha))$. Claramente ℓ es discretamente creciente, y veamos que es continua también: Si γ es límite, entonces $S := \{\ell(\delta) : \delta < \gamma\}$ es un subconjunto no acotado de $C \cap \lambda$ que es cerrado, ergo $\sup S \in C \cap \lambda$ y como $\ell(\gamma)$ es la mínima cota superior de S, se tiene que $\ell(\gamma) = \sup S$. Es decir, ℓ es normal.

   Luego ℓ^ω es una función normal, cuya imagen está conformada por ordinales límite de cofinalidad numerable, es decir, $\operatorname{Img}(\ell^\omega) \subseteq C' \cap \lambda$, y por ser normal es cofinal, lo que prueba que no está acotado.

Es decir, $C' \cap \lambda$ es c.n.a. en λ. Finalmente notar que

$$(C' \cap \lambda) \cap (E \cap \lambda) \subseteq \lambda \cap (E \cap C') = \varnothing$$

donde la última igualdad viene por el hecho de que λ es por definición el mínimo de $E \cap C'$; i.e., $E \cap \lambda$ no es estacionario en λ y por lo tanto $\lambda \in T$. □

Teorema (AE) 4.36 (Solovay): Sea κ un álef regular no numerable, entonces todo conjunto estacionario E en κ puede particionarse en κ conjuntos estacionarios.

Demostración: Consideremos el conjunto T como en el lema anterior. Para cada $\lambda \in T$ sea $g_\lambda : \operatorname{cf} \lambda \to \lambda$ una función normal y cofinal. Si $\operatorname{cf} \lambda > \aleph_0$, entonces $E \cap \lambda$ no es estacionario, y por tanto, $T \cap \lambda$ tampoco, con lo que existe un c.n.a. tal que $T \cap \lambda \cap C = \varnothing$ y definamos $g_\lambda^* : \operatorname{cf} \lambda \to \lambda$ normal por recursión:

$$g_\lambda^*(0) := \min C, \quad g_\lambda^*(\alpha + 1) := \min(C \setminus O_<(\max\{g_\lambda^*(\alpha), g_\lambda(\alpha)\}))$$

que resulta por ende, cofinal con la particularidad de que $g_\lambda^*(\alpha) \notin T$ para todo $\alpha < \operatorname{cf} \lambda$. Denotemos f_λ como g_λ si $\operatorname{cf} \lambda = \aleph_0$ o g_λ^* de lo contrario.

Fijados $\delta, \epsilon < \kappa$ denotemos

$$F_\epsilon^\delta := \{\lambda \in T : \delta < \operatorname{cf}\lambda \wedge f_\lambda(\delta) \geq \epsilon\}.$$

i) Existe un δ tal que para todo ϵ se cumple que F_ϵ^δ es estacionario: Veamoslo por contradicción: si no, entonces para todo δ existe un $\epsilon_\delta < \kappa$ tal que F_ϵ^δ no es estacionario, i.e., existe un c.n.a. C_δ tal que $F_\epsilon^\delta \cap C_\delta = \varnothing$. Luego, sea $C := \Delta_{\alpha<\kappa} C_\alpha$ que resulta ser c.n.a., y como T es estacionario se tiene que Luego, sea $C := \Delta_{\alpha<\kappa} C_\alpha$ que resulta ser c.n.a., y como T es estacionario se tiene que existe $\lambda \in C \cap T$; en consecuencia, se cumple que para todo $\delta < \operatorname{cf}\lambda$ se tiene que $f_\lambda(\delta) < \epsilon_\delta$.

   Sea $D_\delta := C \cap O_>(\epsilon_\delta) = \{\gamma \in C : \gamma > \epsilon_\delta\}$ y notese que es c.n.a. por intersección de dos de ellos, de modo que $D := \Delta_{\alpha<\kappa} D_\alpha$ es c.n.a. y $T \cap D$ es estacionario, de modo que se cumple de dos de ellos, de modo que $D := \Delta_{\alpha<\kappa} D_\alpha$ es c.n.a. y $T \cap D$ es estacionario, de modo que se cumple que $\gamma < \lambda$ pertenecen a la intersección, y para el cuál podemos exigir que γ, λ sean límite. Como $\lambda \in D$, entonces $\lambda \in C \cap T$ y por ende si $\delta < \min\{\gamma, \operatorname{cf}\lambda\}$, entonces $f_\lambda(\delta) < \epsilon_\delta$, y como $\gamma \in D$, entonces $\epsilon_\delta < \gamma$.

   Como f_λ es cofinal existe un $\delta < \operatorname{cf}\lambda$ tal que $\gamma \leq f_\lambda(\delta)$ y por las condiciones anteriores se tiene que $\gamma \leq \delta < \operatorname{cf}\lambda$, de modo que $\operatorname{cf}\lambda > \aleph_0$.

   Finalmente, como f_λ es normal y $f_\lambda(\delta) < \gamma$ para $\delta < \gamma$, se tiene que $f_\lambda(\gamma) = \lim_{\delta\to\lambda} f_\lambda(\delta) \leq \gamma$ y por normalidad se concluye que $f_\lambda(\gamma) = \gamma$, pero esto es absurdo pues $\gamma \in T$, pero $f_\lambda(\gamma) \notin T$ (pues f_λ tiene codominio disjunto de T si $\operatorname{cf}\lambda > \aleph_0$).

ii) Construcción de la partición: Sea δ el encontrado en el item anterior, de modo que podemos erradicar el superíndice en F_ϵ^δ. Como f_λ es cofinal en λ, entonces definir $g : T \to \kappa$ por $g(\lambda) := f_\lambda(\delta)$ resulta en una función regresiva. Para cada $\epsilon < \kappa$, sabemos que F_ϵ es estacionario, de modo que $g \upharpoonright F_\epsilon$ es regresiva sobre un estacionario y por teorema de Fodor posee una fibra $G_\epsilon := (g|_{F_\epsilon})^{-1}[\{\gamma_\epsilon\}]$ estacionaria.

   Sea $\lambda \in G_\epsilon \subseteq F_\epsilon$. Por definición, $\gamma_\epsilon = g(\lambda) = f_\lambda(\delta) \geq \epsilon$, en síntesis, $\gamma_\epsilon \geq \epsilon$, por lo que γ_ϵ forma una κ-sucesión cofinal; como κ es regular, de hecho, el conjunto $\Gamma := \{\gamma_\epsilon : \epsilon < \kappa\}$ tiene cardinal κ, es decir, existe una biyección $h : \kappa \to \Gamma$.

   Finalmente, definamos

$$E_\alpha := G_{h(\alpha)} \subseteq F_{h(\alpha)} \subseteq T \subseteq E$$

entonces los E_α son estacionarios y disjuntos dos a dos (pues sus elementos tienen imagenes distintas bajo la función g), de modo que si definimos
$$U := E \setminus \bigcup_{\alpha<\kappa} E_\alpha$$
y reemplazamos $E_0' := E_0 \cup U$, se comprueba que $(E_\alpha)_{\alpha<\kappa}$ es una partición de E en κ conjuntos estacionarios. □

§4.2.1 Cardinales de Mahlo.

Definición 4.37: Se dice que κ es un cardinal *(débilmente) de Mahlo* si κ es (débilmente) inaccesible y el conjunto de cardinales regulares estrictamente menores que κ es estacionario en κ.

Pensemos qué propiedades tendría el primer cardinal débilmente de Mahlo κ, ¿nos preguntamos si $\kappa = \daleth_0$? Sea $S := \{\mu < \kappa : \mu \text{ es regular}\}$, basta considerar la siguiente endofunción normal $f : \kappa \to \kappa$ por recursión transfinita
$$f(0) := \omega_0 + \omega, \quad f(\alpha + 1) = \omega_{\alpha+1} + \omega$$
y notar que $f[\kappa]$ (que es c.n.a.) es disjunto de S, pues solo toma $f(\lambda) = \omega_\lambda$ cuando λ es límite, y $\omega_\lambda < \daleth_0$ de modo que no es regular y por ende $\omega_\lambda \notin S$. En conclusión, $\kappa \neq \daleth_0$.

¿Pero $\kappa = \daleth_1$? De nuevo la respuesta es no, basta considerar la misma función anterior e intersectarla con $O_>(\daleth_0)$. Y así vemos que $\kappa \neq \daleth_n$ para todo $n < \omega$. Tampoco $\kappa \neq \daleth_\omega$ pues si llamamos $\mu := \sup_{n<\omega} \daleth_n$, entonces si intersectamos $f[\kappa]$ con $O_>(\mu)$ obtenemos nuevamente el vacío.

Una variación del argumento nos permite concluir que:

Proposición 4.38: Si κ es débilmente de Mahlo entonces es κ-débilmente inaccesible.

Demostración: El método funciona casi exactamente como hemos descrito: Sea $E := \{\mu < \kappa : \mu \text{ es regular}\}$ y sea $C_0 := \kappa$, claramente C_0 es c.n.a. luego dado el c.n.a. C_α definamos $C_{\alpha+1}$ como los puntos límite del conjunto $C_\alpha \cap E$ que es estacionario por definición y que es c.n.a. por construcción. Si λ es límite y $\lambda < \kappa$, entonces $C_\lambda := \bigcap_{\delta<\kappa} C_\delta$ es c.n.a.

Finalmente nótese que $R \cap C_\alpha$ siempre consta de los cardinales α-débilmente inaccesibles menores que κ, y que todos conforman series cofinales a κ, de modo que κ es α-débilmente inaccesible para todo $\alpha < \kappa$; ergo es κ-débilmente inaccesible. □

Nótese que nuestro método de conseguir puntos fijos no funciona pues $\beth$ no es normal, y de hecho, una sucesión que converja a κ debe tener longitud κ; por lo tanto, incluso si $\beth_\delta$ existe para todo $\delta < \kappa$ no podemos concluir que $\beth_\kappa$ exista (como conjunto).

Finalmente, igual podemos ampliar nuestra definición de cardinales de Mahlo:

Definición 4.39: Definimos las siguientes clases:

$$\begin{aligned} M_0 &:= \{\kappa \in \Omega_{\text{Card}} : \kappa \text{ es débilmente inaccesible}\} \\ M_{\alpha+1} &:= \{\kappa \in M_\alpha : \{\mu < \kappa : \mu \in M_\alpha\} \text{ es estacionario en } \kappa\} \\ M_\lambda &:= \bigcap_{\delta<\lambda} M_\delta. \end{aligned}$$

Los elementos de la clase M_α se dicen cardinales α-débilmente de Mahlo. En particular, los cardinales débilmente de Mahlo son los 1-débilmente de Mahlo bajo ésta definición.

§4.2.2 El teorema de Silver. Toda esta subsección depende del AE. El objetivo es deducir el teorema de Silver, que señala que en cierta forma se pueden deducir la veracidad de los axiomas HGC y HCS recursivamente. Para ello definamos

$$\begin{aligned} \text{HGC}(\kappa) &\equiv \kappa \text{ es infinito } \implies 2^\kappa = \kappa^+ \\ \text{HCS}(\kappa) &\equiv \kappa \text{ es singular } \implies \kappa^{\operatorname{cf}\kappa} = \kappa^+. \end{aligned}$$

Es claro que $\text{HGC}(\kappa) \implies \text{HCS}(\kappa)$.

Definición 4.40: Sean f, g funciones de dominio λ un ordinal límite. Entonces se dicen *casi disjuntas* si existe $\alpha < \lambda$ tal que para todo $\beta \geq \alpha$ se cumple que $f(\beta) \neq g(\beta)$; equivalentemente, son casi disjuntas si coinciden en un conjunto acotado.

Lema 4.41: Sea κ un álef singular con $\mu := \operatorname{cf}\kappa > \aleph_0$ y supongamos que $\aleph_\alpha^\mu < \kappa$ para todo $\alpha < \mu$. Sea $(A_\alpha)_{\alpha<\mu}$ una sucesión de conjuntos tales que $|A_\alpha| < \aleph_\alpha$ para todo $\alpha < \mu$, y sea F una familia de funciones casi disjuntas dos a dos con

$$F \subseteq \prod_{\alpha<\mu} A_\alpha,$$

entonces $|F| \leq \kappa$.

Demostración: Podemos suponer que $A_\alpha \subseteq \omega_\alpha$. Sea S_0 el conjunto de los ordinales límite $0 < \alpha < \mu$, el cual es un conjunto estacionario. Para todo $f \in F$ y todo $\lambda \in S_0$ sea

$$f^*(\lambda) := \text{mín}\{\beta : f(\alpha) < \omega_\beta\}$$

la cual es una función regresiva, por lo que, por el teorema de Fodor, existe γ tal que $S := (f^*)^{-1}[\{\gamma\}]$ es estacionario, luego $f|_S \colon S \to \omega_\gamma$; y más aún, podemos elegir γ (y por tanto S) como el mínimo que cumple ésto. Definamos $\varphi(f) := f|_S$.

Sean $f, g \in F$ distintas, luego $\varphi(f) \neq \varphi(g)$ dado que son casi disjuntas (y los conjuntos estacionarios no están acotados). Luego φ es una inyección de dominio F y se cumple que

$$|F| \leq 2^\mu \cdot \sum_{\gamma<\mu} \aleph_\gamma^\mu \leq \kappa,$$

donde empleamos que $\aleph_\gamma^\mu < \kappa$ y donde el $2^\mu < \kappa$ es una cota para la cantidad de conjuntos estacionarios sobre μ. □

Lema 4.42: Sea κ un álef singular con $\mu := \operatorname{cf} \kappa > \aleph_0$ y supongamos que $\aleph_\alpha^\mu < \kappa$ para todo $\alpha < \mu$. Sea $F \subseteq \prod_{\alpha<\mu} A_\alpha$ una familia de funciones casi disjuntas dos a dos, donde el conjunto $T := \{\alpha < \mu : |A_\alpha| \leq \aleph_\alpha\}$ es estacionario, entonces $|F| \leq \kappa$.

Pista: Basta redefinir $S_0 := \{\lambda \in T : \lambda \text{ es límite}\}$, notar que también es estacionario y seguir la demostración anterior. □

Lema 4.43: Sea κ un álef singular con $\mu := \operatorname{cf} \kappa > \aleph_0$ y supongamos que $\aleph_\alpha^\mu < \kappa$ para todo $\alpha < \mu$. Sea $f \colon \mu \to \Omega_{\mathrm{Ord}}$ tal que $f(\alpha) < \omega_{\alpha+1}$ para todo $\alpha < \mu$. Sea $F \subseteq \operatorname{Func}(\kappa, \Omega_{\mathrm{Ord}})$ una familia de funciones casi disjuntas, y sea

$$F_f := \{g \in F : \exists T \subseteq \mu \text{ estacionario } \forall \alpha \in T\ g(\alpha) < f(\alpha)\}.$$

Entonces $|F_f| \leq \kappa$.

Demostración: Fijemos un conjunto T estacionario en μ. Sea

$$F_f^T := \{g \in F : \forall \alpha \in T\ g(\alpha) < f(\alpha)\},$$

que tiene cardinalidad $\leq \kappa$ por el lema anterior. Luego $|F| \leq 2^\mu \cdot \kappa = \kappa$. □

Lema 4.44: Sea κ un álef singular con $\mu := \operatorname{cf}\kappa > \aleph_0$ y supongamos que $\aleph_\alpha^\mu < \kappa$ para todo $\alpha < \mu$. Sea $(A_\alpha)_{\alpha<\mu}$ una sucesión de conjuntos con $|A_\alpha| \leq \aleph_{\alpha+1}$ para todo $\alpha < \mu$ y sea $F \subseteq \prod_{\alpha<\mu} A_\alpha$ una familia de funciones casi disjuntas. Entonces $|F| \leq \kappa^+$.

