Carlos Ivorra Castillo

TEORÍA DE CONJUNTOS

Un conjunto es un "muchos" que puede ser pensado como uno.

Georg Cantor

Índice General

Introducción

El propósito de este libro es proporcionar una introducción axiomática rigurosa a la teoría de conjuntos que no presuponga del lector ningún conocimiento técnico de la lógica matemática más allá de una cierta familiaridad con las técnicas de razonamiento informal-formalizable que emplean habitualmente los matemáticos.

Naturalmente, una fundamentación sólida de la teoría de conjuntos *presupone* la lógica formal, y a este respecto podemos decir que "oficialmente" este libro debe considerarse como la continuación de mi libro de *Lógica matemática* ([LM]), en el que, entre otras cosas, se discuten con todo el detalle y los tecnicismos necesarios diversas teorías axiomáticas de conjuntos, entre ellas la de Zermelo-Fraenkel (ZFC) y la de von Neumann-Bernays-Gödel (NBG). Sin embargo, aquí hemos optado por exponer la teoría axiomática de modo que no ha sido necesario hacer ninguna referencia explícita a [LM], de tal forma que quien lea [LM] y continúe con este libro, no sólo no encontrará ninguna laguna entre ambos, sino que de hecho hallará varios solapamientos, los que hemos considerado necesarios para que el lector familiarizado con el razonamiento matemático pueda suplir con dicha familiaridad los requisitos técnicos que proporciona [LM].

De este modo, [LM] y el presente libro suponen dos propuestas alternativas para introducirse en la teoría de conjuntos: o bien empezando por los fundamentos lógicos de [LM] para después adentrarse en los contenidos matemáticos de las teorías de conjuntos allí presentadas, o bien empezar por una introducción axiomática a la teoría de conjuntos apoyada en la familiaridad del lector con el razonamiento matemático para después (opcionalmente) profundizar en sus aspectos lógicos a través de [LM].

Puesto que la distinción entre conjuntos y clases propias resulta inevitable, para eliminar por completo las dificultades conceptuales que conlleva (que se discuten con detalle en [LM]) hemos optado por partir de la teoría axiomática de von Neumann-Bernays-Gödel NBG en lugar de la más habitual, que es ZFC, puesto que así el concepto de clase propia es un concepto formal más que no debería presentar ninguna dificultad especial al lector, en lugar de un concepto metamatemático que tiene que entenderse necesariamente en términos de conceptos lógicos. No obstante, ambas teorías son equivalentes, y el lector familiarizado con [LM] se dará cuenta de que, pasado el capítulo I (en el que exponemos la axiomática básica de NBG), las siglas NBG pueden ser trivial y sistemáticamente

sustituidas por ZFC sin necesidad de modificar absolutamente nada de lo dicho.

En el capítulo II completamos la exposición de los resultados conjuntistas básicos que sirven de fundamento al resto de las disciplinas matemáticas con la construcción del sistema numérico, mientras que los capítulos siguientes, hasta el V exponen los resultados fundamentales de la teoría de conjuntos cantoriana (principalmente la teoría de ordinales y de cardinales), sin perjuicio de que se presenten muchos resultados muy posteriores en el tiempo a la época de Cantor.

Los capítulos siguientes exponen temas más avanzados. El límite principal que nos hemos impuesto al elegir los contenidos ha sido evitar todos aquellos que requieren considerar modelos de la teoría de conjuntos (con todos los aspectos sobre lógica y metamatemática que ello requeriría). No obstante, en el capítulo X presentamos los resultados básicos de la teoría de modelos, pero sin entrar, según acabamos de decir, en el estudio de modelos de la propia teoría de conjuntos, evitando así la necesidad de introducir distinciones sutiles entre fórmulas metamatemáticas y fórmulas definidas en la teoría axiomática. Los capítulos VII y X pueden verse en gran medida como los preliminares necesarios (junto con [LM]) para abordar los problemas relativos a pruebas de consistencia.

Finalmente hemos incluido dos apéndices, en el primero de los cuales probamos que la existencia de bases en espacios vectoriales es equivalente al axioma de elección y demostramos algunos resultados adicionales sobre bases y dimensión de espacios vectoriales. En el segundo damos varias pruebas de la existencia de subconjuntos de $\mathbb{R}$ no medibles Lebesgue, sin la propiedad de Baire y sin subconjuntos perfectos a partir de distintas consecuencias del axioma de elección.

A partir del capítulo VII empiezan a ser necesarios —principalmente en las aplicaciones— resultados topológicos, para los cuales remitimos a mi libro de topología, indicado como [T], el cual a su vez depende de los resultados de este libro. En la introducción de [T] se muestra una tabla que indica una forma posible de compaginar la lectura de ambos libros.

Los únicos resultados que se enuncian sin demostración en este libro son los que afirman la consistencia y la independencia de algunas de las afirmaciones consideradas (como la hipótesis del continuo, la existencia de cardinales inaccesibles, etc.) En algunos casos se esbozan sin rigor los argumentos que permiten concluir que determinados hechos no pueden ser demostrados en NBG (o, equivalentemente, en ZFC). Naturalmente, estas observaciones no demostradas no se usan en ningún momento, salvo para relacionar unas con otras.

Capítulo I

El lenguaje de la teoría de conjuntos

Dedicamos este primer capítulo a presentar los conceptos básicos del lenguaje conjuntista que impregna todas las ramas de la matemática: conjuntos, funciones, relaciones, productos cartesianos, etc.

Si tomamos cualquier concepto matemático, como pueda ser el concepto de "derivada", veremos que todas las propiedades que se demuestran sobre él se deducen en última instancia de su definición, la cual lo reduce a otros conceptos más elementales, como son el de "función", el de "número real", etc. A su vez, estos conceptos pueden definirse a partir de otros más simples, pero este proceso no puede continuar indefinidamente. Tras un número finito de pasos tenemos que llegar a unos conceptos tan elementales que no sean susceptibles de ser definidos en términos de otros más elementales aún. El lector podría especular sobre cuántos son esos conceptos fundamentales, cuántos conceptos primitivos son necesarios para que a partir de ellos puedan definirse los miles y miles de conceptos que manejan los matemáticos. La respuesta es sorprendentemente simple: son suficientes dos conceptos, el de "conjunto" y el de "pertenencia".

Un "conjunto" pretende ser una colección de objetos, y la "pertenencia" pretende ser la relación que puede darse entre un objeto dado y un conjunto dado: si el objeto es uno de los que forman parte del conjunto, se dice que el objeto "pertenece" al conjunto (o que es un elemento del conjunto) y en caso contrario que "no le pertenece".

El lector podría decir en este punto: Pues bueno, acabamos de definir los conceptos de "conjunto" y "pertenencia". ¿Qué tienen de indefinibles? La respuesta es que el párrafo anterior dista mucho de ser una definición en el sentido matemático riguroso. Si quisiéramos razonar acerca de los conjuntos y de la pertenencia a partir de las "definiciones" que acabamos de dar, nos veríamos obligados a recurrir tácitamente a numerosos prejuicios sobre lo que se supone que deben cumplir las colecciones de objetos. Y esto resulta inviable, pues la

historia de la Matemática nos enseña que, cuando uno trata de profundizar en la teoría de conjuntos sin pararse a explicitar convenientemente sus fundamentos, termina encontrándose con *paradojas,* es decir con demostraciones aparentemente válidas de determinadas afirmaciones y también de sus negaciones.

Para evitar que en nuestra teoría de conjuntos surjan contradicciones, nos aseguraremos de explicitar las propiedades que vamos a admitir sobre las colecciones de objetos y la pertenencia mediante una lista de axiomas —los cuales están pensados precisamente para invalidar todos los razonamientos conocidos que dan lugar a paradojas— y no admitiremos ningún razonamiento que contenga implícita o explícitamente nada que no pueda justificarse a partir de dichos axiomas.

Existen varias formas alternativas de "desterrar" las paradojas de la teoría de conjuntos, cada una basada en su propio "truco" ingenioso. Preparando el terreno para el que vamos a emplear nosotros, vamos a reservar la palabra "conjunto" para darle un significado más preciso más adelante y, de momento, para referirnos a las "colecciones de objetos" de las que queremos hablar, usaremos la palabra "clase" en lugar de "conjunto".

Quizá el lector piense que, según lo que estamos diciendo, no va a haber dos, sino tres conceptos fundamentales: el de "clase", el de "pertenencia" y el de los "objetos" que pueden pertenecer o no a una clase dada. Podríamos plantearlo así, pero sucede que los matemáticos definen a menudo clases cuyos elementos son a su vez otras clases, y al final resulta que este tipo de clases a las cuales sólo pertenecen otras clases resultan ser las únicas realmente necesarias para fundamentar todas las matemáticas. Por lo tanto, para no introducir complicaciones innecesarias en la teoría, vamos a considerar que los objetos que pertenecen a cualquier clase dada serán a su vez otras clases.[1]

Las paradojas que afectan a la teoría ingenua de conjuntos (la que resulta de razonar "alegremente" sobre las colecciones de objetos sin más base que lo que nos parece razonable que deberían cumplir) no se deben a confusiones sobre qué es un razonamiento lógico correcto y qué no lo es, sino sólo sobre qué premisas podemos aceptar que cumplen las colecciones de objetos y cuáles no. Por ello, dado que la lógica pura no es un problema, no trataremos de precisar la noción de "razonamiento lógico puro", sino que daremos por hecho que el lector sabe razonar correctamente, y en particular que es consciente de hechos como que si $A = B$ entonces $B = A$, etc.

[1] Quizá al lector le parezca extraño —por no decir imposible— que podamos hablar de clases de objetos sin que haya en última instancia ningún objeto que no sea a su vez una clase. Lo que sucede es que en la teoría que vamos a desarrollar habrá una clase vacía (una clase sin elementos) que representaremos por $\varnothing$, a partir de la cual se pueden formar otras clases como $\{\varnothing\}$, o $\{\{\varnothing\}\}$, o $\{\varnothing, \{\varnothing\}\}$, etc. Y así podemos definir infinitas clases, todas ellas construidas —en un número finito o infinito de pasos— a partir de la clase vacía. Lo que decimos es que éstas son más que suficientes para construir todos los objetos con los que trabajan los matemáticos.

1.1 Clases y conjuntos

Convenimos en usar letras cualesquiera, como $A, B, C, \ldots$ como variables que hacen referencia a *clases.* Escribiremos $A \in B$ para indicar que la clase A *pertenece* a la clase B y $A \notin B$ para indicar que A no pertenece a B.

Según acabamos de explicar, nuestra intención es que las clases representen "colecciones de clases", de modo que $A \in B$ signifique que la clase B es una colección de clases entre las cuales figura la clase A, pero técnicamente estos dos conceptos de "clase" y "pertenencia" serán los dos únicos conceptos primitivos (no definidos) de los que vamos a partir, es decir, que sólo aceptaremos una afirmación sobre clases y pertenencia si podemos demostrarla a partir de la lógica pura (es decir, sin presuponer nada en absoluto sobre qué son las clases o qué es la pertenencia entre clases) o a partir de las afirmaciones que tomaremos explícitamente como axiomas.

El *lenguaje de la teoría de conjuntos*[2] es el lenguaje que consta de variables arbitrarias, el signo $\in$ y los signos lógicos:

$$=, \quad \neg, \quad \to, \quad \vee, \quad \wedge, \quad \leftrightarrow, \quad \bigwedge, \quad \bigvee.$$

No vamos a describir las reglas gramaticales de este lenguaje, pues, aunque las vamos a respetar, nunca serán relevantes y siempre podremos sustituir las afirmaciones expresadas en él por sus equivalentes en el lenguaje natural. Por ejemplo,

$$\bigwedge ABC(A = B \wedge B = C \to A = C)$$

es una fórmula del lenguaje de la teoría de conjuntos y, más concretamente, es un teorema lógico, que puede expresarse equivalentemente así:

> *Si una clase A es igual a otra B, y ésta a su vez es igual a una tercera clase C, entonces también A es igual a C.*

Decimos que es un teorema lógico porque es algo que podemos afirmar sobre las clases sin el más mínimo presupuesto sobre qué son. Se trata de una afirmación puramente lógica que seguiría siendo válida si en vez de hablar de clases estuviéramos hablando de conejos silvestres.

Es indiferente expresar este hecho de cualquiera de las dos formas. Lo que es crucial es entender que si la segunda afirmación puede considerarse una afirmación matemática rigurosa es precisamente porque también puede escribirse de la primera forma, aunque en la práctica no es necesario hacerlo. Basta con saber que puede hacerse. No puede decirse lo mismo de:

[2] Aquí nos referimos al "lenguaje" en el sentido técnico del sistema de signos y reglas gramaticales que determinan qué sucesiones de signos constituyen una afirmación válida y cuáles son meros sinsentidos, como $=\in A == B$. No debemos confundir este concepto técnico de "lenguaje" con el concepto informal que da título a este capítulo, donde al hablar del "lenguaje de la toería de conjuntos" nos referimos al "vocalbulario conjuntista" que se usa habitualmente en matemáticas.

Si una clase A tiene más o menos el mismo tamaño que otra clase B, y ésta a su vez es de un tamaño similar a C, entonces también A y C son aproximadamente del mismo tamaño.

Esto no es una afirmación matemática rigurosa porque no hemos dado ninguna definición precisa de lo que es el "tamaño" de una clase, ni mucho menos de lo que es "tener aproximadamente el mismo tamaño", y las únicas nociones no definidas que vamos a aceptar son la de "clase" y la de "pertenencia".

Cualquier teorema matemático riguroso puede expresarse exclusivamente en términos del signo $\in$, los signos lógicos y variables, pero si pretendiéramos plantearlo así, nos encontraríamos con que un teorema elemental como que $\pi > 3.14$ requeriría decenas de páginas sólo para ser enunciado, y muchas más para ser demostrado sin usar ningún otro signo matemático. Lo que se hace en la práctica es definir nuevos conceptos matemáticos en términos de los conceptos primitivos que acabamos de describir o de otros conceptos definidos previamente. Veamos con detalle un ejemplo de este proceso:

Definición 1.1 Diremos que una clase A es una *subclase de* (o que *está contenida o incluida en*) otra clase B, y lo representaremos por $A \subset B$, si todo elemento de A es también un elemento de B. Equivalentemente:

$$A \subset B \equiv \bigwedge x(x \in A \to x \in B).$$

Diremos que la inclusión es *estricta* (y lo representaremos por $A \subsetneq B$) si además se cumple que $A \neq B$.

Tenemos así dos formas equivalentes de definir la inclusión entre clases. En primer lugar hemos dado la definición en el lenguaje natural, y en segundo lugar en el lenguaje formal de la teoría de conjuntos. Es irrelevante usar una u otra forma. Sólo hay que tener presente que la primera forma es una definición matemática rigurosa precisamente porque puede traducirse a la segunda forma, aunque, sabiendo que es así, no es necesario hacerlo.

Sólo necesitamos recurrir a la lógica pura para demostrar ahora algunos teoremas matemáticos, como:

$$\bigwedge A\ A \subset A, \qquad \bigwedge ABC(A \subset B \wedge B \subset C \to A \subset C).$$

Por ejemplo, la prueba de la segunda afirmación es como sigue:

Suponemos que $A \subset B$ y $B \subset C$. Queremos probar que $A \subset C$, lo cual significa que cualquier clase $x \in A$ debe cumplir también $x \in C$. Suponemos, pues que $x \in A$ y entonces vemos que, aunque no tengamos ni idea de qué significa $x \in A$, la hipótesis $A \subset B$ nos garantiza que también se va a cumplir $x \in B$ y, aunque no tengamos ni idea de lo que esto significa, la hipótesis $B \subset C$ nos garantiza que $x \in C$. ∎

Esta demostración, a pesar de su simplicidad, resume perfectamente la naturaleza del razonamiento lógico: hemos probado que $x \in A \to x \in C$ sin necesidad de presuponer nada sobre qué clase de cosas son x, A, C y sin presuponer nada sobre qué significa $x \in A$ o $x \in C$.

Sin embargo, nuestra capacidad de razonamiento basada en la lógica pura es muy limitada. Por ejemplo, consideremos la afirmación siguiente:

$$\bigwedge AB(\bigwedge x(x \in A \leftrightarrow x \in B) \leftrightarrow A = B)$$

Equivalentemente, podríamos parafrasearla así:

Dos clases A y B son iguales si y sólo si tienen los mismos elementos.

No podemos demostrar tal cosa. Lo que sí podemos probar es que si $A = B$, entonces $x \in A$ es equivalente a $x \in B$, porque $A = B$ significa que A y B nombran en realidad a la misma clase —sea lo que sea una clase—, luego $x \in A$ y $x \in B$ son en realidad un mismo hecho —sea cual sea ese hecho—. Ahora bien, si suponemos que dos clases A y B tienen los mismos elementos, nada nos permite concluir que tienen que ser la misma clase.

El lector podría objetar: pero sí que tienen que serlo. Si hemos dicho que las clases A y B son colecciones de objetos (colecciones de otras clases, para ser más precisos) y resulta que A y B contienen exactamente las mismas clases, entonces es que son la misma colección de clases, luego son la misma cosa, son iguales.

El problema del "razonamiento" precedente es que se basa en que las clases son precisamente "colecciones de clases" y la pertenencia es la pertenencia. Por ejemplo, la afirmación anterior sería claramente falsa si las clases A, B, x fueran conejos silvestres y $x \in A$ significara "el conejo x es el padre del conejo A", porque en tal caso, lo que estamos afirmando es que si dos conejos A y B tienen el mismo padre, entonces son necesariamente el mismo conejo, y esto es falso.

Desde el momento en que la afirmación anterior es falsa si se interpretan los conceptos de "clase" y "pertenencia" de un determinado modo (como "conejo silvestre" y "ser padre de", respectivamente), tenemos que admitir que es imposible demostrarla desde la lógica pura, y que cualquier intento de demostración tendría que recurrir, explícita o implícitamente, a que los conceptos de "clase" y "pertenencia" significan una cosa y no otra. En otras palabras, se tendría que basar en algún tipo de definición de "clase" y "pertenencia", que es justo lo que no tenemos.

Ahora bien, el lector tendría razón en alegar que lo que expresa la afirmación anterior es algo razonable que deberían cumplir las clases y la pertenencia si es que tienen que ser lo que pretendemos que sean. En general, no podemos admitir irreflexivamente todo lo que nos parezca "razonable" sobre clases y pertenencia sin acabar cayendo en paradojas, pero sucede que esta afirmación en particular es una de las que la axiomática que vamos a adoptar acepta como válida, y por ello, para legitimar su uso, la vamos a convertir en nuestro primer axioma:

Axioma de Extensionalidad *Si dos clases tienen los mismos elementos, entonces son iguales, es decir,*

$$\bigwedge AB(\bigwedge x(x \in A \leftrightarrow x \in B) \to A = B).$$

El axioma de extensionalidad afirma que si dos clases no se diferencian por sus elementos, entonces no se diferencian por nada (son iguales) o —dicho de otro modo— que una clase no es ni más ni menos que la colección de sus elementos. Ya hemos señalado que el recíproco del axioma de extensionalidad sí que es un teorema lógico que puede probarse sin necesidad de ningún axioma matemático.

Por ejemplo, ahora podemos demostrar las propiedades básicas de la inclusión de clases:

Teorema 1.2 *Se cumple:*

1. $\bigwedge A\ A \subset A$,
2. $\bigwedge AB(A \subset B \wedge B \subset A \to A = B)$,
3. $\bigwedge ABC(A \subset B \wedge B \subset C \to A \subset C)$.

Demostración: Ya hemos demostrado 3), que es un teorema puramente lógico, al igual que 1), cuya prueba es mucho más simple. Por el contrario, el teorema 2) requiere el axioma de extensionalidad (y de hecho es equivalente a él). Si suponemos que $A \subset B \wedge B \subset A$, entonces tenemos que todo $x \in A$ cumple $x \in B$, y viceversa, es decir, que $x \in A \leftrightarrow x \in B$, luego por el axioma de extensionalidad concluimos que $A = B$. ∎

Lo importante que el lector debe extraer de este resultado, más allá de la trivialidad de lo que afirma en sí mismo, es que en él se pone de manifiesto cómo es posible razonar de forma totalmente rigurosa con unos objetos (las clases) y una propiedad (la pertenencia) que nunca hemos definido de ninguna forma. No importa lo que sean las clases y la pertenencia, que —mientras cumplan el axioma de extensionalidad— tendrán que cumplir necesariamente el teorema anterior. Toda demostración matemática, por sofisticada que sea, es de la misma naturaleza, con la única diferencia de que puede apoyarse en algunos axiomas más que vamos a ir introduciendo paulatinamente.

El lector podría pensar que el axioma de extensionalidad ya plasma la idea de que las clases no son ni más ni menos que colecciones de clases, pero en realidad sólo plasma la mitad de esta idea, pues no garantiza que cualquier colección de clases que un matemático esté interesado en considerar sea realmente la colección de los elementos de una determinada clase. Introduzcamos un axioma que exprese esta idea:

Axioma de comprensión* *Si $\phi(x)$ es una fórmula del lenguaje de la teoría de conjuntos (tal vez con más variables, además de la x explícita), entonces existe una clase A cuyos elementos son las clases que cumplen $\phi(x)$. Equivalentemente:*

$$\bigvee A \bigwedge x(x \in A \leftrightarrow \phi(x)).$$

La clase A cuya existencia afirma el axioma de comprensión es única, pues dos clases que cumplan lo indicado tendrían los mismos elementos, a saber, las clases x que cumplen $\phi(x)$, luego por el axioma de extensionalidad tienen que ser la misma clase.

Cuando un concepto es único podemos darle nombre. Así, a la clase A dada por el axioma de comprensión para la fórmula $\phi(x)$ la representaremos por

$$\{x \mid \phi(x)\}.$$

De este modo, si definimos una clase $A = \{x \mid \phi(x)\}$, la afirmación $x \in A$ es equivalente a $\phi(x)$.

Definición 1.3 He aquí algunas definiciones de clases basadas en el axioma de comprensión:

1. La *unión* de dos clases es $A \cup B = \{x \mid x \in A \vee x \in B\}$.
2. La *intersección* de dos clases es $A \cap B = \{x \mid x \in A \wedge x \in B\}$.
3. La *diferencia* de dos clases es $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.
4. El *complemento* de una clase es $\overline{A} = \{x \mid x \notin A\}$.
5. La *clase vacía* es $\varnothing = \{x \mid x \neq x\}$.
6. La *clase universal* es $V = \{x \mid x = x\}$.

La paradoja de Russell Observemos que la clase vacía es la única clase sin elementos (si dos clases no tienen elementos, entonces ambas tienen los mismos elementos —ninguno—, luego por el axioma de extensionalidad son iguales), mientras que la clase universal contiene a todas las clases. Tenemos así un ejemplo de clase que cumple $V \in V$ (se pertenece a sí misma), mientras que otras clases, como $\varnothing$, cumplen $\varnothing \notin \varnothing$.

Podemos, pues, dividir a las clases en dos categorías: las que se pertenecen a sí mismas y las que no. Definimos la *clase de Russell* como la clase R de todas las clases que no se pertenecen a sí mismas, equivalentemente:

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

Ahora tiene pleno sentido plantearse de cuál de las dos categorías es R, es decir, si $R \in R$ o si, por el contrario, $R \notin R$. Sin embargo, en este punto nos encontramos con una paradoja: si suponemos que $R \notin R$, entonces, R cumple justo la propiedad que define a R, por lo que debería ser $R \in R$ y tenemos una contradicción. Esto nos lleva a que tiene que ser $R \in R$, pero entonces R debe cumplir la propiedad que la define, luego tendría que ser $R \notin R$, luego resulta que ambas posibilidades son contradictorias.

Vemos así que el axioma de comprensión que hemos dado nos permite definir una clase R que no puede existir. En otras palabras, introduce una paradoja en la teoría de conjuntos. (Ése es el significado del asterisco que hemos puesto junto a él: indica que es un axioma contradictorio y que, por consiguiente, no es aceptable.)

Ahora el lector puede entender por qué las precauciones a la hora de "filtrar" los razonamientos admisibles sobre "colecciones de objetos" a través de unos

axiomas cuidadosamente elegidos para evitar paradojas no son gratuitas. La paradoja de Russell es la más sencilla, pero no la única a la que llegaríamos si admitiéramos indiscriminadamente que las clases satisfacen afirmaciones "plausibles" basadas en nuestra idea "vaga" de lo que debería ser una colección de clases. ∎

Conjuntos La paradoja de Russell nos obliga a descartar el axioma de comprensión tal y como lo hemos formulado, pero seguidamente presentaremos una modificación que cierra el paso a todas las paradojas conocidas de la teoría de conjuntos ingenua. El "truco" que vamos a emplear es de Gödel y se basa en definir como sigue el concepto de "conjunto":

Definición 1.4 Diremos que una clase es un *conjunto* si pertenece al menos a otra clase, es decir:

$$\mathrm{cto}\, A \equiv \bigvee B\, A \in B.$$

Las clases que no son conjuntos se llaman *clases propias.*

Así pues, en lo sucesivo no vamos a admitir sin más que cualquier clase puede ser elemento de otra clase, sino que nos vamos a reservar el derecho —según nos convenga— de conceder o no a cada clase el permiso necesario para pertenecer o no a otras clases. Con esta precaución, ya podemos definir un axioma de comprensión que no da lugar a ninguna paradoja conocida:

Axioma de comprensión *Si $\phi(x)$ es cualquier fórmula normal del lenguaje de la teoría de conjuntos, existe una clase cuyos elementos son exactamente los conjuntos x que tienen la propiedad $\phi(x)$, es decir,*

$$\bigvee A \bigwedge x(x \in A \leftrightarrow \mathrm{cto}\, x \wedge \phi(x)).$$

Aquí hemos de entender que una *fórmula normal*[3] es una fórmula cuyos cuantificadores sólo recorren conjuntos, es decir, que en la definición de $\phi(x)$ no se dice nunca "para toda clase A" o "existe una clase A", sino a lo sumo "para todo conjunto A" o "existe un conjunto A".

Nuevamente, el axioma de extensionalidad hace que la clase A cuya existencia postula el axioma de comprensión sea única, pues si hay dos que cumplen el axioma, ambas tienen los mismos elementos (los conjuntos que cumplen $\phi(x)$, luego son la misma. La representaremos igualmente por

$$\{x \mid \phi(x)\},$$

pero es esencial tener presente que ya no se trata de *la clase de todas las clases que cumplen $\phi(x)$,* sino —aunque no esté indicado de forma explícita— de *la clase de todos los conjuntos que cumplen $\phi(x)$.*

[3]Posponemos hasta el final de esta sección la discusión de por qué hemos restringido el axioma de comprensión a fórmulas normales, pero anticipamos aquí que dicha restricción no es esencial y que podríamos eliminarla sin problemas.

Si definimos $A = \{x \mid \phi(x)\}$, la afirmación $x \in A$ no equivale a $\phi(x)$, sino a $\mathrm{cto}\, x \wedge \phi(x)$, de modo que si una clase x cumple $\phi(x)$ pero no es un conjunto, se cumplirá que $x \notin A$.

Veamos que así hemos neutralizado a la paradoja de Russell:

Teorema 1.5 *La clase $R = \{x \mid x \notin x\}$ es una clase propia. En particular, cumple que $R \notin R$.*

DEMOSTRACIÓN: Si suponemos que $R \in R$, entonces, por definición de R, debería ser $\mathrm{cto}\, x$ y $R \notin R$, con lo que tendríamos una contradicción. Por lo tanto, tiene que ser $R \notin R$. Si R fuera un conjunto, tendríamos $\mathrm{cto}\, R \wedge R \notin R$, luego por definición de R sería $R \in R$ y de nuevo tendríamos una contradicción. Concluimos que R no es un conjunto. ∎

De esta manera, al haber planteado que las clases necesitan un "permiso de pertenencia" para pertenecer a otra clase, al definir la clase de Russell R no llegamos a una contradicción, sino a la mera necesidad de que R carezca de tal permiso de pertenencia.

El álgebra de las clases La definición 1.3 sigue siendo válida bajo la versión modificada del axioma de comprensión, pues todas las fórmulas usadas en las definiciones carecen de cuantificadores, luego son normales. Así, la unión $A \cup B$ sigue siendo la clase que contiene a todos los elementos de A y a los de B, pues si un x pertenece a A o a B, por esto mismo ya es un conjunto, luego ya tiene garantizado su derecho de pertenencia a $A \cup B$. Lo mismo vale para la intersección $A \cap B$ y para la diferencia $A \setminus B$.

En cambio, ahora hay que tener presente que $\overline{A}$ no está formada por todas las clases que no pertenecen a A, sino únicamente por aquellas que además son conjuntos. Similarmente, la clase universal V no es la clase de todas las clases, sino la clase de todos los conjuntos. No hay ninguna clase que contenga a todas las clases, pues, por ejemplo, ninguna clase puede contener a la clase de Russell R.

Los conceptos introducidos en 1.3 verifican (junto con la inclusión de clases) una serie de propiedades que se demuestran todas de forma elemental. Por ejemplo, se cumple que

$$\bigwedge ABC(A \cap (B \cup C) = (A \cap B) \cup (A \cap C)).$$

Para probar este tipo de igualdades basta recurrir al axioma de extensionalidad: tomamos un conjunto $x \in A \cap (B \cup C)$ y probamos que pertenece también al otro miembro. En efecto, por definición de intersección $x \in A$ y $x \in B \cup C$, y por definición de unión, o bien $x \in B$ (en cuyo caso $x \in A \cap B$) o bien $x \in C$ (en cuyo caso $x \in A \cap C$), luego en cualquiera de los dos casos $x \in (A \cap B) \cup (A \cap C)$. Esto prueba la implicación

$$x \in A \cap (B \cup C) \to x \in (A \cap B) \cup (A \cap C),$$

y la implicación opuesta se demuestra de forma similar. Entonces el axioma de extensionalidad nos da la igualdad. Alternativamente, podemos considerar que hemos probado la inclusión

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C),$$

y que la implicación contraria prueba la inclusión contraria:

$$(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C),$$

y entonces concluimos mediante 1.2 b). En general una forma de probar una igualdad entre dos clases $X = Y$ es probar la doble inclusión $X \subset Y \wedge Y \subset X$ y aplicar 1.2.2.

No nos molestaremos en enunciar y demostrar una lista de afirmaciones de este tipo porque cualquiera que podamos necesitar en cualquier momento (como $A \subset A \cup B$, etc.) puede probarse en el momento sin dificultad alguna.

Observemos que $\varnothing$ y V son, respectivamente, la menor y la mayor de todas las clases, en el sentido de que

$$\bigwedge A(\varnothing \subset A \wedge A \subset V).$$

En efecto, como los elementos de cualquier clase A son conjuntos, todos ellos son también elementos de V, luego tenemos la inclusión $A \subset V$. Por otra parte, la clase vacía está contenida en cualquier otra clase, porque la implicación $x \in \varnothing \to x \in A$ se cumple trivialmente (no es posible encontrar un conjunto x que cumpla $x \in \varnothing \wedge x \notin A$).

Diremos que dos clases A y B son *disjuntas* si $A \cap B = \varnothing$, es decir, si no tienen elementos en común. ∎

Sí, ¿pero qué es un conjunto? Hemos visto cómo el axioma de extensionalidad y el de comprensión —debidamente "atenuado" mediante la distinción entre clases propias y conjuntos— permiten introducir los conceptos de inclusión, unión, intersección, etc., que aparecen en cualquier texto matemático, y demostrar sus propiedades manteniendo a su vez a raya a la paradoja de Russell. Sin embargo la distinción que hemos introducido entre clases propias y conjuntos no es nada satisfactoria desde un punto de vista conceptual.

Alguien que entienda que un conjunto es una clase que pertenece al menos a otra clase no puede decir por ello que entienda lo que es un conjunto, pese a que ésa es la definición de "conjunto". Cabe preguntarse en qué se diferencia una clase propia de un conjunto, o cómo podemos saber si una clase dada es o no un conjunto. Lo primero que podemos observar es que, de acuerdo con la definición, que una clase sea o no un conjunto no depende de ella misma (no depende de cuáles sean sus elementos), sino de todas las demás clases. Una clase será un conjunto si existe *otra* clase que la contiene como elemento.

Así, por ejemplo, para saber si la clase vacía es o no un conjunto, no sirve de nada pensar en qué elementos tiene y tener bien claro que no hay ninguna. Lo

que necesitamos saber es si hay alguna otra clase que tenga a $\varnothing$ como elemento o si no la hay. Pero en realidad no hay nada que saber. Los axiomas que hemos dado no permiten responder a esa pregunta. Podemos, si así lo deseamos, tomar como axioma que la clase vacía es un conjunto, y también que no lo es, sin que ninguna de las dos opciones dé lugar a ninguna contradicción. Obviamente, la opción que nos interesa es la primera, y por ello introducimos aquí nuestro tercer axioma:

Axioma del conjunto vacío $\mathrm{cto}\,\varnothing$.

Así pues, a partir de aquí podemos hablar del "conjunto vacío" en lugar de la "clase vacía". En particular, ahora podemos afirmar que $\varnothing \in V$, luego $V \neq \varnothing$.

La mayor parte de los axiomas que tenemos pendiente introducir tienen por objeto garantizar que la mayoría de las clases que podemos definir con el axioma de comprensión son conjuntos. Sin embargo, esto no resuelve el problema fundamental: hay clases (como la clase de Russell R) que dan lugar a contradicciones si suponemos que son conjuntos, y otras que no. ¿De qué depende esto? ¿Qué clases podemos postular que son conjuntos sin temor a contradicciones y cuáles vamos a poder demostrar que son clases propias como ha sucedido con la clase R?

Los axiomas que daremos de formación de conjuntos nos darán criterios prácticos para determinar si una clase dada es un conjunto o no, pero una respuesta intrínseca al problema de cuándo una clase es o no un conjunto —es decir, una respuesta que dependa de los elementos de la propia clase y no de la eventual existencia de otra clase que la contenga como elemento— tendrá que esperar hasta que hayamos avanzado bastante en la teoría (teorema 4.20).

Notemos que el axioma del conjunto vacío no nos aporta un gran progreso en el problema de determinar qué clases son conjuntos. Por ejemplo, seguimos sin saber si la clase universal V es o no un conjunto (no puede demostrarse ni refutarse que lo es con los pocos axiomas que hemos dado hasta ahora). Incluso en contextos más terrenales, consideremos la clase

$$\{\varnothing\} = \{x \mid x = \varnothing\}.$$

Si $\varnothing$ fuera una clase propia, tendríamos que $\{\varnothing\} = \varnothing$, pero con el axioma del conjunto vacío podemos afirmar que $\{\varnothing\}$ tiene a $\varnothing$ como único elemento, pero no estamos en condiciones de demostrar o refutar si $\{\varnothing\}$ es o no un conjunto. ∎

Grandes uniones e intersecciones Podemos completar el álgebra de las clases (las operaciones básicas definidas entre clases) introduciendo unos conceptos más generales de unión e intersección:

$$\bigcup A \equiv \{x \mid \bigvee y \in A\ x \in y\}, \quad \bigcap A \equiv \{x \mid \bigwedge y \in A\ x \in y\}.$$

Notemos que la condición $y \in A$ supone implícitamente que y es un conjunto (pues estamos diciendo que pertenece a otra clase), luego las cuantificaciones de

la forma $\bigvee y \in A$ o $\bigwedge y \in A$ son cuantificaciones sobre conjuntos y determinan fórmulas normales (supuesto que lo que vaya a continuación sea normal).

Esta consideración general justifica en particular que la existencia de "gran unión" y la "gran intersección" se sigue de dos aplicaciones legítimas del axioma de comprensión. Claramente, $\bigcup A$ resulta de reunir en una única clase todos los elementos de todos los elementos de A, mientras que $\bigcap A$ contiene a los elementos comunes a todos los elementos de A. Observemos que

$$\bigcup \varnothing = \varnothing, \quad \bigcup V = V, \quad \bigcap \varnothing = V, \quad \bigcap V = \varnothing.$$

En efecto, vamos a probar las dos últimas igualdades:

Si $x \in V$, entonces trivialmente $\bigwedge y \in \varnothing\, x \in y$, pues no es posible encontrar un $y \in \varnothing$ que no cumpla $x \in y$, y esto significa que $x \in \bigcap \varnothing$, luego tenemos la inclusión $V \subset \bigcap \varnothing$, y ya hemos visto que la inclusión contraria se cumple siempre.

Para la última igualdad requerimos el axioma del conjunto vacío. En efecto, si $x \in \bigcap V$, entonces x pertenece a todos los elementos de V, en particular $x \in \varnothing$, lo cual es imposible. Por lo tanto $\bigcap V$ no tiene elementos y es el conjunto vacío. ∎

Observaciones finales En este punto ya podemos entender que los conceptos matemáticos de "clase" y "conjunto" no reflejan con total fidelidad la noción de "colección de objetos", pues obviamente la colección de todas las clases es una colección de objetos que no es una clase. Y no hace falta ir tan alto. Podemos considerar perfectamente las dos clases $\varnothing$ y R. Aquí tenemos una colección de dos clases distintas (no son la misma, pues claramente $\varnothing \in R$), pero no son una clase, pues es imposible que una clase tenga por elementos precisamente a $\varnothing$ y a R. Para ello R tendría que ser un conjunto. Así pues, hay colecciones de tan sólo dos objetos (o incluso de uno solo, como la formada sólo por R) que no se identifican con clase alguna.

Sin embargo, nuestro propósito es demostrar —adoptando para ello los axiomas adecuados— que todas las colecciones que realmente son necesarias para desarrollar las matemáticas —y esto no incluye a la colección formada por $\varnothing$ y R, de la que podemos hablar, pero tampoco pasa nada si no la tenemos en cuenta— son en su mayor parte conjuntos y, en algunos pocos casos, clases propias, pero clases al fin y al cabo.

Finalmente abordamos la cuestión de por qué hemos restringido el axioma de comprensión a fórmulas normales. Según ya hemos advertido, la restricción no es esencial. La teoría axiomática de conjuntos que resulta de aceptar los axiomas que hemos introducido hasta ahora y los que introduciremos en lo sucesivo se conoce como *teoría de conjuntos de von Neumann-Bernays-Gödel,* (NBG), mientras que si eliminamos la restricción de normalidad en el axioma de comprensión tenemos la *teoría de conjuntos de Morse-Kelley* (MK).

La diferencia entre ambas es que en NBG la noción de clase propia es eliminable, es decir, toda la teoría puede ser reformulada para eliminar por completo el concepto de clase propia y trabajar exclusivamente con conjuntos. El resultado es la llamada teoría de conjuntos de Zermelo-Fraenkel (ZF) que es totalmente equivalente a NBG en el sentido de que un teorema que involucre exclusivamente conjuntos es demostrable en NBG si y sólo si es demostrable en ZF. Las clases como R, que en NBG se demuestra que son clases propias, simplemente no existen en ZF. Así, en ZF, en lugar de "la clase de los conjuntos que no se pertenecen a sí mismos no es un conjunto", se demuestra "no existe ningún conjunto cuyos elementos sean los conjuntos que no se pertenecen a sí mismos".

Por el contrario, en MK las clases propias pueden usarse para demostrar resultados sobre conjuntos (incluso afirmaciones que hablan exclusivamente de números naturales) que no son demostrables en NBG ni, por consiguiente, en ZF.

En realidad, al restringirnos a NBG, es decir, al aceptar la restricción del axioma de comprensión a propiedades normales, no es que estemos restringiéndonos a NBG, sino más bien estamos observando que todos los resultados que vamos a probar no requieren más que la forma restringida del axioma de comprensión. En ningún momento nos vamos a encontrar con resultado que "nos gustaría" poder demostrar pero no podemos por culpa de la restricción del axioma de comprensión. Para encontrar resultados así (que los hay) es necesario ahondar mucho en las sutilezas lógicas de la teoría de conjuntos, cosa que no vamos a hacer en este libro. ∎

1.2 Funciones

Ahora vamos a enriquecer sustancialmente el lenguaje de la teoría de conjuntos mostrando que a partir de las meras nociones de clase y pertenencia es posible definir funciones que hagan corresponder unos conjuntos con otros. La clave para ello es el concepto de par ordenado, que a su vez requiere definir previamente el concepto de par desordenado:

Definición 1.6 Dadas dos clases x e y, definimos el *par (desordenado)* formado por ellas como

$$\{x, y\} \equiv \{z \mid z = x \vee z = y\}.$$

Definimos también $\{x\} \equiv \{x, x\} = \{z \mid z = x\}$.

De este modo, $\{x, y\}$ es la clase de todos los conjuntos que son iguales a x o a y. Esto hay que tomarlo con precaución si x o y no son conjuntos. Por ejemplo, $\{\varnothing, R\} = \{\varnothing\}$ y $\{R\} = \varnothing$.

Con los axiomas que hemos presentado hasta ahora no es posible demostrar que exista ningún otro conjunto, aparte de $\varnothing$. Esto cambia drásticamente si añadimos el axioma siguiente:

Axioma del par $\bigwedge xy\ (\mathrm{cto}\, x \wedge \mathrm{cto}\, y \to \mathrm{cto}\{x, y\})$.

En otras palabras, el axioma del par afirma que el par definido por dos conjuntos es un conjunto. El axioma incluye el caso en que $x = y$, en cuyo caso tenemos:

$$\bigwedge x(\mathrm{cto}\, x \to \mathrm{cto}\{x\}).$$

Ahora podemos probar la existencia de muchos conjuntos, como $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, $\{\{\varnothing\}\}$, etc.

Más en general, cuando escribamos expresiones de la forma $\{a, b, c, d\}$, habrá que entender que nos referimos a la clase

$$\{a, b, c, d\} \equiv \{x \mid x = a \vee x = b \vee x = c \vee x = d\}.$$

Se dice entonces que hemos definido la clase $A = \{a, b, c, d\}$ por *extensión,* es decir, especificando sus elementos uno a uno, mientras que las clases definidas especificando una propiedad que deben cumplir sus elementos están definidas por *comprensión.* Obviamente, sólo es posible definir por extensión clases con un número finito de elementos. Los axiomas vistos hasta el momento no nos permiten asegurar que la clase $\{a, b, c, d\}$ sea un conjunto aunque lo sean sus elementos.

Observemos ahora que si x, y son conjuntos, se cumple que $\{x, y\} = \{y, x\}$, pues ambos conjuntos tienen los mismos elementos. Un hecho fundamental es que podemos definir un nuevo concepto de par en el que el orden de sus elementos sea relevante:

Definición 1.7 Definimos el *par ordenado* de *componentes* los conjuntos x e y como el conjunto $(x, y) \equiv \{\{x\}, \{x, y\}\}$.

Observemos que si x e y son conjuntos, entonces $\{x\}$ y $\{x, y\}$ son conjuntos por el axioma del par, y entonces (x, y) es un conjunto por una nueva aplicación de este axioma. La definición está pensada para que se cumpla el teorema fundamental:

Teorema 1.8 *Si x, y, u, v son conjuntos, entonces*

$$(x, y) = (u, v) \leftrightarrow x = u \wedge y = v.$$

Demostración: Una implicación es trivial. Para probar la contraria suponemos que $(x, y) = (u, v)$. Entonces, como $\{x\} \in (x, y)$, tenemos también que $\{x\} \in (u, v)$, luego $\{x\} = \{u\}$ o bien $\{x\} = \{u, v\}$. Si se da el segundo caso, como $u \in \{u, v\} = \{x\}$, concluimos que $u = x$, y en el primer caso llegamos también a la misma conclusión.

Ahora distinguimos otros dos casos: si $x = y$, entonces

$$(x, y) = \{\{x\}, \{x, x\}\} = \{\{x\}\},$$

y como $\{u, v\} \in (u, v) = (x, y)$, será $\{u, v\} = \{x\}$, luego $v \in \{u, v\} = \{x\}$, luego $v = x = y$.

Si, por el contrario, $x \neq y$, no puede ser $\{x, y\} = \{u\}$, pues entonces sería $x = u = y$, y como $\{x, y\} \in (x, y) = (u, v)$, tiene que ser $y \in \{x, y\} = \{u, v\}$, luego $y = u \vee y = v$, pero no puede ser $y = u = x$, luego tiene que ser $y = v$. ∎

Usaremos la notación

$$\{(x, y) \mid \phi(x, y)\} \equiv \{z \mid \bigvee xy(\mathrm{cto}\, x \wedge \mathrm{cto}\, y \wedge z = (x, y) \wedge \phi(x, y))\},$$

es decir, para referirnos a la clase de todos los pares ordenados (x, y) cuyas componentes cumplen la propiedad (normal) $\phi(x, y)$. Observemos que la propiedad

$$\bigvee xy(\mathrm{cto}\, x \wedge \mathrm{cto}\, y \wedge z = (x, y) \wedge \phi(x, y))$$

es normal si ϕ lo es, pues los dos cuantificadores que se añaden a lo que afirma ϕ están restringidos a conjuntos, por lo que si ϕ es normal el axioma de comprensión asegura la existencia de la clase $\{(x, y) \mid \phi(x, y)\}$.

El ejemplo más simple de clase definida de este modo es el producto cartesiano:

Definición 1.9 El *producto cartesiano* de dos clases A y B se define como

$$A \times B \equiv \{(x, y) \mid x \in A \wedge y \in B\}.$$

En otros términos: $A \times B$ es la clase formada por todos los pares ordenados cuya primera componente está en A y su segunda componente está en B. Por ejemplo, $V \times V$ es la clase de todos los pares ordenados.

Definición 1.10 Definimos el *dominio* y el *rango* de una clase F como las clases[4]

$$\mathcal{D}F \equiv \{x \mid \bigvee y\, (\mathrm{cto}\, y \wedge (x, y) \in F\}, \quad \mathcal{R}F \equiv \{y \mid \bigvee x\, (\mathrm{cto}\, x \wedge (x, y) \in F\}$$

Diremos que F es *unívoca* si cumple

$$\mathrm{Un}\, F \equiv \bigwedge xyz(\mathrm{cto}\, x \wedge \mathrm{cto}\, y \wedge \mathrm{cto}\, z \wedge (x, y) \in F \wedge (x, z) \in F \to y = z).$$

Notemos que en la definición de clase unívoca no hemos exigido que todos los elementos de F sean pares ordenados.

Diremos que una clase F es una *función* si cumple

$$\mathrm{Fn}\, F \equiv \bigwedge z \in F \bigvee xy(\mathrm{cto}\, x \wedge \mathrm{cto}\, y \wedge z = (x, y)) \wedge \mathrm{Un}\, F,$$

o, equivalentemente, si $F \subset V \times V \wedge \mathrm{Un}\, F$. Más concretamente, diremos que F es una *aplicación* (o una *función*) de una clase A en una clase B si cumple

$$F : A \longrightarrow B \equiv \mathrm{Fn}\, F \wedge \mathcal{D}F = A \wedge \mathcal{R}F \subset B.$$

[4]Notemos que los cuantificadores $\bigvee y$ y $\bigvee x$ que aparecen en las definiciones del dominio y el rango están restringidas a conjuntos, por lo que la propiedad es normal y el axioma de comprensión es aplicable.

En otras palabras, una clase F es unívoca si para cada $x \in \mathcal{D}F$ existe un único conjunto y (necesariamente en $\mathcal{R}F$) tal que $(x, y) \in F$. Dicho y recibe el nombre de *imagen* de x por F y se representa por

$$F(x) \equiv y \mid (\text{cto}\, y \wedge (x, y) \in F).$$

También se dice que x es una *antiimagen* de y por F, pero, aunque una clase F sea unívoca, un elemento de $\mathcal{R}F$ puede tener varias antiimágenes por F.

Si $F \subset V \times V$ (en particular si F es una función), entonces $F \subset \mathcal{D}F \times \mathcal{R}F$, pero esto no es cierto si F es una clase cualquiera, pues entonces F puede contener elementos que no sean pares ordenados.

Claramente, $F : A \longrightarrow B$ significa que F asigna a cada $x \in A$ una imagen $F(x) \in B$, y entonces $F \subset A \times B$.

Observemos que si $F : A \longrightarrow B$ y $B \subset C$, también se cumple $F : A \longrightarrow C$.

Definimos:

$$\begin{aligned} F : A \longrightarrow B \text{ inyectiva} &\equiv F : A \longrightarrow B \wedge \bigwedge xy \in A(F(x) = F(y) \to x = y),\\ F : A \longrightarrow B \text{ suprayectiva} &\equiv F : A \longrightarrow B \wedge \bigwedge y \in B \bigvee x \in A\ f(x) = y,\\ F : A \longrightarrow B \text{ biyectiva} &\equiv F : A \longrightarrow B \text{ inyectiva y suprayectiva.} \end{aligned}$$

Así, F es inyectiva si asigna a cada elemento de A una imagen distinta en B (no hay dos elementos con la misma imagen), F es suprayectiva si todo elemento de B tiene una antiimagen (o, equivalentemente, si $\mathcal{R}F = B$) y F es biyectiva si a cada elemento de A le asigna un único elemento de B y viceversa.

Usaremos a menudo el criterio siguiente de igualdad de funciones:

Teorema 1.11 *Dos funciones F y G son iguales si y sólo si tienen el mismo dominio A y se cumple que $\bigwedge x \in A\, F(x) = G(x)$.*

Demostración: Una implicación es trivial. Si F y G coinciden sobre su dominio común, dado $z \in F$, por ser una función existen conjuntos x, y tales que $z = (x, y)$. Entonces $x \in A$ por definición de dominio, luego $y = F(x) = G(x)$, luego $z = (x, y) \in G$, y por lo tanto $F \subset G$. Igualmente se prueba la inclusión opuesta. ∎

Veamos más conceptos relacionados con las funciones:

Definición 1.12 La *restricción* de una clase F a una clase X como

$$F|_X \equiv \{(x, y) \mid x \in X \wedge (x, y) \in F\},$$

es decir, se trata de la clase de todos los pares ordenados de F cuya primera componente está en X.

Es fácil ver que si $F : A \longrightarrow B$ y $X \subset A$, entonces $F|_X : X \longrightarrow B$.

Definimos la *clase inversa* de una clase F como la clase

$$F^{-1} \equiv \{(y, x) \mid (x, y) \in F\}.$$

Observemos que si $F \subset V \times V$, entonces $(F^{-1})^{-1} = F$. También es claro que si $F : A \longrightarrow B$ biyectiva entonces $F^{-1} : B \longrightarrow A$ biyectiva.

Definimos la *imagen* de una clase X por una clase F como

$$F[X] \equiv \{y \mid \bigvee x \in X\, (x, y) \in F\}.$$

Equivalentemente, $F[X] \equiv \mathcal{R}(F|_X)$. Notemos que

$$F^{-1}[Y] = \{x \mid \bigvee y \in Y\, (x, y) \in F\}.$$

En particular, si $F : A \longrightarrow B$, $X \subset A$, $Y \subset B$, tenemos que

$$F[X] = \{F(x) \mid x \in X\} \equiv \{y \mid \bigvee x \in X\, F(x) = y\},$$

$$F^{-1}[Y] = \{x \mid x \in A \wedge F(x) \in Y\},$$

de modo que $F[X]$ es la clase de todas las imágenes por F de elementos de X y $F^{-1}[Y]$ es la clase de todas las antiimágenes por F de los elementos de Y.

Es fácil probar que si $F : A \longrightarrow B$, $Y_1, Y_2 \subset B$ y $X_1, X_2 \subset A$, entonces

$$F^{-1}[Y_1 \cup Y_2] = F^{-1}[Y_1] \cup F^{-1}[Y_2], \qquad F^{-1}[Y_1 \cap Y_2] = F^{-1}[Y_1] \cap F^{-1}[Y_2],$$

$$F[X_1 \cup X_2] = F[X_1] \cup F[X_2], \quad \text{pero} \quad F[X_1 \cap X_2] \subset F[X_1] \cap F[X_1]$$

y en general no se da la igualdad (pero se da si F es inyectiva).

Definimos la *composición* de dos clases F y G como la clase

$$F \circ G \equiv \{(x, z) \mid \bigvee y(\mathrm{cto}\, y \wedge (x, y) \in F \wedge (y, z) \in G)\}.$$

En particular, si $F : A \longrightarrow B$ y $G : B \longrightarrow C$, se cumple que $F \circ G : A \longrightarrow C$ y $\bigwedge x \in A\ (F \circ G)(x) = G(F(x))$, de modo que $F \circ G$ es la aplicación que resulta de "encadenar" F y G, es decir, de aplicar primero F y luego aplicar G sobre el resultado obtenido.

También es fácil comprobar que la composición de aplicaciones inyectivas, suprayectivas o biyectivas es inyectiva, suprayectiva o biyectiva, respectivamente. En el último caso se cumple además que $(F \circ G)^{-1} = G^{-1} \circ F^{-1}$.

Observemos que, dadas tres clases cualesquiera F, G, H, se cumple que

$$F \circ (G \circ H) = (F \circ G) \circ H =$$

$$\{(x, w) \mid \bigvee yz(\mathrm{cto}\, y \wedge \mathrm{cto}\, z \wedge (x, y) \in F \wedge (y, z) \in G \wedge (z, w) \in H)\}.$$

Finalmente, definimos la *identidad* en una clase A como la clase

$$I_A \equiv \{(x, y) \mid x \in A \wedge x = y\}.$$

Equivalentemente, se trata de la aplicación $I_A : A \longrightarrow A$ (claramente biyectiva) determinada por $\bigwedge x \in A\ I_A(x) = x$.

Si llamamos $I : V \longrightarrow V$ a la aplicación dada por $I(x) = x$, entonces $I_A = I|_A$.

Si $A \subset B$, entonces se cumple también que $I_A : A \longrightarrow B$ y en este contexto se la llama *inclusión* de A en B.

Es fácil ver que si $F : A \longrightarrow B$, entonces $I_A \circ F = F \circ I_B = F$, y si F es biyectiva entonces $F \circ F^{-1} = I_A$, $F^{-1} \circ F = I_B$.

Una forma de probar que una aplicación es biyectiva es encontrar su inversa, de acuerdo con el teorema siguiente:

Teorema 1.13 *Sean $F : A \longrightarrow B$ y $G : B \longrightarrow A$.*

1. *Si $F \circ G = I_A$ entonces F es inyectiva y G suprayectiva.*
2. *Si además $G \circ F = I_B$ entonces F y G son biyectivas y $G = F^{-1}$.*

Demostración: 1) Para probar que F es inyectiva tomamos $x, y \in A$ y suponemos que $F(x) = F(y)$, con lo que $G(F(x)) = G(F(y))$, pero esto equivale a $(F \circ G)(x) = (F \circ G)(y)$, que por hipótesis es $I_A(x) = I_A(y)$, es decir, $x = y$.

Para probar que la aplicación G es suprayectiva tomamos $x \in A$ y observamos que $y = F(x) \in B$ cumple $G(y) = G(F(x)) = (F \circ G)(x) = I_A(x) = x$.

2) Aplicando 1) con los papeles de F y G intercambiados obtenemos que F y G son biyectivas. Además, $F^{-1} \circ F \circ G = F^{-1} \circ I_A$, luego $I_B \circ G = F^{-1}$, luego $G = F^{-1}$. ∎

Terminamos esta sección discutiendo algunas notaciones habituales relacionadas con las funciones. Ante todo, puesto que el teorema 1.11 nos garantiza que una función queda completamente determinada por su dominio y por la imagen que asigna a cada elemento de éste, habitualmente definiremos las funciones especificando esta información.

Por ejemplo, si decimos "sea F la función definida en la clase A tal que $\bigwedge x \in A\ F(x) = \{x\}$", nos estamos refiriendo a

$$F \equiv \{(x, y) \mid x \in A \wedge y = \{x\}\}.$$

Para que la definición de F sea correcta es necesario comprobar que la propiedad $y = \{x\}$ sea normal, para que el axioma de comprensión sea aplicable, y además que, para cada $x \in A$, su imagen pretendida (en este caso $\{x\}$) sea un conjunto, pues en caso contrario, es decir, si y no es un conjunto, el par (x, y) sería simplemente

$$(x, y) = \{\{x\}, \{x, y\}\} = \{\{x\}, \{x\}\} = \{\{x\}, \{x, x\}\} = (x, x),$$

con lo que tendríamos ciertamente la aplicación F, pero cumpliría $F(x) = x$ para todo $x \in A$ cuya imagen pretendida no fuera un conjunto.[5] Si se cumplen estos dos requisitos, es inmediato comprobar que $F : A \longrightarrow V$ y que, para todo $x \in A$, $F(x)$ toma el valor pretendido.

Hay otra notación sustancialmente distinta que conviene usar a veces para representar ciertas aplicaciones. Para referirnos a una aplicación $X : I \longrightarrow V$ usaremos a veces la notación $\{X_i\}_{i\in I}$, y diremos entonces que $\{X_i\}_{i\in I}$ es una *familia de conjuntos subindicados* por la clase I. En este contexto escribimos $X_i \equiv X(i)$ para referirnos a la imagen de i, y decimos que es el *conjunto de índice* i en la familia considerada.

Notemos que, desde un punto de vista lógico, la expresión $X : I \longrightarrow V$ es la afirmación según la cual X es una aplicación de dominio X, mientras que $\{X_i\}_{i\in I}$ no es una afirmación, sino la forma de representar a una cierta aplicación de dominio I. No hay que confundir esta notación con $\{X_i \mid i \in I\}$, que es una forma de denotar el rango de X, es decir, $\mathcal{R}X$ o $X[I]$.

También podemos usar esta notación para definir una aplicación en los términos explicados anteriormente, es decir, especificando su dominio y la imagen de cada elemento del dominio. Por ejemplo, si tenemos dos familias $\{X_i\}_{i\in I}$ e $\{Y_i\}_{i\in I}$, a partir de ellas podemos definir la familia $\{X_i \cap Y_i\}_{i\in I}$, que ha de entenderse como la aplicación $Z : I \longrightarrow V$ dada por $Z(i) = X_i \cap Y_i$ o, más concretamente

$$Z \equiv \{(i, y) \mid i \in I \wedge y = X_i \cap Y_i\}.$$

Ahora bien, de momento no estamos en condiciones de justificar que esta definición es correcta, pues, aunque la propiedad $y = X_i \cap Y_i$ es ciertamente normal, hay asegurar además que $X_i \cap Y_i$ es un conjunto para todo $i \in I$. Esto lo justificaremos en la sección siguiente, pero para ello será necesario un nuevo axioma.

Esta notación es útil para hablar de grandes uniones e intersecciones, para lo cual introducimos además los convenios de notación

$$\bigcup_{i\in I} X_i \equiv \bigcup\{X_i \mid i \in I\}, \qquad \bigcap_{i\in I} X_i \equiv \bigcap\{X_i \mid i \in I\}.$$

De este modo

$$\bigwedge x(x \in \bigcup_{i\in I} X_i \leftrightarrow \bigvee i \in I\ x \in X_i), \quad \bigwedge x(x \in \bigcap_{i\in I} X_i \leftrightarrow \bigwedge i \in I\ x \in X_i).$$

No obstante, para operar con estas uniones e intersecciones es preferible contar antes con algunos de los resultados sobre formación de conjuntos que veremos en la sección siguiente.

[5] En general, si $t(x)$ es un término del lenguaje de la teoría de conjuntos tal que la fórmula $y = t(x)$ es normal y se demuestra que $\bigwedge x \in A\ \mathrm{cto}\, t(x)$, entonces

$$F \equiv \{(x, y) \mid x \in A \wedge y = t(x)\},$$

define una función a la que más habitualmente nos referiremos como "la función F definida sobre la clase A dada por $\bigwedge x \in A\ F(x) = t(x)$". En el ejemplo que hemos puesto, $t(x) \equiv \{x\}$.

1.3 Formación de conjuntos

En esta sección demostraremos (a partir de los axiomas necesarios) que prácticamente todas las construcciones realizadas a partir de conjuntos dan lugar a nuevos conjuntos. Ya hemos visto dos axiomas de formación de conjuntos (es decir, axiomas que afirman que determinadas clases son, de hecho, conjuntos): el axioma del conjunto vacío y el axioma del par. Aquí presentaremos otros tres. Éste es el más potente:

Axioma de reemplazo *Si $F : A \longrightarrow B$ suprayectiva y A es un conjunto, entonces B también es un conjunto.*[6]

Como primera consecuencia obtenemos:

Teorema 1.14 *Toda subclase de un conjunto es un conjunto.*

Demostración: Sea A un conjunto y $B \subset A$. Si $B = \varnothing$, entonces B es un conjunto por el axioma del conjunto vacío. En caso contrario existe un $b \in B$. Definimos $F : A \longrightarrow B$ mediante

$$F(x) = \begin{cases} x & \text{si } x \in B, \\ b & \text{si } x \notin B. \end{cases}$$

Recordemos que esto es una forma práctica de definir la clase F dada por

$$F \equiv \{(x, y) \mid x \in A \wedge ((x \in B \wedge y = x) \vee (x \notin B \wedge y = b))\}.$$

Claramente $F : A \longrightarrow B$ suprayectiva, luego B es un conjunto por el axioma de reemplazo. ∎

Como consecuencia:

Teorema 1.15 *La clase universal V es una clase propia.*

Demostración: Si V fuera un conjunto, por el teorema anterior todas las clases serían conjuntos, pues todas están contenidas en V, pero sabemos que existen clases propias, como la clase de Russell R, luego V no puede ser un conjunto. ∎

Ahora es inmediato que la intersección de una clase A y un conjunto B (en particular la intersección de dos conjuntos) es un conjunto, pues $A \cap B \subset B$. Para probar que la unión de conjuntos es un conjunto necesitamos un nuevo axioma:

[6] Desde un punto de vista lógico conviene que los axiomas (al menos los más básicos de la teoría) involucren los conceptos más simples que sea posible, y por ello es útil observar que el axioma de reemplazo es equivalente a la versión siguiente, en la que sólo aparecen los conceptos de conjunto, par ordenado y clase unívoca:

$$\bigwedge FA(\mathrm{cto}\, A \wedge \mathrm{Un}\, F \to \bigvee B(\mathrm{cto}\, B \wedge \bigwedge v(v \in B \leftrightarrow \bigvee u \in A\, (u, v) \in F))).$$

Notemos que en esta sentencia necesariamente $B = F[A]$, luego lo que afirma es que si F es unívoca y A es un conjunto, entonces $F[A]$ es un conjunto. Claramente esto implica la forma que hemos adoptado para el axioma de reemplazo y, recíprocamente, a partir de ella podemos demostrar ésta aplicándola a $F|_{A \cap \mathcal{D}F} : A \cap \mathcal{D}F \longrightarrow F[A]$ suprayectiva, teniendo en cuenta que $A \cap \mathcal{D}F$ es un conjunto por el teorema 1.14.

Axioma de la unión $\bigwedge A(\mathrm{cto}\, A \to \mathrm{cto} \bigcup A)$.

En particular:

Teorema 1.16 *Si A y B son conjuntos, también lo es $A \cup B$.*

DEMOSTRACIÓN: Basta tener en cuenta que $A \cup B = \bigcup\{A, B\}$, y que $\{A, B\}$ es un conjunto por el axioma del par. ∎

En particular ahora podemos probar que cualquier clase definida por extensión es un conjunto, pues, por ejemplo,

$$\{a, b, c, d\} = \{a\} \cup \{b\} \cup \{c\} \cup \{d\},$$

y las cuatro clases $\{a\}$, $\{b\}$, $\{c\}$, $\{d\}$ son conjuntos por el axioma del par (o por ser el conjunto vacío si alguna de las clases a, b, c, d no es un conjunto).

Combinando el axioma de reemplazo con el de la unión obtenemos que si $\{X_i\}_{i\in I}$ es una familia de conjuntos e I es un conjunto, entonces la unión $\bigcup\limits_{i\in I} X_i$ es un conjunto, pues dicha unión no es sino $\bigcup \mathcal{R}X$ y $\mathcal{R}X$ es un conjunto por reemplazo y la unión es un conjunto por el axioma de la unión.

Notemos que la intersección $\bigcap\limits_{i\in I} X_i$ es también un conjunto siempre que la clase $I \neq \varnothing$, pues si existe un $i \in I$ entonces $\bigcap\limits_{i\in I} X_i \subset X_i$ y podemos aplicar el teorema 1.14. En cambio, si $I = \varnothing$ tenemos que $\bigcap\limits_{i\in I} X_i = V$, luego no es un conjunto.

Combinando también el axioma de reemplazo con el de la unión obtenemos que el producto cartesiano de conjuntos es de nuevo un conjunto:

Teorema 1.17 *Si A y B son conjuntos, también lo es $A \times B$.*

DEMOSTRACIÓN: Para cada $a \in A$, la clase $\{a\} \times B$ es un conjunto, pues la aplicación $F : B \longrightarrow \{a\} \times B$ dada por $F(b) = (a, b)$ es biyectiva. Esto nos permite considerar la familia de conjuntos $\{\{a\} \times B\}_{a\in A}$, es decir, la aplicación $F : A \longrightarrow V$ dada por $F(a) = \{a\} \times B$. Ahora basta observar que

$$A \times B = \bigcup_{a\in A} \{a\} \times B$$

y aplicar la observación precedente: como A es un conjunto, también lo es $A \times B$. ∎

Es costumbre escribir

$$\{x \in A \mid \phi(x)\} \equiv \{x \mid x \in A \wedge \phi(x)\}$$

para enfatizar que estamos definiendo una subclase de la clase A. Por 1.14 sabemos que si A es un conjunto, toda clase definida así es de hecho un conjunto. Similarmente, usaremos la notación

$$\{(x, y) \in A \times B \mid \phi(x, y)\} \equiv \{(x, y) \mid (x, y) \in A \times B \wedge \phi(x, y)\},$$

que, por el teorema anterior, también da lugar a conjuntos siempre que A y B son conjuntos.

Nota Ahora ya es fácil trabajar con uniones e intersecciones de familias de conjuntos. Por ejemplo en la prueba de 1.17 hemos usado un caso particular de la primera de las propiedades siguientes, cuya prueba no ofrece dificultad:

$$(\bigcup_{i\in I} X_i)\times Y = \bigcup_{i\in I}(X_i\times Y), \quad (\bigcap_{i\in I} X_i)\times Y = \bigcap_{i\in I}(X_i\times Y).$$

(El caso de la intersección requiere suponer que $I\neq\varnothing$).

Obviamente lo mismo vale con uniones e intersecciones en el segundo factor. Notemos que para asegurar que los segundos miembros están bien definidos necesitamos saber que cada $X_i\times Y$ es un conjunto.

Otras propiedades muy útiles son las siguientes: si $\{X_i\}_{i\in I}$ es una familia de subconjuntos de un conjunto X, entonces

$$X\setminus\bigcup_{i\in I} X_i = \bigcap_{i\in I}(X\setminus X_i), \qquad X\setminus\bigcap_{i\in I} X_i = \bigcup_{i\in I}(X\setminus X_i).$$

En principio se requiere que $I\neq\varnothing$, pero cuando se trabaja con familias de subconjuntos de un conjunto fijo X, es conveniente considerar que, por definición, $\bigcap_{i\in\varnothing} X_i = X$, con lo que las igualdades anteriores valen incluso si $I=\varnothing$. ∎

Una consecuencia sencilla de los teoremas precedentes es la siguiente:

Teorema 1.18 *Si $R\subset V\times V$, entonces*

$$\operatorname{cto} R \leftrightarrow \operatorname{cto}\mathcal{D}R \wedge \operatorname{cto}\mathcal{R}R.$$

Demostración: La aplicación $R\longrightarrow \mathcal{D}R$ dada por[7] $(x,y)\mapsto x$ es suprayectiva, luego, por reemplazo, si R es un conjunto también lo es su dominio, y análogamente se razona con el rango. Para la implicación opuesta basta tener en cuenta que $R\subset \mathcal{D}R\times\mathcal{R}R$. ∎

Sin embargo, si F es una función la equivalencia anterior se puede simplificar a $\operatorname{cto} F \leftrightarrow \operatorname{cto}\mathcal{D}F$, puesto que si el dominio de F es un conjunto, puesto que $F:\mathcal{D}F\to\mathcal{R}F$ suprayectiva, por reemplazo tenemos que el rango también es un conjunto. Alternativamente, es fácil definir una biyección entre F y $\mathcal{D}F$. Así pues:

Teorema 1.19 *Una función es un conjunto si y sólo si lo es su dominio.*

Presentamos finalmente el último de los axiomas de formación de conjuntos, para lo cual definimos previamente la clase de *partes* de una clase dada:

$$\mathcal{P}Y \equiv \{x \mid x\subset Y\}$$

[7] Más concretamente, nos referimos a

$$F\equiv\{(z,x)\mid z\in R\wedge \bigvee y\ (\operatorname{cto} y\wedge z=(x,y))\}.$$

En lo sucesivo, en casos similares a éste no nos detendremos a explicitar cómo las funciones que definamos se reducen en última instancia a aplicaciones del axioma de comprensión.

Notemos que $x \subset Y$ es una propiedad normal pues equivale a que todo conjunto que pertenezca a x pertenece también a Y. Hay que tener presente que $\mathcal{P}Y$ es la clase de todos los subconjuntos (no de todas las subclases) de Y. Si Y es un conjunto no hay diferencia y $\mathcal{P}Y$ contiene a todo $x \subset Y$, pues esto ya implica que x es un conjunto. En cambio, si Y es una clase propia, tenemos, por ejemplo, que $Y \subset Y$, pero $Y \notin \mathcal{P}Y$. Por ejemplo, es fácil ver que $\mathcal{P}V = V$.

Axioma de partes (AP) $\bigwedge X(\mathrm{cto}\, X \to \mathrm{cto}\, \mathcal{P}X)$.

En otras palabras, el axioma de partes afirma que la clase de partes de un conjunto es un conjunto. A partir de aquí es fácil demostrar que muchas otras clases son conjuntos. Por ejemplo, definimos

$$A^B \equiv \{f \mid f : B \longrightarrow A\}.$$

Si B es una clase propia, tenemos que $A^B = \varnothing$, pues ninguna $f : B \longrightarrow A$ es un conjunto que pueda pertenecer a A^B. En cambio, si B es un conjunto (aunque A no lo sea) tenemos que A^B contiene a todas las aplicaciones $f : B \longrightarrow A$, pues todas ellas son conjuntos.

Teorema 1.20 $\bigwedge AB(\mathrm{cto}\, A \wedge \mathrm{cto}\, B \to \mathrm{cto}\, A^B)$

Demostración: Basta observar que si $f \in A^B$ entonces $f \subset B \times A$, luego $A^B \subset \mathcal{P}(B \times A)$, y basta aplicar los resultados que ya conocemos de formación de conjuntos. ∎

Más en general, dada una familia de conjuntos $\{X_i\}_{i\in I}$, definimos su *producto cartesiano* como la clase

$$\prod_{i\in I} X_i \equiv \{x \mid x : I \longrightarrow V \wedge \bigwedge i \in I\ x_i \in X_i\}.$$

De este modo, cada elemento del producto cartesiano es una familia de conjuntos $\{x_i\}_{i\in I}$ con la propiedad de que cada *componente* x_i pertenece al conjunto correspondiente X_i.

Observemos que

$$\prod_{i\in I} X_i \subset \Big(\bigcup_{i\in I} X_i\Big)^I,$$

luego, por los resultados precedentes, si I es un conjunto también lo es el producto cartesiano.

Los resultados de esta sección bastan para demostrar que cualquier construcción conjuntista usual proporciona conjuntos cuando parte de conjuntos.

1.4 La teoría de conjuntos NBG*

Llegados a este punto hemos presentado ya los que podemos considerar como axiomas básicos de la teoría de conjuntos, aunque en los capítulos siguientes introduciremos otros tres más. Por ello conviene reunirlos aquí para dejar constancia de la teoría concreta en la que estamos trabajando.

Llamaremos *teoría de conjuntos restringida de Von Neumann-Bernays-Gödel* (NBG*) a la teoría cuyo único concepto no definido es la relación $\in$ de pertenencia (entre clases) y cuyos axiomas son los siguientes:

Extensionalidad	$\bigwedge AB(\bigwedge x(x \in A \leftrightarrow x \in B) \to A = B)$	
Comprensión	$\bigvee A\bigwedge x(x \in A \leftrightarrow \mathrm{cto}\, x \wedge \phi(x))$	$(*)$
Vacío	$\mathrm{cto}\, \varnothing$	
Par	$\bigwedge xy\ (\mathrm{cto}\, x \wedge \mathrm{cto}\, y \to \mathrm{cto}\{x, y\})$	
Unión	$\bigwedge A(\mathrm{cto}\, A \to \mathrm{cto} \bigcup A)$	
Reemplazo	$\bigwedge FAB(F : A \longrightarrow B \text{ suprayectiva} \wedge \mathrm{cto}\, A \to \mathrm{cto}\, B)$	

$(*)$ para toda fórmula normal $\phi(x)$, tal vez con más variables, además de x.

Notemos que no hemos incluido el axioma de partes (AP). Ello se debe a que una parte importante de la teoría de conjuntos puede desarrollarse sin él, y a la larga resulta útil saber qué axiomas (más allá de los axiomas básicos de NBG*) son necesarios para probar cada resultado. En lo sucesivo trabajaremos en NBG* salvo que indiquemos lo contrario.

Como explicábamos al final de la sección 1.1, la teoría NBG* es equivalente a la teoría ZF* (la teoría restringida de Zermelo-Fraenkel) que resulta de eliminar el axioma de comprensión y reformular los restantes para evitar toda referencia a clases que a priori no tengan por qué ser conjuntos.[8] Son equivalentes en el sentido de que un teorema que hable únicamente de conjuntos puede demostrarse en NBG* si y sólo si puede demostrarse en ZF*. Las clases propias en NBG* son, pues, un mero recurso técnico no esencial para trabajar más cómodamente con los conjuntos.

1.5 Equipotencia

A la vista de una figura como ésta:

no es necesario contar cuántos puntos hay en cada fila para asegurar que hay el mismo número de puntos en la primera y en la segunda fila. La razón es que la figura muestra que por debajo de cada punto de la primera fila hay exactamente un punto en la segunda, y viceversa.

[8] Por ejemplo, el axioma del par puede reformularse diciendo que para todo par de conjuntos x, y existe otro conjunto z cuyos únicos elementos son x e y. El único axioma cuya reformulación no es trivial es el de reemplazo.

En general, dos conjuntos X e Y tienen el mismo número de elementos si y sólo si existe una aplicación biyectiva $f : X \longrightarrow Y$. En principio esto vale para conjuntos finitos, pero una de las ideas más originales de Cantor fue darse cuenta de que es perfectamente posible comparar conjuntos infinitos con el mismo criterio:

Definición 1.21 Diremos que dos conjuntos X e Y son *equipotentes,* y lo representaremos por $\overline{\overline{X}} = \overline{\overline{Y}}$, si existe una aplicación $f : X \longrightarrow Y$ biyectiva. Diremos que X es *minuspotente* a Y, y lo representaremos por $\overline{\overline{X}} \leq \overline{\overline{Y}}$, si existe $f : X \longrightarrow Y$ inyectiva. Diremos que X es *estrictamente minuspotente* a Y, en signos $\overline{\overline{X}} < \overline{\overline{Y}}$, si $\overline{\overline{X}} \leq \overline{\overline{Y}}$ y no $\overline{\overline{X}} = \overline{\overline{Y}}$.

Debemos recordar en todo momento que el signo $=$ que aparece en la expresión $\overline{\overline{X}} = \overline{\overline{Y}}$ no es realmente un signo igual, sino que esta expresión no es sino una forma cómoda de indicar que se cumple "$\bigvee f\ f : X \longrightarrow Y$ biyectiva", y aquí no hay ningún igual.

Esta notación se remonta a Cantor. Si X es un conjunto ordenado, Cantor representaba por $\overline{X}$ lo que llamaba su "ordinal", es decir, el concepto resultante de abstraer la naturaleza de los elementos de X, pero conservando su ordenación, y por $\overline{\overline{X}}$ su "cardinal", su número de elementos, es decir, el resultado de abstraer tanto la naturaleza de sus elementos como su ordenación, de modo que la doble barra indicaba una "doble abstracción". Estas consideraciones no cumplen con las exigencias de rigor que nos hemos impuesto. Cantor podía considerar que de este modo había definido el "cardinal" de un conjunto X, pero nosotros debemos aceptar que no hemos definido nada más que una propiedad que pueden cumplir o no dos conjuntos dados.

No deja de ser cierto que con $\overline{\overline{X}} = \overline{\overline{Y}}$ pretendemos expresar que "el cardinal de X" es igual a "el cardinal de Y", pero —insistimos— es fundamental tener presente que, de momento, no hemos definido ningún conjunto al que llamar $\overline{\overline{X}}$.

El teorema siguiente justifica que las definiciones que hemos dado contienen realmente una noción razonable de "número de elementos" de un conjunto.

Teorema 1.22 *Sean X, Y, Z, W conjuntos cualesquiera. Se cumple:*

1. $\overline{\overline{X}} = \overline{\overline{X}}$,
2. $\overline{\overline{X}} = \overline{\overline{Y}}$ *si y sólo si* $\overline{\overline{Y}} = \overline{\overline{X}}$,
3. *Si* $\overline{\overline{X}} = \overline{\overline{Y}}$ *y* $\overline{\overline{Y}} = \overline{\overline{Z}}$, *entonces* $\overline{\overline{X}} = \overline{\overline{Z}}$,
4. $\overline{\overline{X}} \leq \overline{\overline{X}}$,
5. *Si* $\overline{\overline{X}} \leq \overline{\overline{Y}}$ *y* $\overline{\overline{Y}} \leq \overline{\overline{X}}$, *entonces* $\overline{\overline{X}} = \overline{\overline{Y}}$,
6. *Si* $\overline{\overline{X}} \leq \overline{\overline{Y}}$ *y* $\overline{\overline{Y}} \leq \overline{\overline{Z}}$, *entonces* $\overline{\overline{X}} \leq \overline{\overline{Z}}$,
7. *Si* $\overline{\overline{X}} = \overline{\overline{Y}}$ *y* $\overline{\overline{Z}} = \overline{\overline{W}}$, *entonces* $\overline{\overline{X}} \leq \overline{\overline{Z}}$ *si y sólo si* $\overline{\overline{Y}} \leq \overline{\overline{W}}$.

Todas estas propiedades excepto 5) son consecuencias inmediatas de los hechos básicos sobre aplicaciones entre conjuntos. Debemos insistir en que no deben confundirse, pese a la notación, con teoremas lógicos. Por ejemplo, 2) no se cumple por la simetría de la igualdad, ya que, como hemos indicado, la relación involucrada no es la igualdad, sino la equipotencia. La razón por la que se cumple b) es que si existe una biyección $f : X \longrightarrow Y$ entonces $f^{-1} : Y \longrightarrow X$ es también una biyección.

Como decimos, la propiedad 5) no es evidente en absoluto. Explícitamente, afirma que si existen aplicaciones inyectivas $f : X \longrightarrow Y$ y $g : Y \longrightarrow X$ entonces existe una aplicación biyectiva $h : X \longrightarrow Y$. La forma de construir h a partir de f y g no es inmediata. Para probarlo nos apoyaremos en un resultado previo (notemos que, pese a las apariencias, no usa AP).

Teorema 1.23 *Sea X un conjunto y $F : \mathcal{P}X \longrightarrow \mathcal{P}X$ una aplicación tal que si $u \subset v \subset X$ entonces $F(u) \subset F(v)$. Entonces existe un $z \in \mathcal{P}X$ tal que $F(z) = z$.*

Demostración: Sea $A = \{u \in \mathcal{P}X \mid F(u) \subset u\}$. Se cumple que A es una clase no vacía (pues contiene a X). Llamemos $z = \bigcap_{u \in A} u$. Claramente $z \in \mathcal{P}X$ (porque X es un conjunto).

Si $u \in A$, entonces $z \subset u$, luego $F(z) \subset F(u) \subset u$, con lo que $F(z) \subset z$.

Por la hipótesis, $F(F(z)) \subset F(z)$, luego $F(z) \in A$, luego $z \subset F(z)$, lo que nos da la igualdad $F(z) = z$. ∎

Teorema 1.24 (Teorema de Cantor-Bernstein) *Sean X e Y conjuntos tales que existen aplicaciones inyectivas $f : X \longrightarrow Y$ y $g : Y \longrightarrow X$. Entonces existe $h : X \longrightarrow Y$ biyectiva.*

Demostración: Sea $F : \mathcal{P}X \longrightarrow \mathcal{P}X$ la aplicación dada por $F(u) = X \setminus g[Y \setminus f[u]]$. Estamos en las hipótesis del teorema anterior, pues si $u \subset v \subset X$, entonces

$$f[u] \subset f[v], \quad Y \setminus f[v] \subset Y \setminus f[u], \quad g[Y \setminus f[v]] \subset g[Y \setminus f[u]],$$

$$X \setminus g[Y \setminus f[u]] \subset X \setminus g[Y \setminus f[v]],$$

luego $F(u) \subset F(v)$.

En consecuencia existe un subconjunto $z \subset X$ tal que $F(z) = z$, es decir, $X \setminus g[Y \setminus f[z]] = z$ o, equivalentemente, $X \setminus z = g[Y \setminus f[z]]$. Por consiguiente, $f|_z : z \longrightarrow f[z]$ y $g|_{Y \setminus f[z]} : Y \setminus f[z] \longrightarrow X \setminus z$ son ambas biyectivas, luego la unión de la primera con la inversa de la segunda nos da la aplicación h buscada. ∎

Así pues, aunque todavía no hayamos definido nada a lo que llamar "número de elementos" de un conjunto, tenemos probado que podemos hablar coherentemente de si un conjunto tiene un número de elementos mayor, igual o menor que otro. También es fácil probar que, dado cualquier conjunto, aunque sea infinito, siempre hay otro que tiene un número de elementos estrictamente mayor:

Teorema 1.25 (Teorema de Cantor) (AP) *Si X es un conjunto, $\overline{\overline{X}} < \overline{\overline{\mathcal{P}X}}$.*

DEMOSTRACIÓN: La aplicación $f : X \longrightarrow \mathcal{P}X$ dada por $f(x) = \{x\}$ es claramente inyectiva, luego $\overline{\overline{X}} \leq \overline{\overline{\mathcal{P}X}}$. Si se diera la igualdad, existiría una aplicación $g : X \longrightarrow \mathcal{P}(X)$ biyectiva, pero entonces podríamos considerar el conjunto[9] $R = \{x \in X \mid x \notin g(x)\} \in \mathcal{P}X$. Sea $r \in X$ tal que $g(r) = R$. Por definición de R tenemos que $r \in R$ si y sólo si $r \notin g(r) = R$, lo cual es una contradicción. ∎

La paradoja de Cantor El teorema de Cantor daba lugar a otra paradoja de la teoría de conjuntos, esta vez relacionada con la clase universal V. En efecto, si lo aplicamos al "conjunto" de todos los conjuntos, debería cumplirse que $\overline{\overline{V}} < \overline{\overline{\mathcal{P}V}}$, pero por otra parte, todos los elementos de $\mathcal{P}V$ son conjuntos, luego debería ser $\mathcal{P}V \subset V$ y, por consiguiente, $\overline{\overline{\mathcal{P}V}} \leq \overline{\overline{V}}$.

En NBG esto no causa ningún problema pues, dado que todos los elementos de V son conjuntos, se cumple de hecho que $\mathcal{P}V = V$, pero esto no contradice al teorema de Cantor porque éste sólo es válido para conjuntos y V no lo es (la paradoja de Cantor nos da una prueba alternativa de que V no es un conjunto). Si uno rastrea la prueba para ver en qué falla cuando se intenta aplicar a una clase propia, por ejemplo, tomando como $f : V \longrightarrow \mathcal{P}V$ la aplicación identidad, se encuentra con que la clase R construida en la prueba no es sino la clase de Russell $R = \{x \mid x \notin x\}$, que no es un conjunto, por lo que $R \notin \mathcal{P}V$, por lo que no podemos tomarle una antiimagen por f como se hace en la prueba. De hecho, así fue como Bertrand Russell descubrió la paradoja que lleva su nombre. ∎

En la sección 2.2, tras haber definido los números naturales, definiremos los conjuntos finitos y veremos cómo asignarles un número natural que "mida" su número de elementos. En el capítulo V generalizaremos esto a conjuntos arbitrarios, no necesariamente finitos.

Dedicamos las secciones siguientes a completar la exposición del "vocabulario conjuntista" básico, pero para evitar que el lector tenga que asimilar una larga lista de definiciones sin tener ningún ejemplo no trivial al que aplicarlas, le recomendamos que en este punto pase al capítulo siguiente y que vaya leyendo el resto de este capítulo a medida que vaya encontrando referencias a sus secciones.

1.6 Relaciones

Tras haber introducido el vocabulario conjuntista relacionado con las funciones, ahora vamos a hacer lo propio con las relaciones. La definición conjuntista de "relación" es muy simple:

[9] Aquí usamos decisivamente que X es un conjunto, pues esto implica que R también lo es y por eso podemos afirmar que $R \in \mathcal{P}X$.

Definición 1.26 Una *relación* (binaria) en una clase A es una clase $R \subset A \times A$. Si R es una relación en A y $a, b \in A$, escribiremos

$$a\,R\,b \equiv (a, b) \in R,$$

y en tal caso diremos que *a está relacionado con b* respecto de la relación R.

Observemos que, trivialmente, toda relación en un conjunto es un conjunto. Si R es una relación en una clase A, tenemos definida su inversa R^{-1}, que con la notación que acabamos de introducir es la relación en A determinada por que

$$a\,R^{-1}b \leftrightarrow b\,R\,a.$$

Diremos que una relación R en una clase A es:

1. *Reflexiva* si $\bigwedge x \in A\ x\,R\,x$,
2. *Irreflexiva* si $\bigwedge x \in A\ \neg x\,R\,x$,
3. *Simétrica* si $\bigwedge xy \in A\,(x\,R\,y \to y\,R\,x)$,
4. *Antisimétrica* si $\bigwedge xy \in A\,(x\,R\,y \wedge y\,R\,x \to x = y)$
5. *Asimétrica* si $\bigwedge xy \in A\,(x\,R\,y \to \neg y\,R\,x)$
6. *Transitiva* si $\bigwedge xyz \in A\,(x\,R\,y \wedge y\,R\,z \to x\,R\,z)$
7. *Conexa* si $\bigwedge xy \in A\,(x\,R\,y \vee y\,R\,x)$
8. *Débilmente conexa* si $\bigwedge xy \in A(x\,R\,y \vee y\,R\,x \vee x = y)$

Relaciones de orden Una *relación de orden parcial* en una clase A es una relación reflexiva, antisimétrica y transitiva en A. Si además es *conexa* se dice que es una *relación de orden total.*

Es costumbre usar el signo $\leq$ para representar relaciones de orden arbitrarias (de modo que si decimos que $\leq$ es una relación de orden en una clase A hay que entender que $\leq$ es una clase y que $\leq \subset A \times A$). En estos términos, las propiedades que definen una relación de orden se escriben así:

1. $\bigwedge a \in A\,a \leq a$,
2. $\bigwedge ab \in A(a \leq b \wedge b \leq a \to a = b)$,
3. $\bigwedge abc \in A(a \leq b \wedge b \leq c \to a \leq c)$.

La relación es de orden total si además $\bigwedge ab \in A(a \leq b \vee b \leq a)$.

Una *relación de orden estricto* en una clase A es una relación asimétrica y transitiva en A. Si además es débilmente conexa entonces es una *relación de orden total estricto.*

Notemos que, pese a la nomenclatura, una relación de orden estricto no es una relación de orden. La relación entre ambos conceptos es que si $\leq$ es una relación de orden en A, entonces la relación dada por

$$a < b \leftrightarrow a \leq b \wedge a \neq b$$

es una relación de orden estricto en A y, recíprocamente, si $<$ es una relación de orden estricto en A, entonces la relación dada por

$$a \leq b \leftrightarrow a < b \vee a = b$$

es una relación de orden en A. Estas dos construcciones son mutuamente inversas, en el sentido de que si aplicamos una y luego la otra volvemos a la relación de partida. Así pues, es indistinto definir una relación de orden o una relación de orden estricto en una clase dada, pues de una se pasa trivialmente a la otra. Usaremos también la notación $a \geq b \equiv b \leq a$ y $a > b \equiv b < a$ para las relaciones inversas correspondientes.

Cuando digamos que $(A, \leq)$ es una clase total o parcialmente ordenada querremos decir[10] que $\leq$ es una relación de orden (total o parcial) en A.

Sea A una clase ordenada por la relación $\leq$ y sea $B \subset A$. Entonces:

1. $M \in A$ es una *cota superior* de B si $\bigwedge x \in B\ x \leq M$,
2. $m \in A$ es una *cota inferior* de B si $\bigwedge x \in B\ m \leq x$,
3. $M \in A$ es un *maximal* de B si $M \in B$ y $\bigwedge x \in B(M \leq x \to M = x)$.
4. $m \in A$ es un *minimal* de B si $m \in B$ y $\bigwedge x \in B(x \leq m \to x = m)$.
5. $M \in A$ es el *supremo* de B si M es una cota superior de B y $\bigwedge x \in A(x$ es una cota superior de $B \to M \leq x)$.
6. $m \in A$ es el *ínfimo* de B si m es una cota inferior de B y $\bigwedge x \in A(x$ es una cota inferior de $B \to x \leq m)$.
7. $M \in A$ es el *máximo* de B si $M \in B$ y M es una cota superior de B.
8. $m \in A$ es el *mínimo* de B si $m \in B$ y m es una cota inferior de B.

[10]Si A es un conjunto podemos entender esto como una afirmación sobre el par ordenado $(A, \leq)$, pero usaremos esta misma expresión incluso si A es una clase propia, aunque ahora la afirmación "$(A, \leq)$ es una clase total o parcialmente ordenada" no puede interpretarse como una afirmación sobre el par ordenado $(A, \leq) = \{\{\varnothing\}\}$, sino literalmente como hemos indicado: como una forma cómoda de expresar que $\leq$ es una relación de orden en la clase A.

Ejemplo Si A es cualquier clase, la inclusión define una relación de orden parcial en $\mathcal{P}A$, es decir, podemos considerar en esta clase la relación dada por

$$X \leq Y \leftrightarrow X \subset Y.$$

Es inmediato comprobar que se trata de una relación de orden parcial cuya relación de orden estricto asociada es la inclusión estricta $X \subsetneq Y$.

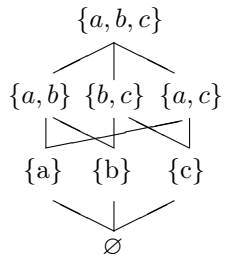
Respecto de esta relación, $\mathcal{P}A$ tiene como mínimo elemento a $\varnothing$. Si A es un conjunto, entonces $\mathcal{P}A$ tiene como máximo elemento a A, pero si A no es un conjunto, entonces $\mathcal{P}A$ no tiene máximo elemento, pues dado cualquier $X \in \mathcal{P}A$, será $X \subsetneq A$, luego existe un $x \in A \setminus X$, luego $X \subsetneq X \cup \{x\} \in \mathcal{P}A$, luego X no es el máximo de $\mathcal{P}A$.

Si $A \neq \varnothing$, la subclase $B = \mathcal{P}A \setminus \{\varnothing\}$ tiene por minimales a los elementos de la forma $\{a\}$, con $a \in A$, pero no tiene mínimo, salvo en el caso en que $A = \{a\}$, pues si A contiene al menos dos elementos a y b, entonces no se cumple $\{a\} \subset \{b\}$, luego $\{a\}$ no es mínimo de B, pero es minimal porque ningún elemento de B es menor que $\{a\}$.

Si B es un subconjunto de A, entonces $\bigcup B$ es el supremo de B en $\mathcal{P}A$, pues todo $x \in B$ cumple $x \subset \bigcup B$, luego $\bigcup B$ es una cota superior de B, y si $M \in \mathcal{P}A$ es una cota superior de B, esto significa que $\bigwedge x \in B\ x \subset M$, de donde se sigue que $\bigcup B \subset M$, luego $\bigcup B$ es la menor cota superior de B.

Similarmente, si $B \subset A$ es no vacío, entonces $\bigcap B$ es el ínfimo de B en $\mathcal{P}A$.

Así pues, si A tiene más de un elemento, hemos visto que $B = \mathcal{P}A \setminus \{\varnothing\}$ no tiene mínimo elemento, pero tiene por ínfimo a $\varnothing$.



Más concretamente, si $A = \{a, b, c\}$, donde los conjuntos a, b, c son distintos dos a dos, la relación de orden dada por la inclusión es la que muestra la figura. Vemos entonces que $\mathcal{P}A$ tiene por mínimo a $\varnothing$ y por máximo a A. En cambio, $\mathcal{P}A \setminus \{A\}$ no tiene máximo elemento, pero tiene tres elementos maximales, los tres conjuntos con dos elementos. Similarmente, $\mathcal{P}A \setminus \{\varnothing\}$ no tiene mínimo, pero tiene tres minimales, a saber, los conjuntos $\{a\}$, $\{b\}, \{c\}$, y también tiene ínfimo, concretamente $\varnothing$. El conjunto $B = \{\{a\}, \{b\}, \varnothing\}$ no tiene máximo, pero tiene por supremo a $\{a, b\}$. ∎

Es fácil ver que en un conjunto totalmente ordenado todo maximal es máximo y todo minimal es mínimo. Si un conjunto tiene máximo o mínimo, supremo o ínfimo, entonces éstos son únicos. El supremo (ínfimo) de una clase es máximo (mínimo) si y sólo si pertenece a la clase.

Cuando tenemos una clase A ordenada por una relación $\leq$ y una subclase $B \subset A$, consideramos, aunque no se indique explícitamente, que B está ordenada por la restricción de $\leq$ a B, es decir, con la intersección de $\leq$ con $B \times B$, de modo que si x, $y \in B$, se cumple $x \leq y$ como elementos de B si y sólo si se cumple como elementos de A. Es inmediato comprobar que esta restricción es un orden en B. Más aún, B está totalmente ordenada si A lo está.

Diremos que $F : (A, \leq_1) \longrightarrow (B, \leq_2)$ es *monótona creciente* o, simplemente, *creciente* si $\leq_1$ y $\leq_2$ son relaciones de orden parcial en A y B respectivamente, $F : A \longrightarrow B$ y

$$\bigwedge xy \in A(x \leq_1 y \to F(x) \leq_2 F(y)).$$

Se dice que F es *monótona decreciente* o *decreciente* si cumple

$$\bigwedge xy \in A(x \leq_1 y \to F(y) \leq_2 F(x)).$$

Se dice que F es *estrictamente* monótona creciente o decreciente si se cumple esto mismo cambiando las desigualdades no estrictas $\leq$ por desigualdades estrictas $<$.

Es fácil comprobar que si $F : (A, \leq_1) \longrightarrow (B, \leq_2)$ y $G : (B, \leq_2) \longrightarrow (C, \leq_3)$ son ambas monótonas crecientes o decrecientes estrictas o no, lo mismo le sucede a la composición $F \circ G : (A, \leq_1) \longrightarrow (C, \leq_3)$.

Diremos que $F : (A, \leq_1) \longrightarrow (B, \leq_2)$ es una *semejanza* si es biyectiva y tanto F como F^{-1} son crecientes. El carácter creciente de F y F^{-1} equivale a

$$\bigwedge xy \in A(x \leq_1 y \leftrightarrow F(x) \leq_2 F(y)).$$

Observemos que si $(A, \leq_1)$ está totalmente ordenada, entonces toda aplicación biyectiva y creciente $F : (A, \leq_1) \longrightarrow (B, \leq_2)$ es una semejanza, pues si $F(x) \leq_2 F(y)$, entonces $x \leq_1 y \vee y \leq_1 x$, pero si se da el segundo caso entonces $F(y) \leq_2 F(x)$ por la monotonía, luego $F(x) = F(y)$, por la antisimetría, luego $x = y$ por la biyectividad, luego igualmente $x_1 \leq_1 y$ por la reflexividad.

Las propiedades siguientes son inmediatas:

1. Para toda clase parcialmente ordenada $(A, \leq)$, se cumple que la identidad $I_A : (A, \leq) \longrightarrow (A, \leq)$ es una semejanza.

2. Si $F : (A, \leq_1) \longrightarrow (B, \leq_2)$ es una semejanza, entonces la aplicación inversa $F^{-1} : (B, \leq_2) \longrightarrow (A, \leq_1)$ también lo es.

3. Si $F : (A, \leq_1) \longrightarrow (B, \leq_2)$ y $G : (B, \leq_2) \longrightarrow (C, \leq_3)$ son semejanzas, entonces la composición $F \circ G : (A, \leq_1) \longrightarrow (C, \leq_3)$ también lo es.

Diremos que dos clases parcialmente ordenadas $(A, \leq_1)$ y $(B, \leq_2)$ son *semejantes,* y lo representaremos por $(A, \leq_1) \cong (B, \leq_2)$, si existe una semejanza $F : (A, \leq_1) \longrightarrow (B, \leq_2)$.

Las propiedades anteriores de las semejanzas se traducen inmediatamente en las propiedades siguientes de la semejanza entre clases parcialmente ordenadas:

1. Para toda clase parcialmente ordenada $(A, \leq)$, se cumple $(A, \leq) \cong (A, \leq)$.

2. Si $(A, \leq_1) \cong (B, \leq_2)$, entonces $(B, \leq_2) \cong (A, \leq_1)$.

3. Si $(A, \leq_1) \cong (B, \leq_2)$ y $(B, \leq_2) \cong (C, \leq_3)$, entonces $(A, \leq_1) \cong (C, \leq_3)$.

La idea subyacente en estos conceptos es que, al conservar las relaciones de orden, una semejanza $F : (A, \leq_1) \longrightarrow (B, \leq_2)$ conserva todas las propiedades relacionadas con el orden. Por ejemplo, si $X \subset A$ y m es el máximo, o el mínimo, o el supremo, o el ínfimo, o una cota superior/inferior de X, entonces $F(m)$ es lo mismo de $F[X]$. En general, toda propiedad que cumplan unos elementos y subconjuntos de A la cumplirán también las imágenes por F de estos elementos o conjuntos, y esto hace que dos clases semejantes tengan las mismas propiedades de orden (una está totalmente ordenada si y sólo si lo está la otra, una tiene máximo si y sólo si lo tiene la otra, etc.).

Clases bien ordenadas Un *buen orden* en una clase A es una relación de orden parcial respecto a la cual todas subclase[11] no vacía de A tiene mínimo elemento. Decimos que $(A, \leq)$ es una *clase bien ordenada* si $\leq$ es un buen orden en A.

En el capítulo III veremos que las buenas relaciones de orden desempeñan un papel central en la teoría de conjuntos, pero de momento presentaremos aquí únicamente las consecuencias inmediatas de la definición.

Ante todo, aunque hemos definido un buen orden como una relación de orden parcial, lo cierto es que la existencia de mínimos implica que es total, pues si $(A, \leq)$ es una clase bien ordenada y $x, y \in A$, el conjunto $\{x, y\}$ debe tener un mínimo elemento m, y entonces se cumple $x \leq y$ o bien $y \leq x$ según que sea $m = x$ o $m = y$.

También es evidente que toda subclase de una clase bien ordenada está bien ordenada.

En general, si $(A \leq)$ es un conjunto bien ordenado y $x \in A$, usaremos la notación

$$A_x^{\leq} \equiv \{a \in A \mid a \leq x\}, \qquad A_x^{<} \equiv \{a \in A \mid a < x\}.$$

Nos referiremos a ellos como la *sección inicial* no estricta (o estricta, respectivamente) determinada por x, que no es sino la clase de todos los elementos de A anteriores (o estrictamente anteriores) a x.

Una de las razones por las que las clases bien ordenadas son importantes es porque permiten razonar por inducción en el sentido del teorema siguiente:

Teorema 1.27 (Principio de inducción para clases bien ordenadas) *Si $(A, \leq)$ es una clase bien ordenada y $B \subset A$ cumple $\bigwedge x \in A(A_x^{<} \subset B \to x \in B)$, entonces $B = A$.*

Demostración: Si $B \neq A$, entonces $A \setminus B \neq \varnothing$, luego por la buena ordenación esta clase tiene un mínimo elemento x. Eso quiere decir que si $a < x$ entonces $a \notin A \setminus B$, luego $a \in B$. Equivalentemente, $A_x^{<} \subset B$, y por hipótesis,

[11] Observemos que la propiedad "$(A, \leq)$ es una clase bien ordenada" no es normal, porque contiene una cuantificación sobre todas las subclases de A, pero "$(A, \leq)$ es un conjunto bien ordenado" sí que lo es, porque ahora la existencia de mínimo se requiere para todos los subconjuntos no vacíos de A, luego el cuantificador está restringido a conjuntos.

esto implica $x \in B$, con lo que tenemos una contradicción, pues hemos tomado $x \in A \setminus B$. ∎

En la práctica esto significa que si queremos probar que todo elemento de una clase bien ordenada $(A, \leq)$ cumple una determinada propiedad normal $\phi(x)$, podemos fijar un $x \in A$ arbitrario y tomar como hipótesis de inducción que todos los elementos $a < x$ cumplen $\phi(a)$, y demostrar a partir de ahí $\phi(x)$. Si logramos esto, el teorema anterior aplicado a la clase $B = \{a \in A \mid \phi(a)\}$ implica que $B = A$, luego todo elemento de A cumple $\phi(x)$.

Veamos ahora una propiedad elemental que, no obstante, resulta de gran utilidad:

Teorema 1.28 *Si $F : (A, \leq) \longrightarrow (A, \leq)$ es una aplicación estrictamente creciente en una clase bien ordenada, entonces $\bigwedge a \in A\ a \leq F(a)$.*

Demostración: Supongamos que existe un $a \in A$ tal que $F(a) < a$. Entonces la clase $B = \{a \in A \mid F(a) < a\}$ no es vacía, luego tiene un mínimo elemento m. En particular $F(m) < m$ y, como F es estrictamente creciente, $F(F(m)) < F(m)$, pero entonces $a = F(m)$ cumple $a \in B$ y $a < m$, en contradicción con que m era el mínimo de B. ∎

De aquí extraemos dos consecuencias de interés:

Teorema 1.29 *Una clase bien ordenada no puede ser semejante a una de sus secciones iniciales estrictas.*

Demostración: Sea $(A, \leq)$ una clase bien ordenada, y supongamos que existe $x \in A$ tal que existe una semejanza[12] $F : (A, \leq) \longrightarrow (A^<_x, \leq)$. En particular $F : (A, \leq) \longrightarrow (A, \leq)$ es estrictamente creciente, pero $F(x) \in A^<_x$, luego $F(x) < x$, en contradicción con el teorema anterior. ∎

Teorema 1.30 *Si dos clases bien ordenadas son semejantes, entonces existe una única semejanza entre ellas.*

Demostración: Supongamos que $F, G : (A, \leq_1) \longrightarrow (B, \leq_2)$ son dos semejanzas entre las mismas clases bien ordenadas. Entonces la composición $F \circ G^{-1} : (A, \leq_1) \longrightarrow (A, \leq_1)$ es también una semejanza, luego por 1.28 tenemos que $\bigwedge a \in A\ a \leq_1 G^{-1}(F(a))$, y aplicando G resulta $\bigwedge a \in A\ G(a) \leq_1 F(a)$. Pero las hipótesis son las mismas para F y G, luego igualmente podemos probar la desigualdad opuesta, y concluimos que $\bigwedge a \in A\ F(a) = G(a)$, luego $F = G$. ∎

No vamos a probar aquí más resultados sobre clases bien ordenadas porque en el capítulo III estaremos en condiciones de razonar más cómodamente sobre ellas.