DEMOSTRACIÓN: Sea U un ultrafiltro en μ que extiende al filtro $\mathbf{cna}(\mu)$; así pues, todos sus elementos son conjuntos estacionarios. Sin perdida de generalidad sean $A_\alpha \subseteq \omega_{\alpha+1}$ y definamos la relación $\prec$ sobre F como:

$$f \prec g \iff \{\alpha < \mu : f(\alpha) < g(\alpha)\} \in U$$

Probaremos que $\preceq$ determina un orden lineal:

1. Transitividad: Si $f \prec g$ y $g \prec h$ entonces

$$\{\alpha : f(\alpha) < h(\alpha)\} \supseteq \{\alpha : f(\alpha) < g(\alpha)\} \cup \{\alpha : g(\alpha) < h(\alpha)\} \in U$$

   lo que prueba que $f \prec h$.

2. Conexión: Sean $f, g \in F$ distintos. Como son casi disjuntos se cumple que $\{\alpha < \mu : f(\alpha) = g(\alpha)\}$ está acotado, luego tiene cardinalidad $< \mu$, pero μ es regular, así que el conjunto no puede ser estacionario y no puede estar en U. Finalmente, como U es un ultrafiltro se ha de cumplir que alguno de los dos conjuntos:

$$\{\alpha < \mu : f(\alpha) < g(\alpha)\}, \qquad \{\alpha < \mu : f(\alpha) > g(\alpha)\}$$

   está en U.

Fijemos un $f \in F$. Si $g \prec f$, entonces

$$g \in F_f := \{h \in F : \exists T \text{ estacionario } \forall \alpha \in T\ h(\alpha) < f(\alpha)\},$$

de modo que $O_\prec(f) \subseteq F_f$ y $|F_f| \leq \kappa < \kappa^+$. Finalmente, por el teorema 3.55 se concluye que $|F| \leq \kappa^+$. □

Teorema 4.45 – *Teorema de Silver*: Sea κ un álef singular con $\mu := \operatorname{cf}\kappa > \aleph_0$ y supongamos que $\aleph_\alpha^\mu < \kappa$ para todo $\alpha < \mu$. Si el conjunto $\{\alpha < \mu : \mathrm{HGC}(\alpha)\}$ es estacionario (en particular, si $\mathrm{HGC}(\alpha)$ para todo álef $\alpha < \mu$), entonces $\mathrm{HGC}(\kappa)$.

Demostración: Para todo $\alpha < \mu$ sea $A_\alpha := \mathcal{P}\omega_\alpha$, de modo que $|A_\alpha| = \aleph_{\alpha+1}$ para $\alpha \in T$ donde T es estacionario (y en particular, no está acotado) en μ. Para todo $X \subseteq \kappa$ definamos $f_X \in \prod_{\alpha\in T} A_\alpha$ como

$$f_X(\alpha) := X \cap \omega_\alpha.$$

Nótese que si $X \neq Y \subseteq \kappa$, entonces f_X, f_Y son casi disjuntas pues si α es el primer ordinal tal que $X \cap \omega_\alpha \neq Y \cap \omega_\alpha$, entonces $f_X(\beta) \neq f_Y(\beta)$ para todo $\beta \geq \alpha$. Luego $F := \{f_X : X \subseteq \kappa\}$ es una familia de funciones casi disjuntas y, por el lema anterior, $|F| \leq \kappa^+$. Finalmente hemos visto que $2^\kappa \leq \kappa^+$, pero $2^\kappa \geq \kappa^+$ por el teorema de Cantor, lo que concluye la igualdad. □

5

Teoría combinatoria de conjuntos

5.1 Teoría de Ramsey

Vamos a comenzar éste capítulo con una notación muy importante:

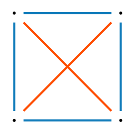
Definición 5.1 – *Notación flecha de Erdős-Rado*: La expresión «$\kappa \to (\mu)^r_s$» significa que para todo conjunto S de cardinalidad κ y toda partición $C_0 \cup \cdots \cup C_{s-1} = [S]^r$, siempre existe un subconjunto $H \subseteq S$, llamado *homogéneo*, de cardinalidad μ, tal que $[H]^r \subseteq C_i$ para algún $0 \leq i \leq s-1$. Intuitivamente pensamos que «pintamos» los conjuntos de r elementos de S con s colores, existe un conjunto H de cardinalidad μ que es «monocromático».

Una variación es que $\kappa \to (\mu_0, \dots, \mu_{s-1})^r$ significa que para todo S de cardinalidad κ y toda partición $C_0 \cup \cdots \cup C_{s-1} = [S]^r$ existe $H \subseteq S$ tal que $[H]^r \subseteq C_i$ y $|H| = \mu_i$.

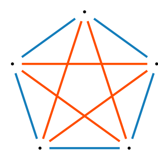
Varios problemas de combinatoria pueden expresarse en el lenguaje de la notación flecha de Erdős-Rado.

Ejemplo.
- Para todo κ, r, s se cumplen $\kappa \to (r)^r_s$, $\kappa \to (\kappa)^r_1$ y si $n \in \mathbb{N}_{>1}$ se cumple $n \nrightarrow (n)^{n-1}_s$. Si $\mu > \kappa$, entonces $\kappa \nrightarrow (\mu)^r_s$.
- Hay una manera muy visual de representar los problemas del estilo $n \xrightarrow{?} (\mu)^2_s$, pues los subconjuntos de 2 elementos de n pueden ver-

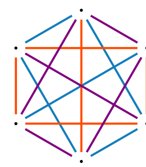
se como nodos entre pares de puntos. Así pues, las siguientes figuras proponen contraejemplos formales:



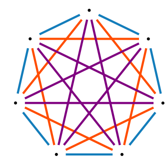
$4 \nrightarrow (3)^2_2$



$5 \nrightarrow (3)^2_2$



$6 \nrightarrow (3)^2_3$



$7 \nrightarrow (3)^2_3$

Proposición 5.2: Supongamos que $\kappa \to (\mu)^r_s$ donde todos los números son no nulos. Si $\kappa' \geq \kappa$, $\mu' \leq \mu$, $r' \leq r$ y $s' \leq s$, entonces $\kappa' \to (\mu')^{r'}_{s'}$.

Del ejemplo de $6 \nrightarrow (3)^2_3$ y de $7 \nrightarrow (3)^2_3$, abstraiga y generalice el siguiente resultado:

Proposición 5.3: Para todo $n \in \mathbb{N}_{\geq 2}$ se satisface que $2n \nrightarrow (3)^2_n$ y $2n+1 \nrightarrow (3)^2_n$.

Teorema 5.4 – *Teorema finito de Ramsey*: Para todo $k, r, s \in \mathbb{N}_{\neq 0}$ existe $n \in \mathbb{N}_{\neq 0}$ tal que $n \to (k)^r_s$.

Demostración: La demostración emplea una serie de inducciones anodadas. Comenzaremos por ver el caso $s = 2$. Probaremos que dados $p, q, r \in \mathbb{N}_{\neq 0}$ existe $n \in \mathbb{N}_{\neq 0}$ tal que $n \to (p, q)^r_2$ por inducción sobre r: Para el caso base $r = 1$ elijamos $n := p + q - 1$, de modo que si $|S| = n$ y $[S]^1 \approx S = A_0 \cup A_1$, luego o bien $|A_0| \geq p$ (en cuyo caso, elijamos $H = A_0$) o bien $|A_1| \geq q$ (en cuyo caso, elijamos $H = A_1$).

En general, denotemos $R(p, q; r)$ como el mínimo n tal que $n \to (p, q)^r_2$. El caso inductivo $r + 1$ lo haremos por inducción fuerte sobre $(p + q)$: Sea $|S| = n > 0$ (donde n no está fijo) y $[S]^{r+1} = A_0 \cup A_1$. Si $p < r$ (o $q < r$ resp.) entonces elejimos $|H| = p$ ($|H| = q$ resp.) y notamos que $[H]^r = \varnothing$. Si $p = q = r$, entonces algún $A_i \neq \varnothing$ y elegimos $H \in A_i$. En particular, podemos elegir $p > r$ y $q > r$, lo cual demuestra el caso base, y suponer que el enunciado vale p', q' (sin fijar) tales que $p' + q' < p + q$.

Sea $a \in S$ y sea $B_0 \cup B_1 = [S_{\neq a}]^r$ una partición con $X \in B_i$ syss $X \cup \{a\} \in A_i$. Ahora podemos elegir n tal que $n - 1 = R(p', q'; r)$ (nótese que n está fijo en función de p', q'), luego existe $H \subseteq S$ tal que alguno es cierto:

(a) $[H_{\neq a}]^r \subseteq B_0$ y $|H_{\neq a}| \geq p'$.

(b) $[H_{\neq a}]^r \subseteq B_1$ y $|H_{\neq a}| \geq q'$.

De modo que todos los subconjuntos $X \in [H_{\neq a}]^r$ de r elementos de $H_{\neq a}$ tienen el mismo color, y en consecuente, los $X \cup \{a\} \in [H]^{r+1}$ también; basta probar que los $Y \in [H]^{r+1}$ con $a \notin Y$ también.

En el caso de (a): Por hipótesis inductiva fijemos $p' := R(p-1, q; r+1)$. Luego, como se cumple (a), existe $H' \subseteq H_{\neq a}$ tal que $|H'| \geq p-1$ y $[H']^{r+1} \subseteq A_0$ (en cuyo caso $H := H' \cup \{a\}$ basta), o bien existe $H'' \subseteq H_{\neq a}$ tal que $|H''| \geq q$ y $[H'']^{r+1} \subseteq A_1$ (en cuyo caso $H := H''$ basta).

En el caso de (b): Análogamente se cumple para $q' := R(p, q-1; r+1)$

Así pues, definiendo $n := R(p', q'; r+1)$ vemos, por los casos anteriores, que se cumple $n \to (p, q)_2^{r+1}$ lo que completa la inducción sobre $(p+q)$, y también sobre r.

¿Por qué se puede elegir dicho n?

Finalmente, demostraremos el enunciado del teorema por inducción sobre s: Nótese que el caso $s = 1$ es trivial (ver ejemplos) y que hemos probado $s = 2$ (con $p = q := k$).

Sea m tal que se satisface que $m \to (k)_s^r$. Sea $|S| = n > 0$ (n sin fijar), luego consideremos una partición $A_0 \cup \cdots \cup A_s = [S]^r$ de $(s+1)$ colores. Podemos definir:

$$B_0 := \bigcup_{i=0}^{s-1} A_i, \qquad B_1 := A_s,$$

y notar que forman una partición de 2 colores. Definamos $n := R(l, l; r)$ (con l sin fijar), luego existe $H' \subseteq S$ homogéneo en el sentido de que $|H'| \geq l$ y $[H']^r \subseteq B_i$. Si $[H']^r \subseteq B_0$, entonces fijamos $l := \max\{m, k\}$, de modo que existe $H \subseteq H'$ con $|H| = k$ tal que $[H]^r \subseteq A_i$ con $i = 0, \ldots, s-1$; es decir, $H \subseteq S$ es el que conjunto homogéneo que buscabamos. Si $[H']^r \subseteq B_1 = A_s$, entonces H' también es homogéneo respecto de nuestros $(s+1)$ colores. Ésto concluye la inducción. $\square$

Los valores que toma $R(p, q; r)$ se llaman *números de Ramsey*; a veces se denota $R(p, q) := R(p, q; 2)$. Éstos números son generalmente difícil de calcularse y crecen rapidamente; como vimos en los (contra)ejemplos no es tan difícil comprobar que determinado n satisface $n \not\to (k)_s^2$, pues basta construir un cierto grafo ingenioso, pero demostrar que $n \to (k)_s^2$ es un problema complicado, y por tanto, lo es bastante el calcular los números de Ramsey.

Vamos a dar un ejemplo conocido:

Teorema 5.5 (de la amistad): $6 \to (3)^2_2$.

El nombre se debe a la siguiente analogía: Admitiendo que «conocerse» es una relación simétrica, en un grupo de 6 personas siempre existen 3 que se conocen o se desconocen mutuamente.

Demostración del teorema de la amistad.

La primera pregunta de la teoría combinatoria de conjuntos sería si es que un análogo del teorema finito de Ramsey se cumple, y hemos de ver que hay ciertas restricciones al trabajar con infinitos.

Teorema 5.6: Sean $\aleph_0 \leq r \leq \mu \leq \kappa$ álefs. Entonces $\kappa \nrightarrow (\mu)^r_s$.

Demostración: Identifiquemos el conjunto $[\kappa]^r$ con las funciones $f\colon r \to \kappa$ estrictamente crecientes. Así, definimos sobre $[\kappa]^r$ la siguiente relación de equivalencia:

$$f \sim g \iff \{\alpha < r : f(\alpha) \neq g(\alpha)\} \text{ es finito.}$$

Como $|[\kappa]^r| = \kappa$ está bien ordenado podemos elegir un conjunto $S \subseteq [\kappa]^r$ que contenga a un elemento por cada clase de equivalencia, y denotamos $r(f)$ al único elemento relacionado con f que está en S. Así pues, definimos la coloración:

$$\begin{aligned} F\colon [\kappa]^r &\longrightarrow 2 \\ f &\longmapsto \begin{cases} 0, & \{\alpha < r : f(\alpha) \neq r(f)(\alpha)\} \text{ tiene cardinalidad par} \\ 1, & \{\alpha < r : f(\alpha) \neq r(f)(\alpha)\} \text{ tiene cardinalidad impar} \end{cases} \end{aligned}$$

Supongamos, por contradicción, que existe $H \subseteq \kappa$ homogéneo respecto a F tal que $|H| \geq r$; en particular, H ha de ser infinito y $[H]^r \neq \varnothing$. Luego, podemos construir $f \in [H]^r$ tal que para todo $\alpha < r$ existe $h \in H$ tal que $f(\alpha) < h < f(\alpha + 1)$. Consideremos el conjunto $S := \{\alpha < r : f(\alpha) \neq r(f)(\alpha)\}$, entonces elijamos $\beta \notin S$ y construyamos $g \in [H]^r$ exactamente igual a f en todos los puntos salvo en β en donde $f(\beta) < g(\beta) = h < f(\beta+1)$. Finalmente notamos que $F(f) \neq F(g)$ en cualquier caso lo que contradice la homogeneidad de H. □

El primer resultado interesante es el siguiente:

Teorema 5.7 – *Teorema de Ramsey*: Para todo $r, s \in \mathbb{N}_{\neq 0}$ se cumple que $\aleph_0 \to (\aleph_0)^r_s$.