[12] Técnicamente junto a $A^<_x$ no deberíamos escribir $\leq$, sino la restricción de $\leq$ a $A^<_x$, pero no pasa nada por relajar la notación en estos contextos.

Relaciones de equivalencia Una *relación de equivalencia* en una clase A es una relación reflexiva, simétrica y transitiva en A.

Si R es una relación de equivalencia en A y $a \in A$, definimos la *clase de equivalencia* de a respecto de R como

$$[a]_R \equiv \{b \in A \mid a\,R\,b\},$$

es decir, como la clase de todos los elementos de A relacionados con a. El resultado fundamental sobre clases de equivalencia es el siguiente, cuya prueba dejamos a cargo del lector:

Teorema 1.31 *Sea R una relación de equivalencia en una clase A y consideremos a, $b \in A$. Entonces:*

1. $a\,R\,b \leftrightarrow [a]_R = [b]_R$,
2. $\neg a\,R\,b \leftrightarrow [a]_R \cap [b]_R = \varnothing$.

En particular, dos clases de equivalencia en A son iguales o disjuntas.

Diremos que una relación de equivalencia en una clase A es *conjuntista* si todas las clases de equivalencia que determina son conjuntos. Esto sucede en particular si A es un conjunto, pues en general las clases de equivalencia son subclases de A, luego si A es un conjunto todas ellas lo son también.

Si una relación de equivalencia R en una clase A es conjuntista, podemos definir la *clase cociente* como[13]

$$A/R \equiv \{[a]_R \mid a \in A\}.$$

Naturalmente, también podemos considerar la clase cociente para una relación no conjuntista, pero entonces puede ocurrir perfectamente que $A/R = \varnothing$, lo cual no significa que no haya clases de equivalencia, sino que ninguna de ellas es un conjunto.

En el caso en que R es conjuntista podemos definir la *aplicación canónica* $p : A \longrightarrow A/R$ dada por $p(a) = [a]_R$.

Obviamente es suprayectiva, luego el axioma de reemplazo nos da que si A es un conjunto, A/R también lo es, y hablamos entonces del *conjunto cociente,* en lugar de clase cociente (aunque en este caso se sigue hablando de *clases* de equivalencia).

1.7 Leyes de composición interna

Para terminar con la presentación de los conceptos conjuntistas básicos nos ocupamos ahora de las operaciones definidas sobre una clase.

[13] Técnicamente, la existencia de la clase cociente viene dada por el axioma de comprensión, teniendo en cuenta que $A/R \equiv \{y \mid \bigvee a \in A\ y = [a]_R\}$.

Definición 1.32 Una *ley de composición interna* u *operación* en una clase A es una aplicación $* : A \times A \longrightarrow A$. En este contexto, si $a, b \in A$, escribiremos

$$a * b \equiv *(a, b).$$

Así pues, una operación en A es una función que a cada par de elementos a y b de A (en un cierto orden) les asigna un nuevo elemento $a * b \in A$.

Diremos que una operación en una clase A

1. es *asociativa* si $\bigwedge abc \in A\ (a * b) * c = a * (b * c)$
2. es *conmutativa* si $\bigwedge ab \in A\ a * b = b * a$
3. tiene por *elemento neutro* a $e \in A$ si $\bigwedge a \in A\ a * e = e * a = a$

Observemos que una operación en una clase A puede tener a lo sumo un elemento neutro, pues si tuviera dos, digamos e y e', sería $e = e * e' = e'$.

Si una operación $*$ en una clase A tiene elemento neutro e, se dice que un elemento $b \in A$ es el *inverso* de un elemento $a \in A$ si $a * b = b * a = e$. Si la operación es asociativa y a tiene inverso, éste es único, pues si tuviera dos, digamos b y b', entonces $b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$.

Anillos y cuerpos Para presentar los conceptos siguientes nos restringimos por comodidad a operaciones sobre conjuntos, pues es el único contexto en el que los vamos a encontrar:

Un *anillo* es una terna[14] $(A, +, \cdot)$, donde $+$ y $\cdot$ son operaciones en A (a las que llamaremos *suma* y *producto,* respectivamente, de modo que se cumplen las propiedades siguientes:

1. La suma es asociativa y conmutativa, tiene un elemento neutro, necesariamente único, que representaremos por 0, y cada $a \in A$ tiene un inverso, necesariamente único, que representaremos por $-a$.
2. El producto es asociativo y satisface la *propiedad distributiva* respecto de la suma, es decir,

$$\bigwedge abc \in A\ a(b + c) = ab + ac \quad \text{y} \quad \bigwedge abc \in A\ (b + c)a = ba + ca.$$

Nota En la práctica escribiremos A en lugar de $(A, +, \cdot)$, de modo que cuando digamos que "A es un anillo" querremos decir que estamos considerando un conjunto A con dos operaciones prefijadas $+$ y $\cdot$ con las cuales $(A, +, \cdot)$ es un anillo.

También es costumbre (tal y como hemos hecho ya al enunciar la propiedad distributiva) escribir $ab \equiv a \cdot b$ cuando ello no induce a confusión, así como abreviar $a + (-b) \equiv a - b$.

[14] En general, podemos definir una terna de conjuntos como $(a, b, c) \equiv ((a, b), c)$, e igualmente una cuádrupla es $(a, b, c, d) \equiv (((a, b), c), d)$, etc.

Por último la propiedad asociativa de la suma y el producto hace que no sea necesario agrupar sumandos o factores con paréntesis, de modo que podemos escribir $a+b+c=(a+b)+c=a+(b+c)$. ∎

Si el producto de un anillo tiene elemento neutro se dice que el anillo es *unitario,* y dicho neutro se representa por 1.

Si el producto es conmutativo se dice que el anillo es *conmutativo.*

Si un elemento a de un anillo tiene inverso para el producto se dice que es *inversible*, y su inverso se representa por a^{-1}.

El producto de dos elementos inversibles es inversible, pues es fácil ver que $(ab)^{-1}=b^{-1}a^{-1}$. Además, el inverso de un elemento inversible es inversible, pues trivialmente $(a^{-1})^{-1}=a$. Puesto que $1\cdot 1=1$, tenemos que 1 es inversible y $1^{-1}=1$.

Observemos que estos hechos se demuestran igualmente para la suma, donde la existencia de inverso esta garantizada. Concretamente:

$$-(a+b)=-a-b,\quad -(-a)=a,\quad -0=0.$$

Los inversos (si existen) permiten despejar en ecuaciones, es decir:

$$a+b=c\to a=c-b,\qquad ab=c\to a=cb^{-1}.$$

En todo anillo A se cumple que $\bigwedge a\in A\ a\cdot 0=0\cdot a=0$. En efecto:

$$a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0,$$

y sumando $-(a\cdot 0)$ a ambos miembros concluimos que $a\cdot 0=0$. Igualmente sucede si multiplicamos el 0 por la izquierda.

Esto tiene varias consecuencias. Por ejemplo, podemos suprimir los paréntesis en expresiones de la forma

$$-(ab)=(-a)b=a(-b).$$

En efecto: $ab+(-a)b=(a-a)b=0b=0$, luego $(-a)b=-(ab)$, y la otra igualdad se prueba análogamente.

En un anillo unitario se cumple que $(-1)a=a(-1)=-a$, pues

$$a+(-1)a=1a+(-1)a=(1-1)a=0\cdot a=0.$$

En particular $(-1)(-1)=-(-1)=1$. Así pues, tanto 1 como -1 son inversibles y cada uno es su propio inverso.

Salvo en el caso trivial en que $1=0$, en un anillo unitario el 0 no puede tener inverso para el producto, pues, para todo $a\in A$, se cumple $0\cdot a=0\neq 1$.

Un *dominio íntegro* es un anillo conmutativo y unitario A en el que $1\neq 0$ y además

$$\bigwedge ab\in A(ab=0\to a=0\vee b=0)$$

Esto implica en particular que los elementos no nulos son simplificables, es decir, que

$$\bigwedge abc \in A(a \neq 0 \wedge ab = ac \to b = c).$$

En efecto: si $ab = ac$, entonces $a(b - c) = 0$ y, como $a \neq 0$, tiene que ser $b - c = 0$, luego $b = c$. (Y lo mismo vale si a multiplica por la derecha.)

Observemos que esta propiedad es trivialmente cierta para la suma en cualquier anillo:

$$\bigwedge abc \in A(a + b = a + c \to b = c).$$

Para probarlo basta sumar $-a$ a ambos miembros.

Un *cuerpo* es un anillo conmutativo y unitario en el que $1 \neq 0$ y todo elemento distinto de 0 tiene inverso para el producto.

Un cuerpo es siempre un dominio íntegro, pues si $ab = 0$ y $a \neq 0$, entonces $a^{-1}ab = a^{-1}0 = 0$, luego $b = 1b = 0$.

Si $(A, +, \cdot)$ es un cuerpo y $a, b \in A$, con $b \neq 0$, es frecuente representar

$$\frac{a}{b} = ab^{-1} = b^{-1}a.$$

Se dice entonces que la expresión a/b es una *fracción* de *numerador* a y *denominador* b. Es inmediato entonces que

$$\frac{a}{b} = \frac{c}{d} \leftrightarrow ad = bc.$$

Además, si $c \neq 0$, se cumple que

$$\frac{a}{b} = \frac{ac}{bc}, \qquad c \cdot \frac{a}{b} = \frac{ca}{b}, \qquad -\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b},$$

y también se comprueba sin dificultad (suponiendo siempre que los denominadores son no nulos) que

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

Definición 1.33 Una aplicación $f : A \longrightarrow B$ entre dos anillos es un *homomorfismo de anillos* si cumple[15]

$$\bigwedge xy \in A\ f(x + y) = f(x) + f(y), \qquad \bigwedge xy \in A\ f(xy) = f(x)f(y).$$

Si además es inyectiva, suprayectiva o biyectiva se dice que es un *monomorfismo, epimorfismo* o *isomorfismo* de anillos, respectivamente. Dos anillos son *isomorfos* si existe un isomorfismo de anillos entre ellos.

Si dos anillos A y B cumplen que $A \subset B$ y las operaciones de A son las restricciones de las de B (es decir, que $x + y$ y xy significa lo mismo en A y en B) entonces se dice que A es un *subanillo* de B.

[15]Estas propiedades implican que $f(0) = 0$, pues $f(0) = f(0 + 0) = f(0) + f(0)$, luego $f(0) = 0$, y si f es un monomorfismo y A y B son dominios íntegros entonces $f(1) = 1$, pues igualmente $f(1) = f(1)f(1)$, luego $f(1)(1 - f(1)) = 0$ y $f(1) \neq f(0) = 0$, luego $f(1) = 1$.

Si $f : A \longrightarrow B$ es un homomorfismo de anillos, entonces $f[A]$ es un subanillo de B con la suma y el producto de B, pues dos elementos de $f[A]$ son de la forma $f(x)$ y $f(y)$, para ciertos x, $y \in A$, luego su suma y su producto son $f(x) + f(y) = f(x + y) \in f[A]$, $f(x)f(y) = f(xy) \in f[A]$, luego al sumar y multiplicar con las operaciones de B no nos salimos de $f[A]$, y tenemos, por consiguiente, dos leyes de composición interna en $i[A]$, que obviamente cumplen todas las propiedades requeridas para formar un anillo.

Si además f es un monomorfismo, entonces $f : A \longrightarrow f[A]$ es por definición un isomorfismo de anillos, por lo que podemos decir que A es isomorfo a un subanillo de B.

Por último, si dos anillos son isomorfos, esto significa que tienen las mismas propiedades que dependan únicamente de la suma y del producto.

Anillos ordenados Un *anillo ordenado* es una cuádrupla $(A, +, \cdot, \leq)$ donde $(A, +, \cdot)$ es un anillo conmutativo y $(A, \leq)$ es un conjunto totalmente ordenado, de modo que se cumplan las dos *propiedades de compatibilidad* siguientes:

1. $\bigwedge abc \in A\ (a \leq b \to a + c \leq b + c)$
2. $\bigwedge ab \in A\ (a \geq 0 \wedge b \geq 0 \to ab \geq 0)$

Diremos que un elemento a de un anillo ordenado es

1. *positivo* si $a \geq 0$,
2. *estrictamente positivo* si $a > 0$,
3. *negativo* si $a \leq 0$,
4. *estrictamente negativo* si $a < 0$.

Representaremos por

$$A^+ \equiv \{a \in A \mid a > 0\}, \qquad A^- \equiv \{a \in A \mid a < 0\},$$

los conjuntos de elementos estrictamente positivos y estrictamente negativos, respectivamente, de un anillo ordenado A. De este modo, A se descompone en unión disjunta $A = A^- \cup \{0\} \cup A^+$.

La primera propiedad de compatibilidad nos permite despejar sumas:

$$a + b \leq c \to a \leq c - b.$$

En particular, $0 \leq a \leftrightarrow -a \leq 0$, de modo que el inverso de un elemento (estrictamente) positivo es (estrictamente) negativo, y viceversa.

La segunda propiedad de compatibilidad implica que la multiplicación por elementos positivos conserva las desigualdades:

$$\bigwedge abc \in A(a \leq b \wedge c \geq 0 \to ac \leq bc).$$

En efecto, como $b-a \geq 0$, resulta que $(b-a)c = bc - ac \geq 0$, luego $ac \leq bc$.

En cambio, la multiplicación por elementos negativos invierte las desigualdades:

$$\bigwedge abc \in A(a \leq b \wedge c \leq 0 \to ac \geq bc).$$

En efecto, como $-c \geq 0$, tenemos que $-ac \leq -bc$, de donde, despejando dos veces, $bc \leq ac$.

De estas dos propiedades se sigue en particular que el producto de dos elementos positivos o dos elementos negativos es positivo, mientras que el producto de un positivo por un negativo es negativo. En particular, todo cuadrado (todo producto de un elemento por sí mismo) es positivo.

En particular, en un anillo unitario ordenado en el que $1 \neq 0$ se cumple que $-1 < 0 < 1$. En efecto, basta tener en cuenta que $1 = 1 \cdot 1 > 0$.

Además, la igualdad $a \cdot a^{-1} = 1 > 0$ implica que el inverso de un elemento positivo (resp. negativo) es positivo (resp. negativo).

En todo anillo ordenado A podemos definir la función *valor absoluto*

$$|\ \ | : A \longrightarrow A^+ \cup \{0\}$$

dada por

$$|a| = \begin{cases} a & \text{si } a \geq 0, \\ -a & \text{si } a \leq 0. \end{cases}$$

Se cumplen las propiedades siguientes:

1. $|a| = 0 \leftrightarrow a = 0$,
2. $|a+b| \leq |a| + |b|$,
3. $|ab| = |a||b|$,
4. $|-a| = |a|$,
5. $||a| - |b|| \leq |a-b|$.

En efecto, la propiedad a) es evidente, para probar b) conviene observar que

$$|a| \leq b \leftrightarrow -b \leq a \leq b.$$

Las dos implicaciones se prueban trivialmente distinguiendo dos casos, según si a es positivo o negativo. En particular, como $|a| \leq |a|$ y $|b| \leq |b|$, tenemos que

$$-|a| \leq a \leq |a|, \qquad -|b| \leq b \leq |b|,$$

de donde, aplicando varias veces las propiedades de compatibilidad,

$$-|a| - |b| \leq a + b \leq |a| + |b|,$$

lo que a su vez implica que $|a+b| \leq |a|+|b|$. Las propiedades c) y d) se obtienen fácilmente distinguiendo casos. Para probar e) observamos que

$$|a| = |a - b + b| \leq |a - b| + |b| \Rightarrow |a| - |b| \leq |a - b|.$$

Invirtiendo los papeles probamos que $|b| - |a| \leq |b - a| = |-(a - b)| = |a - b|$, luego

$$-|a - b| \leq |a| - |b| \leq |a - b|,$$

y hemos visto que esto equivale a $||a| - |b|| \leq |a - b|$. ∎

Definición 1.34 Un *homomorfismo* (resp. *monomorfismo, epimorfismo, isomorfismo*) de anillos ordenados es un homomorfismo (resp. monomorfismo, epimorfismo, isomorfismo) de anillos $f : A \longrightarrow B$ que además cumpla la relación

$$\bigwedge xy \in A(x \leq y \to f(x) \leq f(y)).$$

Equivalentemente, un isomorfismo de anillos ordenados es un isomorfismo de anillos que además es una semejanza, lo cual hace que ambos anillos sean indistinguibles respecto de todas las propiedades definibles en términos de la suma, el producto o la relación de orden.

Ideales y anillos cociente Presentamos algunos elementos más de la teoría de anillos que nos serán útiles más adelante:

Definición 1.35 Sea A un anillo conmutativo y unitario. Un *ideal* de A es un conjunto $I \subset A$ tal que:

1. $0 \in I$,
2. $\bigwedge xy \in I\ x + y \in I$,
3. $\bigwedge a \in A \bigwedge b \in I\ ab \in I$.

Por ejemplo, si $x \in A$ el conjunto $(x) = \{ax \mid a \in A\}$ de los múltiplos de x es claramente un ideal[16] de A. Los ideales de esta forma se llaman *ideales principales* de A.

También es claro que $\{0\}$ y A son ideales de A. El ideal $\{0\}$ se llama *ideal trivial*. Un ideal I es *propio* si $I \neq A$ e $I \neq \{0\}$.

Observemos que un ideal I cumple $I = A$ si y sólo si contiene un elemento inversible, pues si es propio contiene a 1 y, si contiene a un elemento inversible x, entonces contiene a $1 = x^{-1}x$ por c) y, dado $a \in A$, tenemos que $a = a \cdot 1 \in I$ de nuevo por c).

Esto implica que un anillo conmutativo y unitario A es un cuerpo si y sólo si no tiene ideales propios. En efecto, si A es un cuerpo, todo ideal no trivial

[16] De hecho, históricamente el concepto de ideal surgió como una abstracción de los conjuntos de múltiplos, de modo que I puede verse como el conjunto de los múltiplos de un "elemento ideal" de A, que será un elemento real de A si I es de la forma $I = (x)$.

contiene un elemento inversible, luego es impropio. Recíprocamente, si A no es un cuerpo, tiene un elemento no nulo no inversible x, y entonces (x) es un ideal propio (porque si fuera $(x) = A$ tendríamos que $1 \in (x)$, y entonces x sería inversible).

Si I es un ideal en un anillo A, definimos la relación de *congruencia módulo I* como la relación en A dada por

$$x \equiv y \text{ (mód } I) \leftrightarrow x - y \in I.$$

Se trata de una relación de equivalencia: es reflexiva por la propiedad a), es simétrica por c) (pues $y - x = (-1)(x - y)$) y es transitiva por b).

Representaremos por A/I el conjunto cociente de A respecto de la congruencia módulo I. El resultado fundamental es el siguiente:

Teorema 1.36 *Si A es un anillo conmutativo y unitario e I es un ideal de A, entonces A/I se convierte en un anillo conmutativo y unitario con las operaciones dadas por $[a] + [b] = [a + b]$ y $[a][b] = [ab]$.*

Demostración: Lo único que no es inmediato es que las operaciones están bien definidas, es decir, que si $[a] = [a']$ y $[b] = [b']$ entonces $[a + b] = [a' + b']$ y $[ab] = [a'b']$. Ahora bien, tenemos que

$$a - a' = u \in I, \qquad b - b' = v \in I,$$

luego $a + b - (a' + b') = u + v \in I$ y

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' = av + ub' \in I.$$

A partir de aquí, cada propiedad de la suma y el producto de A implica trivialmente la propiedad correspondiente en A/I. ∎

En vista del teorema anterior, A/I se conoce como el *anillo cociente* de A determinado por I.

Teorema 1.37 (Teorema de isomorfía) *Si $f : A \longrightarrow B$ es un epimorfismo de anillos, entonces su núcleo $\mathrm{N}(f) = \{a \in A \mid f(a) = 0\}$ es un ideal de A y f induce un isomorfismo $\bar{f} : A/\mathrm{N}(f) \longrightarrow B$ dado por $\bar{f}([a]) = f(a)$.*

Demostración: Es inmediato comprobar que $\mathrm{N}(f)$ es un ideal. Si $[a] = [b] \in A/\mathrm{N}(f)$, entonces $a - b \in Nuc(f)$, luego $f(a) - f(b) = 0$, es decir, $f(a) = f(b)$, lo que prueba que $\bar{f}$ está bien definida, y es inmediato comprobar que es un isomorfismo de anillos. ∎

Definición 1.38 Un ideal M de un anillo A es *maximal* si $M \subsetneq A$ y no existe ningún ideal $M \subsetneq I \subsetneq A$. Un ideal P de A es *primo* si $P \neq A$ y

$$\bigwedge xy \in A\ (xy \in P \to x \in P \vee y \in P).$$

Estos conceptos son muy importantes en el estudio de la aritmética de un anillo, pero aquí sólo necesitaremos el resultado siguiente:

Teorema 1.39 *Si A es un anillo conmutativo y unitario, entonces un ideal I de A es maximal si y sólo si A/I es un cuerpo. A su vez, I es primo si y sólo si A/I es un dominio íntegro.*

DEMOSTRACIÓN: Si I es maximal, observamos en primer lugar que $1 \notin I$, luego $[1] \neq [0]$, que es uno de los requisitos que debe cumplir A/I para ser cuerpo. Tomemos $[x] \in A/I$ tal que $[x] \neq 0$, lo cual equivale a que $x \notin I$. Es fácil ver que

$$J = \{u + ax \mid u \in I \wedge a \in A\}$$

es un ideal de A que contiene a I y a x, luego $I \subsetneq J \subset A$. Por la maximalidad de I tiene que ser $J = A$, luego $1 \in J$, luego $1 = u + ax$, para cierto $u \in I$ y cierto $a \in A$, luego $1 = [1] = [a][x]$, luego $[x]$ tiene inverso y por lo tanto A/I es un cuerpo.

Si A/I es un cuerpo entonces $[1] \neq [0]$, luego $1 \notin I$, luego $I \neq A$. Si un ideal cumple $I \subsetneq J \subset A$, tomemos $x \in J \setminus I$, entonces $[x] \neq 0$, luego existe un $a \in A$ tal que $[a][x] = [1]$, luego $1 = ax + u$, para cierto $u \in I$, luego $1 \in J$, luego $J = A$. Esto prueba que I es maximal.

Si I es primo, como el en caso anterior vemos que $[1] \neq [0]$, lo cual es parte de la definición de dominio íntegro. Sean x, $y \in A$ tales que $[x][y] = [0]$. Entonces $xy \in I$, luego $x \in I$ o bien $y \in I$, luego $[x] = 0$ o $[y] = 0$. Esto prueba que A/I es un dominio íntegro.

Recíprocamente, si A/I es un dominio íntegro entonces, como antes, $I \neq A$, y si $xy \in I$, entonces $[x][y] = 0$, luego $[x] = 0$ o bien $[y] = 0$, luego $x \in I$ o bien $y \in I$. Esto prueba que I es primo. ∎

En particular, como todo cuerpo es un dominio íntegro, concluimos que todo ideal maximal es primo.

Capítulo II

El sistema numérico

Si la teoría de conjuntos sirve como fundamento a todas las ramas de la matemática no es sólo porque —tal y como hemos visto en el capítulo anterior— introduzca un vocabulario útil para todas ellas, sino, sobre todo, porque permite construir todos los objetos matemáticos de interés. La práctica totalidad de tales objetos se construyen a partir de los números (naturales, enteros, racionales, etc.), así que vamos a dedicar este capítulo a construir el sistema numérico a partir de la teoría axiomática que hemos presentado.

En realidad para ello necesitamos un axioma adicional, pues los conjuntos numéricos son conjuntos infinitos, y sucede que ninguno de los axiomas que hemos dado hasta ahora garantiza la existencia de conjuntos infinitos (la clase universal V es infinita, pues contiene, por ejemplo, a los conjuntos

$$\varnothing, \quad \{\varnothing\}, \quad \{\{\varnothing\}\}, \quad \ldots$$

pero no es un conjunto).

2.1 Los números naturales

Más adelante veremos que es posible definir los números naturales sin necesidad de ningún axioma adicional, pero de momento lo haremos a partir del axioma siguiente:

Axioma de infinitud *Existe un conjunto X con una aplicación $S : X \longrightarrow X$ inyectiva y no suprayectiva.*

Todavía no hemos definido los conceptos de "conjunto finito" o "conjunto infinito", pero el lector se convencerá fácilmente de que toda aplicación inyectiva de un conjunto finito en sí mismo tiene que ser suprayectiva, por lo que el axioma de infinitud es una forma de postular la existencia de un conjunto infinito sin necesidad de haber definido tal concepto.

En lo que sigue razonaremos en la teoría NBG* más el axioma de infinitud. En particular, no necesitamos suponer el axioma de partes.

Teorema 2.1 (Axiomas de Peano) *Existe un conjunto N, una aplicación $S : N \longrightarrow N$ y otro conjunto 0 de modo que se cumplen las propiedades siguientes:*

1. $0 \in N$.
2. *Si $n \in N$, entonces $S(n) \in N$.*
3. *No existe ningún $n \in N$ tal que $S(n) = 0$.*
4. *Si $m, n \in N$ y $S(m) = S(n)$, entonces $m = n$.*
5. *Si $A \subset N$ tiene la propiedad de que $0 \in A$ y siempre que $n \in A$ también $S(n) \in A$, entonces $A = N$.*

Demostración: Sea $S : X \longrightarrow X$ una aplicación inyectiva y no suprayectiva, tal y como postula el axioma de infinitud y elijamos un elemento $0 \in X$ que no tenga antiimagen.

Diremos que un subconjunto $A \subset X$ es *inductivo* si $0 \in A$ y, cuando $n \in A$, entonces también $S(n) \in A$. Llamemos $\mathcal{I}$ a la clase de todos los conjuntos inductivos, es decir,

$$\mathcal{I} = \{A \mid A \subset X \wedge A \text{ es inductivo}\}.$$

Como $\mathcal{I} \subset \mathcal{P}X$, el axioma de partes nos permitiría probar que $\mathcal{I}$ es un conjunto, pero no vamos a necesitar este hecho. Observemos que $\mathcal{I} \neq \varnothing$, ya que $X \in \mathcal{I}$. Sea $N = \bigcap \mathcal{I}$. Así $N \subset X$, luego N es un conjunto.

Se cumple que $0 \in N$, pues esto equivale a que $0 \in A$ para todo $A \in \mathcal{I}$, y esto es cierto por definición de conjunto inductivo.

Similarmente, si $n \in N$, se cumple que $S(n) \in N$, pues, para todo $A \in \mathcal{I}$, tenemos que A es inductivo y que $n \in A$, por lo que $S(n) \in A$, y esto implica que $S(n) \in N$.

Esto nos permite restringir $S|_N : N \longrightarrow N$. Si pasamos a llamar S a esta restricción, tenemos que cumple las propiedades 1) y 2). La propiedad 3) se cumple también, porque hemos elegido 0 sin antiimagen por S, luego sigue sin tener antiimagen por la restricción de S. La propiedad 4) se cumple porque S es inyectiva y la propiedad 5) se cumple porque su hipótesis es que $A \subset N$ es inductivo, luego $A \in \mathcal{I}$, luego $N \subset A$, luego $A = N$. ∎

Definición 2.2 Un *sistema de Peano* es una terna[1] $(N, S, 0)$ que cumple las cinco propiedades del teorema anterior.

En todo sistema de Peano podemos definir:

$$1 = S(0), \quad 2 = S(1), \quad 3 = S(2), \quad 4 = S(3), \quad 5 = S(4),$$

$$6 = S(5), \quad 7 = S(6), \quad 8 = S(7), \quad 9 = S(8).$$

[1] En general podemos definir una terna como $(a, b, c) = ((a, b), c)$.

En general, para cada $n \in N$, el conjunto $S(n)$ recibe el nombre de "sucesor" o "siguiente" de n (respecto del sistema de Peano dado). Si $S(n) = m$ se dice también que n es el "anterior" de m.

Nuestra intención es definir los números naturales como los elementos de cualquier sistema de Peano. En estos términos, lo que dicen los axiomas de Peano es:

1. *Hay un número natural llamado* 0 *(cero).*
2. *Todo número natural* n *tiene un sucesor* $S(n)$*.*
3. *El* 0 *no es el sucesor de ningún número natural.*
4. *Números naturales distintos tienen sucesores distintos.*
5. **(Principio de inducción)** *Si* $A \subset N$ *y podemos probar que* $0 \in A$ *y, suponiendo que* $n \in A$*, podemos probar que también* $S(n) \in A$*, entonces necesariamente* A *es el conjunto de todos los números naturales.*

Notemos que $n \in A$ permite expresar el hecho de que n cumple cualquier propiedad $\phi(n)$, sin más que definir $A = \{n \in N \mid \phi(n)\}$. Veamos un ejemplo sencillo de aplicación del principio de inducción:

Teorema 2.3 *En un sistema de Peano, todo elemento distinto de* 0 *tiene un anterior.*

Demostración: Sea $(N, S, 0)$ un sistema de Peano y sea

$$A = \{n \in N \mid n = 0 \vee \bigvee m \in N\ n = S(m)\}.$$

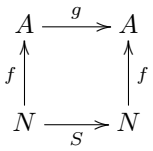
Es inmediato que $0 \in A$, así como que, si $n \in A$, entonces $S(n) \in A$, luego por el principio de inducción $A = N$, lo cual significa que todo $n \in N$ que no sea 0 tiene un anterior. ∎

Vemos que el axioma de infinitud es equivalente a la existencia de un sistema de Peano (pues hemos probado que existe un a partir del axioma y, recíprocamente, la función sucesor S de un sistema de Peano es una aplicación inyectiva y no suprayectiva).

Para que sea razonable definir los números naturales como los elementos de cualquier sistema de Peano prefijado debemos justificar que es irrelevante el sistema elegido. Para ello demostraremos en primer lugar un resultado fundamental sobre números naturales, junto con el principio de inducción:

Teorema 2.4 (Principio de recursión) *Sea* $(N, S, 0)$ *un sistema de Peano, sea* $g : A \longrightarrow A$ *una aplicación arbitraria y sea* $a \in A$*. Entonces existe una única aplicación* $f : N \longrightarrow A$ *tal que* $f(0) = a$ *y para todo* $n \in N$ *se cumple que* $f(S(n)) = g(f(n))$*.*

La última propiedad se expresa a menudo diciendo que el diagrama siguiente es conmutativo:



Decir que un diagrama de este tipo es conmutativo quiere decir que si vamos de un punto a otro por dos caminos diferentes el resultado es el mismo, en este caso $f \circ g = S \circ f$, que es justo lo que afirma el teorema.

En la práctica, el principio de recursión afirma que para definir una aplicación $f : N \longrightarrow A$ en una clase A (no necesariamente un conjunto) no es necesario definir explícitamente $f(0)$, $f(1)$, $f(2)$, etc., sino que basta definir $f(0)$ como un cierto $a \in A$ y explicar cómo se calcula $f(S(n))$ supuesto que ya hayamos calculado $f(n)$, es decir, dar una función g que determine $f(S(n))$ a partir de $f(n)$. Esto determina completamente la función f, que vendrá dada por:

$$f(0) = a, \quad f(1) = f(S(0)) = g(a), \quad f(2) = f(S(1)) = g(g(a)),$$

$$f(3) = g(g(g(a))), \quad f(4) = g(g(g(g(a)))), \quad \ldots$$

Cuando definimos una función de este modo se dice que la estamos definiendo *por recurrencia*, o que la definición es *recursiva.*

Antes de ver ejemplos y aplicaciones vamos a demostrar el teorema:

DEMOSTRACIÓN: Diremos que $h : X \longrightarrow A$ es una *aproximación* si:

1. $X \subset N$, $0 \in X$ y siempre que $n \in X$ y $n \neq 0$ existe un $m \in X$ tal que $n = S(m)$
2. $h(0) = a$ y siempre que $n \in X$ y $S(n) \in X$, entonces $h(S(n)) = g(h(n))$.

Así, las aproximaciones son funciones que cumplen lo que requiere el teorema salvo que no tienen por qué estar definidas en todo N.

Veamos en primer lugar que si $h : X \longrightarrow A$ y $h' : X' \longrightarrow A$ son aproximaciones y $n \in X \cap X'$, entonces $h(n) = h'(n)$.

Lo probamos por inducción sobre n. Concretamente, consideramos el conjunto

$$P = \{n \in N \mid n \in X \cap X' \to h(n) = h'(n)\}$$

y vamos a probar que $P = N$.

Se cumple que $0 \in P$, porque por definición de aproximación $0 \in X \cap X'$ y $h(0) = a = h'(0)$.

Supongamos, como hipótesis de inducción, que si $n \in X \cap X'$, entonces $h(n) = h'(n)$ y vamos a probar que lo mismo vale para $S(n)$. Para ello suponemos que $S(n) \in X \cap X'$. Entonces, por definición de aproximación, $n \in X \cap X'$ (aquí usamos el cuarto axioma de Peano, que dice que n es el único anterior

de $S(n)$). Entonces, por hipótesis de inducción $h(n) = h'(n)$, y por definición de aproximación $h(S(n)) = g(h(n)) = g(h'(n)) = h'(S(n))$. Esto termina la prueba.

Ahora probamos que para todo $n \in N$ existe una aproximación h con n en su dominio. Lo probamos nuevamente por inducción sobre n. Es inmediato que la aplicación $h : \{0\} \longrightarrow A$ dada por $h(0) = a$ es una aproximación, y tiene a 0 en su dominio, luego el resultado es cierto para 0.

Supongamos, por hipótesis de inducción que $h : X \longrightarrow A$ es una aproximación tal que $n \in X$. Si $S(n) \in X$, entonces h cumple lo requerido para $S(n)$. En caso contrario es fácil ver que $h' : X \cup \{S(n)\} \longrightarrow A$ definida como h sobre los elementos de X y como $h'(S(n)) = g(h(n))$ es una aproximación con $S(n)$ en su dominio.

Ahora ya podemos definir $f : N \longrightarrow A$ como sigue: para cada $n \in N$, sabemos que existe una aproximación $h : X \longrightarrow A$ con n en su dominio y que, si tomamos dos cualesquiera, el valor de $h(n)$ va a ser el mismo para ambas. Por lo tanto podemos definir $f(n) = h(n)$.

Esto hace que, en particular, $f(0) = a$, porque todas las aproximaciones asignan a 0 la imagen a. Por otra parte, si $n \in N$ y $h : X \longrightarrow A$ es una aproximación tal que $S(n) \in X$, entonces, por definición de aproximación, $n \in X$, luego por definición de f tenemos que $f(n) = h(n)$ y $f(S(n)) = h(S(n))$, y por definición de aproximación

$$f(S(n)) = h(S(n)) = g(h(n)) = g(f(n)).$$

Por lo tanto, f cumple lo pedido, y sólo falta probar que sólo hay una f que cumpla esta propiedad. Para ello tenemos que probar que si $f : N \longrightarrow A$ y $f' : N \longrightarrow A$ cumplen las condiciones del enunciado, entonces $f = f'$, para lo cual a su vez basta probar que si $n \in N$ entonces $f(n) = f'(n)$. Esto lo probamos por inducción. Para $n = 0$ se cumple, pues $f(0) = a = f'(0)$. Si suponemos como hipótesis de inducción que $f(n) = f'(n)$, entonces

$$f(S(n)) = g(f(n)) = g(f'(n)) = f'(S(n)).$$

esto termina la prueba de la unicidad de f. ∎

Como primera aplicación demostramos la equivalencia entre todos los sistemas de Peano:

Teorema 2.5 *Si $(N, S, 0)$ y $(N', S', 0')$ son dos sistemas de Peano, entonces existe $f : N \longrightarrow N'$ biyectiva tal que $f(0) = 0'$ y que hace conmutativo el diagrama siguiente:*

$$\begin{array}{ccc} N & \xrightarrow{f} & N' \\ {\scriptstyle S}\uparrow & & \uparrow{\scriptstyle S'} \\ N & \xrightarrow[f]{} & N' \end{array}$$

Observemos que esto significa que $f(1) = f(S(0)) = S'(f(0)) = S'(0') = 1'$, $f(2) = f(S(1)) = S'(f(1)) = S'(1') = 2'$ y, en general, que f transforma el 0 de un sistema en el $0'$ del otro, el 1 de un sistema en el $1'$ del otro, y así sucesivamente. En definitiva, f es como un "diccionario" que traduce "cero" por "zero", "uno" por "one", "dos" por "two" y así sucesivamente, poniendo en evidencia que los dos sistemas de Peano no son más que dos ristras de nombres alternativos para los números naturales, de modo que es lo mismo partir de "dos", calcular el siguiente "tres" y luego traducir "three" que partir de "dos", traducir "two" y luego calcular el siguiente "three".

DEMOSTRACIÓN: Aplicamos el teorema de recursión a $0' \in N'$ y a la función $S' : N' \longrightarrow N'$. La conclusión es que existe una función $f : N \longrightarrow N'$ tal que $f(0) = 0'$ y para todo $n \in N$ se cumple que $f(S(n)) = S'(f(n))$, que es la condición de conmutatividad para el diagrama. Sólo falta probar que f es biyectiva.

Para ello invertimos los papeles y definimos $f' : N' \longrightarrow N$ mediante el teorema de recursión aplicado al segundo sistema de Peano, de modo que $f'(0') = 0$ y para todo $n' \in N'$ se cumple que $f'(S'(n')) = S(f'(n'))$.

Ahora demostramos por inducción que $f'(f(n)) = n$ para todo $n \in N$. Para $n = 0$ tenemos que $f'(f(0)) = f'(0') = 0$. Si vale para n, entonces $f'(f(S(n))) = f'(S'(f(n))) = S(f'(f(n))) = S(n)$.

Esto prueba que $f \circ f'$ es la identidad en N, y el teorema 1.13 nos da que f es inyectiva. Pero invirtiendo los papeles obtenemos también que $f' \circ f$ es la identidad, luego f es suprayectiva, y concluimos que es biyectiva. ∎

A partir de aquí fijamos un sistema de Peano cualquiera $(\mathbb{N}, S, 0)$ y llamaremos *números naturales* a los elementos de $\mathbb{N}$.

Vamos a aplicar el teorema de recursión tomando como a un número natural $m \in \mathbb{N}$ y como g la aplicación sucesor $S : \mathbb{N} \longrightarrow \mathbb{N}$. El teorema nos da que existe una única $f_m : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $f_m(0) = m$ y $f_m(S(n)) = S(f_m(n))$. A su vez, esto nos permite definir una aplicación

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

mediante $+(m, n) = f_m(n)$. Si convenimos en adoptar la notación más habitual $m + n$ en lugar de $+(m, n)$, las propiedades que determinan por recurrencia la función f_m se escriben así:

$$m + 0 = m, \qquad m + S(n) = S(m + n).$$

En particular, observamos que $m+1 = m+S(0) = S(m+0) = S(m)$, por lo que a partir de ahora ya no volveremos a escribir $S(n)$ para referirnos al siguiente de un número natural, sino que usaremos la notación $m + 1$. Puesto que ésta será la notación que emplearemos en lo sucesivo, conviene reescribir en estos términos los resultados que hemos enunciado hasta ahora con la notación S:

Principio de inducción *Si probamos que* 0 *cumple una propiedad* $\phi(0)$ *y bajo la hipótesis de que* $n \in \mathbb{N}$ *cumple la propiedad* $\phi(n)$ *(hipótesis de inducción) podemos demostrar que también se cumple* $\phi(n+1)$*, entonces podemos asegurar que todo número natural cumple* $\phi(n)$*.*

Principio de recursión *Si* $g : A \longrightarrow A$ *es una aplicación arbitraria (sobre una clase* A*, no necesariamente un conjunto) y* $a \in A$*, existe una única aplicación* $f : \mathbb{N} \longrightarrow A$ *tal que* $f(0) = a$ *y para todo* $n \in \mathbb{N}$ *se cumple que* $f(n+1) = g(f(n))$

Suma de números naturales Llamamos *suma* de números naturales a la única aplicación $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ que, para cualquier par de números m, $n \in \mathbb{N}$, cumple las propiedades siguientes:

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

Esta definición se corresponde con la suma que el lector conoce sin duda desde sus primeros años. Por ejemplo:

$$2 + 3 = 2 + (2+1) = (2+2) + 1 = (2 + (1+1)) + 1 = ((2+1)+1) + 1$$
$$= (3+1) + 1 = 4 + 1 = 5.$$

Producto de números naturales Llamamos *producto* de números naturales a la única aplicación $\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ que, para todo m, $n \in \mathbb{N}$, cumple las propiedades siguientes:

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

Observemos que la definición de producto se basa en el teorema de recursión tomando $a = 0$ y como $g : \mathbb{N} \longrightarrow \mathbb{N}$ la aplicación dada por $g(n) = n + m$. Esto nos define una función g_m, pero en lugar de $g_m(n)$ escribimos $m \cdot n$, o simplemente mn. Como en el caso de la suma, este producto es el producto "de toda la vida". No obstante, antes de hacer cuentas con él es conveniente demostrar las propiedades básicas de estas operaciones:

1. $(m+n) + r = m + (n+r)$.

   Por inducción[2] sobre r. Para $r = 0$ se reduce a $m + n = m + n$. Si vale para r, entonces

   $$(m+n) + (r+1) = ((m+n)+r) + 1 = (m + (n+r)) + 1$$
   $$= m + ((n+r)+1) = m + (n + (r+1)),$$

   donde hemos aplicado la definición de suma, la hipótesis de inducción, y dos veces más la definición de suma.

[2]"Por inducción sobre r" significa que vamos a aplicar el principio de inducción a la propiedad $\phi(r) \equiv (m+n) + r = m + (n+r)$, considerando m y n fijos.

Esta propiedad nos permite escribir expresiones $m+n+r$ sin necesidad de intercalar paréntesis. Así, por ejemplo,

$$3+3=3+2+1=3+1+1+1=3+1+1=5+1=6.$$

2. $m+n=n+m$.

   Para probar esto demostramos antes algunos casos particulares. En primer lugar demostramos que $0+n=n$ por inducción sobre n (notemos que $n+0=n$ se cumple por la definición de suma). Para $n=0$ es $0+0=0$, Si vale para n, entonces

   $$0+(n+1)=(0+n)+1=n+1.$$

   En segundo lugar demostramos que $1+n=n+1$, también por inducción sobre n. Para $n=0$ es $1+0=1=0+1$, la primera igualdad por la definición de suma y la segunda porque ya hemos visto que sumar 1 equivale a pasar al siguiente. Si vale para n, entonces

   $$1+(n+1)=(1+n)+1=(n+1)+1.$$

   Ahora probamos el caso general por inducción sobre n. Para $n=0$ es $m+0=m=0+m$. Si vale para n, entonces

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

   donde hemos usado las propiedades precedentes.

3. $(m+n)r=mr+nr$.

   Por inducción sobre r. Para $r=0$ es $(m+n)0=0=0+0=m\cdot 0+n\cdot 0$. Si vale para r entonces

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

4. $m(n+r)=mn+mr$.

   Por inducción sobre r. Para $r=0$ es $mn=mn$. Si vale para n, entonces

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

5. $(mn)r=m(nr)$.

   Por inducción sobre r. Para $r=0$ es $(mn)0=0=m(0)=m(n0)$. Si vale para r, entonces

   $$(mn)(r+1)=(mn)r+mn=m(nr)+mn=m(nr+n)=m(n(r+1)),$$

   donde hemos usado la propiedad anterior.

   Como en el caso de la suma, esta propiedad hace innecesarios los paréntesis entre los términos de una multiplicación.

6. $n \cdot 1 = n$.

   $n \cdot 1 = n(0+1) = n \cdot 0 + n = 0 + n = n$.

7. $mn = nm$.

   Demostramos antes algunos casos particulares. En primer lugar vemos que $0 \cdot n = 0$. Para $n = 0$ es $0 \cdot 0 = 0$. Si vale para n, entonces

   $$0 \cdot (n+1) = 0 \cdot n + 0 = 0 + 0 = 0.$$

   En segundo lugar $1 \cdot n = n$. Para $n = 0$ es $1 \cdot 0 = 0$. Si vale para n, entonces $1(n+1) = 1 \cdot n + 1 \cdot 1 = n + 1$. Ahora probamos el caso general, por inducción sobre n. Para $n = 0$ es $m0 = 0 = 0m$. Si vale para n, entonces

   $$m(n+1) = mn + m = nm + m = nm + 1 \cdot m = (n+1)m,$$

   donde hemos usado la propiedad 3.

8. Si $m + r = n + r$, entonces $m = n$.

   Por inducción sobre r. Para $r = 0$ tenemos $m+0 = n+0$, luego ciertamente $m = n$. Si vale para r y tenemos $m + (r+1) = n + (r+1)$, esto es lo mismo que $(m+r)+1 = (n+r)+1$, o también $S(m+r) = S(n+r)$, luego por el cuarto axioma de Peano $m + r = n + r$, luego $m = n$ por hipótesis de inducción.

9. Si $m + n = 0$, entonces $m = n = 0$.

   En efecto, si fuera $n \neq 0$, entonces $n = r + 1$ para cierto r (teorema 2.3), y entonces $m + n = (m+r) + 1 \neq 0$, pues el 0 no es el siguiente de ningún número natural.

10. Si $mn = 0$, entonces $m = 0$ o bien $n = 0$.

    En caso contrario, $m = m' + 1$, $n = n' + 1$, luego, al igual que antes,

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

Ahora ya es fácil operar con números naturales. Por ejemplo,

$$3 \cdot 2 = 3(1+1) = 3 + 3 = 6.$$

Una nueva aplicación del teorema de recursión nos permite definir la exponenciación de números naturales:

Exponenciación de números naturales La *exponenciación* de dos números naturales es la única aplicación $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ determinada por las propiedades siguientes:

$$m^0 = 1, \qquad m^{n+1} = m^n \cdot m.$$

Dejamos como ejercicio demostrar sus propiedades básicas:

1. Si $n \neq 0$, entonces $0^n = 0$ (pero $0^0 = 1$, por definición).
2. $1^n = 1$.
3. $m^{n+r} = m^n \cdot m^r$.
4. $(m^n)^r = m^{nr}$.
5. $(mn)^r = m^r \cdot n^r$.

Ordenación de los números naturales Diremos que un número natural m es menor o igual que otro n, y lo representaremos por $m \leq n$, si existe un $r \in \mathbb{N}$ tal que $m + r = n$. Observemos que en tal caso dicho r es único por la propiedad 8 precedente, por lo que podemos llamarlo *resta* de n y m, y lo representaremos por $n - m$.

Notemos que $m \leq m$, porque $m + 0 = m$. Escribiremos $m < n$ para indicar que $m \leq n$ y $m \neq n$.

Por ejemplo, como $2 + 3 = 5$, se cumple que $2 < 5$ y que $5 - 2 = 3$.

Veamos ahora las propiedades correspondientes:

1. Para todo natural n se cumple que $0 \leq n$.

   En efecto, $0 + n = n$.

2. Si m y n son números naturales, entonces $m \leq n$ o bien $n \leq m$.

   Por inducción sobre n, si $n = 0$ se cumple $n = 0 \leq m$. Si vale para n, tenemos que $m \leq n$ o bien $n \leq m$. Si se da el primer caso, existe un r tal que $m + r = n$, luego $m + r + 1 = n + 1$, luego $m \leq n + 1$, como había que probar.

   Supongamos ahora que $n \leq m$ y sea r tal que $n + r = m$. Si $r = 0$ entonces $n = m$, luego $n + 1 = m + 1$, luego $m \leq n + 1$, como había que probar. Si $r \neq 0$, existe un r' tal que $r = r' + 1$, luego $n + r' + 1 = m$, luego $n + 1 \leq m$.

3. Si $m \leq n$ y $n \leq m$, entonces $m = n$.

   Tenemos que $m + r = n$ y $n + r' = m$, luego $m + r + r' = m = m + 0$, luego $r + r' = 0$, luego $r = r' = 0$, luego $m = n$.

4. Si $m \leq n$ y $n \leq r$, entonces $m \leq r$.

   Tenemos que $m + u = n$ y $n + v = r$, luego $m + u + v = r$, luego $m \leq r$.

5. Se cumple $m \leq n$ si y sólo si $m + r \leq n + r$.

   En efecto, $m \leq n$ equivale a que exista un u tal que $m + u = n$, lo cual equivale a que $m + r + u = n + r$, lo cual equivale a que $m + r \leq n + r$.

6. Si $r \neq 0$ y $mr = nr$, entonces $m = n$.

   En efecto, no perdemos generalidad si suponemos $m \leq n$, de modo que $n = m + u$, luego $nr = mr + ur$, luego $mr + 0 = mr + ur$, luego $ur = 0$, luego $u = 0$, luego $m = n$.

7. Si $r \neq 0$, entonces $m \leq n$ si y sólo si $mr \leq nr$.

   Si $m \leq n$, existe un u tal que $m + u = n$, luego $mr + ur = nr$, luego $mr \leq nr$. Recíprocamente, si $mr \leq nr$, entonces o bien $m \leq n$, como queremos probar, o bien $n \leq m$, en cuyo caso $nr \leq mr$ por la parte ya probada, luego $nr = mr$ por 3, luego $n = m$ por 6, luego $m \leq n$.

Notemos que, trivialmente, $n < S(n)$, luego la ordenación que acabamos de introducir se corresponde con la que resulta al ir generando los números naturales a partir del 0 mediante la operación "siguiente", es decir:

$$0 < 1 < 2 < 3 < 4 < \cdots$$

La relación de orden en $\mathbb{N}$ permite dar un significado preciso a algunas expresiones con "puntos suspensivos". Por ejemplo, para cada $n \in \mathbb{N}$ podemos definir

$$I_n = \{1, \ldots, n\}, \qquad I_n^* = \{0, \ldots, n-1\}$$

y esto hay que entenderlo como que $I_n = \{m \in \mathbb{N} \mid 1 \leq m \leq n\}$ (con lo que en particular $I_0 = \varnothing$) e igualmente $I_n^* = \{m \in \mathbb{N} \mid m < n\}$, que son definiciones válidas por especificación.

En este punto el lector debería estudiar —si no lo ha hecho ya— el apartado sobre "Relaciones de orden" de la sección 1.6. En los términos introducidos allí, la ordenación de $\mathbb{N}$ que acabamos de introducir puede expresarse en términos de una relación de orden total

$$\leq = \{(m, n) \in \mathbb{N} \mid m \leq n\}.$$

En particular tenemos definido el concepto de "mínimo" de un subconjunto de un conjunto ordenado. Por ejemplo, es fácil ver que, para todo número natural n, se cumple que

$$n + 1 = \text{mín}\{m \in \mathbb{N} \mid m > n\},$$

es decir, que el siguiente de n es el mínimo número natural mayor que n.

En efecto, es claro que $n < n + 1$, y sólo hay que ver que si $n < m$, entonces $n + 1 \leq m$. Tenemos que existe un $k \in \mathbb{N}$ tal que $n + k = m$, pero no puede ser $k = 0$, pues entonces sería $n = m$, luego $k = k' + 1$, luego $n + 1 + k' = m$, luego $n + 1 \leq m$.

La ordenación de los números naturales cumple una propiedad fundamental:

Teorema 2.6 (Principio de buena ordenación) *Todo subconjunto no vacío de* $\mathbb{N}$ *tiene un mínimo elemento.*

DEMOSTRACIÓN: Sea $X \subset \mathbb{N}$ un conjunto no vacío, de modo que existe un cierto $m \in X$. Consideremos el conjunto de sus cotas inferiores

$$A = \{c \in \mathbb{N} \mid \bigwedge n \in X\, c \leq n\}.$$

Claramente $0 \in A$, y $m+1 \notin A$, pues no es cierto que $m+1 \leq m$. Si fuera cierto que cuando $c \in A$ se cumple también $c+1 \in A$, el principio de inducción nos daría que $A = \mathbb{N}$, y hemos visto que eso es falso. Por lo tanto, tiene que existir un $c \in \mathbb{N}$ que cumpla $c \in A$, pero $c+1 \notin A$. En otras palabras, c es una cota inferior de X, pero $c+1$ no lo es. Lo segundo significa que existe un $n \in X$ tal que $n < c+1$, y lo primero implica que $c \leq n < c+1$ y, por la observación previa al teorema, esto implica que $c = n$, luego $c \in X$ es el mínimo de X. ∎

Los conjuntos totalmente ordenados con esta propiedad de que todo subconjunto no vacío tenga un mínimo elemento las estudiamos en el apartado "Clases bien ordenadas" de la sección 1.6, pero el lector puede posponer su estudio hasta el capítulo III, pues de momento no vamos a usar ningún hecho probado allí.

El principio de buena ordenación hace que si tenemos que existe un número natural que cumple una propiedad $\phi(n)$, podamos considerar "el mínimo número natural n que cumple $\phi(n)$", es decir, el mínimo elemento del conjunto no vacío $\{n \in \mathbb{N} \mid \phi(n)\}$, con lo que tenemos un número que, además de cumplir $\phi(n)$, cumple que ningún natural $m < n$ cumple $\phi(m)$. Veamos un ejemplo de este tipo de argumentación:

Teorema 2.7 (División euclídea) *Dados dos números naturales D y d, con $d \neq 0$, existen unos únicos c y r tales que $D = dc + r$ y $r < d$.*

DEMOSTRACIÓN: Como $d \neq 0$, tenemos que $1 \leq d$, luego $D \leq dD$. Así pues, D es un número natural x que cumple $D \leq dx$, luego podemos tomar el mínimo número natural x que cumple $D \leq dx$.

Si $D = dx$, entonces basta tomar $c = x$ y $r = 0$. Si, por el contrario, $D < dx$ entonces necesariamente $x \neq 0$, luego podemos considerar $c = x - 1 < x$. Por la minimalidad de x tiene que ser $dc < D < d(c+1) = dc + d$. Sea $r = D - dc$, de modo que $dc + r < dc + d$, luego $r < d$.

Con esto tenemos probado que existen c y r que cumplen lo pedido. Ahora tenemos que ver que son únicos. Si c_1, c_2, r_1, r_2 cumplieran lo requerido y $c_1 \neq c_2$, podemos suponer que $c_1 < c_2$. Entonces

$$D = dc_1 + r_1 < dc_1 + d = d(c_1+1) \leq dc_2 \leq dc_2 + r_2 = D,$$

contradicción. Por lo tanto, $c_1 = c_2$, y entonces $D = dc_1 + r_1 = dc_1 + r_2$, luego $r_1 = r_2$. ∎

En las condiciones del teorema anterior, se dice que c y r son, respectivamente, el *cociente* y el *resto* de la *división euclídea* del *dividendo* D entre el *divisor* d.

El proceso de tomar el menor número natural que cumple una propiedad puede usarse en una forma fuerte de razonamiento por reducción al absurdo

conocida como *"demostración por contraejemplo mínimo"*. Esto significa que si queremos probar que todo número natural cumple una propiedad $\phi(n)$, podemos suponer, por reducción al absurdo que existe un número natural que no cumple $\phi(n)$, y entonces tomar el mínimo número natural n que no cumple $\phi(n)$. Así, para llegar a un absurdo no sólo contamos con que n no cumple $\phi(n)$, sino también con que todos los números $m < n$ cumplen $\phi(m)$.

2.2 Conjuntos finitos

Ya estamos en condiciones de definir lo que es un conjunto finito y de asignar un cardinal o "número de elementos" a cada conjunto finito. Para ello necesitamos algunos resultados previos. Recordemos que hemos definido $I_n = \{1, \ldots, n\}$, donde hay que entender que $I_0 = \varnothing$.

La existencia de una aplicación inyectiva $f : A \longrightarrow B$ se traduce en que los objetos de A pueden emparejarse uno a uno con los de B, aunque pueden sobrar objetos en B (que no sobren equivale a que f sea suprayectiva y, por consiguiente, biyectiva). Por lo tanto, el teorema siguiente es intuitivamente obvio, aunque una prueba formal requiere distinguir algunos casos:

Teorema 2.8 *Para todo par de números naturales m y n, existe una aplicación inyectiva $f : I_m \longrightarrow I_n$ si y sólo si $m \leq n$.*

Demostración: Si $m \leq n$, es claro que $I_m \subset I_n$, por lo que la inclusión $i : I_m \longrightarrow I_n$ es una aplicación inyectiva.

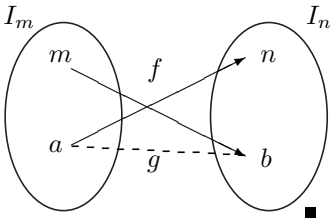
Falta probar que si $m > n$ no puede existir $f : I_m \longrightarrow I_n$ inyectiva. De no ser así, podemos tomar el menor número natural m para el que existe una aplicación $f : I_m \longrightarrow I_n$ inyectiva para cierto $n < m$.

El conjunto I_n tiene que contener las imágenes por f de los elementos de I_m, luego $I_n \neq \varnothing$, luego $n \neq 0$. A su vez esto implica que $m \neq 0$. Digamos que $m = m' + 1$ y que $n = n' + 1$.

Si n no tiene antiimagen por f, entonces $f|_{I_{m'}} : I_{m'} \longrightarrow I_{n'}$ inyectiva, y $n' < m'$, con lo que $m' < m$ cumple la misma propiedad que m, cuando se suponía que m era el mínimo que la cumplía, contradicción.

Supongamos pues que existe un $a \in I_m$ tal que $f(a) = n$. Si $a = m$, sigue siendo cierto que $f|_{I_{m'}} : I_{m'} \longrightarrow I_{n'}$ es inyectiva, pues al quitar m del dominio de la aplicación, ya no necesitamos a n en la imagen, y tenemos la misma contradicción.

Supongamos, por último, que $a < m$. Entonces $f(m) = b \in I_n$, con $b \neq n$, pues si fuera $b = n$ sería $f(m) = f(a)$, luego $m = a$. Por lo tanto $b \in I_{n'}$. Esto nos permite definir $g : I_{m'} \longrightarrow I_{n'}$ como la aplicación que coincide con f salvo que $f(a) = b$, que sigue siendo inyectiva y nos lleva a la misma contradicción.



■

En particular, si $\overline{\overline{I}}_m = \overline{\overline{I}}_n$, tenemos aplicaciones biyectivas (luego inyectivas) de uno en otro y viceversa, luego el teorema anterior nos da que $m = n$. Esto justifica la definición siguiente:

Definición 2.9 Un conjunto X es *finito* si existe un $n \in \mathbb{N}$ tal que $\overline{\overline{X}} = \overline{\overline{I}}_n$. En tal caso n es único y recibe el nombre de *cardinal* de X. Lo representaremos por $|X|$. Las clases que no son conjuntos finitos se llaman *infinitas.*

Así pues, si X es un conjunto infinito, la relación $\overline{\overline{X}} = \overline{\overline{I}}_n$ es equivalente a $|X| = n$, donde aquí tenemos una auténtica igualdad. En particular tenemos que $|I_n| = n$ y, más en particular, $|\varnothing| = 0$. De hecho, $\varnothing$ es el único conjunto de cardinal 0.

El cálculo del cardinal de un conjunto es lo que normalmente se llama "contar". Por ejemplo, un conjunto $A = \{a, b, c\}$, donde a, b y c son distintos dos a dos, cumple $|A| = 3$, porque podemos definir $f : I_3 \longrightarrow A$ biyectiva mediante $f(1) = a$, $f(2) = b$, $f(3) = c$.

El resultado fundamental sobre cardinales es el siguiente:

Teorema 2.10 *Dos conjuntos finitos son equipotentes si y sólo si tienen el mismo cardinal. Todo conjunto equipotente a un conjunto finito es finito.*

Demostración: Si X es un conjunto finito y $\overline{\overline{X}} = \overline{\overline{Y}}$, entonces existe un n tal que $\overline{\overline{I}}_n = \overline{\overline{X}} = \overline{\overline{Y}}$, luego $\overline{\overline{I}}_n = \overline{\overline{Y}}$, luego Y es finito y $|Y| = |X| = n$. Si $|X| = |Y| = n$, entonces $\overline{\overline{X}} = \overline{\overline{I}}_n = \overline{\overline{Y}}$, luego $\overline{\overline{X}} = \overline{\overline{Y}}$. ∎

Otro hecho básico es el siguiente:

Teorema 2.11 *Si X es un conjunto finito e $Y \subset X$, entonces Y es finito, $|Y| \leq |X|$ y se da la igualdad $|Y| = |X|$ si y sólo si $Y = X$.*

Demostración: Sea X un conjunto finito y supongamos que existe un $x \in X$. Sea $n = |X|$ y sea $f : I_n \longrightarrow X$ biyectiva. Notemos que $n \neq 0$, pues estamos suponiendo que $X \neq \varnothing$. Por lo tanto $n = n' + 1$.

Podemos suponer que $f(n) = x$, pues si la antiimagen de x es un $m < n$, podemos considerar la aplicación $g : I_n \longrightarrow X$ que coincide con f salvo que $g(n) = f(m)$ y $g(m) = f(n)$. Es fácil ver que g sigue siendo biyectiva, pero así se restringe a una biyección $I_{n'} \longrightarrow X \setminus \{x\}$. Por lo tanto, $X \setminus \{x\}$ es finito y $|X \setminus \{x\}| = |X| - 1$.

Pasemos ya a probar el enunciado, por inducción sobre $|X|$. Si $|X| = 0$ entonces $X = \varnothing$, luego necesariamente $Y = \varnothing$ y $|X| = |Y| = 0$.

Si vale para conjuntos de cardinal n y $|X| = n + 1$, distinguimos dos casos: si $Y = X$ entonces trivialmente Y es finito y tiene el mismo cardinal que X. En caso contrario existe un $x \in X \setminus Y$, con lo que $Y \subset X \setminus \{x\}$, que según hemos probado es un conjunto finito de cardinal n. Por la hipótesis de inducción Y es finito y $|Y| \leq |X \setminus \{x\}| = n < n + 1 = |X|$. ∎

Por ejemplo, ahora podemos probar:

Teorema 2.12 $\mathbb{N}$ *es infinito.*

DEMOSTRACIÓN: Si $\mathbb{N}$ fuera finito, tendría un cardinal $n \in \mathbb{N}$, pero eso es imposible, porque $I_{n+1} \subset \mathbb{N}$ y, según el teorema anterior, se cumpliría que $n+1 = |I_{n+1}| \leq |\mathbb{N}| = n$, contradicción. ∎

Para probar que un conjunto X tiene cardinal menor o igual que otro conjunto Y no hace falta que $X \subset Y$, sino que basta con que exista una aplicación inyectiva de X en Y. Más en general:

Teorema 2.13 *Sea $X \neq \varnothing$ un conjunto arbitrario e Y un conjunto finito. Las afirmaciones siguientes son equivalentes:*[3]

1. *X es finito y $|X| \leq |Y|$.*
2. *Existe una aplicación $f : X \longrightarrow Y$ inyectiva.*
3. *Existe una aplicación $g : Y \longrightarrow X$ suprayectiva.*

DEMOSTRACIÓN: $1 \Rightarrow 2$. Sea $|X| = n$, $|Y| = m$. Basta componer una biyección $X \longrightarrow I_n$ con la inclusión $I_n \longrightarrow I_m$ con una biyección $I_m \longrightarrow Y$. El resultado es una aplicación $f : X \longrightarrow Y$ inyectiva.

$2 \Rightarrow 1$. Tenemos que $f[X] \subset Y$, luego $f[X]$ es finito y $|f[X]| \leq |Y|$. Además $f : X \longrightarrow f[X]$ biyectiva, luego X es finito y $|X| = |f[X]| \leq |Y|$.

$2 \Rightarrow 3$. Fijemos $x_0 \in X$ y definimos $g : Y \longrightarrow X$ mediante

$$g(y) = \begin{cases} f^{-1}(y) & \text{si } y \in f[X], \\ x_0 & \text{si } y \in Y \setminus f[X]. \end{cases}$$

Es inmediato comprobar que g es suprayectiva, pues cada $x \in X$ tiene a $f(x)$ por antiimagen.

$3 \Rightarrow 2$. Sea $|Y| = n$ y fijemos una aplicación $h : I_n \longrightarrow Y$ biyectiva. Entonces $g' = h \circ g : I_n \longrightarrow X$ es suprayectiva. Sea $f' : X \longrightarrow I_n$ la aplicación dada por $f'(x) = \min g'^{-1}[x]$. Es fácil ver que es inyectiva, al igual que lo es $f = f' \circ h : X \longrightarrow Y$. ∎

Otro resultado notable sobre aplicaciones entre conjuntos finitos es el siguiente:

Teorema 2.14 *Sea $f : X \longrightarrow Y$ una aplicación entre dos conjuntos finitos del mismo cardinal. Entonces f es inyectiva si y sólo si f es suprayectiva si y sólo si f es biyectiva.*

[3]El hecho de que la negación de 1 implique la negación de 2 se conoce como "principio del palomar", pues se ilustra con este ejemplo: si en un palomar hay más palomos que nidos, tiene que haber al menos un nido con más de un palomo (porque la aplicación que a cada palomo le asigna su nido no puede ser inyectiva).

DEMOSTRACIÓN: Si f es inyectiva, entonces $f : X \longrightarrow f[X]$ biyectiva, luego $|f[X]| = |X| = |Y|$, luego $f[X] = Y$ por 2.11, luego f es suprayectiva.

Si f es suprayectiva pero no inyectiva, existen x, $x' \in X$ distintos tales que $f(x) = f(x')$, pero entonces $f|_{X\setminus\{x\}} : X \setminus \{x\} \longrightarrow Y$ sigue siendo suprayectiva, luego $|Y| \leq |X \setminus \{x\}| < |X| = |Y|$, contradicción. ∎

Hemos definido la suma de números naturales mediante una relación recurrente que la caracteriza. Ahora podemos demostrar que la suma se corresponde con la idea que todos tenemos de ella: $m+n$ es el número de cosas que tenemos cuando juntamos m cosas a otras n cosas.

Teorema 2.15 *Si X e Y son conjuntos finitos disjuntos, entonces $X \cup Y$ es finito, y $|X \cup Y| = |X| + |Y|$.*

DEMOSTRACIÓN: Sean $f : I_m \longrightarrow X$, $g : I_n \longrightarrow Y$ biyectivas. Entonces podemos definir $h : I_{m+n} \longrightarrow X \cup Y$ mediante

$$h(u) = \begin{cases} f(u) & \text{si } 1 \leq u \leq m, \\ g(u-m) & \text{si } m+1 \leq u \leq m+n. \end{cases}$$

Notemos que si $m+1 \leq u \leq m+n$, entonces $1 \leq u-m \leq n$, luego $u-m \in I_n$. Es fácil ver que h es biyectiva, luego $X \cup Y$ es finito y $|X \cup Y| = m+n = |X|+|Y|$. ∎

Ahora probamos un resultado más general:

Teorema 2.16 *Si X e Y son conjuntos finitos, entonces*

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

DEMOSTRACIÓN: Basta tener en cuenta que $X \cup Y = X \cup (Y \setminus (X \cap Y))$, donde X e $Y \setminus (X \cap Y)$ son disjuntos. Por el teorema anterior

$$|X \cup Y| = |X| + |Y \setminus (X \cap Y)|.$$

Por otra parte $Y = (X \cap Y) \cup (Y \setminus (X \cap Y))$ y los dos conjuntos son disjuntos, luego nuevamente por el teorema anterior

$$|Y| = |X \cap Y| + |Y \setminus (X \cap Y)|.$$

Por lo tanto $|Y \setminus (X \cap Y)| = |Y| - |X \cap Y|$, luego sustituyendo en la primera ecuación obtenemos la fórmula del enunciado. ∎

Ahora interpretamos el producto:

Teorema 2.17 *Si X e Y son conjuntos finitos, entonces $X \times Y$ es finito y $|X \times Y| = |X||Y|$.*

DEMOSTRACIÓN: Lo probamos por inducción sobre $|Y|$. Si $|Y| = 0$ entonces $Y = \varnothing$, y es claro que $X \times Y = \varnothing$, luego es finito y $|X \times Y| = 0 = |X||Y|$.

Si vale cuando $|Y| = n$ y suponemos que $|Y| = n + 1$, tomamos $y \in Y$, de modo que $|Y \setminus \{y\}| = n$, y por hipótesis de inducción $X \times (Y \setminus \{y\})$ es finito y $|X \times (Y \setminus \{y\})| = |X| \cdot n$. Ahora basta observar que

$$X \times Y = (X \times (Y \setminus \{y\}) \cup (X \times \{y\}),$$

que la unión es disjunta y que $\overline{\overline{X \times \{y\}}} = \overline{\overline{X}}$ (a través de la biyección $(x, y) \mapsto x$), luego $X \times \{y\}$ es finito y $|X \times \{y\}| = |X|$. Por el teorema 2.15 concluimos que $X \times Y$ es finito y que

$$|X \times Y| = |X| \cdot n + |X| = |X|(n + 1) = |X||Y|. \qquad \blacksquare$$

Vamos a contar algunos conjuntos más. Observemos que si $f : A \longrightarrow B$ entonces $f \subset A \times B$, luego $f \in \mathcal{P}(A \times B)$. Por lo tanto, si definimos, por especificación,

$$B^A = \{f \in \mathcal{P}(A \times B) \mid f : A \longrightarrow B\},$$

entonces B^A es el conjunto de todas las aplicaciones de A en B. El que se represente con esa notación se debe al teorema siguiente:

Teorema 2.18 *Si A y B son conjuntos finitos, entonces B^A es un conjunto finito y $|B^A| = |B|^{|A|}$.*

DEMOSTRACIÓN: Por inducción sobre $|A|$. Si $|A| = 0$, entonces $A = \varnothing$, y "técnicamente" existe una aplicación de A en B, porque $\varnothing : \varnothing \longrightarrow B$ es cierto, si nos ajustamos a la definición de aplicación. Por lo tanto $B^A = \{\varnothing\}$ y es un conjunto finito de cardinal $|B^A| = 1 = |B|^0 = |B|^{|A|}$.

Supongamos que el resultado es cierto cuando $|A| = n$ y supongamos que $|A| = n + 1$. Sea $a \in A$ y sea $A' = A \setminus \{a\}$, que es un conjunto finito de cardinal n. Por hipótesis de inducción $B^{A'}$ es finito y $|B^{A'}| = |B|^n$.

Definimos $f : B^A \longrightarrow B^{A'} \times B$ mediante $f(g) = (g|_{A'}, g(a))$. Es fácil ver que f es biyectiva. Por lo tanto $\overline{\overline{B^A}} = \overline{\overline{B^{A'} \times B}}$, y el teorema anterior nos da que B^A es finito y $|B^A| = |B^{A'}||B| = |B|^n|B| = |B|^{n+1} = |B|^{|A|}$. $\blacksquare$

Teorema 2.19 *Si X es un conjunto finito, $\mathcal{P}X$ es finito y $|\mathcal{P}X| = 2^{|X|}$.*

DEMOSTRACIÓN: Basta observar que $f : \{0, 1\}^X \longrightarrow \mathcal{P}X$ definida por $f(g) = g^{-1}[1]$ es biyectiva, y luego aplicar el teorema anterior. $\blacksquare$

He aquí otra propiedad importante de los conjuntos finitos:

Teorema 2.20 *Si X es un conjunto finito parcialmente ordenado no vacío, entonces tiene al menos un elemento maximal y un elemento minimal. Por consiguiente, todo conjunto finito totalmente ordenado tiene máximo y mínimo elemento, luego todo conjunto finito totalmente ordenado está bien ordenado.*

DEMOSTRACIÓN: Por inducción sobre $|X|$. Suponemos que el resultado es cierto cuando $|X| < n$ y suponemos que $|X| = n$. Tomamos $u \in X$. Si es minimal, no hay nada que probar. En caso contrario, consideramos el conjunto $Y = \{v \in X \mid v < u\}$, que es finito, no vacío y $|Y| < |X|$, luego tiene un elemento minimal v, que claramente es minimal de X. Igualmente se prueba la existencia de maximales.

La parte para conjuntos totalmente ordenados es inmediata (pues en un conjunto totalmente ordenado todo minimal es un mínimo y todo maximal es un máximo) y, por consiguiente, si X es un conjunto finito totalmente ordenado está bien ordenado, ya que todo subconjunto de X no vacío es también un conjunto finito totalmente ordenado, luego tiene mínimo. ∎

Notemos que hemos probado algo ligeramente más fuerte: todo elemento u de un conjunto finito parcialmente ordenado está por encima de un minimal y por debajo de un maximal.

En la sección siguiente usaremos este teorema:

Teorema 2.21 *Si $(J, \leq)$ es un conjunto finito totalmente ordenado y $|J| = k$, existe una única semejanza $f : (I_k^*, \leq) \longrightarrow (J, \leq)$.*

DEMOSTRACIÓN: Por inducción sobre k. Si $k = 0$ es que $J = \varnothing = I_0^*$, y la conclusión es trivial. Si vale para k y $|J| = k + 1$, sea m el máximo de J, que existe por el teorema anterior. Aplicamos la hipótesis de inducción a $J \setminus \{m\}$, con lo que existe una única semejanza $f : I_k^* \longrightarrow J \setminus \{m\}$, la cual se extiende claramente a una semejanza $f' : I_{k+1}^* \longrightarrow J$ sin más que definir $f^*(k) = m$.

Si tenemos dos semejanzas $f, g : I_{k+1}^* \longrightarrow J$, necesariamente se cumple que $f(k) = m = g(k)$, pues k es el máximo de I_{k+1}^*, luego $f|_{I_k^*}, g|_{I_k^*} : I_k^* \longrightarrow J \setminus \{m\}$ son también semejanzas y, por hipótesis de inducción, son iguales, luego también se cumple que $f = g$. ∎

Esto significa que J puede numerarse en la forma $x_0 < x_1 < \cdots < x_{k-1}$, es decir, de modo que la relación de orden en los índices se corresponda con la relación de orden dada en J.

2.3 Sumas finitas

Consideremos una clase A (no necesariamente un conjunto) en la que hay definida una ley de composición interna[4] $+ : A \times A \longrightarrow A$ con neutro 0.

Para cada sucesión[5] $\{a_i\}_{i<n}$ en A, con $n \in \mathbb{N}$, consideramos la única aplicación $I_n^* \cup \{n\} \longrightarrow A$ que cumple

$$\sum_{i<0} a_i = 0, \qquad \sum_{i<k+1} a_i = \sum_{i<k} a_i + a_k.$$

En particular, así queda definida la suma $\sum_{i<n} a_i \in A$.

[4] Véase la definición 1.32 de la sección 1.7. En esta sección no necesitaremos nada más.

[5] Esto significa simplemente que $a : I_n^* \longrightarrow A$, donde $I_n^* = \{0, \ldots, n-1\}$.

Más en general, si $(J, \leq)$ es un conjunto finito totalmente ordenado y tenemos una sucesión $\{a_i\}_{i\in J}$ en A, por el teorema 2.21 existe una única semejanza $s : I_k^* \longrightarrow J$ (por simplicidad omitimos la referencia a las relaciones de orden) y podemos considerar la sucesión $\{a_{s(j)}\}_{j<k}$. Definimos

$$\sum_{i\in J} a_i = \sum_{j<k} a_{s(i)}.$$

Es fácil ver que si $J = \varnothing$, entonces $\sum_{i\in J} a_i = 0$, y si $J = J' \cup \{m\}$, donde, m es el máximo de J, entonces

$$\sum_{i\in J} a_i = \sum_{i\in J'} a_i + a_m.$$

A partir de aquí suponemos que la operación $+$ es asociativa, es decir, que cumple $(a + b) + c = a + (b + c)$ para todos los elementos a, b, $c \in A$.

Observemos que si partimos $J = J_1 \cup J_2$ de modo que todo elemento de J_1 es menor que todo elemento de J_2, entonces

$$\sum_{i\in J} a_i = \sum_{i\in J_1} a_i + \sum_{i\in J_2} a_i.$$

En efecto, razonamos por inducción sobre el cardinal de J_2. Si es 0 es que $J_2 = \varnothing$ e $J = J_1$, con lo que la igualdad es trivial. Supuesto cierto cuando J_2 tiene cardinal k, supongamos que su cardinal es $k + 1$. Entonces J_2 tiene un máximo elemento m, que será también el máximo de J. Sea $J_2' = J_2 \setminus \{m\}$. Entonces (y aquí usamos la asociatividad de $+$):

$$\sum_{i\in J} a_i = \sum_{i\in J_1\cup J_2'} a_i + a_m = \sum_{i\in J_1} a_i + \sum_{i\in J_2'} a_i + a_m = \sum_{i\in J_1} a_i + \sum_{i\in J_2} a_i.$$

A su vez podemos probar la generalización siguiente:

Teorema 2.22 (Propiedad asociativa generalizada) *Sea A una clase en la que hay definida una operación $+$ asociativa y con elemento neutro. Sea J un conjunto finito totalmente ordenado descompuesto como $J = \bigcup_{i<k} J_i$, de modo que si $i < j < k$, todo elemento de J_i es menor que todo elemento de J_j, y sea $\{a_i\}_{i\in J}$ una sucesión en A. Entonces,*

$$\sum_{j\in J} a_j = \sum_{i<k} \sum_{j\in J_i} a_j.$$

Demostración: Razonamos por inducción sobre $m \leq k$ que

$$\sum_{j\in \bigcup_{i<m} J_i} a_j = \sum_{i<m} \sum_{j\in J_i} a_j.$$

Para $m = 0$ ambos términos valen 0. Si vale para m, entonces, como $\bigcup_{i<m+1} J_i = \bigcup_{i<m} J_i \cup J_m$ está en las hipótesis del caso considerado antes del enunciado, tenemos que

$$\sum_{j\in \bigcup_{i<m+1} J_i} a_j = \sum_{j\in \bigcup_{i<m} J_i} a_j + \sum_{j\in J_m} a_j = \sum_{i<m} \sum_{j\in J_i} a_j + \sum_{j\in J_m} a_j = \sum_{i<m+1} \sum_{j\in J_i} a_j. \qquad \blacksquare$$

En la práctica, si $J = \{i \mid m \leq i \leq n\}$, usaremos las notaciones alternativas

$$a_m + \cdots + a_n \equiv \sum_{i=m}^{n} a_i \equiv \sum_{i \in J} a_i.$$

En estos términos, por ejemplo, hemos probado que si $m \leq k < n$, se cumple

$$a_m + \cdots + a_n = (a_m + \cdots + a_k) + (a_{k+1} + \cdots + a_n).$$

Las sumas finitas que acabamos de definir verifican una serie de propiedades que generalizan de forma obvia las propiedades de las sumas de dos sumandos y que se demuestran mediante inducciones rutinarias. No vamos a entrar en ello, sino que usaremos estas propiedades según vayan siendo necesarias sin más advertencia.

Hasta aquí hemos considerado sumatorios sobre conjuntos ordenados de índices porque la suma puede depender del orden de los sumandos, pero esto no es así si suponemos además que la suma es conmutativa, es decir, que cumple la relación $a+b = b+a$ para todo $a, b \in A$. En tal caso la ordenación del conjunto de índices es irrelevante, como se deduce del teorema siguiente:

Teorema 2.23 *Sea A una clase y $+$ una operación en A asociativa, conmutativa y con elemento neutro 0. Sea $\sigma : I_n^* \longrightarrow I_n^*$ biyectiva y sea $\{a_i\}_{i<n}$ una sucesión finita en A. Entonces*

$$\sum_{i<n} a_i = \sum_{i<n} a_{\sigma(i)}.$$

Demostración: Lo probamos por inducción sobre n. Si $n = 0$, por definición ambos términos son 0. Si vale para n, consideramos una sucesión $\{a_i\}_{i<n+1}$ en A y una biyección $\sigma : I_{n+1}^* \longrightarrow I_{n+1}^*$. Si $\sigma(n) = n$, entonces, aplicando la hipótesis de inducción a $\sigma|_{I_n^*} : I_n^* \longrightarrow I_n^*$, vemos que

$$\sum_{i<n+1} a_i = \sum_{i<n} a_i + a_n = \sum_{i<n} a_{\sigma(i)} + a_{\sigma(n)} = \sum_{i<n+1} a_{\sigma(i)}.$$

Supongamos ahora que $\sigma(n) = k < n$. Entonces, por la asociatividad generalizada tenemos que

$$\sum_{i<n+1} a_i = \sum_{i=0}^{k-1} a_i + a_k + \sum_{i=k+1}^{n} a_i = \sum_{i \in I} a_i + a_k,$$

donde $I = (n+1) \setminus \{k\}$. Sea $s : I_n^* \longrightarrow I$ la semejanza, que no es sino

$$s(i) = \begin{cases} i & \text{si } i < k, \\ i+1 & \text{si } k \leq i, \end{cases}$$

y sea $\tau : I_n^* \longrightarrow I_n^*$ la biyección dada por

$$\tau(i) = \begin{cases} \sigma(i) & \text{si } \sigma(i) < k, \\ \sigma(i) - 1 & \text{si } \sigma(i) > k. \end{cases}$$

Entonces, aplicando a τ la hipótesis de inducción,

$$\sum_{i<n+1} a_i = \sum_{i\in I} a_i + a_k = \sum_{i<n} a_{s(i)} + a_{\sigma(n)} =$$

$$\sum_{i<n} a_{s(\tau(i))} + a_{\sigma(n)} = \sum_{i<n} a_{\sigma(i)} + a_{\sigma(n)} = \sum_{i<n+1} a_{\sigma(i)}.$$

■

De este modo, si J es un conjunto finito cualquiera, $\{a_i\}_{i\in J}$ es una sucesión en A y en A tenemos definida una operación en las condiciones del teorema anterior, podemos definir

$$\sum_{i\in J} a_i = \sum_{j<n} a_{s(j)},$$

donde $s : I_n^* \longrightarrow J$ es cualquier biyección. El resultado no depende de la biyección elegida porque si $t : I_n^* \longrightarrow J$ es otra biyección, podemos aplicar el teorema anterior a $\sigma = t \circ s^{-1} : I_n^* \longrightarrow I_n^*$, lo que nos da la igualdad

$$\sum_{j<n} a_{s(j)} = \sum_{j<n} a_{t(j)}.$$

Notemos que una suma de la forma $\sum_{i\in J} a_i$ para cierta ordenación del conjunto J coincide con la que acabamos de definir, pues siempre podemos tomar como biyección $s : I_n^* \longrightarrow J$ la semejanza que define la suma ordenada.

Ahora podemos expresar la propiedad asociativa generalizada bajo hipótesis más generales que en 2.22:

Teorema 2.24 (Propiedad asociativa generalizada) *Sea A una clase en la que hay definida una operación $+$ asociativa, conmutativa y con elemento neutro. Sea $\{J_i\}_{i<k}$ una familia de conjuntos finitos disjuntos dos a dos, sea $J = \bigcup_{i<k} J_i$ y sea $\{a_i\}_{i\in J}$ una sucesión en A. Entonces,*

$$\sum_{j\in J} a_j = \sum_{i<k} \sum_{j\in J_i} a_j.$$

Demostración: Basta observar que podemos ordenar J de modo que la familia $\{J_i\}_{i<k}$ cumpla las condiciones del teorema 2.22. ■

Veamos una aplicación de estas sumas finitas:

Teorema 2.25 *Si $k > 1$ es un número natural, para cada $m \in \mathbb{N}$ no nulo existe una única sucesión $\{c_i\}_{i\leq n}$ de números menores que k tal que $c_n \neq 0$ y*

$$m = \sum_{i=0}^{n} c_i k^i.$$

Demostración: Como $k > 1$, es fácil ver por inducción sobre m que se cumple $m \leq k^m < k^{m+1}$, luego hay un mínimo $n^* \leq m+1$ tal que $m < k^{n^*}$. No puede ser $n^* = 0$, pues entonces sería $m = 0$, luego $n^* = n+1$ y se cumple $k^n \leq m < k^{n+1}$. Observemos que la unicidad de n^* implica la de n, es decir, hemos probado que para todo natural $m > 0$ existe un único natural n tal que $k^n \leq m < k^{n+1}$. Llamaremos $o(m)$ a este único n.

Si dividimos $m = k^n c + m'$, con $m' < k^n$, tiene que ser $c < k$, ya que si fuera $c \geq k$, tendríamos $m \geq k^n k = k^{n+1}$. Además $c > 0$, o de lo contrario $m = m' < k^n$. Así pues, todo número natural $m > 0$ puede expresarse en la forma

$$m = ck^n + m', \qquad 0 < c < k, \qquad m' < k^n \leq m.$$

Observemos que esta expresión es única, pues necesariamente $n = o(m)$ (ya que $m < (k-1)k^n + k^n = kk^n = k^{n+1}$) y entonces c y m' están unívocamente determinados como cociente y resto de la división euclídea. Vamos a probar que todo natural m no nulo admite una descomposición como la que indica el enunciado con $n = o(m)$.

Razonamos por inducción sobre m. Supuesto cierto para todo $m' < m$, consideramos la expresión $m = ck^n + m'$. Si $m' = 0$ entonces $m = ck^n$ ya tiene la forma deseada. En caso contrario, por hipótesis de inducción

$$m' = \sum_{i=0}^{n'} c_i k^i,$$

donde $n' = o(m') < n$ (porque $m' < k^n$) y, definiendo $c_i = 0$ para $n' < i < n$ y $c_n = c$, tenemos que

$$m = \sum_{i=0}^{n'} c_i k^i + \sum_{i=n'+1}^{n-1} c_i k^i + c_n k^n = \sum_{i=0}^{n} c_i k^i.$$

Para probar la unicidad observamos que

$$k^n \leq \sum_{i=0}^{n} c_i k^i < k^{n+1}.$$

En efecto, la primera desigualdad se sigue de que $c_n \neq 0$ separando el último sumando, y la segunda se prueba por inducción sobre n. Si vale para n, entonces

$$\sum_{i=0}^{n+1} c_i k^i = \sum_{i=0}^{n} c_i k^i + c_{n+1} k^{n+1} < k^{n+1} + (k-1)k^{n+1} = k^{n+2}.$$

Por lo tanto, razonando por inducción sobre m, si tenemos dos descomposiciones

$$m = \sum_{i=0}^{n} c_i k^i = \sum_{i=0}^{n'} c'_i k^i$$

en las condiciones del enunciado, necesariamente $n = n' = o(n)$, con lo que, por la unicidad de la descomposición

$$c_n k^n + \sum_{i=0}^{n-1} c_i k^i = c'_n k^n + \sum_{i=0}^{n-1} c'_i k^i$$

(notemos que hemos probado que los segundos sumandos son $< k^n$), tenemos que $c_n = c'_n$ y

$$\sum_{i=0}^{n-1} c_i k^i = \sum_{i=0}^{n-1} c'_i k^i.$$

Llamamos $\bar{n}$ y $\bar{n}'$ a los máximos naturales tales que $c_{\bar{n}} \neq 0$ y $c'_{\bar{n}'} \neq 0$, respectivamente, de modo que

$$\sum_{i=0}^{\bar{n}} c_i k^i = \sum_{i=0}^{\bar{n}'} c'_i k^i.$$

Por hipótesis de inducción $\bar{n} = \bar{n}'$ y $c_i = c'_i$ para todo $i < \bar{n}$, lo que implica que las dos sucesiones $\{c_i\}_{i\leq n}$ y $\{c'_i\}_{i\leq n}$ son iguales. ∎

Definición 2.26 La sucesión $\{c_i\}_{i\leq n}$ dada por el teorema anterior se llama *representación en base k* del número m. Es habitual usar la notación

$$c_n \cdots c_{0(k)} \equiv \sum_{i=0}^{n} c_i k^i,$$

de modo que, por ejemplo, $k = 0 \cdot k^0 + 1 \cdot k = 10_{(k)}$.

Cuando no se especifica la base se entiende que es $k = 9'$, de modo que la notación usual para $9'$ es 10 y, en general,

$$c_n \cdots c_0 \equiv \sum_{i=0}^{n} c_i 10^i.$$

De este modo, todo número natural tiene un nombre canónico en términos de las diez cifras $0, \ldots, 9$, aunque la elección del número 10 es puramente arbitraria. En principio, la menor base admisible es $k = 2$, de modo que, por ejemplo, es fácil ver que $10 = 2 + 2^3 = 1010_{(2)}$. Por lo tanto, todo número natural admite un nombre canónico en términos únicamente de las cifras 0 y 1.

2.4 Conjuntos numerables

Los conjuntos finitos son los que se pueden contar mediante los números naturales, pero apurando este concepto de "contar" podemos extenderlo a algunos conjuntos infinitos:

Definición 2.27 Un conjunto A es *numerable* si es finito[6] o bien existe una biyección $f : \mathbb{N} \longrightarrow A$.

En otros términos, un conjunto A es infinito numerable si sus elementos se pueden organizar como una sucesión infinita

$$a_0, \quad a_1, \quad a_2, \quad a_3, \quad a_4, \quad \ldots$$

sin repeticiones o, dicho de otro modo, los conjuntos infinitos numerables son los que se pueden "contar" a expensas de agotar los números naturales en el proceso de cómputo. En contra de lo que se podría conjeturar, no todos los conjuntos infinitos son numerables. Esto fue uno de los grandes hallazgos de Cantor. Por ejemplo, (suponiendo AP) el teorema 1.25 que lleva su nombre prueba que $\mathcal{P}\mathbb{N}$ es un conjunto no numerable.

[6] No es infrecuente que se defina un conjunto numerable como un conjunto biyectable con $\mathbb{N}$ (excluyendo así los conjuntos finitos). Según la definición que estamos adoptando, tales conjuntos serán para nosotros los conjuntos *infinitos numerables*.

Todos los resultados que vamos a ver aquí sobre conjuntos numerables son casos particulares de teoremas más generales que probaremos en el capítulo V. Por ello, aquí nos limitaremos a demostrar los que conviene tener disponibles durante la construcción del sistema numérico.

Es evidente que todo conjunto biyectable con un conjunto numerable es numerable. Más aún:

Teorema 2.28 *Si $f : A \longrightarrow B$ es inyectiva y B es numerable, entonces A es numerable.*

DEMOSTRACIÓN: El teorema 2.11 nos da la conclusión cuando B es finito. Supongamos, pues que B es infinito. Si A es finito no hay nada que probar, así que supongamos también que es infinito. Sea $g : \mathbb{N} \longrightarrow B$ biyectiva, de modo que $h = f \circ g^{-1} : A \longrightarrow \mathbb{N}$ es inyectiva. Como $h : A \longrightarrow h[A]$ es biyectiva, tenemos que $h[A]$ es infinito, y basta probar que es numerable. Equivalentemente, podemos suponer que $A \subset \mathbb{N}$, es decir, sólo hay que probar que todo subconjunto infinito de $\mathbb{N}$ es numerable.

Definimos recurrentemente una aplicación $k : \mathbb{N} \longrightarrow A$: suponiendo definidos $k(0), \ldots, k(n-1)$, tomamos

$$k(n) = \text{mín}(A \setminus \{k(0), \ldots, k(n-1)\}).$$

Notemos que la definición es correcta, porque $\{k(0), \ldots, k(n)\} \subset A$ es un conjunto finito y, como A es infinito, tenemos que $A \setminus \{k(0), \ldots, k(n-1)\} \neq \varnothing$, luego tiene un mínimo elemento, que es el que tomamos como $k(n)$.

En particular, si $m < n$, tenemos que $k(m) \neq k(n)$, pues se cumple que $k(m) \in \{k(0), \ldots, k(n-1)\}$. Esto prueba que k es inyectiva. Veamos que también es suprayectiva. Si existe un $a \in A$ que no tiene antiimagen, podemos tomar el mínimo de ellos. Consideremos $I = \{n \in \mathbb{N} \mid k(n) < a\}$. Entonces $k|_I : I \longrightarrow \{0, \ldots, a-1\}$ biyectiva, luego I es un subconjunto finito de $\mathbb{N}$, y esto implica que tiene un máximo elemento n. Pero entonces tiene que ser $k(n+1) = a$, porque ciertamente a es el mínimo del conjunto $\mathbb{N} \setminus \{k(0), \ldots, k(n)\}$, ya que todo número $m < a$ es de la forma $k(i)$ con $i \in I$, luego $i \leq n$, luego $m \in \{k(0), \ldots, k(n)\}$, y así tenemos una contradicción. ∎

En particular, todo subconjunto de un conjunto numerable es numerable. Veamos una variante del teorema anterior:

Teorema 2.29 *Si $f : A \longrightarrow B$ es suprayectiva y A es numerable, entonces B es numerable y $|B| \leq |A|$.*

DEMOSTRACIÓN: Sea $g : \mathbb{N} \longrightarrow A$ biyectiva, de modo que $g \circ f : \mathbb{N} \longrightarrow B$ es también suprayectiva. Equivalentemente, podemos suponer que $A = \mathbb{N}$. Pero entonces podemos definir $h : B \longrightarrow \mathbb{N}$ inyectiva mediante $h(a) = \text{mín}\, f^{-1}[a]$, y basta aplicar el teorema anterior. ∎

Otra consecuencia inmediata del teorema 2.28 es que un conjunto A es numerable (finito o infinito) si y sólo si existe $f : A \longrightarrow \mathbb{N}$ inyectiva.

A continuación vamos a demostrar que $\mathbb{N} \times \mathbb{N}$ es numerable. La idea subyacente a la prueba se muestra en la tabla siguiente:

$\vdots$						
4	10					
3	6	11				
2	3	7	12			
1	1	4	8	13		
0	0	2	5	9	14	
	0	1	2	3	4	$\cdots$

En ella vamos disponiendo los números naturales completando diagonales: en la primera diagonal ponemos el 0, en la diagonal siguiente el 1 y el 2, en la siguiente el 3, el 4 y el 5, y así sucesivamente. Entonces a cada par ordenado de números naturales le corresponde el número natural que ponemos en su fila y su columna. Por ejemplo, $f(3,1) = 13$. Esto determina una biyección $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$. En realidad f admite una definición algebraica muy simple:

$$f(x,y) = \frac{(x+y)(x+y+1)}{2} + x.$$

La idea para llegar a esta expresión también es sencilla: por ejemplo, la imagen $f(3,1) = 13$ está en la diagonal formada por los pares cuyas componentes suman $x + y = 4$. Para llegar a ella ha que pasar antes por las diagonales anteriores, que contienen $1+2+3+4 = 10$ números, pero como empezamos en el 0 resulta que el $f(0,4) = 10$ es ya ya el primero de dicha diagonal. Para llegar a $f(3,1)$ hemos de avanzar $x = 3$ posiciones. En general, el par $f(x,y)$ se alcanza en la posición

$$1 + 2 + \cdots + (x+y) + x = \frac{(x+y)(x+y+1)}{2} + x.$$

Vamos a dar una justificación puramente aritmética de estos hechos. Para ello observamos que la función

$$g(n) = \frac{n(n+1)}{2}$$

cumple $n \leq g(n)$, pues esto equivale a que $2n \leq n^2 + n$, o a que $n \leq n^2$, lo cual se cumple si $n = 0$ y, en caso contrario equivale a $1 \leq n$, que también se cumple.

Por lo tanto, para cada natural z existe un mínimo n' tal que $z < g(n')$. No puede ser $n' = 0$, luego existe un único $n = n' - 1$ tal que $g(n) \leq z < g(n+1)$. Ahora bien,

$$g(n+1) - g(n) = \frac{(n+1)(n+2) - n(n+1)}{2} = \frac{(n+1)2}{2} = n + 1,$$

luego existe un único número natural $0 \leq x \leq n$ tal que $z = g(n) + x$. Llamando $y = n - x$ tenemos que $z = g(x+y) + x = f(x,y)$. Esto prueba que f es suprayectiva.

La inyectividad se debe a que si $f(x,y) = f(x',y')$, entonces, llamando $n = x+y$ y $n' = x'+y'$ tenemos que $g(n) \leq z < g(n+1)$ y $g(n') \leq z < g(n'+1)$, lo cual sólo es posible si $n = n'$, luego

$$f(x,y) = g(n) + x = g(n) + x',$$

de donde $x = x'$ y, por consiguiente, de $x + y = x' + y'$ obtenemos que $y = y'$.

Más en general, ahora podemos probar:

Teorema 2.30 *Si A y B son conjuntos numerables, entonces el producto cartesiano $A \times B$ es numerable.*

DEMOSTRACIÓN: Sean $g_1 : A \longrightarrow \mathbb{N}$ y $g_2 : B \longrightarrow \mathbb{N}$ inyectivas. Entonces la función $g : A \times B \longrightarrow \mathbb{N} \times \mathbb{N}$ dada por $g(a,b) = (g_1(a), g_2(b))$ es inyectiva, y su composición con la biyección $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ que hemos construido es una aplicación $A \times B \longrightarrow \mathbb{N}$ inyectiva, luego $A \times B$ es numerable. ∎

Es claro que si uno de los dos conjuntos es infinito numerable y el otro es no vacío (finito o infinito), entonces $A \times B$ es infinito numerable.

2.5 Los números enteros

En esta sección construiremos los números enteros. Para ello será necesario el apartado "Relaciones de equivalencia" de la sección 1.6, así como el apartado "Anillos y cuerpos" de la sección 1.7.

En el conjunto $\mathbb{N}$ de los números naturales tenemos definidas una suma y un producto, pero no forman un anillo, principalmente porque ningún número natural (salvo el cero) tiene un opuesto para la suma. El conjunto $\mathbb{Z}$ de los números enteros surge de forma natural como la menor extensión posible de $\mathbb{N}$ que es un anillo.

La idea básica es que queremos que en $\mathbb{Z}$ haya números suficientes para calcular la resta $m - n$ de cualquier par de números naturales m y n. Una primera aproximación al problema sería definir $\mathbb{Z} = \mathbb{N} \times \mathbb{N}$ y definir una suma y un producto de forma que el par (m,n) acabara siendo "el resultado de restar $m - n$". Ahora bien, este intento tiene un fallo, y es que es fácil convencerse de que, por ejemplo, la resta $5 - 7$ debería dar lo mismo que la resta $1 - 3$ (igual que $7 - 5 = 3 - 1$). En general, debe cumplirse

$$a - b = c - d \leftrightarrow a + d = b + c,$$

donde la resta del miembro izquierdo es una operación que todavía no tenemos definida, mientras que la suma del miembro derecho es simplemente la suma de números naturales. Eliminando la operación no definida, lo que queremos es que el número asociado al par (a,b) sea el mismo que el asociado al par (c,d) si y sólo si $a + d = b + c$. La forma típica de conseguir esto es formar un conjunto cociente:

Definición 2.31 Definimos en $\mathbb{N}\times\mathbb{N}$ la relación R dada por

$$(a,b)\,R\,(c,d) \leftrightarrow a+d=b+c.$$

Es fácil probar que se trata de una relación de equivalencia. Llamaremos $[a,b]$ a la clase de equivalencia del par (a,b).

Llamaremos conjunto de los *números enteros* al cociente $\mathbb{Z}=(\mathbb{N}\times\mathbb{N})/R$. La letra Z es por el alemán *Zahl* (número).

Ahora podemos afirmar con rigor que

$$[a,b]=[c,d] \leftrightarrow a+d=b+c.$$

Definimos en $\mathbb{Z}$ la suma y el producto dados por:

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

Notemos que son las operaciones "obligadas" por la idea de que $[a,b]$ debe ser la resta $a-b$:

$$(a-b)+(c-d)=(a+c)-(b+d), \quad (a-b)(c-d)=(ac+bd)-(ad+bc).$$

Para que estas definiciones sean correctas debemos comprobar que no dependen de los representantes elegidos en las clases, es decir, que si $[a,b]=[a',b']$ y $[c,d]=[c',d']$, entonces

$$[a+c,b+d]=[a'+c',b'+d'] \quad \text{y} \quad [ac+bd,ad+bc]=[a'c'+b'd',a'd'+b'c'].$$

Esto se comprueba sin dificultad a partir de las definiciones. A partir de ahí es una pura rutina comprobar que $\mathbb{Z}$ con la suma y el producto así definido es un anillo conmutativo y unitario. El elemento neutro para la suma es $0=[0,0]$, y el simétrico de un número $[a,b]$ es $-[a,b]=[b,a]$, pues

$$[a,b]+[b,a]=[a+b,a+b]=[0,0].$$

Para cada $n\in\mathbb{N}$, definimos $+n\equiv[n,0]$. Observamos que

$$+m=+n \leftrightarrow m=n, \quad +m+(+n)=+(m+n), \quad (+m)(+n)=+(mn).$$

La aplicación $i:\mathbb{N}\longrightarrow\mathbb{Z}$ dada por $i(n)=+n$ es inyectiva y nos permite identificar cada número natural n con el número entero $+n$, de tal forma que, en lo que se refiere a la suma y el producto, es indiferente trabajar con los números de $\mathbb{N}$ o con los de $i[\mathbb{N}]$, porque se suman y se multiplican igual. Si en $\mathbb{N}$ tenemos, por ejemplo, $3\cdot 4=12$, en $\mathbb{Z}$ tenemos que $(+3)(+4)=+12$.

Así, cuando identificamos el número natural n con el entero $+n$, resulta que tiene opuesto para la suma, a saber, el número entero $-n\equiv[0,n]$. Además, cualquier número entero se descompone como

$$[m,n]=[m,0]+[0,n]=(+m)+(-n)=(+m)-(+n),$$

con lo que acabamos de materializar la idea que había guiado la construcción de $\mathbb{Z}$.

Observemos ahora que la igualdad $+n = -m$ equivale a $m + n = 0$ y sólo se da si $m = n = 0$, en cuyo caso tenemos que $+0 = -0 = 0$. Esto nos lleva a definir los conjuntos

$$\mathbb{Z}^+ = \{+n \mid n \in \mathbb{N} \setminus \{0\}\}, \qquad \mathbb{Z}^- = \{-n \mid n \in \mathbb{N} \setminus \{0\}\}$$

y se cumple que $\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$, donde la unión es disjunta. En efecto, ya hemos probado que la unión es disjunta, y contiene a todos los números enteros porque, dado $[m, n] \in \mathbb{Z}$, o bien $m < n$, en cuyo caso $[m, n] = [m - n, 0] \in \mathbb{Z}^+$, o bien $n < m$, en cuyo caso $[m, n] = [0, n - m] \in \mathbb{Z}^-$, o bien $m = n$, en cuyo caso $[m, n] = [0, 0] = 0$.

Así pues, $\mathbb{Z}$ consta exclusivamente de los números

$$\cdots \quad -3, \quad -2, \quad -1, \quad 0, \quad +1, \quad +2, \quad +3, \quad \cdots$$

y todos ellos son distintos entre sí.