Demostración: Fijaremos el conjunto numerable como $\mathbb{N}$. Lo haremos por inducción sobre r, donde el caso base $r = 1$ se reduce al principio del palomar. También será útil sustituir la partición por una función $F\colon [\mathbb{N}]^{r+1} \to \{1, \ldots, s\}$, y así, un conjunto $H \subseteq \mathbb{N}$ es homogéneo si $F \upharpoonright [H]^{r+1}$ es constante. Para todo $a \in \mathbb{N}$ definimos la siguiente coloración:

$$\begin{aligned} F_a\colon [\mathbb{N}_{\neq a}]^r &\longrightarrow \{1, \ldots, s\} \\ X &\longmapsto F(X \cup \{a\}) \end{aligned}$$

Que, por hipótesis inductiva, admite un conjunto infinito homogéneo. Pero más aún, para todo $S \subseteq \mathbb{N}$ infinito y todo $a \in \mathbb{N}$ existe un subconjunto infinito $H_a^S \subseteq S_{\neq a}$ que es homogéneo respecto a la coloración F_a. Así, aprovechamos ésto para construir un par de sucesiones $(a_n)_{n\in\mathbb{N}}$ de naturales y $(S_n)_{n\in\mathbb{N}}$ de subconjuntos de $\mathbb{N}$ por recursión: $S_0 := \mathbb{N}$ y $a_0 := 0$; $S_{n+1} := H_{a_n}^{S_n}$ y a_{n+1} es el mínimo elemento de S_{n+1} mayor que a_n. Nótese que S_{n+1} no contiene a $a_0, \ldots, a_n$ y de que $S_0 \supset S_1 \supset S_2 \supset \cdots$, por lo que, como S_{n+1} es homogéneo respecto a F_{a_n}, entonces $\{a_i : i > n\}$ también es homogéneo y la función vale $G(a_n)$ allí. Así pues, $G\colon \{a_n\}_{n\in\mathbb{N}} \to \{1, \ldots, s\}$, por lo que, por el principio del palomar, existe $H \subseteq \{a_n\}_{n\in\mathbb{N}}$ infinito tal que $G \upharpoonright H$ es constante. Finalmente, H es homogéneo respecto a F puesto que dado $x_1 < \cdots < x_{r+1}$ en H se tiene que $F(\{x_1, \ldots, x_{r+1}\}) = F_{x_1}(\{x_2, \ldots, x_{r+1}\}) = G(x_1)$. □

Naturalmente, uno esperaría que un teorema similar aplicase para $\aleph_1$, pero veremos que de hecho falla estrepitosamente:

Teorema (AE($\mathbb{R}$)) 5.8: $2^{\aleph_0} \nrightarrow (\aleph_1)^2_2$ y, en consecuencia, $\aleph_1 \nrightarrow (\aleph_1)^2_2$.

Demostración: Consideremos a $\mathbb{R}$, el cual $|\mathbb{R}| = 2^{\aleph_0}$. Con elección vemos que $\mathbb{R}$ posee algún buen orden $\preceq$ y así consideramos la siguiente coloración:

$$A_0 := \{\{x, y\} \in [\mathbb{R}]^2 : x \prec y, x < y\}, \qquad A_1 := \{\{x, y\} \in [\mathbb{R}]^2 : x \prec y, x > y\}.$$

Supongamos que existe un conjunto $H \subseteq \mathbb{R}$ no numerable homogéneo. Luego, H hereda el buen orden en $\mathbb{R}$ y por lo tanto, existe un único ordinal γ y un único $f\colon \gamma \to H$ isomorfismo de orden. Nótese además que $\gamma \geq \omega_1$.

Si $[H]^2 \subseteq A_0$, entonces para todo $\alpha < \beta < \gamma$ se cumple que $f(\alpha) < f(\beta)$; de modo que $\{\big(f(\alpha), f(\alpha + 1)\big) : \alpha < \gamma\}$ es una familia no numerable de conjuntos abiertos disjuntos dos a dos de $\mathbb{R}$, pero ésto es absurdo. □

Citar resultado del libro de topología.

En general, el resultado de Ramsey es interesante, entre otras razones porque varias relaciones combinatoriales fallan entre álefs. Veremos un ejemplo:

Lema 5.9: Para todo álef κ se cumple que $2^\kappa \nrightarrow (\aleph_0)^2_\kappa$ y, más fuerte aún, $2^\kappa \nrightarrow (3)^2_\kappa$.

Demostración: Sea $S := \operatorname{Func}(\kappa; \{0,1\})$, y consideremos la coloración $F\colon [S]^2 \to \kappa$ dada por

$$F(\{f,g\}) := \min\{\alpha < \kappa : f(\alpha) \neq g(\alpha)\}.$$

Luego, es fácil ver que si $f, g, h \in S$ son distintos, entonces no puede ocurrir que $F(\{f,g\}) = F(\{f,h\}) = F(\{g,h\})$. □

Lema 5.10: El conjunto $S := \operatorname{Func}(\kappa; \{0,1\})$ con orden lexicográfico no posee una sucesión de largo κ^+ que sea estrictamente monótona.

Demostración: En primer lugar, recordemos que aquí, orden lexicográfico significa que dados f, g distintos $f \prec g$ significa que para el mínimo $\alpha < \kappa$ tal que $f(\alpha) \neq g(\alpha)$ se cumple que $f(\alpha) < g(\alpha)$. Sea, por contradicción, $f_-\colon \kappa^+ \to S$ una sucesión estrictamente monótona y, sin perdida de generalidad, creciente. Sea $\gamma \leq \kappa$ el mínimo ordinal tal que el conjunto $\{f_\alpha \upharpoonright \gamma : \alpha < \kappa^+\}$ tiene cardinalidad κ^+, y sea Z un subconjunto de la sucesión de cardinalidad κ^+ tal que $f|_\gamma \neq g|_\gamma$ para todo $f, g \in Z$ distintos. Podemos reajustar los índices de manera que $f_\alpha \upharpoonright \gamma \neq f_\beta \upharpoonright \gamma$ para todo $\alpha \neq \beta$.

Para todo $\alpha < \kappa^+$ definamos δ_α como el mínimo ordinal tal que $f_\alpha \upharpoonright \delta_\alpha = f_{\alpha+1} \upharpoonright \delta_\alpha$, $f_\alpha(\delta_\alpha) = 0$ y $f_{\alpha+1}(\delta_\alpha) = 1$; nótese que $\delta_\alpha < \gamma \leq \kappa^+$. Luego, necesariamente existe δ tal que $\delta = \delta_\alpha$ para κ^+ ordinales α. Si $\delta = \delta_\alpha = \delta_\beta$ y $f_\alpha \upharpoonright \delta = f_\beta \upharpoonright \delta$, entonces $f_\alpha \prec f_{\beta+1}$ y $f_\beta \prec f_{\alpha+1}$, por lo que $f_\alpha = f_\beta$; por lo tanto, el conjunto

$$\{f_\alpha \upharpoonright \delta : \alpha < \kappa^+\}$$

tiene cardinalidad κ^+ y $\delta < \gamma$, lo que contradice la minimalidad de γ. □

Con ésto, podemos generalizar el teorema 5.8:

Lema (AE) 5.11: Para todo κ álef, $2^\kappa \nrightarrow (\kappa^+)^2$.

Demostración: Sea $S := \operatorname{Func}(\kappa; \{0,1\})$ y sea $S = \{f_\alpha\}_{\alpha<\mu}$, donde μ es un álef por AE. Denotemos $\preceq$ el orden lexicográfico sobre S y $\leq$ el buen orden usual sobre μ como ordinal, y construyamos la siguiente coloración de $[S]^2$:

$$A_0 := \{\{f_\alpha, f_\beta\} \in [S]^2 : \alpha < \beta, f_\alpha \prec f_\beta\},$$

$$A_1 := \{\{f_\alpha, f_\beta\} \in [S]^2 : \alpha < \beta, f_\alpha \succ f_\beta\}.$$

Sea $H \subseteq \mu$ un conjunto homogéneo de cardinalidad κ^+. Luego, los subíndices de sus elementos le permiten enumerarlos con un ordinal y resulta ser una sucesión estrictamente monótona en el orden lexicográfico, lo cual es absurdo por el lema anterior. □

Teorema (AE) 5.12 – *Teorema de Erdős-Rado*: Para todo $n \in \mathbb{N}$ y se cumple que $\beth_n^+ \to (\aleph_1)_{\aleph_0}^{n+1}$. En particular, $(2^{\aleph_0})^+ \to (\aleph_1)_{\aleph_0}^2$.

Demostración: El caso $n = 0$ es claro y probaremos el caso $n = 1$ pues el resto es bastante similar. Sea $\mu := (2^{\aleph_0})^+$ y sea $F\colon [\mu]^2 \to \mathbb{N}$ una coloración arbitraria. Para todo $a \in \mu$ definamos:

$$\begin{aligned} F_a\colon \mu_{\neq a} &\longrightarrow \mathbb{N} \\ x &\longmapsto F(\{a, x\}) \end{aligned}$$

Probaremos que existe un subconjunto $A \subseteq \mu$ de cardinalidad $2^{\aleph_0}$ tal que para todo $C \subseteq A$ numerable y todo $u \in \mu \setminus C$ existe $v \in A \setminus C$ tal que $F_u \upharpoonright C = F_v \upharpoonright C$. Para hacerlo construyamos una sucesión $(A_\alpha)_{\alpha<\omega_1}$ de conjuntos por recursión transfinita como prosigue:

- $A_0 \subseteq \mu$ es un conjunto arbitrario de cardinalidad $2^{\aleph_0}$.
- $A_{\alpha+1} \supseteq A_\alpha$ es un conjunto de cardinalidad $2^{\aleph_0}$ tal que para todo $C \subseteq A_\alpha$ numerable y todo $u \in \mu \setminus C$ existe $v \in A_{\alpha+1} \setminus C$ tal que $F_u \upharpoonright C = F_v \upharpoonright C$. Éste conjunto existe puesto que la cantidad de v's que hemos de agregar está acotada por
$$|A_{\alpha+1} \setminus A_\alpha| \leq \left| \bigcup_{C \in [A_\alpha]^{\aleph_0}} \operatorname{Func}(C; \mathbb{N}) \right| \leq 2^{\aleph_0} \cdot |C|^{\aleph_0} = 2^{\aleph_0}.$$
- $A_\lambda := \bigcup_{\delta<\lambda} A_\delta$.

Finalmente $A := \bigcup_{\alpha<\omega_1} A_\alpha$ satisface lo deseado.

Fijemos $a \in \mu \setminus A$. Entonces construyamos una sucesión $(x_\alpha)_{\alpha<\omega_1}$ en A por recursión transfinita como prosigue: Elijamos $x_0 \in A$ arbitrario y dados $\{x_\beta\}_{\beta<\alpha} =: C \subseteq A$ numerable, elijamos $x_\alpha \in A \setminus C$ tal que $F_{x_\alpha} \upharpoonright C = F_a \upharpoonright C$. Definamos $X := \{x_\alpha\}_{\alpha<\omega_1}$.

Ahora, definamos $G\colon X \to \mathbb{N}$ dado por $G(x) := F_a(x)$. Como el dominio de G tiene cardinalidad $\aleph_1$ y el codominio $\aleph_0$, entonces existe $H \subseteq X$ de cardinalidad $\aleph_1$ tal que G es constante en H. Sean $\{x_\alpha, x_\beta\} \in [H]^2$ con $\alpha < \beta$, entonces

$$F(\{x_\alpha, x_\beta\}) = F_{x_\beta}(x_\alpha) = F_a(x_\alpha) = G(x_\alpha),$$

lo que prueba que H es homogéneo y completa el caso $n = 1$.

Veamos el caso $n+1$: Sea $\mu := \beth_n^+$ y sea $F\colon [\mu]^{n+1} \to \mathbb{N}$ una coloración. Para todo $a \in \mu$ definamos $F_a\colon [\mu_{\neq a}]^n \to \mathbb{N}$ por $F_a(X) := F(X \cup \{a\})$. Al igual que en el caso anterior, existe $A \subseteq \mu$ de cardinalidad $\beth_n$ tal que para todo $C \subseteq A$ de cardinalidad $\leq \beth_{n-1}$ y todo $u \in \mu \setminus C$ existe $v \in A \setminus C$ tal que $F_u \upharpoonright [C]^n = F_v \upharpoonright [C]^n$. Al igual que antes, fijando $a \in \mu \setminus A$ construimos una sucesión $X := \{x_\alpha : \alpha < \beth_{n-1}^+\} \subseteq A$ por recursión así: $x_0 \in A$ arbitrario y dado $\{x_\beta : \beta < \alpha\} =: C \subseteq A$ se elije $x_\alpha \in A \setminus C$ tal que $F_{x_\alpha} \upharpoonright [C]^n = F_a \upharpoonright [C]^n$.

Finalmente definimos $G\colon [X]^n \to \mathbb{N}$ dado por $G(S) := F_a(S)$ y, por hipótesis inductiva, existe $H \subseteq X$ de cardinalidad $\aleph_1$ homogéneo respecto a G, y se puede comprobar que también es homogéneo respecto a F. □

El resultado anterior admite una generalización adicional, mediante la siguiente notación:

$$\exp_0(\kappa) := \kappa, \qquad \exp_{n+1}(\kappa) := 2^{\exp_n(\kappa)}.$$

Teorema (AE) 5.13 (Erdős-Rado): Para todo $n \in \mathbb{N}$ y todo álef κ se cumple que $\exp_n(\kappa)^+ \to (\kappa^+)^{n+1}_\kappa$. En particular, $(2^\kappa)^+ \to (\kappa^+)^2_\kappa$.

Antes de seguir, nótese que la definición original es una pregunta que sólo depende de *cardinalidad*, pero es útil también reforzar la pregunta:

Definición 5.14 – *Notación flecha ordinal*: Sean κ, r, s cardinales. Se denota «$\kappa \to (\lambda)^r_s$», donde λ es un ordinal (límite), si para toda coloración $F\colon [\kappa]^r \to s$ existe un conjunto $H \subseteq \kappa$ homogéneo cuyo tipo de orden es λ.

Así mismo, $\kappa \to (\lambda_0, \dots, \lambda_{s-1})^r$ significa que dada una coloración $F\colon [\kappa]^r \to s$ existe $H \subseteq \kappa$ tal que $F \upharpoonright [H]^r$ es constante, vale α y H tiene tipo de orden λ_α.

Así pues $\kappa \to (\omega)^r_s$ y $\kappa \to (\aleph_0)^r_s$ no son lo mismo.

Teorema 5.15 – *Teorema de Erdős-Dushnik-Miller*: Para todo álef κ se cumple $\kappa \to (\kappa, \omega)^2$.

Demostración: Sea $[\kappa]^2 = A \cup B$ una partición. Para todo $x \in \kappa$ definamos

$$B_x := \{y \in \kappa : x < y, \{x, y\} \in B\}.$$

Distinguimos dos casos:

a) Supongamos que para todo $X \in [\kappa]^\kappa$ existe $x \in X$ tal que $|B_x \cap X| = \kappa$.

   En éste caso, podemos construir H homogéneo infinito como prosigue: Definamos por recursión $X_0 := \kappa$ y $x_0 \in X_0$ tal que $|B_{x_0} \cap X_0| = \kappa$ en el caso base; $X_{n+1} := X_n \cap B_{x_n}$ y $x_{n+1} \in X_{n+1}$ tal que $|B_{x_{n+1}} \cap X_n| = \kappa$ (de modo que $x_{n+1} > x_n$). Así pues, sea $H := \{x_n : n \in \mathbb{N}\}$ es fácil notar que $[H]^2 \subseteq B$ (¿por qué?).

b) Supongamos que existe $S \in [\kappa]^\kappa$ tal que para todo $x \in S$ se cumple que $|B_x \cap S| < \kappa$.

   Si κ es un cardinal regular, entonces, por la propiedad anterior, podemos construir una sucesión $(x_\alpha)_{\alpha<\kappa}$ de elementos de S que es estrictamente creciente y tal que es homogéneo en A (ésto debido a que S siempre tiene κ elementos en A).

   Si κ es un cardinal singular con $\mu := \operatorname{cf} \kappa$, entonces sea $(\kappa_\alpha)_{\alpha<\mu}$ una sucesión creciente de cardinales regulares $> \mu$ que sea cofinal en κ; de modo que $\kappa_\alpha \to (\kappa_\alpha, \omega)^2$ por el caso anterior para todo $\alpha < \mu$. Supongamos que no existe H infinito tal que $[H]^2 \subseteq B$. Finalmente sea $S = \bigcup_{\alpha<\mu} S_\alpha$ una partición tal que $|S_\alpha| = \kappa_\alpha$ para todo $\alpha < \mu$. Por la inexistencia de H se satisface que para todo $\alpha < \mu$ necesariamente existe $K_\alpha \subseteq S_\alpha$ de cardinalidad κ_α tal que $[K_\alpha]^2 \subseteq A$ y tal que para todo $x \in K_\alpha$ se cumple que $|B_x \cap K_\alpha| < \kappa_\alpha$.

□

5.2 Árboles

Definición 5.16: Un *árbol* es un conjunto $(A, \leq)$ parcialmente ordenado tal que para todo $x \in A$ se cumple que $O_<(x)$ es un conjunto bien ordenado. Los elementos de un árbol se dicen *nodos*.

Para un árbol $(A, \leq)$ fijo, definimos:

1. $\mathrm{alt}_A(x) :=$ el tipo de orden de $O_<(x)$. A ésto le llamamos la *altura* del nodo x.
2. $\mathrm{Niv}_\alpha(A) := \{x \in A : \mathrm{alt}_A(x) = \alpha\}$. A éste le llamamos el *nivel* α-ésimo del árbol.
3. $\mathrm{alt}(A) := \sup\{\mathrm{alt}_A(x) + 1 : x \in A\}$. A ésto le llamamos la *altura* del árbol.

Una (α-)*rama* de un árbol es una cadena maximal (respecto a la inclusión) y es, por lo tanto, un conjunto bien ordenado con un tipo de orden α. Sea $\gamma := \mathrm{alt}(A)$, entonces a las γ-ramas se les dicen *caminos* del árbol.

Los nodos de altura 0 se dicen *semillas* del árbol. Un árbol se dice *conexo* si posee a lo más una semilla. Un subconjunto $S \subseteq A$ es un *subárbol* si para todo $x \in S$ y todo $y \in A$ tal que $y \leq x$ se cumple que $y \in S$. Dado un árbol A y una semilla $s \in A$, se dice que el subárbol $O_\geq(s) := \{x \in A : x \geq s\}$ es una *componente conexa* del árbol. Dado un nodo $x \in A$, se dice que otro nodo $y \in A$ es un *sucesor inmediato* de x si $x < y$ y no existe $z \in A$ tal que $x < z < y$.

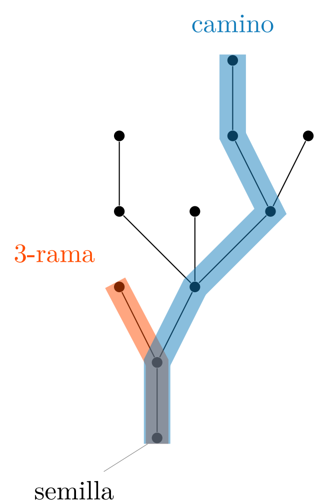


Figura 5.1. Un árbol conexo de altura 6.

Si la cuestión en la teoría de Ramsey es la existencia del κ tal que $\kappa \to (\mu)^r_s$, la cuestión entre los árboles es la (in)existencia de caminos. Una observación vital es que el AE (en particular, el lema de Zorn) permite notar que todo árbol posee ramas (y más generalmente, que toda cadena se extiende a una rama), pero no nos permite decidir si un árbol posee caminos.

Ejemplo.
- Sea X un conjunto arbitrario. Entonces podemos añadirle un orden parcial $\leq$ dado por que $x \leq y$ syss $x = y$. Ésto hace que $(X, \leq)$ sea un árbol tal que todos sus nodos son semillas y que todas sus componentes conexas sean singulares. A éste le llamamos un *árbol trivial*.
- Similar al ejemplo anterior, podemos tomar un conjunto arbitrario Y y un elemento $s \notin Y$. Luego definamos $X := Y \cup \{s\}$ con el orden $s \leq x$ para todo $x \in X$ y $y \leq z$ con $y, z \in Y$ syss $y = z$. Así, $(X, \leq)$ es un árbol conexo y $\mathrm{Niv}_1(X) = Y$.
- Sea $(X, \leq)$ un conjunto bien ordenado, entonces es un árbol que de hecho sólo posee una rama que es además un camino.
- Sea $\{(X_i, \leq_i)\}_{i\in I}$ una familia de árboles disjuntos dos a dos, entonces podemos definir: $\coprod_{i\in I} X_i$ como el conjunto $\bigcup_{i\in I} X_i$ con el orden
$$x \leq y \iff \exists i \in I\ x, y \in X_i \wedge x \leq_i y.$$
A ésto le llamamos *pegar árboles*.

Una acotación es que varios libros no distinguen entre árboles conexos y disconexos, y trabajan indistinctivamente entre ellos; sólo las propiedades esenciales:

Proposición 5.17: Sea $(A, \leq)$ un árbol, entonces existe la familia $\{C_i\}_{i\in I}$ de las componentes conexas de A forma una partición de A, que cada C_i es conexo como árbol, que se cumple
$$\mathrm{Niv}_\alpha(A) = \bigcup_{i\in I} \mathrm{Niv}_\alpha(C_i), \qquad \mathrm{alt}(A) = \sup_{i\in I} \mathrm{alt}(C_i),$$
y las ramas de A son ramas de alguna de sus componentes. En particular, los caminos de A son los caminos de alguna de sus componentes.

No obstante, es claro que los caminos de sus componentes no necesariamente son caminos del árbol original (ejemplifique). Otra cuestión es que si pegamos árboles, entonces las componentes conexas de la unión es la unión de las componentes conexas.

Respecto a la pregunta de que sí los árboles siempre poseen caminos, la respuesta es que no:

Ejemplo 2: Sea λ un ordinal límite, entonces sea $(\alpha_\delta)_{\delta<\gamma}$ una sucesión cofinal en λ (que bien puede ser la sucesión $0, 1, 2, \dots$) entonces considerando a α_δ como conjunto bien ordenado (luego como árbol) podemos pegar los árboles:

$$A := \coprod_{\delta<\gamma} \alpha_\delta,$$

de modo que A es un árbol de altura λ sin caminos. Ésto debido a que toda rama de A es necesariamente un ordinal $\alpha_\delta < \lambda$ el cual nunca es isomorfo a λ.

Nótese, sin embargo, que hay una serie de cualidades «degeneradas» en éste ejemplo. Una de ellas puede ser que el árbol es disconexo, pero igualmente se puede construir un ejemplo muy similar que sí es conexo (¡hágalo!). La principal peculiaridad es que si elegimos a $\lambda = \kappa$ un cardinal regular, entonces cada nivel tiene cardinalidad κ, en particular, cada nivel es infinito, pero ¿y si no lo fuese, tendría caminos?

Para ello introduzcamos un par de definiciones adicionales:

Definición 5.18: Se dice que un árbol A es un *κ-árbol* si tiene altura κ y para todo $\alpha < \kappa$ entonces $|\operatorname{Niv}_\alpha(A)| < \kappa$.

Se dice que un κ-árbol A está *bien podado* si es conexo y para todo $x \in A$ y todo $\alpha < \kappa$ existe $y \in A$ de altura α tal que $\{x, y\}$ es una cadena.

Intuitivamente un árbol bien podado es tal que desde cualquier punto se puede subir a cualquier altura.

En primer lugar, ateniéndonos a la pregunta de conexión:

Teorema (AE) 5.19: Sea κ un álef regular. Todo κ-árbol posee un κ-subárbol bien podado.

Demostración: Sea A un κ-árbol y definamos:

$$A' := \{x \in A : |O_>(x)| = \kappa\}.$$

Nótese que A' es un subárbol y es no vacío puesto que A posee $< \kappa$ componentes conexas y $|A| = \kappa$ ($\geq$ es claro, ¿por qué se tiene la igualdad?), luego alguna componente conexa tiene cardinalidad κ y está contenida en A'. De momento A' no es ni siquiera conexo, pero veremos que es el único defecto que tiene.

Sean $x \in A'$ y $\alpha < \kappa$ tales que $\operatorname{alt}_A(x) < \alpha$; queremos encontrar algún elemento en A' mayor que x a altura α. Sea $Y := \{y \in \operatorname{Niv}_\alpha A : y > x\} = \operatorname{Niv}_\alpha(A) \cap O_>(x)$, entonces:

$$O_>(x) = \{z \in A : z > x \wedge \operatorname{alt}_A(z) \leq \alpha\} \cup \{z \in A : z > x \wedge \operatorname{alt}_A(z) > \alpha\},$$

como $x \in A'$ el conjunto del lado izquierdo tiene cardinalidad κ y en el lado derecho el conjunto de la izquierda tiene cardinalidad $< \kappa$, luego el de la derecha tiene cardinalidad κ, pero

$$\{z \in A : z > x \wedge \operatorname{alt}_A(z) > \alpha\} = \bigcup_{y \in Y} O_>(y),$$

de modo que existe $y \in Y$ tal que $|O_>(y)| = \kappa$ y se cumple que $y \in A'$, $y > x$ y $\operatorname{alt}_A(y) = \alpha$ como se quería ver.

Finalmente reemplazando A' por cualquiera de sus componentes conexas llegamos al resultado buscado. □

Teorema (AEN) 5.20 (König): Todo $\aleph_0$-árbol posee caminos.

DEMOSTRACIÓN: Por el teorema anterior, podemos suponer que el árbol A está bien podado. Luego, y empleando AEN, construimos una sucesión por recursión, definiendo x_0 como la única semilla de A y $x_{n+1} \in \operatorname{Niv}_{n+1}(A)$ como cualquier elemento tal que $x_n < x_{n+1}$ (por definición de bien podado). Finalmente $C := \{x_n : n \in \mathbb{N}\}$ es un camino. □

Ésto se puede generalizar:

Teorema (AE) 5.21 (König): Sea κ un álef regular y $\mu < \kappa$ un cardinal. Si A es un árbol de altura κ cuyos niveles tienen cardinalidad $< \mu$, entonces A posee caminos. En particular, si sus niveles son finitos, entonces posee caminos.

DEMOSTRACIÓN: ... □

Pero, si cambiamos «finito» por «cardinalidad $< \kappa$», ¿sigue siendo válido? Para ello admitamos la siguiente definición:

Definición 5.22: Sea κ un álef, se dice que $(A, \leq)$ es un *κ-árbol de Aronszajn* si es un κ-árbol que no posee caminos.

Se dice que un álef κ posee la *propiedad de los árboles* si no existen κ-árboles de Aronszajn.

El lema de König dice pues que $\aleph_0$ posee la propiedad de los árboles. Siguiendo el ejemplo 2 es fácil ver que los cardinales singulares no poseen la propiedad de los árboles.

Teorema 5.23: Existen $\aleph_1$-árboles de Aronszajn.

Parte II.

Teoría de modelos y de las demostraciones

6

Introducción a la teoría de modelos

La teoría de modelos es en esencia el puente fundamental de la lógica con las matemáticas. En este capítulo trataremos de formalizar nociones previas, se advierte que la primera sección vendrá sobrecargada de definiciones y disprovista de pocos resultados.

6.1 Introducción a los lenguajes formales

Definición 6.1 – *Lenguaje, modelo*: Un *lenguaje* $\mathcal{L}$ es simplemente un conjunto numerable[a] de símbolos separados en cuatro tipos:

1. *Constantes*:
   a) *Constantes* individuales, usualmente denotadas c_i.
   b) *Funtores* n-ádicos denotados f_i^n.
   c) *Relatores* n-ádicos denotados R_i^n.
2. *Variables:* denotadas x_i.
3. *Conectores lógicos:* Los ya vistos $\neg$, $\implies$ y el cuantificador $\forall$.
4. *Símbolos auxiliares:* Los paréntesis y la coma.

Una *cadena de signos* ζ en $\mathcal{L}$ no es más que una tupla ordenada de símbolos. Si ζ_1, ζ_2 son cadenas de signos, denotamos $\zeta_1 \equiv \zeta_2$ syss las cadenas consistentes de los mismos símbolos en el mismo orden.

Una cadena de signos es una *expresión* si "está bien escrita" en el sentido de que si ocupamos un cuantificador, le prosigue una variable y luego otra cadena de signos, o si por ejemplo, no se escribe un funtor sin seguirlo de n *términos* (más adelante precisamos que es un término).

Se dice que M es un $\mathcal{L}$-*modelo* (o *estructura*) si consta de:

- Una clase U llamada *universo* de M.
- Para toda constante c se cumple que $\overline{c} \in U$.
- Para todo funtor f_i^n se cumple que $\overline{f}_i^n : U^n \to U$.
- Para todo relator R_i^n se cumple que $\overline{R}_i^n \subseteq U^n$.

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

También, para evitar confusiones, si c es una constante y $u \in U$ un elemento tales que $\overline{c}$ y u son el mismo elemento de U, lo denotaremos por $\overline{c} \equiv u$ para evitar confusiones pues "$=$" suele ser un símbolo de $\mathcal{L}$.

[a] Algunos llaman a éstos, un *lenguaje formal numerable*, pero en la práctica jamás tendremos que lidiar con lenguajes con no-numerables símbolos, y acotar la cantidad de símbolos será útil como se verá más adelante.

En la práctica nos permitiremos usar el resto de conectores lógicos identificándoles como abreviaciones de mezclas entre los ya presentes, es decir:

$$\alpha \lor \beta \equiv (\neg\alpha) \implies \beta, \quad \alpha \land \beta \equiv \neg(\neg\alpha \lor \neg\beta), \quad \exists x\, \phi \equiv \neg\forall x\, \neg\phi.$$

Ejemplo (lenguaje arbitrario). Digamos que $\mathcal{L}$ es un lenguaje con tres constantes p, j, d (léase Pedro, Juan y Diana), un funtor monádico P (léase "padre de") y dos relatores diádicos: $=$ (el igualador) y A (léase "son amigos"). Podríamos denotar algo como $Pd = j$ que se lee como "el padre de Diana es Juan" y Apj que se lee como "Pedro y Juan son amigos". Nótese que $Pd = j$ puede ser cierto, pero $Pd \not\equiv j$ pues no están conformados de los mismos signos.

Notación polaca. Si nuestro objetivo fuera reducir el lenguaje (la cantidad de símbolos, no significados, naturalmente), la verdad es que podemos forzar aún más nuestras condiciones y deshacernos de los símbolos auxiliares (paréntesis y comas), pues si f es un funtor, podemos obviarlos en $f(x_1, \dots, x_n) \equiv f x_1 \dots x_n$, de modo que por ejemplo no se escribe $a + b$ sino

$+ab$. Ésto tiene una ventaja pues por ejemplo expresiones como $a+b\cdot c$ que ocasionan confusión sobre si significa $a+(b\cdot c)$ o $(a+b)\cdot c$, eliminan duda al escribirse como $a+(b\cdot c) \equiv +a\cdot bc$ y $(a+b)\cdot c \equiv \cdot{+abc}$. En el siguiente ejemplo empleamos la notación polaca escribiendo $2+2=4 \equiv = +224$, pero considere que jamás la emplearemos en contextos comunes. La ventaja de la notación polaca es que nos permite definir adecuadamente la longitud de una expresión, de modo que los símbolos auxiliares no interfieran.