Ahora veamos que es posible extender la relación de orden de $\mathbb{N}$ a $\mathbb{Z}$ para formar un anillo ordenado (aquí usaremos el apartado "Anillos ordenados" de la sección 1.7). La guía es que en todo anillo ordenado debe cumplirse:

$$(a - b) \leq (c - d) \leftrightarrow a + d \leq b + c,$$

lo que nos lleva a definir la relación en $\mathbb{Z}$ dada por

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

Esto supone comprobar que si $[a, b] = [a', b']$ y $[c, d] = [c', d']$ entonces

$$a + d \leq b + c \leftrightarrow a' + d' \leq b' + c',$$

lo cual no ofrece ninguna dificultad, al igual que comprobar que se trata de una relación de orden total que satisface las dos propiedades que definen los anillos ordenados (página 38). Para comprobar la segunda, es decir, que

$$\bigwedge ab \in \mathbb{Z}(a \geq 0 \wedge b \geq 0 \to ab \geq 0),$$

es más fácil observar primero que los números enteros estrictamente positivos son los de $\mathbb{Z}^+$, mientras que los estrictamente negativos son los de $\mathbb{Z}^-$, luego la propiedad se reduce a comprobar que $\bigwedge ab \in \mathbb{N}\ a \cdot b \in \mathbb{N}$, lo cual ya lo sabemos.

También es inmediato a partir de las definiciones que, si m, $n \in \mathbb{N}$, entonces $m \leq n \leftrightarrow +m \leq +n$, lo cual significa que $\mathbb{N}$ e $i[\mathbb{N}]$ tampoco se distinguen por lo que respecta al orden, de modo que, por ejemplo, $3 < 7$ es equivalente a $+3 < +7$.

Las propiedades generales de los anillos ordenados implican ahora que

$$\bigwedge mn \in \mathbb{N}\ (-m < -n \leftrightarrow n < m),$$

lo que en definitiva se traduce en que los números enteros están ordenados así:

$$\cdots -3 < -2 < -1 < 0 < +1 < +2 < +3 < \cdots$$

Ahora es inmediato que $\mathbb{Z}$ es un dominio íntegro, pues si $ab = 0$, entonces $|ab| = |a||b| = 0$, pero los valores absolutos están en $i[\mathbb{N}]$ y, como tiene las mismas propiedades que $\mathbb{N}$, podemos concluir que $|a| = 0 \vee |b| = 0$, luego $a = 0 \vee b = 0$.

En lo sucesivo identificaremos los números naturales con los enteros positivos, de modo que escribiremos 3 en lugar de $+3$ y se cumplirá que $\mathbb{N} \subset \mathbb{Z}$ (esto no supone más que cambiar un sistema de Peano por otro).

Observemos que el conjunto $\mathbb{Z}$ es numerable, pues la proyección en el cociente es una aplicación $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Z}$ suprayectiva y $\mathbb{N} \times \mathbb{N}$ es numerable, luego $\mathbb{Z}$ también lo es. Más explícitamente, es fácil enumerar los números enteros en la forma:

$$a_0 = 0, \quad a_1 = 1, \quad a_2 = -1, \quad a_3 = 2, \quad a_4 = -2, \ldots$$

Una última propiedad relevante de la aritmética básica de los números enteros es que admite la división euclídea en los términos siguientes:

Teorema 2.32 $\bigwedge Dd \in \mathbb{Z}(d \neq 0 \to \overset{1}{\bigvee} cr \in \mathbb{Z}\ (D = dc + r \wedge 0 \leq r < d))$

Demostración: Aplicamos el teorema de la división euclídea a los números naturales $|D|$ y $|d|$, lo que nos da que existen naturales c y r de manera que $|D| = |d|c + r$, con $0 \leq r < |d|$.

Si $r = 0$ entonces cambiando el signo de c si es preciso tenemos $D = dc + 0$. Supongamos $r > 0$ y distingamos cuatro casos:

- Si $D \geq 0$ y $d > 0$ entonces tenemos $D = dc + r$, como queríamos.
- $D \geq 0$ y $d < 0$ entonces sirve $D = d(-c) + r$.
- $D < 0$ y $d > 0$ entonces $D = d(-c - 1) + (d - r)$.
- $D < 0$ y $d < 0$ entonces $D = d(c + 1) + (-d - r)$.

Si tuviéramos dos expresiones distintas $D = dc + r = dc' + r'$, entonces sea $\bar{c} = c$ si $d > 0$ y $\bar{c} = -c$ si $d < 0$. Igualmente definimos $\bar{c}'$. Así $dc = |d|\bar{c}$, $dc' = |d|'\bar{c}'$. Supongamos que $\bar{c} < \bar{c}'$. Entonces

$$D = dc + r = |d|\bar{c} + r < |d|\bar{c} + |d| = |d|(\bar{c} + 1) \leq |d|\bar{c}' = dc' \leq dc' + r' = D,$$

y esto es una contradicción. Por lo tanto ha de ser $c = c'$ y de aquí que $dc + r = dc + r'$, luego $r = r'$. ∎

Observemos ahora que si A es cualquier anillo, podemos definir recurrentemente una aplicación $\cdot a : \mathbb{N} \longrightarrow A$ mediante

$$0a = 0 \wedge \bigwedge n \in \mathbb{N}\ (n + 1)a = na + a.$$

Equivalentemente, $na = \sum_{i<n} a$. Si $n \in \mathbb{Z}$ cumple $n < 0$, definimos $na = (-n)a$, con lo que tenemos definido un producto $\mathbb{Z} \times A \longrightarrow A$ (esto es lo que se llama una *ley de composición externa* en A con coeficientes en $\mathbb{Z}$). Alternativamente, la definición se resume en:

$$ma = \begin{cases} \overbrace{a + \cdots + a}^{m\text{veces}} & \text{si } m > 0, \\ 0 & \text{si } m = 0, \\ \underbrace{-a - \cdots - a}_{-m\text{veces}} & \text{si } m < 0. \end{cases}$$

Es fácil comprobar las propiedades siguientes:

$$(m+n)a = ma + na, \quad m(a+b) = ma + mb, \quad m(na) = (mn)a.$$

Por ejemplo, la primera se prueba para todo $m \in \mathbb{Z}$ y todo $n \in \mathbb{N}$ por inducción sobre n, y luego se prueba, también por inducción sobre n, que

$$(m + (-n))a = ma + (-n)a,$$

con lo que vale para todo m y todo n en $\mathbb{Z}$.

De esta primera propiedad se sigue claramente que $-(na) = (-n)a = n(-a)$.

Estas propiedades implican que, si A es un anillo unitario, la aplicación $i : \mathbb{Z} \longrightarrow A$ dada por $i(m) = m \cdot 1$ es un homomorfismo de anillos. En la práctica escribiremos m en lugar de $m \cdot 1$, lo cual significa que, en un anillo arbitrario, llamamos, por ejemplo, 3 al elemento $1 + 1 + 1$, y llamamos -5 al elemento $-1 - 1 - 1 - 1 - 1$.

El hecho de que i sea un homomorfismo implica que las ecuaciones $2 + 3 = 5$ o $-2 \cdot 3 = -6$, al ser válidas en $\mathbb{Z}$, valen también en cualquier anillo, pero hay que tener presente que la aplicación i no es en general un monomorfismo, de modo que puede ocurrir que en un cierto anillo se cumpla, por ejemplo, $3 = 8$. Esto no sucede si el anillo está ordenado:

Teorema 2.33 *Si A es un anillo ordenado, la aplicación $i : \mathbb{Z} \longrightarrow A$ dada por $i(m) = m \cdot 1$ es un monomorfismo de anillos ordenados.*

DEMOSTRACIÓN: Basta probar que $\bigwedge mn \in \mathbb{Z}(m < n \to i(m) < i(n))$, pues esto ya implica la inyectividad. Observemos en primer lugar que si $n > 0$ entonces $i(n) > 0$. Para $n = 1$ se reduce al hecho de que en todo anillo ordenado $1 > 0$, y si $i(n) > 0$, entonces $i(n+1) = i(n) + 1 > 0 + 1 = 1 > 0$. Por lo tanto, si $n < 0$ tenemos que $i(n) = -i(-n) < 0$.

Ahora probamos por inducción la tercera propiedad para $n \geq 0$. Si $m < 0$ acabamos de ver que $i(m) < 0 = i(0)$. Si vale para n y tenemos que $m < n + 1$, entonces $m \leq n$, luego $m < n \vee m = n$, luego $i(m) < i(n) \vee i(m) = i(n)$, luego $i(m) \leq i(n) < i(n) + 1 = i(n + 1)$.

Por último, si $m < n < 0$, entonces $0 < -n < -m$, luego $i(-n) < i(-m)$, que es lo mismo que $-i(n) < -i(m)$, luego $i(m) < i(n)$. ∎

Esto significa que si A es un anillo ordenado, los elementos de A de la forma $m \cdot 1$, con $m \in \mathbb{Z}$, es decir, los elementos de $i[\mathbb{Z}]$, con la notación del teorema anterior, forman un subanillo ordenado isomorfo a $\mathbb{Z}$, luego indistinguible de $\mathbb{Z}$ en todo lo tocante al orden, la suma y el producto, por lo que en la práctica podemos considerar que $\mathbb{Z} \subset A$ y que la suma, el producto y el orden en $\mathbb{Z}$ son (las restricciones de) los de A.

En estos términos, el teorema anterior afirma que todo anillo ordenado contiene un subanillo isomorfo a $\mathbb{Z}$. También podemos expresar esto diciendo que $\mathbb{Z}$ es el menor anillo ordenado.

Definición 2.34 Diremos que un anillo ordenado A es *arquimediano* si $\mathbb{N}$ no está acotado superiormente en A, es decir, si[7] $\bigwedge a \in A \bigvee n \in \mathbb{N}\ a < n$.

Es inmediato comprobar que esto equivale a que $\mathbb{Z}$ no esté acotado inferiormente en A o a que $\mathbb{Z}$ no esté acotado ni superior ni inferiormente en A.

Trivialmente, $\mathbb{Z}$ es un anillo ordenado arquimediano, pues para todo $m \in \mathbb{Z}$ se cumple que $m < 0$ o, en caso contrario, $m < m + 1$, y en ambos casos el término de la derecha es un número natural.

Es fácil ver que si A es un anillo arquimediano, para cada $a \in A$ existe un único $m \in \mathbb{Z}$ tal que $m \leq a < m + 1$. Dicho m recibe el nombre de *parte entera* (por defecto) de a, y la representaremos por $E[a]$.

El valor $F[a] = a - E[a]$ recibe el nombre de *parte fraccionaria* de a, de modo que a admite una única descomposición:

$$a = E[a] + F[a], \qquad E[A] \in \mathbb{Z}, \quad 0 \leq F[a] < 1.$$

2.6 Los números racionales

El cuerpo $\mathbb{Q}$ de los números racionales es el menor cuerpo que contiene al anillo $\mathbb{Z}$ de los números enteros. La construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ puede realizarse sin esfuerzo adicional alguno en un contexto algebraico general:

Cuerpos de cocientes En todo este apartado $(D, +, \cdot)$ será un dominio íntegro prefijado, aunque nos interesará especialmente el caso en que $D = \mathbb{Z}$. Definimos $D^* = D \setminus \{0\}$ y consideramos en $D \times D^*$ la relación de equivalencia dada por

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

Es fácil ver que ciertamente es una relación de equivalencia. Por ejemplo, para probar la transitividad partimos de que $(a, b) \sim (c, d) \sim (e, f)$, lo que significa que $ad = bc$ y $cf = de$, de donde $adcf = bcde$ y, como los elementos no nulos son simplificables, si $c \neq 0$ podemos concluir $af = be$, mientras que si $c = 0$ tenemos que $ad = 0 = de$, luego $a = e = 0$, luego $af = be$ igualmente.

[7] Notemos que aquí estamos considerando $\mathbb{N} \subset \mathbb{Z} \subset A$, si no quisiéramos hacer esta identificación, simplemente deberíamos escribir $a < n \cdot 1$ en lugar de $a < n$.

Representamos por $K_D = (D \times D^*)/\sim$ el conjunto cociente. Para cada par $(a, b) \in D \times D^*$, representaremos por a/b su clase de equivalencia. Claramente, el teorema 1.31 1) se traduce en este caso en la equivalencia

$$\frac{a}{b} = \frac{c}{d} \leftrightarrow ad = bc.$$

Definimos en K_D las operaciones $+$ y $\cdot$ dadas por

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

Observemos que, desde un punto de vista conjuntista,

$$+ \equiv \{((x, y), z) \in (K_D \times K_D) \times K_D \mid \bigvee abcd \in D(x = a/b \wedge y = c/d$$

$$\wedge z = (ad + bc)/bd)\}.$$

La definición es correcta, en el sentido de que determina un conjunto $+$, pero no podemos asegurar a priori que sea una función $+ : K_D \times K_D \longrightarrow K_D$.

En primer lugar, el hecho de que todo par (x, y) tenga al menos una imagen z se debe a que, por definición de cociente, siempre podemos expresar $x = a/b$, $y = c/d$ y, como $bd \neq 0$ (ya que D es un dominio íntegro), podemos formar la fracción $z = (ad + bc)/bd$, con lo que $((x, y), z) \in +$.

Por otra parte, debemos probar que la imagen z es única. Para ello suponemos que $((x, y), x), (x, y), z') \in +$, lo cual significa que podemos expresar

$$x = \frac{a}{b} = \frac{a'}{b'}, \qquad y = \frac{c}{d} = \frac{c'}{d'},$$

y que

$$z = \frac{ad + bc}{bd}, \qquad z' = \frac{a'd' + b'c'}{b'd'},$$

y debemos demostrar que $z = z'$. Esto equivale a que

$$(ad + bc)b'd' = (a'd' + b'c')bd,$$

o también a que $(ab')(dd') + (cd')(bb') = (a'b)(dd') + (c'd)(bb')$, y esto se sigue inmediatamente de las igualdades de las expresiones para x e y.

El hecho que acabamos de comprobar suele enunciarse diciendo que la suma está bien definida. En general, cuando definimos una aplicación f y uno o varios de sus argumentos son clases de equivalencia de uno o varios conjuntos cociente y en la definición de f usamos un elemento concreto de cada clase de equivalencia, decimos que f está *bien definida* cuando comprobamos que la imagen de unos argumentos dados no depende del representante concreto elegido en cada clase de equivalencia.

Por ejemplo, la forma habitual de tratar las situaciones como la que estamos considerando sin entrar en detalles conjuntistas que podríamos calificar de

pedantes es decir, en el caso del producto, "vamos a comprobar que el producto está bien definido", lo cual supone comprobar que

$$\text{si} \quad \frac{a}{b} = \frac{a'}{b'} \quad y \quad \frac{c}{d} = \frac{d'}{d'}, \quad \text{entonces} \quad \frac{ac}{bd} = \frac{a'c'}{b'd'},$$

es decir, que el producto definido con unos representantes de las fracciones es el mismo que el definido con otros. (Aparte de esto, hay que observar que el producto es realmente una fracción porque $bd \neq 0$.)

Omitimos la comprobación, que es más sencilla que la de la suma, así como la comprobación rutinaria de que la suma y el producto de fracciones cumplen todas las propiedades requeridas por la definición de anillo. Indiquemos únicamente que el neutro para la suma es la fracción $0 = 0/1$ y que el opuesto de una fracción es $-(a/b) = (-a)/b$.

En cuanto al producto, es inmediato comprobar que tiene por neutro a la fracción $1 = 1/1$ y que todo elemento no nulo tiene inverso, pues si $a/b \neq 0/1$, entonces $a \neq 0$, luego podemos considerar la fracción b/a, que claramente es la inversa de a/b, es decir:

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

Por lo tanto, K_D es un cuerpo con las operaciones que hemos definido. Consideramos ahora la aplicación $i_D : D \longrightarrow K_D$ dada por $i_D(a) = a/1$. Es trivial comprobar que es inyectiva, así como que

$$i_D(a+b) = i_D(a) + i_D(b), \qquad i_D(ab) = i_D(a)i_D(b).$$

Con esto hemos probado es que $i_D : D \longrightarrow K$ es un monomorfismo de dominios íntegros. Si llamamos $\bar{D} = i_D[D] \subset K_D$, resulta que $\bar{D}$, con las operaciones de K_D es un anillo y $i_D : D \longrightarrow \bar{D}$ es un isomorfismo de anillos, pero $\bar{D}$ cumple además que está contenido en un cuerpo. En definitiva, hemos probado que todo dominio íntegro puede reemplazarse por otro isomorfo contenido en un cuerpo. El cuerpo K_D que hemos construido se llama *cuerpo de cocientes* o *cuerpo de fracciones* de D.

Más aún, si D es un anillo ordenado, podemos transportar la relación de orden a K_D definiendo

$$x \leq y \equiv \bigvee abcd \in D(c > 0 \wedge d > 0 \wedge x = \frac{a}{b} \wedge y = \frac{c}{d} \wedge ad \leq bc).$$

En primer lugar observamos que, puesto que

$$\frac{a}{b} = \frac{-a}{-b},$$

toda fracción admite un representante con denominador positivo. Y si tomamos dos fracciones a/b y c/d con denominador positivo, entonces

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

Una implicación se cumple por la definición que hemos dado de $\leq$, pero la otra no es inmediata, pues, en principio, que se cumpla la parte izquierda significa que

$$\frac{a}{b} = \frac{a'}{b'}, \quad \frac{c}{d} = \frac{c'}{d'},$$

con $b', d' > 0$ y $a'd' \leq b'c'$. Vamos a probar que esto implica $ad \leq bc$. En principio tenemos que $ab' = ba'$ y $cd' = dc'$. Notemos también que c es positivo si y sólo si lo es cd', si y sólo si lo es $c'd$ si y sólo si lo es c'. Hay que distinguir dos casos, según si c y c' son ambos positivos o son ambos negativos. Trataremos el caso en que ambos son negativos y dejamos el otro a cargo del lector:

$$a'd' \leq b'c' \Rightarrow a'bd'c \geq b'c'bc \Rightarrow b'c'ad \geq b'c'bc \Rightarrow b'd'(ad - bc) \geq 0$$

$$\Rightarrow ad - bc \leq 0 \Rightarrow ad \leq bc.$$

Observemos que, dadas tres fracciones cualesquiera se pueden expresar en la forma

$$\frac{a}{d}, \quad \frac{b}{d}, \quad \frac{c}{d}$$

con $d > 0$. En efecto, si en principio las fracciones son a/b, a'/b', a''/b'', donde podemos suponer que los denominadores son positivos, y entonces

$$\frac{a}{b} = \frac{ab'b''}{bb'b''}, \quad \frac{a'}{b'} = \frac{ba'b''}{bb'b''}, \quad \frac{a''}{b''} = \frac{bb'a''}{bb'b''},$$

con denominador positivo.

Para fracciones con denominador común positivo la relación que hemos definido se reduce a

$$\frac{a}{d} \leq \frac{c}{d} \leftrightarrow a \leq c.$$

Teniendo esto en cuenta es inmediato comprobar que la relación $\leq$ es una relación de orden en K_D y que es compatible con la estructura de anillo, es decir, que convierte a K_D es un cuerpo ordenado. Tambiñen es claro que la aplicación $i_D : D \longrightarrow K_D$ es un monomorfismo de anillos ordenados, es decir, que

$$\bigwedge ab \in D \ (a \leq b \leftrightarrow i_D(a) \leq i_D(b)).$$

Por lo tanto $i_D : D \longrightarrow \bar{D}$ es una semejanza cuando consideramos en $\bar{D}$ el orden de K_D. Así pues, sustituyendo D por una "copia" isomorfa, tenemos que todo dominio íntegro ordenado puede extenderse a un cuerpo ordenado.

Terminamos este apartado insistiendo en que lo importante en nuestro contexto de los argumentos que acabamos de dar es que todos ellos son demostrables a partir de los axiomas de NBG*. Observemos que los resultados que hemos visto sobre formación de conjuntos nos garantizan que todos los objetos que hemos construido son conjuntos. Por ejemplo, si D es un conjunto, D^* lo es por ser un subconjunto de D, y $D \times D^*$ lo es porque el producto cartesiano de conjuntos es un conjunto, y K_D lo es porque todo cociente de un conjunto es

un conjunto, y las operaciones en K_D son conjuntos porque son funciones cuyo dominio es un conjunto, etc.

En general, todas las construcciones que realizan los matemáticos para construir unos conjuntos a partir de otros pueden ser justificadas en NBG. Para las más elementales (como la que acabamos de ver) basta con NBG*, aunque otras pueden requerir AP o incluso los axiomas de infinitud y elección que todavía no hemos presentado. ∎

Definición 2.35 Definimos el cuerpo de los *números racionales* al cuerpo de cocientes $\mathbb{Q}$ de $\mathbb{Z}$.

Sabemos, pues, que $\mathbb{Q}$ es un cuerpo ordenado que contiene un subanillo ordenado isomorfo a $\mathbb{Z}$, cuyos elementos son fracciones de la forma a/b, donde $a, b \in \mathbb{Z}$ con $b \neq 0$, con el criterio de igualdad de fracciones dado por

$$\frac{a}{b} = \frac{c}{d} \leftrightarrow ad = bc.$$

Con las identificaciones oportunas, podemos considerar que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

Aunque no es fácil enumerar de forma explícita todos los números racionales, sí que es fácil probar que, de todos modos, $\mathbb{Q}$ es un conjunto numerable. Basta observar que la proyección en el cociente es una aplicación suprayectiva $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \longrightarrow \mathbb{Q}$ y el término de la izquierda es un producto cartesiano de dos conjuntos numerables, luego es numerable y en consecuencia $\mathbb{Q}$ también lo es.

En el mismo sentido en que podemos decir que $\mathbb{Z}$ es el menor anillo ordenado, podemos decir que $\mathbb{Q}$ es el menor cuerpo ordenado:

Teorema 2.36 *Si K es un cuerpo ordenado, la aplicación $i : \mathbb{Q} \longrightarrow K$ dada por $i(a/b) = (a \cdot 1)/(b \cdot 1)$ es un monomorfismo de cuerpos ordenados.*

Demostración: En primer lugar debemos probar que está bien definida, es decir, que no depende del representante elegido para la fracción o, más concretamente, que si $a/b = c/d$ entonces $(a \cdot 1)/(b \cdot 1) = (c \cdot 1)/(d \cdot 1)$. Ante todo, sabemos que la aplicación $i_0 : \mathbb{Z} \longrightarrow K$ dada por $i_0(n) = n \cdot 1$ es un monomorfismo de anillos. En particular, si $b \neq 0$ se cumple que $i_0(b) \neq 0$ y tiene sentido el cociente $(a \cdot 1)/(b \cdot 1)$.

Por la inyectividad de i_0 tenemos que $ad - bc = 0$ si y sólo si se cumple $i_0(a)i_0(d) - i_0(b)i_0(c) = 0$, si y sólo si $(a \cdot 1)/(b \cdot 1) = (c \cdot 1)/(d \cdot 1)$. Con esto hemos probado que i está bien definida y que es inyectiva. La prueba de que es un monomorfismo de cuerpos ordenados no ofrece ninguna dificultad. ∎

Notemos que si, en el contexto del teorema anterior, adoptamos el criterio usual de escribir a en lugar de $a \cdot 1$, entonces la imagen de una fracción $a/b \in \mathbb{Q}$ es simplemente $a/b \in K$, es decir, que estamos identificando, por ejemplo, $2/3 \in \mathbb{Q}$ con $(1 + 1)/(1 + 1 + 1) \in K$.

Se cumple trivialmente que $\mathbb{Q}$ es arquimediano, pues si $a/b \in \mathbb{Q}$, o bien $a/b < 0$, o bien podemos suponer que $a \geq 0$, $b \geq 1$, y entonces

$$\frac{a}{b} = \frac{a}{b} \cdot 1 \leq \frac{a}{b} \cdot b = a < a + 1,$$

luego en cualquier caso a/b no acota a los números naturales.

Definición 2.37 Se dice que un conjunto ordenado $(A, \leq)$ es *denso* (en sí mismo) si $\bigwedge ab \in A(a < b \to \bigvee c \in A\ a < c < b)$.

Es decir, un conjunto ordenado es denso si entre dos cualesquiera de sus elementos hay siempre un tercero. Esta propiedad la tienen todos los cuerpos ordenados, en particular $\mathbb{Q}$:

Teorema 2.38 *Si K es un cuerpo ordenado, entonces K es denso en sí mismo y no tiene ni máximo ni mínimo.*

Demostración: En todo anillo ordenado se cumple que $2 = 1+1 > 0$. Por lo tanto, si $a < b$ son dos elementos de K, es claro que $a < (a + b)/2 < b$. Por otra parte, $a - 1 < a < a + 1$, luego a no es ni el máximo ni el mínimo de K. ∎

Esta propiedad de $\mathbb{Q}$ contrasta con el caso de $\mathbb{Z}$, donde todo número entero n tiene un inmediato anterior y un inmediato posterior $n - 1 < n < n + 1$, de modo que no hay ningún otro número entre $n - 1$ y n o entre n y $n + 1$.

Veamos ahora que las propiedades del teorema anterior, junto con la numerabilidad, caracterizan el orden de $\mathbb{Q}$:

Teorema 2.39 (Cantor) *Un conjunto totalmente ordenado $(D, \leq)$ es semejante a $\mathbb{Q}$ si y sólo si es numerable, denso en sí mismo y no tiene ni máximo ni mínimo.*

Demostración: Sean $\mathbb{Q} = \{q_n \mid n \in \mathbb{N}\}$ y $D = \{d_n \mid n \in \mathbb{N}\}$. Definimos por recurrencia una sucesión de pares $\{(i_k, j_k)\}_{k\in\mathbb{N}}$ de números naturales de modo que

$$f_n = \{(q_{i_k}, d_{j_k}) \mid k < n\}$$

sea una semejanza entre $\{q_{i_k} \mid k < n\}$ y $\{d_{j_k} \mid k < n\}$. Para ello tomamos $i_0 = j_0 = 0$, de modo que $f_1(q_0) = d_0$. Supuesta definida la sucesión $\{(i_k, j_k)\}_{k<n}$, distinguimos dos casos, según que n sea par o impar.

Si n es par definimos i_n como el mínimo natural que no esté en $\{i_k \mid k < n\}$ y definimos j_n como el mínimo natural tal que d_{j_n} está respecto de $\{d_{j_k} \mid k < n\}$ en la misma posición que q_{i_n} está respecto de $\{q_{i_k} \mid k < n\}$. Las hipótesis del teorema aseguran que siempre existe tal j_n.

Si n es impar definimos j_n como el mínimo natural que no esté en $\{j_k \mid k < n\}$ y definimos i_n como el mínimo natural tal que q_{i_n} está respecto de $\{q_{i_k} \mid k < n\}$ en la misma posición que d_{j_n} está respecto de $\{d_{j_k} \mid k < n\}$. Como $\mathbb{Q}$ también cumple las hipótesis exigidas a D, la existencia de i_n está garantizada.

Llamamos $f = \{(q_{i_k}, d_{j_k}) \mid k \in \mathbb{N}\}$. Por construcción es claro que f es una semejanza de un cierto subconjunto de $\mathbb{Q}$ en un cierto subconjunto de D. Basta probar que $\mathcal{D}f = \mathbb{Q}$ y $\mathcal{R}f = D$. La simetría de la construcción hace que las dos pruebas sean análogas. Veamos, por ejemplo, la primera. Si $\mathcal{D}f \neq \mathbb{Q}$, existe un mínimo i que no aparece nunca en la sucesión $\{i_k\}_{k\in\mathbb{N}}$. Sea $m \in \mathbb{N}$ tal que todos los números menores que i aparecen en la sucesión $\{i_k\}_{k<2m}$, entonces i_{2m} es por definición el menor número natural que no aparece en dicha sucesión, con lo que debería ser $i_{2m} = i$, contradicción. ∎

En particular, vemos que dos cuerpos ordenados numerables son necesariamente semejantes (aunque no necesariamente isomorfos).

2.7 Los números reales

En esta sección, además del axioma de infinitud, supondremos el axioma de partes. Supongamos que X es un conjunto totalmente ordenado y que podemos descomponerlo como $X = A \cup B$, donde todo elemento de A es menor que todo elemento de B. Equivalentemente, A es el conjunto de las cotas inferiores de B y B es el conjunto de las cotas superiores de A.

Si A tiene un máximo elemento m y B tiene un mínimo elemento M, con lo que $m < M$, podemos decir que X "tiene un agujero" entre m y M. Es lo que le ocurre a $\mathbb{Z}$, que tiene un agujero entre cada par de enteros consecutivos.

Pero si A no tiene máximo y B no tiene mínimo (equivalentemente, si B no tiene ínfimo y A no tiene supremo), podemos decir también que X tiene un "agujero microscópico" entre A y B, en el sentido de que no hay ningún punto situado entre ambos, bien como máximo de A o bien como mínimo de B.

Veremos que $\mathbb{Q}$ está lleno de tales "agujeros" y el resultado de "taparlos" es el cuerpo $\mathbb{R}$ de los números reales. Una parte de la construcción puede hacerse en un contexto general:

Conjuntos totalmente ordenados completos Vamos a introducir algunos conceptos adicionales sobre conjuntos totalmente ordenados:

Definición 2.40 Sea X un conjunto totalmente ordenado. Llamaremos *intervalos* en X a los conjuntos siguientes, para todo a, $b \in X$:

$$\begin{aligned}
]a,b[&= \{x \in X \mid a < x < b\}, & [a,b] &= \{x \in X \mid a \leq x \leq b\},\\
]a,b] &= \{x \in X \mid a < x \leq b\}, & [a,b[&= \{x \in X \mid a \leq x < b\},\\
]-\infty,b[&= \{x \in X \mid x < b\}, &]a,+\infty[&= \{x \in X \mid a < x\},\\
]-\infty,b] &= \{x \in X \mid x \leq b\}, & [a,+\infty[&= \{x \in X \mid a \leq x\},\\
&&]-\infty,+\infty[&= X.
\end{aligned}$$

El elemento a (en los intervalos en los que interviene) se llama *extremo inferior* del intervalo, mientras que b (cuando procede) es el *extremo superior*. Los intervalos de la forma $]a,b[$, incluso si a o b es infinito, se llaman *intervalos abiertos*, mientras que los de tipo $[a,b]$ se llaman *intervalos cerrados*.

Observemos que si X tiene máximo M, entonces

$$]a, +\infty[=]a, M]\,, \qquad [a, +\infty[= [a, M]\,,$$

y si tiene mínimo m entonces

$$]-\infty, b[= [m, b[\,, \qquad]-\infty, b] = [m, b]\,,$$

y si tiene máximo y mínimo entonces $]-\infty, +\infty[= [m, M]$, por lo que los intervalos con extremos infinitos sólo son relevantes en ausencia de máximo o de mínimo. En tal caso son conjuntos no acotados, y se llaman *intervalos no acotados.*

Teorema 2.41 *Si X es un conjunto totalmente ordenado, las afirmaciones siguientes son equivalentes:*

1. *Todo subconjunto de X no vacío y acotado superiormente tiene supremo.*
2. *Todo subconjunto de X no vacío y acotado inferiormente tiene ínfimo.*
3. *Un conjunto $I \subset X$ es un intervalo si y sólo si*

$$\bigwedge ab \in I \bigwedge c \in X(a < c < b \to c \in I).$$

4. *Si $X = A \cup B$ de modo que $A \neq \varnothing \neq B$ y todo elemento de A es menor que todo elemento de B, entonces, o bien A tiene máximo, o bien B tiene mínimo.*

Demostración: 1) $\Rightarrow$ 2) Sea B un subconjunto de X no vacío y acotado inferiormente. Sea A el conjunto de las cotas inferiores de A. Como B está acotado, A no es vacío, y como B no es vacío, cualquiera de sus elementos es una cota superior de A, luego A tiene supremo i, que es el ínfimo de B, pues todo elemento $b \in B$ es una cota superior de A, por lo que $i \leq b$, y si c es una cota inferior de B, entonces $c \in A$, luego $c \leq i$.

Análogamente se prueba que 2) $\Rightarrow$ 1). Veamos que 1) y 2) implican 3). Es inmediato que todo intervalo tiene la propiedad indicada. Se trata de probar el recíproco. Supongamos, pues, que I cumple la condición. Si $I = \varnothing$, entonces $I =]-\infty, +\infty[$ si $X = \varnothing$, o bien $I =]a, a[$ si existe un $a \in X$, luego es un intervalo.

Supongamos, pues, que $I \neq \varnothing$. Si I no está acotado ni superior ni inferiormente, entonces $I =]-\infty, +\infty[$, pues, para todo $x \in X$, como no es ni una cota superior ni una cota inferior de I, existen a, $b \in I$ tales que $a < x < b$, luego $x \in I$.

Si I tiene cota superior pero no inferior, tomamos $b = \sup I$ y observamos que $]-\infty, b[\subset I \subset]-\infty, b]$, con lo que I será uno de los dos intervalos según si $b \notin I$ o bien $b \in I$.

En efecto, si $x \in]-\infty, b[$, como x no es cota inferior de I existe un $a \in I$ tal que $a < x$ y, como b es el supremo de I, no puede ser que x sea una cota superior, luego existe un $c \in I$ tal que $a < x < c$, luego $x \in I$. La otra inclusión es trivial, puesto que b es una cota superior.

Los casos restantes (combinaciones de que I tenga o no tenga cota superior e inferior) se tratan análogamente.

3) $\Rightarrow$ 4) Si tenemos $u < x < v$ con $u, v \in A$ y $x \in X$, no puede ser $x \in B$, puesto que tendría que ser mayor que v, luego tiene que ser $x \in A$, luego A es un intervalo, y análogamente se razona que B lo es. Es claro que la única opción para A es ser un intervalo de la forma $A =]-\infty, c[$ o bien $A =]-\infty, c]$, en cuyo caso, B tiene que ser respectivamente de la forma $B = [c, +\infty[$ o bien $B =]c, +\infty[$. En el primer caso B tiene mínimo, y en el segundo A tiene máximo.

4) $\Rightarrow$ 1) Sea $C \subset X$ un conjunto no vacío y acotado superiormente. Llamemos A al conjunto de elementos de X que no son cotas superiores de C y B al conjunto de los elementos que sí que lo son. Obviamente $X = A \cup B$ y si $a \in A$ y $b \in B$, tenemos que A no es una cota superior de C, luego existe un $c \in C$ tal que $a < c$ y, como b es cota superior, $a < c \leq b$. Por 4) existe $s \in X$ que es el máximo de A o bien el mínimo de B. Si es el mínimo de B, entonces es la menor cota superior de C, luego s es el supremo de C. Si s es el máximo de A, entonces existe un $c \in C$ tal que $s < c$, pero $c \in B$, luego c es una cota superior de C, luego c es el máximo, y en particular el supremo, de C. ∎

Definición 2.42 Un conjunto totalmente ordenado es *completo* si cumple cualquiera de las condiciones del teorema anterior.

Notemos que si X tiene máximo y mínimo la completitud equivale a que todo subconjunto de X tenga supremo e ínfimo, pues todo conjunto está acotado superior e inferiormente y $\varnothing$ tiene al mínimo por supremo y al máximo por ínfimo.]

En estos términos, decíamos antes que $\mathbb{Q}$ dista mucho de ser completo con su ordenación usual. A los conjuntos totalmente ordenados densos en sí mismos (como es el caso de $\mathbb{Q}$) los llamaremos *precontinuos,* mientras que un *continuo* será un precontinuo completo.

Si X es un precontinuo, diremos que un subconjunto $D \subset X$ es *denso* si

$$\bigwedge xy \in X(x < y \to \bigvee d \in D\ (x < d < y)).$$

Una aplicación $f : X \longrightarrow Y$ entre dos precontinuos es una *inmersión densa* si es estrictamente monótona creciente, es decir, si

$$\bigwedge uv \in X\ (u < v \to f(u) < f(v)),$$

y $f[X]$ es denso en Y.

Observación Si X es un continuo y $x \in X$ no es máximo ni mínimo de X entonces $X \setminus \{x\}$ deja de ser un continuo, pues el conjunto $]-\infty, x[$ no es vacío (porque x no es mínimo de X) y está acotado superiormente (porque x no es el máximo de X), pero no tiene supremo en $X \setminus \{x\}$.

Por el contrario, es pura rutina comprobar que si a un continuo le quitamos su mínimo o su máximo, el conjunto resultante sigue siendo un continuo, pero ahora sin mínimo o sin máximo, mientras que si a un continuo sin mínimo o sin máximo le añadimos un elemento nuevo y extendemos la relación de orden de modo que se convierta en el mínimo o el máximo, el conjunto resultante sigue siendo un continuo.

Esto se traduce en que los continuos "vienen en grupos de cuatro", en el sentido de que si a un continuo X le quitamos su mínimo y su máximo en caso de que los tenga y llamamos Y al continuo resultante, entonces X es semejante a uno de los cuatro continuos

$$Y, \qquad \{m\} \cup Y, \qquad Y \cup \{M\}, \qquad \{m\} \cup Y \cup \{M\},$$

donde m, M son conjuntos que no pertenecen a Y y sobre los que la relación de orden se extiende de modo que m sea el mínimo y M sea el máximo. ∎

Teorema 2.43 *Sean X e Y dos continuos de modo que X tiene máximo (resp. mínimo) si y sólo si Y también lo tiene, sea $D \subset X$ un conjunto denso y sea $f : D \longrightarrow Y$ una inmersión densa. Entonces existe una única semejanza $F : X \longrightarrow Y$ que extiende a f.*

Demostración: Dado $x \in X$, consideramos el conjunto $D_x =]-\infty, x[\cap D$. Entonces $x = \sup D_x$, pues ciertamente x es una cota superior de D_x y si $y < x$, existe un $d \in D$ tal que $y < d < x$, luego $d \in D_x$, luego y no es cota superior de D_x, luego x es la menor cota superior de D_x.

Si x no es el máximo de X, entonces existe un $d \in D$ tal que $d > x$, con lo que d es una cota superior de D_x y $f(d)$ es una cota superior de $f[D_x]$. Si x es el máximo de X, entonces Y también tiene máximo por hipótesis, luego $f[D_x]$ está igualmente acotado en Y (por su máximo).

Si x no es el mínimo de D_x, entonces existe un $d \in D$ tal que $d < x$, luego $D_x \neq \varnothing$ y $f[D_x] \neq \varnothing$, luego la completitud de Y implica que $f[D_x]$ tiene supremo. Si x es el mínimo de X entonces $D_x = \varnothing$ y $f[D_x] = \varnothing$, pero por hipótesis Y tiene mínimo, y dicho mínimo es el supremo de $\varnothing$.

Así pues, podemos definir $F : X \longrightarrow Y$ mediante $F(x) = \sup f[D_x]$. Veamos que F es una inmersión. Si $x < x'$, existen d, $d' \in D$ tal que $x < d < d' < x'$. Entonces d es una cota superior de D_x y $d' \in D_{x'}$, luego $f(d)$ es una cota superior de $f[D_x]$ y $f(d') \in f[D_{x'}]$, luego $F(x) \leq f(d) < f(d') \leq F(x')$.

Se cumple que $F|_D = f$, pues si $d \in D$, entonces $f(d)$ es una cota superior de $f[D_d]$, luego $F(d) \leq f(d)$. Si la desigualdad fuera estricta, como $f[D]$ es denso existiría un d' en D tal que $F(d) < f(d') < f(d)$, pero entonces $d' < d$, luego $d' \in D_d$ y $f(d') \leq F(d)$, contradicción.

Para probar que F es suprayectiva (y, por consiguiente, una semejanza) basta observar que podemos definir igualmente $F^* : Y \longrightarrow X$ usando la inmersión densa $f^{-1} : f[D] \longrightarrow X$, pero entonces $H = F^* \circ F : Y \longrightarrow Y$ es estrictamente

creciente y restringida a $f[D]$ es la identidad. Esto implica que H es la identidad, pues si $y \in Y$, entonces no puede ser $y < H(y)$, porque existiría un $d \in f[D]$ tal que $y < d < H(y)$, luego $H(y) < H(d) = d$, contradicción, e igualmente si $H(y) < y$. Esto implica que F es suprayectiva.

La unicidad es clara, pues si $G : X \longrightarrow Y$ es una semejanza tal que $G|_D = f$, entonces necesariamente

$$G(x) = G(\sup D_x) = \sup G[D_x] = \sup f[D_x] = F(x). \qquad \blacksquare$$

Veamos ahora que todo precontinuo se puede sumergir densamente en un continuo:

Definición 2.44 Sea X un precontinuo sin máximo ni mínimo. Una *sección inicial abierta* de X es un conjunto $\alpha \subset X$ que cumpla las propiedades siguientes:

1. $\bigwedge x \in X \bigwedge a \in \alpha(x \leq a \to x \in \alpha)$.
2. α no tiene máximo elemento.

Llamaremos $\overline{C(X)}$ al conjunto[8] de todas las secciones iniciales abiertas de X, y la llamaremos *compleción fuerte* de X. Si definimos $-\infty = \varnothing$ y $+\infty = X$, es claro que $\pm\infty \in \overline{C(X)}$. Definimos la *compleción* de X como el conjunto $C(X) = \overline{C(X)} \setminus \{-\infty, +\infty\}$.

Observemos que si α, $\beta \in \overline{C(X)}$, entonces $\alpha \subset \beta \vee \beta \subset \alpha$. En efecto, si no se cumple $\beta \subset \alpha$ es que existe un $b \in \beta \setminus \alpha$. Dado $a \in \alpha$, no puede ser $b \leq a$, ya que entonces $b \in \alpha$ por la primera propiedad de la definición anterior. Por consiguiente, $a < b$, pero entonces $a \in \beta$, con lo que hemos probado que $\alpha \subset \beta$.

En lo sucesivo consideraremos siempre a la compleción $\overline{C(X)}$ como conjunto totalmente ordenado con la relación de inclusión, de modo que si α, $\beta \in \overline{C(X)}$, escribiremos $\alpha \leq \beta$ en lugar de $\alpha \subset \beta$. Claramente, $-\infty$ y $+\infty$ son el mínimo y el máximo de $\overline{C(X)}$, respectivamente.

Pero sucede que $\overline{C(X)}$ es trivialmente completo, pues si $A \subset C(X)$, entonces se comprueba inmediatamente que $\alpha = \bigcup A$ es una sección inicial abierta de X y obviamente es la menor que contiene a todos elementos de A, luego se trata de su supremo.

Consideramos la aplicación $i : X \longrightarrow C(X)$ dada por $i(a) =]-\infty, a[$.

Observemos que ciertamente $i(a) \in C(X)$, pues cumple trivialmente la primera condición de la definición de sección inicial abierta y la segunda la cumple porque si $x \in i(a)$, como X es denso en sí mismo existe un $y \in X$ tal que $x < y < a$, luego $y \in i(a)$, luego $i(a)$ no tiene máximo. Además, como X no tiene mínimo existe un $x \in i(a) \neq -\infty$, y como no tiene máximo existe un $x \in X$ tal que $a < x$, luego $x \notin i(a) \neq +\infty$.

[8] Notemos que es un conjunto porque $\overline{C(X)} \subset \mathcal{P}X$, y usamos el axioma de partes. No obstante, es interesante observar que sin suponer AP podemos trabajar igualmente con la clase $\overline{C(X)}$, aunque no podamos probar que es un conjunto.

También es claro que i es estrictamente monótona creciente, es decir, que

$$\bigwedge xy \in X\ (x < y \to i(x) < i(y)).$$

La desigualdad $i(x) \leq i(y)$ es trivial. Para ver que es estricta usamos que X es denso en sí mismo, con lo que existe un z tal que $x < z < y$, y entonces $z \in i(y) \setminus i(x)$.

De hecho, i es una inmersión densa, ya que si $\alpha < \beta$ son dos elementos de $C(X)$, entonces existe un $b \in \beta \setminus \alpha$. Como b no es máximo de β, existe un $b' \in \beta$ tal que $b < b'$, y podemos tomar $c \in X$ tal que $b < x < b'$. Entonces es claro que $A \leq i(b) < i(x) < i(b') \leq \beta$.

Notemos que esto implica en particular que $C(X)$ es denso en sí mismo. Además no tiene máximo ni mínimo, pues si $\alpha \in C(X)$, entonces $\alpha \neq X$, luego existe un $u \in X \setminus \alpha$, luego $\alpha \leq i(u)$ y, como u no es el máximo de X, existe $v \in X$ tal que $u < v$ y $\alpha \leq i(u) < i(v)$, luego α no es el máximo de $C(X)$. Por otra parte, como $\alpha \neq \varnothing$, existe $v \in \alpha$ y existe $u < v$, luego $i(u) < i(v) \leq \alpha$, luego α no es el mínimo de $C(X)$. Esto implica a su vez que $\overline{C(X)}$ (que resulta de añadir a $C(X)$ un máximo y un mínimo) también en denso en sí mismo.

Recapitulando:

Teorema 2.45 *Sea X un precontinuo sin máximo ni mínimo. Entonces $C(X)$ es un continuo sin máximo ni mínimo, $i : X \longrightarrow C(X)$ es una inmersión densa y si Y es un continuo sin máximo ni mínimo tal que existe una inmersión densa $j : X \longrightarrow Y$, entonces existe una única semejanza $f : C(X) \longrightarrow Y$ tal que $i \circ f = j$.*

Demostración: Acabamos de ver que $C(X)$ es un continuo sin máximo ni mínimo tal que i es una inmersión densa. Si $j : X \longrightarrow Y$ es una inmersión densa, entonces $i^{-1} \circ j : i[X] \longrightarrow j[X]$ es una semejanza a la que podemos aplicar el teorema 2.43, que nos da una única semejanza f que extiende a $i^{-1} \circ j$. Es fácil ver que es también la única que cumple $i \circ f = j$. ∎

Nota El teorema anterior admite varias versiones similares. Por ejemplo, podemos cambiar $C(X)$ por $\overline{C(X)}$, con el único cambio de que ahora $C(X)$ tiene máximo y mínimo y hay que exigir lo mismo de Y.

Si X tiene máximo y mínimo, definimos $C(X) = \overline{C(X')}$, donde X' es el precontinuo que resulta de eliminar el máximo y el mínimo de X. Entonces la inmersión densa $i : X' \longrightarrow \overline{C(X')} = C(X)$ dada por el teorema anterior se extiende trivialmente a una inmersión densa $i : X \longrightarrow C(X)$ para la que vale igualmente la condición de unicidad.

Por último, se pueden considerar los casos intermedios para continuos con máximo y sin mínimo o viceversa. ∎

Definición 2.46 Llamaremos conjunto de los *números reales* a la compleción $\mathbb{R} = C(\mathbb{Q})$ de $\mathbb{Q}$, con el orden dado por la inclusión. Así $\mathbb{R}$ es un continuo sin máximo ni mínimo y podemos identificar a $\mathbb{Q}$ con un subconjunto denso de $\mathbb{R}$. También tenemos definido $\overline{R} = \overline{C(\mathbb{Q})} = \mathbb{R} \cup \{\pm\infty\}$, que es un continuo con máximo y mínimo.

Si α, $\beta \in \mathbb{R}$, definimos

$$\alpha + \beta = \sup\{r + s \mid r,\, s \in \mathbb{Q},\, r < \alpha, s < \beta\}.$$

Ciertamente tenemos que $\alpha+\beta \in \mathbb{R}$, pues el conjunto está acotado superiormente por la suma de dos números racionales mayores que α y β, respectivamente.

Si α y β son números reales positivos, definimos

$$\alpha\beta = \sup\{rs \mid r,\, s \in \mathbb{Q},\, 0 < r < \alpha,\, 0 < s < \beta\}.$$

De nuevo es claro que $\alpha\beta \in \mathbb{R}$. El producto de dos números reales no nulos se define por las relaciones:

$$\alpha\beta = \begin{cases} -\big((-\alpha)\beta\big) & \text{si } \alpha < 0,\ \beta > 0, \\ -\big(\alpha(-\beta)\big) & \text{si } \alpha > 0,\ \beta < 0, \\ (-\alpha)(-\beta) & \text{si } \alpha < 0,\ \beta < 0. \end{cases}$$

Finalmente, si $\alpha = 0$ o $\beta = 0$ definimos $\alpha\beta = 0$.

Teorema 2.47 *Con las operaciones que acabamos de definir, $\mathbb{R}$ es un cuerpo ordenado que contiene a $\mathbb{Q}$ como subcuerpo ordenado.*

Demostración:

- La suma de números reales es asociativa.

  Si $x \in \mathbb{Q}$, $x < (\alpha + \beta) + \gamma$, entonces existen y, $t \in \mathbb{Q}$ tales que $x < y + t$, $y < \alpha + \beta$, $t < \gamma$, luego existen $r, s \in \mathbb{Q}$, tales que $y < r + s$, $r < \alpha$, $s < \beta$, luego $s+t < \beta+\gamma$ y $x < r+(s+t) < \alpha+(\beta+\gamma)$. Similarmente se recorre el camino contrario, luego $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

- La suma de números reales es conmutativa.

  Esto es inmediato por la definición.

- Para todo $\alpha \in \mathbb{R}$, se cumple que $\alpha + 0 = \alpha$.

  Si $x \in \mathbb{Q}$, $x < \alpha + 0$ existen r, $s \in \mathbb{Q}$ tales que $x < r + s$, $r < \alpha$, $s < 0$, luego $x < r + s < r < \alpha$. Igualmente, si $r \in \mathbb{Q}$, $r < \alpha$ entonces existe un $s \in \mathbb{Q}$ tal que $r < s < \alpha$, con lo que $r = s + (r - s) < \alpha + 0$.

- Dado un número real α, definimos $-\alpha = \sup\{-r \mid r \in \mathbb{Q},\, \alpha < r\}$. Una cota superior del conjunto es $-s$, donde $s \in \mathbb{Q}$, $s < \alpha$, luego $-\alpha \in \mathbb{R}$. Veamos que $\alpha + (-\alpha) = 0$.

Si $x \in \mathbb{Q}$, $x < \alpha + (-\alpha)$ entonces existen r, $s \in \mathbb{Q}$ tales que $x < r + s$, $r < \alpha$, $-s > \alpha$, luego $x < r + s < 0$. Recíprocamente, si $x \in \mathbb{Q}$, $x < 0$, tomamos números racionales $x < -u < 0$ y $v < \alpha$. Entonces la sucesión $v + nu$ sobrepasará (un número racional mayor que) α para algún $n \in \mathbb{N}$, que podemos tomar mínimo. Así obtenemos un número $r < \alpha$ tal que $s = r + u > \alpha$ (si $r + u = \alpha$ cambiamos u por un número mayor que siga cumpliendo $x < -u < 0$). Entonces $x < -u = r - s < \alpha + (-\alpha)$.

- La suma de números reales extiende a la de números racionales.

  Dados $u, v \in \mathbb{Q}$, si $x \in \mathbb{Q}$ cumple $x < i(u) + i(v)$ entonces existen r, $s \in \mathbb{Q}$ tales que $x < r + s$, $r < u$, $s < v$, luego $x < u + v$, luego $x < i(u + v)$. Si $x < i(u + v)$ tomamos $r \in \mathbb{Q}$ tal que $0 < r < (u + v - x)/2$, de modo que $x < (u - r) + (v - r) < i(u) + i(v)$. Por lo tanto $i(u + v) = i(u) + i(v)$.

- Si $\alpha \leq \beta$ entonces $\alpha + \gamma \leq \beta + \gamma$.

  Si $r < \alpha$ y $s < \gamma$ son números racionales y $\alpha \leq \beta$, entonces $r + s \leq \beta + \gamma$ por definición de suma, luego tomando el supremo, $\alpha + \gamma \leq \beta + \gamma$.

La prueba de que el producto de números reales positivos es asociativo, conmutativo, tiene por neutro a 1 y de que todo número real positivo α tiene un inverso α^{-1}, así como de que el producto de números reales extiende al de números racionales, se obtiene cambiando sumas por productos en la prueba de que la suma de números reales tiene estas propiedades. Después las propiedades se trasladan formalmente a números reales arbitrarios a partir de la definición de producto.

Para probar que $\mathbb{R}$ es un cuerpo sólo queda comprobar que la suma distribuye al producto. Tomemos primero α, β, $\gamma > 0$ y veamos que $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Si $r \in \mathbb{Q}$ cumple $0 < r < \alpha(\beta + \gamma)$, entonces existen u, $v \in \mathbb{Q}$ positivos y tales que $r < uv$, $u < \alpha$, $v < \beta + \gamma$, luego existen x, $y \in \mathbb{Q}$ positivos tales que $v < x + y$, $x < \beta$, $y < \gamma$. Entonces $r < u(x + y) = ux + uy \leq \alpha\beta + \alpha\gamma$.

Si $0 < r < \alpha\beta + \alpha\gamma$ entonces existen u, $v \in \mathbb{Q}$ positivos tales que $r < u + v$, $u < \alpha\beta$, $v < \alpha\gamma$. A su vez existen a, b, c, $d \in \mathbb{Q}$ positivos de modo que $r < ab + cd$, $a < \alpha$, $b < \beta$, $c < \alpha$, $d < \gamma$. Sea $e = \max\{a, c\}$. Entonces $e < \alpha$ y $r < eb + ed = e(b + d) < \alpha(\beta + \gamma)$. Esto prueba la igualdad.

Si $\beta + \gamma \geq 0$, $\beta \geq 0, \gamma < 0$, entonces $\alpha\beta = \alpha\big((\beta + \gamma) - \gamma\big) = \alpha(\beta + \gamma) + \alpha(-\beta)$ (puesto que $\beta + \gamma \geq 0$ y $-\gamma \geq 0$), de donde $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$. Los demás casos se siguen formalmente de éstos dos.

De la propia definición de producto se sigue que el producto de números positivos es positivo, por lo que $\mathbb{R}$ resulta ser un cuerpo ordenado. ∎

Tenemos, pues, que $\mathbb{R}$ es un cuerpo ordenado completo (en el sentido de que es completo como conjunto totalmente ordenado). Vamos a probar que esto caracteriza a $\mathbb{R}$ salvo isomorfismo, por lo que la construcción particular con la que lo hemos obtenido resulta ser irrelevante. Empezamos observando lo siguiente:

Teorema 2.48 *Todo cuerpo ordenado completo es arquimediano.*

DEMOSTRACIÓN: Sea R un cuerpo ordenado completo. Si no es arquimediano, entonces $\mathbb{N}$ está acotado superiormente, luego tiene supremo, digamos s. Por definición de supremo, $s-1/2$ no es cota superior de $\mathbb{N}$, luego existe un $n \in \mathbb{N}$ tal que $s - 1/2 < n \leq s$, pero entonces $s < n + 1/2 < n + 1$, en contradicción con que s sea cota superior de $\mathbb{N}$. ∎

Teorema 2.49 *Todo cuerpo ordenado arquimediano contiene un subcuerpo denso isomorfo a $\mathbb{Q}$.*

DEMOSTRACIÓN: Sea R un cuerpo ordenado arquimediano. Por 2.36, sabemos que R contiene un subcuerpo isomorfo a $\mathbb{Q}$. Dados $a < b$ en R, sea n un número natural tal que $1/(b-a) < n$, con lo que $1/n < b-a$. Sea $m = E[na]+1$, de modo que $m - 1 \leq na < m$, luego

$$a < \frac{m}{n} = \frac{m-1}{n} + \frac{1}{n} < a + b - a = b.$$

Así, $q = m/n$ cumple $a < q < b$. ∎

Teorema 2.50 *Todo cuerpo ordenado completo es isomorfo a $\mathbb{R}$.*

DEMOSTRACIÓN: Sea R un cuerpo ordenado completo y sea $i : \mathbb{Q} \longrightarrow R$ un isomorfismo (y semejanza) entre $\mathbb{Q}$ y un subcuerpo denso de R. Por 2.45, tenemos que i se extiende a una semejanza $i : \mathbb{R} \longrightarrow R$. Vamos a probar que se trata de un isomorfismo de cuerpos.

Sean $\alpha, \beta \in \mathbb{R}$ y supongamos que $i(\alpha+\beta) < i(\alpha)+i(\beta)$. Entonces existe un $r \in \mathbb{Q}$ tal que $i(\alpha + \beta) < i(r) < i(\alpha) + i(\beta)$ (porque $i[\mathbb{Q}]$ es denso en R), luego $\alpha+\beta < r$, luego existe $r_1 \in \mathbb{Q}$ tal que $\alpha < r_1 < r-\beta$, luego $r_2 = r-r_1 > \beta$, y así $r = r_1+r_2$, con $\alpha < r_1$ y $\beta < r_2$. Por lo tanto, $i(r) = i(r_1)+i(r_2) > i(\alpha)+i(\beta)$, contradicción.

Igualmente llegamos a una contradicción si $i(\alpha+\beta) > i(\alpha)+i(\beta)$, luego tiene que ser $i(\alpha + \beta) = i(\alpha) + i(\beta)$. De aquí se sigue a su vez que $i(-\alpha) = -i(\alpha)$.

El mismo razonamiento prueba que $i(\alpha\beta) = i(\alpha)i(\beta)$ cuando α, β son números reales positivos, y la relación $i(-\alpha) = -i(\alpha)$ nos da el caso general. ∎

Del mismo modo que el teorema 2.39 caracteriza el tipo de orden de $\mathbb{Q}$, el teorema siguiente caracteriza el tipo de orden de $\mathbb{R}$:

Teorema 2.51 *Un conjunto ordenado es semejante a $\mathbb{R}$ si y sólo si tiene las propiedades siguientes:*

1. *Está totalmente ordenado, no tiene máximo ni mínimo y es denso en sí mismo.*
2. *Es completo.*
3. *Tiene un subconjunto denso numerable.*

(En otras palabras, si y sólo si es un continuo sin máximo ni mínimo y con un subconjunto denso numerable.)

DEMOSTRACIÓN: Trivialmente, todo conjunto ordenado semejante a $\mathbb{R}$ tiene estas características, porque $\mathbb{R}$ las tiene. Recíprocamente, si X es un continuo con un subconjunto denso numerable D, es necesario que D sea un precontinuo, pues, por la propia densidad, entre dos puntos de D debe haber un tercer punto de D, y no puede tener ni máximo ni mínimo, pues por encima de un punto de D tiene que haber uno de X, y entre ambos tiene que haber otro de D (e igualmente para el caso del mínimo).

El teorema 2.39 nos da una semejanza $f : \mathbb{Q} \longrightarrow D$, que es una inmersión densa $f : \mathbb{Q} \longrightarrow X$. El teorema 2.45 implica que i se extiende a una semejanza $F : C(\mathbb{Q}) \longrightarrow X$, luego $X \cong C(\mathbb{Q}) = \mathbb{R}$. ∎

Por ejemplo, si $\alpha < \beta$ son dos números reales, es fácil ver que el intervalo $]\alpha, \beta[$ cumple las condiciones del teorema anterior, por lo que $]\alpha, \beta[\cong \mathbb{R}$.

En realidad, nada de lo que hemos probado aquí nos asegura que $\mathbb{R} \neq \mathbb{Q}$. Vamos a demostrar algo mucho más fuerte, a saber, que, a diferencia de lo que sucede con $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$, el conjunto $\mathbb{R}$ de los números reales no es numerable. Para ello nos apoyaremos en la consecuencia siguiente de la completitud de $\mathbb{R}$:

Teorema 2.52 (de los intervalos encajados de Cantor) *Si X es un continuo y $\{a_n\}_{n\in\mathbb{N}}$ y $\{b_n\}_{n\in\mathbb{N}}$ son dos sucesiones en X tales que, para todo índice n, se cumple $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$, entonces existe un $l \in X$ tal que $\bigwedge n \in \mathbb{N}\ a_n \leq l \leq b_n$.*

DEMOSTRACIÓN: El conjunto $A = \{a_n \mid n \in \mathbb{N}\}$ es no vacío y está acotado superiormente por cualquier b_n, luego tiene supremo l, de modo que $a_n \leq l \leq b_n$. ∎

Teorema 2.53 $\overline{\overline{\mathbb{R}}} = \overline{\overline{\mathcal{P}\mathbb{N}}}$. *En particular, $\mathbb{R}$ no es numerable.*

DEMOSTRACIÓN: Sabemos que $\overline{\overline{\mathbb{Q}}} = \overline{\overline{\mathbb{N}}}$ y si $f : \mathbb{N} \longrightarrow \mathbb{Q}$ es cualquier biyección, es claro que $A \mapsto f[A]$ determina una biyección entre $\mathcal{P}\mathbb{N}$ y $\mathcal{P}\mathbb{Q}$, luego también $\overline{\overline{\mathcal{P}\mathbb{N}}} = \overline{\overline{\mathcal{P}\mathbb{Q}}}$. Como $\mathbb{R} \subset \mathcal{P}\mathbb{Q}$, tenemos que $\overline{\overline{\mathbb{R}}} \leq \overline{\overline{\mathcal{P}\mathbb{Q}}}$, luego también $\overline{\overline{\mathbb{R}}} \leq \overline{\overline{\mathcal{P}\mathbb{N}}}$.

En virtud del teorema de Cantor-Bernstein, basta probar la "desigualdad" opuesta. Para ello consideramos el conjunto $C = \{0, 1\}^{\mathbb{N}}$ de todas las aplicaciones de $\mathbb{N}$ en $\{0, 1\}$. Se cumple que $\overline{\overline{C}} = \overline{\overline{\mathcal{P}\mathbb{N}}}$, pues una biyección entre ambos es la dada por $s \mapsto s^{-1}[\{1\}]$. Así pues, basta probar que $\overline{\overline{C}} \leq \overline{\overline{\mathbb{R}}}$.

Si $\alpha < \beta$ son dos números reales, podemos dividir el intervalo $I = [\alpha, \beta]$ en tres partes iguales:

$$\alpha < \alpha + \frac{\beta - \alpha}{3} < \alpha + \frac{2(\beta - \alpha)}{3} < \beta.$$

Definimos $I_0 = [\alpha, \alpha + (\beta - \alpha)/3]$, $I_1 = [\alpha + 2(\beta - \alpha)/3, \beta]$, de modo que $I_0, I_1 \subset I$, $I_0 \cap I_1 = \varnothing$. Más aún, si definimos la longitud de un intervalo $I = [\alpha, \beta]$ como $\ell(I) = \beta - \alpha$, tenemos que $\ell(I_0) = \ell(I_1) = \ell(I)/3$.

Así, si partimos del intervalo $I = [0,1]$, podemos dividirlo en tres partes y quedarnos con las dos extremas, I_0 e I_1, de longitud $1/3$, cada una de las cuales puede a su vez dividirse en tres partes, con lo que obtenemos los intervalos I_{00}, I_{01}, I_{10}, I_{11} de longitud $1/9$ que muestra la figura:

Podemos continuar indefinidamente este proceso de subdivisión. Para formalizar esta construcción consideramos el conjunto $C = \{0,1\}^{\mathbb{N}}$ de todas las sucesiones de ceros y unos. Para cada $s \in C$ y cada $n \in \mathbb{N}$, llamaremos $s|_n$ a la restricción de s al conjunto $I_n^* = \{0, \ldots, n-1\}$.

Fijado $s \in C$, podemos definir recurrentemente intervalos $I_{s,n}$ mediante la relación

$$I_{s,0} = [0,1], \qquad I_{s,n+1} = (I_{s,n})_{s(n)}.$$

Una simple inducción prueba que si $s|_n = t|_n$, entonces $I_{s,n} = I_{t,n}$, es decir, que el intervalo $I_{s,n}$ no depende de s, sino únicamente de $s|_n$, por lo que podemos llamarlo $I_{s|_n}$.

De este modo, cada $I_{s|_n}$ es un intervalo cerrado contenido en $[0,1]$ de longitud $\ell(I_{s|_n}) = 1/3^n$. Además si $m \leq n$ entonces $I_{s|_n} \subset I_{s|_m}$.

Consecuentemente, para cada $s \in C$, la sucesión $\{I_{s|_n}\}_{n\in\mathbb{N}}$ es una sucesión de intervalos encajados en las condiciones del teorema anterior (mejor dicho: si $I_{s|_n} = [a_n, b_n]$, las sucesiones $\{a_n\}_{n\in\mathbb{N}}$ y $\{b_n\}_{n\in\mathbb{N}}$ están en las condiciones del teorema anterior). Por lo tanto, existe un número real $l \in \bigcap_{n\in\mathbb{N}} I_{s|_n}$.

Dicho número real es único, pues si hay dos, digamos $l_1 \leq l_2$, para todo $n \geq 1$ tendríamos que

$$0 \leq l_2 - l_1 \leq b_n - a_n = \frac{1}{3^n} \leq \frac{1}{n},$$

y, por la propiedad arquimediana, esto sólo es posible si $l_1 = l_2$.

Por lo tanto, podemos llamar $x_s \in \mathbb{R}$ al único número real que cumple $\bigcap_{n\in\mathbb{N}} I_{s|_n} = \{x_s\}$. Tenemos así una aplicación $f : C \longrightarrow \mathbb{R}$ dada por $f(s) = x_s$, que es inyectiva, pues si $s \neq t$, existe un mínimo $n \in \mathbb{N}$ tal que $s|_n \neq t|_n$, luego $I_{s|_n} = I_{t|_n}$, pero $x_s \in I_{s|_{n+1}}$, $x_t \in I_{t|_{n+1}}$ y estos intervalos son los dos subintervalos disjuntos que hemos tomado dentro de $I_{s|_n} = I_{t|_n}$, luego $x_s \neq x_t$.

Así pues, $\overline{\overline{C}} \leq \overline{\overline{\mathbb{R}}}$, como queríamos probar. El teorema de Cantor 1.25 implica entonces que $\mathbb{R}$ no es numerable. ∎

Notemos que en realidad hemos probado que el intervalo $I = [0,1]$ no es numerable, y una ligera modificación de la prueba muestra que todo intervalo en $\mathbb{R}$ (no vacío y que no se reduzca a un punto) es no numerable. Alternativamente, esto se deduce del teorema 2.51 (véase la observación posterior).

La diferencia de tamaño entre $\mathbb{R}$ y $\mathbb{Q}$ tiene muchas consecuencias. De momento señalamos una muy simple:

Teorema 2.54 *Entre dos números reales cualesquiera hay infinitos números racionales e infinitos números irracionales.*

DEMOSTRACIÓN: Que entre dos números reales cualesquiera hay infinitos números irracionales es consecuencia de que $\mathbb{Q}$ es denso en $\mathbb{R}$. Por otra parte, si $\alpha < \beta$, entonces

$$[\alpha, \beta] = ([\alpha, \beta] \cap \mathbb{Q}) \cup ([\alpha, \beta] \setminus \mathbb{Q})$$

Sabemos que $[\alpha, \beta] \cap \mathbb{Q}$ es numerable y, si $[\alpha, \beta] \setminus \mathbb{Q}$ fuera finito, es claro que la unión sería también numerable, pero sabemos que no lo es, luego $[\alpha, \beta] \setminus \mathbb{Q}$ es infinito. De hecho, es fácil ver que tiene que ser no numerable. ∎

De este modo, si $p < q$ son dos números racionales, cualquier número irracional $p < \alpha < q$ está llenando un "agujero infinitesimal" en $\mathbb{Q}$, en el sentido de que

$$\mathbb{Q} = \{q \in \mathbb{Q} \mid q < \alpha\} \cup \{q \in \mathbb{Q} \mid q > \alpha\}$$

es una descomposición de $\mathbb{Q}$ en dos conjuntos no vacíos tales que todo elemento del primero es menor que todo elemento del segundo y, sin embargo, no hay ningún número racional que sea el máximo del primero o el mínimo del segundo. En otras palabras, el primer conjunto no tiene supremo y el segundo no tiene ínfimo.

Terminamos con otra aplicación de la completitud de $\mathbb{R}$ que necesitaremos en la construcción de los números complejos:

Teorema 2.55 *Para todo número real $\alpha \geq 0$ existe un único número $\beta \geq 0$ tal que $\beta^2 = \alpha$.*

DEMOSTRACIÓN: Basta tomar $\beta = \sup\{\delta \in \mathbb{R} \mid \delta^2 \leq \alpha\}$. Notemos que el conjunto cuyo supremo estamos calculando no es vacío, pues contiene a 0, y está acotado superiormente por cualquier número natural mayor que α. Por lo tanto, $\beta \in \mathbb{R}$ y $\beta \geq 0$.

Si fuera $\beta^2 < \alpha$, entonces, para todo $0 < \epsilon < 1$, tenemos que

$$(\beta + \epsilon)^2 = \beta^2 + 2\beta\epsilon + \epsilon^2 \leq \beta^2 + 2\beta\epsilon + \epsilon = \beta^2 + (2\beta + 1)\epsilon,$$

luego cualquier $\epsilon < (\alpha - \beta^2)/(2\beta + 1)$ hace que $(\beta + \epsilon)^2 < \alpha$, en contradicción con la definición de β. Si fuera $\beta^2 > \alpha$, entonces

$$(\beta - \epsilon)^2 = \beta^2 - 2\beta\epsilon + \epsilon^2 = \beta^2 - (2\beta - \epsilon)\epsilon > \beta^2 - 2\beta\epsilon,$$

luego todo $\epsilon < (\beta^2 - \alpha)/2\beta$ hace que $(\beta - \epsilon)^2 > \alpha$, luego β no sería la menor cota superior del conjunto del cual es supremo. Por lo tanto, tiene que ser $\beta^2 = \alpha$.

La unicidad es inmediata, pues si $0 \leq \beta_1 < \beta_2$, entonces $\beta_1^2 < \beta_2^2$. ∎

Definición 2.56 Si $\alpha \geq 0$ es un número real, se llama *raíz cuadrada* de α al único número real $\beta \geq 0$ que cumple $\beta^2 = \alpha$. Se representa por $\sqrt{\alpha}$.

De la unicidad de la raíz cuadrada se sigue inmediatamente la relación $\sqrt{\alpha\beta} = \sqrt{\alpha}\sqrt{\beta}$. También es claro que si $0 \leq \alpha \leq \beta$, entonces $\sqrt{\alpha} \leq \sqrt{\beta}$.

2.8 Los números complejos

Terminamos la construcción del sistema numérico discutiendo brevemente el cuerpo $\mathbb{C}$ de los números complejos. Aunque existen construcciones algebraicas más conceptuales, la forma más simple desde un punto de vista conjuntista de definir los números complejos es como $\mathbb{C} = \mathbb{R}^2$, es decir, un *número complejo* es, por definición, un par de números reales. La suma y el producto de números complejos se definen así:

$$(x, y) + (x', y') = (x + x', y + y'), \quad (x, y)(x', y') = (xx' - yy', xy' + x'y).$$

Una comprobación rutinaria muestra que, con estas operaciones, $\mathbb{C}$ tiene estructura de cuerpo, donde $0 = (0, 0)$, $1 = (1, 0)$, $-(x, y) = (-x, -y)$ y

$$(x, y)^{-1} = \left(\frac{x}{x^2 + y^2}, -\frac{y}{x^2 + y^2}\right).$$

Además, la aplicación $i : \mathbb{R} \longrightarrow \mathbb{C}$ dada por $i(x) = (x, 0)$ es un monomorfismo de cuerpos, lo que nos permite identificar los números reales con los números complejos de la forma $(x, 0)$. Si además convenimos en llamar *unidad imaginaria* al número complejo $i = (0, 1)$, sucede que

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (y, 0)(0, 1) = x + yi,$$

por lo que todo número complejo z se expresa de forma única como $z = x + yi$, para ciertos números reales x y y, que reciben el nombre de *parte real* y *parte imaginaria* de z, respectivamente.

Se define el *conjugado* de un número complejo $z = x + yi$ como $\bar{z} = x - yi$. Es claro entonces que un número complejo z es real si y sólo si $z = \bar{z}$.

Una comprobación rutinaria muestra que

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \qquad \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2.$$

En términos algebraicos, esto significa que la conjugación es un automorfismo de $\mathbb{C}$ (un isomorfismo de cuerpos de $\mathbb{C}$ en sí mismo).

Definimos el *módulo* de un número complejo $z = x + yi$ como

$$|z| = \sqrt{z\bar{z}} = \sqrt{x^2 + y^2}.$$

El módulo cumple las propiedades siguientes:

1. $|z| \geq 0$ y $|z| = 0$ si y sólo si $z = 0$,
2. $|z_1 z_2| = |z_1||z_2|$,
3. $|z_1 + z_2| \leq |z_1| + |z_2|$.

La única que no es inmediata es la tercera. Para probarla demostramos primero la relación

$$|x_1y_1 + x_2y_2| \le |z_1||z_2|, \qquad \text{donde } z_j = x_j + y_j\, i, \quad j = 1, 2,$$

En efecto, llamemos $A = |z_1|^2$, $B = |x_1y_1 + x_2y_2|$, $C = |z_2|^2$. Sea $\alpha = \pm 1$ de modo que $B = \alpha(x_1y_1 + x_2y_2)$. Para todo número real $r \ge 0$ se cumple que

$$0 \le |z_1 - r\alpha z_2|^2 = (x_1 - r\alpha x_2)^2 + (y_1 - r\alpha y_2)^2 = A - 2rB + Cr^2.$$

Si $C = 0$, tiene que ser $B = 0$, o la desigualdad sería falsa para r grande. Si $C > 0$, tomamos $f = B/C$ y obtenemos $B^2 \le AC$, que es lo que queríamos probar.

Pasamos ya a probar la propiedad 3):

$$|z_1 + z_2|^2 = (x_1 + x_2)^2 + (y_1 + y_2)^2 = (x_1^2 + y_1^2) + (x_2 + y_2)^2 + 2(x_1x_2 + y_1y_2)$$

$$= |z_1|^2 + |z_2|^2 + 2(x_1x_2 + y_1y_2) \le |z_1|^2 + |z_2|^2 + 2|z_1||z_2| = (|z_1| + |z_2|)^2,$$

y basta tomar raíces cuadradas. ∎

Así, el módulo de los números complejos cumple las mismas propiedades que el valor absoluto en un cuerpo ordenado (las restantes se deducen trivialmente de la definición de módulo o de las que hemos probado), pero $\mathbb{C}$ no admite ninguna estructura de cuerpo ordenado (con la suma y el producto que hemos definido), pues cumple que $i^2 = -1$, y en un cuerpo ordenado tiene que ser $-1 < 0$, mientras que todo cuadrado tiene que ser positivo.

Capítulo III

Ordinales

En los capítulos precedentes hemos presentado casi la totalidad de los elementos básicos que la mayoría de las ramas de la matemática necesitan de la teoría de conjuntos como punto de partida para una fundamentación rigurosa. Sólo faltaría hablar del axioma de elección y sus consecuencias más importantes, así como de algunos resultados básicos sobre cardinales infinitos. De esto nos ocuparemos en los dos capítulos siguientes.

Ahora vamos a presentar uno de los conceptos fundamentales de la teoría de conjuntos como rama específica de las matemáticas, que se usa con poca frecuencia en otras ramas: los ordinales o números transfinitos. El axioma de regularidad, que introduciremos en el capítulo siguiente, convertirá a los ordinales en el "esqueleto" o el "armazón" de la clase universal V, mientras que el axioma de elección los hará capaces de enumerar cualquier conjunto, cualquiera que sea su tamaño, algo que no puede hacerse con los números naturales.

En el capítulo anterior hemos construido los números naturales, pero no hemos definido ningún conjunto $\mathbb{N}$ en particular, sino que hemos llamado $\mathbb{N}$ a cualquier sistema de Peano. Hemos construido uno a partir de una aplicación $S : X \longrightarrow X$ inyectiva y no suprayectiva dada por el axioma de infinitud, de modo que distintas elecciones de S (y del elemento escogido como $0 \in X$) dan lugar a distintos sistemas de Peano.

En este capítulo empezaremos construyendo un sistema de Peano específico, uno de los más simples que cabe imaginar. Así, en lugar de tomar como 0 un cierto elemento de un cierto conjunto X en el que hay definida una cierta función S, definiremos $0 = \varnothing$. A su vez, el 1 no será la imagen de ese cierto conjunto llamado 0 por esa cierta función S, sino que tomaremos concretamente $1 = \{0\}$. En general, vamos a definir unos números naturales de modo que

$$\begin{array}{ll} 0 = \varnothing, & 6 = \{0,1,2,3,4,5\},\\ 1 = \{0\}, & 7 = \{0,1,2,3,4,5,6\},\\ 2 = \{0,1\}, & 8 = \{0,1,2,3,4,5,6,7\},\\ 3 = \{0,1,2\}, & 9 = \{0,1,2,3,4,5,6,7,8\},\\ 4 = \{0,1,2,3\}, & \cdots \end{array}$$

La ventaja de esta construcción, además de su simplicidad estructural, es que se generalizará de forma inmediata hasta el concepto de "número ordinal", que es el que, como hemos indicado, será el objeto central de este capítulo.

Trabajaremos en NBG*, sin suponer el axioma de infinitud o el axioma de partes salvo que lo indiquemos explícitamente.

3.1 La construcción de los ordinales

El primer paso para formalizar la construcción de los números naturales que acabamos de esbozar es el siguiente:

Definición 3.1 Llamaremos $0 \equiv \varnothing$ y, para toda clase x, definimos

$$x' \equiv x \cup \{x\}.$$

Definimos $1 \equiv 0' = \{0\}$, $2 \equiv 1' = \{0, 1\}$, $3 \equiv 2' = \{0, 1, 2\}$, etc.

El etcétera final significa que, prosiguiendo del mismo modo, podemos definir el 4 y el 5 y el 10 472, pero por mucho que prolonguemos las definiciones de números naturales particulares, eso no nos va a proporcionar una definición de "número natural", es decir, una propiedad definida exclusivamente a partir de $\in$ y los signos lógicos (o de propiedades definidas previamente a partir de estos signos básicos) que nos permita definir por comprensión la clase de los números naturales. Para ello "etc." resulta inadmisible porque no está definido a partir de $\in$ y de los signos lógicos.

Presentamos a continuación una lista de propiedades comunes a todos los números naturales que sabemos definir individualmente:

Una clase Y es *transitiva* si cumple

$$Y \text{ transitiva} \equiv \bigwedge x \in Y \; x \subset Y$$

o, equivalentemente (y de aquí el nombre) $\bigwedge uv(u \in v \wedge v \in Y \to u \in Y)$.

Una clase Y es $\in$-*conexa* si cumple

$$\in\text{-conexa } Y \equiv \bigwedge uv \in Y(u \in v \vee v \in u \vee u = v).$$

Una clase Y está *bien fundada* si cumple

$$Y \text{ bien fundada} \equiv \bigwedge X(X \subset Y \wedge X \neq \varnothing \to \bigvee u \in X \; u \cap X = \varnothing).$$

Un conjunto u que cumpla $u \in X \wedge u \cap X = \varnothing$ se llama un $\in$-*minimal* de X, de modo que la buena fundación afirma que toda subclase no vacía de Y tiene al menos un $\in$-minimal. Observemos que u es un $\in$-minimal de X si $u \in X$ y ningún $v \in u$ cumple $v \in X$.

Ciertamente, los números naturales que queremos definir cumplen estas propiedades. Son transitivos, pues, si, por ejemplo, $4 \in 7$, se cumple también que

$4 = \{0, 1, 2, 3\} \subset \{0, 1, 2, 3, 4, 5, 6\} = 7$, y esto no se cumple casualmente en este ejemplo, sino que vale en todos los casos.[1]

En cuanto a la conexión, si por ejemplo tomamos $3, 7 \in 9$, ciertamente se cumple que $3 \in 7$ y, en general, si tomamos dos elementos distintos de un número natural, el menor pertenecerá al mayor. Por lo tanto, los números naturales son $\in$-conexos.

También están bien fundados, pues si tomamos un número natural, por ejemplo 8 y un subconjunto no vacío, por ejemplo $X = \{3, 5, 6\}$, se cumple que X tiene un $\in$-minimal, concretamente $u = 3$, pues ciertamente $3 \in X$, pero ningún $v \in 3$ cumple $v \in X$. De hecho, vemos que cada subconjunto no vacío de un número natural tiene un único $\in$-minimal, a saber, el mínimo número natural que contiene.

El lector debe entender que la cuestión aquí no es demostrar si realmente, lo que hemos constatado con ejemplos particulares vale para todos los números naturales, sino más bien si podemos definir un número natural como un conjunto transitivo, $\in$-conexo y bien fundado, o si, por el contrario, existen conjuntos con estas tres propiedades que no tienen nada que ver con los conjuntos 0, 1, 2, ..., de modo que necesitamos introducir más propiedades para quedarnos únicamente con los números naturales. Como respuesta provisional damos una nueva definición:

Definición 3.2 Una clase Y es un *ordinal* si es transitiva, $\in$-conexa y bien fundada. Llamaremos Ω a la clase de todos los (conjuntos) ordinales.

Observemos que la propiedad "Y es un conjunto y es un ordinal" es normal. El único punto problemático es la definición de clase bien fundada, que incluye una cuantificación sobre toda subclase de Y, pero si Y es un conjunto, es lo mismo decir "para toda clase X, si $X \subset Y \cdots$ " que decir "para todo conjunto X, si $X \subset Y \cdots$ ", porque toda subclase de un conjunto es un conjunto. Por consiguiente

$$\Omega \equiv \{\alpha \mid \mathrm{cto}\,\alpha \wedge \mathrm{ordinal}\,\alpha\}$$

es una aplicación válida del axioma de comprensión.

Así pues, en estos términos la pregunta que nos hacíamos es si existen ordinales que no sean (o no deban ser considerados como) números naturales. En cualquier caso, lo cierto es que los números naturales que pretendemos definir son ordinales, luego al estudiar los ordinales estamos estudiando en particular los números naturales, con la diferencia de que los ordinales los tenemos correctamente definidos mediante una propiedad del lenguaje de la teoría de conjuntos.

[1] No vamos a demostrar que todo número natural es transitivo, en parte porque para ello necesitaríamos una definición de número natural que no tenemos, y en parte porque usaremos la transitividad como parte de la definición de número natural. Lo mismo vale para las otras dos propiedades que estamos considerando.

Empezamos observando que, trivialmente, toda subclase de una clase $\in$-conexa o bien fundada es también $\in$-conexa o bien fundada, pero no podemos decir lo mismo de las clases transitivas (pensemos, por ejemplo, en $\{3,5\} \subset 7$). Veamos ahora un resultado técnico sencillo sobre clases bien fundadas:

Teorema 3.3 *Si x es una clase bien fundada entonces*[2] $x \notin x$.

DEMOSTRACIÓN: Si $x \in x$ entonces x es un conjunto y $\{x\} \subset x \wedge \{x\} \neq \varnothing$. Sea u un elemento $\in$-minimal de $\{x\}$. Necesariamente, $u = x$, pero $x \in x \cap \{x\}$, contradicción. ∎

Con esto podemos probar:

Teorema 3.4 $0 \in \Omega \wedge \bigwedge x \in \Omega\ x' \in \Omega$.

DEMOSTRACIÓN: Notemos que $0 = \varnothing$ cumple trivialmente las tres condiciones de la definición de ordinal (es transitivo porque no existe ningún $u \in \varnothing$ que pueda incumplir la definición, es $\in$-conexo porque no existen $u, v \in \varnothing$ que puedan incumplir la definición, y está bien fundado porque no existe ningún $u \subset \varnothing$, $u \neq \varnothing$ que pueda incumplir la definición).

Supongamos ahora que x es un ordinal. Si $u \in x' = x \cup \{x\}$, entonces $u \in x \vee u = x$, pero en ambos casos $u \subset x$, en el primero porque x es transitivo. Esto prueba que x' es transitivo.

Si $u, v \in x'$, entonces $u \in x \vee u = x$ y $v \in x \vee v = x$. Esto nos da cuatro casos: $u \in x \wedge v \in x$ o bien $u \in x \wedge v = x$, o bien $u = x \wedge v \in x$, o bien $u = x = v$. En el primero tenemos que $u \in v \vee v \in u \vee u = v$ porque x es $\in$-conexo, y en los otros tres tenemos $u \in v$, $v \in u$, $u = v$ respectivamente. Esto prueba que x' es $\in$-conexo.

Tomemos $u \subset x' \wedge u \neq \varnothing$ y veamos que tiene $\in$-minimal. Tratemos aparte el caso en que $u = \{x\}$. Entonces $v = x$ es un $\in$-minimal de u, pues $x \cap \{x\} = \varnothing$. En efecto, si existiera $w \in x \cap \{x\}$, sería $x = w \in x$, en contradicción con el teorema anterior.

Como $u \subset x \cup \{x\}$, si no se da la igualdad $u = \{x\}$ es porque $u \cap x \neq \varnothing$, y tenemos así un subconjunto no vacío de x. Como x está bien fundado existe un $v \in u \cap x$ que es $\in$-minimal para esta intersección. Vamos a ver que es $\in$-minimal de u.

En efecto, si $w \in v \cap u$, entonces $w \in x'$, luego $w \in x \vee w = x$. En el primer caso $w \in u \cap x$ y $w \in v$, lo que contradice que v sea $\in$-minimal de $u \cap x$. En el segundo caso $x = w \in v \in x$, luego, por la transitividad de x, resulta que $x \in x$, en contradicción con el teorema anterior. ∎

En vista de este teorema resulta que 0 es un ordinal, luego $1 = 0'$ es un ordinal, luego $2 = 1'$ es un ordinal y, en definitiva, todos los números naturales

[2] Quizá el lector se pregunte si es posible que una clase (necesariamente un conjunto) cumpla $x \in x$. Nos falta presentar tres axiomas de NBG, uno de los cuales, el axioma de regularidad, afirma precisamente que toda clase está bien fundada, luego, bajo dicho axioma, no puede darse el caso. No obstante, en su momento discutiremos debidamente la situación.

son ordinales, pero no podemos demostrar tal cosa porque no tenemos una definición de número natural.

Observemos que los elementos de los números naturales (que pretendemos definir) son también números naturales. De momento podemos probar que esto es cierto para ordinales:

Teorema 3.5 *Los elementos de los ordinales son ordinales.*

DEMOSTRACIÓN: Sea Y un ordinal y sea $x \in Y$. Por transitividad $x \subset Y$ y por consiguiente x es conexo y bien fundado. Falta probar que es transitivo, es decir, que $\bigwedge uv(u \in v \wedge v \in x \to u \in x)$.

Si $u \in v \wedge v \in x$, tenemos $v \in x \wedge x \in Y$, y como la clase Y es transitiva, $v \in Y$, e igualmente $u \in Y$. Así pues, $\{u, v, x\} \subset Y$. Como Y está bien fundada se cumplirá uno de los tres elementos del subconjunto tiene que ser $\in$-minimal, es decir,

$$u \cap \{u, v, x\} = \varnothing \quad \vee \quad v \cap \{u, v, x\} = \varnothing \quad \vee \quad x \cap \{u, v, x\} = \varnothing,$$

pero $u \in v \cap \{u, v, x\}$ y $v \in x \cap \{u, v, x\}$, luego ha de ser $u \cap \{u, v, x\} = \varnothing$. Como Y es conexa ha de ser $u \in x \vee x \in u \vee u = x$, pero si $x \in u$ entonces $x \in u \cap \{u, v, x\} = \varnothing$, y si $x = u$ entonces $v \in u \cap \{u, v, x\} = \varnothing$. Así pues, se ha de cumplir $u \in x$, como queríamos. ∎

En particular vemos que

$$\bigwedge \alpha\beta(\alpha \in \beta \wedge \beta \in \Omega \to \alpha \in \Omega),$$

pero esto es tanto como decir que la clase Ω es transitiva.

Nuestra observación siguiente es que, para los números naturales que pretendemos definir, la relación de orden usual se corresponde con la inclusión, es decir, es lo mismo $3 \leq 7$ que $3 \subset 7$. Veamos ahora que la inclusión define un buen orden en cualquier ordinal:

Teorema 3.6 *Si Y es un ordinal, entonces la relación de inclusión es un buen orden en Y.*

DEMOSTRACIÓN: Sea Y un ordinal, y consideramos la relación en Y dada por $u \leq v \leftrightarrow u \subset v$. Sabemos que, en general, se trata de una relación de orden parcial. Vamos a probar que toda subclase $X \subset Y$ no vacía tiene mínimo elemento. Más concretamente, tomamos un $\in$-minimal $u \in X$ cualquiera y vamos a ver que es el mínimo de X (lo que, en particular, implica que cada subclase no vacía de un ordinal tiene un único $\in$-minimal).

Si tomamos cualquier otro $v \in X$, tenemos que $u, v \in Y$, luego por la conexión tiene que ser $u \in v \vee v \in u \vee u = v$, pero el caso $v \in u$ contradice la minimalidad de u, luego nos queda $u \in v \vee u = v$, y en ambos casos $u \subset v$ (en el primero porque v es un ordinal, luego es transitivo). Así pues $u \leq v$ para todo $v \in X$. Esto es lo que significa que u sea el mínimo de X. ∎

A continuación notamos que la relación de orden estricto en los números naturales se corresponde con la pertenencia, es decir, que $3 < 7$ es lo mismo que $3 \in 7$. El teorema siguiente demuestra este hecho para ordinales:

Teorema 3.7 *Si X, Y son ordinales, entonces $X \subset Y \leftrightarrow X \in Y \vee X = Y$.*

Demostración: Una implicación es trivial, pues si $X \in Y$ entonces $X \subset Y$ por transitividad. Supongamos ahora que $X \subset Y$ pero $X \neq Y$ y veamos que $X \in Y$.

Tenemos que $Y \setminus X \neq \varnothing$, luego por la buena fundación esta clase tiene un $\in$-minimal $u \in Y \setminus X$. Basta probar que $u = X$.

Si $z \in u$, entonces $z \notin Y \setminus X$ (por la minimalidad de u) y $z \in Y$ (por transitividad, pues $z \in u \in Y$), luego $z \in X$. Por lo tanto $u \subset X$.

Si $z \in X$, entonces tenemos $z, u \in Y$, luego $z \in u \vee u \in z \vee z = u$. Si $u \in z$, entonces $u \in z \in X$, luego $u \in X$, contradicción (pues $u \in Y \setminus X$). Si $z = u$ entonces de nuevo $u \in X$, contradicción. Por lo tanto $z \in u$, y así $X \subset u$. En definitiva, tenemos la igualdad $u = X$. ∎

Ahora necesitamos un sencillo resultado técnico:

Teorema 3.8 *La intersección de dos ordinales es un ordinal.*

Demostración: Sean X, Y ordinales. Como $X \cap Y \subset X$, trivialmente la clase $X \cap Y$ es conexa y bien fundada. Falta ver que es transitiva, pero es cierto en general que la intersección de clases transitivas es transitiva:

Si $u \in X \cap Y$, entonces $u \in X \wedge u \in Y$, $u \subset X \wedge u \subset Y$, luego $u \subset X \cap Y$. ∎

De aquí deducimos una propiedad nada trivial:

Teorema 3.9 *Si X e Y son ordinales, entonces $X \in Y \vee Y \in X \vee X = Y$.*

Demostración: $X \cap Y$ es un ordinal, $X \cap Y \subset X$ y $X \cap Y \subset Y$. Por el teorema 3.7 tenemos $(X \cap Y \in X \vee X \cap Y = X) \wedge (X \cap Y \in Y \vee X \cap Y = Y)$. Esto nos da cuatro casos:

$$(X \cap Y \in X \wedge X \cap Y \in Y) \vee (X \cap Y \in X \wedge X \cap Y = Y)$$

$$\vee (X \cap Y = X \wedge X \cap Y \in Y) \vee (X \cap Y = X \wedge X \cap Y = Y),$$

o sea $X \cap Y \in X \cap Y \quad \vee \quad Y \in X \quad \vee \quad X \in Y \quad \vee \quad X = Y$. El primer caso se descarta por el teorema 3.3. ∎

Notemos que, en principio, la definición de ordinal dice que dos elementos de un mismo ordinal están conectados por la relación de pertenencia, pero lo que acabamos de probar es que dos ordinales cualesquiera, que en principio no tienen ninguna relación entre sí, también están conectados por la relación de pertenencia, y uno tiene que ser un elemento del otro salvo que sean el mismo. En particular,

$$\bigwedge \alpha\beta \in \Omega\ (\alpha \in \beta \vee \beta \in \alpha \vee \alpha = \beta),$$

luego la clase Ω es $\in$-conexa (y ya habíamos probado que era transitiva). De hecho, se cumple algo más fuerte:

Teorema 3.10 *Ω es un ordinal.*

DEMOSTRACIÓN: Ya hemos probado que Ω es transitiva y $\in$-conexa. Sólo falta probar que está bien fundada. Para ello tomamos una clase $X \subset \Omega$ no vacía, y vamos a encontrarle un $\in$-minimal. Tomemos cualquier $u \in X$. Si ya es un $\in$-minimal, no hay nada que probar. En caso contrario $u \cap X \neq \varnothing$ y $u \cap X \subset u$. Como $u \in \Omega$, es un ordinal y está bien fundado, luego $u \cap X$ tiene un $\in$-minimal v, es decir, $v \in u \cap X$ y $v \cap u \cap X = \varnothing$.

Ahora bien, como $v \in u$, por transitividad $v \subset u$, de donde concluimos que $v \cap X = v \cap u \cap X = \varnothing$. Además $v \in X$, luego v es un $\in$-minimal de X. ∎

Con esto termina el "trabajo duro" de la construcción de los ordinales, y podemos empezar a extraer consecuencias:

Teorema 3.11 *Ω es una clase propia.*

DEMOSTRACIÓN: Si Ω fuera un conjunto, puesto que es un ordinal, tendríamos que $\Omega \in \Omega$, en contradicción con el teorema 3.3. ∎

Así pues, la clase de todos los (conjuntos) ordinales es un ordinal que no es un conjunto. Seguidamente probamos que es el único caso:

Teorema 3.12 *Si Y es un ordinal, o bien $Y \in \Omega$, o bien $Y = \Omega$.*

DEMOSTRACIÓN: Basta aplicar el teorema 3.9, que nos da en principio las opciones $Y \in \Omega \vee \Omega \in Y \vee Y = \Omega$, pero la segunda es imposible, pues implica que Ω es un conjunto. ∎

Definición 3.13 Llamaremos *números ordinales* a los elementos de Ω, es decir, a los conjuntos que son ordinales. En lo sucesivo usaremos letras griegas minúsculas para referirnos a los números ordinales, de modo que $\bigwedge\alpha$ o $\bigvee\alpha$ deberá entenderse como $\bigwedge\alpha \in \Omega$ o $\bigvee\alpha \in \Omega$, respectivamente.

Llamaremos $\leq$ a la inclusión en Ω, de modo que, según el teorema 3.6, sabemos que $(\Omega, \leq)$ es una clase bien ordenada. Así pues, $\alpha \leq \beta$ es equivalente a $\alpha \subset \beta$.

El teorema 3.7 implica que la relación de orden estricto asociada a $\leq$ es equivalente a la pertenencia, es decir, que $\alpha < \beta$ es equivalente a $\alpha \in \beta$. (Aquí hay que tener en cuenta que no puede suceder a un tiempo $\alpha \in \beta$ y $\alpha = \beta$, pues entonces tendríamos $\alpha \in \alpha$.)

El teorema siguiente recoge los hechos básicos sobre el buen orden de los ordinales:

Teorema 3.14 *Se cumple:*

1. *0 es el mínimo ordinal.*
2. *Si α es un ordinal, entonces α' también lo es, y es el mínimo ordinal mayor que α (es decir, $\bigwedge\beta \in \Omega\ (\alpha < \beta \to \alpha' \leq \beta)$).*
3. *Todo conjunto de ordinales $A \subset \Omega$ tiene supremo $\sigma = \bigcup A$.*

DEMOSTRACIÓN: 1) ya hemos probado que 0 es un ordinal, y es el mínimo porque el conjunto vacío está contenido en cualquier conjunto.

2) Ya hemos probado que $\alpha' \in \Omega$. Si $\alpha < \beta$ entonces $\alpha \in \beta$, luego $\alpha \subset \beta$, luego $\alpha' = \alpha \cup \{\alpha\} \subset \beta$, luego $\alpha' \leq \beta$.

3) Como todo $\alpha \in A$ está contenido en Ω, es claro que $\sigma \subset \Omega$, luego es un conjunto conexo y bien fundado. Hemos de probar que es transitivo, pero si $\beta \in \sigma$, entonces existe un $\alpha \in A$ tal que $\beta \in \alpha$, luego por la transitividad de α es $\beta \subset \alpha \subset \sigma$. Por consiguiente $\sigma \in \Omega$. Teniendo en cuenta que el orden es la inclusión, es inmediato que σ es el supremo de A. ∎

Volvemos ahora a la cuestión de si hay ordinales que no sean números naturales (aparte de Ω). Para ello introducimos los conceptos siguientes:

Definición 3.15 Un ordinal $\alpha \in \Omega$ es un *ordinal sucesor* si $\bigvee \beta < \alpha\ \alpha = \beta'$, y es un *ordinal límite* si no es 0 ni un ordinal sucesor, es decir, si cumple

$$\alpha \text{ límite} \equiv 0 \in \alpha \wedge \bigwedge \delta \in \alpha\ \delta' \in \alpha.$$

Trivialmente entonces, todo $\alpha \in \Omega$ está en uno (y sólo uno) de los tres casos siguientes: o bien es $\alpha = 0$, o bien es un ordinal sucesor, o bien es un ordinal límite. Usaremos la letra λ para referirnos a ordinales límite, de modo que $\bigwedge \lambda$ y $\bigvee \lambda$ significarán, respectivamente, "para todo ordinal límite λ" y "existe un ordinal límite λ".

Ahora bien, ¿existen ordinales límite? Ciertamente, los números naturales distintos de 0 son ordinales sucesores, luego la existencia de un ordinal límite implica la existencia de un número ordinal que no es un número natural. Antes de entrar en este asunto observamos que ya podemos cumplir el objetivo que nos habíamos marcado:

Definición 3.16 Diremos que un conjunto n es un *número natural* si

$$n \in \Omega \wedge \bigwedge m \in \Omega(m \leq n \to m = 0 \vee \bigvee r \in m\ m = r').$$

Llamaremos ω a la clase de todos los números naturales.

Así pues, hemos definido un número natural como un ordinal tal que los ordinales no nulos menores o iguales son todos sucesores. Enseguida discutiremos si la definición es razonable, pero antes observamos lo siguiente:

Teorema 3.17 *ω es un ordinal.*

DEMOSTRACIÓN: Como $\omega \subset \Omega$, es trivialmente una clase $\in$-conexa y bien fundada, y basta ver que es transitiva. Si $u \in v \wedge v \in \omega$, entonces v es un número natural y u es un ordinal $u < v$, luego todos los ordinales no nulos $m \leq u$ son ordinales no nulos $m \leq v$, luego, al ser v un número natural, todos ellos son sucesores, lo que significa que u también es un número natural, luego $u \in \omega$. ∎

Nuestra definición de número natural está justificada por el teorema siguiente:

Teorema 3.18 (Axiomas de Peano) *Se cumple:*

1. $0 \in \omega$,
2. $\bigwedge n \in \omega\ n' \in \omega$,
3. $\bigwedge n \in \omega\ n' \neq 0$,
4. $\bigwedge mn \in \omega\ (m' = n' \to m = n)$,
5. $\bigwedge A(A \subset \omega \wedge 0 \in A \wedge \bigwedge n \in A\ n' \in A \to A = \omega)$.

DEMOSTRACIÓN: 1) es trivial.

2) Si $n \in \omega$ y $\alpha \leq n'$, entonces, o bien $\alpha \in n'$ o bien $\alpha = n'$. En el primer caso $\alpha \leq n$, luego $\alpha = 0 \vee \bigvee \beta \in \alpha\, \alpha = \beta'$, porque $n \in \omega$. Esto también se cumple en el segundo caso, tomando $\beta = n$. Por consiguiente $n' \in \omega$.

Las propiedades 3) y 4) son trivialmente válidas para ordinales cualesquiera, pues $0 \leq n < n'$, luego $0 \in n'$, luego $n' \neq 0$. Por otra parte, si $m' = n'$, tiene que ser $m = n$, ya que si fuera $m < n$ entonces $m' \leq n < n'$, luego $m' \neq n'$, e igualmente si $n < m$.

5) Si $A \subset \omega \wedge 0 \in A \wedge \bigwedge n \in A\ n' \in A$ pero $A \neq \omega$, entonces, como hemos probado que Ω es un ordinal, existe un $\in$-minimal $n \in \omega \setminus A$. No puede ser $n = 0$, pues $0 \in A$, $n \notin A$. Como n es un número natural, por definición existe un $m \in n$ tal que $n = m'$. Como n es minimal, no puede ser que $m \in \omega \setminus A$, pues entonces $m \in n \cap (\omega \setminus A)$. Por lo tanto $m \in A$ (notemos que $m \in n \in \omega$, luego $m \in \omega$, por transitividad). Pero estamos suponiendo que $m \in A$ implica $n = m' \in A$, contradicción. ∎

En otras palabras, hemos probado que ω, con la aplicación $S : \omega \longrightarrow \omega$ dada por $S(n) = n'$ y con el número natural $0 = \varnothing$ es un sistema de Peano salvo por el hecho de que no sabemos si ω es o no un conjunto.

El hecho de que ω sea un ordinal sólo nos deja dos posibilidades: o bien $\omega = \Omega$, en cuyo caso no hay más ordinales que los números naturales y Ω y no existen ordinales límite, o bien $\omega \in \Omega$, en cuyo caso ω es un ordinal límite, por el segundo axioma de Peano. Más precisamente:

Teorema 3.19 *Las afirmaciones siguientes son equivalentes:*

1. *Existe un conjunto X con una aplicación $S : X \longrightarrow X$ inyectiva y no suprayectiva.*
2. $\bigvee x(\mathrm{cto}\, x \wedge 0 \in x \wedge \bigwedge u \in x\ u' \in x)$,
3. $\mathrm{cto}\, \omega$,
4. $\omega \in \Omega$,
5. *ω es un ordinal límite,*
6. *Existe un ordinal límite.*

DEMOSTRACIÓN: 1) es el axioma de infinitud a partir del cual hemos construido en el capítulo anterior un sistema de Peano $\mathbb{N}$. En virtud del principio de recursión podemos construir una aplicación $f : \mathbb{N} \longrightarrow \Omega$ determinada por que $f(0) = 0$ y $f(n+1) = f(n)'$. Es claro entonces que $f[\mathbb{N}]$ cumple 2).

Si x es un conjunto que cumple 2), entonces $y = x \cap \omega$ está en las condiciones del quinto apartado del teorema 3.18, que nos da que $x \cap \omega = \omega$, es decir, que $\omega \subset x$, luego ω es un conjunto y tenemos 3). A su vez, 3) implica trivialmente 4), que a su vez implica 5) por el segundo apartado del teorema 3.18. Obviamente 5) implica 6), y en un ordinal límite λ podemos definir la aplicación $S : \lambda \longrightarrow \lambda$ dada por $S(\delta) = \delta'$, que es inyectiva y no suprayectiva, luego se cumple 1). ∎

De este modo, cualquiera de las afirmaciones del teorema anterior puede tomarse añadirse a NBG* en calidad de axioma de infinitud. La versión 1) que hemos adoptado en el capítulo anterior es la que permite construir un sistema de Peano más rápidamente, mientras que 2) es la formalmente más simple y 3) la conceptualmente más simple. Aunque para nosotros va a ser irrelevante adoptar una u otra versión, vamos a destacar 2) como posible alternativa a 1):

Axioma de infinitud (AI) $\bigvee x(\mathrm{cto}\, x \wedge 0 \in x \wedge \bigwedge u \in x\ u' \in x)$.

Una consecuencia notable de la construcción de los números naturales como ordinales es que podemos trabajar con ellos hasta cierto punto sin necesidad de suponer el axioma de infinitud, así que de momento seguiremos trabajando en la teoría básica NBG*.