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 M como $\mathcal{L}$-modelo de universo $\mathbb{N}$ donde $M(\spadesuit) \equiv 0$, $M(S(t)) \equiv M(t)+1$, $M(\oplus(a,b)) \equiv M(a)+M(b)$ y $M(\sim) \equiv =$. 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. Algo digno de observar es que no requerimos de más de cuatro símbolos, y de hecho, sólo con $\spadesuit$ y S ya podemos formar todos los números naturales, luego podríamos dar un símbolo $\mathrm{f}(i,n)$ para denotar el i-ésimo funtor n-ádico y reducir aún más la cantidad de símbolos. Toda la aritmética de Peano puede describirse entonces con cuatro símbolos, pese a que posee numerables términos.

Sobre el igualador. En general, tal como exigimos que todo lenguaje posea conectores lógicos, también exigimos que todo lenguaje posea al menos un relator diádico, y que el primero de ellos sea el *igualador*, usualmente denotado "$=$". En todo modelo, debe darse que la interpretación del igualador sea una relación de equivalencia (i.e., reflexividad, simetría y transitividad de la igualdad). Ojo el igualador es un símbolo, de momento no nos permite extraer conclusiones como que $2+2=4$, lo único que sabemos es que es más débil que la equivalencia de cadenas de signos, de modo que lo único certero es que $2=2$, que $2+2=2+2$ y que $4=4$.

Definición 6.2: Se define $\mathcal{T}$ como la mínima clase (bajo inclusión) de cadenas de signos en $\mathcal{L}$ tal que:

1. Contiene a todas las constantes.
2. Contiene a todas las variables.
3. Si $t_1,\dots,t_n \in \mathcal{T}$ entonces $f_i^n(t_1,\dots,t_n) \in \mathcal{T}$.

Los elementos de $\mathcal{T}$ se dicen *términos*.

Se define $\mathcal{F}$ como la mínima clase (bajo inclusión) de cadenas de signos en $\mathcal{L}$ tal que:

1. Si $t_1, \dots, t_n$ son términos de $\mathcal{L}$, entonces $R_i^n(t_1, \dots, t_n) \in \mathcal{F}$.
2. Si $\phi \in \mathcal{F}$, entonces $\neg\phi \in \mathcal{F}$.
3. Si $\phi, \theta \in \mathcal{F}$, entonces $\phi \implies \theta \in \mathcal{F}$.
4. Si x es una variable y $\phi \in \mathcal{F}$ entonces $(\forall x\ \phi) \in \mathcal{F}$.

Los elementos de $\mathcal{F}$ se dicen *fórmulas*. Una *expresión* es cualquier cadena de signos que sea o un término o una fórmula.

Otra cuestión yace en que podemos ver que cosas como "$\forall x \exists x\ \phi$" se cuentan como fórmulas, a pesar de que no parece justo que se utilice la misma variable en dos cuantificadores anodados. Para ello diremos que una variable x está libre en una expresión como "$x+1$", de modo que si tenemos un cuantificador $\forall x\ \phi$ debe darse que x esté libre en ϕ. Así mismo querremos decir que si utilizamos una variable en un cuantificador, entonces la variable queda ligada, de modo que no podemos volver a ocuparla:

Definición 6.3: Dada una expresión en $\mathcal{L}$ y dada una variable x de $\mathcal{L}$, se dice que:

1. x está libre en x_i syss $x \equiv x_i$.
2. x no está libre en c_i.
3. x está libre en $f_i^n(t_1, \dots, t_n)$ syss lo está en algún término t_i.
4. x está libre en $R_i^n(t_1, \dots, t_n)$ syss lo está en algún término t_i.
5. x está libre en $\neg\phi$ syss lo está en ϕ.
6. x está libre en $\phi \implies \theta$ syss lo está en ϕ o en θ.
7. x está libre en $\forall x_i\ \phi$ syss lo está en ϕ y $x \not\equiv x_i$.

Dada una expresión en $\mathcal{L}$ y dada una variable x de $\mathcal{L}$, se dice que:

1. x no está ligada en x_i.
2. x no está ligada en c_i.

3. x está ligada en $f_i^n(t_1, \dots, t_n)$ syss lo está en algún término t_i.
4. x está ligada en $R_i^n(t_1, \dots, t_n)$ syss lo está en algún término t_i.
5. x está ligada en $\neg\phi$ syss lo está en ϕ.
6. x está ligada en $\phi \implies \theta$ syss lo está en ϕ o en θ.
7. x está ligada en $\forall x_i\ \phi$ syss lo está en ϕ o $x \equiv x_i$.

Se dice que una expresión es *abierta* si posee variables libres y *cerrada* si no. Se les llama *designadores* a los términos cerrados y *sentencias* a las fórmulas cerradas.

En general, dada una expresión abierta ϕ cuyas variables libres son $x_1, \dots, x_n$ denotamos $\phi(x_1, \dots, x_n)$ (se interpreta como que depende de las variables x_i).

Por ejemplo, $x+1$ es un término libre y $\forall x\ \neg(Sx = 0)$ es una sentencia. Así, luego veremos que lo que nos interesa es estudiar las sentencias.

Definición 6.4 – *Valoración*: Si x es una variable de $\mathcal{L}$ y a es un elemento de U, entonces

$$v_x^a(y) \equiv \begin{cases} a, & x \equiv y \\ v(y), & x \not\equiv y \end{cases}.$$

Y se dice que v es una *valoración*. Se define por recursividad

$$v_{x_1 \dots x_n x_{n+1}}^{c_1 \cdots c_n c_{n+1}} \equiv (v_{x_1 \cdots x_n}^{c_1 \cdots c_n})_{x_{n+1}}^{c_{n+1}},$$

en ésta valoración decimos que $x_1, \dots, x_{n+1}$ **están** en v. Además, nótese que las valoraciones se leen de derecha a izquierda.

Dado un $\mathcal{L}$-modelo M y una valoración v que contenga las variables $x_1, \dots, x_n$ se define la evaluación de una expresión ζ bajo v como prosigue, admitiendo que ζ es *evaluable* syss todas sus variables libres están contenidas en v:

1. $M(c_i)[v] \equiv \bar{c}_i$.
2. $M(x_i)[v] \equiv v(x_i)$.

3. $M(f_i^m(t_1, \dots, t_m))[v] \equiv \bar{f}_i^m(M(t_1)[v], \dots, M(t_m)[v])$. De éste modo, sabemos como interpretar todo término evaluable mediante una valoración.
4. $M \vDash R_i^m(t_1, \dots, t_m)[v]$ syss $\big(M(t_1)[v], \dots, M(t_m)[v]\big) \in \bar{R}_m^i$.
5. $M \vDash \neg\phi[v]$ syss no $M \vDash \phi[v]$.
6. $M \vDash (\phi \implies \theta)[v]$ syss no $M \vDash \phi[v]$ o $M \vDash \theta[v]$.
7. $M \vDash (\forall x_i\ \phi)[v]$ syss para todo $a \in U$ se cumple que $M \vDash \phi[v_{x_i}^a]$.

La expresión $M \vDash \phi[v]$ quiere decir que la interpretación de ϕ bajo la valoración de v es verdadera.

Nótese que independiente de la valoración, toda expresión cerrada es evaluable. En cierto sentido, ser evaluable es más débil que ser cerrada, pero igualmente, valga la redundancia, evaluable. Otra observación es que un modelo es en cierta forma algo así como una teoría matemática completa, ya que toda fórmula evaluable ϕ satisface que $M \vDash \phi[v]$ o $M \vDash \neg\phi[v]$, es decir, en un modelo las verdades ya vendrían resueltas, mientras que esperamos que las verdades sean deducciones, ésto nos obligará a replantear ciertas cuestiones.

Proposición 6.5: Dadas las variables x, y de $\mathcal{L}$ y los elementos $a, b \in U$, se cumple que:

$$v_{xy}^{ab} \equiv \begin{cases} v_y^b, & x \equiv y \\ v_{yx}^{ba}, & x \not\equiv y \end{cases}$$

Teorema 6.6: Si ϕ es una expresión evaluable en v, w; las cuales son valoraciones que coinciden en sus variables libres, entonces si ϕ es un término, se cumple que $M(\phi)[v] \equiv M(\phi)[w]$, y si ϕ es una fórmula entonces $M \vDash \phi[v]$ syss $M \vDash \phi[w]$.

Demostración: Lo haremos por inducción sobre la longitud de ϕ: Si ϕ es de longitud uno, entonces ha de ser o una variable o una constante. Todas las valoraciones coinciden sobre sus constantes, y si coinciden en las variables libres entonces $M(x)[v] \equiv v(x) \equiv w(x) \equiv M(x)[w]$.

Por otro lado, veamos que el resto de cuestiones salen de traducir la lógica semántica a la lógica formal, por ejemplo, $M(f_i^n(t_1, \dots, t_n))[v] \equiv \bar{f}_i^n(\bar{t}_1, \dots, \bar{t}_n)$ y notemos que la interpretación de un funtor es independiente de la valoración, más aún, por inducción los términos han de ser constantes o variables, las cuales ya coinciden. En consecuencia, todos los términos evaluables coinciden.

Aplicando lo anterior se puede comprobar que $M \vDash R_i^n(t_1, \ldots, t_n)[v]$ syss $M \vDash R_i^n(t_1, \ldots, t_n)[w]$, y así sucesivamente se demuestran el resto de casos. $\square$

Definición 6.7 – *Sustitución*: Dada una expresión ϕ y una variable x en $\mathcal{L}$ admitimos a $\mathrm{S}_x^t\, \phi$ como la sustitución de x por un término t en ϕ, de la siguiente manera recursiva:

1. $\mathrm{S}_x^t\, y \equiv \begin{cases} t, & x \equiv y \\ y, & x \not\equiv y \end{cases}$
2. $\mathrm{S}_x^t\, c \equiv c$.
3. $\mathrm{S}_x^t\, f_i^n(t_1, \ldots, t_n) \equiv f_i^n(\mathrm{S}_x^t\, t_1, \ldots, \mathrm{S}_x^t\, t_n)$.
4. $\mathrm{S}_x^t\, R_i^n(t_1, \ldots, t_n) \equiv R_i^n(\mathrm{S}_x^t\, t_1, \ldots, \mathrm{S}_x^t\, t_n)$.
5. $\mathrm{S}_x^t\, \neg\phi \equiv \neg\, \mathrm{S}_x^t\, \phi$.
6. $\mathrm{S}_x^t(\phi \implies \theta) \equiv \mathrm{S}_x^t\, \phi \implies \mathrm{S}_x^t\, \theta$.
7. $\mathrm{S}_x^t\, \forall x_i\, \phi \equiv \begin{cases} \forall x_i\, \phi & \text{si } x \text{ no está libre en } \forall x_i\, \phi \\ \forall x_i\ \mathrm{S}_x^t\, \phi & \text{si } x \text{ está libre en } \forall x_i\, \phi \\ & \text{y } x_i \text{ no lo está en } t \\ \forall x_j\ \mathrm{S}_x^t\, \mathrm{S}_{x_i}^{x_j}\, \phi & \text{si } x \text{ está libre en } \forall x_i\, \phi,\ x_i \text{ está libre} \\ & \text{en } t \text{ y } x_j \text{ es la primera variable que no} \\ & \text{está contenida en } \forall x_i\, \phi \text{ ni } t \end{cases}$

Notemos que la valoración es como una sustitución pero a nivel del modelo, en cambio la sustitución propia aquí definida está a nivel del lenguaje.

Teorema 6.8: Dada una valoración v, ϕ una expresión evaluable, x una variable y t un término de $\mathcal{L}$. Si ϕ es un término, entonces

$$M(\mathrm{S}_x^t\, \phi)[v] \equiv M(\phi)[v_x^{M(t)[v]}]$$

y si ϕ es una fórmula, entonces

$$M \vDash \mathrm{S}_x^t\, \phi[v] \qquad \text{syss} \qquad M \vDash \phi[v_x^{M(t)[v]}]$$

PISTA: También se hace por inducción sobre la longitud de la expresión. □

Definición 6.9: Se dice que una fórmula ϕ es *verdadera* en el $\mathcal{L}$-modelo M, denotado $M \vDash \phi$, si para toda valoración v que hace que ϕ sea evaluable se cumple que $M \vDash \phi[v]$. Si $M \vDash \neg\phi$ entonces decimos que ϕ es *falsa*.

Si Γ es un conjunto de fórmulas, denotamos que $M \vDash \Gamma$ si todas las fórmulas de Γ son verdaderas, en este caso decimos que M es un modelo para Γ.

Proposición 6.10: En un $\mathcal{L}$-modelo se cumple:

1. Una fórmula no puede ser verdadera y falsa al mismo tiempo (principio del tercero excluído). Ojo que hay fórmulas que ni son verdaderas ni falsas como $x = 1$ que lo es para la valoración v_x^1 y falsa para la valoración v_x^0.
2. Toda sentencia es o verdadera o falsa (principio del tercero excluído).
3. ϕ es verdadera syss $\neg\phi$ es falsa, y viceversa, ϕ es falsa syss $\neg\phi$ es verdadera.

6.2 Teorías

Definición 6.11 (Teoría): Un conjunto de $\mathcal{L}$-fórmulas T se dice una *teoría*. Denotamos que $T \vDash \phi$ si $M \vDash \phi$ para todo $\mathcal{L}$-modelo tal que $M \vDash T$. Si en toda teoría T se cumple que $T \vDash \phi$, entonces denotamos $\vDash \phi$. A las fórmulas de una teoría se le suelen decir *premisas*. Si $T \vDash \phi$, entonces se dice que ésta es una regla semántica.

Si $\vDash \phi$, entonces decimos que es una tautología, si $\vDash \neg\phi$, entonces decimos que es una contradicción, si existe un $\mathcal{L}$-modelo M tal que $M \vDash \phi$ entonces decimos que es *satisfacible* y si existe un $\mathcal{L}$-modelo M tal que $M \vDash \neg\phi$ entonces decimos que es *falseable*.

En general a lo referente a «$\vDash$», es decir, a las demostraciones basadas en modelos, se le llama *semántica*. Lo que veremos acontinuación es que varias proposiciones clásicas de la lógica, algunas ya vistas en la primera sección del libro, se deducen de manera sencilla mediante semántica.

Corolario 6.12: Se cumple:

1. ϕ es tautología syss $\neg\phi$ es contradicción. Y viceversa, ϕ es contradicción syss $\neg\phi$ es tautología.

2. ϕ es satisfacible syss $\neg\phi$ es falseable. Y viceversa, ϕ es falseable syss $\neg\phi$ es satisfacible.

3. Toda tautología (resp. contradicción) es satisfacible (resp. falseable). En consecuencia, no se puede ser tautología (resp. contradicción) y falseable (resp. satisfacible) al mismo tiempo.

Definición 6.13: En $\mathcal{L}$, donde ϕ, θ son $\mathcal{L}$-fórmulas, se define:

$$\begin{aligned}
\phi \lor \theta &\equiv \neg\phi \implies \theta \\
\phi \land \theta &\equiv \neg(\neg\phi \lor \neg\theta) \\
\phi \iff \theta &\equiv (\phi \implies \theta) \land (\theta \implies \phi) \\
\exists x : \phi &\equiv \neg(\forall x\, \neg\phi) \\
\exists! x : \phi &\equiv \exists x \forall y\, (\mathrm{S}_x^y\, \phi \implies x = y)
\end{aligned}$$

Teorema 6.14: Dadas las fórmulas ϕ, θ se cumple:

1. $\phi \implies \theta, \phi \vDash \theta$ (*modus ponendo ponens*, MP).

2. $\phi \land \theta, \neg\phi \vDash \theta$ (*modus tollendo ponens*).