3.2 Inducción y recursión transfinita

Vamos a generalizar a ordinales los teoremas de inducción y recursión que en el capítulo anterior hemos probado para números naturales. Necesitaremos los resultados del apartado "Clases bien ordenadas" de la sección 1.6. Empezamos con el principio de inducción, que no es sino un caso particular del teorema 1.27:

Teorema 3.20 (Inducción transfinita)

$$\bigwedge A(\bigwedge \alpha(\alpha \subset A \to \alpha \in A) \to \Omega \subset A).$$

Es decir: si bajo la hipótesis de inducción de que todos los ordinales $\beta < \alpha$ pertenecen a una clase A podemos probar que $\alpha \in A$, entonces todo número ordinal está en A. La prueba es la misma que la de 1.27:

DEMOSTRACIÓN: Si no se cumpliera $\Omega \subset A$, entonces $\Omega \setminus A \neq \varnothing$, y debe existir un mínimo elemento $\alpha \in \Omega \setminus A$, pero esto significa que todo ordinal menor que α está en A, es decir, $\alpha \subset A$, luego la hipótesis nos da que $\alpha \in A$, contradicción. ∎

En la práctica aplicaremos este teorema a clases de la forma

$$A = \{\alpha \in \Omega \mid \phi(\alpha)\},$$

para cierta propiedad (normal) $\phi(x)$, de modo que lo que estamos afirmando es que si el hecho de que todos los ordinales menores que un α tienen la propiedad ϕ implica que α también la tiene, entonces todos los números ordinales tienen la propiedad ϕ.

A menudo el planteamiento de la inducción se simplifica si distinguimos casos según si $\alpha = 0$ (en cuyo caso la hipótesis de inducción es vacía), si α es un sucesor (en cuyo caso a menudo basta aplicar la hipótesis de inducción a su anterior) o si es un límite. Esto nos lleva al enunciado siguiente:

Teorema 3.21 (Inducción transfinita)

$$\bigwedge A(0 \in A \wedge \bigwedge \alpha(\alpha \in A \to \alpha' \in A)$$

$$\wedge \bigwedge \lambda(\bigwedge \delta(\delta < \lambda \to \delta \in A) \to \lambda \in A) \to \Omega \subset A).$$

En otras palabras, una forma alternativa de probar que todos los ordinales tienen una propiedad (cosa que puede expresarse como la pertenencia a una clase A) es probar que 0 la tiene, que si un ordinal α la tiene entonces también la tiene α', y que si todos los ordinales menores que un límite λ la tienen, también la tiene λ.

La prueba sigue el mismo argumento: si no fuera $\Omega \subset A$ la clase $\Omega \setminus A$ debería tener un mínimo elemento β, pero no puede ser $\beta = 0$ por la primera parte de la hipótesis, ni $\beta = \alpha'$ por la segunda (porque $\alpha < \beta$ estaría en A y entonces β también debería cumplir $\beta \in A$) ni puede ser un límite por la tercera, luego tenemos una contradicción.

Vemos así que los resultados de inducción son poco menos que triviales. La parte delicada es demostrar el teorema de recursión transfinita. Se trata de probar que para definir una función $F : \Omega \longrightarrow A$ podemos definir $F(\alpha)$ suponiendo que F ya está definida para los ordinales menores que α, es decir, usando los valores $F(\delta)$ con $\delta < \alpha$ para definir $F(\alpha)$ o, más precisamente, usando $F|_\alpha$ para definir $F(\alpha)$. Con exactitud:

Teorema 3.22 (Recursión transfinita) *Sea A una clase cualquiera, sea*

$$X \equiv \{f \mid \bigvee \alpha\ f : \alpha \longrightarrow A\}$$

y sea $G : X \longrightarrow A$. Entonces existe una única función $F : \Omega \longrightarrow A$ caracterizada por que $\bigwedge \alpha\, F(\alpha) = G(F|_\alpha)$.

Demostración: Diremos que $f : \beta \longrightarrow$ A es una *β-aproximación* si para todo $\alpha < \beta$ se cumple $f(\alpha) = G(f|_\alpha)$. Es claro que si existe una β-aproximación entonces es única. En efecto, supongamos que f y g son dos β-aproximaciones. Entonces sea $\alpha < \beta$ el mínimo ordinal en el que difieran (si es que existe). Esto significa que $f|_\alpha = g|_\alpha$, pero que $f(\alpha) \neq g(\alpha)$. Ahora bien, esto es absurdo, pues $f(\alpha) = G(f|_\alpha) = G(g|_\alpha) = g(\alpha)$.

Ahora veamos por inducción que existen β-aproximaciones para todo β.

Es claro que $\varnothing$ es trivialmente una 0-aproximación. Si $f : \alpha \longrightarrow \mathrm{A}$ es una α-aproximación, entonces $g = f \cup \{(\alpha, G(f))\}$ es una α'-aproximación. En efecto, tenemos que $g : \alpha' \longrightarrow \mathrm{A}$ y si $\beta < \alpha'$, o bien $\beta < \alpha$, en cuyo caso $g(\beta) = f(\beta) = G(f|_\beta) = G(g|_\beta)$, o bien $\beta = \alpha$, en cuyo caso $g(\beta) = G(f) = G(g|_\beta)$.

Finalmente, supongamos que existen δ-aproximaciones para todo $\delta < \lambda$ y veamos que existe una λ-aproximación.

Por la unicidad que hemos probado, para cada $\delta < \lambda$ existe una única δ-aproximación, a la que podemos dar nombre. Definimos:

$$f_\delta \equiv f | f \text{ es una } \delta\text{-aproximación},$$

y así $\bigwedge\delta(\delta < \lambda \to f_\delta$ es una δ-aproximación).

De la definición se sigue inmediatamente que si $\delta < \epsilon < \lambda$ entonces $f_\epsilon|_\delta$ es una δ-aproximación, luego la unicidad implica que $f_\epsilon|_\delta = f_\delta$. Esto implica que

$$f = \bigcup_{\delta<\lambda} f_\delta : \lambda \longrightarrow A,$$

y f es una λ-aproximación, pues si $\delta < \lambda$ entonces

$$f(\delta) = f_{\delta'}(\delta) = G(f_{\delta'}|_\delta) = G(f|_\delta).$$

Con esto hemos probado que existen α-aproximaciones para todo ordinal α. Por el mismo argumento que en el caso límite de la inducción podemos definir $f_\alpha : \alpha \longrightarrow \mathrm{A}$ como la única α aproximación y, de nuevo, la unicidad nos da que si $\alpha < \beta$ entonces $f_\beta|_\alpha = f_\alpha$, lo cual nos permite definir

$$F = \bigcup_{\alpha\in\Omega} f_\alpha : \Omega \longrightarrow \mathrm{A}.$$

Claramente F cumple lo pedido, y el mismo argumento que probaba la unicidad de las aproximaciones prueba que F es única. ∎

En realidad el teorema de recursión transfinita puede usarse para definir funciones sobre un ordinal γ cualquiera, no necesariamente Ω. En tal caso nos basta con que la función G esté definida sobre la clase

$$X_\gamma \equiv \{f \mid \bigvee\alpha < \gamma\ f : \alpha \longrightarrow A\}.$$

Dada $G : X_\gamma \longrightarrow A$, podemos extenderla a $G^* : X \longrightarrow A$ sin más que definir $G^*(f) = 0$ si $f \notin X_\gamma$, obtener $F^* : \Omega \longrightarrow A$ por el teorema anterior, y tomar $F = F^*|_\gamma : \gamma \longrightarrow A$. Es fácil ver que F es la única función que cumple

$$\bigwedge\alpha < \gamma\ F(\alpha) = G(F|_\alpha).$$

Enunciamos ahora un caso particular del teorema de recursión que nos será útil para construir la aritmética ordinal:

Teorema 3.23 *Sea $\beta \in \Omega$ y $H : \Omega \longrightarrow \Omega$. Entonces existe una única aplicación $F : \Omega \longrightarrow \Omega$ caracterizada por:*

$$F(0) = \beta \quad \wedge \quad \bigwedge\alpha\, F(\alpha') = H(F(\alpha)) \quad \wedge \quad \bigwedge\lambda\, F(\lambda) = \bigcup_{\delta<\lambda} F(\delta).$$

DEMOSTRACIÓN: Basta tomar como $G : X \longrightarrow \Omega$ la función dada por

$$G(f) = \begin{cases} \beta & \text{si } \mathcal{D}f = 0, \\ H(f(\alpha)) & \text{si } \mathcal{D}f = \alpha', \\ \bigcup\limits_{\delta<\lambda} f(\delta) & \text{si } \mathcal{D}f = \lambda. \end{cases}$$

La función $F : \Omega \longrightarrow \Omega$ dada por el teorema de recursión cumple lo pedido, pues

$$F(0) = G(F|_0) = \beta,$$
$$F(\alpha') = G(F|_{\alpha'}) = H(F|_{\alpha'}(\alpha)) = H(F(\alpha)),$$
$$F(\lambda) = G(F|_\lambda) = \bigcup_{\delta<\lambda} F|_\lambda(\delta) = \bigcup_{\delta<\lambda} F(\delta).$$

La unicidad se debe a que si F^* cumple lo mismo, entonces una simple inducción prueba que $\bigwedge\alpha\ F(\alpha) = F^*(\alpha)$. En efecto, se cumple que $F(0) = \beta = F^*(0)$, supuesto que $F(\alpha) = F^*(\alpha)$ se cumple que

$$F(\alpha') = H(F(\alpha)) = H(F^*(\alpha)) = F^*(\alpha')$$

y si se cumple $\bigwedge\delta < \lambda\ F(\delta) = F^*(\delta)$, entonces

$$F(\lambda) = \bigcup_{\delta<\lambda} F(\delta) = \bigcup_{\delta<\lambda} F^*(\delta) = F^*(\lambda).$$

■

3.3 Ordinales y buenos órdenes

En principio, la definición que hemos dado de número ordinal como conjunto transitivo $\in$-conexo y bien fundado es arbitraria, pero vamos a probar que el concepto que obtenemos con ella tiene un significado intrínseco que no depende de la forma en que hemos elegido definirlo. Vamos a probar que los ordinales representan todas las formas posibles de ordenar bien un conjunto:

Teorema 3.24 *Todo conjunto bien ordenado es semejante a un único ordinal.*

DEMOSTRACIÓN: La unicidad se debe a que si un mismo conjunto bien ordenado fuera semejante a dos ordinales, éstos serían semejantes entre sí, luego basta probar que dos ordinales semejantes tienen que ser iguales. Ello se debe a que si $\alpha < \beta$, entonces $\alpha = \beta^<_\alpha$, y el teorema 1.29 implica que α y β no son semejantes.

Consideremos ahora un conjunto bien ordenado $(A, \leq)$ y vamos a ver que es semejante a un ordinal. Si $A = \varnothing$ el resultado es trivial, pues de hecho A es

un ordinal. Supongamos que $A \neq \varnothing$ y sea m el mínimo de A. Definimos una aplicación $G : X \longrightarrow A$ mediante

$$G(f) = \begin{cases} \text{mín}(A \setminus \mathcal{R}f) & \text{si } A \setminus \mathcal{R}f \neq \varnothing, \\ m & \text{si } A = \mathcal{R}f. \end{cases}$$

Sea $F : \Omega \longrightarrow A$ la aplicación dada por el teorema de recursión, de modo que[3]

$$\bigwedge\alpha\ F(\alpha) = \begin{cases} \text{mín}(A \setminus F[\alpha]) & \text{si } F[\alpha] \subsetneq A, \\ m & \text{si } F[\alpha] = A. \end{cases}$$

La aplicación F no puede ser inyectiva, pues en tal caso A sería una clase propia. Por consiguiente, existen ordinales $\beta < \alpha$ tales que $F(\beta) = F(\alpha)$. Podemos tomar el mínimo ordinal α para el cual existe un $\beta < \alpha$ con la misma imagen. De este modo, $f = F|_\alpha : \alpha \longrightarrow A$ inyectiva.

Además f es suprayectiva, ya que si $F[\alpha] \neq A$ sería $F(\alpha) \in A \setminus F[\alpha]$, cuando estamos suponiendo que $F(\alpha) = F(\beta) \in F[\alpha]$. Así pues, f es biyectiva.

Para probar que es una semejanza basta ver que para todo $\gamma < \alpha$ se cumple que $f[\gamma] = \{u \in A \mid u < f(\gamma)\}$, pues entonces, si si $\delta < \gamma < \alpha$ tenemos que $f(\delta) \in f[\gamma]$, luego se cumple $f(\delta) < f(\gamma)$ y así f es una semejanza.

Lo probamos por inducción. Supongamos que se cumple para todo $\delta < \gamma$. Entonces, si $u < f(\gamma)$, por definición de f ha de ser $u \in f[\gamma]$. Recíprocamente, si $u \in f[\gamma]$, entonces $u = f(\delta)$, para un $\delta < \gamma$. Todo $v < u$ cumple $v < f(\delta)$ luego, por hipótesis de inducción, $v \in f[\delta] \subset f[\gamma]$. Vemos, pues, que todo $v \leq u$ cumple $v \in f[\gamma]$ y, como $f(\gamma) \notin f[\gamma]$, ha de ser $u < f(\gamma)$. ∎

Definición 3.25 Llamaremos *ordinal* de un conjunto bien ordenado $(A, \leq)$ al único ordinal al cual es semejante. Lo representaremos por $\text{ord}(A, \leq)$.

Conviene recordar que, por el teorema 1.29, si $\text{ord}(A, \leq) = \alpha$, existe una única semejanza $f : (A, \leq) \longrightarrow \alpha$. Otra observación elemental es la siguiente:

Teorema 3.26 *Si B es un conjunto bien ordenado y $A \subset B$, entonces se cumple que* $\text{ord}\, A \leq \text{ord}\, B$.

Demostración: Sean $\alpha = \text{ord}\, A$, $\beta = \text{ord}\, B$ y consideremos las semejanzas $f : A \longrightarrow \alpha$ y $g : B \longrightarrow \beta$. Si fuera $\beta < \alpha$ tendríamos que $f^{-1} \circ g : \alpha \longrightarrow \beta$ sería estrictamente creciente, en contradicción con 1.29. ∎

Si una clase propia bien ordenada es semejante a un ordinal, ha de ser semejante a Ω, pues es el único ordinal que es una clase propia, pero esto no tiene por qué ser cierto. El teorema siguiente nos da una condición necesaria y suficiente para que así sea:

[3] En lo sucesivo no explicitaremos la función G con la que aplicamos el teorema de recursión, sino que nos limitaremos a definir $F(\alpha)$ en términos de $F|_\alpha$, o de cualquier concepto deducible de $F|_\alpha$, como es en este caso $F[\alpha] = \mathcal{R}F|_\alpha$. La función G considerada siempre se puede deducir de la definición recurrente.

Teorema 3.27 *Una clase propia A bien ordenada es semejante a Ω si y sólo si, para todo $u \in A$, la sección inicial $A_u^<$ es un conjunto.*

DEMOSTRACIÓN: La condición es claramente necesaria: si existe una semejanza $F : A \longrightarrow \Omega$ y $F(u) = \alpha$, entonces $F[A_u^<] = \Omega_\alpha^< = \alpha$, luego $A_u^<$ ha de ser un conjunto, pues toda clase biyectable con un conjunto es un conjunto, por reemplazo.

Si se cumple la condición, para cada $u \in A$ tenemos que $A_u^<$ es un conjunto bien ordenado, luego podemos considerar su ordinal α_u. Sea $f_u : A_u^< \longrightarrow \alpha_u$ la (única) semejanza entre ellos.

Si $u < v$ es fácil ver que[4] $f_v[A_u^<] = (\alpha_v)^<_{f_v(u)} = f_v(u)$. Así pues, tenemos que $f_v|_{A_u^<} : A_u^< \longrightarrow f_v(u)$ es una semejanza y, por la unicidad, $\alpha_u = f_v(u)$ y $f_v|_{A_u^<} = f_u$. Esto significa que dos funciones f_u y f_v coinciden en su dominio común.

Observemos ahora que A no puede tener un máximo elemento, pues si M fuera el máximo de A, entonces $A_M^< = A \setminus \{M\}$ sería un conjunto, luego A también sería un conjunto. Esto implica que

$$A = \bigcup_{v \in A} A_v^<$$

y, por consiguiente, si definimos $F = \bigcup_{v \in A} F_v$, se cumple que $F : A \longrightarrow \Omega$. Notemos que F es simplemente la función que a cada $u \in A$ le asigna su imagen por cualquiera de las funciones f_v definidas sobre u. No importa cuál tomemos, pues todas dan el mismo valor.

Se cumple que F es inyectiva y creciente, pues si $u < u'$ son elementos de A, como no hay máximo, existe un $v \in A$ tal que $u < u' < v$, luego se cumple que $F(u) = f_v(u) < f_v(u') = F(u')$. Por último, F es suprayectiva, pues claramente $F[\Omega] = \bigcup_{v \in A} \alpha_v$, que es claramente un ordinal (es una subclase transitiva de Ω), pero no puede ser un conjunto, ya que entonces A sería un conjunto, luego $F[\Omega] = \Omega$. Concluimos que F es una semejanza. ∎

Ejemplo Sea M un conjunto que no sea un ordinal (por ejemplo, $M = \{1\}$), sea $\Omega^* = \Omega \cup \{M\}$ y consideremos el orden en Ω^* dado por

$$x \leq^* y \leftrightarrow (x, y \in \Omega \wedge x \leq y) \vee y = M.$$

Es fácil ver que $(\Omega^*, \leq^*)$ es una clase bien ordenada con M como máximo elemento. Esto implica a su vez que $(\Omega^*)_M^< = \Omega$, luego, por el teorema anterior no es semejante a Ω (ni mucho menos a un número ordinal). ∎

[4]En general, si $F : A \longrightarrow B$ es una semejanza entre clases parcialmente ordenadas y $a \in A$, es fácil ver que $F[A_a^<] = B^<_{F(a)}$. Esto es un caso particular del hecho de que las semejanzas conservan todas las propiedades relacionadas con los órdenes implicados.

La antinomia de Burali-Forti Del mismo modo que el hecho de que la clase de Russell R no es un conjunto "resuelve" la paradoja de Russell en NBG, el hecho de que la clase Ω no sea un conjunto "resuelve" la llamada *antinomia de Burali-Forti,* que es otra de las paradojas a las que daba lugar la teoría de conjuntos cantoriana.

Cantor concebía los ordinales de forma distinta a como los hemos construido, pero demostraba el "conjunto" O de todos los ordinales estaba bien ordenado, y si α era un ordinal cualquiera, entonces $\operatorname{ord} O^<_\alpha = \alpha$. El problema surgía al considerar $\Omega = \operatorname{ord} O$, es decir, el ordinal del "conjunto" de todos los ordinales, pues la propiedad anterior implicaba que todo ordinal α cumple $\alpha < \Omega$, pero en particular, tendría que ser $\Omega < \Omega$. Más aún, también podía probarse que todo ordinal tiene un siguiente, de modo que, por una parte, debería ser $\Omega < \Omega'$ y, por otra, como todo ordinal, Ω' debería cumplir $\Omega' < \Omega$.

En nuestro contexto no hay contradicción alguna, porque todo conjunto bien ordenado (no toda clase) es semejante a un ordinal, y esto no se aplica a la clase Ω de todos los conjuntos. La clase bien ordenada Ω^* del ejemplo anterior "debería" tener por ordinal al ordinal siguiente de Ω, pero no existe tal ordinal, y no hay contradicción en ello, pues ningún teorema afirma que deba existir. ∎

Ejemplo Consideremos en $\Omega \times \Omega$ el orden lexicográfico, es decir, el dado por

$$(\alpha, \beta) \leq (\gamma, \delta) \leftrightarrow \beta < \delta \vee (\beta = \delta \wedge \alpha \leq \gamma).$$

Es fácil ver que $\Omega \times \Omega$ es una clase bien ordenada, pero no es semejante a Ω, ya que todos los pares $(\alpha, 0)$ son menores que el par $(0, 1)$, luego tenemos una aplicación inyectiva $\Omega \longrightarrow (\Omega \times \Omega)_{(0,1)}$, luego esta sección no es un conjunto. ∎

En cambio, con una ligera modificación del orden obtenemos otro que sí que es semejante a Ω:

Definición 3.28 Definimos el *orden canónico* en $\Omega \times \Omega$ como el orden dado por

$$(\alpha, \beta) \leq (\gamma, \delta) \leftrightarrow \operatorname{máx}\{\alpha, \beta\} < \operatorname{máx}\{\gamma, \delta\} \vee$$

$$(\operatorname{máx}\{\alpha, \beta\} = \operatorname{máx}\{\gamma, \delta\} \wedge \beta < \delta) \vee$$

$$(\operatorname{máx}\{\alpha, \beta\} = \operatorname{máx}\{\gamma, \delta\} \wedge \beta = \delta \wedge \alpha \leq \gamma).$$

Es decir, para comparar dos pares, primero comparamos sus máximas componentes, en caso de empate comparamos las de la derecha y si de nuevo hay empate comparamos las de la izquierda. Es fácil comprobar que es un buen orden, y sus secciones iniciales son conjuntos, ya que la clase de pares menores que (γ, δ) está contenida en el conjunto $\operatorname{máx}\{\gamma', \delta'\} \times \operatorname{máx}\{\gamma', \delta'\}$. Por 3.27 existe una (única) semejanza $F : \Omega \times \Omega \longrightarrow \Omega$.

3.4 Funciones normales

Presentamos aquí unos resultados generales sobre una clase de funciones que simplificarán considerablemente los argumentos de la sección siguiente, en la que introduciremos la aritmética ordinal.

Definición 3.29 Sea Λ un ordinal límite o bien $\Lambda = \Omega$. Diremos que una función $F : \Lambda \longrightarrow \Omega$ es *normal* si

$$\bigwedge\alpha \in \Lambda\, F(\alpha) < F(\alpha') \wedge \bigwedge\lambda \in \Lambda\, F(\lambda) = \bigcup_{\delta<\lambda} F(\delta).$$

Por ejemplo, si aplicamos el teorema 3.23 a una función H que cumpla la propiedad $\bigwedge\alpha\, \alpha < H(\alpha)$, entonces la función F que obtenemos es normal.

La normalidad es fácil de comprobar y tiene varias consecuencias útiles:

Teorema 3.30 *Toda función normal F es estrictamente monótona, es decir, si $\alpha < \beta$ entonces $F(\alpha) < F(\beta)$. En particular F es inyectiva.*

Demostración: Sea Λ el dominio de F. Fijado $\alpha \in \Lambda$, veamos que

$$\bigwedge\beta \in \Lambda(\alpha < \beta \to F(\alpha) < F(\beta))$$

por inducción sobre β. Para $\beta = 0$ es trivialmente cierto. Si vale para β y tenemos $\alpha < \beta'$, entonces $\alpha < \beta$ o $\alpha = \beta$. Por hipótesis de inducción en el primer caso y trivialmente en el segundo, $F(\alpha) \leq F(\beta)$ y como F es normal $F(\alpha) < F(\beta')$.

Si es cierto para todo $\delta < \lambda$ y $\alpha < \lambda \in \Lambda$, entonces $\alpha < \alpha' < \lambda$ y, por hipótesis de inducción $F(\alpha) < F(\alpha')$. De nuevo por la normalidad de F es $F(\alpha) < F(\lambda)$. ∎

En particular, las funciones normales cumplen el teorema 1.29, es decir, si $F : \Lambda \longrightarrow \Lambda$ es normal, entonces $\bigwedge\alpha \in \Lambda\, \alpha \leq F(\alpha)$.

Teorema 3.31 *Si $F : \Lambda \longrightarrow \Omega$ es una función normal y $\lambda \in \Lambda$, entonces $F(\lambda)$ es un ordinal límite.*

Demostración: Como $0 < \lambda$, es $0 \leq F(0) < F(\lambda)$, luego $F(\lambda) \neq 0$. Si $\alpha < F(\lambda)$, por la normalidad $\alpha < F(\delta)$, para un cierto $\delta < \lambda$. Entonces $\delta < \delta' < \lambda$, luego $\alpha' \leq F(\delta) < F(\delta') \leq F(\lambda)$. Así pues, $F(\lambda) \neq \alpha'$ para todo α. ∎

Teorema 3.32 *Si F, $G : \Lambda \longrightarrow \Lambda$ son funciones normales, entonces $F \circ G$ también lo es.*

Demostración: Claramente, si $\alpha \in \Lambda$ tenemos que $F(\alpha) < F(\alpha')$, luego $G(F(\alpha)) < G(F(\alpha'))$. Tomemos ahora un ordinal límite $\lambda \in \Lambda$. Hemos de probar que

$$G(F(\lambda)) = \bigcup_{\delta<\lambda} G(F(\delta)).$$

Si $\alpha \in G(F(\lambda))$, como $F(\lambda)$ es un ordinal límite tenemos que $\alpha < G(\eta)$, para un $\eta \in F(\lambda)$. A su vez, $\eta \in F(\delta)$ con $\delta < \lambda$. En total $\alpha < G(\eta) < G(F(\delta))$, luego α está en el miembro derecho de la igualdad.

Recíprocamente, si $\alpha \in G(F(\delta))$, con $\delta < \lambda$, entonces $F(\delta) < F(\lambda)$, luego $\alpha < G(F(\delta)) < G(F(\lambda))$. ∎

3.5 La aritmética ordinal

Vamos a definir una suma, un producto y una exponenciación entre ordinales que generalizan a las operaciones análogas sobre los números naturales. Estas operaciones resultan útiles para definir ordinales y aplicaciones entre ordinales.

Suma de ordinales Si A y B son dos conjuntos ordenados, podemos definir su suma como el conjunto $A \oplus B = A \times \{0\} \cup B \times \{1\}$ con el orden dado por $(u, v) < (w, x) \leftrightarrow v < x \vee (v = x \wedge u \leq w)$.

En definitiva, $A \oplus B$ consta de un primer tramo semejante a A seguido de un segundo tramo semejante a B. Es fácil ver que la suma de conjuntos bien ordenados está bien ordenada. Podríamos definir la suma de dos ordinales como $\alpha + \beta = \mathrm{ord}(\alpha \oplus \beta)$, es decir, el ordinal que representa el orden que empieza como α y termina como β. Por ejemplo (suponiendo (AI)), $\omega + 1$ es el ordinal del conjunto

$$(0,0) < (1,0) < (2,0) < \cdots (0,1).$$

Es claro que este conjunto es semejante a $\omega' = \{0, 1, 2, \ldots, \omega\}$. Así pues, $\omega + 1 = \omega'$. En cambio, $1 + \omega$ es el ordinal del conjunto

$$(0,0) < (0,1) < (1,1) < (2,1) < \cdots$$

y es claro entonces que $1 + \omega = \omega$. Así pues, $\omega + 1 \neq 1 + \omega$, luego vemos que la suma de ordinales no es conmutativa. En otras palabras, lo que sucede es que si añadimos un elemento a la sucesión de los números naturales por la izquierda "no se nota", pero si lo añadimos por la derecha sí.

Por comodidad vamos a introducir la suma con una definición recurrente más manejable. De todos modos, cuando contemos con las propiedades básicas será fácil ver que se trata de la misma operación que acabamos de considerar.

Definición 3.33 Para cada ordinal $\alpha \in \Omega$ definimos $(\alpha+) : \Omega \longrightarrow \Omega$ como la única aplicación que cumple

$$(\alpha+)(0) = \alpha \quad \wedge \quad \bigwedge\beta\, (\alpha+)(\beta') = (\alpha+)(\beta)' \quad \wedge \quad \bigwedge\lambda\, (\alpha+)(\lambda) = \bigcup_{\delta<\lambda} (\alpha+)(\delta).$$

Naturalmente, esta definición es correcta por el teorema 3.23. Estas aplicaciones nos permiten definir la operación $+ : \Omega \times \Omega \longrightarrow \Omega$ dada por

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

Observemos además que, teniendo en cuenta que $1 \equiv 0'$, se cumple que

$$\alpha + 1 = (\alpha+)(0') = (\alpha+)(0)' = \alpha'.$$

En vista de esto, en lo sucesivo ya nunca escribiremos α', sino que escribiremos $\alpha + 1$ en su lugar. En estos términos, las propiedades que caracterizan a la suma de ordinales se expresan así:

$$\alpha + 0 = \alpha \quad \wedge \quad \bigwedge\beta\ \alpha + (\beta + 1) = (\alpha + \beta) + 1 \quad \wedge \quad \bigwedge\lambda\, \alpha + \lambda = \bigcup_{\delta<\lambda} (\alpha + \delta).$$

Puesto que $\alpha + \beta < (\alpha + \beta) + 1$, es inmediato que la función $\alpha+$ es normal. Esto nos da ya algunas propiedades de la suma, como la monotonía:

$$\bigwedge\alpha\beta\gamma(\beta < \gamma \to \alpha + \beta < \alpha + \gamma), \qquad \bigwedge\alpha\beta\, \beta \leq \alpha + \beta.$$

o el hecho de que los ordinales $\alpha + \lambda$ son ordinales límite.

Todas las propiedades de la suma se demuestran por inducción. Por ejemplo, es inmediato comprobar que $\bigwedge\alpha\ 0 + \alpha = \alpha$. Veamos un ejemplo detallado:

Teorema 3.34 $\bigwedge\alpha\beta\gamma(\alpha \leq \beta \to \alpha + \gamma \leq \beta + \gamma)$.

Demostración: Lo probamos por inducción sobre γ. Para $\gamma = 0$ es obvio. Si vale para γ, entonces

$$\alpha + (\gamma + 1) = (\alpha + \gamma) + 1 \leq (\beta + \gamma) + 1 = \beta + (\gamma + 1).$$

Si es cierto para todo $\delta < \lambda$, entonces $\alpha + \delta \leq \beta + \delta \leq \beta + \lambda$ y, tomando el supremo en δ, queda $\alpha + \lambda \leq \beta + \lambda$. ∎

De las desigualdades que hemos probado se sigue sin dificultad (sin necesidad de más inducciones) el siguiente resultado general de monotonía:

$$\bigwedge\alpha\beta\gamma\delta(\alpha \leq \beta \wedge \gamma < \delta \to \alpha + \gamma < \beta + \delta),$$

del cual se sigue, obviamente, el caso en que todas las desigualdades son no estrictas.

Una simple inducción demuestra que la suma de números naturales es un número natural, por lo que la suma de ordinales se restringe a una operación $+ : \omega \times \omega \longrightarrow \omega$ de números naturales.

Suponiendo el axioma de infinitud (para que tenga sentido operar con ω) vemos que si $n \in \omega$ entonces

$$\omega \leq n + \omega = \bigcup_{m\in\omega} n + m \leq \omega,$$

luego $\bigwedge n \in \omega\ n + \omega = \omega$, como ya habíamos anticipado.

Pasemos ahora a las propiedades algebraicas de la suma. Como las funciones $\alpha+$ son normales —luego inyectivas— los sumandos son simplificables por la izquierda:

$$\bigwedge\alpha\beta\gamma(\alpha+\beta=\alpha+\gamma\to\beta=\gamma).$$

En cambio (suponiendo AI), tenemos que $5+\omega=8+\omega$ y no podemos simplificar. El teorema siguiente ilustra el uso de la normalidad en el caso límite de una inducción:

Teorema 3.35 $\bigwedge\alpha\beta\gamma\ ((\alpha+\beta)+\gamma=\alpha+(\beta+\gamma))$.

Demostración: Por inducción sobre γ. Para $\gamma=0$ es trivial. Si vale para γ, entonces

$$(\alpha+\beta)+(\gamma+1)=((\alpha+\beta)+\gamma)+1=(\alpha+(\beta+\gamma))+1$$
$$=\alpha+((\beta+\gamma)+1)=\alpha+(\beta+(\gamma+1)).$$

Si vale para todo $\delta<\lambda$, entonces

$$(\alpha+\beta)+\lambda=\bigcup_{\delta<\lambda}(\alpha+\beta)+\delta=\bigcup_{\delta<\lambda}\alpha+(\beta+\delta)$$
$$=\bigcup_{\delta<\lambda}((\beta+)\circ(\alpha+))(\delta)=((\beta+)\circ(\alpha+))(\lambda)=\alpha+(\beta+\lambda),$$

donde en el penúltimo paso hemos usado la normalidad de la composición de las dos sumas. ∎

Así pues, la suma de números naturales es una operación asociativa en Ω. A partir de aquí ya no será necesario escribir paréntesis entre sumandos.

Hemos visto que, bajo AI, la suma de ordinales no es conmutativa, pues, por ejemplo, $1+\omega=\omega\neq\omega+1$, sin embargo, la suma de números naturales sí que lo es:

Teorema 3.36 $\bigwedge mn\in\omega\ m+n=n+m$.

Demostración: Una simple inducción prueba que $\bigwedge n\in\omega\ 1+n=n+1$, y esto se usa a su vez para, fijado un $m\in\omega$, demostrar por inducción sobre n que $\bigwedge n\in\omega\ m+n=n+m$. En efecto: para 0 es claro y, si vale para n, tenemos

$$m+(n+1)=m+n+1=n+m+1=n+1+m=(n+1)+m.$$ ∎

Teorema 3.37 $\bigwedge\alpha\beta(\alpha\leq\beta\to\overset{1}{\bigvee}\gamma\ \alpha+\gamma=\beta)$.

Demostración: Sabemos que $\beta\leq\alpha+\beta<\alpha+\beta+1$, luego podemos tomar el mínimo ordinal η tal que $\beta<\alpha+\eta$. Obviamente no puede ser $\eta=0$ y si η fuera un límite existiría $\delta<\eta$ tal que $\beta<\alpha+\delta$, en contra de la minimalidad de η. Así pues, $\eta=\gamma+1$ para cierto γ tal que $\alpha+\gamma\leq\beta<\alpha+\gamma+1$. Claramente $\beta=\alpha+\gamma$. La unicidad se sigue de que la suma es simplificable por la izquierda. ∎

En particular, si $\delta<\alpha+\beta$, o bien $\delta<\alpha$, o bien $\alpha\leq\delta$, en cuyo caso, por el teorema anterior, existe un γ tal que $\delta=\alpha+\gamma<\alpha+\beta$, luego $\gamma<\beta$. Así pues:

Teorema 3.38 $\bigwedge\alpha\beta\delta(\delta < \alpha+\beta \leftrightarrow \delta < \alpha \vee \bigvee\gamma < \beta\ \delta = \alpha+\gamma)$.

Ahora es fácil probar que si A y B son dos conjuntos bien ordenados y $f_1 : A \longrightarrow \alpha$, $f_2 : B \longrightarrow \beta$ son las semejanzas en sus ordinales, entonces, la aplicación $f : A \oplus B \longrightarrow \alpha+\beta$ dada por

$$f(u,v) = \begin{cases} f_1(u) & \text{si } v = 0, \\ \alpha + f_2(u) & \text{si } v = 1, \end{cases}$$

es una semejanza, luego $\operatorname{ord}(A \oplus B) = \operatorname{ord} A + \operatorname{ord} B$ y, en particular, la suma de ordinales que hemos definido es equivalente a la definida al principio de la sección.

Producto de ordinales Aunque vamos a definir el producto mediante una relación recurrente análoga a la de la suma, también en este caso podríamos dar una definición en términos de buenos órdenes. Concretamente, si A y B son dos conjuntos ordenados, podemos considerar $A \times B$ con el *orden lexicográfico,* es decir, el orden dado por

$$(u,v) \leq (w,x) \leftrightarrow v < x \vee (v = x \wedge u \leq w).$$

Es fácil ver que el producto de dos conjuntos bien ordenados está bien ordenado, lo que nos permitiría definir $\alpha \cdot \beta = \operatorname{ord}(\alpha \times \beta)$. Por ejemplo (bajo AI), $\omega \cdot 2$ sería el ordinal de

$$(0,0) < (1,0) < (2,0) < \cdots (0,1) < (1,1) < (2,1) < \cdots$$

y es claro que este conjunto es semejante a

$$\omega + \omega = \{0, 1, 2, \ldots, \omega, \omega+1, \omega+2, \ldots\}.$$

En cambio, $2 \cdot \omega$ es el ordinal de

$$(0,0) < (1,0) < (0,1) < (1,1) < (0,2) < (1,2) < \cdots$$

por lo que $2 \cdot \omega = \omega$.

Definición 3.39 Para cada ordinal $\alpha \in \Omega$ definimos $\alpha\cdot : \Omega \longrightarrow \Omega$ como la única aplicación que cumple

$$\alpha \cdot 0 = 0 \quad \wedge \quad \bigwedge\beta\ \alpha \cdot (\beta+1) = (\alpha \cdot \beta) + \alpha \quad \wedge \quad \bigwedge\lambda\ \alpha \cdot \lambda = \bigcup_{\delta<\lambda} (\alpha \cdot \delta).$$

Nuevamente, las funciones $\alpha\cdot$ se combinan para definir una ley de composición interna $\cdot : \Omega \times \Omega \longrightarrow \Omega$.

Es claro que si $\alpha \neq 0$ entonces $\alpha\cdot$ es una función normal, mientras que una simple inducción prueba que $\bigwedge\alpha\ 0 \cdot \alpha = 0$ (luego el producto por cero no es normal, ya que no es estrictamente creciente). Tampoco ofrece dificultad alguna demostrar que $\bigwedge\alpha(\alpha \cdot 1 = 1 \cdot \alpha = \alpha)$.

Como consecuencia inmediata de la normalidad tenemos la monotonía:

$$\bigwedge\alpha\beta\gamma(\alpha < \beta \wedge \gamma \neq 0 \to \gamma \cdot \alpha < \gamma \cdot \beta)$$

Si multiplicamos por la derecha la desigualdad tiene que ser no estricta:

$$\bigwedge\alpha\beta\gamma(\alpha \leq \beta \to \alpha \cdot \gamma \leq \beta \cdot \gamma).$$

Esto se prueba exactamente igual que el resultado análogo para la suma. Combinando estas desigualdades tenemos:

$$\bigwedge\alpha\beta\gamma\delta(\alpha \leq \beta \wedge \gamma < \delta \wedge \beta \neq 0 \to \alpha \cdot \gamma < \beta \cdot \delta).$$

De aquí se sigue, en particular, que $\bigwedge\alpha\beta(\alpha \cdot \beta = 0 \leftrightarrow \alpha = 0 \vee \beta = 0)$, pues si $1 \leq \alpha$ y $1 \leq \beta$, entonces $1 \leq \alpha\beta$.

También es claro que los factores no nulos se simplifican por la izquierda en las igualdades (por normalidad).

Una simple inducción demuestra que el producto de números naturales es un número natural, con lo que el producto de ordinales se restringe a un producto $\cdot : \omega \times \omega \longrightarrow \omega$.

Ejercicio: (AI) Probar que $\bigwedge n \in \omega(n \neq 0 \to n\omega = \omega)$.

Veamos ahora las propiedades algebraicas:

Teorema 3.40 $\bigwedge\alpha\beta\gamma\ \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Demostración: Podemos suponer $\alpha \neq 0$. Lo probamos por inducción sobre γ. Para $\gamma = 0$ es obvio. Si vale para γ, entonces

$$\alpha(\beta + \gamma + 1) = \alpha(\beta + \gamma) + \alpha = \alpha\beta + \alpha\gamma + \alpha = \alpha\beta + \alpha(\gamma + 1).$$

Si vale para todo $\delta < \lambda$, entonces, usando que la composición de funciones normales es normal,

$$\alpha(\beta + \lambda) = ((\beta+) \circ (\alpha\cdot))(\lambda) = \bigcup_{\delta<\lambda} ((\beta+) \circ (\alpha\cdot))(\delta) = \bigcup_{\delta<\lambda} (\alpha(\beta + \delta))$$

$$= \bigcup_{\delta<\lambda} (\alpha\beta + \alpha\delta) = \bigcup_{\delta<\lambda} ((\alpha\cdot) \circ (\alpha\beta+))(\delta) = ((\alpha\cdot) \circ (\alpha\beta+))(\lambda) = \alpha\beta + \alpha\lambda.$$

■

Exactamente igual se demuestra:

Teorema 3.41 $\bigwedge\alpha\beta\gamma\ (\alpha\beta)\gamma = \alpha(\beta\gamma)$.

Por lo tanto, no necesitamos escribir paréntesis entre factores. Suponiendo AI, el producto no es conmutativo, pues, por ejemplo,

$$\omega \cdot 2 = \omega(1 + 1) = \omega + \omega > \omega + 0 = \omega,$$

mientras que $2 \cdot \omega = \omega$. De aquí se sigue también que la propiedad distributiva por la derecha es falsa, así como que no se pueden simplificar factores por la izquierda. En cambio, el producto de números naturales es conmutativo:

Teorema 3.42 $\bigwedge mn \in \omega\ mn = nm$.

DEMOSTRACIÓN: Primero probamos por inducción sobre r que

$$\bigwedge r \in \omega (m+n)r = mr + nr.$$

En efecto, para $r = 0$ es trivial y si vale para r

$$(m+n)(r+1) = (m+n)r + m + n = mr + nr + m + n$$

$$= (mr + m) + (nr + n) = m(r+1) + n(r+1).$$

Y con esto ya podemos probar el enunciado por inducción sobre n. Para $n = 0$ es trivial y, si vale para n,

$$m(n+1) = mn + m = nm + m = (n+1)m.$$

■

La división euclídea es válida para ordinales cualesquiera:

Teorema 3.43 $\bigwedge \alpha\beta(\beta \neq 0 \to \overset{1}{\bigvee}\gamma\delta(\alpha = \beta\gamma + \delta \wedge \delta < \beta))$.

DEMOSTRACIÓN: Como $1 \leq \beta$, tenemos que $\alpha \leq \beta\alpha < \beta\alpha + \beta = \beta(\alpha + 1)$. Sea η el mínimo ordinal tal que $\alpha < \beta\eta$. Obviamente no puede ser $\eta = 0$ y tampoco puede ser un ordinal límite, ya que entonces sería $\alpha < \beta\epsilon$, para $\epsilon < \eta$, en contra de la minimalidad de η. Así pues, $\eta = \gamma + 1$, para cierto γ. Tenemos que

$$\beta\gamma \leq \alpha < \beta(\gamma + 1) = \beta\gamma + \beta.$$

Por el teorema 3.37 existe un δ tal que $\alpha = \beta\gamma + \delta$. Como $\beta\gamma + \delta < \beta\gamma + \beta$, por la normalidad de $\beta\gamma+$ concluimos que $\delta < \beta$.

Veamos la unicidad. Si tenemos dos soluciones γ_1, γ_2, δ_1, δ_2 y $\gamma_1 < \gamma_2$, entonces

$$\alpha = \beta\gamma_1 + \delta_1 < \beta\gamma_1 + \beta = \beta(\gamma_1 + 1) \leq \beta\gamma_2 \leq \beta\gamma_2 + \delta_2 = \alpha,$$

lo cual es contradictorio. Similarmente es imposible que $\gamma_2 < \gamma_1$, luego $\gamma_1 = \gamma_2$. Por consiguiente, $\beta\gamma_1 + \delta_1 = \beta\gamma_1 + \delta_2$, de donde $\delta_1 = \delta_2$. ■

Como consecuencia:

Teorema 3.44 $\bigwedge \alpha\beta\epsilon\ (\epsilon < \alpha\beta \leftrightarrow \bigvee \gamma < \beta \bigvee \delta < \alpha\ \epsilon = \alpha\gamma + \delta)$

DEMOSTRACIÓN: Si $\epsilon < \alpha\beta$, podemos expresarlo como $\epsilon = \alpha\gamma + \delta$, con $\delta < \alpha$, y también tiene que ser $\gamma < \beta$, pues si $\beta \leq \gamma$, entonces $\alpha\beta \leq \alpha\gamma \leq \alpha\gamma + \delta = \epsilon$. Recíprocamente, si $\epsilon = \alpha\gamma + \delta$ con $\gamma < \beta$ y $\delta < \alpha$, entonces

$$\epsilon = \alpha\gamma + \delta < \alpha\gamma + \alpha = \alpha(\gamma + 1) \leq \alpha\beta.$$

■

Ahora, si $f_1 : A \longrightarrow \alpha$ y $f_2 : B \longrightarrow \beta$ son semejanzas de dos conjuntos bien ordenados en sus ordinales correspondientes, es fácil ver que[5] la aplicación $f : A \times B \longrightarrow \alpha\beta$ dada por

$$f(a, b) = \alpha f_2(b) + f_1(a)$$

es una semejanza cuando en $A \times B$ consideramos el orden lexicográfico descrito en la página 113, con lo que

$$\operatorname{ord}(A \times B) = (\operatorname{ord} A)(\operatorname{ord} B)$$

y, en particular, el producto de ordinales que hemos considerado coincide con el definido en términos del producto lexicográfico de buenos órdenes.

Exponenciación de ordinales Veamos en primer lugar una definición recurrente de la exponenciación de ordinales y luego discutiremos su interpretación en términos de conjuntos bien ordenados:

Definición 3.45 Para cada ordinal $\alpha \neq 0$ definimos $\alpha^{(\ )} : \Omega \longrightarrow \Omega$ como la única función que cumple

$$\alpha^0 = 1 \wedge \bigwedge\beta\ \alpha^{\beta+1} = \alpha^\beta \cdot \alpha \wedge \bigwedge\lambda\ \alpha^\lambda = \bigcup_{\delta<\lambda} \alpha^\delta.$$

Convenimos en que $0^\alpha = \begin{cases} 1 & \text{si } \alpha = 0 \\ 0 & \text{en otro caso.} \end{cases}$

Una simple inducción nos da que $\bigwedge\alpha\beta(\alpha \neq 0 \to \alpha^\beta \neq 0)$, de donde se sigue que si $\alpha > 1$ entonces $\alpha^{(\ )}$ es una función normal.

Omitimos las demostraciones de las propiedades siguientes, pues todas ellas son similares a los resultados análogos para la suma y el producto. (A menudo hay que tratar aparte los casos en los que la base es 0 o 1.)

1. $\bigwedge\alpha\ 1^\alpha = 1$,
2. $\bigwedge\alpha\ \alpha^1 = \alpha$,
3. $\bigwedge\alpha\beta\gamma(\alpha < \beta \wedge 1 < \gamma \to \gamma^\alpha < \gamma^\beta)$,
4. $\bigwedge\alpha\beta\gamma(\alpha \leq \beta \to \alpha^\gamma \leq \beta^\gamma)$,
5. $\bigwedge\alpha\beta\gamma(\alpha \leq \beta \wedge 1 < \gamma \wedge \gamma^\alpha = \gamma^\beta \to \alpha = \beta)$,
6. $\bigwedge\alpha\beta\gamma\ \alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$,
7. $\bigwedge\alpha\beta\gamma\ (\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$.

[5] Notemos que si $\gamma_1 < \gamma_2 < \beta$ y $\delta_1, \delta_2 < \alpha$, entonces

$$\alpha\gamma_1 + \delta_1 < \alpha\gamma_1 + \alpha = \alpha(\gamma_1 + 1) \leq \alpha\gamma_2 \leq \alpha\gamma_2 + \delta_2.$$

Por lo tanto, siempre suponiendo $\gamma_1, \gamma_2 < \beta$, $\delta_1, \delta_2 < \alpha$, se cumple

$$\gamma_1 < \gamma_2 \vee (\gamma_1 = \gamma_2 \wedge \delta_1 < \delta_2) \to \alpha\gamma_1 + \delta_1 < \alpha\gamma_2 + \delta_2.$$

Esto implica a su vez que $(a_1, b_1) < (a_2, b_2) \to f(a_1, b_1) < f(a_2, b_2)$.

Como siempre, una simple inducción prueba que la exponenciación de números naturales sea un número natural.

Ejercicio: (AI) Probar que $\bigwedge n \in \omega(1 < n \to n^\omega = \omega)$.

La no conmutatividad del producto hace que, en general, $(\alpha\beta)^\gamma \neq \alpha^\gamma\beta^\gamma$. Por ejemplo,

$$(2 \cdot 2)^\omega = \omega \neq \omega^2 = 2^\omega \cdot 2^\omega.$$

Ahora bien, una simple inducción sobre r prueba que

$$\bigwedge mnr \in \omega\ (mn)^r = m^r n^r.$$

Veamos finalmente la caracterización prometida de la exponenciación:

Definición 3.46 Sean A y B dos conjuntos bien ordenados y sea m el mínimo de A. Definimos

$$A^{(B)} = \{s \mid s : B \longrightarrow A \wedge \{b \in B \mid s(b) \neq m\} \text{ es finito}\}.$$

Si $A = \varnothing$ (en cuyo caso m no está definido) entendemos que $A^{(B)} = \varnothing$, salvo si también $B = \varnothing$, en cuyo caso $A^{(B)} = \{\varnothing\}$, pues $\varnothing : \varnothing \longrightarrow \varnothing$.

Así, si $s, t \in A^{(B)}$ son distintos, el conjunto

$$\{b \in B \mid s(b) \neq t(b)\} \subset \{b \in B \mid s(b) \neq m\} \cup \{b \in B \mid t(b) = m\}$$

es finito, luego tiene un máximo elemento b^* respecto del orden de A. Definimos el orden en $A^{(B)}$ dado por

$$s < t \leftrightarrow s(b^*) < t(b^*).$$

Para probar que esta relación es realmente de orden basta ver que es transitiva. Ahora bien, si tenemos $s < t < u$ y las dos primeras funciones difieren en b_1^* y las dos últimas en b_2^*, entonces la primera y la tercera difieren en $\max\{b_1^*, b_2^*\}$ y si, por ejemplo, este máximo es b_1^*, entonces $s(b_1^*) < t(b_1^*) \leq u(b_1^*)$, y análogamente sucede si el máximo es b_2^*, por lo que $s < u$. Trivialmente el orden es total.

Vamos a ver que es un buen orden, para lo cual podemos simplificar el argumento si observamos que si A y A', al igual que B y B', son pares de conjuntos bien ordenados semejantes, es fácil ver que $A^{(B)} \cong A'^{(B')}$, por lo que podemos limitarnos a probar que si α y β son ordinales, entonces $\alpha^{(\beta)}$ está bien ordenado. De hecho, probaremos que $\operatorname{ord} \alpha^{(\beta)} = \alpha^\beta$ y con ello habremos probado el teorema siguiente:

Teorema 3.47 *Si A y B son conjuntos bien ordenados de ordinales α y β respectivamente, entonces $A^{(B)}$ está bien ordenado, y*

$$\operatorname{ord}(A^{(B)}) = \alpha^\beta.$$

DEMOSTRACIÓN: Por la discusión previa, basta probar que $\alpha^{(\beta)}$ está bien ordenado y tiene ordinal α^β. El caso en que $\alpha = 0$ es trivial, pues entonces

$$\alpha^{(\beta)} = \begin{cases} \{\varnothing\} & \text{si } \beta = 0, \\ \varnothing & \text{si } \beta > 0. \end{cases}$$

Supongamos, pues que $\alpha \neq 0$ y razonamos por inducción sobre β. Si $\beta = 0$ tenemos que $\alpha^{(\beta)} = \{\varnothing\}$ y la conclusión es trivial. Si vale para β, basta observar que la aplicación $f : \alpha^{(\beta+1)} \longrightarrow \alpha^{(\beta)} \times \alpha$ dada por $f(s) = (s|_\beta, s(\beta))$ es una semejanza cuando en el producto consideramos el orden lexicográfico.

Supongamos finalmente que el resultado es cierto para todo $\delta < \lambda$, con lo que tenemos semejanzas $f_\delta : \alpha^{(\delta)} \longrightarrow \alpha^\delta$. Definimos

$$A_\delta = \{s \in \alpha^{(\lambda)} \mid \textstyle\bigwedge \epsilon(\delta \leq \epsilon \to s(\epsilon) = 0)\}.$$

Es inmediato comprobar que $\alpha^{(\lambda)} = \bigcup_{\delta<\lambda} A_\delta$, y que la aplicación $A_\delta \longrightarrow \alpha^{(\delta)}$ dada por $s \mapsto s|_\delta$ es una semejanza, luego A_δ está bien ordenado y $\operatorname{ord} A_\delta = \alpha^\delta$. Además, si $\delta < \delta' < \lambda$, todo elemento de $A_{\delta'} \setminus A_\delta$ es mayor que todo elemento de A_δ, luego si $s_\delta = \min(A_{\delta'} \setminus A_\delta)$, se cumple que $A_\delta = (A_{\delta'})^<_{s_\delta}$. Por consiguiente, si llamamos $f_\delta : A_\delta \longrightarrow \alpha^\delta$ a la semejanza, se cumple que $f_{\delta'}|_{A_\delta} : A_\delta \longrightarrow f_{\delta'}(s_\delta)$ es una semejanza, luego por la unicidad $f_{\delta'}(s_\delta) = \alpha^\delta$ y $f_{\delta'}|_{A_\delta} = f_\delta$. Esto hace que

$$\bigcup_{\delta<\lambda} f_\delta : \alpha^{(\lambda)} \longrightarrow \bigcup_{\delta<\lambda} \alpha^\delta = \alpha^\lambda$$

sea una semejanza. ∎

3.6 La forma normal de Cantor

El teorema 2.25 afirma que, dado un número natural $k \geq 2$, todo número natural admite una única expresión en base k. En esta sección probaremos resultado análogo para ordinales tomando como base $k = \omega$. Trabajaremos en NBG* + AI. En primer lugar conviene que nos formemos una idea orientativa de cómo son los primeros ordinales. Si no se cumple el axioma de infinitud, los ordinales coinciden con los números naturales:

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots$$

Con el axioma de infinitud, por encima de ellos tenemos ω y sus sucesores:

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots \quad \omega, \quad \omega + 1, \quad \omega + 2, \quad \ldots$$

Pero la sucesión de ordinales no acaba ahí, sino que por encima de todos estos está $\omega + \omega = \omega \cdot 2$ y sus sucesores:

$$0, \quad 1, \quad \ldots \quad \omega, \quad \omega + 1, \quad \ldots \quad \omega \cdot 2, \quad \omega \cdot 2 + 1, \quad \omega \cdot 2 + 2, \quad \ldots$$

pero por encima de los ordinales $\omega\cdot 2+n$ está $\omega\cdot 2+\omega=\omega\cdot 3$, y así sucesivamente:

$$0,\quad 1,\quad \ldots\quad \omega,\quad \omega+1,\quad \ldots\quad \omega\cdot 2,\quad \omega\cdot 2+1,\quad \ldots\quad \omega\cdot 3,\quad \ldots\quad \omega\cdot 4,\quad \ldots$$

pero por encima de $\omega\cdot 1$, $\omega\cdot 2$, $\omega\cdot 3$, $\omega\cdot 4$, ... está $\omega\cdot\omega=\omega^2$.

Pero por encima de ω^2 están ω^2+1, $\omega^2+2,\ldots$ y, en general, todos los ordinales de la forma $\omega^2+\omega\cdot n+m$, con m, $n\in\omega$. Y por encima de todos ellos está $\omega^2+\omega^2=\omega^2\cdot 2$, y así podemos ir ascendiendo hasta $\omega^2\cdot 3$, $\omega^2\cdot 4$, ..., y por encima de todos ellos está $\omega^2\cdot\omega=\omega^3$, y si vamos formando ω^3, ω^4, ω^5, ..., con ese patrón tampoco agotamos los ordinales, pues por encima de todos ellos está ω^ω, con lo que podemos volver a empezar con $\omega^\omega+1,\omega^\omega+2,\ldots$ hasta llegar a $\omega^\omega+\omega^\omega=\omega^\omega\cdot 2$. Pero si vamos formando los ordinales $\omega^\omega\cdot 2$, $\omega^\omega\cdot 3$, $\omega^\omega\cdot 4,\ldots$, por encima de todos ellos está $\omega^\omega\cdot\omega=\omega^{\omega+1}$. Así podemos llegar hasta ω^{ω^2} y hasta $\omega^{\omega^3},\ldots$ hasta llegar a ω^{ω^ω}.

Quizá en este punto el lector debería reconsiderar el teorema 3.14 c): dado cualquier conjunto A de ordinales, como pueda ser la sucesión

$$\omega,\quad \omega^\omega,\quad \omega^{\omega^\omega},\quad \omega^{\omega^{\omega^\omega}},\quad \ldots$$

existe su supremo en Ω, es decir, hay un ordinal σ por encima de todos los elementos de A (en particular, por encima de todos los elementos de la sucesión anterior), a partir del cual podemos empezar a sumar de nuevo $\sigma,\sigma+1,\sigma+2,\ldots$

En realidad, con todos los ordinales que hemos escrito aquí, apenas hemos ascendido nada en Ω. Con el teorema de Cantor que vamos a demostrar pondremos "un poco de orden" en esta "jungla" de los "primeros ordinales". Necesitamos algunos resultados previos:

Teorema 3.48 *Si $\alpha\omega\leq\beta$ entonces $\alpha+\beta=\beta$.*

Demostración: Sabemos que existe un γ tal que $\beta=\alpha\omega+\gamma$, por lo que

$$\alpha+\beta=\alpha+\alpha\omega+\gamma=\alpha(1+\omega)+\gamma=\alpha\omega+\gamma=\beta.$$

■

Informalmente, la hipótesis del teorema anterior afirma que β empieza por "infinitas copias" de α, es decir, por $\alpha+\alpha+\alpha+\cdots$, por lo que si añadimos un α más "no se nota".

Ejercicio: Probar el recíproco del teorema anterior.

Teorema 3.49 *Si $\alpha<\beta$ entonces $\omega^\alpha+\omega^\beta=\omega^\beta$.*

Demostración: Es un caso particular del teorema anterior, puesto que se cumple $\omega^\alpha\omega=\omega^{\alpha+1}\leq\omega^\beta$. ■

Teorema 3.50 *Si $\alpha\neq 0$ existen unos únicos η y β tales que $\alpha=\omega^\eta+\beta$, con $\beta<\alpha$. Además η es concretamente el único ordinal que cumple $\omega^\eta\leq\alpha<\omega^{\eta+1}$.*

DEMOSTRACIÓN: Como la función $\omega^{(\ )}$ es normal, $\alpha \leq \omega^\alpha < \omega^{\alpha+1}$, luego podemos tomar el mínimo γ tal que $\alpha < \omega^\gamma$. No puede ser $\gamma = 0$ ni tampoco que sea un límite, luego $\gamma = \eta + 1$ y tenemos $\omega^\eta \leq \alpha < \omega^{\eta+1}$.

Es claro que η es único. Existe un $\beta \leq \alpha$ tal que $\alpha = \omega^\eta + \beta$, pero ha de ser $\beta < \alpha$, pues si se da la igualdad

$$\alpha = \omega^\eta + \alpha = \omega^\eta + \omega^\eta + \alpha = \omega^\eta + \omega^\eta + \omega^\eta + \alpha = \cdots$$

y, en general, $\omega^\eta \cdot n \leq \alpha$, para todo $n \in \omega$. Por consiguiente, $\omega^\eta\omega = \omega^{\eta+1} \leq \alpha$, contradicción.

Recíprocamente, si $\alpha = \omega^\eta + \beta$ con $\beta < \alpha$, ha de ser $\omega^\eta \leq \alpha < \omega^{\eta+1}$ o, de lo contrario, por 3.48 tendríamos que $\alpha = \omega^\eta + \alpha = \omega^\eta + \beta$ y sería $\beta = \alpha$. De aquí se sigue la unicidad de η, que a su vez implica la de β. ∎

Teorema 3.51 *Si $\alpha \neq 0$ existe una única sucesión finita decreciente de ordinales $\eta_0 \geq \eta_1 \geq \cdots \geq \eta_n$ tal que $\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n}$.*

DEMOSTRACIÓN: Aplicamos el teorema anterior repetidamente, con lo que expresamos $\alpha = \omega^{\eta_0} + \alpha_1$, con $\alpha_1 < \alpha$, luego $\alpha_1 = \omega^{\eta_1} + \alpha_2$, con $\alpha_2 < \alpha_1$, etc. Como no podemos tener una sucesión decreciente de ordinales (no tendría mínimo), algún $\alpha_n = 0$, lo que nos da la expresión buscada.

Si fuera $\eta_i < \eta_{i+1}$ para algún i, entonces

$$\alpha_i = \omega^{\eta_i} + \alpha_{i+1} = \omega^{\eta_i} + \omega^{\eta_{i+1}} + \alpha_{i+2} = \omega^{\eta_{i+1}} + \alpha_{i+2} = \alpha_{i+1},$$

contradicción.

Para probar la unicidad observamos que si $\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n}$ y los exponentes son decrecientes, entonces

$$\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n} \leq \omega^{\eta_0} + \cdots + \omega^{\eta_0} = \omega^{\eta_0} \cdot n < \omega^{\eta_0}\omega = \omega^{\eta_0+1},$$

es decir, $\omega^{\eta_0} \leq \alpha < \omega^{\eta_0+1}$, luego η_0 está unívocamente determinado por α. Si tuviéramos dos expresiones distintas, ambas tendrían el mismo primer término, luego podríamos cancelarlo y de aquí deduciríamos que tendrían el mismo segundo término, y así sucesivamente. En definitiva, ambas serían la misma. ∎

El teorema de Cantor se sigue del que acabamos de probar sin más que agrupar los términos con el mismo exponente (por la propiedad asociativa generalizada):

Teorema 3.52 (Forma normal de Cantor) *Si $\alpha \neq 0$ existe una única sucesión finita estrictamente decreciente de ordinales $\eta_0 > \eta_1 > \cdots > \eta_n$ y una única sucesión finita $k_0, \ldots, k_n$ de números naturales no nulos tal que $\alpha = \omega^{\eta_0}k_0 + \cdots + \omega^{\eta_n}k_n$.*

La forma normal de Cantor es especialmente descriptiva para ordinales pequeños. Por ejemplo, si $\alpha < \omega^\omega$ entonces es claro que η_0 ha de ser un número natural, luego tenemos que los ordinales menores que ω^ω se expresan de forma única como polinomios en ω con coeficientes naturales.

Podemos ir algo más lejos, para lo cual conviene definir

$$\omega^{(0)} = 1, \qquad \omega^{(n+1)} = \omega^{\omega^{(n)}}, \qquad \epsilon_0 = \bigcup_{n\in\omega} \omega^{(n)}.$$

Así, $\omega^{(1)} = \omega$, $\omega^{(2)} = \omega^\omega$, $\omega^{(3)} = \omega^{\omega^\omega}$, etc. y ϵ_0 es el supremo de esta sucesión.[6]

Si $\delta < \epsilon_0$, entonces se cumple $\delta < \omega^{(n)}$ para cierto $n \in \omega$, luego tenemos que $\omega^\delta \le \omega^{\omega^{(n)}} = \omega^{(n+1)} \le \epsilon_0$. Tomando el supremo en δ concluimos que $\omega^{\epsilon_0} \le \epsilon_0$. El recíproco es obvio, luego $\omega^{\epsilon_0} = \epsilon_0$.

Definición 3.53 Un *número épsilon* es un ordinal $\epsilon \in \Omega$ tal que $\omega^\epsilon = \epsilon$.

Acabamos de probar que existen números ϵ. De hecho, vamos a ver que el número ϵ_0 que hemos construido es el menor número ϵ. Para ello, para cada $\alpha < \epsilon_0$ no nulo, llamamos $o(\alpha)$ al único $n \in \omega$ tal que $\omega^{(n)} \le \alpha < \omega^{(n+1)}$.

Es claro que entonces $\omega^{(n+1)} \le \omega^\alpha < \omega^{(n+2)}$, es decir, tenemos que

$$o(\omega^\alpha) = 1 + o(\alpha).$$

En particular $\omega^\alpha \ne \alpha$, luego α no es un número ϵ.

Los números naturales (no nulos) son los ordinales de rango 0, los números entre ω y ω^ω son los ordinales de rango 1 (y son, como hemos visto, los polinomios en ω con coeficientes naturales).

Observemos ahora lo siguiente:

Teorema 3.54 *Si ξ es un ordinal, se cumple:*

1. $\bigwedge\alpha\beta < \xi\ \alpha + \beta < \xi$ *y sólo si* $\xi = 0 \vee \bigvee\eta\ \xi = \omega^\eta$.
2. $\bigwedge\alpha\beta < \xi\ \alpha \cdot \beta < \xi$ *si y sólo si* $\xi = 0, 1, 2 \vee \bigvee\eta\ \xi = \omega^{\omega^\eta}$.
3. $\bigwedge\alpha\beta < \xi\ \alpha^\beta < \xi$ *si y sólo si* $\xi = 0, 1, 2, \omega \vee \xi$ *es un número épsilon.*

Demostración: a) Veamos por inducción sobre η que ω^η cumple la propiedad indicada: para $\eta = 0$ es trivial. Si vale para η y $\alpha, \beta < \omega^{\eta+1} = \omega^\eta \cdot \omega$, entonces existe un $n < \omega$ tal que $\alpha, \beta < \omega^\eta \cdot n$, luego

$$\alpha + \beta < \omega^\eta(n + n) < \omega^\eta \cdot \omega = \omega^{\eta+1}.$$

Si vale para todo $\delta < \lambda$ y $\alpha, \beta < \omega^\lambda$, entonces existe un $\delta < \lambda$ tal que $\alpha, \beta < \omega^\delta$, luego $\alpha + \beta < \omega^\delta < \omega^\lambda$.

[6] Es el ordinal que hemos "rozado" en nuestra "escalada" por Ω al principio de esta sección.

Recíprocamente, si $\xi > 0$ tiene la propiedad, consideramos la expresión $\xi = \omega^\eta + \beta$ dada por el teorema 3.50. Como $\beta < \xi$ y $\omega^\eta \leq \xi$, tiene que ser $\xi = \omega^\eta$.

b) Claramente $\omega^{\omega^0} = \omega$ cumple lo pedido. Si $\alpha, \beta < \omega^{\omega^\eta}$, con $\eta > 0$, entonces existe un $\delta < \omega^\eta$ tal que $\alpha, \beta < \omega^\delta$, luego $\alpha\beta < \omega^{\delta+\delta} < \omega^{\omega^\eta}$, donde hemos usado el apartado anterior.

Recíprocamente, si $\xi > 2$ cumple la propiedad indicada, entonces también cumple la del apartado a), porque si $\alpha, \beta < \xi$, tenemos que

$$\alpha + \beta \leq \text{máx}\{\alpha, \beta\} \cdot 2 < \xi.$$

Por lo tanto $\xi = \omega^\delta$. Además, si $\alpha, \beta < \delta$, entonces $\omega^\alpha, \omega^\beta < \xi$, luego se cumple también que $\omega^{\alpha+\beta} < \xi = \omega^\delta$, luego $\alpha + \beta < \delta$, luego $\delta = 0 \vee \delta = \omega^\eta$ por el apartado anterior. En el primer caso resulta el caso trivial $\xi = 1$.

c) Si ξ es un número épsilon y $\alpha, \beta < \xi = \omega^\xi$, entonces existe un $\delta < \xi$ tal que $\alpha < \omega^\delta$, luego

$$\alpha^\beta < (\omega^\delta)^\beta = \omega^{\delta\beta} < \omega^\xi = \xi,$$

donde hemos usado que $\xi = \omega^{\omega^\xi}$ cumple el apartado b).

Recíprocamente, si $\xi > 2$ cumple la propiedad indicada, entonces cumple la propiedad del apartado b), pues si $\alpha, \beta < \xi$, entonces $\alpha\beta \leq \text{máx}\{\alpha, \beta\}^2 < \xi$, luego en particular $\xi = \omega^\eta$. Si $\eta = 0$ queda $\xi = 1$, si $\eta = 1$ queda $\xi = \omega$ y si $\eta > 1$, como $\omega < \xi \wedge \eta \leq \omega^\eta = \xi$, por la hipótesis tiene que ser $\eta = \omega^\eta = \xi$, luego $\xi = \omega^\xi$ es un número épsilon. ∎

Notemos que un número épsilon cumple de hecho los tres apartados del teorema anterior.

De este modo, ω^2 es el menor ordinal que no puede expresarse en términos de sumas de números naturales y ω. A su vez, ω^ω es el menor ordinal que no puede expresarse en términos de sumas y productos de números naturales y de ω, mientras que ϵ_0 es el menor ordinal que no puede expresarse en términos de sumas, productos y potencias de números naturales y de ω. Dicho de otro modo, todos los ordinales que podemos construir mediante las tres operaciones aritméticas a partir de los números naturales y ω son necesariamente menores que ϵ_0.

Teorema 3.55 *Si $\alpha, \beta < \epsilon_0$ son ordinales no nulos, entonces*

$$o(\alpha + \beta) = o(\alpha\beta) = \text{máx}\{o(\alpha), o(\beta)\}.$$

Demostración: Veamos por inducción sobre n que si $\alpha, \beta < \omega^{(n)}$ entonces $\alpha\beta < \omega^{(n)}$. Para $n = 0$ es trivial. Si vale para n y $\alpha, \beta < \omega^{(n+1)} = \omega^{\omega^{(n)}}$, tenemos que existe un $\delta < \omega^{(n)}$ tal que $\alpha, \beta < \omega^\delta$, luego $\alpha\beta < \omega^{\delta\cdot 2}$. Por hipótesis de inducción (si $n > 0$, pues entonces $2 < \omega^{(n)}$, y trivialmente si $n = 0$, pues entonces $\delta = 0$), tenemos que $\delta \cdot 2 < \omega^{(n)}$, luego $\alpha\beta < \omega^{\omega^{(n)}} = \omega^{(n+1)}$.

Así pues, si $o(\alpha) = m$, $o(\beta) = n$ y $r = \max\{m, n\}$, tenemos que

$$\omega^{(m)} \leq \alpha < \omega^{(m+1)}, \quad \omega^{(n)} \leq \alpha < \omega^{(n+1)}.$$

Entonces, por lo que acabamos de probar,

$$\omega^{(r)} \leq \alpha + \beta \leq \max\{\alpha, \beta\} \cdot 2 < \omega^{(r+1)}, \qquad \omega^{(r)} \leq \alpha\beta < \omega^{(r+1)},$$

luego $o(\alpha + \beta) = o(\alpha\beta) = r$. ∎

Por otra parte, ya hemos visto que $o(\omega^\alpha) = 1 + o(\alpha)$. También es obvio que si $\alpha \leq \beta < \epsilon_0$, entonces $o(\alpha) \leq o(\beta)$. Teniendo todo esto en cuenta es claro que, en las condiciones del teorema 3.52,

$$o(\omega^{\eta_i} k_i) = o(\omega^{\eta_i}) = 1 + o(\eta_i) \leq 1 + o(\eta_0),$$

luego $o(\alpha) = 1 + o(\eta_0)$.

Por consiguiente, si tomamos un ordinal $0 < \alpha < \epsilon_0$ con $o(\alpha) = n$ y lo expresamos en forma normal de Cantor, sus exponentes tendrán orden a lo sumo $n - 1$, luego pueden ponerse en forma normal de Cantor con exponentes de orden a lo sumo $n-2$, y así, tras n pasos, habremos expresado α en términos de un número finito de números naturales, sumas, productos y potencias de base ω.

En resumen: los ordinales menores que ϵ_0 son exactamente los ordinales que pueden construirse a partir de los números naturales y ω mediante sumas, productos y potencias, y cada uno de ellos se puede expresar mediante un número finito de sumas, productos y potencias de base ω. De hecho, la expresión es única si exigimos que corresponda a una forma normal de Cantor, con exponentes desarrollados a su vez en forma normal de Cantor, y así sucesivamente.

Esto ya no es cierto para ordinales mayores. Por ejemplo, la forma normal de Cantor de ϵ_0 es $\epsilon_0 = \omega^{\epsilon_0}$, lo cual no dice mucho.

Comparación de ordinales en forma normal Supongamos que tenemos dos ordinales en forma normal de Cantor:

$$\alpha = \omega^{\eta_0} k_0 + \cdots + \omega^{\eta_n} k_n, \qquad \alpha' = \omega^{\eta'_0} k'_0 + \cdots + \omega^{\eta'_{n'}} k'_{n'}.$$

Entonces $\omega^{\eta_0} \leq \alpha < \omega^{\eta_0+1}$, $\omega^{\eta'_0} \leq \alpha' < \omega^{\eta'_0+1}$, luego si $\eta_0 < \eta'_0$, y por consiguiente $\eta_0 + 1 \leq \eta'_0$, se cumple que $\alpha < \alpha'$. Supongamos, por el contrario, que $\eta_0 = \eta'_0$. Si $k_0 < k'_0$, entonces podemos descomponer α' como

$$\alpha' = \omega^{\eta_0} k_0 + \omega^{\eta'_0}(k'_0 - k_0) + \cdots + \omega^{\eta'_{n'}} k'_{n'}$$

y, como, según acabamos de ver, $\eta_0 < \eta'_1$ implica que

$$\omega^{\eta_1} k_1 + \cdots + \omega^{\eta_n} k_n < \omega^{\eta'_0}(k'_0 - k_0) + \cdots + \omega^{\eta'_{n'}} k'_{n'},$$

concluimos que $\alpha < \alpha'$ (aquí suponemos $n > 0$, pero si $n = 0$ se llega trivialmente a la misma conclusión). En el supuesto de que $\eta_0 = \eta'_0$ y $k_0 = k'_0$, se cumplirá $\alpha < \alpha'$ si y sólo si

$$\omega^{\eta_1} k_1 + \cdots + \omega^{\eta_n} k_n < \omega^{\eta'_1} k'_1 + \cdots + \omega^{\eta'_{n'}} k'_{n'},$$

donde cualquiera de los dos miembros puede ser 0.

En definitiva: para determinar cuál de dos ordinales en forma normal de Cantor es el menor, comparamos η_0 y η'_0, y el ordinal para el que este valor sea menor será el menor. En caso de empate comparamos k_0 y k'_0, en caso de empate pasamos a comparar η_1 y η'_1, y en caso de empate k_1 y k'_1. Si se mantiene el empate hasta que una de las dos expresiones "se acaba", dicha expresión corresponde al ordinal menor. Si las dos se acabaran a la vez (sin haber encontrado un desempate) es que las dos expresiones eran la misma, luego los ordinales eran iguales.

Suma de ordinales en forma normal El teorema 3.49 nos permite calcular fácilmente la suma de dos ordinales en forma normal de Cantor. Con la notación anterior, la expresión

$$\alpha + \alpha' = \omega^{\eta_0}k_0 + \cdots + \omega^{\eta_n}k_n + \omega^{\eta'_0}k'_0 + \cdots + \omega^{\eta'_{n'}}k'_{n'}$$

se puede reducir eliminando todos los términos $\omega^{\eta_k}k_i$ con $\eta_i < \eta'_0$ y el resultado estará en forma normal (salvo que un $\eta_i = \eta'_0$, en cuyo caso además habrá que agrupar $\eta_i k_i + \eta'_0 k'_0 = \eta_i(k_i + k'_0)$).

Producto de ordinales en forma normal Para calcular el producto de dos ordinales en forma normal de Cantor nos apoyamos en el teorema siguiente:

Teorema 3.56 *Si $\alpha = \omega^{\eta_0}k_0 + \cdots + \omega^{\eta_n}k_n$ es un ordinal en forma normal de Cantor, entonces $\alpha \cdot \omega^{\eta'} = \omega^{\eta_0+\eta'}$.*

Demostración: Lo probamos por inducción sobre η'. Para $\eta' = 1$ tenemos que

$$\omega^{\eta_0+1} = \omega^{\eta_0} \cdot \omega \leq \alpha \cdot \omega^1 \leq \omega^{\eta_0}(k_0 + \cdots + k_n)\omega = \omega^{\eta_0} \cdot \omega = \omega^{\eta_0+1}.$$

Si vale para η', entonces

$$\alpha \cdot \omega^{\eta'+1} = \alpha \cdot \omega^{\eta'} \cdot \omega = \omega^{\eta_0+\eta'} \cdot \omega = \omega^{\eta_0+\eta'+1}.$$

Por último, si vale para todo $\delta < \lambda$, entonces

$$\alpha \cdot \omega^{\lambda} = \bigcup_{\delta<\lambda}(\alpha \cdot \omega^{\delta}) = \bigcup_{\delta<\lambda}\omega^{\eta_0+\delta} = \omega^{\eta_0+\lambda}.$$

■

Por lo tanto, con la notación de los apartados precedentes, para calcular el producto de dos ordinales en forma normal de Cantor usamos la propiedad distributiva:

$$\alpha\alpha' = \alpha\omega^{\eta'_0}k'_0 + \cdots + \alpha\omega^{\eta'_{n'}}k'_{n'},$$

desarrollamos los productos con el teorema precedente (salvo a lo sumo el último, si $\eta'_{n'} = 0$) y por último desarrollamos las sumas según el apartado anterior, con lo que obtenemos la forma normal del producto.

Capítulo IV

La teoría de conjuntos NBG

Presentamos ahora los dos axiomas que nos faltan para completar la teoría de conjuntos NBG: el axioma de regularidad y el axioma de elección. En gran medida, su papel consiste en estrechar la relación entre la clase universal V y la clase Ω de todos los ordinales: el axioma de regularidad nos estructurará V en una jerarquía transfinita de conjuntos, mientras que el axioma de elección nos permitirá enumerar con ordinales un conjunto arbitrario. Como paso previo a la discusión del axioma de regularidad dedicaremos una sección a generalizar los teoremas de inducción y recursión que hemos probado para ordinales al caso de relaciones mucho más generales que los buenos órdenes.

4.1 Relaciones bien fundadas

Aunque podríamos trabajar en NBG*, por comodidad, en esta sección supondremos el axioma de infinitud. Las relaciones bien fundadas son la clase más general de relaciones sobre las que es posible justificar argumentos de inducción y recursión:

Definición 4.1 Una relación R está *bien fundada* en una clase A si

$$\bigwedge X(X \subset A \wedge X \neq \varnothing \to \bigvee y \in X \bigwedge z \in X\, \neg x\, R\, y).$$

En estas condiciones diremos que y es un *elemento R-minimal* de X.

Por ejemplo, si $\leq$ es un buen orden en una clase A, es claro que la relación de orden estricto $<$ está bien fundada en A, pues si x es un subconjunto no vacío de A, el mínimo de x es un minimal para $<$.

Observemos también que A es una clase bien fundada en el sentido de la definición 3.1 si y sólo si la relación de pertenencia E está bien fundada en A, en el sentido que acabamos de introducir.

De la propia definición se sigue un sencillo teorema de inducción, aunque no es el más general que vamos a demostrar:

Teorema 4.2 (Teorema general de inducción transfinita) *Sea R una relación bien fundada en una clase A y sea B una clase cualquiera. Entonces*

$$\bigwedge x \in A(A_x^R \subset B \to x \in B) \to A \subset B.$$

DEMOSTRACIÓN: Si no se cumple $A \subset B$, entonces $A \setminus B$ es una subclase no vacía de A, luego tiene un R-minimal x, de modo que $A_x^R \subset B$, pero $x \notin B$, contradicción. ∎

Lo que afirma el teorema anterior es que para demostrar que todo elemento $x \in A$ tiene una propiedad (estar en B), podemos suponer como hipótesis de inducción que todos los elementos de $u\,R\,x$ la tienen.

Para manejar relaciones bien fundadas sobre clases propias vamos a necesitar una propiedad adicional que se vuelve trivial si las clases son conjuntos:

Definición 4.3 Una relación R es *conjuntista* en una clase A si para todo $x \in A$ la clase de los anteriores de x

$$A_x^R = \{y \in A \mid y\,R\,x\}$$

es un conjunto.

Obviamente toda relación es conjuntista en todo conjunto. La relación de pertenencia E es conjuntista en cualquier clase, pues $A_x^E = x \cap A$.

Observemos que ya nos hemos encontrado con esta restricción en una ocasión: en el capítulo anterior hemos demostrado que una clase propia bien ordenada es semejante a Ω si y sólo si su relación de orden es conjuntista.

Definición 4.4 Sea R una relación definida sobre una clase A. Diremos que una subclase $B \subset A$ es *R-A-transitiva* si

$$\bigwedge xy \in A(x\,R\,y \wedge y \in B \to x \in B).$$

Es decir, B es R-A-transitiva si cuando partimos de elementos de B y vamos tomando anteriores nunca salimos de B. Las clases transitivas en el sentido de la definición 3.1 son precisamente las clases E-V-transitivas.

Si R es una relación definida sobre una clase A y x es un subconjunto de A, es claro que al considerar los anteriores de x y los anteriores de los anteriores, etc. obtenemos un conjunto R-A-transitivo. En realidad, para que la definición recurrente de este proceso sea correcta hemos de exigir que R sea conjuntista. Veámoslo con detalle:

Definición 4.5 Sea R una relación conjuntista en una clase A y $x \in A$. El teorema de recursión nos da una aplicación $\mathrm{cl}_A^R(x)[\,] : \omega \longrightarrow \mathcal{P}A$ determinada por[1]

$$\mathrm{cl}_A^R(x)[0] = A_x^R \wedge \bigwedge n \in \omega\ \mathrm{cl}_A^R(x)[n+1] = \bigcup_{u \in \mathrm{cl}_A^R(x)[n]} A_u^R.$$

[1] Notemos que esta construcción requiere que la relación sea conjuntista para que podamos asegurar que cada término de la sucesión es un conjunto. Si no, la sucesión no estaría bien definida.

A su vez definimos la *clausura* de x respecto de R en A como el conjunto

$$\mathrm{cl}_A^R(x) \equiv \bigcup_{n\in\omega} \mathrm{cl}_A^R(x)[n].$$

Así $A_x^R \subset \mathrm{cl}_A^R(x) \subset A$.

Cuando E es la relación de pertenencia y $A = \mathrm{V}$, la clausura $\mathrm{cl}_A^E(x)$ se conoce como la *clausura transitiva* de x y se representa por $\mathrm{ct}\, x$. Es claro que admite una definición más sencilla (puesto que ahora $A_x^E = x$):

$$\mathrm{ct}_0 x = x, \qquad \bigwedge n \in \omega\ \mathrm{ct}_{n+1} x = \bigcup_{y\in \mathrm{ct}_n x} y, \qquad \mathrm{ct}\ x = \bigcup_{n\in\omega} \mathrm{ct}_n x.$$

Así, ct x está formada por los elementos de x, los elementos de los elementos de x, etc.

Nuestra intención al definir la clausura de un elemento era formar un conjunto R-A-transitivo. Vamos a ver que, efectivamente, así es. Más concretamente, $\mathrm{cl}_A^R(x)$ es el menor conjunto R-A-transitivo que contiene a A_x^R:

Teorema 4.6 *Sea R una relación conjuntista en una clase A y sea $x \in A$. Se cumple*

1. $A_x^R \subset \mathrm{cl}_A^R(x)$.
2. $\mathrm{cl}_A^R(x)$ *es un conjunto R-A-transitivo.*
3. *Si $A_x^R \subset T$ y $T \subset A$ es una clase R-A-transitiva, entonces* $\mathrm{cl}_A^R(x) \subset T$.
4. $\mathrm{cl}_A^R(x) = A_x^R \cup \bigcup_{y\in A_x^R} \mathrm{cl}_A^R(y)$.

Demostración: Demostración: 1) $A_x^R = \mathrm{cl}_A^R(x)[0] \subset \mathrm{cl}_A^R(x)$.

2) Supongamos que u, $y \in A$ cumplen $u\, R\, y \wedge y \in \mathrm{cl}_A^R(x)$. Entonces existe un $n \in \omega$ tal que $y \in \mathrm{cl}_A^R(x)[n]$, con lo que $u \in A_y^R \subset \mathrm{cl}_A^R(x)[n+1] \subset \mathrm{cl}_A^R(x)$.

3) Una simple inducción prueba que $\mathrm{cl}_A^R(x)[n] \subset T$. En efecto, para 0 lo tenemos por hipótesis y, si vale para n, entonces todo $u \in \mathrm{cl}_A^R(x)[n+1]$ cumple $u \in A_y^R$, para cierto $y \in \mathrm{cl}_A^R(x)[n]$, con lo que $u\, R\, y \wedge y \in T$. Por transitividad $u \in T$. Por definición de clausura concluimos que $\mathrm{cl}_A^R(x) \subset T$.

4) Si $y \in A_x^R$, entonces $A_y^R \subset \mathrm{cl}_A^R(x)[1] \subset \mathrm{cl}_A^R(x)$, luego por 2) y 3) obtenemos que $\mathrm{cl}_A^R(y) \subset \mathrm{cl}_A^R(x)$. Por consiguiente el conjunto $T = A_x^R \cup \bigcup_{y\in A_x^R} \mathrm{cl}_A^R(y)$ está contenido en $\mathrm{cl}_A^R(x)$.

Para demostrar la otra inclusión basta probar T es transitivo y aplicar 3). Sean, pues, u, $v \in A$ tales que $u\, R\, v \wedge v \in T$. Si $v \in \mathrm{cl}_A^R(y)$ para un $y \in A_x^R$, entonces, por la transitividad de la clausura $u \in \mathrm{cl}_A^R(y)$, luego $u \in T$.

Si $v \in A_x^R$, entonces $u \in \mathrm{cl}_A^R(v) \subset T$. ∎

Conviene observar la particularización de este teorema al caso de la relación de pertenencia sobre la clase universal:

Teorema 4.7 *Sea x un conjunto arbitrario. Entonces*

1. $x \subset \mathrm{ct}\ x$.
2. $\mathrm{ct}\ x$ *es un conjunto transitivo.*
3. *Si* $x \subset T$ *y* T *es una clase transitiva, entonces* $\mathrm{ct}\ x \subset T$.
4. $\mathrm{ct}\ x = x \cup \bigcup_{y \in x} \mathrm{ct}\ y$.
5. x *es transitivo si y sólo si* $x = \mathrm{ct}\ x$.

La última propiedad es consecuencia inmediata de las anteriores. Como primera aplicación del concepto de clausura demostramos un resultado técnico:

Teorema 4.8 *Sea R una relación conjuntista en una clase A. Entonces R está bien fundada en A si y sólo si todo subconjunto no vacío de A tiene un R-minimal.*

Demostración: Una implicación es obvia. Para la otra, suponemos que todo subconjunto no vacío tiene un R-minimal y hemos de probar que lo mismo vale para toda subclase no vacía B. Tomemos un $x \in B$. Si x no es ya un R-minimal de B, entonces existe un $y \in B$ tal que $y\,R\,x$, luego $y \in B \cap \mathrm{cl}_A^R(x)$, que es un subconjunto no vacío de A. Por hipótesis tiene un R-minimal, digamos z.

Vamos a ver que z es un R-minimal de B. En efecto, si existiera un $v \in B$ tal que $v\,R\,z$, entonces, por la transitividad de la clausura, $v \in B \cap \mathrm{cl}_A^R(x)$, pero esto contradice la minimalidad de z. ∎

Esto implica que el concepto de relación bien fundada es, pese a lo que en principio podría parecer, una fórmula normal (pues el cuantificador "para toda subclase no vacía" puede sustituirse por "para todo subconjunto no vacío").

Con esto estamos en condiciones de demostrar el teorema de recursión. En esencia afirma que para definir una función $F : A \longrightarrow B$, si en A tenemos definida una relación conjuntista y bien fundada, podemos definir $F(x)$ suponiendo que F está ya definida sobre los elementos de A_x^R:

Teorema 4.9 (Teorema general de recursión transfinita) *Sea R una relación conjuntista y bien fundada en una clase A y sea $G : A \times V \longrightarrow B$ una aplicación arbitraria. Entonces existe una única función $F : A \longrightarrow B$ tal que*

$$\bigwedge x \in A\, F(x) = G(x, F|_{A_x^R}).$$

Demostración: Por abreviar, a lo largo de esta prueba, "transitivo" significará R-A-transitivo.

Si $d \subset A$ es un conjunto transitivo, diremos que $h : d \longrightarrow B$ es una *d-aproximación* si

$$\bigwedge x \in d\ h(x) = G(x, h|_{A_x^R}).$$

Para cada $x \in A$, definimos

$$\hat{x} = \{x\} \cup \mathrm{cl}_A^R(x).$$

Es claro que $\hat{x}$ es transitivo y $x \in \hat{x}$ (de hecho, es el menor conjunto transitivo que contiene a x). Dividimos la prueba en varios pasos:

1) *Si h es una d-aproximación y h' es una d'-aproximación, entonces se cumple $h|_{d\cap d'} = h'|_{d\cap d'}$. En particular, para cada conjunto transitivo $d \subset A$ existe a lo sumo una d-aproximación.*

Lo probamos por inducción en $d \cap d'$, es decir, vamos a probar que todo elemento de $d \cap d'$ está en $\{u \in d \cap d' \mid h(u) = h'(u)\}$. Para ello tomamos $x \in d \cap d'$ y suponemos que $h(u) = h(u')$ siempre que $u \in (d \cap d')_x^R$. Ahora bien, es inmediato que $d \cap d'$ es transitivo, de donde se sigue que $(d \cap d')_x^R = A_x^R$. Por consiguiente tenemos que $h|_{A_x^R} = h'|_{A_x^R}$, luego

$$h(x) = G(x, h|_{A_x^R}) = G(x, h'|_{A_x^R}) = h'(x).$$

2) *Para todo $x \in A$ existe una $\hat{x}$-aproximación.*

Lo probamos por inducción sobre x, es decir, suponemos que para todo $u \in A_x^R$ existe una $\hat{u}$-aproximación. Por 1) es única, luego podemos definir $h_u \equiv h|h$ es una $\hat{u}$-aproximación. Definimos $h = \bigcup_{u\in A_x^R} h_u$. De nuevo por 1) tenemos que h es una función y su dominio es

$$\bigcup_{u\in A_x^R} \hat{u} = \bigcup_{u\in A_x^R} (\{u\} \cup \mathrm{cl}_A^R(u)) = A_x^R \cup \bigcup_{u\in A_x^R} \mathrm{cl}_A^R(u) = \mathrm{cl}_A^R(x),$$

donde hemos aplicado el teorema 4.6.

Si $v \in \mathrm{cl}_A^R(x)$, entonces $h(v) = h_u(v)$, para cierto $u \in A_x^R$ tal que $v \in \hat{u}$. Puesto que $h_u \subset h$ y $A_v^R \subset \hat{u}$ (por ser $\hat{u}$ transitivo) tenemos que $h_u|_{A_v^R} = h|_{A_v^R}$. Como h_u es una $\hat{u}$-aproximación,

$$h(v) = h_u(v) = G(v, h_u|_{A_v^R}) = G(v, h|_{A_v^R}),$$

con lo que h resulta ser una $\mathrm{cl}_A^R(x)$-aproximación.

Puede probarse que $x \notin \mathrm{cl}_A^R(x)$, pero no es necesario, en cualquier caso podemos definir

$$h' = h \cup \{(x, G(x, h|_{A_x^R}))\},$$

de modo que $h : \hat{x} \longrightarrow \mathrm{V}$ y es inmediato que para todo $v \in \hat{x}$ se cumple $h'|_{A_v^R} = h|_{A_v^R}$, de donde se sigue claramente que h' es una $\hat{x}$-aproximación.

3) *Definimos $F = \bigcup_{x\in A} h_x$, donde $h_x \equiv h|h$ es una $\hat{x}$-aproximación.*

La unicidad de 1) hace que $F : A \longrightarrow B$, y los mismos razonamientos que hemos aplicado a h en el paso anterior prueban que para todo $x \in A$ se cumple $F(x) = G(x, F|_{A_x^R})$.

4) *La unicidad de F se prueba igual que* 1) ∎

Como primera aplicación de este teorema, dada una clase con una relación conjuntista y bien fundada, vamos a asociar a cada uno de sus elementos un ordinal que exprese su "altura" en la relación, entendiendo que un elemento es más alto cuantos más elementos tiene por debajo.

Definición 4.10 Sea R una relación conjuntista y bien fundada en una clase A. Definimos $\operatorname{rang} : A \longrightarrow \Omega$ como la única aplicación que cumple

$$\bigwedge x \in A \ \operatorname{rang}_A^R(x) = \bigcup_{y \in A_x^R} (\operatorname{rang}_A^R(y) + 1),$$

donde estamos representando por $\alpha + 1$ el ordinal siguiente a α.

Observemos que hemos definido el rango de un elemento supuesto definido el rango de los elementos anteriores a él. Más concretamente, estamos aplicando el teorema anterior a la función $G : V \longrightarrow \Omega$ dada por

$$G(z) = \begin{cases} \bigcup\limits_{y \in A_x^R} (s(y) + 1) & \text{si } z = (x, s), \text{ con } x \in A \wedge s : A_x^R \longrightarrow \Omega, \\ 0 & \text{en otro caso.} \end{cases}$$

Recordemos que la unión de un conjunto de ordinales no es más que su supremo. Hemos de entender que el supremo del conjunto vacío es 0 (lo cual es cierto, pues 0 es la menor cota superior de $\varnothing$). De este modo, los minimales de A tienen todos rango 0 y, en general, el rango de un elemento es el mínimo ordinal estrictamente mayor que los rangos de todos sus anteriores.

Teorema 4.11 *Sea R una relación conjuntista y bien fundada en una clase A. Sean x, $y \in A$. Si $x \in \operatorname{cl}_A^R(y)$, entonces $\operatorname{rang}_A^R x < \operatorname{rang}_A^R y$.*

Demostración: Por inducción sobre y, es decir, suponemos que el resultado es cierto para todo $u \in A_y^R$ y suponemos que $x \in \operatorname{cl}_A^R(y)$. Entonces hay dos posibilidades, o bien $x \in A_y^R$, en cuyo caso $\operatorname{rang}_A^R(x) < \operatorname{rang}_A^R(y)$ por definición de rango, o bien $x \in \operatorname{cl}_A^R(u)$, para cierto $u \in A_y^R$. Entonces aplicamos la hipótesis de inducción: $\operatorname{rang}_A^R(x) < \operatorname{rang}_A^R(u) < \operatorname{rang}_A^R(y)$. ∎

Con la ayuda del rango podemos demostrar teoremas de inducción y recursión aún más potentes. En el caso de la inducción, vamos a ver que podemos tomar como hipótesis de inducción, no ya que todos los elementos anteriores a uno dado cumplen lo que queremos probar, sino que todos los elementos de su clausura lo cumplen (o sea, los anteriores, y los anteriores de los anteriores, etc.).

Teorema 4.12 (Teorema general de inducción transfinita) *Sea R una relación conjuntista y bien fundada sobre una clase A y sea B una clase cualquiera. Entonces*

$$\bigwedge x \in A(\operatorname{cl}_A^R(x) \subset B \to x \in B) \to A \subset B.$$

DEMOSTRACIÓN: Si no se da la inclusión podemos tomar un $x \in A \setminus B$ de rango mínimo. Si $u \in \mathrm{cl}_A^R(x)$, entonces $\mathrm{rang}_A^R u < \mathrm{rang}_A^R x$, luego por minimalidad $u \in B$. Pero entonces la hipótesis nos da que $x \in B$, lo cual es absurdo. ∎

Similarmente, para definir una función sobre x podemos suponer que está ya definida sobre $\mathrm{cl}_A^R(x)$:

Teorema 4.13 (Teorema general de recursión transfinita) *Sea R una relación conjuntista y bien fundada en una clase A y sea $G : A \times V \longrightarrow B$ una aplicación arbitraria. Entonces existe una única función $F : A \longrightarrow B$ tal que*

$$\bigwedge x \in A\, F(x) = G(x, F|_{\mathrm{cl}_A^R(x)}).$$

La prueba de este teorema es idéntica a la de 4.9, salvo que el paso 1) y la unicidad de F se demuestran usando la versión fuerte del teorema general de inducción transfinita en lugar de la débil.

Es claro que los teoremas que acabamos de probar generalizan a los que demostramos en el capítulo anterior para ordinales. Observemos que la relación de pertenencia E es conjuntista y bien fundada en Ω. Además, como Ω es transitiva, las clases E-Ω-transitivas son simplemente las subclases transitivas de Ω y $\mathrm{cl}_\Omega^E(\alpha) = \alpha$.

4.2 El axioma de regularidad

¿Puede existir un conjunto x con la propiedad de que $x = \{x\}$? Ciertamente, un conjunto así contradice la idea intuitiva que tenemos de lo que es (o debe ser) un conjunto, pero lo cierto es que los axiomas que hemos considerado hasta ahora no contradicen que pueda existir un conjunto así. El axioma de regularidad, que presentaremos aquí, tiene como finalidad erradicar posibilidades "patológicas" como ésta.

Pero no se trata de prohibir meramente la existencia de conjuntos que cumplan $x = \{x\}$, pues con eso no impediríamos que pudiera existir, por ejemplo, un conjunto $x = \{y\}$, con $y \neq x$, pero de modo que $y = \{x\}$. Una pareja de conjuntos $x = \{y\}$, $y = \{x\}$ no es menos patológica, pero es una patología distinta. Un tercer tipo de patología sería la existencia de una sucesión de conjuntos $\{x_n\}_{n\in\omega}$ tal que $\bigwedge n \in \omega\ x_n = \{x_{n+1}\}$. Lo que tienen en común estos ejemplos es que todos ellos dan lugar a una sucesión decreciente

$$\cdots \in x_4 \in x_3 \in x_2 \in x_1 \in x_0.$$

En el primer ejemplo, todos los términos de la sucesión serían iguales a x, mientras que en el segundo alternarían x e y. Y si tenemos una sucesión decreciente de este tipo, el conjunto $A = \{x_n \mid n \in \omega\}$ es un conjunto no vacío sin $\in$-minimal, pues ningún x_n es $\in$-minimal, ya que $x_{n+1} \in A \cap x_n$.

Por consiguiente, una forma de librarnos de todas estas patologías es tomar como axioma que todo conjunto está bien fundado. Eso es, ciertamente, lo que afirma el axioma de regularidad, pero antes de adoptar este axioma, para formarnos una idea clara de lo que supone, vamos a trabajar sin él y vamos a estudiar una clase de conjuntos libres de patologías como las que estamos considerando.

Como en la sección anterior, trabajaremos en NBG* + AI.

Definición 4.14 Un conjunto x es *regular* si su clausura transitiva $\mathrm{ct}\, x$ está bien fundada. Llamaremos R a la clase de los conjuntos regulares.

Observemos que no hubiera sido buena idea llamar conjuntos regulares a los conjuntos bien fundados. Por ejemplo, si $x = \{y\}$ con $y = \{x\}$ (pero $y \neq x$), entonces tanto x como y están bien fundados, pero el problema se pone de manifiesto en $\mathrm{ct}\, x = \mathrm{ct}\, y = \{x, y\}$, que no está bien fundada.

Vamos a cerciorarnos de que entre los conjuntos regulares no pueden darse patologías de las que estamos considerando. Empezamos probando sus propiedades básicas:

Teorema 4.15 *Se cumple:*

1. *R es una clase transitiva.*
2. *$\Omega \subset R$, luego R es una clase propia.*
3. *La relación de pertenencia está bien fundada en R.*
4. *$\mathcal{P}R = R$.*
5. *$\bigwedge A(R \cap \mathcal{P}A \subset A \to R \subset A)$.*
   En particular, $\bigwedge A(\mathcal{P}A \subset A \to R \subset A)$.

Demostración: 1) Se trata de probar que los elementos de los conjuntos regulares son regulares. Supongamos que $u \in v \in R$. Entonces $u \in \mathrm{ct}\, v$, luego $u \subset \mathrm{ct}\, v$, luego u está contenido en un conjunto transitivo y bien fundado, luego $u \in R$.

2) Todo ordinal es un conjunto transitivo y bien fundado, luego cumple la definición de conjunto regular.

3) Sea $A \subset R$ una clase no vacía y tomemos $y \in A$. Si $y \cap A = \varnothing$, entonces y es ya un $\in$-minimal de A. En caso contrario, sea $u \in y \cap A$. Como y es regular, su clausura transitiva está bien fundada. Definimos $x = \mathrm{ct}\, y \cap A$, que no es vacío, pues $u \in x$. Como $\mathrm{ct}\, y$ está bien fundada, x tiene un $\in$-minimal u, que es también un $\in$-minimal de A, ya que ciertamente $u \in x \subset A$ y si $v \in u \cap A$ entonces $v \in u \in x \subset \mathrm{ct}\, y$, luego $v \in \mathrm{ct}\, y$ por la transitividad de $\mathrm{ct}\, y$, luego $v \in u \cap x = \varnothing$, contradicción. Por lo tanto, $u \cap A = \varnothing$.

4) La inclusión $R \subset \mathcal{P}R$ es equivalente a la transitividad de R. Si $x \subset R$, entonces para cada $u \in x$ la clausura $\mathrm{ct}\, u$ está bien fundada, luego $\mathrm{ct}\, u \in R$, luego $\mathrm{ct}\, u \subset R$. Por 4.7 d) tenemos que $\mathrm{ct}\, x \subset R$, y esta clausura está bien fundada por 3), luego $x \in R$.

5) Si R no está contenida en A, por c) existe un $\in$-minimal $u \in R \setminus A$, pero entonces $u \in (R \cap \mathcal{P}A) \setminus A$. ∎

Observemos que 5) es un principio de inducción: si queremos probar que todo conjunto regular tiene una propiedad (pertenecer a la clase A) podemos tomar como hipótesis de inducción que todos los elementos de un conjunto regular x tienen la propiedad y demostrar a partir de ahí que x también la tiene.

En particular, sobre los conjuntos regulares está definida la aplicación rango dada por 4.10 (para la relación de pertenencia E). Explícitamente:

Definición 4.16 La aplicación *rango* es la aplicación $\operatorname{rang} : R \longrightarrow \Omega$ determinada por

$$\operatorname{rang} x = \bigcup_{y \in x} (\operatorname{rang} y + 1).$$

Para cada $\alpha \in \Omega$ definimos la clase $R_\alpha = \{x \in R \mid \operatorname{rang} x < \alpha\}$.

El teorema siguiente nos muestra qué es R:

Teorema 4.17 $R_0 = \varnothing \wedge \bigwedge \alpha\ R_{\alpha+1} = \mathcal{P}R_\alpha \wedge \bigwedge \lambda\ R_\lambda = \bigcup_{\delta<\lambda} R_\delta$,

$$R = \bigcup_{\alpha \in \Omega} R_\alpha.$$

Demostración: La única igualdad que no es trivial es $R_{\alpha+1} = \mathcal{P}R_\alpha$. Si $x \in \mathcal{P}R_\alpha$, entonces $x \subset R_\alpha$, luego

$$\operatorname{rang} x = \bigcup_{y \in x} (\operatorname{rang} y + 1) \leq \alpha < \alpha + 1,$$

luego $x \in R_{\alpha+1}$. Recíprocamente, si $x \in R_{\alpha+1}$, entonces todo $y \in x$ cumple $\operatorname{rang} y + 1 \leq \operatorname{rang} x < \alpha + 1$, luego $\operatorname{rang} y < \alpha$, luego $y \in R_\alpha$. Así pues, $x \subset R_\alpha$. ∎

Hay que señalar que el miembro derecho de la igualdad

$$R_\lambda = \bigcup_{\delta<\lambda} R_\delta$$

no puede entenderse como la unión de una familia de conjuntos $\{R_\delta\}_{\delta<\lambda}$, pues las clases R_δ no tienen por qué ser conjuntos. Hay que entender la igualdad como una forma cómoda de expresar que

$$\bigwedge x(x \in R_\lambda \leftrightarrow \bigvee \delta < \lambda\ x \in R_\delta),$$

y lo mismo vale para la igualdad del enunciado del teorema anterior. No obstante, si suponemos el axioma de partes (AP), entonces una inducción trivial prueba $\bigwedge \alpha\ \operatorname{cto} R_\alpha$, con lo que sí que podemos definir la sucesión transfinita de conjuntos $\{R_\alpha\}_{\alpha \in \Omega}$. De hecho, bajo AP podemos usar el teorema 4.17 como una definición alternativa de la clase R y del rango de un conjunto regular (que puede definirse entonces como el menor α tal que $x \subset R_\alpha$).