3. $\vDash \phi \lor \neg\phi$ (tercero excluido).

4. $t_1 = t_2, t_2 = t_3 \vDash t_1 = t_3$ (transitividad del igualador).

5. $\forall x\, \phi(x) \vDash \mathrm{S}_x^t\, \phi$ (eliminación del generalizador, EG).

6. $\phi \vDash \forall x\, \phi$ (introducción del generalizador, IG).

7. Si $\phi \vDash \theta$ y $\theta \vDash \psi$, entonces $\phi \vDash \psi$ (transitividad de reglas semánticas).

8. Si ϕ es tautología, entonces $\phi \vDash \theta$ syss θ es tautología.

9. Si ϕ es contradicción, entonces para todo θ se cumple que $\phi \vDash \theta$.

Demostración: Todas son más que una caracterización lógica de los símbolos, vamos a hacer unas pocas:

1. Para ésta, vamos a usar una tabla de verdad, nótese que

ϕ	θ	$\phi \implies \theta$
V	V	**V**
V	F	F
F	V	V
F	F	V

4. Sea M un modelo en donde $t_1 = t_2$ y $t_2 = t_3$, y sea v una valoración que les evalúe. Entonces $M(t_1)[v] \equiv M(t_2)[v] \equiv M(t_3)[v]$, ergo, $M(t_1)[v] \equiv M(t_3)[v]$, es decir, $M \vDash t_1 = t_2$.

   Notemos que lo que hicimos fue interpretar las $\mathcal{L}$-fórmulas y traducir la transitividad del signo igualador a su interpretación en un modelo cualquiera, en donde sí que se cumple.

5. Si M es un modelo donde $M \vDash \forall x\ \phi$, entonces para toda valoración v se cumple que $(M \vDash \forall x\ \phi)[v]$, es decir, para todo $a \in U$ se cumple que $M \vDash \phi[v_x^a]$. Sea t un término cualquiera fijado, entonces vemos que $(M \vDash \mathrm{S}_x^t\, \phi)[v]$ syss $M \vDash \phi[v_x^{M(t)[v]}]$. Luego, aplicamos la conclusión inicial con $a \equiv M(t)[v]$ para comprobar que $M \vDash \mathrm{S}_x^t\, \phi$ como se quería probar. □

Definición 6.15 – *Sistema deductivo*: F se dice un *sistema deductivo* sobre un lenguaje $\mathcal{L}$ si consiste de una serie de fórmulas, a las que llamamos *axiomas* y un conjunto de reglas, llamadas de inferencia, que determina si una fórmula es consecuencia inmediata de otras anteriores.

Dado un conjunto de fórmulas Γ, se dice que una *deducción* sobre F es una sucesión $\phi_1, \dots, \phi_n$ de $\mathcal{L}$-fórmulas donde cada ϕ_i es un axioma, una fórmula de Γ o es consecuencia inmediata de las fórmulas previas; en cuyo caso decimos que $\theta \equiv \phi_n$ es la conclusión de la deducción, lo que denotaremos por $\Gamma \vdash_F \theta$. En este caso decimos que Γ son *premisas* de θ. Una conclusión sin premisas, es decir, si $\vdash_F \theta$, entonces decimos que θ es un *teorema* y cualquier deducción de θ es una *demostración*. También denotamos $\Gamma \dashv\vdash \Delta$ si $\Gamma \vdash \Delta$ y $\Delta \vdash \Gamma$.

Un sistema deductivo es *correcto* si sus axiomas son tautologías y sus reglas de inferencia son reglas semánticas.

Corolario 6.16: Si $\Gamma \vdash_F \phi$, entonces existen finitas premisas de Γ tales que $\theta_1, \dots, \theta_n \vdash_F \phi$.

Teorema 6.17 (Sonoro): Si F es un sistema deductivo correcto sobre

$\mathcal{L}$ y Γ es un conjunto de $\mathcal{L}$-fórmulas. Entonces si $\Gamma \vdash_F \phi$, entonces $\Gamma \vDash \phi$. En consecuencia, todos los teoremas de F son tautologías.

Demostración: Sea $\phi_1, \dots, \phi_n$ una deducción de ϕ a partir de Γ. Probaremos que si M es un $\mathcal{L}$-modelo de Γ, entonces $M \vDash \phi_i$ por inducción. En primer lugar ϕ_1 ha de ser o una tautología (de modo que es cierta) o una premisa, de modo que $M \vDash \phi_1$ por construcción de M. Si $\Gamma \vDash \phi_1, \dots, \phi_i$ veremos que $\Gamma \vDash \phi_{i+1}$, si es una tautología o una premisa entonces es claro; si no lo es, entonces como es consecuencia directa de las anteriores vemos que:

$$\Gamma \vDash \phi_1, \dots, \phi_i \vDash \phi_{i+1},$$

pues las reglas de inferencia son reglas semánticas. □

Definición 6.18: Denotamos[1] por $K_{\mathcal{L}}$ al sistema que posee los siguientes axiomas, donde ϕ, θ, ψ son $\mathcal{L}$-fórmulas y t es un $\mathcal{L}$-término cualquiera:

K1. $\phi \implies (\theta \implies \phi)$.

K2. $(\phi \implies (\theta \implies \psi)) \implies ((\phi \implies \theta) \implies (\phi \implies \psi))$.

K3. $(\neg\phi \implies \neg\theta) \implies (\theta \implies \phi)$.

K4. $\forall x\, \phi \implies \mathrm{S}_x^t\, \phi$.

K5. Si x no está libre en ϕ, entonces $\forall x\, (\phi \implies \theta) \implies (\phi \implies \forall x\, \theta)$.

K6. Si x no está libre en t, entonces $\forall x\, (x = t \implies \phi) \iff \mathrm{S}_x^t\, \phi$.

K7. $\exists! x_i\, \phi \implies \mathrm{S}_{x_i}^{x_j : \phi}\, \phi$.

K8. $\neg\exists! x_i\, \phi \implies x_i : \phi = x_j : (x_j = x_j)$.

Y cuyas reglas de inferencia son:

MP De ϕ y $\phi \implies \theta$ se concluye θ.

IG De ϕ se concluye $\forall x\, \phi$.

La versión particular del teorema sonoro que nos interesa es la siguiente:

Teorema 6.19: $K_{\mathcal{L}}$ es un sistema correcto.

[1] Otros emplean **LK**, abreviación del ger. *logistischer klassischer Kalkül*: cálculo de la lógica de predicados.

Demostración: Las reglas de inferencia y el axioma K4 ya están probados, los axiomas K1-3 salen de tablas de verdad.

Vamos a ver como probaríamos el K5: $M \vDash \forall x\ (\phi \implies \theta)$ syss $M \vDash (\phi \implies \theta)[v]$ para toda valoración v. Lo que significa que para una valoración fijada v y todo $a \in U$ se cumple que $M \nvDash \phi[v_x^a]$ o $M \vDash \theta[v_x^a]$ Si x no está libre en ϕ, entonces $M \vDash \phi[v_x^a]$ syss $M \vDash \phi[v]$. De modo que para v fija se tiene que no $M \vDash \phi[v]$ o $M \vDash \theta[v_x^a]$ para todo $a \in U$. Vemos que eso es exactamente lo que el derecho significa. □

De aquí en adelante admitiremos las siguientes notaciones para una fórmula ϕ:

$$\Gamma \vdash \phi \equiv \Gamma \underset{K_{\mathcal{L}}}{\vdash} \phi.$$

En general a lo referente al símbolo «⊢» le decimos *sintáctica* o *sintaxis*. Traduciendo el teorema sonoro nos dice que toda verdad sintáctica, es decir todo aquello que admite demostración lógica, es verdad semánticamente, es decir es válido en todo modelo. En la siguiente sección demostraremos varias verdades semánticas de manera sintáctica; el (meta)teorema motivacional en la lógica de modelos consiste en ver el converso del teorema sonoro: esto es, que toda verdad semántica es también sintáctica; ésto se conoce como el teorema de completitud de Gödel (no confundir con los teoremas de <u>in</u>completitud) y es fundamental en la teoría de modelos.

§6.2.1 Reglas de inferencia.

Proposición 6.20: Si ϕ es una fórmula entonces $\vdash (\phi \implies \phi)$.

Demostración: Veamos una demostración formal:

1.	$\phi \implies ((\phi \implies \phi) \implies \phi)$	K1
2.	$\phi \implies ((\phi \implies \phi) \implies \phi) \implies ((\phi \implies (\phi \implies \phi)) \implies (\phi \implies \phi))$	K2
3.	$(\phi \implies (\phi \implies \phi)) \implies (\phi \implies \phi)$	MP 1,2
4.	$\phi \implies (\phi \implies \phi)$	K1
5.	$\phi \implies \phi$	MP 3,4

□

Nota: Hay varias notaciones para las demostraciones formales, éste libro sigue el estilo de Fitch sobre el estilo clásico de Gentzen.

Corolario 6.21: Se cumple $\phi \vdash \phi$ (regla de repetición, R). Ésto puede parecer obvio, pero en realidad ésto es un teorema que nos permite repetir líneas en una deducción.

Notemos que en éste contexto, los teoremas además tienen la utilidad de abreviar pasos en otras deducciones.

Teorema 6.22 (de deducción): Sea Γ un conjunto de fórmulas y ϕ, θ dos fórmulas. Si $\Gamma, \phi \vdash \theta$, entonces $\Gamma \vdash (\phi \implies \theta)$.

Demostración: Por definición existe una deducción $\psi_1, \ldots, \psi_n \equiv \theta$ de θ cuyas premisas son fórmulas de Γ y/o ϕ. Demostraremos, por inducción fuerte, que para cada ψ_i se demuestra que $\phi \implies \psi_i$ mediante premisas de Γ.

a) $\psi_i \equiv \phi$: Entonces ya vimos que se da que $\phi \implies \phi$ en $K_{\mathcal{L}}$.

b) ψ_i es un axioma o premisa de Γ: Entonces para probar $\phi \implies \psi_i$ basta la siguiente demostración:

1.	ψ_i	Axioma o premisa
2.	$\psi_i \implies (\phi \implies \psi_i)$	K1
3.	$\phi \implies \psi_i$	MP 1,2

c) ψ_i se infiere de las anteriores: Entonces puede ser inferida en $K_{\mathcal{L}}$ por MP: mediante las fórmulas ψ_j y $\psi_j \implies \psi_i$ en cuyo caso:

1.	$\phi \implies \psi_j$	Hipótesis
2.	$\phi \implies (\psi_j \implies \psi_i)$	Hipótesis
3.	$(\phi \implies (\psi_j \implies \psi_i)) \implies ((\phi \implies \psi_j) \implies (\phi \implies \psi_i))$	K2
4.	$(\phi \implies \psi_j) \implies (\phi \implies \psi_i)$	MP 3, 2
5.	$\phi \implies \psi_i$	MP 4, 1

O puede ser inferida en $K_{\mathcal{L}}$ por IG: donde $\psi_i \equiv \forall x \psi_j$, en cuyo caso:

1.	$\phi \implies \psi_j$	Hipótesis
2.	$\forall x\, (\phi \implies \psi_j) \implies (\phi \implies \forall x\, \psi_j)$	K5
3.	$\phi \implies \forall x\, \psi_j$	MP 2, 1

que es exactamente ver que $\phi \implies \psi_i$. $\square$

Teorema 6.23: Dadas las $\mathcal{L}$-fórmulas ϕ, θ, ψ se cumplen:

1. $\phi \implies \theta, \theta \implies \psi \vdash \phi \implies \psi$ (*modus barbara*, MB).
2. $\phi \dashv\vdash \neg\neg\phi$ (doble negación, DN).
3. $\phi, \neg\phi \vdash \theta$ (regla de la contradicción, C).
4. $\phi \implies \theta \dashv\vdash \neg\theta \implies \neg\phi$ y $\phi \implies \neg\theta \dashv\vdash \theta \implies \neg\phi$ (reglas de la «contrarrecíproca» o «contrapositiva», CR).
5. $\phi \implies \theta, \neg\theta \vdash \neg\phi$ (*modus tollendo tollens*, MT).
6. $\phi \lor \theta \dashv\vdash \theta \lor \phi$ (conmutatividad).
7. $\vdash \phi \lor \neg\phi$ (tercero excluido, TND).
8. Leyes de De Morgan (DM):

$$\begin{aligned} \phi \lor \theta &\dashv\vdash \neg(\neg\phi \land \neg\theta), & \phi \land \theta &\dashv\vdash \neg(\neg\phi \lor \neg\theta) \\ \neg(\phi \lor \theta) &\dashv\vdash \neg\phi \land \neg\theta, & \neg(\phi \land \theta) &\dashv\vdash \neg\phi \lor \neg\theta \end{aligned}$$

9. $\phi \land \theta \dashv\vdash \theta \land \phi$ (conmutatividad).
10. $\vdash \neg(\phi \land \neg\phi)$ (regla de la no contradicción, NC).
11. $\phi \lor \theta, \neg\phi \vdash \theta$ y $\phi \lor \theta, \neg\theta \vdash \phi$ (*modus tollendo ponens*, MTP).
12. $\phi \vdash \phi \lor \theta$ (introducción del disyuntor, ID).
13. $\phi, \theta \vdash \phi \land \theta$ (introducción del conjuntor, IC).
14. $\phi \lor \phi \vdash \phi$ (eliminación del disyuntor, ED).
15. $\phi \land \theta \vdash \phi$ y $\phi \land \theta \vdash \theta$ (eliminación del conjuntor, EC).
16. $\phi \implies \theta, \theta \implies \phi \vdash \phi \iff \theta$ (introducción del bicondicional, IB).
17. $\phi \iff \theta \vdash \phi \implies \theta$ y $\phi \iff \theta \vdash \theta \implies \phi$ (eliminación del bicondicional, EB).

DEMOSTRACIÓN: Demostraremos algunas y el resto quedaran de ejercicio al lector:

1.

1.	$\phi \implies \theta$	Premisa
2.	$\theta \implies \psi$	Premisa
3.	ϕ	Hipótesis
4.	θ	MP 1, 3
5.	ψ	MP 2, 4
6.	$\phi \implies \psi$	Deducción

2. Primero veamos que $\neg\neg\phi \vdash \phi$:

1.	$\neg\neg\phi$	Premisa
2.	$\neg\neg\phi \implies (\neg\neg\neg\neg\phi \implies \neg\neg\phi)$	K1
3.	$\neg\neg\neg\neg\phi \implies \neg\neg\phi$	MP 2, 1
4.	$(\neg\neg\neg\neg\phi \implies \neg\neg\phi) \implies (\neg\phi \implies \neg\neg\neg\phi)$	K3
5.	$\neg\phi \implies \neg\neg\neg\phi$	MP 4, 3
6.	$(\neg\phi \implies \neg\neg\neg\phi) \implies (\neg\neg\phi \implies \phi)$	K3
7.	$\neg\neg\phi \implies \phi$	MP 6, 5
8.	ϕ	MP 7, 1

Por el teorema de deducción podemos reescribir la regla como que $\vdash (\neg\neg\theta \implies \theta)$. Reemplazando $\theta \equiv \neg\phi$ obtenemos un teorema que emplearemos en la otra demostración:

1.	ϕ	Premisa
2.	$(\neg\neg\neg\phi \implies \neg\phi) \implies (\phi \implies \neg\neg\phi)$	K3
3.	$\neg\neg\neg\phi \implies \neg\phi$	DN
4.	$\phi \implies \neg\neg\phi$	MP 2, 3
5.	$\neg\neg\phi$	MP 4, 1

3.