Como se muestra en el teorema siguiente, las clases R_α forman una sucesión transfinita creciente de clases transitivas y en cada nivel aparecen nuevos conjuntos (al menos un ordinal) que no están en los anteriores:

Teorema 4.18 *Se cumple:*

1. *Si $\alpha \leq \beta$ son ordinales, entonces $R_\alpha \subset R_\beta$.*
2. *Para cada ordinal α, la clase R_α es transitiva.*
3. *Para cada ordinal α, se cumple* $\operatorname{rang}\alpha = \alpha$*, luego $R_\alpha \cap \Omega = \alpha$.*

DEMOSTRACIÓN: a) es trivial.

b) Si $y \in x \in R_\alpha$, entonces $\operatorname{rang} y < \operatorname{rang} x < \alpha$, luego $y \in R_\alpha$.

c) Por inducción sobre α: si suponemos que $\operatorname{rang}\beta = \beta$ para todo $\beta < \alpha$, entonces

$$\operatorname{rang}\alpha = \bigcup_{\beta<\alpha} (\operatorname{rang}\beta + 1) = \bigcup_{\beta<\alpha} (\beta + 1) = \alpha. \qquad \blacksquare$$

Ahora ya podemos presentar el axioma de regularidad en condiciones de que se pueda valorar su contenido:

Teorema 4.19 *Las afirmaciones siguientes son equivalentes:*

1. $\bigwedge x(\operatorname{cto} x \wedge x \neq \varnothing \to \bigvee u \in x\ u \cap x = \varnothing)$.
2. *Todo conjunto está bien fundado.*
3. *Todo conjunto es regular, es decir, $V = R$.*

DEMOSTRACIÓN: La propiedad a) afirma que todo conjunto no vacío tiene un $\in$-minimal, y la propiedad b) es que todo subconjunto no vacío de todo conjunto tiene un $\in$-minimal. Es claro, pues, que a) $\Rightarrow$ b). También es obvio que si todo conjunto está bien fundado, entonces la clausura transitiva de todo conjunto está bien fundada, luego tenemos que b) $\Rightarrow$ c). Por último, si $V = R$, entonces la clase V está bien fundada, luego todos sus subconjuntos (todos los conjuntos) no vacíos tienen $\in$-minimal, luego c) $\Rightarrow$ a).

Aunque normalmente se hace referencia a él como $V = R$, lo habitual es tomar como axioma de regularidad la más simple de estas afirmaciones, es decir:

Axioma de regularidad (V=R) $\bigwedge x(\operatorname{cto} x \wedge x \neq \varnothing \to \bigvee u \in x\ u \cap x = \varnothing)$.

Este axioma es el menos relevante de toda la teoría de conjuntos. Ello se debe a que todas las construcciones conjuntistas realizadas a partir de conjuntos regulares dan lugar a conjuntos regulares, hecho que se sigue inmediatamente de la propiedad $\mathcal{P}R = R$.

Por ejemplo, si $x, y \in R$, entonces $\{x, y\} \in \mathcal{P}R = R$, de donde a su vez $(x, y) \in \mathcal{P}R = R$, luego si A y B son conjuntos regulares, $A \times B \in \mathcal{P}R = R$, y lo mismo vale para toda $f : A \longrightarrow B$, y (suponiendo AP) para el conjunto B^A de todas las aplicaciones de A en B, etc.

Uniendo esto a que todos los ordinales son regulares, y en particular lo es el conjunto de los números naturales, y teniendo en cuenta que todos los conjuntos que los matemáticos consideran habitualmente están construidos mediante

las operaciones conjuntistas básicas que ya conocemos (uniones, intersecciones, productos cartesianos, conjuntos de partes, conjuntos de sucesiones o de funciones de un conjunto en otro, etc.) partiendo en último extremo del conjunto de los números naturales, resulta en definitiva que los matemáticos trabajan exclusivamente con conjuntos regulares, independientemente de que la teoría de conjuntos admita o no la existencia de conjuntos "patológicos".

Por ello, postular que todo conjunto es regular no debe verse como una afirmación profunda sobre la naturaleza de los conjuntos, sino más bien como algo análogo a lo que hace un algebrista cuando dice "sólo voy a considerar anillos conmutativos y unitarios", lo cual no signifique que niegue la existencia de anillos más generales, sino que simplemente anuncia que no va a ocuparse de ellos.

Así pues, lo único que hace el axioma de regularidad es restringir el alcance de la teoría a los conjuntos que realmente nos van a interesar. Naturalmente, esto no contradice que alguien pueda considerar que los conjuntos no regulares, no sólo no interesan, sino que son una perversión de la idea de conjunto y que al erradicarlos sólo estamos aumentando la fidelidad de la noción formal de conjunto a nuestra idea intuitiva de conjunto.

Cuando se asume el axioma de regularidad, es habitual escribir $V_\alpha \equiv R_\alpha$, de modo la clase universal queda estructurada en la jerarquía transfinita creciente de clases transitivas (conjuntos si suponemos AP) dada por:

$$\mathrm{V}_0 = \varnothing \quad \wedge \quad \bigwedge\alpha\ \mathrm{V}_{\alpha+1} = \mathcal{P}\mathrm{V}_\alpha \quad \wedge \quad \bigwedge\lambda\ \mathrm{V}_\lambda = \bigcup_{\delta<\lambda} \mathrm{V}_\delta \quad \wedge \quad \mathrm{V} = \bigcup_{\alpha\in\Omega} \mathrm{V}_\alpha,$$

y así todo conjunto puede pensarse como construido a partir de $\varnothing$ en una cantidad transfinita de pasos, en el sentido de que si rastreamos sus elementos y los elementos de sus elementos, etc. siempre terminamos en $\varnothing$.

El rango está entonces definido para todos los conjuntos, y es una medida de su complejidad, del número de pasos que hay que dar para obtenerlo en la jerarquía de los conjuntos regulares.

Si suponemos AP, tenemos una distinción intrínseca entre los conjuntos y las clases propias, es decir, un criterio que nos permite distinguir si una clase es o no un conjunto sin más que analizar sus elementos:

Teorema 4.20 *Una clase es propia si y sólo si contiene conjuntos de rango arbitrariamente grande.*

DEMOSTRACIÓN: Si todos los elementos de una clase X tienen rango menor que un ordinal α entonces $X \subset \mathrm{V}_\alpha$, luego X es un conjunto. Recíprocamente, si X es un conjunto, la imagen de X por la aplicación rango es un subconjunto de Ω (por el axioma del reemplazo), luego está acotado. ∎

Así pues, las clases propias son las clases que contienen "demasiados elementos" como para caber en un conjunto V_α, las que se distribuyen por toda la jerarquía de los conjuntos V_α de modo que ningún conjunto es suficientemente grande como para contenerlas.

4.3 El axioma de elección

Consideremos la afirmación siguiente:

Principio de elecciones dependientes (ED) *Para todo conjunto $A \neq \varnothing$ y toda relación $R \subset A \times A$ tal que $\bigwedge a \in A \bigvee b \in A\, b\, R\, a$, existe $f : \omega \longrightarrow A$ tal que $\bigwedge n \in \omega\ f(n+1)\, R\, f(n)$.*

Y consideremos la siguiente "demostración":

> Como A no es vacío, podemos tomar $x_0 \in A$. Por hipótesis existe un $x_1 \in A$ tal que $x_1\, R\, x_0$, por el mismo motivo, existe un $x_2 \in A$ tal que $x_2\, R\, x_1$. Como este proceso puede prolongarse indefinidamente, concluimos que existe una sucesión $\{x_n\}_{n\in\omega}$ de elementos de A tal que $\bigwedge n \in \omega\ x_{n+1}\, R\, x_n$, pero tal sucesión no es sino una función $f : \omega \longrightarrow A$ que cumple lo requerido.

Cualquier matemático daría esto por bueno, pero, si pretende ser una demostración a partir de los axiomas que hemos considerado hasta ahora, lo cierto es que no lo es. La existencia de la sucesión $\{x_n\}_{n\in\omega}$ no puede ser demostrada a partir del hecho de que R no está bien fundada en A (no si tomamos como única base admisible los axiomas que estamos considerando).

Para entender cuál es el fallo, observemos que lo que se pretende es afirmar la existencia de una cierta función $f : \omega \longrightarrow A$, una función con la propiedad de que $\bigwedge n \in \omega\ f(n+1)\, R\, f(n)$, pero ¿cuál es esa función? ¿cómo y cuándo hemos probado su existencia?

Lo que hemos probado es que existe una función $s_1 : 2 \longrightarrow A$ tal que $s_1(1) \in s_1(0)$, y luego hemos probado que puede extenderse hasta una función $s_2 : 3 \longrightarrow A$ tal que $s_2(2) \in s_2(1) \in s_2(0)$, y de ahí hemos pasado a afirmar directamente la existencia de f sin más explicaciones. ¿Es posible justificar ese último paso?

Obviamente, ningún matemático aceptará que porque algo se cumpla para $0, 1, 2$ (en nuestro contexto, trivialmente para 0), se vaya a cumplir en general, pero no es extraño que los matemáticos den saltos así cuando son justificables por argumentos inductivos. Ahora bien, en nuestro caso, si continuamos el argumento por inducción, lo que podemos demostrar sin dificultad es que

$$\bigwedge n \bigvee s(s : n+1 \longrightarrow A \wedge \bigwedge i < n\ s(i+1)\, R\, s(i)).$$

Hasta aquí todo es correcto, pero ¿cómo se obtiene la existencia de f a partir de aquí?

Un matemático podría decir: "para cada $n \in \omega$, tomemos $s_n : n+1 \longrightarrow A$ en las condiciones indicadas". Eso es admisible en la práctica habitual del matemático, pero no es una consecuencia lógica de los axiomas que hemos visto hasta el momento. Una cosa es que, fijado un n, la lógica nos dice que podemos eliminar los cuantificadores y considerar un s que cumpla lo indicado, e incluso que podemos llamarlo s_n si preferimos llamarlo así, pero otra cosa muy distinta, y que está implícita en lo que entiende el matemático al "tomar s_n", es afirmar

la existencia de una función s que a cada n le asigne una sucesión finita s_n. La existencia de semejante función s no es una consecuencia de eliminar un par de cuantificadores, es una afirmación sobre la existencia de un conjunto que tendría que ser respaldada por algún axioma que justifique la existencia de tal conjunto. Y, aun suponiendo que tuviéramos a nuestra disposición tal función s, nada nos garantiza que cada s_{n+1} fuera una extensión de s_n, cosa que nos haría falta si quisiéramos definir f a partir de s.

Si el lector se convence de que por ahí no hay salida, tal vez pase a considerar la posibilidad de que f pueda definirse por recursión: fijamos $x_0 \in A$ y aplicamos el teorema 3.22 para concluir que existe una función $f : \omega \longrightarrow A$ tal que $f(0) = x_0$ y, para cada $n \in \omega$, $f(n+1)$ es cualquier elemento de A tal que $f(n+1)\,R\,f(n)$, que existe por hipótesis.

Tenemos aquí una aplicación incorrecta del teorema de recursión, pues éste exige que $f(n) = G(f|_n)$, para una cierta función G, definida en este caso sobre el conjunto $X_\omega \equiv \{s \mid \bigvee n \in \omega\ s : n \longrightarrow A\}$ pero ¿cuál es en nuestro caso la función G? Debería ser algo así como

$$G(s) = \begin{cases} x_0 & \text{si } \mathcal{D}s = \varnothing, \\ x & \text{si } \mathcal{D}s = n+1 \wedge x \in A \wedge x\,R\,s(n), \end{cases}$$

pero esto no es una definición aceptable de una función. La única forma aceptable de definir una clase es mediante el axioma de comprensión. Habría que expresar G en la forma $G = \{z \mid \phi(z)\}$, para una cierta propiedad normal $\phi(z)$ o, si se prefiere, usando los convenios de notación que hemos establecido,

$$G = \{(s,x) \in X_\omega \times A \mid \phi(s,x)\},$$

pero esto no es posible (y no por culpa del requisito de normalidad, que no afecta aquí para nada, pues tratamos únicamente con conjuntos). El planteamiento debería ser algo así como:

$$G = \{(s,x) \in X_\omega \times A \mid \bigvee m \in \omega(s : m \longrightarrow A \wedge$$

$$((m = 0 \wedge x = x_0) \vee (\bigvee n \in \omega(m = n+1 \wedge x\,R\,s(n))))\},$$

pero esto no define necesariamente una función, pues para un mismo $s \in X_\omega$, nada impide que haya varios $x \in A$ que cumplan la condición requerida para que $(s,x) \in G$, y entonces s no tiene una única imagen.

El problema es que, aunque tengamos garantizado que existe un x que cumple una condición (en este caso $x\,R\,s(n)$), la lógica permite formalizar la idea de "tomar uno de ellos" para razonar con él, pero no permite formalizar la idea de "tomar uno cualquiera, pero sólo uno", que es lo que necesitaríamos para definir G y, a la larga, para construir f.

Esto no significa que los intentos de razonamiento que hemos expuesto estén mal en términos absolutos, sino que requieren un axioma más, el llamado axioma de elección, el cual, junto con los otros axiomas que hemos discutido hasta aquí,

completa la teoría NBG. En nuestro caso concreto, para llevar a buen puerto nuestros intentos de construir f, sólo necesitamos una función $E : \mathcal{P}A \longrightarrow A$ con la propiedad de que

$$\bigwedge X(X \subset A \wedge X \neq \varnothing \to E(X) \in X),$$

es decir, una función que elija un elemento de cada subconjunto no vacío de A. La función E resuelve todos nuestros problemas, pues ahora podemos definir

$$f(0) = x_0 \wedge \bigwedge n \in \omega\ f(n+1) = E(\{x \in A \mid x\, R\, f(n)\}),$$

que es una aplicación legítima del teorema de recursión, correspondiente a la función

$$G(s) = \begin{cases} x_0 & \text{si } \mathcal{D}s = \varnothing, \\ E(\{x \in A \mid x\, R\, s(n)\}) & \text{si } \mathcal{D}s = n+1, \end{cases}$$

que, si se quiere, se puede expresar sin dificultad como una clase definida de acuerdo con el axioma de comprensión.

En general, el enunciado del axioma de elección es como sigue:

Axioma de elección (AE)

$$\bigwedge X(\mathrm{cto}\, X \to \bigvee f(f : X \longrightarrow V \wedge \bigwedge u \in X(u \neq \varnothing \to f(u) \in u)).$$

Así, AE afirma que, dado cualquier conjunto X, existe una función que a cada elemento $u \in X$ no vacío le elige uno de sus elementos. A una función de estas características se la llama una *función de elección* sobre X.

Observemos que no siempre es necesario apelar al axioma de elección para obtener una función de elección. Por ejemplo, imaginemos que restringimos el problema que hemos planteado al principio de esta sección a una relación R definida sobre $A = \omega$. Entonces podemos demostrar la existencia de una función de elección tomando, por ejemplo,

$$E(X) = \begin{cases} \varnothing & \text{si } X = \varnothing, \\ \min X & \text{si } X \neq \varnothing, \end{cases}$$

y la existencia de la sucesión $\{x_n\}_{n\in\omega}$ puede justificarse, por consiguiente, sin necesidad de AE.

Así pues, el axioma de elección sólo es necesario para garantizar la existencia de funciones de elección en ausencia de un criterio explícito que permita construir una. Las situaciones en las que carecemos de tal criterio son muy frecuentes. Ya hemos visto una: si partimos de una relación R en una clase A y sabemos que para cada $a \in A$ el conjunto $A_a^R = \{b \in A \mid b\, R\, a\}$ no es vacío, ello no nos da un criterio para elegir uno de sus elementos para cada $x \in A$, y necesitamos recurrir al axioma de elección.

En definitiva, el axioma de comprensión y el axioma de elección son los únicos axiomas de NBG que permiten probar la existencia de una clase con unas

características determinadas (los demás axiomas, salvo el de extensionalidad, que no es un axioma existencial, se limitan a afirmar que ciertas clases dadas de antemano son conjuntos).

Teniendo en cuenta estas consideraciones, el ejemplo que hemos discutido se traduce finalmente en el teorema siguiente (en el que hemos modificado ligeramente el argumento para evitar el uso de AP):

Teorema 4.21 (AI) AE → ED.

DEMOSTRACIÓN: Consideremos un conjunto A y una relación R en las condiciones de ED. Consideremos el conjunto $X = \{A^R_a \mid a \in A\}$ que, por hipótesis, es una familia de conjuntos no vacíos. Sea $f : X \longrightarrow A$ una función de elección y sea $g : A \longrightarrow A$ la función dada por $g(a) = f(A^R_a)$. De este modo se cumple que $\bigwedge a \in A\,(g(a) \in A \wedge g(a)\,R\,a)$.

Ahora fijamos un $a_0 \in A$ y definimos por recurrencia una función $x : \omega \longrightarrow A$ mediante $x_0 = a_0 \wedge x_{n+1} = g(x_n)$. Es claro que la sucesión $\{x_n\}_{n\in\omega}$ cumple lo requerido. ∎

Como ya hemos explicado en la discusión previa a este teorema, no hay que confundir el uso del axioma de elección con la eliminación de un cuantificador existencial. En las páginas precedentes hemos tenido incontables ocasiones de pasar de una premisa del tipo $\bigvee x\ x \in A$ a elegir un $x \in A$ para razonar con él, y no importa que no tengamos ningún criterio específico para seleccionar un elemento de A en concreto, que ello no supone el uso del axioma de elección (ni del axioma de comprensión), sino que es una mera consecuencia lógica de la premisa: estamos usando la existencia de un $x \in A$ y la premisa afirmaba precisamente la existencia de un x en A. En cambio, si tenemos una familia $\{X_i\}_{i\in I}$ de conjuntos no vacíos, esto significa que $\bigwedge i \in I \bigvee x\ x \in X_i$, y de aquí no podemos pasar a considerar una sucesión $\{x_i\}_{i\in I}$ tal que $\bigwedge i \in I\ x_i \in X_i$ sin recurrir al axioma de comprensión (si tenemos algún criterio explícito para seleccionar un elemento de cada X_i) o al axioma de elección (si no lo tenemos), pues la conclusión va más allá de lo contenido en la premisa: partimos de la existencia de conjuntos en cada X_i y pretendemos concluir la existencia de un conjunto que no es ninguno de los conjuntos cuya existencia se postula, sino una aplicación $x : I \longrightarrow \bigcup_{i\in I} X_i$.

No obstante, a partir del hecho de que podemos eliminar cuantificadores existenciales, podemos probar un caso particular del axioma de elección incluso en ausencia de criterios para realizar las elecciones. Se trata de que todo conjunto finito siempre admite una función de elección.

En 2.9 hemos definido el concepto de "conjunto finito" en términos de un sistema de Peano arbitrario, pero es claro que en términos de ω puede reformularse así:

Un conjunto es finito si $\bigvee n \in \omega \bigvee f\ f : n \longrightarrow x$ biyectiva).

Aquí usamos que, con la notación de la sección 2.2 todo $n \in \omega$ cumple que $n = I^*_n$, y es equipotente a I_n.

Teorema 4.22 *Todo conjunto finito tiene una función de elección.*

DEMOSTRACIÓN: Basta probar, por inducción sobre n, que

$$\bigwedge x(\bigvee f\ f : n \longrightarrow x \text{ biyectiva} \to x \text{ tiene una función de elección}).$$

En efecto, para $n = 0$ tenemos que $x = \varnothing$ y $h = \varnothing$ es trivialmente una función de elección en x. Si es cierto para n, supongamos que $f : n+1 \longrightarrow x$ biyectiva, sea $u = f(n)$ y $x' = f[n]$. Es claro entonces que $f|_n : n \longrightarrow x'$ biyectiva, luego por hipótesis de inducción existe una función de elección $h : x' \longrightarrow V$. Si $u \neq \varnothing$, tomamos $v \in u$, y si $u = \varnothing$ tomamos $v = \varnothing$. Es claro entonces que $h \cup \{(u, v)\}$ es una función de elección sobre x. ∎

En cambio, no es posible demostrar sin el axioma de elección que todo conjunto numerable tiene una función de elección. Sin embargo, para una gran parte de las matemáticas que requieren el axioma de elección basta con el siguiente caso particular:

Axioma de elección numerable (AEN) *Todo conjunto numerable tiene una función de elección.*

O a lo sumo con el principio de elecciones dependientes ED, que es ligeramente más fuerte, como se ve en el teorema siguiente:

Teorema 4.23 (AI, AP) ED → AEN.

DEMOSTRACIÓN: Sea $X = \{x_n \mid n < \omega\}$ un conjunto numerable y sea A el conjunto de las funciones de elección sobre conjuntos $X_m = \{x_n \mid n < m\}$, es decir, $f \in A$ si y sólo si existe un $m \in \omega$ tal que $f : X_m \longrightarrow \{\varnothing\} \cup \bigcup_{n<m} x_n$ cumple que $\bigwedge n < m(x_n \neq \varnothing \to f(x_n) \in x_n)$.

Claramente $A \neq \varnothing$ y podemos definir en A la relación dada por $f\,R\,g$ si y sólo si $g \subsetneq f$. Así A y R cumplen las hipótesis de ED, pues si $g \in A$ y $\mathcal{D}f = \{x_n \mid n < m\}$, si $x_m \neq \varnothing$ tomamos un $u \in x_m$, y en caso contrario tomamos $u = \varnothing$, de modo que $f = g \cup \{(x_m, u)\}$ cumple $f \in A \wedge f\,R\,g$. Por ED existe una sucesión $\{f_n\}_{n<\omega}$ de elementos de A de modo que

$$\bigwedge n < \omega(f_n \in A \wedge f_n \subsetneq f_{n+1}).$$

Es claro entonces que $f = \bigcup_{n\in\omega} f_n : X \longrightarrow V$ y es una función de elección sobre X. ∎

Nota Observemos que ED no puede probarse[2] a partir de AEN, pues en la prueba de ED a partir de AE hemos necesitado una función de elección sobre el conjunto de todos los conjuntos de la forma A_a^R, que no es necesariamente numerable. Al final, lo que proporciona ED es una cantidad numerable de elecciones, al igual que AEN, pero las elecciones de ED son "dependientes" en el sentido de

[2]No estamos aquí en condiciones de justificar ningún resultado negativo de este tipo. Esta nota sólo pretende explicar por qué es imposible, sin probarlo realmente

que se elige x_{n+1} en función de cuál es el x_n elegido previamente (más precisamente, elegimos x_{n+1} en el conjunto $A^R_{x_n}$, que depende de la elección anterior), mientras que AEN sólo proporciona una cantidad numerable de elecciones independientes (fijamos un conjunto numerable y elegimos un elemento de cada uno de sus elementos, sin tener en cuenta cuál hemos elegido en otro cualquiera de ellos). ∎

Otra consecuencia de ED (luego de AE) que no puede probarse a partir de AEN es esta caracterización de las relaciones bien fundadas:

Teorema 4.24 (AI, ED) *Una relación R está en un conjunto A está bien fundada si y sólo si no existe ninguna sucesión $\{x_n\}_{n\in\omega}$ de elementos de A tal que $\bigwedge n \in \omega\ x_{n+1}\,R\,x_n$.*

Demostración: Una implicación es inmediata y no requiere ninguna forma de AE: si existe tal sucesión, entonces el conjunto $B = \{x_n \mid n \in \omega\}$ es un subconjunto no vacío de A que no tiene R-minimal, luego la relación no está bien fundada.

Supongamos ahora que la relación R no está bien fundada, con lo que existe un $B \subset A$ no vacío sin R-minimal. Esto quiere decir que si $x \in B$, al no ser R-minimal existe un $y \in B$ tal que $y\,R\,x$, pero esto significa que B y R cumplen las hipótesis de ED, luego existe una sucesión $\{x_n\}_{n\in\omega}$ de elementos de B (luego de A) que cumple la condición del enunciado. ∎

Veamos un uso típico del axioma de elección numerable:

Teorema 4.25 (AEN) *Toda unión numerable de conjuntos numerables es numerable.*

Demostración: Sea $\{A_n\}_{n\in\omega}$ una familia de conjuntos numerables. Cambiando cada A_n por $A_n \setminus \bigcup_{m<n} A_m$ tenemos otra familia de conjuntos numerables con la misma unión, pero que además son disjuntos dos a dos, luego no perdemos generalidad si suponemos que los A_n dados son disjuntos dos a dos.

La razón por la que necesitamos el uso del axioma de elección para probar que su unión es numerable es que necesitamos elegir funciones inyectivas $f_n : A_n \longrightarrow \omega$. Una vez elegidas, ya es elemental que podemos formar una función inyectiva $f : \bigcup_{n\in\omega} A_n \longrightarrow \omega \times \omega$ mediante $f(a) = (n, f_n(a))$, donde n es el único número natural tal que $a \in A_n$. Como $\omega \times \omega$ es numerable, concluimos que $\bigcup_{n\in\omega} A_n$ también lo es. ∎

Hay un resultado que parece muy elemental, pero en realidad requiere el axioma de elección:

Teorema 4.26 (AE) *Sean x e y dos conjuntos no vacíos. Existe $f : x \longrightarrow y$ inyectiva si y sólo si existe $g : y \longrightarrow x$ suprayectiva.*

DEMOSTRACIÓN: Supongamos que existe $f : x \longrightarrow y$ inyectiva y veamos cómo construir la aplicación g. Esta implicación no requiere el axioma de elección, pues basta tomar un $u \in x$ y definir

$$g(v) = \begin{cases} f^{-1}(v) & \text{si } v \in f[x], \\ u & \text{si } v \in y \setminus f[x]. \end{cases}$$

Es claro entonces que g es suprayectiva. Más aún, es claro que $f \circ g = I_x$, luego la suprayectividad de g es consecuencia del teorema 1.13.

Supongamos ahora que $g : y \longrightarrow x$ suprayectiva y sea

$$X = \{g^{-1}[u] \mid u \in x\},$$

que es un conjunto por reemplazo (la aplicación $x \longrightarrow X$ dada por $u \mapsto g^{-1}[u]$ es suprayectiva). Por el axioma de elección, existe una función de elección $E : X \longrightarrow V$. Definimos $f : x \longrightarrow y$ mediante $f(u) = E(g^{-1}[u])$. De este modo, para cada $u \in x$ tenemos que $f(u) \in g^{-1}[u]$, luego $g(f(u)) = u$, luego $f \circ g = I_x$ y de nuevo 1.13 implica que f es inyectiva. ∎

Notemos que el teorema anterior no requiere el axioma de elección si suponemos que existe un buen orden en y (lo que sucede, por ejemplo, si $y = \omega$), pues entonces podemos definir la función de elección como $E(a) = \text{mín } a$, para todo $a \in X$, pues se cumple que $a \subset y$.

Si al teorema anterior le añadimos la condición $f \circ g = I_x$ que hemos obtenido en la prueba, tenemos de hecho una equivalencia con el axioma de elección. La probamos a continuación junto con otras más:

Teorema 4.27 *Las afirmaciones siguientes son equivalentes:*

1. AE
2. *Si $g : y \longrightarrow x$ es una aplicación suprayectiva, existe $f : x \longrightarrow y$ tal que $f \circ g = I_x$.*
3. *Para toda familia $\{X_i\}_{i\in I}$ de conjuntos no vacíos (donde I es un conjunto) existe otra familia $\{s_i\}_{i\in I}$ tal que $\bigwedge i \in I\ s_i \in x_i$.*
4. *Para todo conjunto X formado por conjuntos no vacíos disjuntos dos a dos, existe un conjunto $a \subset \bigcup X$ tal que $\bigwedge u \in X \bigvee v\ u \cap a = \{v\}$.*

DEMOSTRACIÓN: 1) ⇒ 2) se sigue de la demostración del teorema anterior.

2) ⇒ 3) Consideremos la aplicación $g : \bigcup_{i\in I} \{i\} \times X_i \longrightarrow I$ dada por $g(i, u) = i$. Como los conjuntos X_i son no vacíos, tenemos que g es suprayectiva. Sea $f : I \longrightarrow \bigcup_{i\in I} (\{i\} \times X_i)$ según 2), es decir, tal que, para cada $i \in I$, se cumple que $f(i) = (i, v)$, para cierto $v \in X_i$. Basta tomar $s = \mathcal{R}f$.

3) ⇒ 4) Podemos ver a X como una familia $\{i\}_{i\in X}$ de conjuntos no vacíos. Por 3) existe $\{s_i\}_{i\in X}$ tal que $\bigwedge i \in X\ s_i \in i$. Basta tomar $a = \mathcal{R}s$.

4) $\Rightarrow$ 1) Dado un conjunto X, no perdemos generalidad si suponemos que no contiene a $\varnothing$. El conjunto $X' = \{\{i\} \times i \mid i \in X\}$ está formado por conjuntos no vacíos disjuntos dos a dos. Por 4) existe un conjunto f que contiene exactamente un elemento de cada uno de ellos. Es claro que f es una función de elección sobre X. ∎

Nota La familia $\{s_i\}_{i\in I}$ no es más que un elemento del producto cartesiano

$$\prod_{i\in I} X_i \equiv \{s \mid s : I \longrightarrow \bigcup_{i\in I} X_i \wedge \bigwedge i \in I\ s_i \in X_i\},$$

por lo que AE resulta ser equivalente a que el producto cartesiano de una familia de conjuntos no vacíos es no vacío. ∎

El axioma de elección interviene de forma esencial en la demostración de numerosos teoremas importantes del álgebra, el análisis o la topología (para probar la existencia de base en todo espacio vectorial, la existencia de ideales maximales en anillos unitarios, la existencia de clausuras algebraicas, el teorema de Tychonoff, el teorema de Hann-Banach, etc.) En la prueba de estos resultados y otros muchos, es mucho más práctico utilizar una forma equivalente, un tanto técnica, conocida como lema de Zorn:

Una *cadena* en un conjunto parcialmente ordenado X es un subconjunto $C \subset X$ para el que se cumpla $\bigwedge uv \in C(u \leq v \vee v \leq u)$. El teorema siguiente contiene el enunciado del lema de Zorn junto con otras afirmaciones equivalentes menos técnicas:

Teorema 4.28 (AP) *Las afirmaciones siguientes son equivalentes:*

1. **Axioma de elección** *Todo conjunto tiene una función de elección.*
2. **Principio de numerabilidad** *Todo conjunto puede biyectarse con un ordinal.*
3. **Principio de buena ordenación** *Todo conjunto puede ser bien ordenado.*
4. **Lema de Zorn** *Todo conjunto parcialmente ordenado no vacío en el que toda cadena tenga una cota superior tiene un elemento maximal.*
5. **Lema de Zorn (variante)** *En todo conjunto parcialmente ordenado no vacío en el que toda cadena tenga una cota superior, cada elemento está por debajo de un elemento maximal.*

Demostración: 1) $\Rightarrow$ 2) Supongamos que un conjunto x no puede biyectarse con ningún ordinal. En particular tenemos que $x \neq \varnothing$. Fijemos una función de elección $f : \mathcal{P}x \longrightarrow x$. El teorema de recursión 3.22 nos da una función $F : \Omega \longrightarrow x$ tal que

$$\bigwedge \alpha \in \Omega\ F(\alpha) = f(x \setminus F[\alpha]).$$

Veamos por inducción sobre α que $F|_\alpha : \alpha \longrightarrow x$ inyectiva.

Si $\alpha = 0$ es trivial. Si es cierto para α, entonces $F[\alpha] \neq x$, porque estamos suponiendo que x no puede biyectarse con un ordinal. Entonces, puesto que $x \setminus F[\alpha] \neq \varnothing$, tenemos que $F(\alpha) = f(x \setminus F[\alpha]) \in x \setminus F[\alpha]$, de donde se sigue claramente que $F|_{\alpha+1}$ es inyectiva.

Si λ es un ordinal límite y $F|_\alpha$ es inyectiva para todo $\alpha < \lambda$, entonces es claro que $F|_\lambda$ es inyectiva, pues si $\delta < \epsilon < \lambda$, también $\delta < \epsilon < \epsilon + 1 < \lambda$, y la inyectividad de $F|_{\epsilon+1}$ implica que $F(\delta) \neq F(\epsilon)$.

A su vez esto implica que $F : \Omega \longrightarrow x$ inyectiva, pero esto es imposible, pues entonces $F[\Omega] \subset x$ sería un conjunto y por reemplazo también lo sería Ω.

2) $\Rightarrow$ 3) es inmediato: dado un conjunto x, tomamos un ordinal α y una biyección $f : x \longrightarrow \alpha$ y definimos la relación en x dada por $u \leq v \leftrightarrow f(u) \leq f(v)$. Es inmediato comprobar que se trata de un buen orden en x.

3) $\Rightarrow$ 5) Sea $(x, \leq)$ un conjunto en las hipótesis del lema de Zorn y fijemos un $u_0 \in x$. Hemos de encontrar un elemento maximal $m \in x$ tal que $u_0 \leq m$. Para ello suponemos que no existe tal elemento maximal, es decir, que si $u_0 \leq v$, siempre existe un $v' \in x$ tal que $v < v'$.

Como consecuencia, si $c \subset x$ es una cadena tal que $u_0 \in c$, existe un $v \in x$ tal que $\bigwedge u \in c\ u < v$. En efecto, estamos suponiendo que la cadena tiene cota superior, es decir, que existe un $v \in x$ tal que $\bigwedge u \in c\ u \leq v$. En particular, $u_0 \leq v$, luego, según acabamos de indicar, existe un $v' \in x$ tal que $v < v'$, y este v' cumple lo pedido.

De acuerdo con 3), fijamos un buen orden $(x, \trianglelefteq)$ en el conjunto x. Consideramos la función $G : V \longrightarrow x$ dada por $G(s) = v$ si y sólo si $\mathcal{R}s$ es una cadena en x que contiene a u_0 y entonces v es el mínimo respecto de la relación $\trianglelefteq$ del conjunto $\{v \in x \mid \bigwedge u \in \mathcal{R}s\ u < v\}$, o bien $v = u_0$ en cualquier otro caso.

El teorema de recursión 3.22 nos da una función $F : \Omega \longrightarrow x$ determinada por la condición $F(\alpha) = G(F|_\alpha)$. Como $\mathcal{R}F|_0 = \varnothing$ no contiene a u_0, la definición de G nos da que $F(0) = u_0$.

Veamos por inducción sobre α que $\bigwedge \delta < \alpha\ F(\delta) < F(\alpha)$.

Suponemos que el resultado es cierto para todo $\alpha < \beta$, y podemos suponer que $\beta > 0$, pues en caso contrario no hay nada que probar. Tenemos, pues, que si $\delta < \alpha < \beta$, entonces $F(\delta) < F(\alpha)$, lo que implica que $\mathcal{R}(F|_\beta) = F[\beta]$ es una cadena en x que contiene a $F(0) = u_0$. Por lo tanto, por definición de G, tenemos que $F(\beta)$ cumple $\bigwedge u \in F[\beta]\ u < F(\beta)$, pero esto es justo lo que teníamos que probar.

Consecuentemente tenemos que $F : \Omega \longrightarrow x$ inyectiva, pero eso es imposible, porque entonces $F[\Omega] \subset x$ sería un conjunto y por reemplazo Ω también.

5) $\Rightarrow$ 4) es trivial.

4) $\Rightarrow$ 1) Fijemos un conjunto x, que podemos suponer no vacío y tal que $\varnothing \notin x$, y sea

$$y = \{p \in \mathcal{P}(x \times \bigcup x) \mid \bigvee a(a \subset x \wedge p : a \longrightarrow \bigcup x \wedge \bigwedge u \in a(u \neq \varnothing \to p(u) \in u))\}$$

el conjunto de las funciones de elección sobre subconjuntos de x. Notemos que $\varnothing \in y$, luego $y \neq \varnothing$. Consideramos en y el orden parcial dado por la inclusión. Es claro que si $c \subset y$ es una cadena, entonces tiene por cota superior a $\bigcup c$, luego el lema de Zorn nos da un $f : a \longrightarrow \bigcup x$ en y maximal respecto de la inclusión. Basta probar que $a = x$, pues entonces f es una función de elección sobre x.

En caso contrario, tomamos $u \in x \setminus a$ y $v \in u$ (lo cual es posible, pues estamos suponiendo que $\varnothing \notin x$). Es claro entonces que $f \cup \{(u, v)\} \in y$ y contradice la maximalidad de f. Así pues, $a = x$. ∎

El principio de numerabilidad afirma que los ordinales bastan para "contar" cualquier conjunto, es decir, que todo conjunto se puede poner en la forma $\{x_\alpha\}_{\alpha<\beta}$, para cierto ordinal β.

De la demostración del teorema anterior se sigue, más concretamente, que un conjunto x admite un buen orden si y sólo si $\mathcal{P}x$ admite una función de elección. Una implicación es trivial, pues un buen orden en x permite definir una función de elección en $\mathcal{P}x$ mediante

$$E(u) = \begin{cases} \text{mín}\, u & \text{si } u \neq \varnothing, \\ \varnothing & \text{si } u = \varnothing. \end{cases}$$

Veamos ahora una aplicación del lema de Zorn que requiere el concepto de ideal de un anillo, definido en el apartado "Ideales y anillos cociente" de la sección 1.7:

Teorema 4.29 (AP, AE) *Si A es un anillo conmutativo y unitario, e $I \subsetneq A$ es un ideal, existe un ideal maximal M tal que $I \subset M \subsetneq A$.*

Demostración: Sea $\mathcal{M}$ el conjunto de todos los ideales[3] de A distintos de A. Consideramos en $\mathcal{M}$ el orden dado por la inclusión. De la propia definición de ideal maximal se sigue que un ideal maximal de A es simplemente un elemento maximal de $\mathcal{M}$, luego basta probar que $\mathcal{M}$ cumple las hipótesis del lema de Zorn. Ciertamente, $\mathcal{M} \neq \varnothing$, pues $\{0\} \in \mathcal{M}$ (notemos que $\{0\} \subset I \subsetneq A$). Si $C \subset \mathcal{M}$ es una cadena (que podemos suponer no vacía), es fácil ver que $I = \bigcup C$ es un ideal de A. En efecto:

1. Si $J \in C$, tenemos que $0 \in J \subset I$.

2. Si $x, y \in I$, entonces existen $J_1, J_2 \in C$ tales que $x \in J_1$, $y \in J_2$. Como C es una cadena existe un $J \in C$ tal que $J_1, J_2 \subset J$, luego $x, y \in J$, luego $x + y \in J \subset I$.

[3]Se cumple que $\mathcal{M}$ es un conjunto porque $\mathcal{M} \subset \mathcal{P}A$, y estamos suponiendo AP.

3. Si $x \in I$, $a \in A$, existe un $J \in C$ tal que $x \in J$, luego $ax \in J \subset C$.

Además $I \neq A$, pues en caso contrario $1 \in I$, luego existe un $J \in C$ tal que $1 \in J$, luego $J = A$, en contradicción con que $J \in \mathcal{M}$. Esto implica que $I \in \mathcal{M}$ y es claramente una cota superior de C. ∎

El siguiente teorema que vamos a probar es en realidad un caso particular del anterior, pero en estos momentos no estamos en condiciones de ver que es así (véanse las observaciones tras la definición 7.7). En [T 1.50] hemos introducido el concepto de filtro en un conjunto, cuya definición reproducimos aquí:

Definición 4.30 Sea X un conjunto no vacío. Un *filtro* en X es una familia F de subconjuntos de X tal que:

1. $\varnothing \notin F$ y $X \in F$.
2. Si A, $B \in F$ entonces $A \cap B \in F$
3. Si $A \in F$ y $A \subset B \subset X$, entonces $B \in F$.

   Definimos ahora el concepto de *ultrafiltro* en un conjunto X, que no es sino un filtro F con la propiedad adicional:

4. Si $A \subset X$, entonces $A \in F$ o bien $X \setminus A \in F$.

El teorema al que nos referíamos es un teorema de existencia de ultrafiltros, pero antes de probarlo probaremos algunas caracterizaciones:

Teorema 4.31 *Si U es un filtro en un conjunto X, las afirmaciones siguientes son equivalentes:*

1. *U es un ultrafiltro.*
2. *Si $A \subset X$ corta a todo elemento de U, entonces $A \in U$.*
3. *U es un filtro maximal, en el sentido de que no está estrictamente contenido en ningún otro filtro.*

Demostración: 1) ⇒ 2) Si $A \notin U$, entonces $X \setminus A \in U$, luego A no corta a todos los elementos de U.

2) ⇒ 3) Si F es un filtro en X tal que $U \subset F$, todo $A \in F$ corta a todos los elementos de F, luego en particular a todos los elementos de U, luego $A \in U$, luego $U = F$.

3) ⇒ 2) Si U es maximal y $A \subset X$ corta a todo elemento de U, entonces

$$F = \{B \subset X \mid \bigvee C \in U\, A \cap C \subset B\}$$

es un filtro en X que contiene a U, luego $A \in F = U$.

2) ⇒ 1) Si $A \subset X$ cumple que $A \notin U$, por 2) tenemos que existe un $B \in U$ tal que $A \cap B = \varnothing$, luego $B \subset X \setminus A$, luego $X \setminus A \in U$. ∎

Teorema 4.32 (Teorema de los ultrafiltros (AP, AE)) *Todo filtro en un conjunto está contenido en un ultrafiltro.*

DEMOSTRACIÓN: Basta aplicar el lema de Zorn a la familia de todos los filtros de un conjunto X que contienen un filtro dado. ∎

Por ejemplo, es inmediato que si $a \in X$, entonces $(a) = \{A \subset X \mid a \in A\}$ es un ultrafiltro en X. Los ultrafiltros de esta forma se llaman *ultrafiltros fijos.* Los ultrafiltros que no son fijos se llaman *libres.*

En general, si un ultrafiltro U en un conjunto X contiene un conjunto finito $A = \{a_1, \ldots, a_n\}$, entonces contiene un a_i (pues en caso contrario cada complementario $X \setminus \{a_i\} \in U$ y, formando la intersección, $X \setminus F \in U$) y por consiguiente $U = (a_i)$ es fijo. En otras palabras, un ultrafiltro es libre si y sólo si no contiene conjuntos finitos.

Por otra parte, si X es un conjunto infinito, $F = \{A \subset X \mid X \setminus A \text{ es finito}\}$ es claramente un filtro en X, y tenemos que un ultrafiltro en X es libre si y sólo si contiene a F, luego la existencia de ultrafiltros libres en un conjunto infinito X equivale a la existencia de ultrafiltros que contengan a F. El teorema del ultrafiltro implica que todo conjunto tiene ultrafiltros libres, pero sucede que esto no se puede probar sin ayuda del axioma de elección ni siquiera en los casos más simples, como $X = \omega$.

Para terminar demostramos una forma equivalente del axioma de elección que tiene la peculiaridad de ser uno de los raros resultados que requiere esencialmente de todos los axiomas de NBG, incluyendo el axioma de regularidad.

Teorema 4.33 (NBG-AE) *El axioma de elección es equivalente a que, para todo ordinal α, el conjunto $\mathcal{P}\alpha$ puede ser bien ordenado.*

DEMOSTRACIÓN: Basta probar que, para todo ordinal α, el conjunto V_α puede ser bien ordenado, pues todo conjunto está contenido en un V_α, luego también puede ser bien ordenado.

Observemos que si V_α puede ser bien ordenado, entonces $V_{\alpha+1}$ también. En efecto, si V_α puede ser bien ordenado, existe una semejanza $f : V_\alpha \longrightarrow \beta$ en un ordinal, la cual induce una biyección $F : V_{\alpha+1} \longrightarrow \mathcal{P}\beta$. Por hipótesis $\mathcal{P}\beta$ puede ser bien ordenado, luego $V_{\alpha+1}$ también.

Supongamos que existe un λ tal que V_λ no puede ser bien ordenado, en cuyo caso podemos tomar el mínimo posible. Obviamente $\lambda \neq 0$ y, por lo que acabamos de razonar, no puede ser un ordinal sucesor, luego λ es un ordinal límite.

Notemos que, en estas condiciones, para cada $\alpha < \lambda$, tenemos que V_α puede ser bien ordenado, pero no podemos decir "sea $\leq_\alpha$ un buen orden en V_α", porque así estaríamos usando el axioma de elección que queremos demostrar.

No obstante, el hecho de que V_α pueda ser bien ordenado implica que es biyectable con un ordinal, y podemos definir κ_α como el mínimo ordinal tal que existe una biyección $V_\alpha \longrightarrow \kappa_\alpha$. A su vez podemos formar el ordinal $\kappa = \bigcup_{\alpha<\lambda} \kappa_\alpha$.

Por hipótesis $\mathcal{P}\kappa$ admite un buen orden, con el cual será semejante a otro ordinal ξ. A su vez, $\mathcal{P}\xi$ puede ser bien ordenado, y fijamos un buen orden concreto en $\mathcal{P}\xi$, digamos $\leq^*$.

Ahora vamos a construir recurrentemente una sucesión $\{\leq_\alpha\}_{\alpha<\lambda}$ de modo que cada $\leq_\alpha$ sea un buen orden en V_α y de modo que si $\alpha < \beta < \lambda$ entonces el orden $\leq_\beta$ de V_β restringido a V_α sea $\leq_\alpha$ y V_α sea un segmento inicial de V_β.

Necesariamente, definimos $\leq_0 = \varnothing$, y así $\leq_0$ es un buen orden de $V_0 = \varnothing$. Supuestos definidos $\{\leq_\alpha\}_{\alpha<\delta}$ en las condiciones indicadas, donde $\delta \leq \lambda$ es un ordinal límite, podemos definir $\leq_\delta = \bigcup_{\alpha<\delta} \leq_\alpha$, y ciertamente es un buen orden en V_δ.

El único punto delicado es suponer definido el buen orden $\leq_\alpha$ en V_α y definir un buen orden $\leq_{\alpha+1}$ en $V_{\alpha+1}$. De la hipótesis se deduce trivialmente que existe uno, pero el problema es que tenemos que dar un criterio que no dependa del axioma de elección para seleccionar uno en la construcción de la sucesión transfinita de buenos órdenes.

Como $\leq_\alpha$ es un buen orden en V_α, por 3.24 tenemos que $(V_\alpha, \leq_\alpha)$ es semejante a un único ordinal β_α, y por 1.30 existe una única semejanza $f_\alpha : (V_\alpha, \leq_\alpha) \longrightarrow \beta_\alpha$.

Ahora observamos que tiene que ser $\beta_\alpha < \xi$, pues si fuera $\xi \leq \beta_\alpha$, podríamos definir aplicaciones inyectivas

$$\beta_\alpha \longrightarrow \kappa_\alpha \longrightarrow \kappa \longrightarrow \mathcal{P}\kappa \longrightarrow \xi \longrightarrow \beta_\alpha,$$

luego el teorema de Cantor-Bernstein nos daría una biyección $\kappa \longrightarrow \mathcal{P}\kappa$, en contradicción con el teorema de Cantor 1.25.

Por lo tanto, la semejanza f_α induce una biyección $F_\alpha : V_{\alpha+1} \longrightarrow \mathcal{P}\beta_\alpha \subset \mathcal{P}\xi$, y el buen orden $\leq^*$ que hemos fijado en $\mathcal{P}\xi$ determina un buen orden explícito en $V_{\alpha+1}$, digamos $\leq_*$. Para hacerelo compatible con $\leq_\alpha$ definimos

$$x \leq_{\alpha+1} y \leftrightarrow (x, y \in V_\alpha \wedge x \leq_\alpha y) \vee (x \in V_\alpha \wedge y \in V_{\alpha+1} \setminus V_\alpha)$$

$$\vee\, (x, y \in V_{\alpha+1} \setminus V_\alpha \wedge x \leq_* y).$$

Es claro que esto define un buen orden en $V_{\alpha+1}$ sin la intervención del axioma de elección. Concluimos que $\leq_\lambda$ es un buen orden en V_λ, en contradicción con la hipótesis. ∎

Ahora disponemos ya de todos los axiomas de NBG, lo cual significa en la práctica que todo teorema que podamos encontrar en cualquier libro de álgebra, análisis, topología, etc. puede probarse a partir de los axiomas que hemos presentado. Ocasionalmente se demuestran teoremas partiendo de axiomas más fuertes, pero en tales casos siempre se indica explícitamente cuáles son dichos axiomas adicionales.

Capítulo V

Cardinales

Uno de los resultados más impactantes de la teoría de conjuntos de Cantor es que permite extender la noción de cardinal o "número de elementos" a conjuntos arbitrarios, no necesariamente finitos, de modo que, al igual que hay conjuntos finitos con más o con menos elementos, lo mismo sucede con los conjuntos infinitos, que los hay más grandes y más pequeños. Dedicamos este capítulo a desarrollar esas ideas. En general trabajaremos en NBG − AE e indicaremos explícitamente los resultados que dependen del axioma de elección. El punto de partida es la noción de "equipotencia" que hemos introducido y estudiado en la sección 1.5. Allí trabajábamos en NBG*, pero esta teoría resulta ser insuficiente para dar una definición satisfactoria de lo que es el cardinal de un conjunto, es decir, para asignar a cada conjunto otro conjunto llamado su "cardinal" de modo que dos conjuntos sean equipotentes si y sólo si tienen el mismo cardinal. En la sección 2.2 hicimos esto para los conjuntos finitos y ahora estamos finalmente en condiciones de abordar el caso general.

5.1 Números cardinales

En la sección 1.5 definimos la relación de equipotencia $\overline{\overline{X}} = \overline{\overline{Y}}$, pero insistimos en que esta notación no expresa realmente una igualdad, ya que no tenemos definido ningún objeto al que llamar $\overline{\overline{X}}$. Hay dos formas de asociar a cada conjunto X un cardinal $\overline{\overline{X}}$, una se apoya en los axiomas de partes y regularidad, mientras que la otra se apoya en el axioma de elección. En realidad hay una (tercera) forma muy sencilla de definir el cardinal de un conjunto sin necesidad de recurrir a ninguno de los axiomas que acabamos de mencionar. Basta tener en cuenta que la relación de equipotencia determina una relación de equivalencia en V, la dada por

$$X\,R\,Y \leftrightarrow \overline{\overline{X}} = \overline{\overline{Y}},$$

luego podríamos definir el cardinal de un conjunto X como su clase de equivalencia: $\overline{\overline{X}} \equiv [X]_R = \{Y \mid \overline{\overline{X}} = \overline{\overline{Y}}\}$.

Así se cumple ciertamente que $\overline{\overline{X}} = \overline{\overline{Y}}$ (entendido como igualdad de clases de equivalencia) si y sólo si $\overline{\overline{X}} = \overline{\overline{Y}}$ (entendido como que X e Y son equipotentes). Sin embargo, no es una buena opción pues, salvo para $X = \varnothing$, un cardinal así definido es siempre una clase propia. En efecto, la aplicación $V \longrightarrow \overline{\overline{X}}$ dada por $Y \mapsto X \times \{Y\}$ es claramente inyectiva, luego su imagen es una clase propia contenida en $\overline{\overline{X}}$, luego éste no puede ser un conjunto.

Esto no es del todo inviable, pero es técnicamente desaconsejable pues, por ejemplo, nos impide definir la clase de todos los cardinales, ya que los cardinales son clases propias y no pueden pertenecer a ninguna clase. Aunque podríamos arreglárnoslas para definir una suma de cardinales, dicha suma no podría verse como una ley de composición interna, porque eso requeriría que los cardinales fueran conjuntos, etc.

Pero este "primer intento" se puede refinar. Para ello suponemos los axiomas de partes y regularidad, lo cual nos da la descomposición de la clase universal

$$V = \bigcup_{\alpha\in\Omega} V_\alpha,$$

donde cada V_α es un conjunto, así como la aplicación rang : $V \longrightarrow \Omega$, que a cada conjunto x le asigna el menor ordinal α tal que $x \subset V_\alpha$. De este modo podemos definir el cardinal de un conjunto X, no como la clase de todos los conjuntos equipotentes a X (que no es un conjunto), sino como el conjunto de todos los conjuntos equipotentes a X del menor rango posible. Esto es un conjunto porque si α es el menor rango de un conjunto equipotente a X, entonces el cardinal así definido es un subconjunto del conjunto $V_{\alpha+1}$. Concretamente:

Definición 5.1 Un *cardinal* es un conjunto no vacío $\mathfrak{p}$ tal que[1]

1. $\bigwedge xy \in \mathfrak{p}(\overline{\overline{x}} = \overline{\overline{y}}\,)$,
2. $\bigvee\alpha\bigwedge x \in \mathfrak{p}$ rang $x = \alpha$,
3. $\bigwedge xy(x \in \mathfrak{p} \wedge \overline{\overline{x}} = \overline{\overline{y}} \wedge \text{rang } x = \text{rang } y \to y \in \mathfrak{p})$,
4. $\neg\bigvee xy(y \in \mathfrak{p} \wedge \overline{\overline{x}} = \overline{\overline{y}} \wedge \text{rang } x < \text{rang } y)$.

Llamaremos $\mathfrak{C}$ a la clase de todos los cardinales.

La primera condición dice que todos los elementos de un cardinal $\mathfrak{p}$ son equipotentes entre sí. La segunda afirma que todos tienen un mismo rango α. La tercera dice que todo conjunto equipotente a un conjunto de $\mathfrak{p}$ que tenga el rango de los elementos de $\mathfrak{p}$ está en $\mathfrak{p}$, y la última afirma que no existen conjuntos equipotentes a los de $\mathfrak{p}$ de rango menor al rango de los elementos de $\mathfrak{p}$. En suma, un cardinal es un conjunto no vacío de conjuntos equipotentes entre sí de rango mínimo.

[1] En lo sucesivo las letras góticas $\mathfrak{p}$, $\mathfrak{q}$, ... denotarán siempre cardinales, aunque no se indique explícitamente.

Si X es un conjunto cualquiera, definimos su *cardinal* como

$$\overline{\overline{X}} \equiv \{Y \mid \overline{\overline{X}} = \overline{\overline{Y}} \wedge \neg\bigvee Z(\mathrm{cto}\, Z \wedge \mathrm{rang}\ Z < \mathrm{rang}\ Y \wedge \overline{\overline{X}} = \overline{\overline{Z}}\ )\}.$$

Es claro que $\overline{\overline{X}}$ es realmente un cardinal. En efecto, puesto que existe al menos un conjunto equipotente a X (el propio X), la clase

$$\{\alpha \in \Omega \mid \bigvee Y(\mathrm{cto}\, Y \wedge \overline{\overline{Y}} = \overline{\overline{X}} \wedge \mathrm{rang}\, Y = \alpha)\}$$

no es vacía, luego tiene un mínimo elemento α, lo cual significa que existe un conjunto Y_0 equipotente a X de rango α y que si $\overline{\overline{Z}} = \overline{\overline{X}}$ entonces rang Z $\geq \alpha$. Por lo tanto, $Y_0 \in \overline{\overline{X}}$, luego $\overline{\overline{X}} \neq \varnothing$, y no ofrece ninguna dificultad comprobar que $\overline{\overline{X}}$ no es sino el conjunto de todos los conjuntos equipotentes a X de rango α, de donde se sigue a su vez que cumple las propiedades 1) – 4) de la definición de cardinal.

Aunque estas definiciones sean técnicamente complejas, esto carece de importancia, pues podemos olvidarnos de ellas en cuanto nos convencemos de lo siguiente:

Teorema 5.2 *Se cumple:*

1. *Para cada conjunto x tenemos definido $\overline{\overline{x}} \in \mathfrak{C}$ y para todo $\mathfrak{p} \in \mathfrak{C}$ existe un conjunto x tal que $\overline{\overline{x}} = \mathfrak{p}$.*
2. *Dados dos conjuntos x e y, se cumple $\overline{\overline{x}} = \overline{\overline{y}}$ (entendido como igualdad de cardinales) si y sólo si x e y son equipotentes.*

Demostración: Si $\mathfrak{p} \in \mathfrak{C}$, por definición no es vacío, luego existe un $x \in \mathfrak{p}$, y es fácil ver que $\mathfrak{p} = \overline{\overline{x}}$.

Si dos conjuntos x e y son equipotentes, entonces los conjuntos de rango mínimo equipotentes a uno de ellos coinciden con los conjuntos de rango mínimo equipotentes al otro, luego sus cardinales son iguales. Recíprocamente, si ambos tienen el mismo cardinal $\overline{\overline{x}} = \overline{\overline{y}} = \mathfrak{p}$ y $z \in \mathfrak{p}$, entonces z es equipotente a x y a y, luego ambos son equipotentes entre sí. ∎

Así pues, hemos conseguido nuestro propósito: las fórmulas $\overline{\overline{x}} = \overline{\overline{y}}$ tienen el mismo significado que les hemos dado en la definición 1.21, pero ahora son auténticas igualdades de cardinales.

Definición 5.3 Definimos la relación en $\mathfrak{C}$ dada por

$$\mathfrak{p} \leq \mathfrak{q} \equiv \bigvee xy(\mathrm{cto}\, x \wedge \mathrm{cto}\, y \wedge \mathfrak{p} = \overline{\overline{x}} \wedge \mathfrak{q} = \overline{\overline{y}} \wedge x \text{ es minuspontente a } y).$$

Esta definición no depende de la elección de x e y en virtud del último apartado del teorema 1.22, de modo que, para todo par de conjuntos x e y, se cumple que

$$\overline{\overline{x}} \leq \overline{\overline{y}} \quad \text{si y sólo si} \quad x \text{ es minuspotente a } y,$$

es decir, que la fórmula $\overline{\overline{x}} \leq \overline{\overline{y}}$ (entendida en términos de la relación que acabamos de definir) tiene el mismo significado que tenía en 1.21, pero ahora es una auténtica desigualdad entre cardinales.

El teorema 1.22 implica inmediatamente que la relación que acabamos de definir es ciertamente una relación de orden (no necesariamente de orden total) sobre la clase $\mathfrak{C}$.

Ahora veamos otra forma alternativa de definir el cardinal de un conjunto que no requiere ni el axioma de regularidad ni el de partes, pero (para que sirva realmente para todo conjunto) requiere el axioma de elección. La idea es que, bajo AE, todo conjunto x puede biyectarse con un ordinal, luego podemos definir el cardinal de x como el menor ordinal equipotente a x. En lugar de suponer AE, restringiremos las definiciones a conjuntos biyectables con ordinales:

Definición 5.4 La clase de los *cardinales de von Neumann* es la clase[2]

$$K = \{\alpha \in \Omega \mid \neg\bigvee\beta < \alpha\ \overline{\beta} = \overline{\alpha}\}.$$

Usaremos las letras griegas κ, μ, ν, ... para referirnos a cardinales de von Neumann, aunque no lo indiquemos explícitamente.

De este modo, un cardinal (de von Neumann) es un ordinal no equipotente a ningún ordinal anterior. Por lo tanto, si κ y μ son cardinales de von Neumann, se tiene que $\bar{\kappa} = \bar{\mu} \leftrightarrow \kappa = \mu$, ya que si $\bar{\kappa} = \bar{\mu}$ pero $\kappa < \mu$ o $\mu < \kappa$, entonces μ (en el primer caso) o κ (en el segundo) no sería un cardinal, pues sería equipotente a un ordinal anterior.

Diremos que un conjunto es *bien ordenable* si admite una buena ordenación o, equivalentemente, si es equipotente a un ordinal.

Para cada conjunto bien ordenable x, el menor ordinal equipotente a x no puede ser equipotente a ningún ordinal anterior (pues dicho ordinal anterior sería también equipotente a x), luego es un cardinal de von Neumann. En definitiva, si definimos

$$|x| = \kappa \mid (\kappa \in K \wedge \overline{\kappa} = \overline{\overline{x}}),$$

tenemos que para todo conjunto bien ordenable x se cumple que $|x| \in K$ y es un ordinal equipotente a x.

Más aún, si x e y son conjuntos bien ordenables entonces $|x| = |y|$ si y sólo si x es equipotente a y.

En efecto, tenemos que x es equipotente a $|x|$ e y es equipotente a $|y|$, luego x es equipotente a y si y sólo si $|x|$ es equipotente a $|y|$ si y sólo si $|x| = |y|$.

[2]Por seguir la tradición cantoriana, escribiremos $\overline{\alpha}$ en lugar de $\overline{\overline{\alpha}}$ cuando α sea un ordinal. Recordemos que para Cantor una barra significaba "ordinal" y una barra sobre el ordinal (o sea, dos barras sobre un conjunto) significaba "cardinal".

Así pues, si aceptamos AE, todo conjunto tiene asociado un cardinal de von Neumann, luego podemos olvidarnos de la definición de $\mathfrak{C}$ y trabajar únicamente con K.

Por otra parte, si no suponemos AE, la relación entre ambas definiciones es que tenemos una inmersión $K \longrightarrow \mathfrak{C}$ dada por $\kappa \mapsto \overline{\kappa}$, es decir, a cada cardinal de von Neumann le asociamos su cardinal en el sentido de 5.1. La aplicación es inyectiva, pues si $\overline{\kappa} = \overline{\mu}$, entonces κ y μ son cardinales equipotentes, luego son iguales.

Si esta inmersión es suprayectiva, entonces para todo conjunto x tenemos que $\overline{\overline{x}} = \overline{\kappa}$, para cierto $\kappa \in K$, luego x es equipotente a κ y, por consiguiente, bien ordenable. En suma, la suprayectividad de la inmersión de K en $\mathfrak{C}$ equivale al axioma de elección.

Por otra parte, si consideramos en K el orden de Ω, tenemos que la inmersión es una semejanza en la imagen, es decir, $\kappa \leq \mu$ si y sólo si $\overline{\kappa} \leq \overline{\mu}$.

En efecto, si $\kappa \leq \mu$, entonces $\kappa \subset \mu$, luego es obvio que $\overline{\kappa} \leq \overline{\mu}$. Recíprocamente, si $\overline{\kappa} \leq \overline{\mu}$, no puede ser $\mu < \kappa$, pues entonces $\overline{\mu} \leq \overline{\kappa}$, luego $\overline{\kappa} = \overline{\mu}$, luego $\kappa = \mu$, contradicción. Así pues, $\kappa \leq \mu$.

En particular, si x e y son conjuntos bien ordenables, tenemos que $|x| \leq |y|$ si y sólo si x es minuspotente a y. Un poco más en general:

Teorema 5.5 *Sean x, y dos conjuntos tales que y es bien ordenable y $x \neq \varnothing$. Entonces, las afirmaciones siguientes son equivalentes:*

1. *x es bien ordenable y $|x| \leq |y|$.*
2. *Existe $f : x \longrightarrow y$ inyectiva.*
3. *Existe $g : y \longrightarrow x$ suprayectiva.*

Demostración: Teniendo en cuenta que 2) implica obviamente que x es bien ordenable, la observación previa al teorema nos da que 1) $\Leftrightarrow$ 2), mientras que el teorema 4.26 nos da que 2) $\Leftrightarrow$ 3) teniendo en cuenta la observación que le sigue, que justifica que en este caso no es necesario AE. ∎

Puede probarse que sin el axioma de elección es imposible demostrar que la relación de orden en $\mathfrak{C}$ sea un orden total, mientras que con el axioma de elección $\mathfrak{C}$ es semejante a K y, por consiguiente, $\mathfrak{C}$ resulta estar no sólo totalmente ordenado, sino incluso bien ordenado.

En la práctica identificaremos K con su imagen en $\mathfrak{C}$, en el sentido de que si $\mathfrak{p} \in \mathfrak{C}$ y afirmamos que $\mathfrak{p} \in K$ deberemos entender que $\mathfrak{p} = \overline{\kappa}$ para un cierto $\kappa \in K$. Por ejemplo, es obvio que si $\overline{\overline{X}} \leq \overline{\overline{Y}}$ e Y es bien ordenable, entonces X también lo es. Alternativamente, podemos expresar esto diciendo que si $\mathfrak{p} \leq \kappa$, entonces $\mathfrak{p} \in K$.

Veamos algunos resultados básicos sobre los cardinales de von Neumann:

Teorema 5.6 $\omega \subset K$.

DEMOSTRACIÓN: Probamos por inducción que todo número natural es un cardinal. Obviamente 0 no es equipotente a ningún ordinal anterior, luego $0 \in K$. Supongamos que $n \in K$ pero que $n+1 \notin K$. Entonces existe un ordinal anterior $m < n+1$ y una biyección $f : n+1 \longrightarrow m$. Es claro que m no puede ser 0, luego $m = r+1$. Veamos que podemos suponer que $f(n) = r$. En caso contrario, sea $n' = f^{-1}(r)$. Definimos

$$f' = (f \setminus \{(n, f(n)), (n', r)\}) \cup \{(n, r), (n', f(n))\},$$

y es claro que f' es una biyección como f pero tal que $f(n) = r$.

Ahora bien, $r < n$ y $f'|_n : n \longrightarrow r$ biyectiva, lo cual contradice que n sea un cardinal. ∎

En realidad el teorema anterior es simplemente una variante de 2.8. Ahora es inmediato que un conjunto X es finito (según la definición 2.9) si y sólo si es bien ordenable y $|X| \in \omega$, y en tal caso $|X|$ es el mismo número natural definido en 2.9.

Teorema 5.7 $\omega \in K$.

DEMOSTRACIÓN: En caso contrario existiría un $n \in \omega$ tal que $\overline{n} = \overline{\omega}$, pero como $n \subset n+1 \subset \omega$ es claro que $\overline{n} \leq \overline{n+1} \leq \overline{\omega} = \overline{n}$, luego sería $\overline{n} = \overline{n+1}$ y $n+1$ no sería un cardinal, en contra del teorema anterior. ∎

El siguiente cardinal ya no es tan fácil de encontrar. Ciertamente no puede ser $\omega + 1$, como muestra el teorema siguiente:

Teorema 5.8 $\bigwedge\kappa(\omega \leq \kappa \to \kappa$ *es un ordinal límite*$)$.

DEMOSTRACIÓN: Vamos a ver que no puede existir un ordinal α tal que $\kappa = \alpha + 1$. En efecto, en tal caso podríamos definir una aplicación $f : \kappa \longrightarrow \alpha$ biyectiva mediante

$$f(\beta) = \begin{cases} \beta & \text{si } \beta \in \alpha \setminus \omega, \\ \beta + 1 & \text{si } \beta \in \omega, \\ 0 & \text{si } \beta = \alpha. \end{cases}$$

Por consiguiente κ no sería un cardinal. ∎

La forma más natural de encontrar un cardinal mayor que ω es tomar un ordinal equipotente a $\mathcal{P}\omega$ y aplicar el teorema de Cantor. No obstante, no podemos encontrar dicho ordinal sin el axioma de elección, pues sin él no puede probarse que $\mathcal{P}\omega$ pueda ser bien ordenado. Pero es posible probar la existencia de cardinales arbitrariamente grandes sin necesidad del axioma de elección. En cualquier caso, el axioma que necesitaremos inevitablemente es el axioma de partes, pues sin él no puede demostrarse la existencia de conjuntos no numerables (es decir, de conjuntos de cardinal mayor que ω). Así, el teorema siguiente es el segundo en el que usamos AP de forma esencial, después del teorema de Cantor (que hasta ahora no hemos usado para nada):

Teorema 5.9 $\bigwedge\alpha\bigvee\kappa\ \alpha < \kappa$.

DEMOSTRACIÓN: Sea

$$A = \{R \in \mathcal{P}(\alpha \times \alpha) \mid R \text{ es un buen orden en } \alpha\},$$

es decir, A es el conjunto de todos los buenos órdenes posibles en α. Se cumple que es un conjunto por el axioma de partes.

Sea $f : A \longrightarrow \Omega$ la aplicación dada por $f(R) = \mathrm{ord}(\alpha, R)$. Por el axioma del reemplazo $f[A]$ es un subconjunto de Ω, luego está acotado. Sea $\beta \in \Omega$ tal que $\bigwedge\delta \in f[A]\, \delta < \beta$.

Si R es la relación de orden usual en α, tenemos que $R \in A$ y $f(R) = \alpha$, luego $\alpha < \beta$. Si fuera $\overline{\alpha} = \overline{\beta}$, entonces tendríamos una biyección $g : \alpha \longrightarrow \beta$, la cual nos permitiría definir la relación en α dada por $\delta\, R\, \epsilon$ si y sólo si $g(\delta) < g(\epsilon)$. Claramente R es un buen orden en α y $g : (\alpha, R) \longrightarrow \beta$ es una semejanza. Por consiguiente $f(R) = \beta \in f[A]$, en contradicción con la elección de β. Así pues, como obviamente $\overline{\alpha} \leq \overline{\beta}$, ha de ser $\overline{\alpha} < \overline{\beta}$.

Llamemos κ al mínimo ordinal tal que $\overline{\alpha} < \overline{\kappa}$. Claramente $\kappa \in K$, pues si existiera un $\gamma < \kappa$ tal que $\overline{\gamma} = \overline{\kappa}$, también tendríamos que $\overline{\alpha} < \overline{\gamma}$, en contra de la definición de κ.

Además $\alpha < \kappa$, pues de lo contrario sería $\overline{\kappa} \leq \overline{\alpha}$, y esto contradice a $\overline{\alpha} < \overline{\kappa}$, por el teorema de Cantor-Bernstein. ∎

Definición 5.10 Dado un ordinal α llamaremos *cardinal siguiente* de α al mínimo cardinal mayor que α y lo representaremos por α^+.

Según hemos visto, $\bigwedge n \in \omega\ n^+ = n+1$, mientras que si α es infinito esto ya no es cierto, pues entonces α^+ es un ordinal límite.

Ahora ya tenemos demostrada la existencia de infinitos cardinales infinitos. Más aún, hemos probado que K no está acotado en Ω, lo que implica que la clase de todos los cardinales no es un conjunto. Otro hecho importante es el siguiente:

Teorema 5.11 *El supremo de un conjunto de cardinales es un cardinal.*

DEMOSTRACIÓN: Sea $A \subset K$ un conjunto y sea $\kappa = \bigcup_{\mu \in A} \mu$. Ciertamente $\kappa \in \Omega$ y hemos de probar que es un cardinal. Si existiera un $\alpha < \kappa$ tal que $\overline{\alpha} = \overline{\kappa}$, entonces existe un $\mu \in A$ tal que $\alpha < \mu \leq \kappa$. Entonces

$$\overline{\alpha} \leq \overline{\mu} \leq \overline{\kappa} = \overline{\alpha}.$$

Por consiguiente $\overline{\alpha} = \overline{\mu}$, en contra de que μ sea un cardinal. ∎

Definición 5.12 Llamaremos $\aleph : \Omega \longrightarrow \Omega$ (función álef) a la única aplicación que cumple

$$\aleph_0 = \omega \quad \wedge \quad \bigwedge\alpha\ \aleph_{\alpha+1} = \aleph_\alpha^+ \quad \wedge \quad \bigwedge\lambda\ \aleph_\lambda = \bigcup_{\delta<\lambda} \aleph_\delta.$$

Es claro que se trata de una función normal. Vamos a probar que recorre todos los cardinales infinitos.

Teorema 5.13 $\aleph : \Omega \longrightarrow K \setminus \omega$ *biyectiva.*

Demostración: Como $\aleph$ es normal sabemos que es inyectiva, luego basta probar que es suprayectiva. Una simple inducción demuestra que $\bigwedge\alpha\, \aleph_\alpha \in K$ (el caso límite es el teorema 5.11). Esto significa que $\aleph[\Omega] \subset K$. Como $\aleph$ es creciente y $\aleph_0 = \omega$, ciertamente $\aleph[\Omega] \subset K \setminus \omega$. Sólo nos falta probar que si $\kappa \in K \setminus \omega$ existe un α tal que $\kappa = \aleph_\alpha$.

Por la normalidad tenemos que $\kappa \leq \aleph_\kappa < \aleph_{\kappa+1}$. Sea β el mínimo ordinal tal que $\kappa < \aleph_\beta$. No puede ser $\beta = 0$, pues entonces $\kappa \in \aleph_0 = \omega$. Por la definición de $\aleph$ tampoco puede ocurrir que β sea un ordinal límite. Consecuentemente, $\beta = \alpha + 1$ y tenemos que $\aleph_\alpha \leq \kappa < \aleph_{\alpha+1} = \aleph_\alpha^+$. Necesariamente entonces $\kappa = \aleph_\alpha$. ∎

Según esto, tenemos que $\aleph_0 = \omega$ es el cardinal de los conjuntos numerables, aunque es costumbre no usar las dos notaciones indiscriminadamente, sino que se usa $\aleph_0$ cuando lo consideramos como un cardinal y ω cuando lo consideramos como un ordinal. Similarmente, es costumbre representar $\aleph_\alpha$ como ω_α cuando lo consideramos como un ordinal.

Tenemos entonces que la sucesión de los cardinales infinitos (de von Neumann) empieza así:

$$\aleph_0,\ \aleph_1,\ \aleph_2,\ \ldots\ \aleph_\omega,\ \aleph_{\omega+1},\ \aleph_{\omega+2},\ \ldots\ \aleph_{\omega_1},\ \aleph_{\omega_1+1},\ \ldots\ \aleph_{\omega_1+\omega},\ \ldots$$

Es claro que el axioma de elección equivale a que todo cardinal infinito es un álef.

5.2 La aritmética cardinal

La aritmética cardinal permite reducir el cálculo del cardinal de un conjunto al de otros conocidos. Empezamos estudiando la suma y el producto de cardinales, que, a diferencia de lo que ocurre con la exponenciación, son muy fáciles de calcular.

Suma y producto La definición se apoya en el siguiente hecho elemental:

Si X, Y, X', Y' son conjuntos cualesquiera y $\overline{\overline{X}} = \overline{\overline{X'}}$, $\overline{\overline{Y}} = \overline{\overline{Y'}}$, entonces

$$\overline{\overline{X \times \{0\} \cup Y \times \{1\}}} = \overline{\overline{X' \times \{0\} \cup Y' \times \{1\}}}, \qquad \overline{\overline{X \times Y}} = \overline{\overline{X' \times Y'}}.$$

La comprobación no ofrece ninguna dificultad.

Definición 5.14 Definimos las operaciones + y · en $\mathfrak{C}$ dadas por

$$\mathfrak{p}+\mathfrak{q}=\overline{\overline{X\times\{0\}\cup Y\times\{1\}}},\qquad \mathfrak{p}\mathfrak{q}=\overline{\overline{X\times Y}},$$

donde $\mathfrak{p}=\overline{\overline{X}}$, $\mathfrak{q}=\overline{\overline{Y}}$.

La observación anterior justifica que esta definición no depende de la elección de los conjuntos X e Y. Más aún, es fácil probar:

Teorema 5.15 *1) Si X e Y son conjuntos disjuntos, $\overline{\overline{X\cup Y}}=\overline{\overline{X}}+\overline{\overline{Y}}$.*

2) Si X e Y son conjuntos cualesquiera, $\overline{\overline{X\times Y}}=\overline{\overline{X}}\cdot\overline{\overline{Y}}$.

El teorema siguiente se demuestra sin dificultad sin más que manipular de forma obvia aplicaciones entre conjuntos:

Teorema 5.16 *Para todos los cardinales $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$, $\mathfrak{s}$ se cumple:*

1. $(\mathfrak{p}+\mathfrak{q})+\mathfrak{r}=\mathfrak{p}+(\mathfrak{q}+\mathfrak{r})$,
2. $\mathfrak{p}+\mathfrak{q}=\mathfrak{q}+\mathfrak{p}$,
3. $\mathfrak{p}+0=\mathfrak{p}$,
4. $\mathfrak{p}\le\mathfrak{q}\wedge\mathfrak{r}\le\mathfrak{s}\to\mathfrak{p}+\mathfrak{r}\le\mathfrak{q}+\mathfrak{s}$,
5. $(\mathfrak{p}\mathfrak{q})\mathfrak{r}=\mathfrak{p}(\mathfrak{q}\mathfrak{r})$,
6. $\mathfrak{p}\mathfrak{q}=\mathfrak{q}\mathfrak{p}$,
7. $\mathfrak{p}\cdot 0=0\wedge\mathfrak{p}\cdot 1=\mathfrak{p}$,
8. $\mathfrak{p}(\mathfrak{q}+\mathfrak{r})=\mathfrak{p}\mathfrak{q}+\mathfrak{p}\mathfrak{r}$,
9. $\mathfrak{p}\le\mathfrak{q}\wedge\mathfrak{r}\le\mathfrak{s}\to\mathfrak{p}+\mathfrak{r}\le\mathfrak{q}+\mathfrak{s}\wedge\mathfrak{p}\mathfrak{r}\le\mathfrak{q}\mathfrak{s}$.

Estas propiedades permiten operar fácilmente con cardinales. Veamos un ejemplo:

Teorema 5.17 *Para todo par de conjuntos X, Y se cumple*

$$\overline{\overline{X}}+\overline{\overline{Y}}=\overline{\overline{X\cup Y}}+\overline{\overline{X\cap Y}}.$$

En particular $\overline{\overline{X\cup Y}}\le\overline{\overline{X}}+\overline{\overline{Y}}$.

Demostración: Claramente X se descompone en la unión disjunta $X=(X\setminus(X\cap Y))\cup(X\cap Y)$, luego $\overline{\overline{X}}=\overline{\overline{X\setminus(X\cap Y)}}+\overline{\overline{X\cap Y}}$. Por lo tanto

$$\overline{\overline{X}}+\overline{\overline{Y}}=\overline{\overline{X\setminus(X\cap Y)}}+\overline{\overline{Y}}+\overline{\overline{X\cap Y}}=\overline{\overline{(X\setminus(X\cap Y))\cup Y}}+\overline{\overline{X\cap Y}},$$

donde hemos usado que los dos primeros sumandos del término central son disjuntos. Es claro que el último miembro coincide con $\overline{\overline{X\cup Y}}+\overline{\overline{X\cap Y}}$. La desigualdad se sigue del último apartado del teorema anterior. ∎

Veamos ahora que la suma y el producto de cardinales de K está también en K. De hecho, podemos definir directamente las operaciones en K sin pasar por $\mathfrak{C}$:

Definición 5.18 Definimos las operaciones + y · en K dadas por

$$\kappa + \mu = |\kappa \times \{0\} \cup \mu \times \{1\}|, \qquad \kappa\mu = |\kappa \times \mu|.$$

Para que esta definición sea correcta (al menos sin suponer AE) debemos justificar que los conjuntos $\kappa \times \{0\} \cup \mu \times \{1\}$ y $\kappa \times \mu$ son bien ordenables. De hecho, esto es cierto para ordinales cualesquiera:

En la sección 3.5 hemos visto que si α y β son dos ordinales cualesquiera, entonces $\alpha + \beta = \mathrm{ord}(\alpha \oplus \beta)$ y $\alpha\beta = \mathrm{ord}(\alpha \times \beta)$, donde en los conjuntos $\alpha \oplus \beta = \alpha \times \{0\} \cup \beta \times \{1\}$ y $\alpha \times \beta$ se considera el orden lexicográfico, luego en particular ambos conjuntos son bien ordenables. Esto justifica que la definición anterior es correcta, pero prueba además que

$$\overline{\alpha + \beta} = \overline{\overline{\alpha \times \{0\} \cup \beta \times \{1\}}} = \overline{\alpha} + \overline{\beta}, \qquad \overline{\alpha\,\beta} = \overline{\overline{\alpha \times \beta}} = \overline{\alpha}\,\overline{\beta},$$

donde la suma y el producto de los miembros izquierdos son la suma y producto de ordinales, mientras que en los miembros derechos tenemos la suma y el producto de cardinales definidas en 5.14.

En particular esto vale para κ, $\mu \in K$, lo que significa que, si tenemos dos cardinales en K, es lo mismo sumarlos o multiplicarlos como cardinales en K y luego considerar sus cardinales asociados en $\mathfrak{C}$ que sumar o multiplicar en $\mathfrak{C}$ sus cardinales asociados. En definitiva, que a la hora de sumar y multiplicar cardinales de K, da igual hacerlo en K o en $\mathfrak{C}$, pues los resultados se corresponden a través de la inclusión $K \longrightarrow \mathfrak{C}$.

Por consiguiente, si X e Y son conjuntos bien ordenables, también lo son $X \cup Y$ y $X \times Y$. En efecto, si son disjuntos, tenemos que

$$\overline{\overline{X \cup Y}} = \overline{\overline{X}} + \overline{\overline{Y}} = \overline{|X|} + \overline{|Y|} = \overline{|X| + |Y|},$$

luego el cardinal de $X \cup Y$ es un cardinal de K, lo que significa que $X \cup Y$ es bien ordenable y

$$|X \cup Y| = |X| + |Y|.$$

Si X e Y no son disjuntos, sabemos de todos modos que

$$\overline{\overline{X \cup Y}} \leq \overline{\overline{X}} + \overline{\overline{Y}} = \overline{|X| + |Y|},$$

luego $X \cup Y$ es minuspotente al cardinal $|X| + |Y|$, luego es bien ordenable igualmente. Con el producto sucede lo mismo:

$$\overline{\overline{X \times Y}} = \overline{\overline{X}}\;\overline{\overline{Y}} = \overline{|X|} + \overline{|Y|} = \overline{|X|\,|Y|},$$

luego el cardinal de $X \times Y$ es un cardinal de K, luego es bien ordenable y

$$|X \times Y| = |X|\,|Y|.$$

Ahora es inmediato que todas las propiedades del teorema 5.16 valen también para las operaciones en K. Por ejemplo, $\kappa + \mu = \mu + \kappa$ porque ambos cardinales

de K se corresponden con el cardinal $\overline{\kappa}+\overline{\mu}=\overline{\mu}+\overline{\kappa}$ de $\mathfrak{C}$, y la inmersión es inyectiva. Igualmente, el teorema 5.17 se traduce en que, si X e Y son conjuntos bien ordenables,

$$|X|+|Y|=|X\cup Y|+|X\cap Y|,$$

simplemente porque, precisamente por 5.17, ambos miembros se corresponden con el mismo cardinal de $\mathfrak{C}$. También hemos probado lo siguiente:

Teorema 5.19 *Para todos los ordinales α y β, se cumple*

$$|\alpha+\beta|=|\alpha|+|\beta|, \qquad |\alpha\beta|=|\alpha||\beta|,$$

donde la suma y el producto de los miembros izquierdos son la suma y el producto de ordinales, y los de los miembros derechos son la suma y el producto de cardinales.

(Por ejemplo, para la suma hemos visto que ambos miembros se corresponden con el cardinal $\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta}$ de $\mathfrak{C}$, e igualmente sucede con el producto.)

Es importante tener presente que ahora tenemos dos sumas y dos productos definidos sobre todos los cardinales de K: la suma y el producto de ordinales (cuyo resultado no está necesariamente en K) y la suma y el producto de cardinales. Son distintas. Por ejemplo, las operaciones ordinales no son conmutativas, pero las cardinales sí. Un ejemplo concreto: $\omega+1\neq\aleph_0+1$, pues el miembro izquierdo no es un cardinal (los cardinales infinitos son ordinales límite) y el miembro derecho sí que lo es. El teorema anterior muestra la relación entre ellas, pero lo que necesitamos ahora son resultados que nos permitan calcular sumas y productos de cardinales. El caso finito es trivial:

Teorema 5.20 *Sobre los números naturales, la suma cardinal coincide con la suma ordinal.*

Demostración: Es consecuencia inmediata del teorema anterior, teniendo en cuenta que todo $n\in\omega$ cumple $|n|=n$. ∎

La suma y el producto en K quedan completamente determinados por el teorema siguiente:

Teorema 5.21 *Para todo álef κ se cumple $\kappa\kappa=\kappa$.*

Demostración: Lo probamos por inducción, es decir, suponemos que para todo álef $\mu<\kappa$ se cumple $\mu\mu=\mu$. Entonces, $\bigwedge\mu<\kappa\ \mu\mu<\kappa$, pues μ ha de ser un álef o bien un número natural.

Consideramos en $\kappa\times\kappa$ la restricción del orden canónico de $\Omega\times\Omega$ definido en 3.28.

Sea $\alpha=\operatorname{ord}(\kappa\times\kappa)$. Entonces $\alpha\geq|\alpha|=\kappa\kappa\geq\kappa$. Supongamos que fuera $\kappa<\alpha$ y sea $f:\alpha\longrightarrow\kappa\times\kappa$ la semejanza. Sea $f(\kappa)=(\beta,\gamma)$. Como κ es un ordinal límite, podemos tomar $\delta<\kappa$ tal que $\beta,\gamma<\delta$.

Como κ está formado por los ordinales menores que κ, tenemos que $f[\kappa]$ está formado por los pares menores que (β,γ). Ahora bien, por la definición del orden canónico, si $(\beta',\gamma') < (\beta,\gamma)$, entonces β', $\gamma' < \delta$, es decir, $f[\kappa] \subset \delta \times \delta$.

Por consiguiente, $\kappa = |f[\kappa]| \leq |\delta \times \delta| = |\delta|\,|\delta| < \kappa$, contradicción. Por consiguiente $\alpha = \kappa$, lo cual prueba que $\kappa \times \kappa$ es equipotente a κ. ∎

Como consecuencia:

Teorema 5.22 *Se cumple:*

$$\bigwedge\kappa\mu(\kappa \leq \mu \wedge \aleph_0 \leq \mu \to \kappa + \mu = \mu),$$

$$\bigwedge\kappa\mu(\kappa \leq \mu \wedge \aleph_0 \leq \mu \wedge \kappa \neq 0 \to \kappa\mu = \mu).$$

DEMOSTRACIÓN: $\mu \leq \kappa + \mu \leq \mu + \mu = 2\mu \leq \mu\mu = \mu$, luego $\kappa + \mu = \mu$.
$\mu \leq \kappa\mu \leq \mu\mu = \mu$, luego $\kappa\mu = \mu$. ∎

Así pues, la aritmética de K es muy sencilla:

$$\aleph_0 + \aleph_1 = \aleph_1, \quad \aleph_{\omega_{15}} + \aleph_3 = \aleph_{\omega_{15}}, \quad 3\aleph_7 = \aleph_7, \quad \aleph_{23}\,\aleph_7 = \aleph_{23}, \quad \text{etc.}$$

Ejercicio: Probar que si Y es un conjunto infinito bien ordenable y $|X| < |Y|$, entonces $|Y \setminus X| = |Y|$.

Nota En la prueba del teorema 5.21 hemos visto que si κ es un álef y consideramos el orden canónico en $\kappa \times \kappa$, entonces $\mathrm{ord}(\kappa \times \kappa) = \kappa$. De la definición del orden canónico se sigue fácilmente que el producto es la sección inicial $\kappa \times \kappa = (\Omega \times \Omega)^<_{(\kappa,0)}$. ∎

Respecto a la aritmética de los cardinales no bien ordenables, poco podemos decir. Un concepto útil en su estudio es el siguiente:

Definición 5.23 Sea X un conjunto infinito. Sea

$$B = \{R \mid R \text{ es un buen orden en un subconjunto de } X\}.$$

Se cumple que B es un conjunto porque $B \subset \mathcal{P}(X \times X)$. Llamaremos *número de Hartogs* de X a $\aleph(X) = \{\mathrm{ord}(\mathcal{D}R, R) \mid R \in B\}$.

Como $\aleph(X)$ es imagen de B, por el axioma del reemplazo es un conjunto de ordinales. Es claro que $\alpha \in \aleph(X)$ si y sólo si existe $f : \alpha \longrightarrow X$ inyectiva, de donde se sigue claramente que $\aleph(X)$ es un conjunto transitivo y, por consiguiente, un ordinal.

Más aún, si $|\alpha| = |\beta|$ y $\beta < \aleph(X)$, entonces $\alpha < \aleph(X)$, de donde se sigue que $\aleph(X)$ es, de hecho, un cardinal, y una simple inducción prueba que si X es infinito existe $f : n \longrightarrow X$ inyectiva para todo n, luego $\aleph(X)$ es un cardinal infinito, es decir, un álef.

También es inmediato que si $\overline{\overline{X}} = \overline{\overline{Y}}$ entonces $\aleph(X) = \aleph(Y)$, luego, para cada cardinal $\mathfrak{p}$, podemos definir $\aleph(\mathfrak{p}) = \aleph(X)$, donde X es cualquier conjunto tal que $\overline{\overline{X}} = \mathfrak{p}$.

Es claro que $\aleph(\mathfrak{p})$ es el menor álef κ que no cumple $\kappa \leq \mathfrak{p}$ (notemos que si fuera $\aleph(\mathfrak{p}) \leq \mathfrak{p}$ entonces tendríamos $\aleph(\mathfrak{p}) < \aleph(\mathfrak{p})$). En particular, si κ es un álef, se cumple $\aleph(\kappa) = \kappa^+$.

Teorema 5.24 *Sean $\mathfrak{p}$ y κ cardinales infinitos tales que $\mathfrak{p} + \kappa = \mathfrak{p}\kappa$. Entonces $\mathfrak{p} \leq \kappa$ o $\kappa \leq \mathfrak{p}$. En particular, si $\mathfrak{p} + \aleph(\mathfrak{p}) = \mathfrak{p}\aleph(\mathfrak{p})$, entonces $\mathfrak{p}$ es un álef.*

DEMOSTRACIÓN: Sea X un conjunto de cardinal $\mathfrak{p}$. Por hipótesis existen conjuntos disjuntos A y B tales que $X \times \kappa = A \cup B$, $\overline{\overline{A}} = \mathfrak{p}$, $\overline{\overline{B}} = \kappa$.

Si existe un $x \in X$ tal que $\{(x, \alpha) \mid \alpha < \kappa\} \subset A$, entonces claramente $\kappa \leq \mathfrak{p}$.

En caso contrario, para cada $x \in X$ existe un mínimo $\alpha_x \in \kappa$ tal que $(x, \alpha_x) \notin A$, de donde $\{(x, \alpha_x) \mid x \in X\} \subset B$, por lo que $\mathfrak{p} \leq \kappa$.

En el caso particular en que $\kappa = \aleph(\mathfrak{p})$ no puede ocurrir $\aleph(\mathfrak{p}) \leq \mathfrak{p}$, luego ha de ser $\mathfrak{p} \leq \aleph(\mathfrak{p})$ y, por consiguiente, $\mathfrak{p}$ es un álef. ∎

Como aplicación tenemos un resultado interesante:

Teorema 5.25 *El axioma de elección equivale a que $\mathfrak{p}\mathfrak{p} = \mathfrak{p}$ para todo cardinal infinito $\mathfrak{p}$.*

DEMOSTRACIÓN: Si suponemos el axioma de elección entonces todo cardinal infinito es un álef y basta aplicar el teorema 5.21. Para el recíproco basta probar que todo cardinal infinito $\mathfrak{p}$ es un álef y, a su vez, para ello basta probar que $\mathfrak{p} + \aleph(\mathfrak{p}) = \mathfrak{p}\aleph(\mathfrak{p})$. De hecho basta ver que $\mathfrak{p}\aleph(\mathfrak{p}) \leq \mathfrak{p} + \aleph(\mathfrak{p})$, ya que la otra desigualdad se da siempre trivialmente. Ahora bien:

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

∎

Exponenciación Finalmente introducimos la exponenciación de cardinales, una operación tan natural como la suma y el producto pero cuyo comportamiento es muy diferente. Recordemos que $A^B = \{f \mid f : B \longrightarrow A\}$. La definición de la exponenciación de cardinales se apoya en el siguiente hecho obvio:

> *Si A, A', B y B' son conjuntos tales que $\overline{\overline{A}} = \overline{\overline{A'}}$ y $\overline{\overline{B}} = \overline{\overline{B'}}$ entonces se cumple $\overline{\overline{A^B}} = \overline{\overline{A'^{B'}}}$.*

Definición 5.26 Dados dos cardinales $\mathfrak{p}$ y $\mathfrak{q}$, definimos $\mathfrak{p}^\mathfrak{q} = \overline{\overline{A^B}}$, donde $\overline{\overline{A}} = \mathfrak{p}$ y $\overline{\overline{B}} = \mathfrak{q}$.

La observación precedente demuestra que $\mathfrak{p}^\mathfrak{q}$ no depende de la elección de los conjuntos A y B. Las propiedades siguientes se demuestran sin dificultad:

Teorema 5.27 *Para todos los cardinales* $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$ *se cumple:*

1. $\mathfrak{p} \neq 0 \to 0^{\mathfrak{p}} = 0$,
2. $\mathfrak{p}^0 = 1, \quad 1^{\mathfrak{p}} = 1, \quad \mathfrak{p}^1 = \mathfrak{p}$,
3. $\mathfrak{q} \leq \mathfrak{r} \to \mathfrak{p}^{\mathfrak{q}} \leq \mathfrak{p}^{\mathfrak{r}}$,
4. $\mathfrak{p} \neq 0 \wedge \mathfrak{q} \neq 0 \wedge \mathfrak{q} \leq \mathfrak{r} \to \mathfrak{p}^{\mathfrak{q}} \leq \mathfrak{p}^{\mathfrak{r}}$,
5. $\mathfrak{p}^{\mathfrak{q}+\mathfrak{r}} = \mathfrak{p}^{\mathfrak{q}}\mathfrak{p}^{\mathfrak{r}}$,
6. $(\mathfrak{p}\mathfrak{q})^{\mathfrak{r}} = \mathfrak{p}^{\mathfrak{r}}\mathfrak{q}^{\mathfrak{r}}$.

Una simple inducción basada en estas propiedades demuestra que la exponenciación cardinal sobre los números naturales coincide con la exponenciación ordinal. Otro resultado notable es el siguiente:

Teorema 5.28 *Para todo conjunto* X, *se cumple* $\overline{\overline{\mathcal{P}X}} = 2^{\overline{\overline{X}}}$.

Demostración: Basta observar que la aplicación $f : 2^X \longrightarrow \mathcal{P}X$ dada por $h \mapsto h^{-1}[\{1\}]$ es biyectiva. ∎

En estos términos se cumple que $\overline{\overline{\mathbb{R}}} = \overline{\overline{\mathcal{P}\omega}} = 2^{\aleph_0}$. Por otra parte, ahora el teorema de Cantor admite esta formulación aritmética:

Teorema 5.29 (Teorema de Cantor) *Para todo cardinal* $\mathfrak{p}$ *se cumple*

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

Observaciones El hecho de que la exponenciación cardinal esté tan vinculada al operador $\mathcal{P}$ hace que los axiomas de la teoría de conjuntos dejen sin decidir los hechos más importantes sobre la misma. En efecto, dichos axiomas se limitan a imponer la existencia de los conjuntos que un matemático necesita, es decir, garantizan la existencia de uniones, intersecciones, de los conjuntos de números, etc., pero no dicen nada sobre qué clase de cosa es un conjunto y, en particular, no dicen nada sobre qué contiene $\mathcal{P}X$, ni de lo grande o pequeño que pueda ser este conjunto.

Como muestra de lo "reacia" que es la teoría de conjuntos a pronunciarse sobre la exponenciación cardinal, observamos que sin el axioma de elección no podemos asegurar que A^B o incluso $\mathcal{P}A$ sean bien ordenables aunque A y B lo sean. Esto hace que no podamos desarrollar una aritmética de la exponenciación de K que no requiera el axioma de elección, al contrario de lo que sucede con la suma y el producto. El hecho de que cualquier resultado no trivial requiera el axioma de elección es una muestra de que, por muy bien que conozcamos los conjuntos A y B, en realidad no sabemos casi nada de A^B (y lo mismo vale para $\mathcal{P}X$). De todos modos, aunque el axioma de elección hace que la exponenciación cardinal tenga un comportamiento bastante razonable, lo cierto es que no resuelve en absoluto las cuestiones centrales en torno a ella.

Por ejemplo, la *hipótesis del continuo* es la conjetura de Cantor según la cual $2^{\aleph_0} = \aleph_1$. Sin el axioma de elección hemos probado que $2^{\aleph_0} > \aleph_0$ y, con el axioma de elección (¡pero no sin él!), lo único que podemos añadir a esto es que $2^{\aleph_0} \geq \aleph_1$. Naturalmente, el problema es idéntico para cardinales mayores:

Definición 5.30 Se llama *hipótesis del continuo generalizada* a la siguiente sentencia:

(HCG) Si $\mathfrak{p}$ es un cardinal infinito, no existe ningún cardinal $\mathfrak{q}$ tal que

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

Con el axioma de elección esto equivale a que $2^\kappa = \kappa^+$ para todo cardinal infinito κ, o también a que

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

Sucesiones y partes finitas Para completar los cálculos aritméticos básicos, dado un conjunto bien ordenable A, vamos a calcular el cardinal de los conjuntos

$$A^{<\omega} = \bigcup_{n\in\omega} A^n, \quad \text{y} \quad [A]^{<\omega} = \{x \mid x \subset A \wedge |x| < \aleph_0\},$$

es decir, el conjunto de las sucesiones finitas en A y el de los subconjuntos finitos de A.

Teorema 5.31 *Si A es un conjunto bien ordenable no vacío, entonces $A^{<\omega}$ es bien ordenable, y $|A^{<\omega}| = \aleph_0|A|$.*

Demostración: Supongamos en primer lugar que A es infinito. Entonces $|A \times A| = |A|$, luego podemos fijar una biyección $h : A \times A \longrightarrow A$. Vamos a definir por recurrencia, para cada $n \in \omega$, una biyección $f_n : A^{n+1} \longrightarrow A$. Definimos $f_0 : A^1 \longrightarrow A$ mediante $f_0(s) = s(0)$. Claramente es una biyección. Supuesta definida f_n, definimos $f_{n+1} : A^{n+2} \longrightarrow A$ mediante

$$f_{n+2}(s) = h(f_{n+1}(s|_{n+1}), s(n+1)).$$

Una simple inducción prueba que cada f_n es biyectiva. Ahora definimos la aplicación $\bar{f}_n : A^{n+1} \longrightarrow A \times \{n\}$ mediante $\bar{f}_n(s) = (f_n(s), n)$. Es claro entonces que

$$\bigcup_{n\in\omega} \bar{f}_n : A^{<\omega} \setminus \{\varnothing\} \longrightarrow A \times \omega \text{ biyectiva.}$$

Esto prueba que $A^{<\omega} \setminus \{\varnothing\}$ es bien ordenable, y que su cardinal es $|A|\,\aleph_0$ (que en este caso es $|A|$). Obviamente entonces, $|A^{<\omega}| = |A| + 1 = |A|$.

Si A es finito, a partir de una aplicación inyectiva $A \longrightarrow \omega$ se construye fácilmente una aplicación $A^{<\omega} \longrightarrow \omega^{<\omega}$ también inyectiva, de donde resulta que $|A^{<\omega}| \leq |\omega^{<\omega}| = \aleph_0$.

Por otra parte, fijado un $a \in A$, la aplicación $\omega \longrightarrow A^{<\omega}$ que a cada $n \in \omega$ le asigna la función $c_a^n = n \times \{a\}$ (es decir, la función $n \longrightarrow A$ que toma siempre el valor a) es claramente inyectiva, luego $\aleph_0 \leq |A^{<\omega}|$ y concluimos que $|A^{<\omega}| = \aleph_0 = |A|\,\aleph_0$. ∎

Si A es un conjunto finito, entonces todos sus subconjuntos son finitos, luego $|[A]^{<\omega}| = |\mathcal{P}A| = 2^{|A|}$, que es un número natural, luego $\mathcal{P}A$ y $[A]^{<\omega}$ son conjuntos finitos. Si A es infinito y bien ordenable, tenemos lo siguiente:

Teorema 5.32 *Si A es un conjunto infinito bien ordenable, entonces $[A]^{<\omega}$ también es bien ordenable, y $|[A]^{<\omega}| = |A|$.*

Demostración: La aplicación $A^{<\omega} \longrightarrow [A]^{<\omega}$ dada por $s \mapsto \mathcal{R}s$ es claramente suprayectiva, luego existe una aplicación $[A]^{<\omega} \longrightarrow A^{<\omega}$ inyectiva,[3] lo que prueba que $[A]^{<\omega}$ es bien ordenable, y $|[A]^{<\omega}| \leq |A^{<\omega}| = |A|$.

Por otra parte, la aplicación $A \longrightarrow [A]^{<\omega}$ dada por $a \mapsto \{a\}$ es inyectiva, luego $|A| \leq |[A]^{<\omega}|$ y tenemos la igualdad. ∎

Conjuntos *D*-infinitos En la sección 2.1 tomamos como axioma de infinitud la existencia de un conjunto X en el que existe una aplicación $S : X \longrightarrow X$ inyectiva y no suprayectiva, y explicamos que esto era una forma de postular la existencia de un conjunto infinito.

Los conjuntos X con esta propiedad reciben el nombre de conjuntos *D–infinitos* (o *infinitos de Dedekind*), y los conjuntos que no son D–infinitos se llaman *D–finitos.* Así, el axioma de infinitud adoptado en la sección 2.1 postula la existencia de un conjunto D–infinito.

El teorema 2.14 prueba que todo conjunto finito es D–finito, luego todo conjunto D–infinito es infinito. Por lo tanto, el axioma de infinitud cumple ciertamente su cometido, como, por otra parte, ya hemos comprobado sobradamente. Sin embargo, conviene destacar que no es posible probar que todo conjunto D–finito es finito sin usar el axioma de elección.[4] Lo más que podemos probar es que un conjunto N es D–infinito si y sólo si tiene un subconjunto infinito numerable, es decir, si $\aleph_0 \leq \overline{\overline{N}}$.

En efecto, en la prueba del teorema 2.1 hemos visto que todo conjunto D–infinito X contiene un subconjunto N sobre el que hay definida una función sucesor que cumple los axiomas de Peano, por lo que puede tomarse como conjunto de los números naturales y es, por consiguiente, numerable.

Recíprocamente, si $\aleph_0 \leq \overline{\overline{N}}$, tenemos $F : \omega \longrightarrow N$ inyectiva, y podemos definir $g : N \longrightarrow N$ inyectiva y no suprayectiva mediante

$$g(u) = \begin{cases} F(F^{-1}(u)+1) & \text{si } u \in F[\omega], \\ u & \text{si } u \notin F[\omega]. \end{cases}$$

Con AE tenemos la equivalencia, pues si N es infinito entonces no $|N| < \aleph_0$, luego $\aleph_0 \leq |N|$ y, por consiguiente, N es D–infinito. ∎

[3] Notemos que aquí no usamos el axioma de elección porque $A^{<\omega}$ es bien ordenable.

[4] En realidad basta ED. Si X es un conjunto infinito, consideramos el conjunto A de todas las funciones $s : n \longrightarrow X$ inyectivas, con $n \in \omega$, con la relación $s\,R\,t \leftrightarrow t \subsetneq s$. Claramente ED proporciona una sucesión $\{s_n\}_{n\in\omega}$ que determina una aplicación $f = \bigcup_{n\in\omega} s_n : \omega \longrightarrow X$ inyectiva.

5.3 Sumas y productos infinitos

El cálculo explícito del cardinal de determinados conjuntos requiere considerar sumas y productos infinitos de otros cardinales conocidos. Prácticamente todos los resultados sobre estas sumas y productos dependen del axioma de elección, pues cuando tenemos infinitos conjuntos a menudo es imprescindible escoger una biyección entre cada uno de ellos y su cardinal. Así pues, en esta sección usaremos libremente dicho axioma sin mención explícita.

Definición 5.33 La *suma* de una familia de cardinales $\{\kappa_i\}_{i\in I}$ se define como

$$\sum_{i\in I}\kappa_i = \Big|\bigcup_{i\in I}\kappa_i\times\{i\}\Big|.$$

El resultado fundamental sobre sumas infinitas es el siguiente:

Teorema 5.34 *Para cualquier familia de conjuntos $\{X_i\}_{i\in I}$ se cumple que*

$$\Big|\bigcup_{i\in I}X_i\Big| \le \sum_{i\in I}|X_i|,$$

y si los conjuntos son disjuntos dos a dos entonces se da la igualdad.

Demostración: Por el axioma de elección existe una familia de aplicaciones biyectivas $f_i : |X_i|\times\{i\} \longrightarrow X_i$. Claramente

$$\bigcup_{i\in I} f_i : \bigcup_{i\in I}|X_i|\times\{i\} \longrightarrow \bigcup_{i\in I}X_i$$

es suprayectiva y si los conjuntos X_i son disjuntos dos a dos es biyectiva. Consecuentemente

$$\Big|\bigcup_{i\in I}X_i\Big| \le \Big|\bigcup_{i\in I}|X_i|\times\{i\}\Big| = \sum_{i\in I}|X_i|,$$

y se da la igualdad si los conjuntos son disjuntos. ∎

El teorema siguiente se demuestra sin dificultad:

Teorema 5.35 *Se cumple*

1. *Si $\bigwedge i\in I\ \kappa_i \le \mu_i$, entonces $\sum_{i\in I}\kappa_i \le \sum_{i\in I}\mu_i$,*
2. $\sum_{i\in I}\kappa = |I|\,\kappa$,
3. $\mu\sum_{i\in I}\kappa_i = \sum_{i\in I}\mu\kappa_i$.

A modo de ejemplo demostraremos la asociatividad generalizada de la suma de cardinales:

Teorema 5.36 *Si $I = \bigcup_{j\in J} I_j$ y los conjuntos I_j son disjuntos dos a dos, entonces*

$$\sum_{i\in I}\kappa_i = \sum_{j\in J}\sum_{i\in I_j}\kappa_i.$$

DEMOSTRACIÓN: En efecto:

$$\sum_{i\in I}\kappa_i = \Big|\bigcup_{i\in I}\kappa_i\times\{i\}\Big| = \Big|\bigcup_{j\in J}\bigcup_{i\in I_j}\kappa_i\times\{i\}\Big| = \sum_{j\in J}\Big|\bigcup_{i\in I_j}\kappa_i\times\{i\}\Big| = \sum_{j\in J}\sum_{i\in I_j}\kappa_i.$$

■

Finalmente demostramos el teorema que nos permite calcular cualquier suma de cardinales. Las hipótesis excluyen el caso de una suma finita de cardinales finitos, pero esto es una suma usual de números naturales.

Teorema 5.37 *Si $\{\kappa_i\}_{i\in I}$ es una familia de cardinales no nulos de modo que I es infinito o algún κ_i lo es, entonces*

$$\sum_{i\in I}\kappa_i = |I|\ \sup_{i\in I}\kappa_i.$$

DEMOSTRACIÓN: Llamemos κ al supremo de los κ_i. Como los κ_i son no nulos tenemos que $1 \le \kappa_i \le \kappa$, luego

$$|I| = \sum_{i\in I} 1 \le \sum_{i\in I}\kappa_i \le \sum_{i\in I}\kappa = |I|\,\kappa.$$

Como cada $\kappa_i \le \sum_{i\in I}\kappa_i$, también $\kappa \le \sum_{i\in I}\kappa_i$.

Multiplicando las desigualdades (y teniendo en cuenta que, por las hipótesis, la suma es un cardinal infinito) obtenemos

$$|I|\,\kappa \le \Big(\sum_{i\in I}\kappa_i\Big)^2 = \sum_{i\in I}\kappa_i.$$

■

Pasemos ahora a estudiar los productos infinitos. No podemos obtener resultados tan concluyentes como los que hemos obtenido para las sumas debido a su proximidad a la exponenciación cardinal. Recordemos la definición del producto cartesiano de una familia de conjuntos:

$$\prod_{i\in I} X_i = \{f \mid f : I \longrightarrow \bigcup_{i\in I} X_i \wedge \bigwedge i \in I\ f(i) \in X_i\}.$$

El producto cartesiano de un conjunto de conjuntos es un conjunto porque está contenido en $\mathcal{P}(I \times \bigcup_{i\in I} X_i)$.

Definición 5.38 Llamaremos *producto* de una familia de cardinales $\{\kappa_i\}_{i\in I}$ al cardinal

$$\prod_{i\in I}\kappa_i = \Big|\prod_{i\in I}\kappa_i\Big|,$$

donde el producto de la izquierda es el que estamos definiendo y el de la derecha es el producto cartesiano.

El resultado básico sobre productos infinitos es el siguiente:

Teorema 5.39 *Si $\{X_i\}_{i\in I}$ es una familia de conjuntos infinitos, entonces*

$$\Big|\prod_{i\in I} X_i\Big| = \prod_{i\in I} |X_i|.$$

DEMOSTRACIÓN: Por el axioma de elección existe una familia de aplicaciones biyectivas $f_i : X_i \longrightarrow |X_i|$. Entonces la aplicación $f : \prod_{i\in I} X_i \longrightarrow \prod_{i\in I} |X_i|$ dada por $f(\{x_i\}_{i\in I}) = \{f(x_i)\}_{i\in I}$ es claramente biyectiva. Así pues,

$$\Big|\prod_{i\in I} X_i\Big| = \Big|\prod_{i\in I} |X_i|\Big| = \prod_{i\in I} |X_i|.$$

■

Recogemos en el teorema siguiente las propiedades sencillas de los productos:

Teorema 5.40 *Se cumple:*

1. *Si algún $\kappa_i = 0$, entonces $\prod_{i\in I} \kappa_i = 0$,*
2. $\prod_{i\in I} \kappa = \kappa^{|I|}$,
3. $\Big(\prod_{i\in I} \kappa_i\Big)^\mu = \prod_{i\in I} \kappa_i^\mu$,
4. $\prod_{i\in I} \kappa^{\mu_i} = \kappa^{\sum_{i\in I} \mu_i}$,
5. *Si $\bigwedge i \in I\ \kappa_i \leq \mu_i$, entonces $\prod_{i\in I} \kappa_i \leq \prod_{i\in I} \mu_i$,*
6. *Si $I = \bigcup_{j\in J} I_j$, donde los conjuntos I_j son disjuntos dos a dos, entonces*

$$\prod_{i\in I} \kappa_i = \prod_{j\in J} \prod_{i\in I_j} \kappa_i.$$

No es posible demostrar un teorema tan general como 5.37 para el cálculo de productos infinitos, pero a menudo basta el teorema siguiente:

Teorema 5.41 *Sea $\{\kappa_\alpha\}_{\alpha<\mu}$ una familia de cardinales no nulos (donde μ es un cardinal infinito) tal que si $\alpha \leq \beta < \mu$ entonces $\kappa_\alpha \leq \kappa_\beta$. Entonces*

$$\prod_{\alpha<\mu} \kappa_\alpha = (\sup_{\alpha<\mu} \kappa_\alpha)^\mu.$$

DEMOSTRACIÓN: Sea $\kappa = \sup_{\alpha<\mu} \kappa_\alpha$. Entonces $\prod_{\alpha<\mu} \kappa_\alpha \leq \prod_{\alpha<\mu} \kappa = \kappa^\mu$.

Tomemos una aplicación biyectiva $f : \mu \times \mu \longrightarrow \mu$. Sea $A_\alpha = f[\mu \times \{\alpha\}]$. Así $\mu = \bigcup_{\alpha<\mu} A_\alpha$ y los conjuntos A_α tienen cardinal μ y son disjuntos dos a dos. En particular no están acotados en μ (o tendrían cardinal menor). Teniendo en cuenta la monotonía de la sucesión κ_α, es claro que $\sup_{\beta\in A_\alpha} \kappa_\beta = \kappa$.

Como los κ_β son no nulos, tenemos que $\kappa_\beta \leq \prod_{\beta\in A_\alpha} \kappa_\beta$, luego

$$\kappa = \sup_{\beta\in A_\alpha} \kappa_\beta \leq \prod_{\beta\in A_\alpha} \kappa_\beta.$$

Por consiguiente

$$\kappa^\mu = \prod_{\alpha<\mu} \kappa \leq \prod_{\alpha<\mu} \prod_{\beta\in A_\alpha} \kappa_\beta = \prod_{\alpha<\mu} \kappa_\alpha \leq \kappa^\mu.$$

■

Por ejemplo,

$$\prod_{n\in\omega} \aleph_n = \aleph_\omega^{\aleph_0}.$$

Ejercicio: Probar que el teorema anterior sigue siendo válido si sustituimos μ por un ordinal límite λ y suponemos que λ contiene $|\lambda|$ subconjuntos no acotados disjuntos dos a dos. En particular, probar que es cierto siempre que $\lambda < \omega_1$. Más adelante veremos que en general estas restricciones no pueden ser eliminadas.

Veamos ahora una desigualdad entre una suma y un producto:

Teorema 5.42 *Si* $\bigwedge i \in I\ 2 \leq \kappa_i$, *entonces* $\sum_{i\in I} \kappa_i \leq \prod_{i\in I} \kappa_i$.

DEMOSTRACIÓN: Claramente $|I| \leq 2^{|I|} = \prod_{i\in I} 2 \leq \prod_{i\in I} \kappa_i$. Por otra parte, $\kappa_i \leq \prod_{i\in I} \kappa_i$, luego $\sup_{i\in I} \kappa_i \leq \prod_{i\in I} \kappa_i$. El teorema 5.37 nos da la conclusión si I es infinito o algún κ_i es infinito. El caso restante se demuestra fácilmente por inducción sobre el cardinal de I (aunque nunca vamos a necesitar este caso).

■

Si nos fijamos en todos los teoremas sobre cardinales infinitos que hemos demostrado hasta ahora, no encontraremos más que una desigualdad estricta: el teorema de Cantor. El próximo teorema es la desigualdad estricta más general que se conoce sobre cardinales infinitos. Cualquier otra es un caso particular de ésta. Por ejemplo, el teorema de Cantor se obtiene haciendo $\kappa_i = 1$ y $\mu_i = 2$.

Teorema 5.43 (Teorema de König) *Si* $\bigwedge i \in I\ \kappa_i < \mu_i$, *entonces*

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

DEMOSTRACIÓN: Si $I = \varnothing$ el teorema se reduce a $0 < 1$. En otro caso, sea $I' = \{i \in I \mid \kappa_i > 0\}$. Para $i \in I'$ tenemos que $1 \leq \kappa_i < \mu_i$, luego $2 \leq \mu_i$ y podemos aplicar el teorema anterior:

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

Supongamos que se diera la igualdad, es decir, que existe una aplicación biyectiva

$$f : \bigcup_{i\in I}\kappa_i \times \{i\} \longrightarrow \prod_{i\in I}\mu_i.$$

Sea $f_i : \kappa_i \longrightarrow \mu_i$ dada por $f_i(\alpha) = f(\alpha, i)(i)$.

Como $\kappa_i < \mu_i$ la aplicación f_i no puede ser suprayectiva, luego existe un $\alpha_i \in \mu_i \setminus f_i[\kappa_i]$. Los α_i determinan un elemento $\alpha = (\alpha_i)_{i\in I} \in \prod_{i\in I}\mu_i$. Como f es biyectiva, α tiene una antiimagen, de modo que $f(\beta, j) = \alpha$. Entonces $\beta \in \kappa_j$ y $f_j(\beta) = f(\beta, j)(j) = \alpha_j \in f_j[\kappa_j]$, en contradicción con la elección de α_j. ∎

5.4 Cofinalidad

El concepto de cofinalidad es esencial en el estudio de los cardinales infinitos, y en particular en el estudio de la exponenciación cardinal que todavía tenemos pendiente. En esta sección no usamos el axioma de elección salvo en unos pocos casos, donde lo indicaremos explícitamente.

Definición 5.44 Diremos que una aplicación $f : \alpha \longrightarrow \beta$ entre dos ordinales es *cofinal* si $f[\alpha]$ no está acotado estrictamente en β, es decir, si se cumple que $\bigwedge\gamma < \beta \bigvee\delta < \alpha\ \gamma \leq f(\delta)$.

Llamaremos *cofinalidad* de β al menor ordinal α tal que existe una aplicación cofinal $f : \alpha \longrightarrow \beta$. Lo representaremos por $\operatorname{cf}\beta$. Como la identidad en β es obviamente cofinal, vemos que $\operatorname{cf}\beta$ está bien definida y además $\operatorname{cf}\beta \leq \beta$.

Informalmente, podemos decir que $\operatorname{cf}\beta$ es el mínimo número de pasos que hay que dar para ascender completamente por β, es decir, para ascender rebasando (o, al menos, igualando) cualquier ordinal menor que β. Obviamente $\operatorname{cf} 0 = 0$ y $\operatorname{cf}(\alpha + 1) = 1$. En efecto, la aplicación $f : 1 \longrightarrow \alpha + 1$ dada por $f(0) = \alpha$ es cofinal ($\alpha + 1$ tiene un máximo elemento y basta un paso para llegar hasta él).

Así pues, la cofinalidad sólo tiene interés sobre los ordinales límite, los cuales no se pueden recorrer en un paso. De hecho, siempre hacen falta infinitos pasos:

Teorema 5.45 $\bigwedge\lambda\ \omega \leq \operatorname{cf}\lambda \leq \lambda$.

DEMOSTRACIÓN: Ya sabemos que $\operatorname{cf}\lambda \leq \lambda$. Por otra parte $\operatorname{cf}\lambda$ no puede ser un número natural n, ya que si $f : n \longrightarrow \lambda$, entonces $f[n]$ es un conjunto finito, luego tiene un máximo $\alpha < \lambda$, luego $\alpha + 1 < \lambda$ es una cota estricta de $f[n]$, luego f no es cofinal. ∎

Decimos que $\operatorname{cf}\alpha$ es el mínimo número de pasos necesarios para ascender completamente por α. Este "número de pasos" es ciertamente un cardinal:

Teorema 5.46 $\bigwedge\alpha\ \operatorname{cf}\alpha \in K$.

DEMOSTRACIÓN: Si $\alpha = 0$ o $\alpha = \beta + 1$ sabemos que $\operatorname{cf}\alpha$ es 0 o 1, luego es un cardinal. Basta probar entonces que $\bigwedge\lambda\ \operatorname{cf}\lambda \in K$. Supongamos que $|\operatorname{cf}\lambda| < \operatorname{cf}\lambda$. Sea $f : |\operatorname{cf}\lambda| \longrightarrow \operatorname{cf}\lambda$ biyectiva y sea $g : \operatorname{cf}\lambda \longrightarrow \lambda$ cofinal. Entonces $f \circ g : |\operatorname{cf}\lambda| \longrightarrow \lambda$ tiene la misma imagen que g, luego es cofinal, en contra de la minimalidad de $\operatorname{cf}\lambda$. ∎

A partir de aquí trataremos únicamente con ordinales límite. Notemos que $f : \alpha \longrightarrow \lambda$ es cofinal si y sólo si $f[\alpha]$ no está acotado en λ, es decir, si y sólo si

$$\lambda = \sup f[\alpha] = \bigcup_{\delta<\alpha} f(\delta).$$

La forma más económica de ascender por un ordinal es no retrocediendo nunca. Veamos que esto siempre es posible:

Teorema 5.47 $\bigwedge\lambda\bigvee f\ f : \operatorname{cf}\lambda \longrightarrow \lambda$ *cofinal y normal.*

DEMOSTRACIÓN: Sea $g : \operatorname{cf}\lambda \longrightarrow \lambda$ cofinal. Definimos $f : \operatorname{cf}\lambda \longrightarrow \Omega$ como la única aplicación que cumple

$$\begin{aligned}
&f(0) = g(0),\\
&\textstyle\bigwedge\alpha < \operatorname{cf}\lambda\ f(\alpha+1) = \max\{g(\alpha), f(\alpha)+1\},\\
&\textstyle\bigwedge\lambda' < \operatorname{cf}\lambda\ f(\lambda') = \bigcup_{\delta<\lambda'} f(\delta).
\end{aligned}$$

Claramente f es normal. Veamos por inducción que $\bigwedge\alpha < \operatorname{cf}\lambda\ f(\alpha) < \lambda$. En efecto, para $\alpha = 0$ es obvio y si vale para α vale claramente para $\alpha + 1$. Supongamos que $\lambda' < \operatorname{cf}\lambda$ y que $\bigwedge\delta < \lambda' f(\delta) < \lambda$. Entonces es claro que $f(\lambda') \leq \lambda$, pero no puede darse la igualdad porque entonces $f|'_\lambda$ sería cofinal en λ, en contradicción con que $\lambda' < \operatorname{cf}\lambda$. Así pues, también se cumple para λ'.

Tenemos entonces que $f : \operatorname{cf}\lambda \longrightarrow \lambda$ normal y, como $\bigwedge\alpha < \operatorname{cf}\lambda\ g(\alpha) \leq f(\alpha)$, es claro que f es cofinal. ∎

Este teorema nos permite expresar la cofinalidad de un ordinal límite en términos únicamente de sus subconjuntos acotados:

Teorema 5.48 *La cofinalidad de un ordinal límite λ es el mínimo cardinal κ tal que existe un subconjunto $a \subset \lambda$ no acotado de cardinal κ.*

DEMOSTRACIÓN: Si $f : \operatorname{cf}\lambda \longrightarrow \lambda$ es cofinal y normal, entonces $a = f[\operatorname{cf}\lambda]$ es un subconjunto no acotado de λ y, como f es inyectiva, su cardinal es $\operatorname{cf}\lambda$.

Recíprocamente, si $a \subset \lambda$ es un subconjunto no acotado, sea $f : |a| \longrightarrow a$ una biyección. Entonces es claro que $f : |a| \longrightarrow \lambda$ cofinal, luego $\operatorname{cf}\lambda \leq |a|$. ∎

En general, la composición de aplicaciones cofinales no es necesariamente cofinal (es fácil encontrar ejemplos). El teorema siguiente nos da una condición suficiente:

Teorema 5.49 *Si $f : \lambda_1 \longrightarrow \lambda_2$ y $g : \lambda_2 \longrightarrow \lambda_3$ son cofinales y además g es creciente, entonces $f \circ g : \lambda_1 \longrightarrow \lambda_3$ es cofinal.*

DEMOSTRACIÓN: Sea $\alpha < \lambda_3$. Como g es cofinal existe $\beta < \lambda_2$ tal que $\alpha \leq g(\beta)$. Como f es cofinal existe $\gamma < \lambda_1$ tal que $\beta \leq f(\gamma)$. Como g es creciente, $\alpha \leq g(\beta) \leq g(f(\gamma)) = (f \circ g)(\gamma)$, luego $f \circ g$ es cofinal. ∎

Esto tiene una consecuencia destacable:

Teorema 5.50 *Si $f : \lambda_1 \longrightarrow \lambda_2$ es cofinal y creciente, entonces* $\operatorname{cf} \lambda_1 = \operatorname{cf} \lambda_2$.

DEMOSTRACIÓN: Sea $g : \operatorname{cf} \lambda_1 \longrightarrow \lambda_1$ cofinal. Por el teorema anterior $g \circ f : \operatorname{cf} \lambda_1 \longrightarrow \lambda_2$ es cofinal, luego $\operatorname{cf} \lambda_2 \leq \operatorname{cf} \lambda_1$.

Sea ahora $h : \operatorname{cf} \lambda_2 \longrightarrow \lambda_2$ cofinal y definamos $r : \operatorname{cf} \lambda_2 \longrightarrow \lambda_1$ de modo que $r(\alpha)$ sea el menor $\beta < \lambda_1$ tal que $h(\alpha) < f(\beta)$, que existe porque f es cofinal. Entonces r es cofinal, pues si $\gamma < \lambda_1$ entonces $f(\gamma) < \lambda_2$, luego existe un $\delta < \operatorname{cf} \lambda_2$ tal que $f(\gamma) \leq h(\delta)$. Por definición de r tenemos que $h(\delta) < f(r(\delta))$, y si fuera $r(\delta) \leq \gamma$ sería $f(r(\delta)) \leq f(\gamma) \leq h(\delta)$, contradicción, luego $\gamma \leq r(\delta)$ y r es cofinal. Por consiguiente $\operatorname{cf} \lambda_1 \leq \operatorname{cf} \lambda_2$ y tenemos la igualdad. ∎

Este teorema, además de servir para calcular cofinalidades, tiene una lectura negativa: en la prueba del teorema 5.47 hemos partido de una aplicación cofinal arbitraria y la hemos modificado para hacerla cofinal y normal, en particular creciente. Ahora vemos que esto no siempre puede hacerse: pueden darse casos en los que exista una aplicación cofinal entre dos ordinales límite y no exista ninguna aplicación cofinal y creciente, pues una condición necesaria para que esto ocurra es que ambos ordinales tengan la misma cofinalidad.

Respecto al cálculo de cofinalidades, el teorema siguiente es una consecuencia sencilla del anterior, pero más cómodo en la práctica:

Teorema 5.51 *Si $f : \lambda_1 \longrightarrow \Omega$ es normal y $\lambda < \lambda_1$, entonces* $\operatorname{cf} \lambda = \operatorname{cf} f(\lambda)$.

DEMOSTRACIÓN: Es claro que $f|_\lambda : \lambda \longrightarrow f(\lambda)$ es cofinal y creciente. Basta aplicar el teorema anterior. ∎

Por ejemplo, $\operatorname{cf} \aleph_{\omega^2} = \operatorname{cf} \omega^2 = \operatorname{cf}(\omega \cdot \omega) = \operatorname{cf} \omega = \aleph_0$, donde hemos usado la normalidad de las funciones $\aleph$ y $\omega\cdot$. Una función cofinal de ω en $\aleph_{\omega^2}$ es $f(n) = \aleph_{\omega \cdot n}$.

Veamos un ejemplo típico de la utilidad del concepto de cofinalidad.

Definición 5.52 Sea $f : \lambda \longrightarrow \lambda$, donde λ cumple $\operatorname{cf} \lambda > \aleph_0$ o bien $\lambda = \Omega$. Para cada $\alpha \in \lambda$ definimos

$$f^0(\alpha) = \alpha,$$
$$f^{n+1}(\alpha) = f(f^n(\alpha)),$$
$$f^\omega(\alpha) = \sup_{n \in \omega} f^n(\alpha).$$

Una simple inducción prueba que $\bigwedge n \in \omega\ f^n(\alpha) \in \lambda$, y la hipótesis sobre λ asegura que el conjunto numerable $\{f^n(\alpha) \mid n \in \omega\}$ tiene que estar acotado

en λ (teorema 5.48), luego $f^\omega(\alpha) \in \lambda$. Así pues, tenemos definida una función $f^\omega : \lambda \longrightarrow \lambda$ a la que llamaremos *función iterada* de f.

Es inmediato a partir de esta construcción que $\bigwedge\alpha \in \lambda\ \alpha \leq f^\omega(\alpha)$.

Informalmente, $f^\omega(\alpha)$ resulta de aplicar infinitas veces f a α, lo cual hace que si aplicamos f una vez más no se nota:

Teorema 5.53 *Sea $f : \lambda \longrightarrow \lambda$ una función normal, donde $\operatorname{cf}\lambda > \aleph_0$ o bien $\lambda = \Omega$. Entonces $\bigwedge\alpha \in \lambda\ f(f^\omega(\alpha)) = f^\omega(\alpha)$.*

Demostración: Como f es normal, se cumple que $f^\omega(\alpha) \leq f(f^\omega(\alpha))$. Para probar la otra desigualdad distinguimos tres casos:

Si $f^\omega(\alpha) = 0$, entonces $\alpha = f(\alpha) = 0$, pues tanto α como $f(\alpha)$ están bajo $f^\omega(\alpha)$. Por consiguiente $f(f^\omega(\alpha)) = f(0) = f(\alpha) \leq f^\omega(\alpha)$.

Si $f^\omega(\alpha) = \gamma + 1$, entonces $\gamma < f^\omega(\alpha)$, luego $\gamma < f^n(\alpha)$ para cierto $n \in \omega$. Así,

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

Si $f^\omega(\alpha)$ es un ordinal límite, como f es normal,

$$f(f^\omega(\alpha)) = \bigcup_{\delta < f^\omega(\alpha)} f(\delta) \leq \bigcup_{n\in\omega} f(f^n(\alpha)) \leq \bigcup_{n\in\omega} f^{n+1}(\alpha) \leq f^\omega(\alpha).$$

■

En particular hemos demostrado:

Teorema 5.54 (Teorema de punto fijo para funciones normales) *Sea $f : \lambda \longrightarrow \lambda$ una función normal, donde $\operatorname{cf}\lambda > \aleph_0$ o bien $\lambda = \Omega$. Entonces*

$$\bigwedge\alpha \in \lambda \bigvee\beta \in \lambda(\alpha \leq \beta \wedge f(\beta) = \beta).$$

La función $(\omega+) : \omega^2 \longrightarrow \omega^2$ es un ejemplo de función normal sin puntos fijos. Destaquemos el papel que desempeña la hipótesis sobre la cofinalidad: para construir puntos fijos necesitamos ascender $\aleph_0$ pasos, luego necesitamos que la cofinalidad de λ sea no numerable para garantizar que con el ascenso no nos salimos de λ.

Así, por ejemplo, existen cardinales κ arbitrariamente grandes tales que $\kappa = \aleph_\kappa$.

Pasemos ahora al cálculo de la cofinalidad de los cardinales infinitos. Ello requiere el axioma de elección. En primer lugar damos una caracterización en términos de la aritmética cardinal:

Teorema 5.55 (AE) *Sea κ un cardinal infinito. Entonces $\operatorname{cf}\kappa$ es el menor cardinal μ tal que existe una familia de cardinales $\{\nu_\alpha\}_{\alpha<\mu}$ tales que*

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

DEMOSTRACIÓN: Sea $f : \operatorname{cf}\kappa \longrightarrow \kappa$ cofinal. Entonces $\kappa = \bigcup_{\alpha<\operatorname{cf}\kappa} f(\alpha)$. Sea $\nu_\alpha = |f(\alpha)| < \kappa$. Entonces

$$\kappa = |\kappa| = \Big|\bigcup_{\alpha<\operatorname{cf}\kappa} f(\alpha)\Big| \leq \sum_{\alpha<\operatorname{cf}\kappa} \nu_\alpha \leq \sum_{\alpha<\operatorname{cf}\kappa} \kappa = \kappa \operatorname{cf}\kappa = \kappa.$$

Por consiguiente $\kappa = \sum_{\alpha<\operatorname{cf}\kappa} \nu_\alpha$. Ahora veamos que $\operatorname{cf}\kappa$ es el mínimo cardinal que cumple esto. Tomemos $\mu < \operatorname{cf}\kappa$ y sea $\{\nu_\alpha\}_{\alpha<\mu}$ una familia de cardinales tal que $\bigwedge\alpha < \mu\ \nu_\alpha < \kappa$.

La aplicación $f : \mu \longrightarrow \kappa$ dada por $f(\alpha) = \nu_\alpha$ no puede ser cofinal, luego existe un ordinal $\beta < \kappa$ tal que $\bigwedge\alpha < \mu\ \nu_\alpha < \beta$ y así

$$\sum_{\alpha<\mu} \nu_\alpha \leq \sum_{\alpha<\mu} |\beta| = \mu\,|\beta| < \kappa,$$

luego, en efecto, $\operatorname{cf}\kappa$ es el mínimo cardinal con la propiedad del enunciado. ∎

Así pues, tenemos lo siguiente sobre las cofinalidades de los cardinales infinitos:

Teorema 5.56 *Se cumple*

1. $\operatorname{cf}\aleph_0 = \aleph_0$,
2. $\bigwedge\lambda\ \operatorname{cf}\aleph_\lambda = \operatorname{cf}\lambda$,
3. (AE) $\bigwedge\alpha\ \operatorname{cf}\aleph_{\alpha+1} = \aleph_{\alpha+1}$.

DEMOSTRACIÓN: 1) es consecuencia inmediata de 5.45, 2) es un caso particular de 5.51. Veamos c). En caso contrario, sería $\operatorname{cf}\aleph_{\alpha_1} \leq \aleph_\alpha$ y por el teorema anterior existirían cardinales $\{\nu_\delta\}_{\delta<\operatorname{cf}\aleph_{\alpha+1}}$ tales que $\bigwedge\delta < \operatorname{cf}\aleph_{\alpha+1}\ \nu_\delta \leq \aleph_\alpha$ y

$$\aleph_{\alpha+1} = \sum_{\delta<\operatorname{cf}\aleph_{\alpha+1}} \nu_\delta \leq \sum_{\delta<\operatorname{cf}\aleph_{\alpha+1}} \aleph_\alpha = \aleph_\alpha\ \operatorname{cf}\aleph_{\alpha+1} = \aleph_\alpha,$$

contradicción. ∎

Así pues, el hecho de que $\operatorname{cf}\aleph_0 = \aleph_0$ expresa que la unión finita de conjuntos finitos es finita e, igualmente, $\operatorname{cf}\aleph_1 = \aleph_1$ expresa que la unión de una cantidad numerable de conjuntos numerables es numerable. En cambio, podemos obtener un conjunto de cardinal $\aleph_\omega$ uniendo tan sólo una cantidad numerable de conjuntos de cardinal menor que $\aleph_\omega$, pues basta unir un conjunto de cardinal $\aleph_0$ con otro de cardinal $\aleph_1$, con otro de cardinal $\aleph_2$, etc. Por ello, $\operatorname{cf}\aleph_\omega = \aleph_0$.

Definición 5.57 Un cardinal infinito κ es *regular* si $\operatorname{cf}\kappa = \kappa$ y es *singular* si $\operatorname{cf}\kappa < \kappa$.

Un cardinal infinito κ es un *cardinal sucesor* si es de la forma μ^+, para otro cardinal μ y es un *cardinal límite* en caso contrario. Es claro que los cardinales límite son $\aleph_0$ y los de la forma $\aleph_\lambda$, mientras que los cardinales sucesores son

los de la forma $\aleph_{\alpha+1}$. Hemos probado que $\aleph_0$ y todos los cardinales sucesores son regulares. En cambio, $\aleph_\omega$ o $\aleph_{\omega_3}$ son ejemplos de cardinales singulares (de cofinalidades, respectivamente, $\aleph_0$ y $\aleph_3$).

De los teoremas 5.47 y 5.50 se sigue inmediatamente:

Teorema 5.58 $\bigwedge\alpha$ $\operatorname{cf}\alpha$ *es un cardinal regular.*

Todo cardinal sucesor es regular y conocemos ejemplos de cardinales límite singulares. Queda abierta la cuestión de si existen cardinales límite regulares aparte de $\aleph_0$.

Definición 5.59 Un *cardinal débilmente inaccesible* es un cardinal límite regular distinto de $\aleph_0$.

Sucede que a partir de los axiomas que estamos considerando no es posible demostrar la existencia de cardinales débilmente inaccesibles. Terminamos probando una propiedad de estos cardinales:

Teorema 5.60 *Un cardinal regular κ es débilmente inaccesible si y sólo si cumple $\kappa = \aleph_\kappa$.*

Demostración: Una implicación es obvia. Si κ es débilmente inaccesible, entonces $\kappa = \aleph_\lambda$, para cierto λ tal que

$$\lambda \leq \aleph_\lambda = \kappa = \operatorname{cf}\kappa = \operatorname{cf}\aleph_\lambda = \operatorname{cf}\lambda \leq \lambda.$$

■

Naturalmente, la función $\aleph$ tiene infinitos puntos fijos que no son cardinales inaccesibles (porque son singulares).

5.5 Exponenciación de cardinales

La exponenciación de cardinales es muy diferente de la suma y el producto, en cuanto que éstos están completamente determinados y pueden ser calculados con facilidad, de modo que podemos afirmar, por ejemplo, que

$$\aleph_5 + \aleph_7 = \aleph_5\aleph_7 = \aleph_7.$$

En cambio, los axiomas de NBG no permiten determinar ni siquiera el valor de $2^{\aleph_0}$, que es el cardinal de un conjunto tan "relativamente simple" como $\mathcal{P}\omega$. De hecho, la exponenciación cardinal sigue siendo hoy en día objeto de investigación, pues no se sabe a ciencia cierta dónde acaba lo que se puede decir sobre ella sin más base que los axiomas usuales de la teoría de conjuntos y qué posibilidades son consistentes con ellos aunque indemostrables a partir de ellos.

Hasta ahora hemos presentado únicamente las propiedades más elementales de la exponenciación de cardinales, que pueden probarse incluso sin el axioma de elección. Aquí vamos a obtener más resultados trabajando con la axiomática completa de NBG.

Nota En lo sucesivo usaremos la notación ${}^{\beta}\alpha$ para representar al conjunto de las aplicaciones de β en α cuando la notación usual α^β pueda confundirse con la exponenciación ordinal o cardinal. ∎

Sabemos que la exponenciación de números naturales se reduce a la usual, por lo que podemos centrarnos en el caso en que al menos uno de los cardinales es infinito. Más concretamente, el caso realmente interesante se da cuando el exponente es infinito, ya que si es finito la potencia se reduce a las propiedades del producto de cardinales por inducción. De hecho, en virtud del teorema 5.25, el teorema siguiente (enunciado para cardinales no necesariamente bien ordenables) es una forma equivalente del axioma de elección:

Teorema 5.61 *Si κ es un cardinal infinito y n un número natural no nulo, entonces $\kappa^n = \kappa$.*

Si la base es finita (mayor que 1, o si no el cálculo es trivial), el problema se reduce al caso en que es igual a 2. Más en general:

Teorema 5.62 *Sean κ y μ cardinales tales que $2 \leq \kappa \leq \mu$ y $\aleph_0 \leq \mu$. Entonces $\kappa^\mu = 2^\mu$.*

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

Si la base es infinita podemos centrarnos en el caso en que sea un cardinal límite, en virtud de la fórmula que probamos a continuación. En la prueba hacemos uso de un argumento general que conviene destacar porque nos va a aparecer más veces:

Si $\mu < \operatorname{cf}\kappa$, entonces

$$ {}^{\mu}\kappa = \bigcup_{\alpha<\kappa} {}^{\mu}\alpha.$$

En efecto, esto es una forma de expresar que toda función $f : \mu \longrightarrow \kappa$ está acotada.

Teorema 5.63 (Fórmula de Hausdorff) *Se cumple:*

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

Demostración: Si $\alpha + 1 \leq \beta$, entonces $\aleph_{\alpha+1} \leq \aleph_\beta < 2^{\aleph_\beta}$, luego

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

Si, por el contrario, $\beta < \alpha + 1$, entonces, como $\aleph_{\alpha+1}$ es regular,

$$ {}^{\omega_\beta}\omega_{\alpha+1} = \bigcup_{\delta<\omega_{\alpha+1}} {}^{\omega_\beta}\delta,$$

luego

$$\aleph_{\alpha+1}^{\aleph_\beta} = |{}^{\omega_\beta}\omega_{\alpha+1}| = \Big|\bigcup_{\delta<\omega_{\alpha+1}} {}^{\omega_\beta}\delta\Big| \leq \sum_{\delta<\omega_{\alpha+1}} |\delta|^{\aleph_\beta} \leq \sum_{\delta<\omega_{\alpha+1}} \aleph_\alpha^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta}\aleph_{\alpha+1}.$$

La otra desigualdad es obvia. ∎

Al igual que 5.62, muchos de los resultados sobre exponenciación cardinal involucran la función 2^κ, la cual, ciertamente, es el esqueleto de la exponenciación. Por ello es conveniente darle un nombre:

Definición 5.64 Se llama *función del continuo* a la función $\kappa \mapsto 2^\kappa$ definida sobre los cardinales infinitos.

Así, la hipótesis del continuo generalizada no es más que una determinación de la función del continuo, en virtud de la cual $2^\kappa = \kappa^+$. Ya hemos comentado que esta hipótesis no puede ser demostrada ni refutada, lo que significa que hay otras alternativas igualmente consistentes con los axiomas de NBG (supuesto, claro, que éstos sean consistentes). De todos modos, no sirve cualquier determinación total o parcial de la función del continuo. Por ejemplo, es obvio que sería contradictorio suponer que

$$2^{\aleph_0} = \aleph_5 \wedge 2^{\aleph_1} = \aleph_3.$$

Más en general, la función del continuo ha de respetar la monotonía:

$$\kappa \leq \mu \to 2^\kappa \leq 2^\mu.$$

Otra restricción a la función del continuo es el teorema de Cantor: sería contradictorio suponer que $2^\kappa = \kappa$ para todo cardinal κ, a pesar de que esta función del continuo sí que es monótona. En realidad, la función del continuo está sometida a una desigualdad más fina que el teorema de Cantor, consecuencia del teorema de König 5.43 y, más concretamente, del teorema siguiente:

Teorema 5.65 (Teorema de König) *Para todo cardinal infinito κ se cumple $\kappa < \kappa^{\operatorname{cf}\kappa}$.*

Demostración: Sea $\{\mu_\alpha\}_{\alpha<\operatorname{cf}\kappa}$ una familia de cardinales menores que κ tales que $\kappa = \sum_{\alpha<\operatorname{cf}\kappa} \mu_\alpha$. Por el teorema 5.43 resulta que

$$\kappa = \sum_{\alpha<\operatorname{cf}\kappa} \mu_\alpha < \prod_{\alpha<\operatorname{cf}\kappa} \kappa = \kappa^{\operatorname{cf}\kappa}.$$

■

Ciertamente, este teorema refina al teorema de Cantor, pues en virtud del teorema 5.62 éste puede expresarse como $\kappa < \kappa^\kappa$, y en el teorema anterior el exponente es menor o igual que κ. De todos modos, podemos expresar esta restricción en términos de la función del continuo:

Teorema 5.66 (Teorema de König) *Si κ es un cardinal infinito, entonces $\kappa < \operatorname{cf} 2^\kappa$.*

Demostración: Si $\operatorname{cf} 2^\kappa \leq \kappa$, entonces $(2^\kappa)^{\operatorname{cf} 2^\kappa} \leq (2^\kappa)^\kappa = 2^\kappa$, en contradicción con el teorema anterior. ■

Así pues, $2^{\aleph_0}$ puede ser $\aleph_1$, $\aleph_2$, $\aleph_{\omega+1}$ o $\aleph_{\omega_3}$, pero no $\aleph_\omega$. Cuando decimos "puede ser" queremos decir que es consistente suponer que lo es. En efecto,

aunque no lo vamos a probar aquí, este teorema y la monotonía es todo lo que puede probarse sobre la función del continuo sobre cardinales regulares, en el sentido de que cualquier axioma que determine la función del continuo sobre cardinales regulares que sea compatible con estos dos requisitos es consistente con los axiomas de NBG (supuesto que éstos sean consistentes).

Notemos que no exigimos que la función 2^κ sea estrictamente monótona, de modo que, por ejemplo, es consistente suponer que $2^{\aleph_0} = 2^{\aleph_1} = \aleph_5$.

Debemos resaltar la restricción a cardinales regulares. Si no fuera así podríamos decir que comprendemos completamente la función del continuo, en cuanto que sabríamos decir exactamente qué posibilidades son consistentes y cuáles no. Sin embargo, la situación en los cardinales límite es muy confusa. Por ejemplo, es contradictorio suponer que

$$\bigwedge\alpha\ 2^{\aleph_\alpha} = \aleph_{\alpha+\omega+2},$$

a pesar de que esta (presunta) función del continuo respeta tanto la monotonía como el teorema de König. Según lo dicho, no hay inconveniente en postular este axioma únicamente para cardinales regulares, pero no puede cumplirse para todos los cardinales singulares, como muestra el teorema siguiente:

Teorema 5.67 *Si un ordinal β cumple $\bigwedge\alpha\ 2^{\aleph_\alpha} = \aleph_{\alpha+\beta}$, entonces $\beta < \omega$.*

Demostración: Supongamos que β es infinito y sea α el mínimo ordinal tal que $\beta < \alpha + \beta$. Claramente $0 < \alpha \leq \beta$. Necesariamente α es un ordinal límite, pues si $\alpha = \gamma + 1$ entonces

$$\beta < \alpha + \beta = \gamma + 1 + \beta = \gamma + \beta,$$

luego γ cumple lo mismo que α, en contra de la minimalidad de α.

$$\begin{aligned}\aleph_{\alpha+\alpha+\beta} &= 2^{\aleph_{\alpha+\alpha}} = 2^{\sum\limits_{\delta<\alpha}\aleph_{\alpha+\delta}} = \prod_{\delta<\alpha} 2^{\aleph_{\alpha+\delta}} = \prod_{\delta<\alpha}\aleph_{\alpha+\delta+\beta} = \prod_{\delta<\alpha}\aleph_{\alpha+\beta}\\ &= \prod_{\delta<\alpha} 2^{\aleph_\alpha} = (2^{\aleph_\alpha})^{|\alpha|} = 2^{\aleph_\alpha} = \aleph_{\alpha+\beta}.\end{aligned}$$

Por consiguiente, $\alpha + \alpha + \beta = \alpha + \beta$, y de aquí $\alpha + \beta = \beta$, en contra de la elección de α. ∎

Para continuar nuestro estudio conviene introducir una operación muy relacionada con la exponenciación de cardinales:

Definición 5.68 Si β es un ordinal y A es un conjunto, definimos

$$A^{<\beta} = {}^{<\beta}A = \bigcup_{\alpha<\beta} A^\alpha,$$

es decir, $A^{<\beta}$ es el conjunto de las aplicaciones de un ordinal menor que β en A. Usaremos la segunda notación cuando pueda haber confusión con el cardinal

$$\kappa^{<\mu} = |{}^{<\mu}\kappa|.$$

El teorema siguiente, que generaliza a 5.31, nos da varias caracterizaciones interesantes de esta operación:

Teorema 5.69 *Si μ es infinito y $\kappa \geq 2$, entonces*

$$\kappa^{<\mu} = \sup_{\nu<\mu} \kappa^\nu = \sum_{\nu<\mu} \kappa^\nu,$$

donde ν recorre los cardinales menores que μ (no los ordinales).

DEMOSTRACIÓN: Si μ es un cardinal límite, $\mu = \sup_{\nu<\mu} \nu \leq \sup_{\nu<\mu} \kappa^\nu$.

Si $\mu = \nu^+$ entonces $\nu < \kappa^\nu$, pues si $\nu < \kappa$ es obvio y si $\kappa \leq \nu$ entonces $\nu < 2^\nu = \kappa^\nu$, luego $\nu < \sup_{\nu<\mu} \kappa^\nu$ y así $\mu = \nu^+ \leq \sup_{\nu<\mu} \kappa^\nu$. En cualquier caso

$$\sum_{\nu<\mu} \kappa^\nu = \sup_{\nu<\mu} \kappa^\nu.$$

Por consiguiente

$$\kappa^{<\mu} = \Big|\bigcup_{\alpha<\mu} {}^\alpha\kappa\Big| = \sum_{\alpha<\mu} \kappa^{|\alpha|} \leq \sum_{\alpha<\mu} \sup_{\nu<\mu} \kappa^\nu = \sup_{\nu<\mu} \kappa^\nu.$$

Si $\nu < \mu$, entonces ${}^\nu\kappa \subset {}^{<\mu}\kappa$, luego $\kappa^\nu \leq |{}^{<\mu}\kappa| = \kappa^{<\mu}$. Así pues, tomando el supremo, $\sup_{\nu<\mu} \kappa^\nu \leq \kappa^{<\mu}$ y tenemos la igualdad. ∎

A partir de este teorema es inmediato que si μ es infinito entonces

$$\kappa^{<\mu^+} = \kappa^\mu,$$

luego $\kappa^{<\mu}$ sólo tiene interés cuando μ es un cardinal límite.

Volviendo a la función del continuo, ahora podemos expresar la condición de monotonía como que $2^{<\kappa} \leq 2^\kappa$. El teorema siguiente es un refinamiento de esta relación que para cardinales sucesores es trivial, pero no así para cardinales límite:

Teorema 5.70 *Si κ es un cardinal infinito, entonces $2^\kappa = (2^{<\kappa})^{\mathrm{cf}\,\kappa}$.*

DEMOSTRACIÓN: Sea $\kappa = \sum_{\alpha<\mathrm{cf}\,\kappa} \nu_\alpha$, donde $\bigwedge\alpha < \mathrm{cf}\,\kappa\ \nu_\alpha < \kappa$. Entonces

$$2^\kappa = 2^{\sum_{\alpha<\mathrm{cf}\,\kappa} \nu_\alpha} = \prod_{\alpha<\mathrm{cf}\,\kappa} 2^{\nu_\alpha} \leq \prod_{\alpha<\mathrm{cf}\,\kappa} 2^{<\kappa} = (2^{<\kappa})^{\mathrm{cf}\,\kappa} \leq (2^\kappa)^{\mathrm{cf}\,\kappa} = 2^\kappa.$$

∎

Notemos que si $\kappa = \mu^+$ entonces la igualdad se reduce a $2^{\mu^+} = 2^{\mu^+}$, luego es trivial, tal y como advertíamos, pero para cardinales límite puede no serlo. Por ejemplo, si $\bigwedge n \in \omega\ 2^{\aleph_n} = 2^{\aleph_0}$ (lo cual es consistente), entonces $2^{<\aleph_\omega} = 2^{\aleph_0}$ y necesariamente $2^{\aleph_\omega} = 2^{\aleph_0}$.

Por otra parte, este teorema tampoco es definitivo pues, si tenemos, por ejemplo, $\bigwedge n \in \omega\ 2^{\aleph_n} = \aleph_{\omega+n+1}$, entonces $2^{<\aleph_\omega} = \aleph_{\omega+\omega}$ y sólo concluimos que $2^{\aleph_\omega} = \aleph_{\omega+\omega}^{\aleph_0}$, pero no sabemos qué valores puede tomar esta expresión.

Esto está relacionado con el problema de la relación que hay entre la función del continuo y la exponenciación en general κ^μ (una muestra es el teorema 5.62). Comprenderemos mejor esta relación en la sección siguiente. De momento acabamos ésta con algunos resultados técnicos de interés:

Teorema 5.71 *Si μ es un cardinal regular y $\kappa \geq 2$, entonces $(\kappa^{<\mu})^{<\mu} = \kappa^{<\mu}$.*

Demostración: Si $\mu = \xi^+$ es inmediato, así que podemos suponer que μ es un cardinal límite. Al ser regular, los subconjuntos no acotados en μ tienen cardinal μ. En particular, hay μ cardinales $\nu < \mu$, de donde

$$\mu \leq \sum_{\nu<\mu} \kappa^\nu = \kappa^{<\mu}.$$

Sea $\pi < \mu$. Como μ es regular se cumple que

$$^\pi \sup_{\nu<\mu} \kappa^\nu \subset \bigcup_{\nu<\mu} {}^\pi(\kappa^\nu).$$

En efecto, dada f en el miembro izquierdo, la aplicación $\pi \longrightarrow \mu$ que a cada $\alpha < \pi$ le asigna el mínimo $\nu < \mu$ tal que $f(\alpha) < \kappa^\nu$ no puede ser cofinal, luego ha de existir un $\nu < \mu$ tal que $f[\pi] \subset \kappa^\nu$ y f está en el miembro derecho.

Así pues, tomando cardinales,

$$(\kappa^{<\mu})^\pi \leq \sum_{\nu<\mu} \kappa^{\nu\pi} \leq \sum_{\nu<\mu} \kappa^{<\mu} = \mu\ \kappa^{<\mu} = \kappa^{<\mu}.$$

Tomando el supremo en π obtenemos $(\kappa^{<\mu})^{<\mu} \leq \kappa^{<\mu}$, y la otra desigualdad es obvia. ∎

Definición 5.72 Dado un conjunto A y un cardinal κ, llamaremos

$$\begin{aligned} [A]^\kappa &= \{x \mid x \subset A \wedge |x| = \kappa\}, \\ [A]^{<\kappa} &= \{x \mid x \subset A \wedge |x| < \kappa\}. \end{aligned}$$

La exponenciación cardinal permite calcular los cardinales de estos conjuntos. El teorema siguiente generaliza a 5.32:

Teorema 5.73 *Sea A un conjunto infinito y κ un cardinal $\kappa \leq |A|$, Entonces*

$$|[A]^\kappa| = |A|^\kappa, \qquad |[A]^{<\kappa}| = |A|^{<\kappa}.$$

En particular A tiene $|A|$ subconjuntos finitos.

DEMOSTRACIÓN: Podemos suponer $\kappa > 0$. Sea $\mu = |A| = \kappa\mu = |\kappa \times \mu|$. Para la primera igualdad basta probar que $|[\kappa \times \mu]^\kappa| = \mu^\kappa$, pero es inmediato que ${}^\kappa\mu \subset [\kappa \times \mu]^\kappa$, de donde $\mu^\kappa \leq |[\kappa \times \mu]^\kappa|$ y, por otra parte, para cada $x \in [\kappa \times \mu]^\kappa$ podemos escoger una biyección $f_x : \kappa \longrightarrow x$, de modo que la aplicación $g : [\kappa \times \mu]^\kappa \longrightarrow {}^\kappa(\kappa \times \mu)$ dada por $g(x) = f_x$ es inyectiva, de donde $|[\kappa \times \mu]^\kappa| \leq |{}^\kappa(\kappa \times \mu)| = |\kappa \times \mu|^\kappa = \mu^\kappa$.

Respecto a la segunda igualdad,

$$|[A]^{<\kappa}| = \Big|\bigcup_{\mu<\kappa} [A]^\mu\Big| = \sum_{\mu<\kappa} |[A]^\mu| = \sum_{\mu<\kappa} |A|^\mu = |A|^{<\kappa}.$$

■

En el apéndice A presentamos algunas aplicaciones al álgebra de la aritmética cardinal.

5.6 La hipótesis de los cardinales singulares

La función del continuo más simple posible es, sin duda, la que postula la hipótesis del continuo generalizada:

$$2^\kappa = \kappa^+.$$

Sucede que esta hipótesis determina de hecho toda la exponenciación cardinal. En efecto:

Teorema 5.74 (HCG) *Si κ y μ son cardinales y μ es infinito, entonces*

$$\kappa^\mu = \begin{cases} \kappa & \text{si } \mu < \operatorname{cf}\kappa, \\ \kappa^+ & \text{si } \operatorname{cf}\kappa \leq \mu \leq \kappa, \\ \mu^+ & \text{si } \kappa \leq \mu. \end{cases}$$

DEMOSTRACIÓN: Si $\mu < \operatorname{cf}\kappa$ tenemos la inclusión ${}^\mu\kappa \subset \bigcup_{\alpha<\kappa} {}^\mu\alpha$, de donde $\kappa^\mu \leq \sum_{\alpha<\kappa} |\alpha|^\mu$. Ahora bien, dado $\alpha < \kappa$, se cumple que $\nu = \max\{|\alpha|, \mu\} < \kappa$, luego $|\alpha|^\mu \leq \nu^\nu = \nu^+ \leq \kappa$. Por consiguiente,

$$\kappa \leq \kappa^\mu \leq \sum_{\alpha<\kappa} \kappa = \kappa.$$

Si $\operatorname{cf}\kappa \leq \mu \leq \kappa$ entonces, por el teorema de König,

$$\kappa^+ \leq \kappa^{\operatorname{cf}\kappa} \leq \kappa^\mu \leq \kappa^\kappa = 2^\kappa = \kappa^+.$$

Finalmente, si $\kappa \leq \mu$ entonces $\kappa^\mu = 2^\mu = \mu^+$. ■

En particular es claro que la HCG implica, para $\kappa \geq 2$ y μ un cardinal límite:

$$\kappa^{<\mu} = \begin{cases} \kappa & \text{si } \mu \leq \operatorname{cf}\kappa, \\ \kappa^+ & \text{si } \operatorname{cf}\kappa < \mu \leq \kappa, \\ \mu & \text{si } \kappa < \mu. \end{cases}$$

Ejemplo Suponiendo la HCG tenemos:

$$\aleph_3^{\aleph_5} = \aleph_6, \quad \aleph_7^{\aleph_2} = \aleph_7, \quad \aleph_{\omega_2}^{\aleph_1} = \aleph_{\omega_2}, \quad \aleph_{\omega_6}^{\aleph_8} = \aleph_{\omega_6}^+.$$

■

A la vista de este resultado, es natural conjeturar que la función del continuo determina la exponenciación cardinal. En realidad existía una razón de mucho mayor peso que corroboraba esta conjetura: Durante mucho tiempo, las técnicas conocidas para construir modelos con funciones del continuo alternativas forzaban el resto de la exponenciación, es decir, se sabía cómo construir modelos con cualquier función del continuo sobre los cardinales regulares, pero, una vez determinada ésta, el resto de la exponenciación venía determinada por la construcción, además por un criterio muy simple. Esto podía deberse a que las técnicas conocidas no eran suficientemente generales o bien a un teorema desconocido que hiciese necesarias las restricciones encontradas. Además se conocía el enunciado de este hipotético teorema:

Definición 5.75 Llamaremos *hipótesis de los cardinales singulares* a la sentencia siguiente:

(HCS) *Para todo cardinal singular κ, si $2^{\operatorname{cf}\kappa} < \kappa$, entonces $\kappa^{\operatorname{cf}\kappa} = \kappa^+$.*

Notemos que la condición $2^{\operatorname{cf}\kappa} < \kappa$ ya implica que κ es singular. Lo expresamos explícitamente para enfatizar que la HCS sólo impone una restricción a los cardinales singulares.

Vamos a demostrar que, bajo la hipótesis de los cardinales singulares, la función del continuo sobre los cardinales regulares determina completamente la exponenciación cardinal (en particular la función del continuo sobre los cardinales singulares). En realidad la HCS no es un teorema de NBG, pero —por razones que comentaremos más adelante— es difícil construir modelos donde no se cumpla. En particular, los modelos a los que nos referíamos antes cumplen todos esta hipótesis, y ésta es la razón de que en ellos la exponenciación cardinal esté determinada por la función del continuo. Precisamente por ello, podemos asegurar que la HCS es consistente con cualquier determinación de la función del continuo sobre los cardinales regulares compatible con la monotonía y con el teorema de König. Por otra parte, es inmediato que HCG $\to$ HCS, lo cual explica que la HCG determine la exponenciación cardinal.

Veamos ahora cómo la HCS determina la función del continuo sobre los cardinales singulares.

Ejemplo Supongamos que $\bigwedge\alpha(\aleph_\alpha \text{ regular} \to 2^{\aleph_\alpha} = \aleph_{\alpha+\omega+5})$. Entonces, usando el teorema 5.70 vemos que

$$\begin{aligned} 2^{\aleph_\omega} &= \aleph_{\omega+5}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = \aleph_{\omega+5}, \\ 2^{\aleph_{\omega_1}} &= \aleph_{\omega_1}^{\aleph_1} = \aleph_{\omega_1+1}, \end{aligned}$$

donde en la última igualdad hemos usado la HCS. Vamos a demostrar que la función del continuo en un cardinal singular puede calcularse siempre con uno de estos dos argumentos. ∎

Definición 5.76 Diremos que la función del continuo es *finalmente constante* bajo un cardinal límite κ si existe un $\mu < \kappa$ tal que si $\mu \leq \nu < \kappa$ entonces $2^\nu = 2^\mu$.

En tal caso es obvio que $2^{<\kappa} = 2^\mu$. Notemos además que si la condición se cumple para todo ν regular, entonces se cumple para todo ν, por la monotonía. Así mismo, no perdemos generalidad si suponemos que μ es regular.

Teniendo esto en cuenta, el teorema siguiente nos permite calcular 2^κ para un cardinal singular κ supuesto que sabemos calcular 2^μ para todo cardinal regular $\mu < \kappa$. Más aún, lo que probamos es que la HCS implica que 2^κ toma siempre el mínimo valor posible:

Teorema 5.77 *Sea κ un cardinal singular.*

1. *Si la función del continuo es finalmente constante bajo κ, entonces*
$$2^\kappa = 2^{<\kappa}.$$
2. *En caso contrario $2^\kappa \geq (2^{<\kappa})^+$ y si suponemos la* HCS *tenemos la igualdad.*

Demostración: En el caso 1), sea $\mu < \kappa$ tal que si $\mu \leq \nu < \kappa$ entonces $2^\nu = 2^\mu$. Así, $2^{<\kappa} = 2^\mu$ y, por 5.70, tenemos que $2^\kappa = (2^\mu)^{\operatorname{cf}\kappa} = 2^{\mu\operatorname{cf}\kappa} = 2^\mu$.

En el caso 2), para todo cardinal $\mu < \kappa$ se cumple que $2^\mu < 2^{<\kappa}$. Por consiguiente, la aplicación $\kappa \longrightarrow 2^{<\kappa}$ dada por $\alpha \mapsto 2^{|\alpha|}$ es cofinal y creciente, luego el teorema 5.50 nos da que $\operatorname{cf} 2^{<\kappa} = \operatorname{cf}\kappa < \kappa$.

Por otra parte, por el teorema de König, $\operatorname{cf} 2^\kappa > \kappa$, luego $2^\kappa \neq 2^{<\kappa}$ y, como la desigualdad $2^{<\kappa} \leq 2^\kappa$ es obvia, tenemos en realidad que $(2^{<\kappa})^+ \leq 2^\kappa$.

Respecto a la otra desigualdad, tenemos que $2^{\operatorname{cf} 2^{<\kappa}} = 2^{\operatorname{cf}\kappa} < 2^{<\kappa}$, luego podemos aplicar la HCS a $2^{<\kappa}$, lo cual nos da que $(2^{<\kappa})^{\operatorname{cf} 2^{<\kappa}} = (2^{<\kappa})^+$, es decir, $2^\kappa = (2^{<\kappa})^{\operatorname{cf}\kappa} = (2^{<\kappa})^+$. ∎

Veamos ahora que la HCS determina toda la exponenciación cardinal a partir de la función del continuo:

Teorema 5.78 (HCS) *Sean κ y μ cardinales infinitos. Entonces*

$$\kappa^\mu = \begin{cases} \kappa & \text{si } 2^\mu < \kappa \wedge \mu < \operatorname{cf}\kappa, \\ \kappa^+ & \text{si } 2^\mu < \kappa \wedge \operatorname{cf}\kappa \leq \mu, \\ 2^\mu & \text{si } \kappa \leq 2^\mu. \end{cases}$$

DEMOSTRACIÓN: Si $\kappa \leq 2^\mu$, entonces $2^\mu \leq \kappa^\mu \leq (2^\mu)^\mu = 2^\mu$.

Observemos que en esta parte no hemos usado la HCS, así como tampoco hace falta para concluir que $\kappa \leq \kappa^\mu$ y que si $\operatorname{cf}\kappa \leq \mu$ entonces $\kappa^+ \leq \kappa^{\operatorname{cf}\kappa} \leq \kappa^\mu$. Así pues, lo que vamos a probar con la ayuda de la HCS es que κ^μ toma siempre el mínimo valor posible.

El caso $2^\mu < \kappa$ lo probamos por inducción sobre κ, es decir, lo suponemos cierto para todos los cardinales menores que κ.

Si $\kappa = \nu^+$, entonces $\mu < 2^\mu < \kappa = \operatorname{cf}\kappa$. Por lo tanto hemos de probar que $\kappa^\mu = \kappa$.

Tenemos que $2^\mu \leq \nu$. Si es $2^\mu < \nu$, entonces por hipótesis de inducción tenemos que $\nu^\mu = \nu$ o bien $\nu^\mu = \nu^+$, y en cualquier caso $\nu^\mu \leq \kappa$. Si, por el contrario, $2^\mu = \nu$ entonces $\nu^\mu = 2^\mu < \kappa$.

Por consiguiente podemos afirmar que $\nu^\mu \leq \kappa$. Por la fórmula de Hausdorff

$$\kappa^\mu = (\nu^+)^\mu = \nu^\mu\nu^+ = \nu^\mu\kappa = \kappa.$$

Consideramos ahora el caso en que κ es un cardinal límite. Si $\nu < \kappa$, por hipótesis de inducción tenemos que ν^μ es ν, ν^+ o 2^μ, pero en cualquier caso $\nu^\mu < \kappa$ (si ν es finito no podemos aplicar la hipótesis de inducción, pero $\nu^\mu = 2^\mu$).

Si $\mu < \operatorname{cf}\kappa$, entonces

$$\kappa \leq \kappa^\mu = |{}^\mu\kappa| \leq \Big|\bigcup_{\alpha<\kappa} {}^\mu\alpha\Big| = \sum_{\alpha<\kappa} |\alpha|^\mu \leq \sum_{\alpha<\kappa} \kappa = \kappa.$$

Por lo tanto $\kappa^\mu = \kappa$.

Si $\operatorname{cf}\kappa \leq \mu$, expresemos $\kappa = \sum_{\alpha<\operatorname{cf}\kappa} \nu_\alpha$, donde $\nu_\alpha < \kappa$. Entonces

$$\kappa^\mu = \Big(\sum_{\alpha<\operatorname{cf}\kappa} \nu_\alpha\Big)^\mu \leq \Big(\prod_{\alpha<\operatorname{cf}\kappa} \nu_\alpha\Big)^\mu = \prod_{\alpha<\operatorname{cf}\kappa} \nu_\alpha^\mu \leq \prod_{\alpha<\operatorname{cf}\kappa} \kappa = \kappa^{\operatorname{cf}\kappa} \leq \kappa^\mu,$$

luego $\kappa^\mu = \kappa^{\operatorname{cf}\kappa}$. Como $2^{\operatorname{cf}\kappa} \leq 2^\mu < \kappa$, la HCS nos da que $\kappa^{\operatorname{cf}\kappa} = \kappa^+$ y tenemos la conclusión. ∎

Ejemplo Si suponemos la HCS y que

$$\bigwedge\alpha(\aleph_\alpha \text{ regular } \to 2^{\aleph_\alpha} = \aleph_{\alpha+\omega+5}),$$

entonces

$$\aleph_5^{\aleph_3} = \aleph_{\omega+5}, \quad \aleph_{\omega_1}^{\aleph_3} = \aleph_{\omega_1+1}, \quad \aleph_{\omega_1+4}^{\aleph_3} = \aleph_{\omega_1+4}.$$

∎

Así pues, la exponenciación cardinal bajo la HCS no está determinada (pues la función del continuo sobre los cardinales regulares puede ser cualquiera que

no contradiga a la monotonía ni al teorema de König) pero sí que está completamente comprendida, en cuanto que sabemos exactamente cómo depende de la función del continuo. El problema es que la HCS no es un teorema de NBG, y lo que no está claro en absoluto es lo que se puede decir exclusivamente en NBG sobre la exponenciación cardinal o sobre la función del continuo sobre los cardinales singulares. Si no suponemos la HCS sólo conocemos hechos aislados, algunos sencillos y otros muy profundos. Veamos un ejemplo de los sencillos:

Teorema 5.79 *Si* $2^{\aleph_1} < \aleph_\omega$ *y* $\aleph_\omega^{\aleph_0} \geq \aleph_{\omega_1}$*, entonces* $\aleph_\omega^{\aleph_0} = \aleph_{\omega_1}^{\aleph_1}$.

Demostración: Aplicamos la fórmula de Hausdorff:

$$\aleph_\omega^{\aleph_0} \leq \aleph_{\omega_1}^{\aleph_1} \leq (\aleph_\omega^{\aleph_0})^{\aleph_1} = \aleph_\omega^{\aleph_1} = \Big(\sum_{n\geq 1} \aleph_n\Big)^{\aleph_1} \leq \Big(\prod_{n\geq 1} \aleph_n\Big)^{\aleph_1}$$

$$= \prod_{n\geq 1} \aleph_n^{\aleph_1} = \prod_{n\geq 1} 2^{\aleph_1}\aleph_n = 2^{\aleph_1}\aleph_\omega^{\aleph_0} = \aleph_\omega^{\aleph_0}.$$

■

Consideremos ahora el valor de $\aleph_\omega^{\aleph_1}$. Se trata de un cardinal que queda invariante al elevarlo a $\aleph_0$, luego el teorema de König nos da que ha de tener cofinalidad no numerable. Por su parte, la monotonía exige que sea mayor que el propio $\aleph_\omega$. Así pues, estas condiciones generales no excluyen la posibilidad de que $\aleph_\omega^{\aleph_0} = \aleph_{\omega_1}$. Más aún, si suponemos que $2^{\aleph_0} = \aleph_{\omega_1}$ (lo cual es consistente) entonces

$$\aleph_{\omega_1} = 2^{\aleph_0} \leq \aleph_\omega^{\aleph_0} \leq \aleph_{\omega_1}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0} = \aleph_{\omega_1},$$

con lo que, de hecho, $\aleph_\omega^{\aleph_0} = \aleph_{\omega_1}$.

Sin embargo, si suponemos que $2^{\aleph_1} < \aleph_\omega$ (lo cual es consistente), la HCS implica que $\aleph_\omega^{\aleph_0} = \aleph_{\omega+1}$, pero sin ella aún podemos asegurar que $\aleph_\omega^{\aleph_0} \neq \aleph_{\omega_1}$, ya que en caso contrario el teorema anterior nos daría $\aleph_{\omega_1}^{\aleph_1} = \aleph_{\omega_1}$, en contradicción con el teorema de König.

Así pues, nos encontramos con una restricción en ZFC al valor que puede tomar $\aleph_\omega^{\aleph_0}$ distinta de las que imponen la monotonía y el teorema de König. Una restricción que, además, depende de forma no trivial de los valores de $2^{\aleph_0}$ y $2^{\aleph_1}$. Si queremos un ejemplo en términos de la función del continuo podemos suponer que $\bigwedge n < \omega\ 2^{\aleph_n} < \aleph_\omega$, en cuyo caso tenemos que $2^{\aleph_\omega} = \aleph_\omega^{\aleph_0} \neq \aleph_{\omega_1}$.

Los resultados básicos sobre la exponenciación de cardinales fueron establecidos por Hausdorff y Tarski. Éste último probó un caso particular del teorema 5.41 y conjeturó que si $\{\kappa_\alpha\}_{\alpha<\lambda}$ es una sucesión estrictamente creciente de cardinales ≥ 2 y $\kappa = \sup_{\alpha<\lambda} \kappa_\alpha$, entonces

$$\prod_{\alpha<\lambda} \kappa_\alpha = \kappa^{|\lambda|}.$$

Observemos que la restricción de que λ sea un ordinal límite es necesaria. Por ejemplo, si tomáramos $\lambda = \omega_1 + 1$ y la sucesión $\{\aleph_\alpha\}_{\alpha<\omega_1} \cup \{\aleph_{\omega_1\cdot 2}\}$ (con lo que $\kappa = \aleph_{\omega_1\cdot 2}$), suponiendo la HCG y aplicando 5.41 obtenemos que

$$\prod_{\alpha<\omega_1} \aleph_\alpha \cdot \aleph_{\omega_1\cdot 2} = \aleph_{\omega_1}^{\aleph_1} \cdot \aleph_{\omega_1\cdot 2} = \aleph_{\omega_1+1} \cdot \aleph_{\omega_1\cdot 2} = \aleph_{\omega_1\cdot 2} < \aleph_{\omega_1\cdot 2+1} = \aleph_{\omega_1\cdot 2}^{\aleph_1}.$$

Más en general, es necesario exigir que $\kappa_\alpha < \kappa$ para todo α. Un contraejemplo sin esta hipótesis (siempre bajo la HCG) sería $\lambda = \omega_1 + \omega$ y

$$\kappa_\alpha = \begin{cases} \aleph_\alpha & \text{si } \alpha < \omega_1, \\ \aleph_{\omega_1\cdot 2} & \text{si } \alpha = \omega_1 + n. \end{cases}$$

En tal caso $\kappa = \aleph_{\omega_1\cdot 2}$ y el producto sigue valiendo $\aleph_{\omega_1\cdot 2}^{\aleph_0} = \aleph_{\omega_1\cdot 2} < \kappa^{\aleph_1}$. Por otra parte la HCS implica la conjetura de Tarski:

Teorema 5.80 (HCS) *Sea λ un ordinal límite y $\{\kappa_\alpha\}_{\alpha<\lambda}$ una sucesión creciente (no exigimos que lo sea estrictamente) de cardinales ≥ 2. Sea $\kappa = \sup\limits_{\alpha<\lambda} \kappa_\alpha$ y supongamos que $\bigwedge \alpha < \lambda\ \kappa_\alpha < \kappa$. Entonces*

$$\prod_{\alpha<\lambda} \kappa_\alpha = \kappa^{|\lambda|}.$$

Demostración: La desigualdad $\leq$ es inmediata por la monotonía de los productos. Si $\kappa \leq 2^{|\lambda|}$ entonces, por el teorema 5.78,

$$\kappa^{|\lambda|} = 2^{|\lambda|} = \prod_{\alpha<\lambda} 2 \leq \prod_{\alpha<\lambda} \kappa_\alpha \leq \kappa^{|\lambda|}.$$

Si $|\lambda| < 2^{|\lambda|} < \kappa$, tomemos una sucesión de ordinales $\{\alpha_\delta\}_{\delta<\operatorname{cf}\lambda}$ cofinal creciente en λ. Entonces

$$\kappa^{|\lambda|} = \Big(\sum_{\delta<\operatorname{cf}\lambda} \kappa_{\alpha_\delta}\Big)^{|\lambda|} \leq \prod_{\delta<\operatorname{cf}\lambda} \kappa_{\alpha_\delta}^{|\lambda|} \leq \prod_{\delta<\operatorname{cf}\lambda} \kappa = \kappa^{\operatorname{cf}\lambda} = \prod_{\delta<\operatorname{cf}\lambda} \kappa_{\alpha_\delta} \leq \prod_{\alpha<\lambda} \kappa_\alpha.$$

Hemos usado que $\kappa_{\alpha_\delta}^{|\lambda|} < \kappa$ por el teorema 5.78. ∎

Nota Puede probarse —aunque es muy complicado— que es consistente que $\aleph_{\omega_1\cdot 2}$ sea un límite fuerte, $\aleph_{\omega_1}^{\aleph_1} = \aleph_{\omega_1\cdot 2+\omega+2}$ y $\aleph_{\omega_1\cdot 2+\omega}^{\aleph_0} = \aleph_{\omega_1\cdot 2+\omega+1}$. En estas condiciones tenemos un contraejemplo a la conjetura de Tarski. Basta tomar $\lambda = \omega_1 + \omega$ y

$$\kappa_\alpha = \begin{cases} \aleph_\alpha & \text{si } \alpha < \omega_1, \\ \aleph_{\omega_1\cdot 2+n} & \text{si } \alpha = \omega_1 + n. \end{cases}$$

En efecto, el producto da

$$\aleph_{\omega_1}^{\aleph_1} \cdot \aleph_{\omega_1\cdot 2+\omega}^{\aleph_0} \leq 2^{\aleph_{\omega_1}} \aleph_{\omega_1\cdot 2+\omega+1} = \aleph_{\omega_1\cdot 2+\omega+1} < \aleph_{\omega_1\cdot 2+\omega}^{|\omega_1+\omega|}.$$

∎

5.7 Cardinales fuertemente inaccesibles

Vamos a estudiar ahora una versión fuerte de los cardinales inaccesibles que introdujimos en el capítulo anterior.

Definición 5.81 Un cardinal infinito κ es un *límite fuerte* si para todo cardinal $\mu < \kappa$ se cumple $2^\mu < \kappa$.

Es claro que un cardinal límite fuerte es en particular un cardinal límite, ya que si fuera $\kappa = \mu^+$, entonces tendría que ser $2^\mu < \mu^+$, lo cual es imposible. Obviamente $\aleph_0$ es un cardinal límite fuerte.

Un cardinal *(fuertemente) inaccesible* es un cardinal límite fuerte regular distinto de $\aleph_0$.

En particular, todo cardinal fuertemente inaccesible es débilmente inaccesible, aunque el recíproco no es necesariamente cierto. En el capítulo anterior señalamos que no es posible demostrar la existencia de cardinales débilmente inaccesibles, luego lo mismo vale para los cardinales fuertemente inaccesibles.

Nota Cuando hablemos de cardinales inaccesibles habrá que entender que son fuertemente inaccesibles.

Conviene observar que bajo la HCG todos los cardinales límite son límites fuertes y, en particular, los cardinales débilmente inaccesibles coinciden con los fuertemente inaccesibles.

También es claro que si κ es un límite fuerte, entonces $2^{<\kappa} = \kappa$. Más aún, si $\mu, \nu < \kappa$, entonces $\mu^\nu < \kappa$, pues si $\xi < \kappa$ es el máximo de μ y ν, tenemos que $\mu^\nu \leq \xi^\xi = 2^\xi < \kappa$. Si κ es fuertemente inaccesible podemos decir más:

Teorema 5.82 *Si κ es un cardinal fuertemente inaccesible entonces $\kappa^{<\kappa} = \kappa$.*

Demostración: Basta probar que $\kappa^\mu \leq \kappa$ para todo $\mu < \kappa$. En efecto, como κ es regular ${}^\mu\kappa = \bigcup_{\alpha<\kappa} {}^\mu\alpha$ luego

$$\kappa^\mu \leq \sum_{\alpha<\kappa} |\alpha|^\mu \leq \sum_{\alpha<\kappa} \kappa = \kappa.$$

■

Del mismo modo que los cardinales límite pueden caracterizarse como los de la forma $\aleph_0$ o $\aleph_\lambda$, existe una caracterización similar para los cardinales límite fuerte, en términos de la llamada función bet.[5]

Definición 5.83 Definimos $\beth : \Omega \longrightarrow K$ (función bet) como la única función que cumple:

$$\beth_0 = \aleph_0 \quad \wedge \quad \bigwedge\alpha\, \beth_{\alpha+1} = 2^{\beth_\alpha} \quad \wedge \quad \bigwedge\lambda\, \beth_\lambda = \bigcup_{\delta<\lambda} \beth_\delta.$$

Teniendo en cuenta que el supremo de un conjunto de cardinales es un cardinal, una simple inducción prueba que $\beth$ toma todos sus valores en K. Obviamente es una función normal.

Ejercicio: La HCG es equivalente a que $\beth = \aleph$.

La caracterización a la que nos referíamos es:

[5] Bet ($\beth$) es la segunda letra del alfabeto hebreo.

Teorema 5.84 *Los cardinales límite fuerte son exactamente los de la forma* $\beth_0$ *o* $\beth_\lambda$.

DEMOSTRACIÓN: Se cumple que $\beth_\lambda$ es un límite fuerte, pues si $\kappa < \beth_\lambda$ entonces existe un $\delta < \lambda$ tal que $\kappa < \beth_\delta$, luego

$$2^\kappa \leq 2^{\beth_\delta} = \beth_{\delta+1} < \beth_{\delta+2} \leq \beth_\lambda.$$

Recíprocamente, si κ es un límite fuerte, entonces $\kappa \leq \beth_\kappa < \beth_{\kappa+1}$, luego podemos tomar el mínimo ordinal α tal que $\kappa < \beth_\alpha$. Ciertamente α no puede ser 0 ni un cardinal límite, luego $\alpha = \gamma + 1$ y, por consiguiente,

$$\beth_\gamma \leq \kappa < \beth_{\gamma+1} = 2^{\beth_\gamma}.$$

Si la primera desigualdad fuera estricta κ no sería un límite fuerte, luego $\kappa = \beth_\gamma$. Falta probar que γ no puede ser de la forma $\delta + 1$, pero es que en tal caso sería $\beth_\delta < \kappa$ y $2^{\beth_\delta} = \kappa$, y de nuevo κ no sería un límite fuerte. Por consiguiente $\gamma = 0$ o bien es un ordinal límite. ∎

La prueba del teorema siguiente es idéntica a la de su análogo 5.60:

Teorema 5.85 *Un cardinal regular* κ *es fuertemente inaccesible si y sólo si* $\kappa = \beth_\kappa$.

Es claro que V_ω es una unión numerable de conjuntos finitos, luego su cardinal es $|\mathrm{V}_\omega| = \aleph_0 = \beth_0$. A partir de aquí, una simple inducción nos da el teorema siguiente:

Teorema 5.86 $\bigwedge\alpha\ |\mathrm{V}_{\omega+\alpha}| = \beth_\alpha$. *En particular,* $\bigwedge\alpha(\omega^2 \leq \alpha \to |\mathrm{V}_\alpha| = \beth_\alpha)$.

(Recordemos que si $\omega^2 \leq \alpha$ entonces $\alpha = \omega^2 + \beta$ y $\omega + \alpha = \omega + \omega^2 + \beta = \omega(1 + \omega) + \beta = \omega^2 + \beta = \alpha$.)

De este modo, si κ es fuertemente inaccesible tenemos que $|\mathrm{V}_\kappa| = \kappa$. Más aún:

Teorema 5.87 *Si* κ *es un cardinal fuertemente inaccesible se cumple que*

$$\bigwedge x(x \in V_\kappa \leftrightarrow x \subset V_\kappa \wedge |x| < \kappa).$$

DEMOSTRACIÓN: Si $x \in \mathrm{V}_\kappa$, entonces $x \in \mathrm{V}_\delta$, para cierto $\delta < \kappa$ (podemos suponer $\omega^2 \leq \delta$), luego $x \subset \mathrm{V}_\delta$ y $|x| \leq |\mathrm{V}_\delta| = \beth_\delta < \beth_\kappa = \kappa$. Además $x \subset V_\kappa$ porque V_κ es transitivo.

Recíprocamente, si $x \subset V_\kappa$ y $|x| < \kappa$, entonces el conjunto

$$A = \{\operatorname{rang} y \mid y \in x\} \subset \kappa$$

es imagen de x, luego tiene cardinal menor que κ y, como κ es regular, A está acotado. Si $\delta < \kappa$ es una cota concluimos que $x \subset V_\delta$, luego $x \in V_{\delta+1} \subset V_\kappa$. ∎

Nota La razón por la que no puede demostrarse la existencia de cardinales inaccesibles es similar a la razón por la que no puede demostrarse la existencia de conjuntos no regulares: imaginemos que existe un cardinal inaccesible κ. Entonces, todas las operaciones conjuntistas, cuando se aplican a conjuntos de V_κ, dan lugar a conjuntos de V_κ, por lo que no es posible construir un conjunto de cardinal κ. Si decidimos llamar "conjuntos" exclusivamente a los conjuntos de V_κ (y llamamos "clases" a los subconjuntos de V_κ), con ello no perdemos ninguno de los conjuntos que sabemos construir, y todos los axiomas de NBG siguen cumpliéndose igualmente (más aún, se cumplen los axiomas de MK, sin la restricción de normalidad en el axioma de comprensión), pero ahora (si κ era el mínimo cardinal inaccesible) ya no hay cardinales inaccesibles.

En suma, no es posible demostrar la existencia de cardinales inaccesibles porque éstos no son necesarios para que se cumplan los axiomas de la teoría de conjuntos. En realidad la razón es la misma por la que no puede demostrarse el axioma de infinitud a partir de los axiomas restantes: todas las construcciones conjuntistas, cuando se aplican a conjuntos finitos, dan conjuntos finitos. La única razón por la que $\aleph_0$ no es un cardinal inaccesible es porque lo hemos excluido en la definición, pero en el fondo $\aleph_0$ es el menor cardinal inaccesible. Del mismo modo que sin el axioma de infinitud no podemos decidir si $\omega = \Omega$ o bien $\omega \in \Omega$ (y en el segundo caso ω pasa a ser el menor cardinal infinito), podemos definir

$$\Omega_1 = \{\alpha \in \Omega \mid \bigwedge \delta \leq \alpha \ \delta \text{ no es inaccesible}\},$$

y así Ω_1 es una clase tal que en NBG no puede decidirse si $\Omega_1 = \Omega$ o bien $\Omega_1 \in \Omega$, y en el segundo caso Ω_1 pasa a ser el menor cardinal inaccesible.

En cuanto postulamos la existencia de un cardinal infinito (ω) tenemos automáticamente la existencia de muchos cardinales infinitos ($\aleph_1$, $\aleph_2$, ...), pero no la existencia de un cardinal inaccesible. Similarmente, la existencia de un cardinal inaccesible no implica la existencia de un segundo, pues si existen dos (mínimos) cardinales inaccesibles $\kappa < \mu$, si restringimos el alcance de la palabra "conjunto" a los conjuntos de V_μ, se siguen cumpliendo los axiomas de la teoría de conjuntos, pero ahora sólo hay un cardinal inaccesible, puesto que μ ha quedado excluido. Equivalentemente: las operaciones conjuntistas aplicadas a conjuntos de V_μ sólo producen conjuntos de V_μ, luego no dan lugar nunca a conjuntos de cardinal μ.

Por ello, aunque añadamos como axioma a NBG que $\Omega_1 \in \Omega$ (que es una "repetición" del axioma de infinitud a otro nivel), podemos definir

$$\Omega_2 = \{\alpha \in \Omega \mid \bigwedge \delta \leq \alpha(\delta \text{ es inaccesible} \to \delta = \Omega_1)\}$$

y de nuevo tenemos que es imposible decidir si $\Omega_2 = \Omega$ o bien $\Omega_2 \in \Omega$, y en el segundo caso Ω_2 es el segundo cardinal inaccesible.

Estos argumentos (algo mejor formalizados) nos permiten concluir que si NBG es consistente, también es consistente añadir como axioma que no existen cardinales inaccesibles (pues, como hemos dicho, tales cardinales son siempre prescindibles). En cambio, un argumento estándar relacionado con el segundo

teorema de incompletitud de Gödel nos da que es imposible demostrar la consistencia de que existan cardinales inaccesibles, es decir, que NBG + $\Omega_1 \in \Omega$ puede ser consistente, pero si lo es, no puede demostrarse que así es, ni siquiera aceptando como hipótesis la consistencia de NBG. Similarmente, aun suponiendo que NBG + $\Omega_1 \in \Omega$ sea consistente, ello no permite demostrar la consistencia de NBG + $\Omega_1 \in \Omega$ + $\Omega_2 \in \Omega$, y así sucesivamente.

Esto permite extender este tipo de razonamientos a los cardinales débilmente inaccesibles, pues, aunque un cardinal débilmente inaccesible no tiene por qué ser fuertemente inaccesible, puede probarse que si es consistente NBG+ "existe un cardinal débilmente inaccesible", también lo es NBG + "existe un cardinal fuertemente inaccesible", luego la consistencia de NBG + "existe un cardinal débilmente inaccesible" no puede ser demostrada, y mucho menos la existencia de tales cardinales (es decir, que si no podemos demostrar que es consistente suponer que existen, mucho menos podemos demostrar que existen).

A su vez, todo esto está relacionado con la hipótesis de los cardinales singulares, pues a partir de ¬HCS puede probarse la consistencia de que existan infinitos cardinales inaccesibles, y ésa es en el fondo la razón de que no pueda demostrarse la HCS en NBG. ∎

Terminamos la sección con una aplicación de la función $\beth$ que no tiene nada que ver con cardinales inaccesibles. El *axioma de elección de Gödel* es la sentencia[6]

(AEG) $\quad \bigvee F(F : \mathrm{V} \longrightarrow \mathrm{V} \wedge \bigwedge x(x \neq \varnothing \to F(x) \in X))$.

El axioma de elección de Gödel postula la existencia de una función de elección sobre la clase universal, por lo que implica trivialmente el axioma de elección de Zermelo, que sólo postula la existencia de una función de elección (distinta) para cada conjunto.

Teorema 5.88 (AEG) *Todas las clases propias son equipotentes.*

Demostración: Basta observar que podemos descomponer V y Ω en respectivas clases de conjuntos disjuntos como sigue:

$$\mathrm{V} = \mathrm{V}_\omega \cup \bigcup_{\alpha\in\Omega} (\mathrm{V}_{\omega+\alpha+1} \setminus \mathrm{V}_{\omega+\alpha}), \qquad \Omega = \beth_0 \cup \bigcup_{\alpha\in\Omega} (\beth_{\alpha+1} \setminus \beth_\alpha).$$

Teniendo en cuenta el teorema 5.86 y la aritmética cardinal básica es claro que

$$|\mathrm{V}_{\omega+\alpha+1} \setminus \mathrm{V}_{\omega+\alpha}| = \beth_{\alpha+1} = |\beth_{\alpha+1} \setminus \beth_\alpha|.$$

El axioma de elección de Gödel nos permite elegir funciones

$$f_\alpha : \mathrm{V}_{\omega+\alpha+1} \setminus \mathrm{V}_{\omega+\alpha} \longrightarrow \beth_{\alpha+1} \setminus \beth_\alpha \text{ biyectivas.}$$

[6]Este axioma involucra esencialmente clases propias, luego no puede ser considerado como sentencia de ZFC, es decir, de la teoría de conjuntos en la que sólo existen conjuntos y no clases propias. Sólo tiene sentido como extensión de NBG. Para incorporarlo a ZF es necesario extender el lenguaje formal con un funtor F que represente la función de elección o con un relator que represente un buen orden sobre la clase universal.

Por otra parte es claro que podemos tomar $f^* : V_\omega \longrightarrow \beth_0$ biyectiva. Con todas estas funciones podemos construir

$$F = f^* \cup \bigcup_{\alpha\in\Omega} f_\alpha : \mathrm{V} \longrightarrow \Omega \text{ biyectiva.}$$

Así, si A es cualquier clase propia, $F[A]$ es una subclase de Ω, es decir, una clase bien ordenada por una relación conjuntista. Por el teorema 3.27 concluimos que $F[A]$ es semejante a Ω (y A es equipotente a $F[A]$), luego toda clase propia es equipotente a Ω. ∎

Observemos que el axioma de regularidad —al contrario de lo que suele suceder— desempeña un papel crucial en la prueba anterior. En estas condiciones tenemos una nueva caracterización de las clases propias: una clase es propia si y sólo si su tamaño es comparable al de la clase universal.

5.8 Aplicaciones sobre el axioma de elección

Terminamos este capítulo con dos aplicaciones de la aritmética cardinal relacionadas con el axioma de elección. La primera es un hecho sorprendente: La hipótesis del continuo generalizada implica el axioma de elección. Esto fue anunciado por Hausdorff, si bien la primera prueba publicada fue de Sierpiński. La demostración que veremos aquí es posterior. Necesitamos algunos resultados previos.

En primer lugar, sin el axioma de elección hemos probado que, para todo ordinal infinito α, se cumple $|\alpha\times\alpha| = |\alpha|$. Ahora necesitamos construir, también sin el axioma de elección,[7] una aplicación que a cada ordinal infinito α le asigne una biyección $f_\alpha : \alpha \times \alpha \longrightarrow \alpha$. Por ejemplo, la prueba de 5.21 muestra que si α es un cardinal entonces $\alpha \times \alpha$ con el orden canónico es semejante a α, luego si nos bastara trabajar con cardinales podríamos definir f_α como la única semejanza entre $\alpha \times \alpha$ y α. El problema es que necesitamos esto para cualquier ordinal $\alpha \geq \omega$. Resolveremos esto en varios pasos.

1. *Para cada par de ordinales α y β, podemos definir explícitamente una biyección $f_{\alpha,\beta} : \alpha + \beta \longrightarrow \beta + \alpha$.*

   Llamamos $g_{\alpha,\beta} : \alpha + \beta \longrightarrow \alpha \times \{0\} \cup \beta \times \{1\}$ a la única semejanza entre ambos conjuntos cuando en el segundo consideramos el orden lexicográfico. Por otra parte podemos considerar la biyección

   $$h_{\alpha,\beta} : \alpha \times \{0\} \cup \beta \times \{1\} \longrightarrow \beta \times \{0\} \cup \alpha \times \{1\}$$

   dada por $h_{\alpha,\beta}(\delta, n) = (\delta, 1 - n)$. Basta tomar $f_{\alpha,\beta} = g_{\alpha,\beta} \circ h_{\alpha,\beta} \circ g^{-1}_{\beta,\alpha}$.

[7] El lector que conozca la clase L de los conjuntos constructibles tiene una alternativa más sencilla a toda la construcción que sigue: basta definir f_α como el mínimo $f \in L$ (respecto del buen orden constructible) tal que $f : \alpha \times \alpha \longrightarrow \alpha$ biyectiva.

2. *Para cada sucesión de ordinales $\eta = \{\eta_i\}_{i<n+1}$ podemos definir una biyección*

$$g_\eta : \omega^{\eta_0} + \cdots + \omega^{\eta_n} \longrightarrow \omega^{\eta_n} + \cdots + \omega^{\eta_0}.$$

En efecto, para ello definimos recurrentemente biyecciones

$$g_\eta^i : \omega^{\eta_0} + \cdots + \omega^{\eta_i} \longrightarrow \omega^{\eta_i} + \cdots + \omega^{\eta_0}.$$

Tomamos como g_η^0 la identidad en ω^{η_0} y, supuesta definida g_η^i, con $i < n$, definimos

$$h_\eta^i : (\omega^{\eta_0} + \cdots + \omega^{\eta_i}) + \omega^{\eta_{i+1}} \longrightarrow (\omega^{\eta_i} + \cdots + \omega^{\eta_0}) + \omega^{\eta_{i+1}}$$

mediante

$$h_\eta^i(\alpha) = \begin{cases} h_\eta^i(\alpha) & \text{si } \alpha < \omega^{\eta_0} + \cdots + \omega^{\eta_i}, \\ (\omega^{\eta_i} + \cdots + \omega^{\eta_0}) + \delta & \text{si } \alpha = (\omega^{\eta_0} + \cdots + \omega^{\eta_i}) + \delta. \end{cases}$$

Y entonces definimos $g_\eta^{i+1} = h_\eta^i \circ f_{\omega^{\eta_0}+\cdots+\omega^{\eta_i},\omega^{\eta_{i+1}}}$. De este modo, basta tomar $g_\eta = g_\eta^{n+1}$.

3. *Si $\alpha = \omega^{\eta_0}k_0 + \cdots + \omega^{\eta_n}k_n$ es la forma normal de Cantor del ordinal α, podemos definir una biyección $c_\alpha^* : \alpha \longrightarrow \omega^{\eta_0}k_0$.*

En efecto, llamamos $\eta'_\alpha = \{\eta'_i\}_{i<m}$ a la única sucesión decreciente de ordinales tal que $\alpha = \omega^{\eta'_0} + \cdots + \omega^{\eta'_m}$ (donde cada ordinal η_i se repite k_i veces). Basta considerar

$$c_\alpha^* = g_{\eta'_\alpha} : \omega^{\eta'_0} + \cdots + \omega^{\eta'_m} \longrightarrow \omega^{\eta'_m} + \cdots + \omega^{\eta'_0},$$

pues por 3.49 todos los sumandos de la última suma se cancelan excepto los que son iguales a η_0, que son los k_0 últimos, luego la última suma es $\omega^{\eta_0}k_0$.

4. *En las condiciones del apartado anterior, si $\alpha \geq \omega$ (con lo que $\eta_0 > 0$) podemos definir una biyección $c_\alpha : \alpha \longrightarrow \omega^{\eta_0}$.*

En efecto, razonando como en el apartado a), pero para el producto en lugar de la suma, podemos definir una biyección $\omega^{\eta_0}k_0 \longrightarrow k_0\omega^{\eta_0} = \omega^{\eta_0}$, y sólo tenemos que componerla con la c_α^* del apartado anterior.

Así pues, si llamamos η_α al exponente director de la forma normal de α, tenemos una biyección $c_\alpha : \alpha \longrightarrow \omega^{\eta_\alpha}$.

5. *Para todo ordinal α se cumple que $\eta_\alpha = \eta_{\alpha+\alpha}$.*

En efecto, $\alpha + \alpha = \alpha \cdot 2$, por lo que la forma normal de $\alpha + \alpha$ se diferencia de la de α en que sus coeficientes están multiplicados por 2 (pero los exponentes son idénticos).

6. *Para cada $\alpha \geq \omega$, podemos definir una biyección $s_\alpha : \alpha \longrightarrow \alpha + \alpha$.*

   Basta tomar $s_\alpha = c_\alpha \circ c_{\alpha+\alpha}^{-1}$, teniendo en cuenta que $\omega^{\eta_\alpha} = \omega^{\eta_{\alpha+\alpha}}$.

7. *Podemos definir una biyección $e_\eta : \omega^\eta \longrightarrow \omega^{\eta+\eta}$.*

   Si η es infinito podemos considerar las semejanzas $u_\eta : \omega^\eta \longrightarrow \omega^{(\eta)}$ y $u_{\eta+\eta} : \omega^{\eta+\eta} \longrightarrow \omega^{(\eta+\eta)}$ dadas por el teorema 3.47. Por otra parte, la aplicación $v_\eta : \omega^{(\eta+\eta)} \longrightarrow \omega^{(\eta)}$ dada por $v_\eta(s) = s_\eta \circ s$ es claramente biyectiva, luego basta tomar $e_\eta = u_\eta \circ v_\eta^{-1} \circ u_{\eta+\eta}^{-1}$.

   Si η es finito (no nulo), consideramos la semejanza $f_0 : \omega \times \omega \longrightarrow \omega$ determinada por el orden canónico. Vamos a definir recurrentemente biyecciones $t_n : \omega \longrightarrow \omega^n$, para $n \geq 1$. Tomamos como t_1 la identidad en ω y, supuesto definido t_n, definimos t_{n+1} como la composición de:

   - la semejanza $\omega^{n+1} = \omega^n \cdot \omega \longrightarrow \omega^n \times \omega$, cuando en el producto consideramos el orden lexicográfico,
   - la biyección $\omega^n \times \omega \longrightarrow \omega \times \omega$ dada por $(\delta, n) \mapsto (t_n(\delta), n)$,
   - la biyección $f_0 : \omega \times \omega \longrightarrow \omega$.

   Ahora basta tomar $e_\eta = t_\eta^{-1} \circ t_{\eta+\eta}$.

8. *Para cada $\alpha \geq \omega$, podemos definir una biyección $f_\alpha : \alpha \longrightarrow \alpha \times \alpha$.*

   Basta definir f_α como la composición de la biyección: $c_\alpha : \alpha \longrightarrow \omega^{\eta_\alpha}$ con $e_{\eta_\alpha} : \omega^{\eta_\alpha} \longrightarrow \omega^{\eta_\alpha+\eta_\alpha} = \omega^{\eta_\alpha} \cdot \omega^{\eta_\alpha}$, con la semejanza $\omega^{\eta_\alpha} \cdot \omega^{\eta_\alpha} \longrightarrow \omega^{\eta_\alpha} \times \omega^{\eta_\alpha}$ con la biyección $\omega^{\eta_\alpha} \times \omega^{\eta_\alpha} \longrightarrow \alpha \times \alpha$ dada por $(\delta, \epsilon) \mapsto (c_\alpha^{-1}(\delta), c_\alpha^{-1}(\epsilon))$.

El paso siguiente es probar lo que sin el axioma de elección es una leve generalización del teorema de Cantor:

Teorema 5.89 *Si $\mathfrak{p} \geq 5$ entonces no $2^\mathfrak{p} \leq \mathfrak{p}^2$.*

Demostración: Para cardinales finitos se demuestra fácilmente por inducción que $n \geq 5 \to n^2 < 2^n$: Para $n < 5$ la implicación es cierta trivialmente, para $n = 5$ se hace el cálculo y, si vale para $n \geq 5$, entonces

$$(n+1)^2 = n^2 + 2n + 1 < n^2 + 3n \leq n^2 + n^2 = 2n^2 < 2 \cdot 2^n = 2^{n+1}.$$

Supongamos ahora que $\mathfrak{p}$ es un cardinal infinito y sea $\overline{\overline{X}} = \mathfrak{p}$. Por reducción al absurdo suponemos una aplicación $f : \mathcal{P}X \longrightarrow X \times X$ inyectiva y vamos a construir una aplicación $G : \Omega \longrightarrow X$ inyectiva, con lo que tendremos una contradicción. En primer lugar veremos que podemos construir $g_\omega : \omega \longrightarrow X$ inyectiva.

Por el teorema 5.32 tenemos que $[\omega]^{<\omega}$ es numerable, luego podemos fijar un buen orden en él. Tomemos elementos distintos $x_0, x_1, x_2, x_3, x_4 \in X$ y definamos $g_\omega(i) = x_i$, para $i < 5$.

Supuesta definida $g_\omega|_n : n \longrightarrow X$ inyectiva, para $n \geq 5$, sea $C_n = g_\omega[n]$. Como $|\mathcal{P}C_n| = 2^n > n^2 = |C_n \times C_n|$, existe un subconjunto U de C_n tal que $f(U) \notin C_n \times C_n$. Elegimos el que cumple que $g_\omega^{-1}[U]$ es mínimo respecto al buen orden que hemos fijado en $[\omega]^{<\omega}$. Si $f(U) = (x, y)$, definimos

$$g_\omega(n+1) = \begin{cases} x & \text{si } x \notin C_n, \\ y & \text{si } x \in C_n. \end{cases}$$

Con esto tenemos que $g_\omega|_{n+1} : n+1 \longrightarrow X$ es inyectiva. El teorema de recursión nos garantiza la existencia de g_ω.

Pasemos ahora a la construcción de $G : \Omega \longrightarrow X$. Para ello nos apoyaremos en las biyecciones $f_\alpha : \alpha \longrightarrow \alpha \times \alpha$ que hemos definido para todo ordinal infinito α (sin el axioma de elección). Suponemos definida $G|_\alpha : \alpha \longrightarrow X$ inyectiva. Sea $C_\alpha = G[\alpha]$.

Definimos $g : \alpha \longrightarrow \mathcal{P}X$ como sigue: dado $\beta < \alpha$ calculamos $f_\alpha(\beta) = (\gamma, \delta)$ y tomamos $g(\beta) = f^{-1}(G(\gamma), G(\delta))$ si el par $(G(\gamma), G(\delta))$ tiene antiimagen por f y $g(\beta) = \varnothing$ en caso contrario.

Sea $U = \{G(\beta) \mid \beta < \alpha \wedge G(\beta) \notin g(\beta)\}$ y sea $f(U) = (x, y)$.

Si $(x, y) \in C_\alpha \times C_\alpha$ entonces $(x, y) = (G(\gamma), G(\delta))$ para ciertos γ, $\delta < \alpha$. Sea $\beta = f_\alpha^{-1}(\gamma, \delta)$, de modo que $g(\beta) = U$ y tenemos una contradicción tanto si $G(\beta) \in U$ como en caso contrario. Por consiguiente $(x, y) \notin C_\alpha \times C_\alpha$, luego podemos definir $G(\alpha) = x$ si $x \notin C_\alpha$ o $G(\alpha) = y$ en caso contrario. El teorema de recursión transfinita nos da entonces la existencia de G. ∎

Nota Sin el axioma de elección no puede probarse en general que $\mathfrak{p}^2 \leq 2^\mathfrak{p}$.

Teorema 5.90 *La hipótesis del continuo generalizada implica el axioma de elección.*

Demostración: Por el teorema 5.25, basta probar que $\mathfrak{p}^2 = \mathfrak{p}$ para todo cardinal infinito $\mathfrak{p}$. En primer lugar probamos que $\mathfrak{p} = \mathfrak{p} + 1$.

Es fácil ver que $\mathfrak{p} \leq \mathfrak{p} + 1 \leq 2^\mathfrak{p}$, pero si fuera $\mathfrak{p} + 1 = 2^\mathfrak{p}$, tendríamos que $2^\mathfrak{p} \leq \mathfrak{p} + 1 \leq \mathfrak{p} + \mathfrak{p} \leq \mathfrak{p}\mathfrak{p}$, en contradicción con el teorema anterior. Así pues, la HCG implica que $\mathfrak{p} = \mathfrak{p} + 1$

Ahora veamos que $\mathfrak{p} = 2\mathfrak{p}$.

En efecto, $\mathfrak{p} \leq 2\mathfrak{p} \leq 2 \cdot 2^\mathfrak{p} = 2^{\mathfrak{p}+1} = 2^\mathfrak{p}$, pero no puede ser $2\mathfrak{p} = 2^\mathfrak{p}$ ya que entonces $2^\mathfrak{p} = 2\mathfrak{p} \leq \mathfrak{p}\mathfrak{p}$, de nuevo en contra del teorema anterior. La HCG nos da, pues, la igualdad $\mathfrak{p} = 2\mathfrak{p}$.

Así, $\mathfrak{p} \leq \mathfrak{p}^2 \leq (2^\mathfrak{p})^2 = 2^{2\mathfrak{p}} = 2^\mathfrak{p}$. El teorema anterior y la HCG nos dan la igualdad $\mathfrak{p}^2 = \mathfrak{p}$. ∎

Hemos demostrado que el axioma de elección equivale a que todo conjunto puede ser bien ordenado. En cambio, sin el axioma de elección no es posible demostrar que $\mathcal{P}\omega$ pueda ser bien ordenado. Nuestra segunda aplicación de la aritmética cardinal será demostrar el teorema siguiente:

Teorema 5.91 *El axioma de elección equivale a que $\mathcal{P}\alpha$ puede ser bien ordenado, para todo ordinal α.*

DEMOSTRACIÓN: Suponemos que $\mathcal{P}\alpha$ puede ser bien ordenado, para todo ordinal α, y vamos a probar que V_α puede ser bien ordenado, también para todo ordinal α. Esto es suficiente, ya que (por el axioma de regularidad) todo conjunto está contenido en un conjunto V_α, luego todo conjunto admitirá entonces un buen orden. Lo probamos por inducción sobre α. Si $\alpha = 0$ es trivial.

Si suponemos que V_α es bien ordenable, existe $f : V_\alpha \longrightarrow \beta$ biyectiva, para cierto ordinal β. Claramente, f induce una biyección $F : V_{\alpha+1} = \mathcal{P}V_\alpha \longrightarrow \mathcal{P}\beta$ y, como estamos suponiendo que $\mathcal{P}\beta$ es bien ordenable, concluimos que $V_{\alpha+1}$ también lo es.

Supongamos ahora que V_δ es bien ordenable, para todo ordinal $\delta < \lambda$. Éste es el caso más delicado, porque no podemos elegir un buen orden en cada V_δ sin más aclaración, ya que entonces estaríamos usando el axioma de elección.

Vamos a construir una sucesión $\{\trianglelefteq_\delta\}_{\delta\leq\lambda}$ de modo que cada $\trianglelefteq_\delta$ es un buen orden en V_δ con la propiedad de que si $\delta < \delta' < \lambda$, entonces V_δ sea una sección inicial de $V_{\delta'}$ respecto a $\trianglelefteq_{\delta'}$.

Antes de ello, observamos que está definida la sucesión $\{|V_\delta|\}_{\delta<\lambda}$, luego podemos considerar el cardinal $\kappa = \bigcup_{\delta<\lambda} |V_\delta|^+$. Fijamos un buen orden $\leq_*$ en el conjunto $\mathcal{P}\kappa$.