1.	$\neg\phi$	Premisa
2.	ϕ	Premisa
3.	$(\neg\theta \implies \neg\phi) \implies (\phi \implies \theta)$	K3
4.	$\neg\phi \implies (\neg\theta \implies \neg\phi)$	K1
5.	$\neg\theta \implies \neg\phi$	MP 4, 1
6.	$\phi \implies \theta$	MP 3, 5
7.	θ	MP 6, 2

13. Por MTP se cumple que $\neg\neg\theta, \neg\phi \vee \neg\theta \vdash \neg\phi$, y por el teorema de deducción se cumple que $\neg\neg\theta \vdash (\neg\phi \vee \neg\theta \implies \neg\phi)$:

1.	θ	Premisa
2.	$\neg\neg\theta$	DN 1
3.	$\neg\phi \vee \neg\theta \implies \neg\phi$	
4.	$\neg\neg\phi \implies \neg(\neg\phi \vee \neg\theta)$	CR 3
5.	ϕ	Premisa
6.	$\neg\neg\phi$	DN 5
7.	$\neg(\neg\phi \vee \neg\theta)$	MP 4, 6
8.	$\phi \wedge \theta$	DM 7

14.

1.	$\phi \vee \phi$	Premisa
2.	$\neg\phi \implies \neg\phi \wedge \neg\phi$	IC
3.	$\neg(\neg\phi \wedge \neg\phi) \implies \phi$	NI 2
4.	$\neg(\neg\phi \wedge \neg\phi)$	DM 1
5.	ϕ	MP 3, 4

$\square$

Teorema 6.24 (reducción al absurdo): Si $\Gamma \vdash \neg\phi \implies \theta \wedge \neg\theta$, entonces $\Gamma \vdash \phi$.

Demostración: Basta notar que $\vdash \neg(\theta \wedge \neg\theta)$ por NC, luego por MT se cumple que $\neg\neg\phi$ y por DM se cumple que ϕ. □

Con éste método se admite una prueba aún más sencilla de ED:

1.	$\phi \vee \phi$	Premisa
2.	$\neg\phi \implies \phi$	R 1
3.	$\quad \neg\phi$	Hipótesis (dem. por contradicción)
4.	$\quad \phi$	MP 2, 3
5.	$\quad \neg\phi \wedge \phi$	IC 3, 4
6.	ϕ	Contradicción

También en general obviaremos la línea 5, pues la anterior ya expone la contradicción.

Proposición 6.25: Dadas las $\mathcal{L}$-fórmulas ϕ, θ, ψ y t, t_1, t_2, t_3 unos $\mathcal{L}$-términos. Entonces:

1. $\forall x\ \phi \vdash \mathrm{S}_x^t\, \phi$ (eliminación del generalizador, EG).
2. $\neg\forall x\ \neg\phi \dashv\vdash \exists x\ \phi$ y $\neg\forall x\ \phi \dashv\vdash \exists x\ \neg\phi$ (negación del generalizador, NG).
3. $\neg\exists x\ \neg\phi \dashv\vdash \forall x\ \phi$ y $\neg\exists x\ \phi \dashv\vdash \forall x\ \neg\phi$ (negación del particularizador, NP).
4. $\mathrm{S}_x^t\, \phi \vdash \exists x\ \phi$ (introducción del particularizador, IP).
5. Si x no está libre en t, entonces $\mathrm{S}_x^t\, \phi \vdash \forall x\ (x = t \implies \phi)$ (introducción del igualador, II) y $\forall x\ (x = t \implies \phi) \vdash \mathrm{S}_x^t\, \phi$ (eliminación del igualador, EI).
6. $t = t$ (reflexividad del igualador, I).
7. $t_1 = t_2 \dashv\vdash t_2 = t_1$ (simetría del igualador, SI).
8. $t_1 = t_2, t_2 = t_3 \vdash t_1 = t_3$ (transitividad del igualador, TI).
9. $t = s \vdash f_i^{n+1}(t_1, \dots, t_n; t) = f_i^{n+1}(t_1, \dots, t_n; s)$ (igualdad bajo funtores, IF).
10. $t = s \vdash R_i^{n+1}(t_1, \dots, t_n; t) \iff R_i^{n+1}(t_1, \dots, t_n; s)$ (equivalencia bajo relatores, ER).

DEMOSTRACIÓN: Igual que con las otras reglas, demostraremos sólo unas pocas:

4.

1.	$\mathrm{S}_x^t\,\phi$	Premisa
2.	$\neg\exists x\ \phi$	Hipótesis (por contradicción)
3.	$\forall x\ \neg\phi$	NP 2
4.	$\mathrm{S}_x^t\,\neg\phi$	EG 3
5.	$\neg\,\mathrm{S}_x^t\,\phi$	R 4 (contradicción con 1)
6.	$\exists x\ \phi$	Conclusión

5. Son consecuencia de K6, EB y MP.

6.

1.	$x = t \implies x = t$	Teorema
2.	$\forall x\ (x = t \implies x = t)$	IG 1
3.	$\forall x\ (x = t \implies x = t) \iff \mathrm{S}_x^t(x = t)$	K6
4.	$\forall x\ (x = t \implies x = t) \implies \mathrm{S}_x^t(x = t)$	EB 3
5.	$\mathrm{S}_x^t(x = t)$	MP 2, 4
6.	$t = t$	R 5

7.

1.	$t_1 = t_2$	Premisa
2.	$t_2 = t_2$	I
3.	$\mathrm{S}_x^{t_2}\,t_2 = x$	R 2
4.	$\forall x\ (x = t_2 \implies t_2 = x)$	II 3
5.	$\mathrm{S}_x^{t_1}(x = t_2 \implies t_2 = x)$	EG 4
6.	$t_1 = t_2 \implies t_2 = t_1$	R 5
7.	$t_2 = t_1$	MP 6, 1

□

6.3 Consistencia y completitud

Definición 6.26 – *Teoría axiomática*: Se dice que un conjunto de $\mathcal{L}$-fórmulas T es una *teoría axiomática* si contiene a todos los axiomas de $K_{\mathcal{L}}$ y sus reglas de inferencia son las de $K_{\mathcal{L}}$; en cuyo caso, llamamos *axiomas propios* a sus axiomas que no son los de $K_{\mathcal{L}}$. Nótese que si Γ son los axiomas propios de T, entonces para toda $\mathcal{L}$-fórmula ϕ se cumple que

$$\underset{T}{\vdash} \phi \iff \Gamma \vdash \phi.$$

Una fórmula ϕ tal que $\vdash_T \phi$ o $\vdash_T \neg\phi$ se dice una *proposición*, las fórmulas que no son proposiciones se dicen *indecibles*.

Se dice que una teoría axiomática es:

Contradictoria Si existe ϕ tal que $\vdash_T \phi$ y $\vdash_T \neg\phi$.

Consistente Si no es contradictoria.

Completa Si toda sentencia es una proposición.

Proposición 6.27: Una teoría axiomática es contradictoria syss en ella se puede probar toda fórmula. En consecuencia, toda teoría axiomática contradictoria es completa.

Demostración: Basta recordar la regla de la contradicción. □

Teorema 6.28: Si una teoría axiomática es satisfacible (si posee un modelo), entonces es consistente.

Demostración: Si una teoría T tiene un modelo M, entonces todos sus teoremas son válidos en todo modelo (por el teorema sonoro), luego las negaciones de ellos son falsedades así pues concluimos que no se puede demostrar toda fórmula. □

Teorema 6.29: Sea Γ un conjunto de fórmulas y ϕ una sentencia. Entonces $\Gamma \cup \{\phi\}$ es consistente syss no $\Gamma \vdash \neg\phi$.

Demostración: $\implies$. Si $\Gamma \vdash \neg\phi$, entonces $\Gamma \cup \{\phi\} \vdash \phi$ y $\Gamma \cup \{\phi\} \vdash \neg\phi$, luego $\Gamma \cup \{\phi\}$ es contradictorio.

$\impliedby$. La haremos por contradicción: Si no $\Gamma \vdash \neg\phi$ y $\Gamma \cup \{\phi\}$ fuese contradictoria, entonces por la regla de contradicción se da que $\Gamma \cup \{\phi\} \vdash \neg\phi$ (pues todo es logicamente demostrable), lo que por el teorema de deducción se satisface que $\Gamma \vdash \phi \implies \neg\phi$, que es equivalente a que $\Gamma \vdash \neg\phi \vee \neg\phi$ y a que $\Gamma \vdash \neg\phi$ lo que contradice la hipótesis. □

Aquí es importante que ϕ sea una sentencia, pues en caso contrario podríamos suponer que Γ consiste de $\exists xy : (x \neq y)$ y que $\phi \equiv x = y$. Nótese que no $\Gamma \vdash x \neq y$, pues de lo contrario podemos introducir y eliminar generalizadores para obtener que $\Gamma \vdash x \neq x$ lo que es falso; sin embargo, $\Delta := \Gamma \cup \{x = y\}$ es contradictorio pues si introducimos generalizadores se obtiene que $\Delta \vdash \forall xy\ (x = y)$ y $\Delta \vdash \exists xy : (x \neq y)$ que son la negación una de la otra por NG.

Definición 6.30: Dadas dos $\mathcal{L}$-teorías axiomáticas T, S; se dice que S es una *extensión* de T si todo axioma propio de T es un teorema de S.

Teorema 6.31 (Lema de Lindenbaum): Toda teoría axiomática consistente admite una extensión consistente y completa.

Demostración: Como $\mathcal{L}$ es numerable, la cantidad de $\mathcal{L}$-sentencias es también numerable luego sea $(\phi_n)_{n\in\mathbb{N}}$ una enumeración de todas las $\mathcal{L}$-sentencias. Luego sea Γ los axiomas propios de la teoría. Construimos por recursión: Γ_0 es la clausura bajo cuantificadores universales de las fórmulas de Γ y

$$\Gamma_{n+1} := \begin{cases} \Gamma_n, & \text{si } \Gamma_n \cup \{\phi_n\} \text{ es contradictorio} \\ \Gamma_n \cup \{\phi_n\}, & \text{si es consistente} \end{cases}$$

Luego sea $\Gamma_\infty := \bigcup_{n\in\mathbb{N}} \Gamma_n$. Es claro que la teoría S cuyos axiomas propios son las sentencias de Γ_∞ es una extensión de T y es consistente, pues de no serlo, entonces una demostración de una contradicción poseería finitas sentencias, que estarían todas contenidas en algún Γ_n y es claro que todos ellos son consistentes.

Veamos finalmente que S es completa: Sea θ una $\mathcal{L}$-sentencia, sea $\phi_i \equiv \theta$, $\phi_j \equiv \neg\theta$ y sin perdida de generalidad supongamos que $i < j$. Si $\theta \in \Gamma_\infty$, entonces no hay nada que probar, pero si no, entonces $\Gamma_i \cup \{\phi_i\}$ es contradictorio y $\Gamma_i \vdash \neg\theta$; luego $\Gamma_j \cup \{\phi_j\}$ es consistente si no $\Gamma_j \vdash \neg\phi_j \equiv \theta$ (DN), pero ésto es claro, pues $\Gamma_j \vdash \Gamma_i \vdash \neg\theta$ y Γ_j es consistente; ergo $\phi_j \in \Gamma_{j+1} \subseteq \Gamma_\infty$ como se quería probar. □

Nótese que podríamos eliminar la exigencia de que el lenguaje sea numerable para obtener una generalización del teorema, cuya demostración fuese una aplicación del lema de Zorn (hágalo explícitamente); sin embargo así obtenemos una demostración sin AE.

Definición 6.32: Una teoría axiomática T cuyos axiomas propios son Γ se dice:

Maximalmente consistente Si para todo $\phi \notin \Gamma$ se cumple que $\Gamma \cup \{\neg\phi\}$ es contradictorio.

Finitamente satisfacible Si para todo $\Delta \subseteq \Gamma$ finito, se cumple que Δ es satisfacible.

Se denota

$$\mathrm{Th}(T) := \{\phi : \phi \text{ es } \mathcal{L}\text{-sentencia} \land T \vdash \phi\}.$$

Teorema 6.33: Una teoría axiomática T es consistente y completa syss $\mathrm{Th}(T)$ es maximalmente consistente.

DEMOSTRACIÓN: $\Longrightarrow$. Sea ϕ una sentencia. Entonces o $T \vdash \phi$ o $T \vdash \neg\phi$ (pues T es completa y consistente). Luego si $T \vdash \phi$, entonces $\phi \in \mathrm{Th}(T)$ y $\neg\phi \notin \mathrm{Th}(T)$; lo que prueba que $\mathrm{Th}(T)$ es consistente. Y si $\theta \notin \mathrm{Th}(T)$, por completitud de T se cumple que $T \vdash \neg\theta$ y $\neg\theta \in \mathrm{Th}(T)$, luego $\mathrm{Th}(T) \cup \theta$ es contradictorio; lo que prueba que $\mathrm{Th}(T)$ es maximalmente consistente.

$\Longleftarrow$. Como $T \subseteq \mathrm{Th}(T)$, entonces es claro que T es consistente. Sea ϕ una sentencia, luego si $\phi \in \mathrm{Th}(T)$ entonces $T \vdash \phi$ y si no, entonces $\mathrm{Th}(T) \cup \{\phi\}$ es contradictorio (pues $\mathrm{Th}(T)$ es maximalmente consistente), es decir, $\mathrm{Th}(T) \vdash \neg\phi$ y $T \vdash \neg\phi$ lo que prueba que T es completo. □

Definición 6.34: Se dice que una teoría axiomática T está *ejemplificada* si para toda sentencia $T \vdash \exists x : \phi$ existe algún designador t tal que $T \vdash \mathrm{S}_x^t\,\phi$. Es decir, si existe algún x tal que ϕ, podemos dar un ejemplo de un x.

Ahora podemos proceder a empezar la demostración del teorema de completitud que consiste en probar que si una teoría es consistente, entonces posee un modelo. Para construir dicho modelo requerimos que éste sea una teoría axiomática maximalmente consistente, lo que ya vimos, pero además necesitamos que sea ejemplificada. Para ello, primero veamos que añadir constantes que ejemplifiquen sentencias con cuantificadores existenciales no afecta al resto de la teoría ni a su consistencia.

Lema 6.35: Sea $\mathcal{L}$ un lenguaje formal y $\mathcal{L}' := \mathcal{L} \cup \{c\}$, donde c es una constante no contenida en $\mathcal{L}$. Sea ϕ una $\mathcal{L}$-fórmula, de modo que c no está en ϕ y tal que x no está ligada en ϕ; si $\vdash_{K_{\mathcal{L}'}} \mathrm{S}_x^c\,\phi$, entonces $\vdash_{K_{\mathcal{L}}} \phi$.

Demostración: Primero nótense éstos dos hechos fundamentales:

(I) Si ϕ es una $\mathcal{L}'$-sentencia que no contiene a x, entonces $\phi \equiv \mathrm{S}_x^c\,\bar{\phi}$ con $\bar{\phi} \equiv \mathrm{S}_c^x\,\phi$, de modo que $\bar{\phi}$ es una $\mathcal{L}$-sentencia que no contiene a c.

(II) Si ϕ, θ son $\mathcal{L}$-sentencias que no contienen a c, entonces $\mathrm{S}_x^c\,\phi \equiv \mathrm{S}_x^c\,\theta$ syss $\phi \equiv \theta$.

Sea ϕ una $\mathcal{L}$-sentencia. Como x no está ligada en ϕ, entonces x no está libre ni ligada en $\mathrm{S}_x^c\,\phi$. Probaremos el teorema por inducción sobre la longitud de la demostración de $\mathrm{S}_x^c\,\phi$.

<u>Caso base:</u> Si la demostración tiene una sola sentencia, entonces es que $\mathrm{S}_x^c\,\phi$ es un axioma de $K_{\mathcal{L}'}$. Supongamos que $\mathrm{S}_x^c\,\phi \equiv \theta \implies (\psi \implies \theta)$ (K1), entonces por (I) se cumple que

$$\mathrm{S}_x^c\,\phi \equiv \mathrm{S}_x^c\,\bar{\theta} \implies (\mathrm{S}_x^c\,\bar{\psi} \implies \mathrm{S}_x^c\,\bar{\theta}) \equiv \mathrm{S}_x^c\left(\bar{\theta} \implies (\bar{\psi} \implies \bar{\theta})\right)$$

ergo, por (II) se cumple que $\phi \equiv \bar{\theta} \implies (\bar{\psi} \implies \bar{\theta})$. De éste mismo modo se prosigue con K2 y K3.

Si $\mathrm{S}_x^c\,\phi \equiv \forall y\ \theta \implies \mathrm{S}_y^t\,\theta$ (K4) –donde x no está ligado ni en θ ni en t por premisa–, entonces, por (I)

$$\mathrm{S}_x^c\,\phi \equiv \forall y\ \mathrm{S}_x^c\,\bar{\theta} \implies \mathrm{S}_y^{\mathrm{S}_x^c\,\bar{t}}\,\mathrm{S}_x^c\,\bar{\theta} \equiv \mathrm{S}_x^c\,\forall y\,\bar{\theta} \implies \mathrm{S}_x^c\,\mathrm{S}_y^{\bar{t}}\,\bar{\theta}$$

de modo que por (II) se obtiene que $\phi \equiv \forall y\ \bar{\theta} \implies \mathrm{S}_y^{\bar{t}}\,\bar{\theta}$.

<u>Caso inductivo:</u> Sea $\phi_1, \dots, \phi_n$ una demostración de $\mathrm{S}_x^c\,\phi$. Si ϕ_n es un axioma remitimos al caso anterior, de lo contrario es una inferencia en alguno de los dos casos:

a) <u>*Modus ponens:*</u> Luego $\mathrm{S}_x^c\,\phi$ viene inferido de ϕ_i y $\phi_i \implies \mathrm{S}_x^c\,\phi$. Por (I), se da que $\phi_i \equiv \mathrm{S}_x^c\,\theta$ y por hipótesis inductiva se cumple que $\vdash_{K_{\mathcal{L}}} \theta$ y $\vdash_{K_{\mathcal{L}}} \theta \implies \phi$; luego por MP se cumple que $\vdash_{K_{\mathcal{L}}} \phi$.

b) <u>Introducción del generalizador:</u> Luego $\mathrm{S}_x^c\,\phi \equiv \forall y \phi_i$ que viene inferido de ϕ_i. Como $\phi_i \equiv \mathrm{S}_x^c\,\theta$, por hipótesis inductiva se cumple $\vdash_{K_{\mathcal{L}}} \theta$ y por IG se cumple que $\vdash_{K_{\mathcal{L}}} \forall y \theta \equiv \phi$. □

Lema 6.36: Sea $\Gamma \cup \{\exists x : \phi\}$ es un conjunto de sentencias consistente en $\mathcal{L}$, $\mathcal{L}' := \mathcal{L} \cup \{c\}$ donde c es una constante no contenida en $\mathcal{L}$; entonces el conjunto de sentencias $\Gamma \cup \{\exists x\ \phi\} \cup \{\mathrm{S}_x^c\,\phi\}$ es consistente en $\mathcal{L}'$.

DEMOSTRACIÓN: Lo haremos por contrarrecíproca: Si $\Gamma \cup \{\exists x\ \phi\} \cup \{\mathrm{S}_x^c\, \phi\}$ es contradictorio, entonces $\Gamma \cup \{\exists x\ \phi\} \vdash_{K_{\mathcal{L}'}} \neg\, \mathrm{S}_x^c\, \phi$. Luego, una demostración involucra finitas sentencias $\theta_1, \dots, \theta_n$ de Γ tales que

$$\theta_1 \wedge \cdots \wedge \theta_n \wedge \exists x\ \phi \underset{K_{\mathcal{L}'}}{\vdash} \neg\, \mathrm{S}_x^c\, \phi$$

podemos elegir una variable y que no esté en θ_i ni en $\exists x\ \phi$, luego por el teorema de deducción se obtiene que

$$\underset{K_{\mathcal{L}'}}{\vdash} \theta_1 \wedge \cdots \wedge \theta_n \wedge \exists x\ \phi \implies \mathrm{S}_y^c\, \mathrm{S}_x^y\, \neg\phi$$
$$\underset{K_{\mathcal{L}'}}{\vdash} \mathrm{S}_y^c(\theta_1 \wedge \cdots \wedge \theta_n \wedge \exists x\ \phi \implies \mathrm{S}_x^y\, \neg\phi).$$

Luego, por el lema se concluye que $\Gamma \cup \{\exists x\ \phi\} \vdash_{K_{\mathcal{L}}} \neg\, \mathrm{S}_x^y\, \phi$. Nótese que por IG y por NP se concluye que $\Gamma \cup \{\exists x\ \phi\} \vdash_{K_{\mathcal{L}}} \neg\exists y\ \mathrm{S}_x^y\, \phi$, o lo que es equivalente que $\Gamma \cup \{\exists x\ \phi\} \vdash_{K_{\mathcal{L}}} \neg\exists x\ \phi$; lo que prueba que $\Gamma \cup \{\exists x\ \phi\}$ es contradictorio. □

Teorema 6.37: Sean Γ un conjunto de sentencias consistente en $\mathcal{L}$, y $\mathcal{L}' := \mathcal{L} \cup \{c_0, c_1, c_2, \cdots\}$ donde c_i son constantes no contenidas en $\mathcal{L}$. Luego existe una extensión numerable Γ' maximalmente consistente y ejemplificada de Γ.

DEMOSTRACIÓN: Sea $(\phi_n)_{n\in\mathbb{N}}$ una enumeración de sentencias de $\mathcal{L}'$. Construyamos Γ_n por recursión: $\Gamma_0 :\equiv \Gamma$ y

$$\Gamma_{n+1} :\equiv \begin{cases} \Gamma_n, & \text{si } \Gamma_n \cup \{\phi_n\} \text{ es contradictorio} \\ \Gamma_n \cup \{\phi_n\}, & \text{si es consistente y } \phi_n \text{ no es de la forma } \exists x\ \theta \\ \Gamma_n \cup \{\phi_n\} \cup \{\mathrm{S}_x^{c_k}\, \theta\}, & \text{si es consistente y } \phi_n \text{ es de la forma } \exists x\ \theta, \\ & \text{donde } c_k \text{ es el primer } c_i \text{ que no está contenido} \\ & \text{en ninguna sentencia de } \Gamma_n. \end{cases}$$

Similar al lema de Lindenbaum podemos probar que $\Gamma_\infty := \bigcup_{n\in\mathbb{N}} \Gamma_n$ es maximalmente consistente y ejemplificado. □

Teorema 6.38 – *Teorema de completitud fuerte*: Si Γ es un conjunto de sentencias consistente en $\mathcal{L}$, entonces posee un modelo numerable. En particular, toda teoría axiomática consistente es satisfacible.

Demostración: Ahora podemos construir el modelo M explícitamente: Sea Γ_∞ una extensión maximalmente consistente y ejemplificada de Γ.

1. Sea U, el universo de nuestro modelo, como las clases de la relación de equivalencia $i \sim j$ syss $t_i = t_j$ en Γ_∞, donde $(t_n)_{n\in\mathbb{N}}$ es una enumeración prefijada de los $\mathcal{L}'$-designadores (¿por qué es una relación de equivalencia?).
2. Para toda $\mathcal{L}'$-constante c_i se cumple que $c_i = t_{j_i}$, pues toda constante es un designador, luego $M(c_i) := [j_i]_\sim$ es una interpretación válida.
3. Para todo funtor n-ádico f_j^n se define una función $\bar{f}_j^n : U^n \to U$ dado por $\bar{f}_j^n([i_1], \dots, [i_n]) := [k]$ tal que $t_k := f_j^n(t_{i_1}, \dots, t_{i_n})$.
4. Para todo relator n-ádico R_j^n se define la relación $\bar{R}_j^n \subseteq U^n$ dado por $([i_1], \dots, [i_n]) \in \bar{R}_j^n$ syss $R_j^n(t_{i_1}, \dots, t_{i_n}) \in \Gamma_\infty$.

Por las reglas de inferencia: IF y ER se cumple que las funciones y relaciones de M están bien definidos y coinciden con su interpretación.

Finalmente hay que probar que $M \vDash \Gamma$, es decir, para todo $\phi \in \Gamma$ hay que probar que $M \vDash \phi$. En su lugar demostraremos que $M \vDash \Gamma_\infty$ por inducción sobre la cantidad de conectores lógicos que posean:

Caso base: Si ϕ no posee conectores lógicos, entonces es de la forma $\phi \equiv R_i^n(t'_1, \dots, t'_n)$. Si todos los términos de ϕ son designadores, entonces es claro que $M \vDash \phi$. De lo contrario, supongamos que sus variables libres son $x_{i_1}, \dots, x_{i_k}$ y sea v una valoración que evalue a ϕ, podemos asumir que ésta remplaza x_{i_1} por $[j_1]$, x_{i_2} por $[j_2]$ y así (recuerdese que las valoraciones sustituyen por elementos del universo). Nótese que se cumple que

1.	$\phi(x_{i_1}, \dots, x_{i_k})$	Teorema de Γ
2.	$\forall x_{i_1}\ \phi(x_{i_1}, \dots, x_{i_k})$	IG 1
3.	$\mathrm{S}_{x_{i_1}}^{t_{j_1}}\ \phi(x_{i_1}, \dots, x_{i_k})$	EG 2
4.	$\phi(t_{j_1}, \dots, x_{i_k})$	R 3

y de manera análoga se demuestra que $\Gamma_\infty \vdash \phi(t_{j_1}, \dots, t_{j_k})$, ergo $\phi(t_{j_1}, \dots, t_{j_k}) \in \Gamma_\infty$ y $M \vDash \phi[v]$. Como v era una valoración arbitraria se nota que aplica para toda valoración.

Caso inductivo: Aquí dividimos a ϕ según sus conectores lógicos:

a) Si $\phi \equiv \neg\theta$, entonces como $\phi \in \Gamma_\infty$, y por consistencia se concluye que $\theta \notin \Gamma_\infty$ luego no $M \vDash \theta$; pero por definición ésto significa que $M \vDash \phi$.

b) Si $\phi \equiv \theta \implies \psi$, entonces, como $\Gamma_\infty \vdash \phi$ se tiene que o $\Gamma_\infty \vdash \psi$ (en cuyo caso ϕ se deduce de K1 y MP) o $\Gamma_\infty, \neg\psi \vdash \neg\theta$ (por MT). Habíamos visto que $M \vDash \phi$ si $M \vDash \psi$ o no $M \vDash \theta$, luego en el primer caso se da que $M \vDash \psi$ y por el item anterior se comprueba que en el segundo caso se que no $M \vDash \theta$.

c) Si $\phi \equiv \forall x\, \theta$. Entonces $M \vDash \forall x\, \theta$ syss para todo $[j] \in U$ se cumple que $M \vDash \theta[v_x^{[j]}]$ lo que es equivalente a ver que $\mathrm{S}_x^{t_j}\, \theta \in \Gamma_\infty$, ques es cierto pues $(\forall x\, \theta) \in \Gamma_\infty$ y se deduce de K4 y MP. □

De éste teorema se desprenden varios corolarios:

Teorema 6.39 (Löwenheim-Skolem): Una teoría axiomática es satisfacible syss posee un modelo numerable.

> ***Teorema 6.40 – Teorema de compacidad de Gödel:*** Una teoría axiomática es consistente syss es finitamente satisfacible.

Demostración: $\implies$. Si una teoría es consistente, entonces es satisfacible, entonces posee un modelo M. Dicho modelo M satisface todo subconjunto finito de los axiomas propios de la teoría.

$\impliedby$. Por contrarrecíproca supongamos que la teoría axiomática no es satisfacible, por lo que por el teorema de completitud fuerte se da que es contradictorio. Luego una demostración de una contradicción es finita, ergo, emplea finitos axiomas de la teoría, los que forman un subconjunto finito que no es satisfacible. □

> ***Teorema 6.41 – Teorema de completitud de Gödel:*** Sea T una teoría axiomática. Entonces, para toda sentencia ϕ se cumple que $T \vDash \phi$ syss $T \vdash \phi$.

Es decir todo aquello que es verdad admite alguna demostración lógica.

Índice de notación

$\mathrm{alt}(A)$	$= \sup\{\mathrm{alt}_A(x) + 1 : x \in A\}$, altura del árbol A, p. 108.
$\mathcal{L}$	Un lenguaje formal, p. 115.
$M \models \phi[v]$	La interpretación de ϕ bajo la valoración v sobre el modelo M es verdadera, p. 120.
$\Gamma \vdash_F \theta$	Desde las premisas Γ se demuestra θ en el sistema deductivo F. Si se obvia F se asume que $F = K_{\mathcal{L}}$, p. 124.
$\Gamma \vdash\dashv \Delta$	$= \Gamma \vdash \Delta$ y $\Delta \vdash \Gamma$, p. 124.
$K_{\mathcal{L}}$	El sistema deductivo de la lógica de predicados, p. 125.

Bibliografía

Las fechas empleadas son aquellas de la primera publicación o del primer registro de Copyright.

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. Herrlich, H. *Axiom of Choice* (Springer-Verlag Berlin Heidelberg, 2006).
4. Jech, T. *Set Theory* (Springer-Verlag Berlin Heidelberg, 2002).
5. Just, W. y Weese, M. *Discovering Modern Set Theory* (American Mathematical Society, 1991).
6. Lévy, A. *Basic Set Theory* (Dover Publications, Inc., 1979).
7. Rubin, H. y Rubin, J. *Equivalents of the Axiom of Choice* (North-Holland, 1963).
8. Vidal, J. C. *Teoría de Conjuntos* `https://www.uv.es/~jkliment/Documentos/SetTheory.pc.pdf` (2010).

Teoría de modelos

9. Castillo, C. I. *Lógica matemática* `https://www.uv.es/ivorra/Libros/LM.pdf` (2020).

10. KUNEN, K. *The Foundations of Mathematics* ISBN: 978-1-904987-14-7 (College Publications, 2009).
11. MARKER, D. *Model theory. An introduction* (Springer Verlag New York, 2002).
12. TAKEUTI, G. *Proof Theory* (Elsevier Science, 1975).

Historia

13. BLASS, A. en *Ω-Bibliography of Mathematical Logic. Set Theory* (ed. MÜLLER, G. H.) xv-xxx (Springer-Verlag Berlin Heidelberg, 1987).

Artículos

14. GILLMAN, L. Two Classical Surprises Concerning the Axiom of Choice and the Continuum Hypothesis. *The American Mathematical Monthly* **109.** doi:10.2307/2695444. https://www.maa.org/sites/default/files/pdf/upload_library/22/Ford/Gillman544-553.pdf (2002).

Libros de autoría propia

15. CUEVAS, J. *Álgebra* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf (2022).
16. CUEVAS, J. *Teoría de categorías y álgebra homológica* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/cats/teoria-categorias.pdf (2022).
17. CUEVAS, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).

Índice alfabético