Ahora definimos $\trianglelefteq_0 = \varnothing$. Supuesto definido $\trianglelefteq_\delta$, consideramos la semejanza $s_\delta : (V_\delta, \trianglelefteq_\delta) \longrightarrow \alpha_\delta$, donde $|\alpha_\delta| = |V_\delta| < \kappa$, luego $\alpha_\delta < \kappa$, luego $\mathcal{P}\alpha_\delta \subset \mathcal{P}\kappa$, luego el buen orden $\leq_*$ induce un buen orden en $\mathcal{P}\alpha_\delta$, que a su vez induce un buen orden $\trianglelefteq^*_{\delta+1}$ en $V_{\delta+1}$ a través de la biyección $\mathcal{P}V_\delta \longrightarrow \mathcal{P}\alpha_\delta$ inducida por s_δ. Por último definimos $\trianglelefteq_{\delta+1}$ mediante:

$$x \trianglelefteq_{\delta+1} y \leftrightarrow (x, y \in V_\delta \wedge x \trianglelefteq_\delta y) \vee (x \in V_\delta \wedge y \in V_{\delta+1} \setminus V_\delta)$$

$$\vee\, (x, y \in V_{\delta+1} \setminus V_\delta \wedge x \trianglelefteq^*_{\delta+1} y).$$

Con este retoque nos aseguramos de que V_δ es una sección inicial de $V_{\delta+1}$.

Si tenemos definidos $\{\trianglelefteq_\delta\}_{\delta<\lambda'}$, para $\lambda' \leq \lambda$, la condición de que cada V_δ sea una sección inicial de los siguientes conjuntos de la jerarquía implica que la unión de todos los buenos órdenes es un buen orden $\trianglelefteq_{\lambda'}$ respecto del cual cada V_δ es una sección inicial de $V_{\lambda'}$.

Así tenemos construida la sucesión de buenos órdenes y, en particular, tenemos el buen orden $\trianglelefteq_\lambda$, que prueba que V_λ es bien ordenable. ∎

Observemos que el axioma de regularidad es esencial en el teorema anterior. Si no suponemos dicho axioma, lo que muestra la prueba es que si $\mathcal{P}\alpha$ puede ser bien ordenado, para todo ordinal α, entonces todo conjunto regular puede ser bien ordenado.

Sin el axioma de elección, ni siquiera es demostrable que todo conjunto pueda ser totalmente ordenado, pero como complemento al teorema anterior conviene observar lo siguiente:

Teorema 5.92 *Si A es un conjunto bien ordenable, entonces $\mathcal{P}A$ admite un orden total.*

DEMOSTRACIÓN: Basta probar que si α es un ordinal, entonces $\mathcal{P}\alpha$ admite un orden total, pero siempre podemos comparar dos subconjuntos $x, y \subset \alpha$ tales que $x \neq y$ tomando el mínimo $\delta_{xy} \in (x \setminus y) \cup (y \setminus x)$ y estableciendo que

$$x < y \leftrightarrow \delta_{xy} \in x.$$

Observemos que la relación es transitiva, pues si $x < y < z$, entonces $\delta_{xy} \neq \delta_{yz}$, pues $\delta_{xy} \notin y \wedge \delta_{yz} \in y$. Si $\delta_{xy} < \delta_{yz}$, entonces $\delta_{xy} \in x \setminus z$, pues si $\delta_{xy} \in z$ cumpliría también $\delta_{xy} \in y$ (por ser menor que el mínimo ordinal que distingue a y y a z) y de hecho $\delta_{xy} = \delta_{xz}$, pues si $\alpha \in (x \setminus z) \cup (z \setminus x)$, o bien $\alpha \in y$, en cuyo caso, o bien $\alpha \in y \setminus z$, luego $\alpha \geq \delta_{yz} > \delta_{xy}$, o bien $\alpha \in y \setminus x$, luego $\alpha \geq \delta_{xy}$. Esto prueba que $x < z$.

Alternativamente, si $\delta_{yz} < \delta_{xy}$, tiene que ser $\delta_{yz} \in x$ (pues está en y y es menor que el mínimo ordinal que distingue a x de y) y se comprueba análogamente que $\delta_{xz} = \delta_{yz}$, luego también $x < z$. ∎

Capítulo VI

Conjuntos cerrados no acotados y estacionarios

Introducimos ahora unos conceptos fundamentales para trabajar con ordinales. Exponemos la teoría general en las dos primeras secciones, mientras que las siguientes contienen diversas aplicaciones independientes entre sí. Entre otras demostraremos un profundo teorema de Silver (1974) sobre la función del continuo en los cardinales singulares. Trabajamos en NBG, incluyendo el axioma de elección.

6.1 Conjuntos cerrados no acotados

El concepto básico alrededor del cual girará todo este capítulo es el siguiente:

Definición 6.1 Sea λ un ordinal límite o bien $\lambda = \Omega$. Una clase $C \subset \lambda$ es *cerrada* en λ si cuando un ordinal límite $\delta < \lambda$ cumple que $\delta \cap C$ no está acotado en δ, entonces $\delta \in C$.

Informalmente, la definición exige que si C contiene ordinales menores que δ tan próximos a δ como se quiera, entonces $\delta \in C$. Es fácil probar que esto equivale a que C sea cerrada respecto a la topología del orden (al menos si C es un conjunto), pero no vamos a necesitar nunca este hecho.

Una caracterización útil es la siguiente:

Teorema 6.2 *Sea λ un ordinal límite o bien $\lambda = \Omega$. Una subclase C de λ es cerrada en λ si y sólo si para todo conjunto $X \subset C$ no vacío y acotado en λ se cumple que* $\sup X \in C$. *Equivalentemente: para todo $X \subset C$ no vacío, si* $\sup X \in \lambda$, *entonces* $\sup X \in C$.

Demostración: Supongamos que C es cerrada y sea X un subconjunto en las condiciones indicadas. Llamemos $\delta = \sup X$.

Si $\delta \in X$ entonces $\delta \in C$. Supongamos que $\delta \notin X$ y veamos que igualmente $\delta \in C$. En primer lugar, δ es un ordinal límite, pues si fuera $\delta = 0$ tendría que ser $X = \{0\}$ y si $\beta < \delta$ entonces $\beta < \alpha$ para cierto $\alpha \in X$, luego $\alpha \leq \delta$, pero, como $\delta \notin X$, ha de ser $\alpha < \delta$, luego $\beta + 1 < \alpha + 1 \leq \delta$.

En realidad hemos probado también que $\delta \cap C$ no está acotado en δ, pues, dado $\beta < \delta$, hemos encontrado un $\alpha \in \delta \cap C$ mayor que β. Por definición de clase cerrada concluimos que $\delta \in C$.

Recíprocamente, si C tiene la propiedad indicada y $\delta < \lambda$ es un ordinal límite tal que $\delta \cap C$ no está acotado en δ, es claro que $\delta = \sup(\delta \cap C)$, luego $\delta \in C$. ∎

Definición 6.3 En lo sucesivo las iniciales c.n.a. significarán "cerrado no acotado", es decir, diremos que una clase $C \subset \lambda$ es c.n.a. en λ si es cerrada en λ y no está acotada en λ.

Un resultado fundamental es que los conjuntos cerrados no acotados se conservan por intersecciones si su número no alcanza la cofinalidad de λ:

Teorema 6.4 *Sea λ un ordinal límite de cofinalidad no numerable, $\beta < \operatorname{cf}\lambda$ y $\{C_\alpha\}_{\alpha<\beta}$ una familia de conjuntos c.n.a. en λ. Entonces se cumple que $\bigcap_{\alpha<\beta} C_\alpha$ es c.n.a. en λ.*

Demostración: Del teorema anterior se sigue inmediatamente que la intersección de cualquier familia de cerrados es cerrada. Sólo queda probar que $\bigcap_{\alpha<\beta} C_\alpha$ no está acotado.

Sea $f_\alpha : \lambda \longrightarrow \lambda$ la función dada por $f_\alpha(\delta) = \text{mín}\{\epsilon \in C_\alpha \mid \delta < \epsilon\}$. La definición es correcta porque C_α no está acotado en λ. Para todo $\delta < \lambda$ tenemos que $\delta < f_\alpha(\delta) \in C_\alpha$.

Sea ahora $g : \lambda \longrightarrow \lambda$ la función dada por $g(\delta) = \sup_{\alpha<\beta} f_\alpha(\delta)$. Notemos que $g(\delta) \in \lambda$ por la hipótesis de que $\beta < \operatorname{cf}\lambda$. Es claro que si $\delta < \lambda$ entonces $\delta < g(\delta) \leq g^\omega(\delta) < \lambda$, donde g^ω es la función iterada de g definida en 5.52.

Además $g^\omega(\delta)$ es un ordinal límite, pues si $\alpha < g^\omega(\delta)$, entonces $\alpha \in g^n(\delta)$ para cierto $n \in \omega$ y así $\alpha + 1 \leq g^n(\delta) < g(g^n(\delta)) = g^{n+1}(\delta) \leq g^\omega(\delta)$.

Se cumple que $g^\omega(\delta) \cap C_\alpha$ no está acotado en $g^\omega(\delta)$, pues si $\gamma \in g^\omega(\delta)$, entonces $\gamma \in g^n(\delta) < f_\alpha(g^n(\delta)) \in C_\alpha$ y $f_\alpha(g^n(\delta)) \leq g(g^n(\delta)) = g^{n+1}(\delta) < g^\omega(\delta)$, o sea, $\gamma < f_\alpha(g^n(\delta)) \in g^\omega(\delta) \cap C_\alpha$.

Como C_α es cerrado podemos concluir que $g^\omega(\delta) \in C_\alpha$, y esto para todo $\alpha < \beta$, luego $\delta < g^\omega(\delta) \in \bigcap_{\alpha<\beta} C_\alpha$, lo que prueba que la intersección es no acotada. ∎

Nota Hemos enunciado el teorema anterior para conjuntos por no complicar el enunciado, pero vale igualmente (con la misma prueba) si $\lambda = \Omega$ y β es un ordinal cualquiera. Se podría objetar que no tiene sentido considerar una sucesión $\{C_\alpha\}_{\alpha<\beta}$ de clases (necesariamente propias) c.n.a.s en Ω, pero tal sucesión puede definirse como una subclase $C \subset \Omega \times \beta$, de modo que $C_\alpha \equiv \{\epsilon \mid (\epsilon, \alpha) \in C\}$. ∎

El teorema siguiente nos proporciona los primeros ejemplos no triviales de cerrados no acotados:

Teorema 6.5 *Sea κ un cardinal regular no numerable. Un conjunto $C \subset \kappa$ es c.n.a. en κ si y sólo si existe una función normal $f : \kappa \longrightarrow \kappa$ tal que $f[\kappa] = C$.*

DEMOSTRACIÓN: Por el teorema 3.26, $\operatorname{ord} C \leq \kappa$ y como $|C| = \kappa$ (porque C no está acotado en κ y κ es regular), ha de ser $\operatorname{ord} C = \kappa$. Sea, pues, $f : \kappa \longrightarrow C$ la semejanza. Basta probar que $f : \kappa \longrightarrow \kappa$ es normal. Claramente sólo hay que ver que si $\lambda < \kappa$ entonces $f(\lambda) = \bigcup_{\delta<\lambda} f(\delta)$. Ahora bien, $\lambda = \sup_\kappa\{\delta \mid \delta < \lambda\}$, luego, al ser f una semejanza,

$$f(\lambda) = \sup_C\{f(\delta) \mid \delta < \lambda\} = \bigcup_{\delta<\lambda} f(\delta).$$

En efecto, como κ es regular tenemos que $\bigcup_{\delta<\lambda} f(\delta) \in \kappa$ y como C es cerrado tenemos que $\bigcup_{\delta<\lambda} f(\delta) \in C$, luego obviamente se trata del supremo del conjunto $\{f(\delta) \mid \delta < \lambda\}$.

Supongamos ahora que C es el rango de una función normal f. Entonces $|C| = \kappa$ y en consecuencia C no está acotado en κ. Si $\delta < \kappa$ es un ordinal límite tal que $\delta \cap C$ no está acotado en δ, entonces sea $\lambda = \{\alpha < \kappa \mid f(\alpha) < \delta\}$. Es fácil ver que λ es un ordinal límite y $f|_\lambda : \lambda \longrightarrow \delta$ es inyectiva, luego $|\lambda| \leq |\delta| < \kappa$, de donde $\lambda < \kappa$. Por consiguiente podemos calcular

$$f(\lambda) = \bigcup_{\alpha<\lambda} f(\alpha) = \sup(\delta \cap C) = \delta,$$

luego $\delta \in C$ y C es cerrado. ∎

Nota La prueba se adapta con cambios mínimos (que la simplifican) al caso en que $\kappa = \Omega$. En tal caso, en lugar del teorema 3.26 aplicamos 3.27, que nos da una semejanza $F : \Omega \longrightarrow C$. El resto de la prueba vale sin más cambio que omitir las referencias a la cofinalidad de κ. Para el recíproco, en lugar de afirmar que $|C| = \kappa$, concluimos que C no está acotado porque toda función normal cumple $\bigwedge\alpha\ \alpha \leq F(\alpha)$, y luego tenemos trivialmente que $\lambda \in \Omega$, sin necesidad de considerar cardinales. ∎

El teorema 5.54 prueba que una función normal en un cardinal regular no numerable tiene un conjunto no acotado de puntos fijos. Ahora probamos que dicho conjunto también es cerrado.

Teorema 6.6 *Sea κ un cardinal regular no numerable o bien $\kappa = \Omega$ y sea $f : \kappa \longrightarrow \kappa$ una función normal. Entonces la clase $F = \{\alpha < \kappa \mid f(\alpha) = \alpha\}$ es c.n.a. en κ.*

DEMOSTRACIÓN: Ya sabemos que F no está acotada en κ. Veamos que es cerrada. Para ello tomamos $\lambda < \kappa$ tal que $\lambda \cap F$ no esté acotado en λ. Entonces

$f(\lambda) = \bigcup_{\delta<\lambda} f(\delta)$. Si $\delta < \lambda$, entonces existe un $\eta \in F$ tal que $\delta < \eta$, luego $f(\delta) < f(\eta) = \eta < \lambda$, y por consiguiente concluimos que $f(\lambda) \leq \lambda$. La otra desigualdad se da por ser f normal, luego $\lambda \in F$, que es, por tanto, cerrada. ∎

A partir de aquí nos restringimos a estudiar conjuntos cerrados no acotados (no clases). La mayor parte de las ocasiones en que se dice que un conjunto es evidentemente c.n.a. se está apelando tácitamente al teorema siguiente:

Teorema 6.7 *Sea κ un cardinal regular no numerable y A un conjunto de aplicaciones $f : {}^n\kappa \longrightarrow \kappa$, donde n es un número natural que depende de f. Supongamos que $|A| < \kappa$. Entonces el conjunto*

$$C = \{\alpha < \kappa \mid \bigwedge f n(f \in A \wedge f : {}^n\kappa \longrightarrow \kappa \to f[{}^n\alpha] \subset \alpha)\}$$

es c.n.a. en κ.

Demostración: Podemos suponer que el conjunto A consta de una única función $f : {}^n\kappa \longrightarrow \kappa$, pues el conjunto C para un conjunto de menos de κ funciones es la intersección de los conjuntos correspondientes a cada una de ellas, luego el caso general se deduce de 6.4.

Sea $\lambda < \kappa$ tal que $C \cap \lambda$ no esté acotado en λ, tomemos $\epsilon_1, \ldots, \epsilon_n \in \lambda$ y sea $\beta \in C \cap \lambda$ mayor que todos ellos.

Así $f(\epsilon_1, \ldots, \epsilon_n) \in f[{}^n\beta] \subset \beta < \lambda$, luego $\bigwedge x \in {}^n\lambda\ f(x) \in \lambda$, es decir, $f[{}^n\lambda] \subset \lambda$, lo que implica que $\lambda \in C$, luego C es, por tanto, cerrado.

Sea $\alpha \in \kappa$. Definimos recurrentemente una sucesión $\{\alpha_m\}$ de ordinales en κ. Tomamos $\alpha_0 = \alpha$ y, supuesto definido α_m, sea α_{m+1} el mínimo ordinal tal que $f[{}^n\alpha_m] \subset \alpha_{m+1} < \kappa$ (existe porque $|f[{}^n\alpha_m]| \leq |{}^n\alpha_m| < \kappa$, luego $f[{}^n\alpha_m]$ está acotado en κ). Finalmente definimos $\alpha^* = \sup_{m\in\omega} \alpha_m \in \kappa$. Claramente $\alpha \leq \alpha^*$. Si probamos que $\alpha^* \in C$ tendremos que C es no acotado.

Tomemos ordinales $\epsilon_1, \ldots, \epsilon_n \in \alpha^*$. Entonces existe un natural m tal que $\epsilon_1, \ldots, \epsilon_n \in \alpha_m$ y así

$$f(\epsilon_1, \ldots, \epsilon_n) \in f[{}^n\alpha_m] \subset \alpha_{m+1} \leq \alpha^*,$$

luego $f[\alpha^*] \subset \alpha^*$ y, consecuentemente, $\alpha^* \in C$. ∎

Si κ es un cardinal regular no numerable, el teorema 6.4 nos da que la intersección de una cantidad menor que κ de subconjuntos c.n.a.s es c.n.a. Obviamente esto no es cierto para familias cualesquiera de κ conjuntos (por ejemplo para $\{\kappa \setminus \alpha\}_{\alpha<\kappa}$), pero sí se cumple un hecho parecido y de gran utilidad. Para enunciarlo necesitamos una definición:

Definición 6.8 Sea $\{X_\alpha\}_{\alpha<\kappa}$ una familia de subconjuntos de un cardinal κ. Llamaremos *intersección diagonal* de la familia al conjunto

$$\triangle_{\alpha<\kappa} X_\alpha = \{\gamma < \kappa \mid \gamma \in \bigcap_{\alpha<\gamma} X_\alpha\}.$$

Si intentamos probar algo "razonable" y "nos gustaría" que una intersección de κ conjuntos c.n.a.s fuera c.n.a., es probable que en realidad nos baste lo siguiente:

Teorema 6.9 *Sea κ un cardinal regular no numerable y $\{C_\alpha\}_{\alpha<\kappa}$ una familia de conjuntos c.n.a. en κ. Entonces $\triangle\limits_{\alpha<\kappa} C_\alpha$ es c.n.a. en κ.*

DEMOSTRACIÓN: Por abreviar, llamaremos D a la intersección diagonal. Tomemos $\lambda < \kappa$ tal que $\lambda \cap D$ no esté acotado en λ. Hemos de probar que $\lambda \in D$, es decir, tomamos $\alpha < \lambda$ y hemos de ver que $\lambda \in C_\alpha$. A su vez, para ello basta probar que $\lambda \cap C_\alpha$ no está acotado en λ, pero si $\beta \in \lambda$ tenemos que existe un $\epsilon \in \lambda \cap D$ tal que $\alpha, \beta < \epsilon$. Como $\epsilon \in D$ se cumple que $\epsilon \in C_\alpha \cap \lambda$, luego, efectivamente, $C_\alpha \cap \lambda$ no está acotado en λ y D es cerrado.

Para cada $\beta < \kappa$, el teorema 6.4 nos permite tomar $g(\beta) \in \bigcap\limits_{\alpha<\beta} C_\alpha$ tal que $\beta < g(\beta)$. Tenemos así una función $g : \kappa \longrightarrow \kappa$.

Por el teorema 6.7, el conjunto

$$C = \{\lambda \in \kappa \mid g[\lambda] \subset \lambda\}$$

es c.n.a. en κ (en principio tenemos que es c.n.a. el conjunto de todos los ordinales $\alpha < \kappa$ tales que $g[\alpha] \subset \alpha$, pero es claro que el conjunto de los $\lambda < \kappa$ también es c.n.a., y C es la intersección de ambos conjuntos). Si probamos que $C \subset D$ tendremos que D no está acotado.

Sea $\lambda \in C$. Tomamos $\alpha < \lambda$ y hemos de ver que $\lambda \in C_\alpha$, para lo cual se ha de cumplir que $\lambda \cap C_\alpha$ no esté acotado en λ. Ahora bien, si $\delta < \lambda$, tomamos $\epsilon \in \lambda$ tal que $\alpha, \delta < \epsilon$. Así $\delta < g(\epsilon) \in \lambda \cap C_\alpha$. ∎

Definición 6.10 Sea λ un ordinal límite de cofinalidad no numerable. Definimos el *filtro de cerrados no acotados* en λ como el conjunto

$$\text{c.n.a.}(\lambda) = \{X \subset \lambda \mid \bigvee C(C \subset X \wedge C \text{ es c.n.a. en } \lambda\} \subset \mathcal{P}\lambda.$$

Es inmediato comprobar que realmente es un filtro en λ en el sentido de la definición 4.30. En general, si κ es un cardinal infinito, un filtro F es κ-completo si cuando $A \subset F$ con $|A| < \kappa$, se cumple que $\bigcap A \in F$. En estos términos, hemos probado que el filtro c.n.a.(λ) es cf λ-completo.

La idea subyacente es que un filtro en un conjunto X puede verse como una determinación de lo que entendemos por subconjuntos "muy grandes" de X. Lo que dice la definición 4.30 es que X es "muy grande" y $\varnothing$ no, que la intersección de dos conjuntos "muy grandes" es "muy grande" y que todo conjunto que contiene a un conjunto "muy grande" es "muy grande".

Equivalentemente, podemos considerar que un subconjunto de X es "muy pequeño" si su complementario es "muy grande". Si un filtro es κ-completo, esto se traduce en que la unión de menos de κ conjuntos "muy pequeños" es "muy pequeña". Por ello, cuando mayor sea κ, más justificado estará el considerar como "muy pequeños" a los complementarios de los conjuntos del filtro y, por consiguiente, más justificado estará considerar como "muy grandes" a los conjuntos del filtro.

El interés de estos conceptos se debe a que, por ejemplo, si tenemos una familia de menos de κ subconjuntos "muy grandes" de un cardinal regular κ, sabemos que la intersección será también "muy grande", y en particular será no vacía, luego podremos tomar ordinales que cumplan simultáneamente las propiedades que definen a todos los conjuntos de la familia. No obstante, es frecuente tener que trabajar con conjuntos que no son "muy grandes", pero puede ser suficiente con que no sean "muy pequeños". Esto nos lleva al concepto de conjunto estacionario que presentamos en la sección siguiente.

6.2 Conjuntos estacionarios

Un conjunto estacionario es un conjunto "no muy pequeño", es decir, cuyo complementario no es "muy grande":

Definición 6.11 Sea λ un ordinal de cofinalidad no numerable. Un conjunto $E \subset \lambda$ es *estacionario* en λ si $\lambda \setminus E \notin$ c.n.a.(λ).

Explícitamente, esto significa que $\lambda \setminus E$ no contiene a ningún c.n.a. o, equivalentemente, a que E corta a todos los c.n.a.s. Así, un conjunto estacionario no es necesariamente "muy grande", pero es lo suficientemente grande como para cortar a cualquier conjunto "muy grande". Incluimos esto como una de las propiedades de los conjuntos estacionarios que recogemos en el teorema siguiente:

Teorema 6.12 *Sea λ un ordinal de cofinalidad no numerable y $E \subset \lambda$. Se cumple:*

1. *Si E es c.n.a en λ entonces E es estacionario en λ.*
2. *E es estacionario en λ si y sólo si corta a todo c.n.a. en λ.*
3. *Si E es estacionario en λ entonces no está acotado en λ.*
4. *Si E es estacionario y C es c.n.a. en λ entonces $E \cap C$ es también estacionario en λ.*

Demostración: 1) es inmediato: si E no fuera estacionario entonces $\lambda \setminus E$ contendría un c.n.a. disjunto de E.

2) E es estacionario si y sólo si $\lambda \setminus E \notin$ *c.n.a.*(λ), si y sólo si no existe ningún c.n.a. C tal que $C \subset \lambda \setminus E$, si y solo si todo c.n.a. C corta a E.

3) Se sigue de 2) junto con el hecho obvio de que si $\alpha \in \lambda$ entonces $\lambda \setminus \alpha$ es c.n.a.

4) Si C' es otro c.n.a. en λ, entonces $C \cap C'$ es c.n.a., luego $E \cap C \cap C' \neq \varnothing$ por b), luego, también por b), $E \cap C$ es estacionario. ∎

Notemos que si E es estacionario en λ y $\delta < \lambda$, entonces E corta a $\lambda \setminus \delta$, porque es c.n.a. en λ, luego E contiene ordinales mayores que δ. Así pues, todo conjunto estacionario es no acotado. También es obvio que todo conjunto que contenga a un conjunto estacionario es estacionario.

Veamos un ejemplo:

Teorema 6.13 *Sea λ un ordinal límite de cofinalidad no numerable y $\kappa < \operatorname{cf}\lambda$ un cardinal regular. Entonces $\{\alpha < \lambda \mid \operatorname{cf}\alpha = \kappa\}$ es estacionario en λ.*

DEMOSTRACIÓN: Llamemos E al conjunto del enunciado. Sea C un c.n.a. en λ y sea $\alpha = \operatorname{ord} C$. Tenemos que $|\alpha| = |C| \geq \operatorname{cf}\lambda > \kappa$. Por lo tanto $\kappa < \alpha$. Sea $f : \alpha \longrightarrow C$ la semejanza. Igual que en la prueba de 6.5 se ve que f es una función normal, por lo que $\operatorname{cf} f(\kappa) = \operatorname{cf}\kappa = \kappa$, de modo que $f(\kappa) \in C \cap E$. Por el teorema anterior concluimos que E es estacionario. ∎

Ejemplo Los conjuntos

$$\{\alpha < \omega_2 \mid \operatorname{cf}\alpha = \aleph_0\} \quad \text{y} \quad \{\alpha < \omega_2 \mid \operatorname{cf}\alpha = \aleph_1\}$$

son estacionarios disjuntos en ω_2, luego vemos que la intersección de conjuntos estacionarios no es necesariamente estacionaria. Más aún, de aquí se deduce que existen conjuntos estacionarios que no son cerrados. ∎

Veamos ahora una caracterización muy útil de los conjuntos estacionarios en un cardinal regular. Para ello necesitamos una definición:

Definición 6.14 Si $A \subset \kappa$, una aplicación $f : A \longrightarrow \kappa$ es *regresiva* si

$$\bigwedge \alpha \in A(\alpha \neq 0 \to f(\alpha) < \alpha).$$

Teorema 6.15 (Fodor) *Sea κ un cardinal regular no numerable y $E \subset \kappa$. Las afirmaciones siguientes son equivalentes:*

1. *E es estacionario en κ,*
2. *Si $f : E \longrightarrow \kappa$ es regresiva, existe un $\alpha < \kappa$ tal que*

$$f^{-1}[\{\alpha\}] = \{\beta \in E \mid f(\beta) = \alpha\}$$

   es estacionario en κ,

3. *Si $f : E \longrightarrow \kappa$ es regresiva, existe un $\alpha < \kappa$ tal que*

$$f^{-1}[\{\alpha\}] = \{\beta \in E \mid f(\beta) = \alpha\}$$

   no está acotado en κ.

DEMOSTRACIÓN: 1) → 2) Si f es regresiva pero $f^{-1}[\{\alpha\}]$ no es estacionario para ningún $\alpha < \kappa$, tomemos un c.n.a. C_α tal que $C_\alpha \cap f^{-1}[\{\alpha\}] = \varnothing$. Entonces $D = \underset{\alpha<\kappa}{\triangle} C_\alpha$ es también c.n.a. en κ. Por consiguiente $E \cap D$ es estacionario, luego podemos tomar $\gamma \in E \cap D$, $\gamma \neq 0$. En particular $\gamma \in \bigcap_{\alpha<\gamma} C_\alpha$. Sea $\delta = f(\gamma) < \gamma$. Así $\gamma \in f^{-1}[\{\delta\}] \cap C_\delta = \varnothing$.

2) → 3) es obvio.

3) $\to$ 1) Si E no es estacionario, sea C un c.n.a. en κ tal que $C \cap E = \varnothing$. Sea $f : E \longrightarrow \kappa$ la aplicación dada por $f(\alpha) = \sup(C \cap \alpha)$. Claramente $f(\alpha) \leq \alpha$, pero $f(\alpha) \in C$ y $\alpha \in E$, luego de hecho $f(\alpha) < \alpha$ y f es regresiva.

Por otra parte, si $\gamma < \kappa$, como C no está acotado, existe un $\alpha \in C$ tal que $\gamma < \alpha$. Vamos a probar que $f^{-1}[\{\gamma\}] \subset \alpha + 1$, es decir, que $f^{-1}[\{\gamma\}]$ está acotado en κ para todo γ, en contradicción con 3). En efecto, si $\delta \in E$ y $\alpha < \delta$, entonces $f(\delta) = \sup(C \cap \delta) \geq \alpha$, pues $\alpha \in C \cap \delta$. Así pues, $f(\delta) \neq \gamma$. ∎

Terminamos la sección con un resultado nada trivial sobre conjuntos estacionarios que tiene aplicaciones importantes. Necesitamos un resultado auxiliar previo.

Teorema 6.16 *Sea κ un cardinal regular no numerable y sea E un subconjunto estacionario en κ. Entonces el conjunto*

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

es estacionario en κ.

Demostración: Tomamos un conjunto c.n.a. C en κ. Hemos de probar que $C \cap T \neq \varnothing$. Sea

$$C' = \{\lambda \in C \mid C \cap \lambda \text{ no está acotado en } \lambda\}.$$

Veamos que C' es c.n.a. Por el teorema 6.5 sabemos que existe una función normal $f : \kappa \longrightarrow \kappa$ tal que $f[\kappa] = C$. Por otra parte, el conjunto $L = \{\lambda | \lambda < \kappa\}$ es claramente c.n.a. en κ, luego existe $g : \kappa \longrightarrow \kappa$ normal tal que $g[\kappa] = L$. Sea $h = g \circ f : \kappa \longrightarrow \kappa$. Basta ver que $C' = h[\kappa]$.

Si $\alpha \in \kappa$, entonces $g(\alpha) \in \kappa$ es un ordinal límite, luego

$$h(\alpha) = f(g(\alpha)) = \bigcup_{\delta \in g(\alpha)} f(\delta),$$

donde cada $f(\delta) \in C$, luego $h(\alpha) \cap C$ no está acotado en $h(\alpha)$. Así pues, $h(\alpha) \in C'$.

Tomemos ahora $\lambda \in C'$. Sea $\alpha < \kappa$ tal que $f(\alpha) = \lambda$. Si $\alpha = 0$ entonces λ es el mínimo de C, luego $C \cap \lambda = \varnothing$ está acotado en λ, lo cual contradice que $\lambda \in C'$.

Si $\alpha = \beta + 1$ entonces $f(\beta)$ es una cota de $C \cap \lambda$ en λ, pues $f(\beta) \in f(\beta+1) = \lambda$ y, si $\delta \in C \cap \lambda$ entonces $\delta = f(\gamma)$ para un $\gamma \in \kappa$. Así, $\delta < \lambda$, $f(\gamma) < f(\alpha)$, $\gamma < \alpha = \beta + 1$, $\gamma \leq \beta$, $\delta = f(\gamma) \leq f(\beta)$, luego también $C \cap \lambda$ resulta estar acotado en λ y tenemos otra contradicción.

La única posibilidad es que α sea un límite, luego existe $\epsilon < \kappa$ tal que $\alpha = g(\epsilon)$, y así $\lambda = h(\epsilon) \in h[\kappa]$.

Como E es estacionario y C' es c.n.a. tenemos que $E \cap C' \neq \varnothing$. Sea λ el mínimo de $E \cap C'$. Si $\operatorname{cf}\lambda = \aleph_0$ entonces $\lambda \in T \cap C \neq \varnothing$. Supongamos que $\operatorname{cf}\lambda > \aleph_0$. Como $\lambda \in C'$ tenemos que $\lambda \cap C$ no está acotado en λ. Vamos a probar que, de hecho, $\lambda \cap C'$ no está acotado en λ. Para ello consideramos la aplicación $f : \lambda \longrightarrow \lambda$ que a cada $\alpha \in \lambda$ le asigna el mínimo ordinal en $\lambda \cap C$ mayor que α.

Vamos a probar que si $\alpha < \lambda$, entonces $f^\omega(\alpha) \in \lambda \cap C'$ y, desde luego, $\alpha \leq f^\omega(\alpha)$. Teniendo en cuenta que $\delta < f(\delta)$ para todo $\delta < \lambda$, es claro que la sucesión $f^n(\alpha)$ es estrictamente creciente de ordinales de $\lambda \cap C$. De aquí deducimos que su supremo $f^\omega(\alpha)$ es un ordinal límite y $f^\omega(\alpha) \cap C$ no está acotado en $f^\omega(\alpha)$. Como C es cerrado concluimos que $f^\omega(\alpha) \in C$ y de aquí a su vez que $f^\omega(\alpha) \in \lambda \cap C'$.

Por otra parte, es inmediato comprobar que $\lambda \cap C'$ es cerrado en λ, luego se trata de un c.n.a. Ahora bien, $(\lambda \cap C') \cap (\lambda \cap E) \subset \lambda \cap (C' \cap E) = \varnothing$, porque λ es el mínimo de $C' \cap E$. Esto significa que $E \cap \lambda$ no es estacionario en λ, luego $\lambda \in T \cap C' \neq \varnothing$. ∎

No es fácil encontrar ejemplos de conjuntos estacionarios disjuntos en ω_1. Sin embargo, lo cierto es que existen, como se desprende del siguiente teorema general:

Teorema 6.17 (Solovay) *Sea κ un cardinal regular no numerable y A un conjunto estacionario en κ. Entonces existen conjuntos $\{E_\alpha\}_{\alpha<\kappa}$ estacionarios en κ y disjuntos dos a dos tales que*

$$A = \bigcup_{\alpha<\kappa} E_\kappa.$$

Demostración: Sea

$$T = \{\lambda \in A \mid \operatorname{cf}\lambda = \aleph_0 \vee (\operatorname{cf}\lambda > \aleph_0 \wedge A \cap \lambda \text{ no es estacionario en } \lambda\},$$

que según el teorema anterior es estacionario en κ. Para cada $\lambda \in T$ tomemos $f_\lambda : \operatorname{cf}\lambda \longrightarrow \lambda$ cofinal y normal. Veamos que si $\operatorname{cf}\lambda > \aleph_0$ podemos exigir que $f_\lambda[\operatorname{cf}\lambda] \cap T = \varnothing$.

En efecto, si $\operatorname{cf}\lambda > \aleph_0$ tenemos que $A \cap \lambda$ no es estacionario en λ, luego tampoco lo es $T \cap \lambda$. Por consiguiente existe un c.n.a. C en λ de manera que $C \cap T \cap \lambda = \varnothing$. Definimos $f^*_\lambda : \operatorname{cf}\lambda \longrightarrow \lambda$ mediante

$f^*_\lambda(0) = \min C$,

$f^*_\lambda(\alpha+1) =$ mínimo ordinal $\epsilon \in C$ tal que $f^*_\lambda(\alpha) < \epsilon$ y $f_\lambda(\alpha) < \epsilon$.

$f^*_\lambda(\lambda') = \bigcup_{\delta<\lambda'} f^*_\lambda(\delta)$.

Claramente f^*_λ es normal y una simple inducción (usando que C es cerrado en el caso límite) prueba que $f^*_\lambda : \operatorname{cf}\lambda \longrightarrow C$. Como $f_\lambda(\alpha) < f^*_\lambda(\alpha+1)$ para todo $\alpha < \lambda$ y f_λ es cofinal, es claro que f^*_λ también lo es, y además $f^*_\lambda[\operatorname{cf}\lambda] \cap T \subset C \cap T = \varnothing$.

En lo sucesivo suprimiremos los asteriscos. Veamos ahora que existe un $\delta < \kappa$ tal que para todo $\epsilon < \kappa$ el conjunto

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

es estacionario en κ.

En caso contrario, para todo $\delta < \kappa$ existe un $\epsilon(\delta) < \kappa$ y un c.n.a. C_δ en κ tales que

$$\{\lambda \in T \mid \delta < \operatorname{cf}\lambda \wedge f_\lambda(\delta) \geq \epsilon(\delta)\} \cap C_\delta = \varnothing.$$

Equivalentemente, para todo $\delta < \kappa$ existe un $\epsilon(\delta) < \kappa$ y un c.n.a. C_δ en κ tales que si $\lambda \in T \cap C_\delta$ y $\delta < \operatorname{cf}\lambda$, entonces $f_\lambda(\delta) < \epsilon(\delta)$.

Sea $C = \triangle\limits_{\alpha<\kappa} C_\alpha$, que es c.n.a. en κ. Si $\lambda \in C \cap T$, entonces

$$\bigwedge \delta < \operatorname{cf}\lambda \; f_\lambda(\delta) < \epsilon(\delta)$$

(puesto que $\lambda \in T \cap C_\delta$).

Claramente, $D^*_\delta = \{\gamma \in \kappa \mid \epsilon(\delta) < \gamma\} = \kappa \setminus (\epsilon(\delta) + 1)$ es c.n.a. en κ. Por consiguiente, $D_\delta = \{\gamma \in C \mid \epsilon(\delta) < \gamma\} = C \cap D^*_\delta$ es c.n.a. en κ y, a su vez, $D = \{\gamma \in C \mid \bigwedge \delta < \gamma \; \epsilon(\delta) < \gamma\} = \triangle\limits_{\delta<\kappa} D_\delta$ es c.n.a. en κ.

En consecuencia $T \cap D$ es estacionario y, en particular, tiene al menos dos elementos $\gamma < \lambda$. Veamos que

$(*)$ Si $\delta < \gamma$ y $\delta < \operatorname{cf}\lambda$, entonces $f_\lambda(\delta) < \epsilon(\delta) < \gamma$.

En efecto, $\lambda \in D$, $\lambda \in C \cap T$, $f_\lambda(\delta) < \epsilon(\delta)$ y, como $\gamma \in D$, también $\epsilon(\delta) < \gamma$.

Como f_λ es cofinal, existe un $\delta < \operatorname{cf}\lambda$ (podemos tomarlo infinito) tal que $\gamma \leq f_\lambda(\delta)$, luego —por lo que acabamos de probar— $\gamma \leq \delta < \operatorname{cf}\lambda$. En particular la condición $\delta < \operatorname{cf}\lambda$ es redundante en $(*)$, y además tenemos que $\operatorname{cf}\lambda > \aleph_0$.

Tenemos, pues, que si $\delta < \gamma$ entonces $f_\lambda(\delta) < \gamma$, luego $f_\lambda(\gamma) = \bigcup\limits_{\delta<\gamma} f_\lambda(\delta) \leq \gamma$. Como f_λ es normal tenemos, de hecho, la igualdad $f_\lambda(\gamma) = \gamma$, pero esto es imposible, pues $\gamma \in T$ y $f_\lambda(\gamma) \notin T$.

Con esto hemos encontrado un $\delta < \kappa$ tal que para todo $\epsilon < \kappa$ el conjunto F_ϵ es estacionario en κ. Sea $g : T \longrightarrow \kappa$ la función dada por $g(\lambda) = f_\lambda(\delta)$, obviamente regresiva.

Para cada $\epsilon < \kappa$ tenemos que $g|_{F_\epsilon} : F_\epsilon \longrightarrow \kappa$ es regresiva, luego por 6.15 existe un $\gamma_\epsilon < \kappa$ tal que $G_\epsilon = (g|_{F_\epsilon})^{-1}(\{\gamma_\epsilon\})$ es estacionario en κ.

Si $\lambda \in G_\epsilon$, entonces $\gamma_\epsilon = g(\lambda) = f_\lambda(\delta) \geq \epsilon$ (porque $G_\epsilon \subset F_\epsilon$). Así pues, $\bigwedge \epsilon < \kappa \; \epsilon \leq \gamma_\epsilon$.

Por consiguiente, el conjunto $B = \{\gamma_\epsilon \mid \epsilon < \kappa\}$ no está acotado en κ, luego tiene cardinal κ. Sea $h : \kappa \longrightarrow B$ biyectiva y sea $E_\alpha = G_{h(\alpha)}$. Así, los conjuntos E_α son estacionarios en κ y disjuntos dos a dos, pues si $\gamma_\epsilon \neq \gamma_{\epsilon'}$ entonces $G_\epsilon \cap G_{\epsilon'} = \varnothing$. Además $E_\alpha = G_{h(\alpha)} \subset F_{h(\alpha)} \subset T \subset A$.

Sea $U = A \setminus \bigcup\limits_{\alpha<\kappa} E_\alpha$. Podemos cambiar E_0 por $E_0 \cup U$, y así conseguimos que la unión de los E_α sea A. ∎

6.3 Un teorema de Silver

Vamos a aplicar los resultados sobre conjuntos estacionarios y cerrados no acotados para probar un importante resultado sobre la hipótesis de los cardinales singulares.

Diremos que un cardinal infinito κ cumple la HCG si $2^\kappa = \kappa^+$. Diremos que κ cumple la HCS si $2^{\operatorname{cf}\kappa} < \kappa \to \kappa^{\operatorname{cf}\kappa} = \kappa^+$.

Es claro que la HCG (resp. la HCS) equivale a que la HCG (la HCS) se cumpla en todos los cardinales.

Teorema 6.18 (Silver) *Se cumple:*

1. *Si κ es un cardinal singular de cofinalidad no numerable y los cardinales (infinitos) menores que κ cumplen la* HCG *entonces κ cumple la* HCG.
2. *Si no se cumple la* HCS, *entonces el mínimo cardinal que no la cumple tiene cofinalidad numerable.*
3. *Si la* HCS *se cumple sobre los cardinales de cofinalidad numerable, entonces se cumple sobre todos los cardinales.*

En adelante supondremos que $\aleph_0 < \mu = \operatorname{cf}\kappa < \kappa$ y que $\{\kappa_\alpha\}_{\alpha<\mu}$ es una sucesión normal de cardinales cofinal en κ.

Definición 6.19 Dos funciones f y g de dominio μ son *casi disjuntas* si el conjunto $\{\alpha < \mu \mid f(\alpha) = g(\alpha)\}$ está acotado en μ.

Una familia $\mathcal{F}$ de funciones de dominio μ es *casi disjunta* si está formada por funciones casi disjuntas dos a dos.

Teorema 6.20 *Si $\bigwedge\nu < \kappa\ \nu^\mu < \kappa$, $\mathcal{F} \subset \prod_{\alpha<\mu} A_\alpha$ es una familia casi disjunta de funciones y el conjunto $\{\alpha < \mu \mid |A_\alpha| \leq \kappa_\alpha\}$ es estacionario en μ, entonces $|\mathcal{F}| \leq \kappa$.*

Demostración: No perdemos generalidad si suponemos que los conjuntos A_α están formados por ordinales y que $\{\alpha < \mu \mid A_\alpha \subset \kappa_\alpha\}$ es estacionario en μ pues, biyectando cada A_α con su cardinal podemos construir otra $\mathcal{F}$ equipotente a la dada y en las mismas condiciones.

Sea $E_0 = \{\lambda < \mu \mid A_\lambda \subset \kappa_\lambda\}$, que es estacionario en μ, pues es la intersección del conjunto que estamos suponiendo que es estacionario con el conjunto de los ordinales límite $< \mu$, que es c.n.a.

Si $f \in \mathcal{F}$, entonces para todo $\lambda \in E_0$ tenemos que $f(\lambda) \in A_\lambda \subset \kappa_\lambda$ y como $\{\kappa_\alpha\}_{\alpha<\mu}$ es normal existe un ordinal $g(\lambda) < \lambda$ tal que $f(\lambda) \in \kappa_{g(\lambda)}$.

Como E_0 es estacionario y $g : E_0 \longrightarrow \mu$ es regresiva, el teorema 6.15 nos da un conjunto estacionario $E_f \subset E_0$ tal que g es constante en E_f: En particular f esta acotada en E_f por un $\kappa_\alpha < \kappa$.

La aplicación que a cada f le asigna $f|_{E_f}$ es inyectiva, pues si $f|_{E_f} = g|_{E_g}$ entonces $f = g$ por ser $\mathcal{F}$ casi disjunta (los conjuntos E_f y E_g son no acotados).

El número de funciones $h : E \longrightarrow \kappa_\alpha$ con $E \subset \mu$ fijo es a lo sumo (teniendo en cuenta la hipótesis)

$$\Big|\bigcup_{\alpha<\mu} \kappa_\alpha^E\Big| \leq \sum_{\alpha<\mu} \kappa_\alpha^\mu \leq \sum_{\alpha<\mu} \kappa = \kappa.$$

Como $|\mathcal{P}\mu| = 2^\mu < \kappa$, el número de funciones $h : E \longrightarrow \kappa_\alpha$ para cualquier E es a lo sumo $2^\mu \cdot \kappa = \kappa$.

Como hemos asociado a cada $f \in \mathcal{F}$ una función $h = f|_{E_f}$ distinta y a lo sumo puede haber κ funciones h, ha de ser $|\mathcal{F}| \leq \kappa$. ∎

En realidad vamos a necesitar una ligera variante de este teorema:

Teorema 6.21 *Si* $\bigwedge\nu < \kappa\ \nu^\mu < \kappa$, $\mathcal{F} \subset \prod_{\alpha<\mu} A_\alpha$ *es una familia casi disjunta de funciones y el conjunto* $\{\alpha < \mu \mid |A_\alpha| \leq \kappa_\alpha^+\}$ *es estacionario en* μ, *entonces* $|\mathcal{F}| \leq \kappa^+$.

Demostración: Como en el teorema anterior podemos suponer que los conjuntos A_α están formados por ordinales y que $E_0 = \{\alpha < \mu \mid A_\alpha \subset \kappa_\alpha^+\}$ es estacionario en μ.

Sea $f \in \mathcal{F}$ y $E \subset E_0$ estacionario. Definimos

$$\mathcal{F}_{f,E} = \{g \in \mathcal{F} \mid \bigwedge\alpha \in E\ g(\alpha) \leq f(\alpha)\}.$$

Claramente se trata de una familia casi disjunta contenida en $\prod_{\alpha<\mu} B_\alpha$, donde

$$B_\alpha = \begin{cases} f(\alpha)+1 & \text{si } \alpha \in E, \\ \kappa & \text{en caso contrario.} \end{cases}$$

Así, si $\alpha \in E \subset E_0$, tenemos que $f(\alpha) \in \kappa_\alpha^+$, luego $|B_\alpha| = |f(\alpha)+1| \leq \kappa$. Por consiguiente el conjunto $\{\alpha < \mu \mid |B_\alpha| \leq \kappa_\alpha\}$ es estacionario (contiene a E) y podemos aplicar el teorema anterior, según el cual $|\mathcal{F}_{f,E}| \leq \kappa$.

Ahora definimos

$$\mathcal{F}_f = \{g \in \mathcal{F} \mid \bigvee E \subset E_0(E \text{ estacionario} \wedge \bigwedge\alpha \in E\, g(\alpha) \leq f(\alpha))\} = \bigcup_E \mathcal{F}_{f,E},$$

donde E varía en los subconjuntos estacionarios de E_0. Claramente

$$|\mathcal{F}_f| \leq \sum_E \kappa \leq 2^\mu\kappa = \kappa.$$

Veamos finalmente que $|\mathcal{F}| \leq \kappa^+$. En otro caso tomemos $\{f_\alpha\}_{\alpha<\kappa^+}$ funciones distintas en $\mathcal{F}$. Tenemos que $\Big|\bigcup_{\alpha<\kappa^+} \mathcal{F}_\alpha\Big| \leq \sum_{\alpha<\kappa^+} \kappa = \kappa^+$, luego ha de existir una función $f \in \mathcal{F} \setminus \bigcup_{\alpha<\kappa^+} \mathcal{F}_\alpha$.

En tal caso el conjunto $\{\gamma \in E_0 \mid f(\gamma) \leq f_\alpha(\gamma)\}$ no es estacionario para ningún $\alpha < \kappa^+$, luego su complementario $\{\gamma \in E_0 \mid f_\alpha(\gamma) \leq f(\gamma)\}$ sí lo es, y esto significa que cada $f_\alpha \in \mathcal{F}_f$, lo cual es imposible, dado que hay κ^+ funciones f_α y $|\mathcal{F}_f| \leq \kappa$. ∎

El apartado 1) del teorema de Silver es un caso particular del teorema siguiente:

Teorema 6.22 *Si el conjunto* $\{\alpha < \mu \mid 2^{\kappa_\alpha} = \kappa_\alpha^+\}$ *es estacionario en* μ, *entonces* $2^\kappa = \kappa^+$.

DEMOSTRACIÓN: Veamos que $\bigwedge\nu < \kappa\ \nu^\mu < \kappa$. En efecto, si $\nu < \kappa$ sea α tal que $\nu,\ \mu < \kappa_\alpha$ y $2^{\kappa_\alpha} = \kappa_\alpha^+$. Entonces $\nu^\mu \le \kappa_\alpha^{\kappa_\alpha} = 2^{\kappa_\alpha} = \kappa_\alpha^+ \le \kappa_{\alpha+1} < \kappa$.

Para cada $X \subset \kappa$ sea $f_X = \{X_\alpha\}_{\alpha<\mu}$, donde $X_\alpha = X \cap \kappa_\alpha$. Definimos $\mathcal{F} = \{f_X \mid X \subset \kappa\}$. Si $X \ne Y$ entonces f_X y f_Y son casi disjuntas, pues ha de existir un α tal que $X \cap \kappa_\alpha \ne Y \cap \kappa_\alpha$ y entonces $\{\delta < \mu \mid f_X(\delta) = f_Y(\delta)\} \subset \alpha$. En particular, si $X \ne Y$ entonces $f_X \ne f_Y$, luego $|\mathcal{F}| = 2^\kappa$.

Por otra parte $\mathcal{F}$ es una familia casi disjunta de funciones contenida en $\prod_{\alpha<\mu} \mathcal{P}\kappa_\alpha$ y el conjunto $\{\alpha < \mu \mid |\mathcal{P}\kappa_\alpha| = \kappa_\alpha^+\}$ es estacionario en μ. El teorema anterior nos da, entonces, que $2^\kappa = |\mathcal{F}| \le \kappa^+$. ∎

Para probar el resto del teorema de Silver necesitamos un paso más:

Teorema 6.23 *Si $\bigwedge\nu < \kappa\ \nu^\mu < \kappa$ y el conjunto $\{\alpha < \mu \mid \kappa_\alpha^{\mathrm{cf}\,\kappa_\alpha} = \kappa_\alpha^+\}$ es estacionario en μ, entonces $\kappa^\mu = \kappa^+$.*

DEMOSTRACIÓN: Para cada $h : \mu \longrightarrow \kappa$ sea $f_h = \{h_\alpha\}_{\alpha<\mu}$, donde las aplicaciones $h_\alpha : \mu \longrightarrow \kappa$ vienen dadas por

$$h_\alpha(\beta) = \begin{cases} h(\beta) & \text{si } h(\beta) < \kappa_\alpha, \\ 0 & \text{en otro caso.} \end{cases}$$

Sea $\mathcal{F} = \{f_h \mid h \in {}^\mu\kappa\}$. Si $h \ne g$, entonces f_g y f_h son casi disjuntas, pues si $h(\delta) \ne g(\delta)$ y ambos son menores que κ_α, entonces

$$\{\delta < \mu \mid f_h(\delta) = f_g(\delta)\} \subset \alpha + 1.$$

En particular si $h \ne g$ se cumple $f_h \ne f_g$, luego $|\mathcal{F}| = \kappa^\mu$. Además $\mathcal{F}$ es casi disjunta y está contenida en $\prod_{\alpha<\mu} {}^\mu\kappa_\alpha$.

Queremos aplicar el teorema 6.21 para concluir que $\kappa^\mu = |\mathcal{F}| \le \kappa^+$. Necesitamos, pues, probar que el conjunto $E = \{\alpha < \mu \mid \kappa_\alpha^\mu = \kappa_\alpha^+\}$ es estacionario en μ. Para ello consideramos el conjunto

$$C = \{\lambda < \mu \mid \textstyle\bigwedge\nu < \kappa_\lambda\ \nu^\mu < \kappa_\lambda\}.$$

Veamos que si $\lambda \in C$ entonces $\kappa_\lambda^{\mathrm{cf}\,\kappa_\lambda} = \kappa_\lambda^\mu$. De aquí se seguirá que

$$\{\alpha < \mu \mid \kappa_\alpha^{\mathrm{cf}\,\kappa_\alpha} = \kappa_\alpha^+\} \cap C \subset E$$

y, como el conjunto de la izquierda es estacionario por hipótesis, si probamos también que C es c.n.a., concluiremos que E es estacionario, tal y como nos hace falta.

Sea, pues, $\lambda \in C$. Entonces $\mathrm{cf}\,\kappa_\lambda = \mathrm{cf}\,\lambda \le \lambda < \mu$. Sea $\kappa_\lambda = \sum_{\alpha<\mathrm{cf}\,\kappa_\lambda} \nu_\alpha$, donde $\bigwedge\alpha < \mathrm{cf}\,\kappa_\lambda\ \nu_\alpha < \kappa_\lambda$. Así

$$\kappa_\lambda^{\mathrm{cf}\,\kappa_\lambda} \le \kappa_\lambda^\mu = \Big(\sum_{\alpha<\mathrm{cf}\,\kappa_\lambda} \nu_\alpha\Big)^\mu \le \prod_{\alpha<\mathrm{cf}\,\kappa_\lambda} \nu_\alpha^\mu \le \prod_{\alpha<\mathrm{cf}\,\kappa_\lambda} \kappa_\lambda = \kappa_\lambda^{\mathrm{cf}\,\kappa_\lambda}.$$

Según lo dicho, ahora sólo queda probar que C es c.n.a. en μ. Para ello definimos $l : \mu \longrightarrow \mu$ mediante

$$l(\alpha) = \text{mín}\{\beta < \mu \mid \kappa_\alpha^\mu < \kappa_\beta\}.$$

Basta probar que

$$C = \{\lambda \mid \lambda < \mu\} \cap \{\alpha < \mu \mid l[\alpha] \subset \alpha\}.$$

En efecto, si $\lambda \in C$ y $\alpha < \lambda$, entonces $\kappa_\alpha^\mu < \kappa_\lambda$, existe un $\beta < \lambda$ tal que $\kappa_\alpha^\mu < \kappa_\beta$, luego $l(\alpha) \leq \beta < \lambda$. Por lo tanto $l[\lambda] \subset \lambda$.

Recíprocamente, si $l[\lambda] \subset \lambda$ y $\nu < \kappa_\lambda$, sea $\alpha < \lambda$ tal que $\nu < \kappa_\alpha$. Entonces $\nu^\mu \leq \kappa_\alpha^\mu < \kappa_{l(\alpha)} < \kappa_\lambda$, luego $\lambda \in C$. ∎

Ahora estamos en condiciones de probar el apartado 2) del teorema de Silver, y el apartado 3) es una consecuencia inmediata. Sea κ el mínimo cardinal que incumple la HCS, es decir, $\kappa > \aleph_0$, $2^{\text{cf}\,\kappa} < \kappa$, pero $\kappa^{\text{cf}\,\kappa} > \kappa^+$. Supongamos que $\text{cf}\,\kappa > \aleph_0$.

Sea $\mu = \text{cf}\,\kappa$ y $\{\kappa_\alpha\}_{\alpha<\mu}$ como en los teoremas precedentes. Tenemos que la HCS se cumple bajo κ, luego el argumento del teorema 5.78 es válido en este contexto y nos permite probar que si $\nu < \kappa$ entonces ν^μ toma uno de los valores 2^μ, μ o μ^+, luego en particular $\bigwedge\nu < \kappa\ \nu^\mu < \kappa$.

Sea $E = \{\alpha < \mu \mid \text{cf}\,\kappa_\alpha = \aleph_0 \wedge 2^{\aleph_0} < \kappa_\alpha\}$. Es claro que E es estacionario en μ, pues contiene a la intersección del c.n.a. $\mu \setminus \alpha_0$, donde α_0 es el mínimo ordinal tal que $2^{\aleph_0} < \kappa_{\alpha_0}$, con el conjunto $\{\lambda < \mu \mid \text{cf}\,\lambda\ (= \text{cf}\,\kappa_\lambda) = \aleph_0\}$, el cual es estacionario por el teorema 6.13.

Si $\alpha \in E$, entonces $2^{\text{cf}\,\kappa_\alpha} < \kappa_\alpha$, con $\text{cf}\,\kappa_\alpha = \aleph_0$ y, como $\kappa_\alpha < \kappa$ cumple la HCS, $\kappa_\alpha^{\text{cf}\,\kappa_\alpha} = \kappa_\alpha^+$, de modo que $E \subset \{\alpha < \mu \mid \kappa_\alpha^{\text{cf}\,\kappa_\alpha} = \kappa_\alpha^+\}$. Concluimos que este último conjunto es estacionario y ello nos permite aplicar el teorema anterior, según el cual $\kappa^{\text{cf}\,\kappa} = \kappa^+$. ∎

Tenemos así un ejemplo no trivial de las numerosas restricciones que se conocen sobre la función del continuo en cardinales singulares. Por ejemplo, si suponemos que $\bigwedge\alpha < \omega_1\ 2^{\aleph_\alpha} = \aleph_{\alpha+1}$, entonces necesariamente $2^{\aleph_{\omega_1}} = \aleph_{\omega_1+1}$. En cambio, aunque supongamos

$$\bigwedge n \in \omega\ 2^{\aleph_n} = \aleph_{n+1}$$

no podemos demostrar —aunque no es fácil probar que así es— que $2^{\aleph_\omega} = \aleph_{\omega+1}$, es decir, la HCS no puede demostrarse ni siquiera para $\aleph_\omega$. Esto no significa que $2^{\aleph_\omega}$ esté libre de este tipo de restricciones. Por ejemplo, un profundo teorema de S. Shelah de 1982 afirma que, para todo ordinal límite λ:

$$\aleph_\lambda^{\text{cf}\,\lambda} < \aleph_{(|\lambda|^{\text{cf}\,\lambda})^+}.$$

En particular, si $\bigwedge n \in \omega\ 2^{\aleph_n} < \aleph_\omega$, entonces $2^{\aleph_\omega} = \aleph_\omega^{\aleph_0} < \aleph_{(2^{\aleph_0})^+}$.

Más sorprendente aún es otro teorema de Shelah de 1990, según el cual, si $2^{\aleph_0} < \aleph_\omega$ entonces $\aleph_\omega^{\aleph_0} < \aleph_{\omega_4}$, con lo que, por 5.70, si $\bigwedge n \in \omega\ 2^{\aleph_n} < \aleph_\omega$, necesariamente $2^{\aleph_\omega} < \aleph_{\omega_4}$. Estos resultados son algunas consecuencias de la llamada teoría de las cofinalidades posibles, descubierta por Shelah y que tiene muchas más consecuencias en muchas ramas de la teoría de conjuntos.

6.4 Cardinales de Mahlo

Los conjuntos estacionarios intervienen también en la definición de una familia de los llamados "cardinales grandes", cardinales cuya existencia no puede ser demostrada porque son "innecesarios" para que se cumplan los axiomas de la teoría de conjuntos. Ya hemos discutido los menores de ellos, los cardinales inaccesibles. Los siguientes en la jerarquía son los cardinales de Mahlo, que ahora vamos a introducir.

Definición 6.24 Un cardinal κ es *(débilmente) de Mahlo* si κ es (débilmente) inaccesible y el conjunto $\{\mu < \kappa \mid \mu \text{ es regular}\}$ es estacionario en κ.

En realidad los cardinales de Mahlo cumplen mucho más de lo que exige la definición:

Teorema 6.25 *Si κ es un cardinal (débilmente) de Mahlo, entonces el conjunto $\{\mu < \kappa \mid \mu$ es (débilmente) inaccesible$\}$ es estacionario en κ.*

Demostración: Basta ver que el conjunto

$$C = \{\mu < \kappa \mid \mu \text{ es un cardinal límite fuerte (resp. límite)}\}$$

es c.n.a. en κ, pues el conjunto del enunciado es la intersección con C del conjunto de la definición de cardinal de Mahlo.

El conjunto C es cerrado porque el supremo de un conjunto no acotado de cardinales es un cardinal límite, y si los cardinales son límites fuertes el supremo también lo es.

Si $\alpha < \kappa$, sea $\mu_0 = \alpha^+$ y definimos $\bigwedge n \in \omega\ \mu_{n+1} = \mu_n^+$ (respectivamente $\bigwedge n \in \omega\ \mu_{n+1} = 2^{\mu_n}$). Como κ es un cardinal límite (fuerte), se cumple que $\bigwedge n \in \omega\ \mu_n \in \kappa$ y, como κ es regular, $\mu = \sup\limits_{n\in\omega} \mu_n \in \kappa$. Claramente μ es un cardinal límite (fuerte), de modo que $\mu \in C \wedge \alpha < \mu$. Así pues, C no está acotado en κ. ∎

Se suele decir que un cardinal de Mahlo es "mas grande" que un cardinal inaccesible, pero esto no ha de ser entendido en sentido literal: pueden existir cardinales $\kappa < \mu$ de modo que κ sea de Mahlo y μ sea (meramente) inaccesible. La comparación debe entenderse en dos sentidos: por una parte, el mínimo cardinal de Mahlo κ (si existe) ha de ser mucho mayor que el mínimo cardinal inaccesible, pues κ ha de dejar bajo sí un conjunto estacionario de cardinales inaccesibles; por otra parte, también se dice que un cardinal de Mahlo es "más grande" en el sentido de que implica la existencia de muchos cardinales inaccesibles, es decir, en el sentido de que suponer la existencia de un cardinal de Mahlo es "más fuerte" que suponer la existencia de un cardinal inaccesible.

Por el mismo razonamiento que empleamos con los cardinales inaccesibles, a partir de la existencia de un cardinal de Mahlo no puede probarse la existencia de dos de ellos, por lo que postular que existen dos es un axioma más fuerte que postular que existe uno. Pero podemos ir mucho más allá:

Definición 6.26 Sea γ un ordinal infinito. Definimos los conjuntos

$$\begin{aligned} M_0(\gamma) &= \{\kappa < \gamma \mid \kappa \text{ es (débilmente) inaccesible}\},\\ M_{\alpha+1}(\gamma) &= \{\kappa \in M_\alpha(\gamma) \mid \{\mu < \kappa \mid \mu \in M_\alpha(\gamma)\} \text{ es estacionario en } \kappa\},\\ M_\lambda(\gamma) &= \bigcap_{\delta<\lambda} M_\delta(\gamma). \end{aligned}$$

Definimos las clases

$$M_\alpha = \bigcup_{\gamma\in\Omega} M_\alpha(\gamma).$$

A los elementos de M_α los llamaremos cardinales (débilmente) α-Mahlo. El ordinal γ que aparece en la definición es un auxiliar técnico para evitar una recurrencia con clases propias que no estaría justificada, pero se comprueba inmediatamente lo siguiente:

Para todo cardinal infinito κ:

- κ es (débilmente) 0-Mahlo si y sólo si es (débilmente) inaccesible.
- κ es (débilmente) $\alpha+1$-Mahlo si y sólo si es (débilmente) α-Mahlo y el conjunto $\{\mu < \kappa \mid \mu$ es (débilmente) α-Mahlo$\}$ es estacionario en κ.
- κ es (débilmente) λ-Mahlo si y sólo si es (débilmente) δ-Mahlo para todo $\delta < \lambda$.

De este modo, los cardinales (débilmente) de Mahlo son precisamente los (débilmente) 1-Mahlo. Es fácil ver que la situación en cuanto a consistencia de los cardinales 2-Mahlo respecto a los 1-Mahlo es la misma que la de los 1-Mahlo respecto a los inaccesibles, con lo que tenemos una escala de cardinales grandes.

Notemos que si κ es un cardinal (débilmente) α-mahlo y para cada $\beta < \alpha$ llamamos μ_β al menor cardinal (débilmente) β-Mahlo, entonces la aplicación $f : \alpha \longrightarrow \kappa$ dada por $f(\beta) = \mu_\beta$ es inyectiva y creciente, luego $\alpha \leq \kappa$. Así pues, un cardinal κ puede a lo sumo ser (débilmente) κ-Mahlo, pero nunca $\kappa+1$-Mahlo.

Esto no significa que los cardinales (débilmente) κ-Mahlo sean "los mayores posibles". Por ejemplo, en la escala de los llamados "cardinales grandes" tienen por encima a los llamados "cardinales débilmente compactos", que estudiaremos en el capítulo XI, de modo que si un cardinal κ es débilmente compacto, el conjunto $\{\mu < \kappa \mid \mu$ es μ-Mahlo$\}$ es estacionario en κ.

Nota Como ya hemos indicado, no es posible demostrar en NBG la existencia de cardinales de ninguno de los tipos que acabamos de definir, lo cual equivale a que podemos suponer que no existen sin que ello pueda introducir ninguna contradicción en la teoría. Cabe entonces preguntarse si, en sentido contrario, es consistente suponer que existen, es decir, si el axioma que afirma la existencia de un cardinal de Mahlo, o de un cardinal κ que sea κ-Mahlo no da lugar a contradicciones. La respuesta es que, si bien es plausible que así sea, es decir,

que no haya contradicción alguna en suponer la existencia de cardinales de estos tipos, no es posible demostrar tal cosa. Más aún, aun suponiendo que NBG más la existencia de un cardinal de Mahlo sea consistente, no podemos probar a partir de ahí que también lo es NBG más la existencia de un cardinal 2-Mahlo, y así sucesivamente.

De este modo, las teorías que resultan de extender NBG añadiendo axiomas cada vez más fuertes sobre existencia de cardinales grandes (la existencia de un cardinal de Mahlo, la existencia de dos cardinales de Mahlo, la existencia de un cardinal 2-Mahlo, etc.) forman una escala de teorías cada vez "más fuertes" en el sentido de que la consistencia de cualquiera de ellas no puede demostrarse ni aunque se suponga la consistencia de las anteriores en la escala.

Esto mismo vale en general para todos los llamados "cardinales grandes", de los cuales los cardinales α-Mahlo son sólo los "más pequeños", y precisamente en ello radica su interés, pues hay muchas afirmaciones conjuntistas, que en principio no tienen nada que ver con cardinales grandes, que no son demostrables en NBG, pero cuya consistencia no puede demostrarse ni siquiera suponiendo la consistencia de NBG, porque es "más fuerte" que ésta. En tal caso, dicha consistencia sólo puede probarse suponiendo la consistencia de NBG más la existencia de uno o varios cardinales grandes "del tamaño adecuado".

Por ejemplo, la negación de la HCS implica la existencia de ciertos cardinales grandes, luego si es consistente NBG + ¬HCS también lo es NBG más la existencia de tales cardinales, y como esto no puede demostrarse a partir de la mera consistencia de NBG, lo máximo que puede probarse respecto de la consistencia de ¬HCS es que si NBG más la existencia de ciertos cardinales grandes es consistente, también lo es NBG + ¬HCS. ∎

6.5 Principios combinatorios

Otro contexto en el que aparecen los conjuntos c.n.a.s y estacionarios es en la formulación de los llamados "principios combinatorios". No existe una definición precisa, pero se conoce con este nombre a una serie de afirmaciones de "aspecto similar" (aunque unas son más fuertes que otras) que tienen entre sus características comunes el no ser demostrables en NBG, pero, al contrario de lo que sucede con los axiomas que postulan la existencia de cardinales grandes, cuya consistencia no puede ser demostrada, sí que es posible demostrar[1] que si NBG es consistente, también lo es la teoría que resulta de añadir como axioma cualquiera de los principios combinatorios que vamos a considerar (o todos ellos a la vez). Por lo tanto, cualquier teorema que se demuestre suponiendo uno o varios principios combinatorios, no será necesariamente un teorema de NBG, pero sabremos que su conclusión no puede ser refutada en NBG (si es que NBG es consistente).

En cierta medida, todos los principios combinatorios que vamos a considerar son generalizaciones o variantes del diamante de Jensen:

[1] Más concretamente, todos son demostrables a partir del axioma de constructibilidad, $V = L$, que puede probarse que es consistente con NBG.

($\diamondsuit$) *Existe una sucesión* $\{A_\alpha\}_{\alpha<\omega_1}$ *tal que* $\bigwedge\alpha<\omega_1\ A_\alpha\subset\alpha$ *y que verifica*

$$\bigwedge A\subset\omega_1\ \{\alpha<\omega_1\mid A\cap\alpha=A_\alpha\}\ \textit{es estacionario en}\ \omega_1.$$

A las sucesiones $\{A_\alpha\}_{\alpha<\omega_1}$ que cumplen $\diamondsuit$ se las llama sucesiones $\diamondsuit$ (diamante).

Veamos algunas de estas generalizaciones y variantes:

Definición 6.27 Sea κ un cardinal regular no numerable, para cada $E\subset\kappa$ estacionario consideramos las sentencias:

($\diamondsuit_E$) Existe una sucesión $\{A_\alpha\}_{\alpha\in E}$ tal que $\bigwedge\alpha\in E\ A_\alpha\subset\alpha$ y que verifica

$$\bigwedge A\subset\kappa\ \{\alpha\in E\mid A\cap\alpha=A_\alpha\}\ \text{es estacionario en}\ \kappa.$$

($\diamondsuit'_E$) Existe una sucesión $\{S_\alpha\}_{\alpha\in E}$ tal que $\bigwedge\alpha\in E\ (S_\alpha\subset\mathcal{P}\alpha\wedge|S_\alpha|<\kappa)$ y que verifica

$$\bigwedge A\subset\kappa\ \{\alpha\in E\mid A\cap\alpha\in S_\alpha\}\ \text{es estacionario en}\ \kappa.$$

($\diamondsuit^*_\kappa$) Existe una sucesión $\{S_\alpha\}_{\alpha\in\kappa}$ tal que $\bigwedge\alpha\in\kappa\ (S_\alpha\subset\mathcal{P}\alpha\wedge|S_\alpha|<\kappa)$ y que verifica

$$\bigwedge A\subset\kappa\bigvee C\ (C\ \text{c.n.a. en}\ \kappa\wedge C\subset\{\alpha\in\kappa\mid A\cap\alpha\in S_\alpha\}).$$

($\diamondsuit^+_\kappa$) Existe una sucesión $\{S_\alpha\}_{\alpha\in\kappa}$ tal que $\bigwedge\alpha\in\kappa\ (S_\alpha\subset\mathcal{P}\alpha\wedge|S_\alpha|<\kappa)$ y que verifica

$$\bigwedge A\subset\kappa\bigvee C\ (C\ \text{c.n.a. en}\ \kappa\wedge C\subset\{\alpha\in\kappa\mid A\cap\alpha\in S_\alpha\wedge C\cap\alpha\in S_\alpha\}).$$

A las sucesiones que cumplen estas propiedades se las llama, respectivamente sucesiones $\diamondsuit_E$, $\diamondsuit'_E$, $\diamondsuit^*_\kappa$, $\diamondsuit^+_\kappa$. En particular se llama $\diamondsuit$, $\diamondsuit'$, etc. a $\diamondsuit_{\omega_1}$, $\diamondsuit'_{\omega_1}$, etc.

Podríamos haber enunciado principios $\diamondsuit^*_E$ y $\diamondsuit^+_E$, para conjuntos estacionarios $E\subset\kappa$, como hemos hecho con $\diamondsuit_E$ y $\diamondsuit'_E$, pero no los vamos a necesitar, así que para ambos principios nos limitaremos a considerar el caso $E=\kappa$. Además, aunque los hemos definido para cardinales regulares cualesquiera, limitaremos nuestro estudio principalmente al caso de los cardinales sucesores.

En el capítulo IX veremos varias aplicaciones de estos principios combinatorios. Aquí estudiaremos las relaciones entre ellos y la aritmética cardinal.

Los hemos presentado todos a la vez para que resulte más fácil compararlos, pero vamos a estudiarlos uno a uno, empezando por $\diamondsuit_E$. Notemos en primer lugar que si $E\subset E'$ son estacionarios en κ entonces $\diamondsuit_E\to\diamondsuit_{E'}$, pues si completamos una sucesión $\diamondsuit_E$ de cualquier modo, por ejemplo, haciendo $A_\alpha=\varnothing$ para $\alpha\in E'\setminus E$, obtenemos una sucesión $\diamondsuit_{E'}$, luego $\diamondsuit_E$ es "más fuerte" cuanto menor es E y así $\diamondsuit_\kappa$ es el más débil de todos los diamantes sobre κ.

Observamos que la condición $\bigwedge\alpha\in E\ A_\alpha\subset\alpha$ se puede suprimir de la definición de $\diamondsuit_E$, pues si una sucesión cumple las condiciones de $\diamondsuit_E$ excepto ésa, entonces $\{A_\alpha\cap\alpha\}_{\alpha\in E}$ es una sucesión $\diamondsuit_E$, ya que en la condición principal da igual escribir A_α que $A_\alpha\cap\alpha$.

El teorema siguiente muestra que los diamantes no pueden demostrarse en NBG:

Teorema 6.28 *Si κ es un cardinal infinito, entonces $\diamondsuit_{\kappa^+} \to 2^\kappa = \kappa^+$.*

DEMOSTRACIÓN: Sea $\{A_\alpha\}_{\alpha<\kappa^+}$ una sucesión $\diamondsuit_{\kappa^+}$. Si $A \subset \kappa$, el conjunto $\{\alpha < \kappa^+ \mid A \cap \alpha = A_\alpha\}$ es estacionario, luego no está acotado, luego contiene un $\alpha > \kappa$, de modo que $A = A \cap \alpha = A_\alpha$. Esto prueba que $\mathcal{P}\kappa \subset \{A_\alpha \mid \alpha \in \kappa^+\}$, luego $|\mathcal{P}\kappa| \leq \kappa^+$, luego $2^\kappa = \kappa^+$. ∎

Veamos ahora que, para $\kappa > \omega$, la implicación del teorema anterior es reversible:

Teorema 6.29 (Shelah) *Sea κ un cardinal tal que $2^\kappa = \kappa^+$. Entonces se cumple $\diamondsuit_E$ para todo conjunto estacionario en κ^+ tal que*

$$E \subset \{\delta < \kappa^+ \mid \operatorname{cf}\delta \neq \operatorname{cf}\kappa\}.$$

En particular, para todo cardinal $\kappa > \omega$, se cumple $\diamondsuit_{\kappa^+} \leftrightarrow 2^\kappa = \kappa^+$.

DEMOSTRACIÓN: La parte final se debe a que si $\kappa > \omega$ y $\operatorname{cf}\kappa > \aleph_0$, por 6.13 sabemos que

$$E = \{\delta < \kappa^+ \mid \operatorname{cf}\delta = \aleph_0\}$$

es estacionario en κ^+ y, cumple las condiciones del teorema, luego si $2^\kappa = \kappa^+$ tenemos $\diamondsuit_E$ y en particular $\diamondsuit_{\kappa^+}$. En el caso en que $\operatorname{cf}\kappa = \aleph_0$ definimos E con $\aleph_1$ en lugar de $\aleph_0$ y concluimos igualmente.

Para probar la primera parte, observamos que el conjunto C_0 de los ordinales límite $\kappa < \lambda < \kappa^+$ es cerrado no acotado en κ^+, luego $E_0 = E \cap C_0$ es estacionario, y basta probar $\diamondsuit_{E_0}$. Equivalentemente, podemos suponer que E está formado únicamente por ordinales límite mayores que κ.

Sea $\mu = \operatorname{cf}\kappa$. Observemos que si $\delta \in E$ entonces $\operatorname{cf}\delta < \kappa$, por hipótesis si $\mu = \kappa$ o porque κ es singular si $\mu < \kappa$ y las cofinalidades son siempre regulares. Fijemos $f : \mu \longrightarrow \kappa$ cofinal creciente, de modo que $\kappa = \bigcup\{f(i) \mid i < \mu\}$. Para cada $\delta \in E$, sea $g : \delta \longrightarrow \kappa$ biyectiva y sea $A_i^\delta = g^{-1}[f(i)]$, de modo que $\{A_i^\delta\}_{i<\mu}$ es una sucesión creciente en $[\delta]^{<\kappa}$ cuya unión es δ.

Como $\operatorname{cf}\delta < \kappa$ podemos añadir a cada A_i^δ un conjunto cofinal en δ y así todos los A_i^δ son cofinales en δ. Por otra parte,

$$|[\mu \times \kappa \times \kappa^+]^{<\kappa^+}| = (\kappa^+)^{<\kappa^+} = (\kappa^+)^\kappa = (2^\kappa)^\kappa = \kappa^+,$$

luego podemos tomar una enumeración $\{X_\beta\}_{\beta<\kappa^+}$ de $[\mu \times \kappa \times \kappa^+]^{<\kappa^+}$.

Si $X \subset \mu \times \kappa \times \kappa^+$, llamamos $(X)_i = \{(\alpha, \alpha') < \kappa \times \kappa^+ \mid (i, \alpha, \alpha') \in X\}$.

Vamos a probar que existe un $i < \mu$ tal que, para todo $Z \subset \kappa \times \kappa^+$ el conjunto siguiente es estacionario:

$$E_{i,Z} = \{\delta \in E \mid \sup\{\alpha \in A_i^\delta \mid \bigvee\beta \in A_i^\delta (Z \cap (\kappa \times \alpha) = (X_\beta)_i)\} = \delta\}.$$

En efecto, suponemos que no se cumple esto. Entonces, para cada $i < \mu$ existe un $Z_i \subset \kappa \times \kappa^+$ y un c.n.a. $C_i \subset \kappa^+$ tal que $C_i \cap E_{i,Z_i} = \varnothing$. Definimos $f : \kappa^+ \longrightarrow \kappa^+$ mediante

$$f(\alpha) = \text{mín}\{\beta < \kappa^+ \mid X_\beta = \bigcup_{j<\mu} (\{j\} \times (Z_j \cap (\kappa \times \alpha)))\}.$$

Por el teorema 6.7, el conjunto $C^* = \{\delta \in \kappa^+ \mid f[\delta] \subset \delta\}$ es c.n.a. en κ^+, y también lo es $C = \bigcap_{i<\kappa} C_i \cap C^*$. Así, si $\delta \in C$ se cumple que

$$A_0^\delta = \{\alpha \in A_0^\delta \mid \bigvee \beta < \delta \bigwedge j < \mu (Z_i \cap (\kappa \times \alpha) = (X_\beta)_j)\}.$$

Como E es estacionario, podemos tomar $\delta \in E \cap C$. Para cada $i < \mu$ sea

$$B_i^\delta = \{\alpha \in A_0^\delta \mid \bigvee \beta \in A_i^\delta \bigwedge j < \mu (Z_j \cap (\kappa \times \alpha) = (X_\beta)_j)\}.$$

Entonces $A_0^\delta = \bigcup_{i<\mu} B_i^\delta$. Si, para todo $i < \mu$, se cumpliera que $\xi_i = \sup B_i^\delta < \delta$, como A_0^δ no está acotado en δ, la sucesión $\{\xi_i\}_{i<\mu}$ sería cofinal en δ y creciente (pues como la sucesión A_i^δ es creciente B_i^δ también lo es, así como la sucesión de sus supremos), y concluimos que $\operatorname{cf} \delta = \mu$, contradicción. Así pues, existe un $i < \mu$ tal que $\sup B_i^\delta = \delta$. En particular, como $A_0^\delta \subset A_i^\delta$,

$$\sup\{\alpha \in A_i^\delta \mid \bigvee \beta \in A_i^\delta \bigwedge j < \mu (Z_j \cap (\kappa \times \alpha) = (X_\beta)_j)\} = \delta,$$

pero esto quiere decir que $\delta \in E_{i,Z_i}$, en contradicción con que $\delta \in C_i$.

Así pues, fijado el $i < \mu$ cuya existencia acabamos de probar, llamamos $A_\delta = A_i^\delta$ y $X_\beta \subset \kappa \times \kappa^+$ al conjunto que hasta ahora llamábamos $(X_\beta)_i$. De este modo tenemos una sucesión $\{A_\delta\}_{\delta \in E}$ con $A_\delta \subset \delta$ y $|A_\delta| < \kappa$ y una sucesión $\{X_\beta\}_{\beta<\kappa^+}$ que recorre todos los elementos de $[\kappa \times \kappa^+]^{<\kappa^+}$ (tal vez con repeticiones) de modo que para todo $Z \subset \kappa \times \kappa^+$ el conjunto siguiente es estacionario:

$$E_Z = \{\delta \in E \mid \sup\{\alpha \in A_\delta \mid \bigvee \beta \in A_\delta (Z \cap (\kappa \times \alpha) = X_\beta)\} = \delta\}.$$

Para cada $\tau < \kappa$ definimos $(X_\beta)_\tau = \{\sigma \mid (\tau, \sigma) \in X_\beta\}$.

Ahora vamos a definir recurrentemente una sucesión $\{(Y_\tau, C_\tau)\}_{\tau<\kappa}$ de pares de subconjuntos de κ^+ de modo que la sucesión $\{C_\tau\}_{\tau<\kappa}$ es decreciente y sus elementos son subconjuntos c.n.a. en κ^+.

Tomamos $Y_0 = C_0 = \kappa^+$. Supongamos definida la sucesión $\{(Y_\tau, C_\tau)\}_{\tau<\gamma}$, para $\gamma < \kappa$, no nulo. Para cada $\delta \in E$ definimos

$$V_\gamma^\delta = \{(\alpha, \beta) \in A_\delta \times A_\delta \mid \bigwedge \tau < \gamma \; Y_\tau \cap \alpha = (X_\beta)_\tau\}.$$

Notemos que si prolongamos la sucesión $\{Y_\tau\}_{\tau<\gamma}$ con cualquier conjunto $Y_\gamma \subset \kappa^+$, se va a cumplir, para todo $\delta \in E$, que $V_{\gamma+1}^\delta \subset V_\gamma^\delta$. Si se puede elegir Y_γ

de modo que exista un c.n.a. $C_\gamma \subset \bigcap_{\tau<\gamma} C_\tau$ tal que, para todo $\delta \in E \cap C_\gamma$ que cumpla

$$\sup\{\alpha < \delta \mid \bigvee \beta < \delta\ (\alpha, \beta) \in V^\delta_{\gamma+1}\} = \delta,$$

se tiene que $V^\delta_{\gamma+1} \subsetneq V^\delta_\gamma$, entonces prolongamos la sucesión con (Y_γ, C_γ). En caso contrario la sucesión termina.

Vamos a probar que la sucesión tiene que terminar en algún $\gamma^* < \kappa$. En caso contrario habríamos construido una sucesión $\{(Y_\tau, C_\tau)\}_{\tau<\kappa}$ de modo que $C = \bigcap_{\tau<\kappa} C_\tau$ sería un c.n.a. en κ^+. Definimos

$$Z = \bigcup_{\tau<\kappa} \{\tau\} \times Y_\tau.$$

Tomamos $\delta \in E_Z \cap C$. Por la definición de E_Z se cumple que

$$\sup\{\alpha \in A_\delta \mid \bigvee \beta \in A_\delta (Z \cap (\kappa \times \alpha) = X_\beta)\} = \delta,$$

que es lo mismo que

$$\sup\{\alpha \in A_\delta \mid \bigvee \beta \in A_\delta \bigwedge \tau < \kappa\ Y_\tau \cap \alpha = (X_\beta)_\tau\} = \delta.$$

Entonces, para todo $\gamma < \kappa$,

$$\sup\{\alpha < \delta \mid \bigvee \beta < \delta\ (\alpha, \beta) \in V^\delta_{\gamma+1}\} = \delta.$$

Entonces, la construcción de la sucesión implica que $\{Y^\delta_\gamma\}_{\gamma<\kappa}$ es estrictamente decreciente en $A_\delta \times A_\delta$, pero esto es imposible, pues $|A_\delta \times A_\delta| < \kappa$.

Fijamos, pues $\gamma^* < \kappa$ tal que la sucesión $\{(Y_\tau, C_\tau)\}_{\tau<\gamma^*}$ ya no puede prolongarse más, sea $C^* = \bigcap_{\tau<\gamma^*} C_\tau$, que es c.n.a. en κ^+, y para cada $\delta \in E \cap C^*$ sea

$$S_\delta = \bigcup_{(\alpha,\beta)\in V^\delta_{\gamma^*}} (X_\beta)_{\gamma^*}.$$

Finalmente, veamos que $\{S_\delta\}_{\delta\in E\cap C^*}$ es una sucesión $\diamondsuit_{E\cap C^*}$, lo que implica $\diamondsuit_E$.

En caso contrario existe un $Y \subset \kappa^+$ y un c.n.a. $C \subset C^*$ tal que

$$\bigwedge \delta \in C \cap E\ S_\delta \neq Y \cap \delta.$$

Para obtener una contradicción, basta probar que la sucesión se puede prolongar tomando $Y_{\gamma^*} = Y$, $C_{\gamma^*} = C$.

Para ello tomamos un $\delta \in E \cap C_{\gamma^*}$ que cumpla

$$\sup\{\alpha < \delta \mid \bigvee \beta < \delta\ (\alpha, \beta) \in V^\delta_{\gamma^*+1}\} = \delta.$$

Esto equivale a

$$\sup\{\alpha \in A_\delta \mid \bigvee \beta \in A_\delta \bigwedge \tau \leq \gamma^*\ Y_\tau \cap \alpha = (X_\beta)_\tau\} = \delta.$$

Por lo tanto, $\sup\{\alpha < \delta \mid \bigvee\beta < \delta(\alpha,\beta) \in V^\delta_{\gamma^*}\} = \delta$, y por otra parte

$$Y_{\gamma^*} \cap \delta = \bigcup_{(\alpha,\beta)\in V^\delta_{\gamma^*+1}} (X_\beta)_{\gamma^*}.$$

Si $V^\delta_{\gamma^*+1} = V^\delta_{\gamma^*}$, entonces la última expresión es $Y^*_\gamma \cap \delta = S_\delta$. Pero esto no sucede, por la elección de Y y de C, luego $V^\delta_{\gamma^*+1} \subsetneq V^\delta_{\gamma^*}$, y ésta es la condición que debe cumplirse para que (Y, C) puedan prolongar la sucesión. ∎

Sucede, en cambio, que $\diamondsuit$ implica la hipótesis del continuo $2^{\aleph_0} = \aleph_1$, pero no es equivalente a ella.

Ya hemos observado que si $E \subset E'$ entonces $\diamondsuit_E \to \diamondsuit_{E'}$. Ahora vamos a probar un recíproco parcial, que nos permite deducir un diamante para un conjunto menor a partir de un diamante para un conjunto mayor:

Teorema 6.30 *Sea κ un cardinal infinito, sea $E \subset \kappa^+$ un conjunto estacionario y sea $E = \bigcup_{\delta<\kappa} E_\delta$ una partición de E en conjuntos disjuntos dos a dos. Si se cumple $\diamondsuit_E$, entonces existe un $\delta < \kappa$ tal que E_δ es estacionario en κ^+ y se cumple $\diamondsuit_{E_\delta}$.*

Demostración: Sea $j : \kappa^+ \longrightarrow \kappa \times \kappa^+$ la semejanza cuando en el producto consideramos el orden lexicográfico. El conjunto $C^* = \{\lambda < \kappa^+ \mid \kappa\lambda = \lambda\}$ (donde el producto es el de ordinales) es c.n.a. en κ^+ y, para cada $\lambda \in C^*$ (como $(\kappa \times \kappa^+)_{(0,\lambda)} = \kappa \times \lambda$ y tiene ordinal $\kappa\lambda = \lambda$), tenemos que $j|_\lambda : \lambda \longrightarrow \kappa \times \lambda$ biyectiva.

Sea $\{A_\alpha\}_{\alpha\in E}$ una sucesión $\diamondsuit_E$ y, para cada $\alpha \in E$, definamos

$$B_\alpha = \begin{cases} j[A_\alpha] & \text{si } \alpha \in C^*, \\ \varnothing & \text{si } \alpha \notin C^*. \end{cases}$$

Así tenemos definida una sucesión $\{B_\alpha\}_{\alpha\in E}$ que cumple lo mismo que las sucesiones $\diamondsuit_E$, pero para subconjuntos de $\kappa \times \kappa^+$, es decir, $B_\alpha \subset \kappa \times \alpha$ y si $X \subset \kappa \times \kappa^+$, entonces $\{\alpha \in E \mid X \cap (\kappa \times \alpha) = B_\alpha\}$ es estacionario en κ^+, pues sabemos que lo es

$$C^* \cap \{\alpha \in E \mid j^{-1}[X] \cap \alpha = A_\alpha\} \subset \{\alpha \in E \mid X \cap (\kappa \times \alpha) = B_\alpha\}.$$

Para cada $\delta < \kappa$ sea $\{A^\delta_\alpha\}_{\alpha\in E_\delta}$ la sucesión dada por

$$A^\delta_\alpha = \{\beta \in \alpha \mid (\beta, \delta) \in B_\alpha\}.$$

Vamos a probar que existe un $\delta < \kappa$ tal que E_δ es estacionario y $\{A^\delta_\alpha\}_{\alpha\in E_\delta}$ es una sucesión $\diamondsuit_{E_\delta}$. En caso contrario, para cada $\delta < \kappa$ existe un $X_\delta \subset \kappa^+$ y un c.n.a. $C_\delta \subset \kappa^+$ de modo que

$$\bigwedge \alpha \in C_\delta \cap E_\delta \; X_\delta \cap \alpha \neq A^\delta_\alpha.$$

Notemos que si lo que falla es que E_δ no es estacionario esto se cumple con cualquier C_δ disjunto de E_δ. Definimos

$$X = \bigcup_{\delta<\kappa} (\{\delta\} \times X_\delta), \qquad C = \bigcap_{\delta<\kappa} C_\delta.$$

Entonces C es c.n.a. en κ^+, luego existe un $\alpha \in E \cap C$ tal que $X \cap (\kappa \times \alpha) = B_\alpha$, luego existe un $\delta < \kappa$ tal que $\alpha \in E_\delta$, y también $\alpha \in C_\delta$, luego

$$\beta \in X_\delta \cap \alpha \leftrightarrow (\delta, \beta) \in X \cap (\kappa \times \alpha) = B_\alpha \leftrightarrow \beta \in A^\delta_\alpha,$$

en contradicción con que $X_\delta \cap \alpha \neq A^\delta_\alpha$. ∎

Observemos ahora la relación entre $\diamondsuit_E$ y $\diamondsuit'_E$: El primero nos asegura que si $A \subset \kappa$ es un conjunto arbitrario, muchas de sus secciones $A \cap \alpha$ son "previsibles", en el sentido de que son términos de una sucesión $\diamondsuit_E$ fijada a priori. En cambio, $\diamondsuit'_E$ es una versión más débil que, en lugar de identificar exactamente (algunas de) estas secciones de A, nos dice únicamente que cada una de ellas será alguno de los elementos de un conjunto prefijado S_α de cardinal $< \kappa$.

Es claro entonces que $\diamondsuit_E \to \diamondsuit'_E$, pues si $\{A_\alpha\}_{\alpha\in E}$ es una sucesión $\diamondsuit_E$, entonces basta definir $S_\alpha = \{A_\alpha\}$ para tener una sucesión $\diamondsuit'_E$. Pero, aunque no es tan evidente, sucede que el recíproco también es cierto:

Teorema 6.31 *Si κ es un cardinal infinito y $E \subset \kappa^+$ es estacionario, entonces $\diamondsuit_E \leftrightarrow \diamondsuit'_E$.*

Demostración: Como en la prueba del teorema anterior, consideramos la semejanza $j : \kappa^+ \longrightarrow \kappa \times \kappa^+$ la semejanza cuando en el producto consideramos el orden lexicográfico y el c.n.a. $C^* = \{\lambda < \kappa^+ \mid \kappa\lambda = \lambda\}$, de modo que para cada $\lambda \in C^*$ se cumple que $j|_\lambda : \lambda \longrightarrow \kappa \times \lambda$ biyectiva.

Si $\{S_\alpha\}_{\alpha\in E}$ es una sucesión $\diamondsuit'_E$, para cada $\alpha \in E$ definimos

$$T_\alpha = \begin{cases} \{j[A] \mid A \in S_\alpha\} & \text{si } \alpha \in C, \\ \{\varnothing\} & \text{si } \alpha \notin C. \end{cases}$$

Así tenemos definida una sucesión $\{T_\alpha\}_{\alpha\in E}$ que cumple lo mismo que las sucesiones $\diamondsuit'_E$, pero para subconjuntos de $\kappa \times \kappa^+$, es decir, $T_\alpha \subset \mathcal{P}(\kappa \times \alpha)$, $|T_\alpha| \leq \kappa$ y si $X \subset \kappa \times \kappa^+$, entonces $\{\alpha \in E \mid X \cap (\kappa \times \alpha) \in T_\alpha\}$ es estacionario.

Enumeremos (con repeticiones, si es preciso) $T_\alpha = \{T^\delta_\alpha \mid \delta < \kappa\}$. Así, para cada $X \subset \kappa \times \kappa^+$ existe $E_0 \subset E$ estacionario tal que

$$\bigwedge \alpha \in E \bigvee \delta < \kappa \; X \cap (\kappa \times \alpha) = T^\delta_\alpha.$$

Veamos ahora que, dado $X \subset \kappa \times \kappa^+$, existe $F \subset E$ estacionario tal que

$$\bigvee \delta < \kappa \bigwedge \alpha \in F \; X \cap (\kappa \times \alpha) = T^\delta_\alpha.$$

En efecto, definimos $f : E_0 \longrightarrow \kappa$ mediante $f(\alpha) = 0$ si $\alpha < \kappa$ y, para $\kappa \leq \alpha < \kappa^+$, tomamos como $f(\alpha)$ el mínimo δ tal que $X \cap (\kappa \times \alpha) = T^\delta_\alpha$. Por el teorema 6.15 sabemos que existe un $\delta < \kappa$ tal que $F = f^{-1}[\delta]$ es estacionario. Claramente F y δ cumplen lo requerido.

Por otra parte, para cada $\alpha \in E$ y $\delta < \kappa$ definimos

$$A^\delta_\alpha = \{\beta \in \alpha \mid (\delta, \beta) \in T^\delta_\alpha\},$$

y afirmamos que existe un $\delta < \kappa$ tal que $\{A^\delta_\alpha\}_{\alpha\in E}$ es una sucesión $\diamondsuit_E$. En caso contrario, para cada $\delta < \kappa$ existe un $X_\delta \subset \kappa^+$ y un c.n.a. $C_\delta \subset \kappa^+$ de modo que

$$\bigwedge \alpha \in C_\delta \ X_\delta \cap \alpha \neq A^\delta_\alpha.$$

Tomamos entonces $X = \bigcup_{\delta<\kappa} (\{\delta\} \times X_\delta)$ y $C = \bigcap_{\delta<\kappa} C_\delta$, que es c.n.a. en κ^+. Según hemos probado, existe un $\delta < \kappa$, un conjunto estacionario $F \subset E$ y un $\alpha \in F \cap C$ de modo que $X \cap (\kappa \times \alpha) = T^\delta_\alpha$. Pero entonces

$$\beta \in X_\delta \cap \alpha \leftrightarrow (\delta, \beta) \in X \cap (\kappa \times \alpha) = T^\delta_\alpha \leftrightarrow \beta \in A^\delta_\alpha,$$

en contradicción con que $X_\delta \cap \alpha \neq A^\delta_\alpha$. ∎

Nota Es evidente que no tiene interés trabajar con $\diamondsuit'_{\kappa^+}$, que es superficialmente más débil que $\diamondsuit_{\kappa^+}$ (aunque en el fondo sea equivalente). El interés de $\diamondsuit'_{\kappa^+}$ es que admite una versión más fuerte, $\diamondsuit^*_{\kappa^+}$, que consiste en cambiar la condición de que el conjunto $\{\alpha \in \kappa^+ \mid A \cap \alpha \in S_\alpha\}$ sea estacionario por la condición de que contenga un c.n.a.

Si tratamos de reforzar de este modo el principio $\diamondsuit_{\kappa^+}$ llegamos a un principio contradictorio:

Existe una sucesión $\{A_\alpha\}_{\alpha\in\kappa}$ *tal que* $\bigwedge\alpha \in \kappa \ A_\alpha \subset \alpha$ *y que verifica*

$$\bigwedge A \subset \kappa \bigvee C \ (C \text{ c.n.a. en } \kappa \wedge C \subset \{\alpha \in \kappa \mid A \cap \alpha = A_\alpha\}).$$

En efecto, esto no puede suceder, porque si A y A' son dos subconjuntos distintos de κ, entonces el conjunto

$$\{\alpha \in \kappa \mid A \cap \alpha = A_\alpha\} \cap \{\alpha \in \kappa \mid A' \cap \alpha = A_\alpha\} \subset \{\alpha \in \kappa \mid A \cap \alpha = A' \cap \alpha\}$$

debería contener un c.n.a., pero claramente el conjunto de la derecha está acotado por cualquier $\beta \in \kappa$ que esté en A y no en A' o viceversa. Así pues, si queremos cambiar "estacionario" por "cerrado no acotado" en $\diamondsuit_{\kappa^+}$, necesitamos partir de la forma equivalente $\diamondsuit'_{\kappa^+}$ para pasar a $\diamondsuit^*_{\kappa^+}$ ∎

Observemos que $\diamondsuit^*_\kappa$ no sólo implica trivialmente $\diamondsuit'_\kappa$, sino que de hecho se cumple:

Teorema 6.32 *Si κ es un cardinal regular, $E \subset \kappa$ es estacionario y se cumple el principio $\diamondsuit^*_\kappa$, entonces también se cumple $\diamondsuit'_E$. En particular, $\diamondsuit^*_{\kappa^+}$ implica todos los principios $\diamondsuit_E$, para todo conjunto estacionario $E \subset \kappa^+$.*

Demostración: Sea $\{S_\alpha\}_{\alpha\in\kappa}$ una sucesión $\diamondsuit_\kappa$. Entonces, dado $A \subset \kappa$, existe un c.n.a. $C \subset \kappa$ tal que $C \subset \{\alpha \in \kappa \mid A \cap \alpha \in S_\alpha\}$, luego

$$C \cap E \subset \{\alpha \in E \mid A \cap \alpha \in S_\alpha\},$$

lo que prueba que el conjunto de la derecha es estacionario, y que $\{S_\alpha\}_{\alpha\in E}$ es una sucesión $\diamondsuit'_E$. ∎

Así pues, tenemos la cadena de implicaciones

$$\diamondsuit^+_{\kappa^+} \to \diamondsuit^*_{\kappa^+} \to \diamondsuit'_E \leftrightarrow \diamondsuit_E \to 2^\kappa = \kappa^+.$$

Introducimos ahora un nuevo principio combinatorio más sofisticado:

Definición 6.33 Sea κ un cardinal infinito y $E \subset \kappa^+$. Llamaremos *cuadrado de Jensen* $\square_\kappa(E)$ a la afirmación siguiente: existe una sucesión $\{C_\lambda\}_{\lambda<\kappa^+}$ (lo que significa que λ recorre los ordinales límite menores que κ^+) tal que:

1. C_λ es c.n.a. en λ.
2. Si $\operatorname{cf}\lambda < \kappa$, entonces $|C_\lambda| < \kappa$.
3. Si $\lambda' < \lambda$ cumple que $C_\lambda \cap \lambda'$ no está acotado en λ', entonces $\lambda' \notin E$ y $C_{\lambda'} = C_\lambda \cap \lambda'$.

Una sucesión que cumpla estas condiciones recibe el nombre de sucesión $\square_\kappa(E)$. Llamaremos $\square_\kappa \equiv \square_\kappa(\varnothing)$.

Observemos que si $E \subset E' \subset \kappa^+$, se cumple que $\square_\kappa(E') \to \square_\kappa(E)$, por lo que $\square_\kappa$ es el más débil de los cuadrados sobre κ.

Los principios $\square_\omega(E)$ se cumplen trivialmente, pues basta tomar como C_λ cualquier sucesión cofinal en λ, de modo que las hipótesis de b) y c) no pueden darse nunca.

Si $\kappa > \omega$, entonces una sucesión $\square_\kappa(E)$ cumple además que si $\operatorname{cf}\lambda = \kappa$ entonces $\operatorname{ord} C_\lambda = \kappa$.

En efecto, si $\gamma = \operatorname{ord} C_\lambda$, la semejanza $f : \gamma \longrightarrow C_\lambda$ es cofinal creciente en λ, luego $\operatorname{cf}\gamma = \operatorname{cf}\lambda = \kappa \leq \gamma$. Si fuera $\kappa < \gamma$, entonces $\kappa < \kappa + \omega < \gamma$ (pues $\operatorname{cf}\gamma = \kappa > \omega$) y $C_\lambda \cap f(\kappa)$ no está acotado en $f(\kappa)$, luego por c) tenemos que $C_{f(\kappa)} = C_\lambda \cap f(\kappa) = f[\kappa]$ tiene ordinal κ. Similarmente, $C_{f(\kappa+\omega)} = C_\lambda \cap f(\kappa+\omega)$, luego $C_{f(\kappa)} \subset C_{f(\kappa+\omega)}$, luego $\kappa = \operatorname{ord} C_{f(\kappa)} \leq \operatorname{ord} C_{f(\kappa+\omega)} < \kappa$ por b) ya que $\operatorname{cf} f(\kappa+\omega) = \omega < \kappa$, y tenemos una contradicción. ∎

El teorema siguiente es trivial salvo si $\operatorname{cf}\kappa = \aleph_0$, y en este caso prueba que, bajo ciertas hipótesis sobre la función del continuo, $\square_\kappa$ implica el caso no trivial de $\diamondsuit_E$ que no se sigue de la mera hipótesis $2^\kappa = \kappa^+$:

Teorema 6.34 *Sea κ un cardinal no numerable tal que $2^{<\kappa} = \kappa$ y $2^\kappa = \kappa^+$. Sea $W = \{\lambda < \kappa \mid \operatorname{cf}\lambda = \aleph_0\}$. Entonces $\square_\kappa \to \diamondsuit_W$.*

Demostración: Si $\operatorname{cf}\kappa > \aleph_0$ entonces se cumple $\diamondsuit_W$ por 6.29, así que podemos suponer que $\operatorname{cf}\kappa = \aleph_0$. Si $\mu \leq \kappa$ tenemos que

$$(\kappa^+)^\mu \leq \kappa^\mu \kappa^+ \leq \kappa^\kappa \kappa^+ = \kappa^+,$$

luego hay exactamente κ^+ subconjuntos de κ^+ de cardinal a lo sumo κ. Sea $\{X_\alpha\}_{\alpha<\kappa^+}$ una enumeración de todos ellos. Podemos exigir que $X_\alpha \subset \alpha$. En

efecto, definimos $f : \kappa^+ \longrightarrow \kappa^+$ de modo que $f(\alpha)$ sea el menor ordinal $\geq \bigcup X_\alpha$ que no esté en $f[\alpha]$, lo cual siempre es posible, pues $|f[\alpha]| \leq \kappa$ y hay κ^+ ordinales en κ^+ mayores que uno dado. Así f es inyectiva por construcción y biyectiva porque si $\delta < \kappa^+$, existe un α tal que $X_\alpha = \delta$ y, o bien $f(\alpha) = \delta$, o bien existe un $\beta < \alpha$ tal que $f(\beta) = \delta$. Basta definir $X'_\alpha = X_{f^{-1}(\alpha)}$ y tenemos una enumeración que cumple lo requerido.

Sea $\Gamma_\alpha = \{X_\delta \mid \delta < \alpha\}$ y sea $\{C_\lambda\}_{\lambda<\kappa^+}$ una sucesión $\square_\kappa$. Para cada $\lambda < \kappa^+$ sea $\theta_\lambda = \operatorname{ord} C_\lambda$ y sea $\{c^\lambda_\delta\}_{\delta<\theta_\lambda}$ la semejanza $\theta_\lambda \longrightarrow C_\lambda$. Sea $\kappa = \bigcup_{\beta<\kappa} A_\beta$ una partición de κ en subconjuntos de cardinal κ disjuntos dos a dos. Sea $f^\alpha_\beta : \Gamma_\alpha \longrightarrow A_\beta$ inyectiva. Para cada $\lambda < \kappa^+$ definimos $f_\lambda : \Gamma_\lambda \longrightarrow \kappa$ mediante $f_\lambda(x) = f^{c^\lambda_\delta}_\delta(x)$, donde $\delta < \theta_\lambda$ es el menor ordinal tal que $x \in \Gamma_{c^\lambda_\delta}$. De este modo f_λ es inyectiva y cumple lo siguiente:

Si $\lambda' < \lambda$ y $C_\lambda \cap \lambda'$ no está acotado en λ', entonces $f_\lambda|_{\Gamma_{\lambda'}} = f_{\lambda'}$.

En efecto, en estas circunstancias se cumple que $C_{\lambda'} = C_\lambda \cap \lambda'$, luego $c^\lambda_\delta = c^{\lambda'}_\delta$ para todo $\delta < \theta_{\lambda'}$ luego si $x \in \Gamma_{\lambda'}$ el δ con el que se definen f_λ y $f_{\lambda'}$ es el mismo, luego $f_\lambda(x) = f_{\lambda'}(x)$.

Para cada $\lambda \in W$ sea $S_\lambda = \{\bigcup f_\lambda^{-1}[x] \mid x \subset \kappa \wedge |x| \leq \aleph_0 \wedge x \text{ acotado en } \kappa\}$. Así $S_\lambda \subset \mathcal{P}\lambda$ y, como (por hipótesis) el número de subconjuntos numerables acotados de κ es κ, tenemos que $|S_\lambda| \leq \kappa$. Vamos a probar que $\{S_\lambda\}_{\lambda\in W}$ es una sucesión $\diamondsuit'_W$.

Fijamos $X \subset \kappa^+$ y un c.n.a. $C \subset \kappa^+$. Tenemos que encontrar un $\lambda \in C \cap W$ tal que $X \cap \lambda \in S_\lambda$. Para ello definimos

$$A = \{\lambda \in \kappa^+ \mid \textstyle\bigwedge \lambda' < \lambda\ X \cap \lambda' \in \Gamma_\lambda\}.$$

Se cumple que A es c.n.a. en κ^+ pues claramente es cerrado y podemos definir $h : \kappa^+ \longrightarrow \kappa^+$ de modo que $h(0) = 0$, $h(\alpha + 1) = 0$ y $h(\lambda')$ es el mínimo ordinal $\lambda < \kappa^+$ tal que $X \cap \lambda' \in \Gamma_\lambda$. Así, $\{\lambda < \kappa^+ \mid g[\lambda] \subset \lambda\} \subset A$ y el conjunto de la izquierda es c.n.a., luego A no está acotado.

Tenemos que $A \cap C$ es c.n.a. en κ^+, y también lo es el conjunto de sus puntos de acumulación (es decir, el conjunto de los λ tales que $\lambda \cap A \cap C$ no está acotado en λ) y, como $\{\lambda \in \kappa^+ \mid \operatorname{cf}\lambda = \aleph_1\}$ es estacionario, podemos tomar $\lambda \in A \cap C$ tal que $\lambda \cap A \cap C$ no esté acotado en λ y $\operatorname{cf}\lambda = \aleph_1$. Entonces $\lambda \cap A \cap C$ es c.n.a. en λ y, como C_λ también lo es, resulta que $A \cap C \cap C_\lambda$ es c.n.a. en λ y podemos tomar una sucesión normal $\{b_\delta\}_{\delta<\omega_1}$ en $A \cap C \cap C_\lambda$ cofinal en λ. Observemos que $X \cap b_\delta \in \Gamma_{b_{\delta+1}}$ para todo $\delta < \omega_1$.

Sea $\{\kappa_n\}_{n<\omega}$ cofinal creciente en κ. Sea $h : \omega_1 \longrightarrow \omega$ la función dada por que $h(\delta)$ es el mínimo n tal que $f_\lambda(X \cap b_\delta) < \kappa_n$. Como es una función regresiva, existe un $E \subset \omega_1$ estacionario sobre el que h toma el mismo valor n.

Sea γ_i el i-ésimo elemento de E, sea $\gamma = \bigcup_{i\in\omega} \gamma_i$ y sea $\lambda' = b_\gamma$. Entonces $\operatorname{cf}\lambda' = \operatorname{cf}\gamma = \omega$, luego $\lambda' \in W$. Por otra parte, $\lambda' \cap C \cap C_\lambda$ no está acotado en λ', ya que los b_{γ_i} están en la intersección, luego $\lambda' \in C \cap C_\lambda$.

Ahora observamos que $X \cap \lambda' = \bigcup_{i\in\omega} X \cap b_{\gamma_i} = \bigcup f_\lambda^{-1}[x]$, donde

$$x = \{f_\lambda(X \cap b_{\gamma_i}) \mid i < \omega\}.$$

Pero por la elección de E tenemos que $x \subset \kappa_n < \kappa$, luego x es un subconjunto numerable y acotado de κ. Además sabemos que $f_\lambda|_{\Gamma_{\lambda'}} = f_{\lambda'}$, luego $X \cap \lambda' \in S_{\lambda'}$ ∎

Por último veamos que $\square_\kappa$ implica una versión más fuerte de sí mismo:

Teorema 6.35 *Sea κ un cardinal no numerable y $W = \{\lambda < \kappa^+ \mid \operatorname{cf}\lambda = \aleph_0\}$. Entonces, si se cumple $\square_\kappa$, existe $E \subset W$ estacionario tal que $\square_\kappa(E)$ y además $\diamondsuit_W \to \diamondsuit_E$.*

Demostración: Sea $\{A_\lambda\}_{\lambda<\kappa^+}$ una sucesión $\square_\kappa$. Para cada λ, sea B_λ el conjunto de los puntos de acumulación de A_λ (los λ' tales que $A_\lambda \cap \lambda'$ no está acotado en λ). La sucesión $\{B_\lambda\}_{\lambda<\kappa^+}$ tiene las propiedades siguientes:

1. B_λ es cerrado en λ.
2. Si $\operatorname{cf}\lambda > \aleph_0$, entonces B_λ no está acotado en λ.
3. Si $\lambda' \in B_\lambda$, entonces $B_{\lambda'} = B_\lambda \cap \lambda'$.
4. Si $\operatorname{cf}\lambda < \kappa$ entonces $|B_\lambda| < \kappa$.

En efecto, a) es inmediato. Para probar b) observamos que, dado $\alpha < \lambda$, podemos formar una sucesión creciente $\alpha < \lambda_0 < \lambda_1 < \cdots$ de elementos de A_λ, y entonces $\alpha < \bigcup_{n<\omega} \lambda_n \in B_\lambda$.

Para c) sabemos que $A_{\lambda'} = A_\lambda \cap \lambda'$, y es claro entonces que los puntos de acumulación de $A_{\lambda'}$ son precisamente los puntos de acumulación de A_λ menores que λ'.

Por último, si $\operatorname{cf}\lambda < \kappa$ tenemos que $|B_\lambda| \le |A_\lambda| < \kappa$, luego se cumple d).

De las propiedades c) y d) se sigue que $\operatorname{ord} B_\lambda \le \kappa$.

En efecto, si $\operatorname{cf}\lambda = \kappa$ y $\gamma = \operatorname{ord} B_\lambda$, sea $f : \gamma \longrightarrow B_\lambda$ la semejanza, que es cofinal en λ por b). Si fuera $\kappa < \gamma$, entonces $\kappa + \omega < \gamma$ (pues $\operatorname{cf}\gamma = \operatorname{cf}\lambda = \kappa$), luego $B_{f(\kappa)} = B_\lambda \cap f(\kappa) = f[\kappa]$ tiene ordinal κ y $B_{f(\kappa+\omega)} = B_\lambda \cap f(\kappa+\omega)$, luego $B_{f(\kappa)} \subset B_{f(\kappa+\omega)}$, y así, por d) llegamos a una contradicción:

$$\kappa = |B_{f(\kappa)}| \le |B_{f(\kappa+\omega)}| < \kappa.$$

Llamamos $W_\delta = \{\lambda \in W \mid \operatorname{ord} B_\lambda = \delta\}$, de modo que $W = \bigcup_{\delta\le\kappa} W_\delta$. Entonces existe un $\delta \le \kappa$ tal que W_δ es estacionario en κ^+ (si para cada δ existiera un c.n.a. C_δ tal que $W_\delta \cap C_\delta = \varnothing$, entonces $\bigcap_{\delta\le\kappa} C_\delta$ sería un c.n.a. disjunto con W).

Más aún, el teorema 6.30 implica que podemos elegir δ de modo que se dé la implicación $\diamondsuit_W \to \diamondsuit_{W_\delta}$. Llamamos $E = W_\delta$. Hemos de probar $\square_\kappa(E)$.

Para cada $\lambda < \kappa^+$, si $\theta_\lambda = \operatorname{ord} B_\lambda \leq \delta$ definimos $D_\lambda = B_\lambda$, y en otro caso D_λ es el conjunto que resulta de quitar a B_λ sus $\delta + 1$ primeros elementos, es decir,

$$D_\lambda = B_\lambda \setminus f_\lambda[\delta + 1],$$

donde $f_\lambda : \theta_\lambda \longrightarrow B_\lambda$ es la semejanza entre B_λ y su ordinal θ_λ.

Vamos a comprobar que la sucesión $\{D_\lambda\}_{\lambda<\kappa^+}$ cumple las mismas propiedades a) – d) y además $D_\lambda \cap E = \varnothing$.

Veamos únicamente la c), pues las demás son inmediatas. Si $\lambda' \in D_\lambda$, entonces $\lambda' \in B_\lambda$, luego $B_{\lambda'} = B_\lambda \cap \lambda'$. Si $\delta < \theta_{\lambda'}$ entonces D_λ y $D_{\lambda'}$ resultan de quitarles a B_λ y $B_{\lambda'}$ los mismos $\delta + 1$ primeros elementos, luego sigue cumpliéndose que $D_{\lambda'} = D_\lambda \cap \lambda'$. No puede ocurrir que $\theta_{\lambda'} \leq \delta < \theta_\lambda$, pues entonces $\lambda' \notin D_\lambda$, y si $\theta_\lambda \leq \delta$ entonces $D_{\lambda'} = B_{\lambda'}$ y $D_\lambda = B_\lambda$, luego la conclusión es trivial.

Por último, si $\lambda' \in D_\lambda \cap E$, entonces $B_{\lambda'} = B_\lambda \cap \lambda'$, luego λ' es el $\delta+1$-ésimo elemento de B_λ, luego $\lambda' \notin D_\lambda$, contradicción.

Ahora definimos por recurrencia una sucesión $\{C_\lambda\}_{\lambda<\kappa^+}$:

Si D_λ no está acotado en λ, definimos $C_\lambda = \bigcup_{\lambda' \in D_\lambda} C_{\lambda'}$ y en caso contrario (lo que implica que $\operatorname{cf}\lambda = \aleph_0$), definimos $C_\lambda = \bigcup_{\lambda' \in D_\lambda} C_{\lambda'} \cup \{\alpha^\lambda_n \mid n \in \omega\}$, donde $\{\theta^\lambda_n\}_{n\in\omega}$ es una sucesión cofinal creciente en λ tal que $\theta^\lambda_0 = \bigcup_{\lambda' \in D_\lambda} C_{\lambda'}$.

Vamos a probar que $\{C_\lambda\}_{\lambda<\kappa^+}$ es una sucesión $\square_\kappa$ y que D_λ es el conjunto de los puntos de acumulación de C_λ (es decir, que $\lambda' \cap C_\lambda$ no está acotado en λ' si y sólo si $\lambda' \in D_\lambda$). Esto implica que se trata de hecho de una sucesión $\square_\kappa(E)$.

Es claro que si $C_{\lambda'}$ no está acotado en λ' para cada $\lambda' < \lambda$, entonces C_λ no está acotado en λ, luego todos los C_λ son conjuntos no acotados en el λ correspondiente.

Veamos ahora, por inducción sobre λ, que si $\lambda' \in D_\lambda$ entonces $C_{\lambda'} = C_\lambda \cap \lambda'$.

Si es cierto para todo $\lambda' < \lambda$ y $\lambda' \in D_\lambda$, por construcción $C_{\lambda'} \subset C_\lambda$, luego $C_{\lambda'} \subset C_\lambda \cap \lambda'$. Tomemos ahora $\alpha \in C_\lambda \cap \lambda'$. Entonces, por construcción $\alpha \in C_{\lambda''} \cap \lambda'$, para cierto $\lambda'' \in D_\lambda$. Si $\lambda'' = \lambda'$ entonces $\alpha \in C_{\lambda'}$. Supongamos ahora que $\lambda'' < \lambda'$. Entonces, como $\lambda' \in D_\lambda$, sabemos que $D_{\lambda'} = D_\lambda \cap \lambda'$, luego $\lambda'' \in D_{\lambda'}$, luego $C_{\lambda''} \subset C_{\lambda'}$, luego $\alpha \in C_{\lambda'}$. Supongamos por último que $\lambda' < \lambda''$. Entonces $\lambda'' \in D_\lambda \cap \lambda' = D_{\lambda'}$, luego por la hipótesis de inducción aplicada a λ' sabemos que $C_{\lambda''} = C_{\lambda'} \cap \lambda''$, luego $\alpha \in C_{\lambda'}$.

Veamos ahora que D_λ es el conjunto de puntos de acumulación de C_λ, también por inducción sobre λ.

Si $\lambda' \in D_\lambda$, tenemos que $C_{\lambda'} \subset C_\lambda \cap \lambda'$ y C'_λ no está acotado en λ', luego ciertamente λ' es un punto de acumulación de C_λ. Recíprocamente, supongamos que $C_\lambda \cap \lambda'$ no está acotado en λ'. Supongamos en primer lugar que D_λ está

acotado en λ. Entonces, por la construcción de C_λ, es claro que λ' debe ser un punto de acumulación de $\bigcup_{\lambda'\in D_\lambda} C_{\lambda'}$. Como D_λ es cerrado en λ, tenemos que $\lambda'' = \bigcup D_\lambda \in D_\lambda$, luego $D_{\lambda''} = D_\lambda \cap \lambda''$ y

$$\bigcup_{\lambda'\in D_\lambda} C_{\lambda'} = \bigcup_{\lambda'\in D_{\lambda''}} C_{\lambda'} \cup C_{\lambda''} = C_{\lambda''} \cup C_{\lambda''} = C_{\lambda''}.$$

Por lo tanto, λ' es un punto de acumulación de $C_{\lambda''}$. Por la hipótesis de inducción para λ'' tenemos que $\lambda' \in D_{\lambda''} = D_\lambda \cap \lambda''$, luego $\lambda' \in D_\lambda$.

Supongamos ahora que D_λ no está acotado en λ. Entonces podemos tomar $\lambda'' \in D_\lambda$ tal que $\lambda' < \lambda''$. Antes hemos probado que $C_{\lambda''} = C_\lambda \cap \lambda''$ y así $C_{\lambda''} \cap \lambda' = C_\lambda \cap \lambda'$ no está acotado en λ', luego por la hipótesis de inducción para λ'' tenemos que $\lambda' \in C_{\lambda''} \subset C_\lambda$.

Veamos ahora, siempre por inducción sobre λ, que C_λ es cerrado en λ.

Supongamos que $C_\lambda \cap \lambda'$ no está acotado en λ'. Hemos visto que entonces $\lambda' \in D_\lambda$. Si $\lambda' = \bigcup D_\lambda$, entonces $\lambda' = \theta_0^\lambda \in C_\lambda$. En caso contrario existe $\lambda'' \in D_\lambda$ tal que $\lambda' < \lambda''$. Hemos probado entonces que $C_{\lambda''} = C_\lambda \cap \lambda''$, pero entonces $C_{\lambda''} \cap \lambda' = C_\lambda \cap \lambda'$ no está acotado en λ', luego por hipótesis de inducción $\lambda' \in C_{\lambda''} \subset C_\lambda$.

Con esto ya tenemos que C_λ es c.n.a. en λ, y sólo falta probar que si $\operatorname{cf}\lambda < \kappa$ entonces $|C_\lambda| < \kappa$.

Si $|C_\lambda| \geq \kappa$, entonces $\operatorname{ord} C_\lambda \geq \kappa$, luego C_λ tiene κ puntos de acumulación, luego $|D_\lambda| = \kappa$, luego $\operatorname{cf}\lambda = \kappa$, por la propiedad d). ∎

Al combinar los dos últimos teoremas obtenemos:

Teorema 6.36 *Si κ es un cardinal no numerable tal que $2^{<\kappa} = \kappa$, $2^\kappa = \kappa^+$ y $\square_\kappa$, existe un conjunto $E \subset \kappa^+$ estacionario tal que $\square_\kappa(E)$ y $\diamondsuit_E$.*

Terminamos demostrando que $\square_\kappa$ es equivalente esta variante:

Definición 6.37 Si κ es un cardinal infinito, llamamos $\square'_\kappa$ a la afirmación siguiente: existe una sucesión $\{B_\lambda\}_{\lambda<\kappa^+}$ tal que:

1. B_λ es cerrado en λ y está formado por ordinales límite.
2. Si $\operatorname{cf}\lambda > \aleph_0$ entonces B_λ no está acotado en λ.
3. $\operatorname{ord} B_\lambda \leq \kappa$.
4. Si $\lambda' \in B_\lambda$, entonces $B_{\lambda'} = B_\lambda \cap \lambda'$.

A las sucesiones que cumplen esto se las llama sucesiones $\square'_\kappa$.

Se cumple trivialmente $\square'_\omega$, sin más que tomar todos los B_λ vacíos.

Teorema 6.38 *Para todo cardinal infinito κ, se cumple que $\square_\kappa \leftrightarrow \square'_\kappa$.*

DEMOSTRACIÓN: La prueba es una modificación del argumento empleado en 6.35. Podemos suponer que $\kappa > \aleph_0$. Una implicación es sencilla: si $\{C_\lambda\}_{\lambda<\kappa^+}$ es una sucesión $\square_\kappa$, basta definir B_λ como el conjunto de los puntos de acumulación de C_λ, es decir, los $\lambda' < \lambda$ tales que $C_\lambda \cap \lambda'$ no está acotado en λ'. (En 6.35 está probado que $\{B_\lambda\}_{\lambda<\kappa^+}$ es una sucesión $\square'_\kappa$.)

Supongamos ahora que $\{B_\lambda\}_{\lambda<\kappa^+}$ es una sucesión $\square'_\kappa$ y definamos C_λ como en 6.35:

Si B_λ no está acotado en λ, definimos $C_\lambda = \bigcup_{\lambda'\in B_\lambda} C_{\lambda'}$ y en caso contrario (lo que implica que $\operatorname{cf}\lambda = \aleph_0$), definimos $C_\lambda = \bigcup_{\lambda'\in B_\lambda} C_{\lambda'} \cup \{\alpha^\lambda_n \mid n \in \omega\}$, donde $\{\theta^\lambda_n\}_{n\in\omega}$ es una sucesión cofinal creciente en λ tal que $\theta^\lambda_0 = \bigcup_{\lambda'\in B_\lambda} C_{\lambda'}$.

Los hechos siguientes (menos el cuarto) se prueban exactamente igual que en 6.35:

- $\lambda' \in B_\lambda$ entonces $C_{\lambda'} = C_\lambda \cap \lambda'$.
- B_λ es el conjunto de puntos de acumulación de C_λ.
- C_λ es c.n.a. en λ.
- $\operatorname{ord} C_\lambda \le \kappa$.

Para probar la última propiedad observamos que si $\operatorname{ord} C_\lambda > \kappa$, entonces también $\operatorname{ord} B_\lambda > \kappa$ (pues $\kappa \longrightarrow \kappa$ dada por $\alpha \mapsto \omega\cdot\alpha$ muestra que un conjunto de ordinal κ tiene κ puntos de acumulación, y si tiene ordinal $\ge \kappa+1$ entonces tiene al menos $\kappa+1$, los κ de ordinal $< \kappa$ y el de ordinal κ), y esto contradice la definición de sucesión $\square'_\kappa$.

Para tener una sucesión $\square_\kappa$ falta que si $\operatorname{cf}\lambda < \kappa$ entonces $\operatorname{ord} C_\lambda < \kappa$. Esto se cumple trivialmente si κ es regular, pues si fuera $\operatorname{ord} C_\lambda = \kappa$ entonces la semejanza $f : \kappa \longrightarrow C_\lambda$ sería cofinal creciente en κ, luego $\kappa = \operatorname{cf}\kappa \le \operatorname{cf}\lambda$.

En el caso en que κ sea singular necesitamos modificar ligeramente los conjuntos C_λ. Sea $\mu = \operatorname{cf}\kappa$ y sea $\{\theta_\alpha\}_{\alpha<\mu}$ una sucesión cofinal y normal en κ tal que $\theta_0 = 0$. Sea $\theta_\mu = \kappa$. Para cada $\lambda < \kappa^+$, sea $f_\lambda : \eta_\lambda \longrightarrow C_\lambda$ la semejanza en su ordinal $\eta_\lambda \le \kappa$.

Si $\theta_\alpha < \eta_\lambda \le \theta_{\alpha+1}$ definimos $C'_\lambda = f_\lambda[\eta_\lambda \setminus (\theta_\alpha + 1)]$, es decir, le quitamos a C_λ sus primeros $\theta_\alpha + 1$ elementos.

En caso contrario $\eta_\lambda = \theta_{\lambda'}$, para cierto $\lambda' \le \mu$, y entonces definimos

$$C'_\lambda = f_\lambda[\{\theta_\alpha \mid \alpha < \lambda'\}].$$

Se cumple entonces que $\{C'_\lambda\}_{\lambda<\kappa^+}$ es una sucesión $\square_\kappa$. En efecto, es claro que C'_λ es c.n.a. en λ (en el segundo caso C'_λ es el rango de una función normal).

Si $C'_\lambda \cap \lambda'$ no está acotado en λ', entonces tampoco lo está $C_\lambda \cap \lambda'$, luego sabemos que $C_{\lambda'} = C_\lambda \cap \lambda'$ y que $\lambda' \in C'_\lambda$, luego $f_{\lambda'} = f_\lambda|_{\eta_{\lambda'}}$ y $\lambda' = f_\lambda(\eta_{\lambda'})$.

Si $\theta_\alpha < \eta_\lambda \leq \theta_{\alpha+1}$, entonces también $\theta_\alpha < \eta_{\lambda'} \leq \theta_{\alpha+1}$, pues en caso contrario $\lambda' \notin C'_\lambda$. Por lo tanto, a C_λ le quitamos los mismos elementos que a $C_{\lambda'}$ y es claro que $C'_{\lambda'} = C'_\lambda \cap \lambda'$.

Si $\eta_\lambda = \theta_{\lambda''}$, entonces $\lambda' = f_\lambda(\eta_{\lambda'}) = f_\lambda(\theta_\beta)$, para cierto $\beta < \lambda''$, luego $\eta_{\lambda'} = \theta_\beta$, y α tiene que ser un ordinal límite, pues

$$C'_\lambda \cap \lambda' = C'_\lambda \cap f_\lambda(\theta_\beta) = \{f_\lambda(\theta_\alpha) \mid \alpha < \beta\}$$

no está acotado en λ', luego no puede tener máximo. Por lo tanto

$$C'_{\lambda'} = f_\lambda[\{\theta_\alpha \mid \alpha < \beta\}] = C'_\lambda \cap f_\lambda(\theta_\beta) = C'_\lambda \cap \lambda'.$$

Finalmente, observamos que se cumple $|C'_\lambda| < \kappa$. En el primer caso de la definición $|C'_\lambda| \leq |\eta_\lambda| \leq |\theta_{\alpha+1}| < \kappa$, mientras que en el segundo vemos que $|C'_\lambda| = |\lambda'| \leq \mu < \kappa$. ∎

6.6 Puntos fijos de funciones normales

El teorema 6.5 (véase la nota posterior) nos da que una clase es c.n.a. en Ω si y sólo si es la imagen de una función normal $F : \Omega \longrightarrow \Omega$ y, por otra parte, el teorema 6.6 nos da que la clase de los puntos fijos de una función normal es c.n.a., luego es a su vez el rango de una función normal, y así sucesivamente. En esta sección precisaremos este "y así sucesivamente".

Definición 6.39 Dada una función normal $F : \Omega \longrightarrow \Omega$, su *derivada* es la función normal $F' : \Omega \longrightarrow \Omega$ tal que $F'[\Omega]$ es la clase de los puntos fijos de F.

Según acabamos de explicar, la existencia de F' está justificada por los teoremas 6.5 y 6.6 (y las notas posteriores a cada uno de ellos). También es posible definir directamente F' por recurrencia, estableciendo que $F'(a)$ es el menor punto fijo de F que no pertenece a $F'[\alpha]$, y se comprueba fácilmente que se trata de una función normal.

Veamos ahora que podemos definir derivadas sucesivas de una función normal. Cuando decimos que una función enumera una clase o conjunto de ordinales queremos decir que es una semejanza entre Ω (o un $\lambda \in \Omega$) y la clase indicada.

Teorema 6.40 *Si $F : \Omega \longrightarrow \Omega$ es una función normal, para cada ordinal γ existe una única función $F^{(\gamma)} : \Omega \longrightarrow \Omega$ (que también es normal) de modo que $F^{(0)} = F$ y, para cada $\gamma > 0$, la función $F^{(\gamma)}$ enumera la clase de los ordinales que son puntos fijos comunes de todas las funciones $F^{(\delta)}$, con $\delta < \gamma$.*

La función $F^{(\gamma)}$ se llama *derivada de orden* γ de F. La existencia de estas derivadas sucesivas no es inmediata porque se trata de definir recurrentemente una sucesión de clases propias, y no es inmediato que esto pueda formalizarse en NBG, sin embargo, vamos a demostrar que sí que es posible.

DEMOSTRACIÓN: Diremos que una función $f : \lambda \longrightarrow \lambda$ es una *derivada de orden* γ de F en λ si existe una sucesión $\{f_\lambda^{(\delta)}\}_{\delta\leq\gamma}$ de funciones $f_\lambda^{(\delta)} : \lambda \longrightarrow \lambda$ tales que $f^{(0)} = F|_\lambda$, cada $f_\lambda^{(\delta)}$ enumera los ordinales $< \lambda$ que son puntos fijos de todas las funciones precedentes y $f = f_\lambda^{(\gamma)}$.

Es inmediato que si existe una derivada de orden γ de F en λ entonces la sucesión $\{f_\lambda^{(\delta)}\}_{\delta\leq\gamma}$ es única. Veamos ahora que cada una de sus funciones es normal.

En efecto, $f_\lambda^{(0)} = F|_\lambda$ es normal y, si es cierto para todo $\epsilon < \delta \leq \gamma$, tenemos que $f_\lambda^{(\delta)}$ es estrictamente creciente por definición, y si $\lambda' < \lambda$ es un ordinal límite, tenemos que $\{f_\lambda^{(\delta)}(\alpha) \mid \alpha < \lambda'\}$ es un conjunto de puntos fijos de $f_\lambda^{(\epsilon)}$, para todo $\epsilon < \delta$. Como $f_\lambda^{(\delta)}$ es estrictamente creciente, el supremo de este conjunto es un ordinal límite y, como $f_\lambda^{(\epsilon)}$ es normal, para todo $\epsilon < \delta$,

$$f_\lambda^{(\epsilon)}(\bigcup_{\alpha<\lambda'} f_\lambda^{(\delta)}(\alpha)) = \bigcup_{\alpha<\lambda'} f_\lambda^{(\epsilon)}(f_\lambda^{(\delta)}(\alpha)) = \bigcup_{\alpha<\lambda'} f_\lambda^{(\delta)}(\alpha),$$

luego, como el supremo es punto fijo de todas las $f_\lambda^{(\epsilon)}$ y es el menor valor que puede tomar $f_\lambda^{(\delta)}(\lambda')$, tiene que ser

$$f_\lambda^{(\delta)}(\lambda') = \bigcup_{\alpha<\lambda'} f_\lambda^{(\delta)}(\alpha),$$

y esto prueba que $f_\lambda^{(\delta)}$ es normal.

Veamos ahora que si $\lambda < \lambda'$ y existen derivadas de orden γ de F en ambos ordinales, se cumple que $f_{\lambda'}^{(\delta)}|_\lambda = f_\lambda^{(\delta)}$ y $f_{\lambda'}^{(\delta)}(\lambda) = \lambda$.

En efecto, trivialmente es cierto para $\delta = 0$ y, si vale para todo $\epsilon < \delta$, tenemos que $f_{\lambda'}^{(\delta)}$ enumera los puntos fijos de las funciones $f_{\lambda'}^{(\epsilon)}$, y los puntos fijos $< \lambda$ de estas funciones son los puntos fijos de las funciones $f_{\lambda'}^{(\epsilon)}|_\lambda = f_\lambda^{(\epsilon)}$, luego $f_{\lambda'}^{(\delta)}[\lambda'] \cap \lambda = f_\lambda^{(\delta)}[\lambda]$. Esto implica que $f_\lambda^{(\delta)}[\lambda]$ es una sección inicial de $f_{\lambda'}^{(\delta)}[\lambda']$ (de ordinal λ), luego la restricción a λ de $f_{\lambda'}^{(\delta)} : \lambda' \longrightarrow f_{\lambda'}^{(\delta)}[\lambda']$ es una semejanza $f_{\lambda'}^{(\delta)}|_\lambda : \lambda \longrightarrow f_\lambda^{(\delta)}[\lambda]$, luego tiene que ser $f_{\lambda'}^{(\delta)}|_\lambda = f_\lambda^{(\delta)}$. En particular $f_{\lambda'}^{(\delta)}[\lambda] \subset \lambda$, luego $f_{\lambda'}^{(\delta)}(\lambda) = \lambda$, porque la función es normal.

Ahora basta probar que para todo γ existen derivadas de orden γ de F sobre ordinales arbitrariamente grandes, pues entonces podemos definir $F^{(\gamma)}$ como la unión de todas las derivadas de orden γ de F. Más aún, al ser uniones de funciones normales podremos afirmar que cada $F^{(\gamma)}$ es normal.

Razonamos por inducción sobre γ. Si $\gamma = 0$ es trivial. Supuesto cierto para todo $\delta < \gamma$, podemos definir las derivadas $F^{(\delta)}$ como la unión de todas las derivadas de orden δ de F (para cada $\delta < \gamma$), y son funciones normales. Por la nota tras 6.4, la clase C de los puntos fijos comunes de todas las funciones $F^{(\delta)}$ es c.n.a. en Ω, pues es la intersección de γ clases c.n.a. Esto implica que C

es el rango de una función normal G. Basta probar que si λ es cualquiera de sus puntos fijos, entonces $f_\lambda^{(\gamma)} = G|_\lambda$ es una derivada de orden γ de F en λ. En efecto, $G(\lambda) = \lambda$ implica que $\lambda \in C$, de donde λ es un punto fijo de todas las funciones $F^{(\delta)}$ con $\delta < \gamma$, luego las restricciones $f_\lambda^{(\delta)} = F^{(\delta)}|_\lambda$ forman, junto con $f_\lambda^{(\gamma)} = G|_\lambda$, una sucesión $\{f_\lambda^{(\delta)}\}_{\delta\leq\gamma}$ que prueba que $f_\lambda^{(\gamma)}$ es realmente una derivada de orden γ. ∎

Es inmediato que $F^{(1)} = F'$. Veamos otras propiedades elementales de las derivadas sucesivas:

Teorema 6.41 *Si $\delta \leq \gamma$, entonces, para todo α se cumple $F^{(\delta)}(\alpha) \leq F^{(\gamma)}(\alpha)$ y si además $\alpha < F(\alpha)$ y $\delta < \gamma$ entonces $F^{(\delta)}(\alpha) < F^{(\gamma)}(\alpha)$.*

Demostración: Claramente $F^{(\gamma)}[\Omega] \subset F^{(\delta)}[\Omega]$ y la función

$$G = F^{(\gamma)} \circ (F^{(\delta)})^{-1} : \Omega \longrightarrow \Omega$$

es creciente. Por lo tanto $F^{(\delta)}(\alpha) \leq F^{(\delta)}(G(\alpha)) = F^{(\gamma)}(\alpha)$. Si

$$\alpha < F(\alpha) = F^{(0)}(\alpha) \leq F^{(\delta)}(\alpha),$$

entonces $F^{(\delta)}(\alpha) < F^{(\delta)}(F^{(\delta)}(\alpha))$, luego $F^{(\delta)}(\alpha)$ no es un punto fijo de $F^{(\delta)}$, luego no puede estar en la imagen de $F^{(\gamma)}$ y no puede ser $F^{(\delta)}(\alpha) = F^{(\gamma)}(\alpha)$. ∎

Las derivadas sucesivas de derivadas sucesivas de una función son derivadas sucesivas de la función de partida:

Teorema 6.42 *Para todo par de ordinales γ, ϵ se cumple que $(F^{(\gamma)})^{(\epsilon)} = F^{(\gamma+\epsilon)}$.*

Demostración: Por inducción sobre ϵ. Para $\epsilon = 0$ es inmediato. Veamos ahora el caso $\epsilon = 1$. Basta tener en cuenta que $F^{(\gamma+1)}$ es la función que enumera los puntos fijos comunes de todas las derivadas $F^{(\delta)}$, con $\delta \leq \gamma$, pero éstos son simplemente los puntos fijos de $F^{(\gamma)}$, pues todo punto fijo de esta derivada lo es de las anteriores. Pero la función que enumera los puntos fijos de $F^{(\gamma)}$ no es sino $(F^{(\gamma)})' = (F^{(\gamma)})^{(1)}$. De aquí se sigue que si el teorema vale para ϵ también vale para $\epsilon + 1$, pues

$$(F^{(\gamma)})^{(\epsilon+1)} = ((F^{(\gamma)})^{(\epsilon)})^{(1)} = (F^{(\gamma+\epsilon)})^{(1)} = F^{(\gamma+\epsilon+1)}.$$

Por último, si ϵ es un ordinal límite y el teorema vale para todo $\delta < \epsilon$, entonces $(F^{(\gamma)})^{(\epsilon)}$ enumera los puntos fijos comunes de todas las funciones $(F^{(\gamma)})^{(\delta)} = F^{(\gamma+\delta)}$, para todo $\delta < \epsilon$, mientras que $F^{(\gamma+\epsilon)}$ enumera los puntos fijos comunes de las funciones $F^{(\beta)}$, con $\beta < \gamma + \epsilon$. Basta observar que ambas clases de puntos fijos son la misma, pues todo $\beta < \gamma + \epsilon$ es de la forma $\beta = \gamma + \delta$ o bien $\beta < \gamma$, y en este segundo caso todo punto fijo de una función $F^{(\gamma+\delta)}$ es también un punto fijo de $F^{(\beta)}$. ∎

Ejemplo 1 *Los puntos fijos de la función $F(\alpha) = \beta + \alpha$ son los ordinales $\geq \beta \cdot \omega$, por lo que sus derivadas son las funciones $F^{(\gamma)}(\alpha) = \beta\omega^\gamma + \alpha$.*

En efecto, la primera parte es el teorema 3.48 y el ejercicio posterior, y la función que enumera los ordinales $\geq \beta \cdot \omega$ es precisamente $F'(\alpha) = \beta\omega + \alpha$.

Si $F^{(\gamma)}(\alpha) = \beta\omega^\gamma + \alpha$, entonces

$$F^{(\gamma+1)}(\alpha) = (F^{(\gamma)})'(\alpha) = \beta\omega^\gamma\omega + \alpha = \beta\omega^{\gamma+1} + \alpha.$$

Si la expresión para la derivada es cierta para todo exponente $\delta < \lambda$, entonces la derivada $F^{(\lambda)}$ es la función que enumera a los puntos fijos de todas las funciones $F^{(\delta)}(\alpha) = \beta\omega^\delta + \alpha$, es decir, a los ordinales que son mayores o iguales que $\beta\omega^\delta$ para todo $\delta < \lambda$, que son precisamente los ordinales mayores o iguales que $\beta\omega^\lambda$, luego $F^{(\lambda)}(\alpha) = \beta\omega^\lambda + \alpha$. ∎

Ejemplo 2 *Los puntos fijos de $F(\alpha) = \beta\alpha$ (para $\beta > 0$) son los ordinales de la forma $\beta^\omega\alpha$, por lo que sus derivadas son las funciones $F^{(\gamma)}(\alpha) = \beta^{\omega^\gamma}\alpha$.*

Ciertamente, $F(\beta^\omega\alpha) = \beta\beta^\omega\alpha = \beta^{1+\omega}\alpha = \beta^\omega\alpha$. Recíprocamente, si se cumple $F(\delta) = \delta$, dividimos $\delta = \beta^\omega\alpha + \epsilon$, con $\epsilon < \beta^\omega$, y tenemos que

$$\delta = F(\delta) = \beta\beta^\omega\alpha + \beta\epsilon = \delta + \beta\epsilon,$$

luego $\beta\epsilon = 0$, luego $\epsilon = 0$ y $\delta = \beta^\omega\alpha$.

La función que enumera los ordinales $\beta^\omega\alpha$ es $F'(\alpha) = \beta^\omega\alpha$. Si se cumple $F^{(\gamma)}(\alpha) = \beta^{\omega^\gamma}(\alpha)$, también

$$F^{(\gamma+1)}(\alpha) = (F^{(\gamma)})'(\alpha) = (\beta^{\omega^\gamma})^\omega\alpha = \beta^{\omega^{\gamma+1}}\alpha.$$

Si la expresión vale para las derivadas de índice $\delta < \lambda$, entonces $F^{(\lambda)}$ es la función que enumera a los ordinales que son múltiplos de β^{ω^δ} para todo $\delta < \lambda$. Basta probar que éstos son los de la forma $\beta^{\omega^\lambda}\alpha$.

Por una parte, por 3.49 tenemos que $\beta^{\omega^\lambda}\alpha = \beta^{\omega^\delta+\omega^\lambda}\alpha = \beta^{\omega^\delta}\beta^{\omega^\lambda}\alpha$, luego en efecto, $\beta^{\omega^\lambda}\alpha$ es múltiplo de todos los β^{ω^δ} con $\delta < \lambda$.

Recíprocamente, si ζ es múltiplo de todos los β^{ω^δ}, para $\delta < \lambda$, dividimos $\zeta = \beta^{\omega^\lambda}\alpha + \epsilon$, con $\epsilon < \beta^{\omega^\lambda}$, con lo que, por la definición de la exponencial, existe un $\delta' < \omega^\lambda$ tal que $\epsilon < \beta^{\delta'}$, luego existe un $\delta < \lambda$ tal que $\delta' < \omega^\delta$ y $\epsilon < \beta^{\omega^\delta}$, pero entonces $\zeta = \beta^{\omega^\delta}\beta^{\omega^\lambda}\alpha + \epsilon$ y, por la unicidad del resto de la división euclídea, dado que ζ es múltiplo de β^{ω^δ}, tiene que ser $\epsilon = 0$, luego $\zeta = \beta^{\omega^\lambda}\alpha$. ∎

Los puntos fijos de las funciones exponenciales ya no pueden expresarse en términos de sumas, productos y potencias:

Definición 6.43 Se llama función ϵ a la derivada de la función $F(\alpha) = \omega^\alpha$

De este modo, los números ϵ_α son precisamente los números épsilon que definimos en 3.53 y, según probamos justo a continuación, ϵ_0 es el mismo ordinal considerado allí, ya que es el menor número épsilon.

Más en general, las derivadas $F^{(\gamma)}$ de la función $F(\alpha) = \omega^\alpha$ se suelen representar con la notación ϕ_γ y reciben el nombre de *funciones de Veblen.* Así, $\phi_0(\alpha) = \omega^\alpha$ y $\phi_1(\alpha) = \epsilon_\alpha$.

Los números épsilon incluyen a todos los cardinales no numerables. Más en general:

Teorema 6.44 *Si κ es un cardinal no numerable y $\delta < \kappa$ entonces $\phi_\delta(\kappa) = \kappa$.*

DEMOSTRACIÓN: Supongamos en primer lugar que κ es regular y veamos por inducción que $\phi_\delta|_\kappa : \kappa \longrightarrow \kappa$.

Para $\delta = 0$ hay que probar que $\delta < \kappa \to \omega^\delta < \kappa$, pero una simple inducción sobre δ muestra que $|\omega^\delta| = \aleph_0|\delta|$ (para $\delta > 0$), luego $\omega^\delta < \kappa$.

Si vale para δ, entonces, como $\phi_\delta|_\kappa$ es una función normal, su conjunto de puntos fijos es un c.n.a. $C \subset \kappa$, luego tiene cardinal κ, pero su ordinal tiene que ser $\leq \kappa$, luego es κ, luego la función que enumera C tiene dominio κ, luego se trata de $\phi_{\delta+1}|_\kappa$, luego $\phi_{\delta+1}|_\kappa : \kappa \longrightarrow \kappa$.

Si el resultado vale para todo $\beta < \lambda < \kappa$, entonces el conjunto de puntos fijos de $\phi_\beta|_\kappa$ es el rango de $\phi_{\beta+1}|_\kappa$, que es un cerrado no acotado en κ. La intersección de menos de κ cerrados no acotados es cerrada no acotada, y tiene ordinal κ, luego $\phi_\lambda|_\kappa : \kappa \longrightarrow \kappa$.

La normalidad de las funciones ϕ_δ implica así que $\phi_\delta(\kappa) = \bigcup_{\epsilon<\kappa} \phi_\delta(\epsilon) \leq \kappa$, luego $\phi_\delta(\kappa) = \kappa$.

Si κ no es regular, es un cardinal límite, y es el supremo de cardinales regulares, que son puntos fijos de cada ϕ_δ, luego κ es también punto fijo de ϕ_δ. ∎

En particular, $\phi_\delta(\alpha)$ es un ordinal numerable siempre que δ y α son numerables.

Observemos que, como $0 < \omega^0$, el teorema 6.41 implica que la sucesión $\{\phi_\alpha(0)\}_{\alpha\in\Omega}$ es estrictamente creciente, luego $\alpha \leq \phi_\alpha(0)$, para todo ordinal α.

En particular, $\alpha < \phi_\alpha(\alpha)$ para todo α (el caso $\alpha = 0$ se comprueba por separado), luego si κ es un cardinal no numerable, por una parte tenemos que ningún $\alpha < \kappa$ puede ser punto fijo de todas las funciones ϕ_δ, con $\delta < \kappa$ (no lo es para $\delta = \alpha$), mientras que κ sí que lo es, por el teorema anterior, luego concluimos que $\phi_\kappa(0) = \kappa$.

Observemos ahora que si $\delta < \epsilon$, entonces cualquier $\phi_\epsilon(\alpha)$ es, por construcción, un punto fijo de ϕ_δ, con lo que tenemos que $\phi_\delta(\phi_\epsilon(\alpha)) = \phi_\epsilon(\alpha)$. Éste es el único caso no trivial en que dos funciones de Veblen pueden coincidir:

Teorema 6.45 *La igualdad $\phi_\delta(\alpha) = \phi_\epsilon(\beta)$ sólo puede darse en uno de los tres casos siguientes:*

1. $\delta = \epsilon \wedge \alpha = \beta$,
2. $\delta < \epsilon \wedge \alpha = \phi_\epsilon(\beta)$,
3. $\epsilon < \delta \wedge \beta = \phi_\delta(\alpha)$.

Similarmente, la desigualdad $\phi_\delta(\alpha) < \phi_\epsilon(\beta)$ sólo puede darse en uno de los tres casos siguientes:

1. $\delta = \epsilon \wedge \alpha < \beta$,
2. $\delta < \epsilon \wedge \alpha < \phi_\epsilon(\beta)$,
3. $\epsilon < \delta \wedge \phi_\delta(\alpha) < \beta$.

DEMOSTRACIÓN: Probamos simultáneamente las dos partes: si $\delta = \epsilon$, es obvio que tiene que ser $\alpha = \beta$ en el primer caso y $\alpha < \beta$ en el segundo.

Supongamos que $\delta < \epsilon$. Entonces $\phi_\epsilon(\beta)$ es punto fijo de ϕ_δ, luego se cumple que $\phi_\delta(\phi_\epsilon(\beta)) = \phi_\epsilon(\beta) \geq \phi_\delta(\alpha)$, luego $\phi_\epsilon(\beta) \geq \alpha$ (con igualdad en el primer caso y desigualdad estricta en el segundo). El caso restante es análogo. Notemos que siempre que se da uno de los tres casos se tiene la igualdad o la desigualdad del enunciado. ∎

Esto nos da un tipo de representación única en términos de funciones de Veblen. Veamos antes un caso particular:

Teorema 6.46 *Todo ordinal de la forma $\alpha = \omega^\beta$ se expresa de forma única como $\alpha = \phi_\delta(\eta)$, con $\eta < \alpha$.*

DEMOSTRACIÓN: La unicidad se debe al teorema anterior: si tuviéramos dos representaciones $\alpha = \phi_\delta(\eta) = \phi_\epsilon(\eta')$, no puede ser $\delta < \epsilon$, pues eso obliga a que $\eta = \phi_\epsilon(\eta') = \alpha$, pero suponemos $\eta < \alpha$. Tampoco puede ser $\epsilon < \delta$, luego $\delta = \epsilon \wedge \eta = \eta'$.

Para probar la existencia observamos que $\alpha \leq \phi_\alpha(0) < \phi_\alpha(\alpha)$, luego podemos tomar el mínimo ordinal δ tal que $\alpha < \phi_\delta(\alpha)$. Si es $\delta = 0$ tenemos que $\alpha = \omega^\beta < \phi_0(\alpha) = \omega^\alpha$, luego $\beta < \alpha$ y sirve la representación $\alpha = \phi_0(\eta)$ con $\eta = \beta$.

Si $\delta > 0$, entonces, por la minimalidad de δ, para todo $\epsilon < \delta$ tenemos que $\phi_\epsilon(\alpha) \leq \alpha$, pero como ϕ_ϵ es normal, se cumple de hecho que $\phi_\epsilon(\alpha) = \alpha$. Así, α es un punto fijo de todas las funciones ϕ_ϵ, con $\epsilon < \delta$, luego existe un η tal que $\alpha = \phi_\delta(\eta) < \phi_\delta(\alpha)$, luego $\eta < \alpha$. ∎

Observemos que, en las condiciones del teorema anterior,

$$\delta \leq \phi_\delta(0) \leq \phi_\delta(\eta) = \alpha,$$

y si se da la igualdad es porque $\phi_\delta(0) = \phi_\delta(\eta)$, luego $\eta = 0$, luego $\alpha = \phi_\alpha(0)$.

Definición 6.47 Un ordinal α es *fuertemente crítico* si $\alpha = \phi_\alpha(0)$.

Acabamos de probar que si $\alpha = \omega^\beta$ no es fuertemente crítico entonces se expresa de forma única como $\phi_\delta(\eta)$ con $\delta, \eta < \alpha$

La existencia de ordinales fuertemente críticos se sigue de la caracterización siguiente:

Teorema 6.48 *Un ordinal ξ es fuertemente crítico si y sólo si*

$$\xi > 0 \wedge \bigwedge \alpha\beta < \xi \ \phi_\alpha(\beta) < \xi.$$

DEMOSTRACIÓN: Si ξ es fuertemente crítico, es claro que $\xi \neq 0$ y si $\alpha, \beta < \xi$, entonces $\phi_\alpha(\beta) < \phi_\alpha(\xi) = \xi$, pues $\xi = \phi_\xi(0)$ es punto fijo de todas las funciones ϕ_α con $\alpha < \xi$.

Recíprocamente, si $\xi > 0$ cumple la condición del enunciado, en particular $1 = \phi_0(0) < \xi$ y $\omega = \phi_0(1) < \xi$. Además ξ tiene que ser un ordinal límite, pues si fuera $\xi = \delta + 1$ entonces $\delta \leq \phi_\delta(0) < \phi_\delta(\delta) < \xi$, luego $\xi = \delta + 1 \leq \phi_\delta(\delta) < \xi$.

Por otra parte, $\bigwedge \delta < \xi \ \omega^\delta < \xi$, luego $\omega^\xi = \xi$, luego ξ es un número ϵ, luego es cerrado para sumas, productos y potencias.

Veamos por inducción sobre α que $\alpha < \phi_\xi(0) \to \alpha < \xi$.

Para $\alpha = 0$ es trivial. Supongamos que vale para todo $\delta < \alpha < \phi_\xi(0)$. Descomponemos $\alpha = \omega^\eta + \beta$, con $\beta < \alpha$ (teorema 3.50). Si $\beta \neq 0$, entonces $\omega^\eta, \beta < \alpha$, luego por hipótesis de inducción $\omega^\eta, \beta < \xi$ y, como ξ es cerrado para sumas, $\alpha < \xi$. Por lo tanto podemos suponer que $\alpha = \omega^\eta$. El teorema 6.46 nos da entonces que $\alpha = \phi_\delta(\eta')$, con $\eta' < \alpha$.

Si también $\delta < \alpha$, entonces por hipótesis de inducción $\delta, \eta' < \xi$, luego $\alpha < \xi$ por la clausura de ξ. Si, por el contrario $\alpha = \phi_\alpha(\eta') \geq \phi_\alpha(0) > \alpha$, tiene que ser $\eta' = 0$, y tenemos que $\alpha = \phi_\alpha(0) < \phi_\xi(0)$, y esto implica $\alpha < \xi$, porque la sucesión $\{\phi_\alpha(0)\}_{\alpha\in\Omega}$ es estrictamente creciente.

Concluimos entonces que $\phi_\xi(0) = \xi$. ∎

Teorema 6.49 *La clase de los ordinales fuertemente críticos es c.n.a. en Ω.*

DEMOSTRACIÓN: Si κ es un cardinal regular no numerable, consideramos la aplicación $f : \kappa \times \kappa \longrightarrow \kappa$ dada por $f(\alpha, \beta) = \phi_\alpha(\beta)$, que está bien definida por el teorema 6.44, y aplicamos el teorema 6.7 y el teorema anterior. Obtenemos que el conjunto C_κ de los ordinales fuertemente críticos menores que κ es c.n.a. en κ. Es claro que esto implica el resultado para Ω. ∎

En particular, existen $\aleph_1$ ordinales fuertemente críticos numerables.

Definición 6.50 Se llama $\Gamma : \Omega \longrightarrow \Omega$ a la función (normal) que enumera a los ordinales fuertemente críticos. El ordinal Γ_0 se llama *ordinal de Feferman-Schütte.*

Sabemos que Γ_0 es un número ϵ cerrado para sumas, productos, potencias y la función ϕ (vista como función de dos argumentos). Es claro que es mucho mayor que ϵ_0.

Hemos probado que si $\alpha = \omega^\beta < \Gamma_0$ entonces se expresa de forma única como $\alpha = \phi_\delta(\eta)$, con $\delta, \eta < \alpha$. Como todo ordinal no nulo se expresa de forma única como $\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n}$, para cierta sucesión decreciente de exponentes (teorema 3.51), concluimos:

Teorema 6.51 *Todo ordinal* $0 < \alpha < \Gamma_0$ *se expresa de forma única como*

$$\alpha = \phi_{\xi_0}(\eta_0) + \cdots + \phi_{\xi_n}(\eta_n),$$

donde $\phi_{\xi_0}(\eta_0) \geq \cdots \geq \phi_{\xi_n}(\eta_n)$, $\xi_i < \alpha$, $\eta_i < \phi_{\xi_i}(\eta_i) < \alpha$.

Si a su vez desarrollamos cada ξ_i y cada η_i en forma normal, y hacemos los mismo con los coeficientes de dichas formas normales, y continuamos el proceso, como los coeficientes que vamos obteniendo son cada vez menores, al cabo de un número finito de pasos tenemos que llegar a coeficientes iguales a 0, que no admiten más desarrollos. En suma, todo ordinal menor que Γ_0 puede calcularse en un número finito de pasos a partir de 0 en términos de sumas y aplicaciones de la función ϕ.

Recíprocamente, si construimos expresiones a partir de 0 y la función ϕ, para asegurarnos de que obtenemos formas normales sólo tenemos que evitar que al aplicar ϕ suceda $\phi_\xi(\eta) = \eta$, pero para que esto ocurra, es decir, para que η sea un punto fijo de ϕ_ξ, en particular tiene que ser de la forma ω^α, luego su forma canónica tiene que ser $\eta = \phi_{\xi'}(\eta')$ con $\eta' < \eta$ (es decir, tiene que tener un único sumando) y, según 6.45, la igualdad $\phi_\xi(\eta) = \phi_{\xi'}(\eta')$ sólo puede darse (y se da) si $\xi < \xi'$, pues los casos $\xi = \xi' \wedge \eta = \eta'$ o $\xi' < \xi \wedge \eta' = \phi_\xi(\eta) \geq \eta$ contradicen $\eta' < \eta$. En suma, para construir expresiones de ordinales en forma normal, sólo hay que evitar aplicar ϕ_ξ a los ordinales cuya forma normal es $\phi'_\xi(\eta')$ con $\xi < \xi'$.

Naturalmente, esto exige comparar formas normales, para lo cual aplicamos el mismo criterio que con la forma normal de Cantor (son formas normales de Cantor), lo que nos reduce el problema a comparar ordinales de la forma $\phi_\xi(\eta)$ y $\phi_{\xi'}(\eta')$, lo cual puede hacerse recurrentemente aplicando el teorema 6.45.

Capítulo VII

Álgebras de Boole

Introducimos ahora una estructura algebraica que proporciona un contexto general para tratar problemas de naturaleza muy diversa, tanto de teoría de conjuntos propiamente dicha, como de lógica, de topología, de análisis matemático o de estadística. Trabajamos en NBG sin el axioma de elección.

7.1 Propiedades algebraicas

El ejemplo típico de álgebra de Boole es $\mathcal{P}X$, donde X es un conjunto arbitrario. En $\mathcal{P}X$ están definidas las operaciones de unión, intersección y complemento respecto de X. Si axiomatizamos las propiedades básicas de estas operaciones llegamos a la noción general de álgebra de Boole:

Definición 7.1 Un *álgebra de Boole* es una cuádrupla $(\mathbb{B}, \wedge, \vee, ')$, donde $\mathbb{B}$ es un conjunto no vacío, $\wedge\colon \mathbb{B}\times\mathbb{B}\longrightarrow\mathbb{B}$, $\vee\colon \mathbb{B}\times\mathbb{B}\longrightarrow\mathbb{B}$ y $'\colon \mathbb{B}\longrightarrow\mathbb{B}$ son aplicaciones que cumplen las propiedades siguientes:

1) $p'' = p$,
2) $p \wedge q = q \wedge p$,
3) $(p \wedge q) \wedge r = p \wedge (q \wedge r)$,
4) $p \wedge p = p$,
5) $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$,
6) $p \vee (p \wedge q) = p$,
7) $(p \wedge q)' = p' \vee q'$,
8) $p \vee p' = q \vee q'$.

A partir de las propiedades 1) y 7) se demuestra que en realidad un álgebra de Boole cumple también las propiedades que resultan de intercambiar $\wedge$ por $\vee$ en los axiomas anteriores. En total, en un álgebra de Boole se cumple:

1)	$p'' = p$,	
2)	$p \wedge q = q \wedge p$,	$p \vee q = q \vee p$,
3)	$(p \wedge q) \wedge r = p \wedge (q \wedge r)$,	$(p \vee q) \vee r = p \vee (q \vee r)$,
4)	$p \wedge p = p$,	$p \vee p = p$,
5)	$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$,	$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$,
6)	$p \vee (p \wedge q) = p$,	$p \wedge (p \vee q) = p$,
7)	$(p \wedge q)' = p' \vee q'$,	$(p \vee q)' = p' \wedge q'$,
8)	$p \vee p' = q \vee q'$,	$p \wedge p' = q \wedge q'$.

Por ejemplo,

$$p \vee q = p'' \vee q'' = (p' \wedge q')' = (q' \wedge p')' = q'' \vee p'' = q \vee p.$$

Igualmente se razonan las demás.

Si $\mathbb{B}$ es un álgebra de Boole, la propiedad 8) establece que existen unos únicos elementos $\mathbb{0}$, $\mathbb{1} \in \mathbb{B}$ tales que para todo $p \in \mathbb{B}$ se cumple $p \wedge p' = \mathbb{0}$, $p \vee p' = \mathbb{1}$. Las propiedades siguientes s demuestran sin dificultad:

$$\begin{array}{ll} \mathbb{0}' = \mathbb{1}, & \mathbb{1}' = \mathbb{0}, \\ p \wedge p' = \mathbb{0}, & p \vee p' = \mathbb{1}, \\ p \vee \mathbb{0} = p, & p \wedge \mathbb{1} = p, \\ p \vee \mathbb{1} = \mathbb{1}, & p \wedge \mathbb{0} = \mathbb{0}. \end{array}$$

Por ejemplo, $p \vee \mathbb{0} = p \vee (p \wedge p') = p$, por la propiedad 6). Igualmente, $p \vee \mathbb{1} = p \vee (p \vee p') = (p \vee p) \vee p' = p \vee p' = \mathbb{1}$.

El lector familiarizado con la lógica proposicional verá una clara relación entre ésta y las álgebras de Boole, que se completa con las definiciones siguientes:

$$p \to q = p' \vee q, \qquad p \leftrightarrow q = (p \to q) \wedge (q \to p).$$

La relación de orden Toda álgebra de Boole tiene una estructura natural de conjunto parcialmente ordenado determinada por el teorema siguiente:

Teorema 7.2 *Sea $\mathbb{B}$ un álgebra de Boole. Entonces la relación en $\mathbb{B}$ dada por*

$$p \leq q \text{ syss } p \wedge q = p \text{ syss } p \vee q = q$$

es una relación de orden parcial (y en lo sucesivo consideraremos a toda álgebra de Boole como conjunto parcialmente ordenado con esta relación). Además se cumplen los hechos siguientes:

1. *$p \wedge q$ es el ínfimo del conjunto $\{p, q\}$,*
2. *$p \vee q$ es el supremo del conjunto $\{p, q\}$,*
3. *$p \leq q$ syss $q' \leq p'$.*
4. *$\mathbb{0}$ y $\mathbb{1}$ son el mínimo y el máximo de $\mathbb{B}$ respectivamente.*
5. *$p \leq q$ syss $p \to q = \mathbb{1}$, y $(p \leftrightarrow q) = \mathbb{1}$ syss $p = q$.*
6. *$p = q'$ syss $p \wedge q = \mathbb{0}$ y $p \vee q = \mathbb{1}$.*

Demostración: Si $p \wedge q = p$, entonces $p \vee q = (p \wedge q) \vee q = q$, por la propiedad 6) de la definición de álgebra de Boole. Igualmente se tiene la otra implicación.

La relación $\leq$ es reflexiva por la propiedad 4). La antisimetría es trivial. En cuanto a la transitividad, si $p \leq q$ y $q \leq r$ entonces

$$p \wedge r = (p \wedge q) \wedge r = p \wedge (q \wedge r) = p \wedge q = p,$$

luego $p \leq r$.

1) Se cumple que $p \wedge q \wedge p = p \wedge p \wedge q = p \wedge q$, luego $p \wedge q \leq p$. Igualmente $p \wedge q \leq q$. Por otra parte, si $r \leq p$ y $r \leq q$ entonces $p \wedge q \wedge r = p \wedge r = r$, luego $r \leq p \wedge q$. Esto prueba que $p \wedge q$ es el ínfimo de $\{p, q\}$.

2) es análogo a 1).

3) Si $p \leq q$ entonces $p \wedge q = p$, luego $p' \vee q' = p'$, luego $q' \leq p'$.

4) es trivial.

5) Si $p \leq q$ entonces $(p \to q) = p' \vee q = p' \vee p \vee q = \mathbb{1} \vee q = \mathbb{1}$.

Si $(p \to q) = \mathbb{1}$, entonces $p' \vee q = \mathbb{1}$, luego

$$p = p \wedge \mathbb{1} = p \wedge (p' \vee q) = (p \wedge p') \vee (p \wedge q) = \mathbb{0} \vee (p \wedge q) = p \wedge q.$$

Así pues, $p \leq q$.

Por último, $(p \leftrightarrow q) = \mathbb{1}$ syss $(p \to q) = (q \to p) = \mathbb{1}$, syss $p \leq q \wedge q \leq p$, syss $p = q$.

6) Tenemos que

$$q = \mathbb{1} \wedge q = (p \vee p') \wedge q = (p \wedge q) \vee (p' \wedge q) = \mathbb{0} \vee (p' \wedge q)$$

$$= (p' \wedge p) \vee (p' \wedge q) = p' \wedge (p \vee q) = p' \wedge \mathbb{1} = p'. \qquad \blacksquare$$

En lo sucesivo consideraremos siempre como conjuntos parcialmente ordenados a las álgebras de Boole con la relación de orden dada por el teorema anterior.

Definición 7.3 Diremos que un álgebra de Boole $\mathbb{B}$ es *degenerada* si $\mathbb{0} = \mathbb{1}$.

Teniendo en cuenta que $\mathbb{0}$ y $\mathbb{1}$ son el mínimo y el máximo de $\mathbb{B}$ es claro que $\mathbb{B}$ es degenerada si y sólo si $\mathbb{B} = \{\mathbb{0}\} = \{\mathbb{1}\}$.

Vamos a trabajar únicamente con álgebras no degeneradas, es decir, que en lo sucesivo entenderemos que "álgebra de Boole" significa "álgebra de Boole no degenerada".

La estructura de anillo Veamos ahora que las álgebras de Boole también tienen una estructura natural de anillo:

Teorema 7.4 *toda álgebra de Boole $\mathbb{B}$ tiene estructura de anillo conmutativo y unitario con las operaciones dadas por*

$$p + q = (p \wedge q') \vee (p' \wedge q) = (p \vee q) \wedge (p \wedge q)' = (p \leftrightarrow q)', \quad p \cdot q = p \wedge q.$$

El elemento neutro de la suma es $\mathbb{0}$ y el del producto es $\mathbb{1}$. Además, se cumple que $\bigwedge b \in \mathbb{B}\ b = -b$.

DEMOSTRACIÓN: Se trata de una comprobación rutinaria. La parte más farragosa es demostrar la asociatividad de la suma:

$$\begin{aligned}(p+q)+r &= ((p+q)\wedge r')\vee((p+q)'\wedge r)\\ &= (((p\wedge q')\vee(p'\wedge q))\wedge r')\vee(((p\vee q)\wedge(p'\vee q'))'\wedge r)\\ &= (p\wedge q'\wedge r')\vee(p'\wedge q\wedge r')\vee(((p\vee q)'\vee(p'\vee q')')\wedge r)\\ &= (p\wedge q'\wedge r')\vee(p'\wedge q\wedge r')\vee(((p'\wedge q')\vee(p\wedge q))\wedge r)\\ &= (p\wedge q'\wedge r')\vee(p'\wedge q\wedge r')\vee(p'\wedge q'\wedge r)\vee(p\wedge q\wedge r),\end{aligned}$$

y es claro que esta expresión no se altera si intercambiamos las posiciones de p, q, r, luego si partimos de $p+(q+r)$ llegamos al mismo resultado. ∎

En lo sucesivo consideraremos siempre a las álgebras de Boole como anillos con estas operaciones. Observemos que, al igual que hemos definido la suma y el producto a partir de las operaciones booleanas $\wedge$, $\vee$ y $'$, también podemos definir las operaciones booleanas a partir de la suma y el producto:

$$x\wedge y = xy, \quad x\vee y = x+y+xy, \quad x' = \mathbb{1}+x\ (=\mathbb{1}-x).$$

Ejercicio: Un *anillo booleano* es un anillo conmutativo y unitario $\mathbb{B}$ que cumple además la propiedad $\bigwedge b\in\mathbb{B}\ bb=b$. Probar que toda álgebra de Boole es un anillo booleano, y que todo anillo booleano se convierte en un álgebra de Boole con las operaciones $\wedge$, $\vee$ y $'$ dadas por las relaciones precedentes.

Subálgebras Si $\mathbb{B}$ es un álgebra de Boole, diremos que un conjunto $\mathbb{C}\subset\mathbb{B}$ es una *subálgebra* de $\mathbb{B}$ si $\mathbb{C}\neq\varnothing$ y para todo p, $q\in\mathbb{C}$ se cumple que $p\wedge q$, $p\vee q$, $p'\in\mathbb{C}$. Entonces $\mathbb{C}$ es un álgebra con las restricciones de las operaciones de $\mathbb{B}$.

Es claro que $\mathbb{0}$ y $\mathbb{1}$ son los mismos en $\mathbb{B}$ y en $\mathbb{C}$ y que la relación de orden $\leq$ en $\mathbb{C}$, así como la suma y el producto en $\mathbb{C}$ son las restricciones de las de $\mathbb{B}$. De hecho, dado que las operaciones de anillo se definen a partir de las de álgebra y viceversa, es claro que las subálgebras de $\mathbb{B}$ coinciden con sus subanillos.

Obviamente $\mathbb{B}$ es una subálgebra de $\mathbb{B}$, las subálgebras de $\mathbb{B}$ distintas de la propia $\mathbb{B}$ se llaman subálgebras *propias.* Además, $\{\mathbb{0},\mathbb{1}\}$ es una subálgebra de $\mathbb{B}$, a la que llamaremos subálgebra *trivial.* Un álgebra $\mathbb{B}$ es *trivial* si coincide con su subálgebra trivial, es decir, si $\mathbb{B}=\{\mathbb{0},\mathbb{1}\}$.

Ejemplo: Álgebras de conjuntos Como ya hemos señalado, si X es un conjunto arbitrario, entonces $\mathbb{B}=\mathcal{P}X$ es un álgebra de Boole tomando como operaciones:

$$x\wedge y = x\cap y, \quad x\vee y = x\cup y, \qquad x' = X\setminus x.$$

Es una simple rutina comprobar que se cumplen todas las propiedades que exige la definición de álgebra de Boole. Además, es claro entonces que

$$\mathbb{0}=\varnothing, \quad \mathbb{1}=X, \quad x\leq y \quad \text{syss} \quad x\subset y.$$

La suma en $\mathcal{P}X$ se corresponde con la operación conjuntista conocida como *diferencia simétrica:*

$$X \triangle Y = (X \setminus Y) \cup (Y \setminus X) = (X \cup Y) \setminus (X \cap Y).$$

En particular vemos que un álgebra $\mathcal{P}X$ es degenerada si y sólo si $X = \varnothing$, mientras que $\mathcal{P}X$ es trivial si y sólo si $|X| = 1$.

Llamaremos *álgebras de conjuntos* a las subálgebras de un álgebra $\mathcal{P}X$. Equivalentemente, un conjunto $\mathbb{B}$ es un *álgebra de conjuntos* sobre un conjunto X si $\mathbb{B} \subset \mathcal{P}X$ y para todo x, $y \in \mathbb{B}$ se cumple que $x \cup y$, $x \cap y$, $X \setminus x \in \mathbb{B}$.

De este modo, si $\mathbb{B}$ es un álgebra de conjuntos sobre X, sus operaciones son la unión, la intersección y el complemento respecto de X, su relación de orden es la inclusión, su suma es la diferencia simétrica y además $\mathbb{0} = \varnothing$, $\mathbb{1} = X$.

Por ejemplo, si X es un espacio topológico (no vacío), el conjunto $\mathbb{B}$ de los subconjuntos de X que son a la vez abiertos y cerrados es un álgebra de conjuntos (no degenerada) sobre X, que es trivial si y sólo si X es conexo. ∎

Restricción de álgebras de Boole Si $\mathbb{B}$ es un álgebra de Boole y $a \in \mathbb{B}$ es un elemento no nulo, definimos

$$\mathbb{B}_a = \{b \in \mathbb{B} \mid b \leq a\}.$$

Una comprobación rutinaria muestra que $\mathbb{B}_a$ se convierte en un álgebra de Boole con las mismas operaciones $\wedge$ y $\vee$ de $\mathbb{B}$ y el complemento dado por $b' = a \wedge b'$ (donde el b' de la derecha es la operación de $\mathbb{B}$). Se cumple además que $\mathbb{0}$ es el mismo de $\mathbb{B}$ y $\mathbb{1} = a$. Notemos que $\mathbb{B}_a$ no es una subálgebra de $\mathbb{B}$ (salvo en el caso trivial en que $a = \mathbb{1}$). ∎

Álgebras atómicas Un *átomo* en un álgebra de Boole $\mathbb{B}$ es un elemento $a \in \mathbb{B}$ tal que $a \neq \mathbb{0}$ y no existe ningún $b \in \mathbb{B}$ tal que $\mathbb{0} < b < a$. Un álgebra de Boole $\mathbb{B}$ es *atómica* si para todo $b \in \mathbb{B}$ no nulo existe un átomo $a \in \mathbb{B}$ tal que $a \leq b$.

Por ejemplo, en un álgebra $\mathcal{P}X$, los átomos son los subconjuntos de X de la forma $\{a\}$, y es claro entonces que las álgebras de tipo $\mathcal{P}X$ son atómicas. ∎

Generadores Se comprueba inmediatamente que la intersección de una familia de subálgebras de un álgebra dada $\mathbb{B}$ es de nuevo una subálgebra. Por consiguiente, si $X \subset \mathbb{B}$, podemos definir la *subálgebra generada* por X en $\mathbb{B}$ como la intersección de todas las subálgebras de $\mathbb{B}$ que contienen a X. La representaremos por $\langle X \rangle$.

Es claro que si $X \subset \mathbb{C} \subset \mathbb{B}$, donde $\mathbb{C}$ es una subálgebra de $\mathbb{B}$, entonces la subálgebra generada por X en $\mathbb{C}$ coincide con la subálgebra generada por X en $\mathbb{B}$. Si $\mathbb{B} = \langle X \rangle$ diremos que X es un *generador* de $\mathbb{B}$.

Teorema 7.5 *Si $\mathbb{B}$ es un álgebra de Boole y $X \subset \mathbb{B}$, el álgebra $\langle X \rangle$ está formada por los elementos de la forma:*

$$\bigvee_{i=1}^{n} \bigwedge_{j=1}^{k_i} x_{ij}, \qquad x_{ij} \in X \cup X'.$$

DEMOSTRACIÓN: Sea $\mathbb{A}$ el conjunto de los elementos de $\mathbb{B}$ que tienen la forma indicada. Claramente $\mathbb{A} \subset \langle X \rangle$. Si probamos que $\mathbb{A}$ es una subálgebra de $\mathbb{B}$, tendremos también la inclusión opuesta. Lo veremos en varios pasos. El primero es inmediato:

1. *Si $a \in \mathbb{A}$ y $x \in X \cup X'$, entonces $a \wedge x \in \mathbb{A}$.*
2. *Si $a, b \in \mathbb{A}$, entonces $a \wedge b \in \mathbb{A}$.*
   En efecto, si $b = \bigvee_{i=1}^{n} \bigwedge_{j=1}^{k_i} x_{ij}$, la propiedad anterior nos da $a \wedge x_{i1} \in \mathbb{A}$, de donde a su vez $a \wedge x_{i1} \wedge x_{i2} \in \mathbb{A}$ y, en definitiva, $a \wedge \bigwedge_{j=1}^{k_i} x_{ij} \in \mathbb{A}$. Pero es inmediato que el supremo de un número finito de elementos de $\mathbb{A}$ está en $\mathbb{A}$, luego de aquí concluimos que $a \wedge b \in \mathbb{A}$.
3. *Si $a \in \mathbb{A}$, entonces $a' \in \mathbb{A}$.*
   En efecto, si $a = \bigvee_{i=1}^{n} \bigwedge_{j=1}^{k_i} x_{ij}$, entonces $a' = \bigwedge_{i=1}^{n} \bigvee_{j=1}^{k_i} x'_{ij}$ que es un ínfimo de elementos de $\mathbb{A}$, luego está en $\mathbb{A}$ por la propiedad anterior. ∎

Del teorema anterior se sigue inmediatamente:

Teorema 7.6 *Toda álgebra de Boole finitamente generada es finita.*

Homomorfismos Diremos que una aplicación $h : \mathbb{B} \longrightarrow \mathbb{C}$ entre álgebras de Boole es un *homomorfismo de álgebras* si para todo $p, q \in \mathbb{B}$ se cumple

$$h(p') = h(p)', \qquad h(p \wedge q) = h(p) \wedge h(q), \qquad h(p \vee q) = h(p) \vee h(q).$$

Es claro que si se da la primera condición las otras dos son equivalentes, por lo que es suficiente comprobar una de las dos. También es claro que un homomorfismo de álgebras de Boole cumple

$$h(p + q) = h(p) + h(q), \quad h(pq) = h(p)h(q), \quad h(\mathbb{0}) = \mathbb{0}, \quad h(\mathbb{1}) = \mathbb{1}$$

y si $p \leq q$ entonces $h(p) \leq h(q)$.

En particular, los homomorfismos de álgebras de Boole son homomorfismos de anillos (de hecho, es claro que una aplicación entre álgebras de Boole es un homomorfismo de álgebras de Boole si y sólo si es un homomorfismo de anillos). En particular, $h[\mathbb{B}]$ es una subálgebra de $\mathbb{C}$.

El teorema 7.5 muestra que si dos homomorfismos de álgebras de Boole coinciden en un generador, entonces son iguales.

Un *monomorfismo, epimorfismo, isomorfismo de álgebras de Boole* es un homomorfismo inyectivo, suprayectivo o biyectivo, respectivamente. Un *automorfismo* de álgebras es un isomorfismo de un álgebra en sí misma.

La composición de homomorfismos es un homomorfismo, la inversa de un isomorfismo es un isomorfismo. Todo isomorfismo de álgebras es una semejanza de conjuntos parcialmente ordenados y el recíproco también es cierto, pues las semejanzas conservan supremos e ínfimos y, si p es un elemento de un álgebra el complemento p' está caracterizado como el único elemento q que cumple las relaciones $p \wedge q = \mathbb{0}$, $p \vee q = \mathbb{1}$.

Ideales, filtros y cocientes Los ideales de las álgebras de Boole tienen una caracterización muy simple en términos de las operaciones del álgebra:

Definición 7.7 Si $\mathbb{B}$ es un álgebra de Boole, un *ideal* de $\mathbb{B}$ es un conjunto $I \subset \mathbb{B}$ que cumpla las propiedades siguientes:

1. $\mathbb{0} \in I \wedge \mathbb{1} \notin I$,
2. $\bigwedge p \in I \bigwedge q \in \mathbb{B}\ (q \leq p \to q \in I)$,
3. $\bigwedge pq \in I\ p \vee q \in I$.

   Diremos que es un *ideal primo* si además cumple

4. $\bigwedge p \in \mathbb{B}\ p \in I \vee p' \in I$.

Un *filtro* de $\mathbb{B}$ es un conjunto $F \subset \mathbb{B}$ que cumpla las propiedades siguientes:

1. $\mathbb{0} \notin F \wedge \mathbb{1} \in F$,
2. $\bigwedge p \in F \bigwedge q \in \mathbb{B}\ (p \leq q \to q \in F)$,
3. $\bigwedge pq \in F\ p \wedge q \in F$.

   Diremos que es un *ultrafiltro* si además cumple

4. $\bigwedge p \in \mathbb{B}\ p \in F \vee p' \in F$.

Si definimos el *conjunto dual* de un conjunto $X \subset \mathbb{B}$ como $X' = \{p' \mid p \in X\}$, es claro que I es un ideal (resp. un ideal primo) si y sólo si el conjunto dual I' es un filtro (resp. un ultrafiltro) y que F es un filtro (resp. un ultrafiltro) si y sólo si F' es un ideal (resp. un ideal primo).

Observemos que los filtros y ultrafiltros en un álgebra $\mathcal{P}X$ no son sino lo que en 4.30 hemos llamado filtros y ultrafiltros en X.

Hemos definido así el concepto de ideal de un álgebra para que la definición no dependa del teorema 7.4, pero en realidad los ideales de un álgebra de Boole $\mathbb{B}$ en este sentido son simplemente los ideales de $\mathbb{B}$ como anillo distintos del propio $\mathbb{B}$. Además, los ideales primos en este sentido coinciden con los ideales primos en el sentido de la teoría de anillos, y también con los ideales maximales.

En efecto, si I es un ideal en este sentido y x, $y \in I$, entonces $x + y \leq x \vee y$, luego $x + y \in I$, y si $x \in \mathbb{B} \wedge y \in I$, entonces $xy \leq y$, luego $xy \in I$. Esto prueba que I es un ideal en el sentido de la teoría de anillos. Recíprocamente, si $I \neq \mathbb{B}$ es un ideal en este sentido general, ciertamente $\mathbb{0} \in I \wedge \mathbb{1} \notin I$, si $p \in I \wedge q \in \mathbb{B} \wedge q \leq p$, entonces $q = qp \in I$, y si p, $q \in I$, entonces $p \vee q = p + q + pq \in I$, luego I es un ideal en el sentido de la definición anterior.

La afirmación sobre ideales primos y maximales será inmediata después de la observación siguiente:

Si $\mathbb{B}$ es un álgebra de Boole e I es un ideal de $\mathbb{B}$, el anillo cociente $\mathbb{B}/I$ tiene estructura de álgebra de Boole con las operaciones dadas por

$$[p] \wedge [q] = [p \wedge q], \quad [p] \vee [q] = [p \vee q], \quad [p]' = [p'].$$

En efecto, es fácil probar que las operaciones están bien definidas, aunque tenemos una justificación indirecta, pues pueden definirse a partir de la suma y el producto, que ya sabemos que están bien definidas:

$$[p] \wedge [q] = [p][q], \quad [p] \vee [q] = [p] + [q] + [p][q], \quad [p]' = [p] + \mathbb{1}.$$

Una vez está justificado que las operaciones están bien definidas, cada propiedad de la definición de álgebra de Boole se cumple en $\mathbb{B}/I$ como consecuencia inmediata de que se cumple en $\mathbb{B}$.

Así pues, nos referiremos a $\mathbb{B}/I$ como el *álgebra cociente* determinada por I. Si F es un filtro en $\mathbb{B}$, representaremos por $\mathbb{B}/F$ al álgebra cociente determinada por el ideal dual F'.

Notemos que si I es un ideal y F es su filtro dual, la congruencia módulo I (es decir, la relación de equivalencia que determina el cociente $\mathbb{B}/I = \mathbb{B}/F$) viene dada por

$$p + q \in I \qquad \text{syss} \qquad p \leftrightarrow q \in F.$$

Observemos también que, como en la definición de ideal hemos exigido la condición $\mathbb{1} \notin I$, las álgebras cociente son no degeneradas.

Ahora es inmediato que I es un ideal primo (en el sentido de la definición anterior) si y sólo si $\mathbb{B}/I = \{\mathbb{0}, \mathbb{1}\}$, pero es claro que el álgebra trivial $\{\mathbb{0}, \mathbb{1}\}$ es la única álgebra que es un dominio íntegro (pues si un álgebra $\mathbb{B}$ contiene un tercer elemento p, entonces $pp' = \mathbb{0}$, luego p es un divisor de cero y $\mathbb{B}$ no es un dominio íntegro), luego en particular es también la única álgebra que es un cuerpo. Ahora el teorema 1.39 implica inmediatamente que los ideales primos de un álgebra en el sentido de la definición anterior coinciden con los ideales primos y maximales en el sentido general de la teoría de anillos.

A su vez, esto implica que un filtro F en un álgebra de Boole $\mathbb{B}$ es un ultrafiltro si y sólo si es maximal, en el sentido de que no existe ningún filtro $F \subsetneq G \subsetneq \mathbb{B}$.

Si $f : \mathbb{B} \longrightarrow \mathbb{C}$ es un homomorfismo de álgebras de Boole, los conjuntos

$$N(f) = \{b \in \mathbb{B} \mid f(b) = \mathbb{0}\}, \qquad N(f)' = \{b \in \mathbb{B} \mid f(b) = \mathbb{1}\}$$

son un ideal y un filtro mutuamente duales. El primero es el *núcleo* de f y el segundo su filtro dual. Claramente, la proyección natural $i : \mathbb{B} \longrightarrow \mathbb{B}/I$ es un epimorfismo de álgebras de Boole con núcleo I.

Generación de filtros e ideales Diremos que un subconjunto X de un álgebra de Boole $\mathbb{B}$ tiene la *propiedad de la intersección finita* si para cualquier conjunto finito de elementos $x_1, \ldots, x_n \in X$ se cumple $x_1 \wedge \cdots \wedge x_n \neq \mathbb{0}$.

Diremos que un conjunto $x_1, \ldots, x_n$ de elementos de $\mathbb{B}$ es un *cubrimiento finito* si $x_1 \vee \cdots \vee x_n = \mathbb{1}$.

El teorema siguiente se demuestra sin dificultad:

Teorema 7.8 *Sea $\mathbb{B}$ un álgebra de Boole.*

1. *La intersección de una familia de ideales/filtros de $\mathbb{B}$ es un ideal/filtro.*
2. *Si $X \subset \mathbb{B}$ tiene la propiedad de la intersección finita, entonces el conjunto*

$$(X)_f = \{p \in \mathbb{B} \mid \text{existen } n \in \omega \text{ y } x_1, \ldots, x_n \in X \text{ tales que } x_1 \wedge \cdots \wedge x_n \leq p\}$$

   es un filtro de $\mathbb{B}$ que contiene a X y está contenido en cualquier otro filtro de $\mathbb{B}$ que contenga a X. Se le llama filtro generado *por X.*

3. *Si $X \subset \mathbb{B}$ no contiene cubrimientos finitos, entonces el conjunto*

$$(X)_i = \{p \in \mathbb{B} \mid \text{existen } n \in \omega \text{ y } x_1, \ldots, x_n \in X \text{ tales que } p \leq x_1 \vee \cdots \vee x_n\}$$

   es un ideal de $\mathbb{B}$ que contiene a X y está contenido en cualquier otro ideal de $\mathbb{B}$ que contenga a X. Se le llama ideal generado *por X.*

4. *Si $f : \mathbb{B} \longrightarrow \mathbb{C}$ es un homomorfismo de álgebras y F e I son un filtro y un ideal duales en $\mathbb{C}$, entonces $f^{-1}[F]$ y $f^{-1}[I]$ son un filtro y un ideal duales en $\mathbb{B}$.*

Ejemplo Si $\mathbb{B} = \mathcal{P}A$ y $a \in A$, entonces el filtro generado por un átomo $\{a\}$ es

$$(a)_f = \{X \in \mathcal{P}A \mid a \in X\}$$

y es inmediato que se trata de hecho de un ultrafiltro. Los ultrafiltros de esta forma se llaman *ultrafiltros fijos,* mientras que los que no son de esta forma se llaman *ultrafiltros libres.* Observemos que si un filtro F de $\mathbb{B}$ contiene un átomo $\{a\}$ entonces $(a)_f \subset F$, luego $F = (a)_f$, porque $(a)_f$ es maximal. En particular un ultrafiltro es fijo si y sólo si contiene un átomo $\{a\}$.

Recíprocamente, si un ultrafiltro F es libre, entonces cada átomo $\{a\}$ está en el ideal dual F', luego cada conjunto finito está en F' (porque la unión finita de elementos de F' está en F'). Notemos que

$$\text{fin} = \{X \in \mathcal{P}A \mid X \text{ es finito}\}$$

es un ideal en $\mathcal{P}A$, cuyo filtro dual es el formado por los conjuntos cofinitos:

$$\text{fin}^* = \{X \in \mathcal{P}A \mid A \setminus X \text{ es finito}\}.$$

Acabamos de justificar que un ultrafiltro F es libre si y sólo si $\text{fin}^* \subset F$. ∎

La existencia de ultrafiltros libres no puede demostrarse sin AE, pero una aplicación elemental del lema de Zorn (compárese con 4.29) nos da los teoremas siguientes:

Teorema 7.9 (de los ideales primos)(AE) *Todo ideal en un álgebra de Boole puede extenderse hasta un ideal primo.*

Teorema 7.10 (de los ultrafiltros) (AE) *Todo filtro en un álgebra de Boole puede extenderse hasta un ultrafiltro.*

En particular, los ultrafiltros en $\mathcal{P}A$ que extienden al filtro $\mathcal{F}$ formado por los conjuntos cofinitos son ultrafiltros libres.

Veamos una aplicación del teorema 7.5:

Teorema 7.11 *Si $\mathbb{B} = \langle X\rangle$ es un álgebra de Boole, un filtro F en $\mathbb{B}$ es un ultrafiltro si y sólo si para todo $x \in X$ se cumple que $x \in F$ o $x' \in F$.*

Demostración: Un elemento arbitrario de $\mathbb{B}$ es $b = \bigvee_{i=1}^{n} \bigwedge_{j=1}^{k_i} x_{ij}$, con $x_{ij} \in X$. Si existe un i tal que, para todo j se cumple $x_{ij} \in F$, entonces $\bigwedge_{j=1}^{k_i} x_{ij} \in F$, luego $b \in F$. En caso contrario, para todo i existe un j tal que $x'_{ij} \in F$, de donde $\bigvee_{j=1}^{k_i} x'_{ij} \in F$ y, tomando el ínfimo de estos elementos, $b' \in F$. ∎

7.2 Espacios de Stone

A la hora de demostrar que un álgebra de Boole satisface determinadas relaciones, como la asociatividad de la suma, demostrada en la prueba del teorema 7.4, tenemos que recurrir en principio a las identidades de la definición de álgebra, mientras que si nos restringimos al caso de un álgebra de conjuntos podemos justificar las igualdades como igualdades conjuntistas, es decir, tomando un elemento arbitrario de un miembro y probando que está en el otro, y viceversa, lo cual suele ser más sencillo. Ahora vamos a probar que este método es general, pues toda álgebra de Boole es isomorfa a un álgebra de conjuntos.

En esta sección usaremos el axioma de elección, pero conviene observar que únicamente lo haremos a través del teorema 7.9, o de 7.10, que es equivalente.

Definición 7.12 Sea $\mathbb{B}$ un álgebra de Boole. Llamaremos $S(\mathbb{B})$ al conjunto de todos los ultrafiltros de $\mathbb{B}$. Para cada $p \in \mathbb{B}$ definimos

$$C_p = \{x \in S(\mathbb{B}) \mid p \in x\}, \qquad \tilde{\mathbb{B}} = \{C_p \mid p \in \mathbb{B}\}.$$

Teorema 7.13 (Teorema de representación de Stone) *Si $\mathbb{B}$ es un álgebra de Boole, entonces $\tilde{\mathbb{B}}$ es un álgebra de conjuntos sobre $S(\mathbb{B})$ y la aplicación $h : \mathbb{B} \longrightarrow \tilde{\mathbb{B}}$ dada por $h(p) = C_p$ es un isomorfismo de álgebras.*

Demostración: Dados $p, q \in \mathbb{B}$, se cumple que

$$x \in C_p \cap C_q \text{ syss } p \in x \wedge q \in x \text{ syss } p \wedge q \in x \text{ syss } x \in C_{p\wedge q}.$$

Así pues, $C_{p\wedge q} = C_p \cap C_q$. Por otra parte,

$$x \in S(\mathbb{B}) \setminus C_p \text{ syss } p \notin x \text{ syss } p' \in x \text{ syss } x \in C_{p'},$$

luego $C_{p'} = S(\mathbb{B}) \setminus C_p$.

Esto prueba que $\tilde{\mathbb{B}}$ es un álgebra de conjuntos y que $h : \mathbb{B} \longrightarrow \tilde{\mathbb{B}}$ es un epimorfismo de álgebras. Para probar que h es inyectiva basta comprobar que si $h(p) = \varnothing$ entonces[1] $p = \mathbb{0}$. En efecto, si $C_p = \varnothing$ tenemos que p no pertenece a ningún ultrafiltro de $\mathbb{B}$, pero todo elemento no nulo de un álgebra genera un filtro que, a su vez, por 7.10, está contenido en un ultrafiltro. Por tanto $p = \mathbb{0}$.

■

Veamos ahora que el teorema de Stone se puede refinar notablemente:

Definición 7.14 Sea $\mathbb{B}$ un álgebra de Boole. Entonces, por ser un álgebra de conjuntos, $\tilde{\mathbb{B}}$ es la base de una topología sobre $S(\mathbb{B})$. Llamaremos *espacio de Stone* del álgebra $\mathbb{B}$ al espacio $S(\mathbb{B})$ con la topología generada por $\tilde{\mathbb{B}}$.

Teorema 7.15 *Sea $\mathbb{B}$ un álgebra de Boole. Entonces $S(\mathbb{B})$ es un espacio de Hausdorff compacto cerodimensional y $\tilde{\mathbb{B}}$ es su álgebra de abiertos-cerrados. Por consiguiente, el teorema de representación de Stone afirma que toda álgebra de Boole es isomorfa al álgebra de abiertos-cerrados de su espacio de Stone.*

Demostración: Sean $x, y \in S(\mathbb{B})$, $x \neq y$. Entonces existe un $p \in x$ tal que $p \notin y$, luego $p \in x$, $p' \in y$, luego $x \in C_p \wedge y \in C_{p'}$, y ciertamente $C_p \cap C_{p'} = \varnothing$, luego C_p y $C_{p'}$ son entornos disjuntos de x e y. Esto prueba que $S(\mathbb{B})$ es un espacio de Hausdorff.

Consideremos un cubrimiento abierto de $S(\mathbb{B})$ que podemos suponer formado por abiertos básicos, es decir, de la forma $\{C_p\}_{p\in I}$, con $I \subset \mathbb{B}$. Si el cubrimiento no admite subcubrimientos finitos, dados $p_1, \ldots, p_n \in I$, tendríamos que $C_{p_1} \cup \cdots \cup C_{p_n} \neq S(\mathbb{B}) = C_{\mathbb{1}}$, luego $p_1 \vee \cdots \vee p_n \neq \mathbb{1}$, luego I no contiene cubrimientos finitos de $\mathbb{B}$, luego genera un ideal que está contenido en un ideal primo P de $\mathbb{B}$. Llamemos $x \in S(\mathbb{B})$ a su ultrafiltro dual.

Entonces, si $p \in I$, tenemos que $p \in P$, luego $p' \in x$, luego $x \notin C_p$, y esto contradice que $\{C_p\}_{p\in I}$ sea un cubrimiento de $S(\mathbb{B})$. Por lo tanto $S(\mathbb{B})$ es compacto.

Claramente los elementos de $\tilde{B}$ son abiertos-cerrados en $S(\mathbb{B})$ y falta probar que son todos los abiertos-cerrados. En efecto, cualquiera de ellos entonces es unión de abiertos de $S(\mathbb{B})$, pero por compacidad es unión de un número finito de ellos, luego está en $\tilde{\mathbb{B}}$. ■

Los ultrafiltros de un álgebra de Boole $\mathbb{B}$ son los puntos de su espacio de Stone $S(\mathbb{B})$. Ahora vamos a probar que los filtros de $\mathbb{B}$ se corresponden con los cerrados de $S(\mathbb{B})$:

[1] Esto es cierto para todo homomorfismo de anillos: si $h(u) = 0 \to u = 0$ entonces h es un monomorfismo, pues si $h(u) = h(v)$, entonces $h(u - v) = 0$, luego $u - v = 0$, luego $u = v$.

Teorema 7.16 *Sea $\mathbb{B}$ un álgebra de Boole.*

1. *Si F es un filtro en $\mathbb{B}$, entonces $C_F = \{x \in S(\mathbb{B}) \mid F \subset x\}$ es un cerrado no vacío en $S(\mathbb{B})$.*
2. *Si $C \subset S(\mathbb{B})$ es un cerrado no vacío, entonces $F_C = \{p \in \mathbb{B} \mid C \subset C_p\}$ es un filtro en $\mathbb{B}$.*
3. *Las correspondencias $F \mapsto C_F$ y $C \mapsto F_C$ son biyecciones mutuamente inversas entre los filtros de $\mathbb{B}$ y los cerrados no vacíos de $S(\mathbb{B})$.*

DEMOSTRACIÓN: Se cumple que $C_F \neq \varnothing$ pues esto equivale a que todo filtro está contenido en un ultrafiltro. Que C_F es cerrado se sigue de que $C_F = \bigcap_{p\in F} C_p$.

En efecto, $x \in C_F$ si y sólo si $F \subset x$, si y sólo si $\bigwedge p \in \mathbb{B}(p \in F \to p \in x)$, lo cual equivale a $\bigwedge p \in \mathbb{B}(p \in F \to x \in C_p)$, lo cual equivale a que $x \in \bigcap_{p\in F} C_p$.

La comprobación de que F_C es un filtro no ofrece ninguna dificultad.

Dado un filtro F en $\mathbb{B}$, se cumple $p \in F_{C_F}$ si y sólo si $C_F \subset C_p$, lo cual equivale a que, para todo ultrafiltro $x \in S(\mathbb{B})$, si $F \subset x$, entonces $p \in x$, y esto sucede exactamente cuando $p \in F$, pues si $p \notin F$, entonces, para todo $a \in F$, se cumple que $a \wedge p' \neq \mathbb{0}$ (o de lo contrario $a \leq p$, luego $p \in F$), luego $F \cup \{p'\}$ genera un filtro, que estará contenido en un ultrafiltro $x \in S(\mathbb{B})$ tal que $F \subset x$ y $p \notin x$. Así pues, $F_{C_F} = F$.

Igualmente, dado un cerrado no vacío $C \subset S(\mathbb{B})$, se cumple que $x \in C_{F_C}$ si y sólo si $F_C \subset x$, si y sólo si, para todo $p \in \mathbb{B}$, si $C \subset C_p$, entonces $p \in x$, lo cual sólo puede ocurrir si $x \in C$, pues si $x \in S(\mathbb{B}) \setminus C$, como C es cerrado, existe un $p \in \mathbb{B}$ tal que $x \in C_p \subset S(\mathbb{B}) \setminus C$, luego $C \subset C_{p'} = S(\mathbb{B}) \setminus C_p$, pero $p' \notin x$. Así pues, $C_{F_C} = C$. ∎

Notemos que, a través de la correspondencia dada por el teorema anterior, si F es un ultrafiltro en $\mathbb{B}$ (y, por consiguiente, también un punto $F = x \in S(\mathbb{B})$) su cerrado asociado es

$$C_x = \{y \in S(\mathbb{B}) \mid x \subset y\} = \{x\}.$$

Equivalentemente, para todo $x \in S(\mathbb{B})$, se cumple que $F_{\{x\}} = x$.

Observemos que si $\mathbb{B}$ es un álgebra de Boole y $p \in \mathbb{B}$, entonces p es un átomo si y sólo si no tiene extensiones no nulas, si y sólo si C_p no contiene estrictamente abiertos no vacíos, si y sólo si $C_p = \{x\}$ para cierto $x \in S(\mathbb{B})$, que será un punto aislado. Recíprocamente, todo punto aislado determina un abierto básico de $S(\mathbb{B})$ que a su vez determina un átomo de $\mathbb{B}$. Es fácil ver que estas correspondencias son mutuamente inversas, de modo que existe una biyección entre los átomos de un álgebra de Boole y los puntos aislados de su espacio de Stone.

Un álgebra de Boole es atómica si y sólo si cada elemento no nulo está por encima de un átomo, lo cual equivale a que los puntos aislados en $S(\mathbb{B})$ sean un conjunto denso.

Los teoremas siguientes demuestran que hay una correspondencia natural entre las álgebras de Boole y los espacios compactos cerodimensionales.

Teorema 7.17 *Sea K un espacio compacto cerodimensional y sea $\mathbb{B}$ su álgebra de abiertos-cerrados. Entonces K es homeomorfo a $S(\mathbb{B})$.*

Demostración: Sea $f : K \longrightarrow S(\mathbb{B})$ dada por $f(x) = \{C \in \mathbb{B} \mid x \in C\}$. Claramente $f(x)$ es un ultrafiltro en $\mathbb{B}$ y f es suprayectiva, pues si $p \in S(\mathbb{B})$ entonces p es una familia de cerrados en K con la propiedad de la intersección finita, luego existe un $x \in K$ que pertenece a todos los elementos de p, es decir, tal que $p \subset f(x)$. Por la maximalidad de p ha de ser $f(x) = p$.

Si x, y son puntos distintos en K, entonces existe un $C \in \mathbb{B}$ tal que $x \in C$, $y \notin C$, luego $C \in f(x) \setminus f(y)$, lo que prueba que f es inyectiva.

Es fácil ver que para todo $A \in \mathbb{B}$ se cumple $f^{-1}[A] = A$, lo que prueba que f es continua y, por compacidad, un homeomorfismo. ∎

Teorema 7.18 *Sea $f : \mathbb{B} \longrightarrow \mathbb{C}$ un homomorfismo de álgebras de Boole. Entonces la aplicación $f^* : S(\mathbb{C}) \longrightarrow S(\mathbb{B})$ dada por $f^*(x) = \{p \in \mathbb{B} \mid f(p) \in x\}$ es continua. Además f es inyectiva si y sólo si f^* es suprayectiva y f es suprayectiva si y sólo si f^* es inyectiva.*

Demostración: Es inmediato comprobar que $f^*(x) \in S(\mathbb{B})$. Además $(f^*)^{-1}[C_p] = C_{f(p)}$, luego f^* es continua.

Si f es inyectiva e $y \in S(\mathbb{B})$, es fácil ver que $\{f(p) \mid p \in y\}$ tiene la propiedad de la intersección finita en $\mathbb{C}$, luego está contenido en un ultrafiltro $x \in S(\mathbb{C})$. Es fácil comprobar así mismo que $f^*(x) = y$.

Si f^* es suprayectiva y $p \in \mathbb{B}$ es no nulo, entonces p está contenido en un ultrafiltro $y \in S(\mathbb{B})$, que tendrá una antiimagen $x \in S(\mathbb{C})$. Así $p \in y = f^*(x)$, luego $f(p) \in x$, luego $f(p) \neq \mathbb{0}$. Así pues, f es inyectiva.

Si f es suprayectiva y $f^*(x) = f^*(y)$, para ciertos x, $y \in S(\mathbb{C})$, entonces para todo $p \in \mathbb{B}$ se cumple $f(p) \in x$ syss $f(p) \in y$, pero esto significa que $x = y$, luego f^* es inyectiva.

Si f^* es suprayectiva entonces es un homeomorfismo en la imagen, luego, dado $q \in \mathbb{C}$, se cumple que $f^*[C_q]$ es abierto en $f^*[S(\mathbb{C})]$, con lo que $f^*[C_q] = f^*[S(\mathbb{C})] \cap A$, donde A es un abierto en $S(\mathbb{B})$. Tenemos que A es unión de abiertos básicos de $\mathbb{B}$, los cuales forman un cubrimiento abierto del compacto $f^*[C_q]$, luego podemos extraer un subcubrimiento finito cuya unión es un abierto básico C_p tal que $f^*[C_q] \subset C_p \subset A$. Por consiguiente $f^*[C_q] = f^*[S(\mathbb{C})] \cap C_p$. Esto implica que $C_q = (f^*)^{-1}[C_p]$, luego

$$\bigwedge x \in S(\mathbb{C})(x \in C_q \leftrightarrow f^*(x) \in C_p),$$

$$\bigwedge x \in S(\mathbb{C})(x \in C_q \leftrightarrow p \in f^*(x)),$$

$$\bigwedge x \in S(\mathbb{C})(x \in C_q \leftrightarrow f(p) \in x),$$

$$\bigwedge x \in S(\mathbb{C})(x \in C_q \leftrightarrow c \in C_{f(p)}),$$

y esto significa que $C_q = C_{f(p)}$, por lo que $f(p) = q$. Así pues, f es suprayectiva. ∎

Teorema 7.19 *Sean $\mathbb{B}$ y $\mathbb{C}$ dos álgebras de Boole y sea $f : S(\mathbb{B}) \longrightarrow S(\mathbb{C})$ una aplicación continua. Entonces la aplicación $f^* : \mathbb{C} \longrightarrow \mathbb{B}$ que a cada $q \in \mathbb{C}$ le asigna el único $p \in \mathbb{B}$ tal que $f^{-1}[C_q] = C_p$ es un homomorfismo de álgebras. Además $f^{**} = f$. Si $g : \mathbb{B} \longrightarrow \mathbb{C}$ es un homomorfismo de álgebras, también se cumple que $g^{**} = g$.*

DEMOSTRACIÓN: No tiene ninguna dificultad probar que f^* es un homomorfismo. Si $x \in S(\mathbb{B})$, entonces

$$f^{**}(x) = \{q \in \mathbb{C} \mid f^*(q) \in x\} = \{q \in \mathbb{C} \mid x \in C_{f^*(q)}\} = \{q \in \mathbb{C} \mid x \in f^{-1}[C_q]\}$$

$$= \{q \in \mathbb{C} \mid f(x) \in C_q\} = \{q \in C \mid q \in f(x)\} = f(x).$$

Si $g : \mathbb{B} \longrightarrow \mathbb{C}$ es un homomorfismo de álgebras y $p \in \mathbb{B}$, entonces $g^{**}(p) = q$ es equivalente a $(g^*)^{-1}[C_p] = C_q$, que a su vez equivale a las fórmulas siguientes:

$\bigwedge x \in S(\mathbb{C})(p \in g^*(x) \leftrightarrow q \in x)$

$\bigwedge x \in S(\mathbb{C})(g(p) \in x \leftrightarrow q \in x)$

$\bigwedge x \in S(\mathbb{C})(x \in C_{g(p)} \leftrightarrow x \in C_q)$,

$C_{g(p)} = C_q$, luego $g^{**}(p) = q$ syss $g(p) = q$, es decir, $g^{**} = g$. ∎

En definitiva, tenemos que a cada álgebra de Boole le corresponde un espacio compacto cerodimensional (su espacio de Stone) y a cada espacio compacto cerodimensional le corresponde un álgebra de Boole (su álgebra de abiertos-cerrados). Además los homomorfismos de álgebras se corresponden con las aplicaciones continuas, de modo que los isomorfismos se corresponden con los homeomorfismos. De este modo álgebras isomorfas tienen espacios de Stone homeomorfos y viceversa.

Nota Esto nos da una prueba alternativa más breve del teorema 7.6: Como $S(\{\mathbb{0}, \mathbb{1}\})$ consta de un único punto, los puntos de $S(\mathbb{B})$ se corresponden biunívocamente con las aplicaciones continuas $S(\{\mathbb{0}, \mathbb{1}\}) \longrightarrow S(\mathbb{B})$, que a su vez se corresponden con los homomorfismos $\mathbb{B} \longrightarrow \{\mathbb{0}, \mathbb{1}\}$. Si $\mathbb{B}$ es finitamente generada, cada homomorfismo está determinado por las imágenes de un generador finito, luego hay un número finito de homomorfismos, luego $S(\mathbb{B})$ es finito, luego $\mathbb{B}$ también. ∎

Teorema 7.20 *Si $\mathbb{B}$ es un álgebra de Boole y F es un filtro en $\mathbb{B}$, el espacio de Stone $S(\mathbb{B}/F)$ es homeomorfo al cerrado $C_F \subset S(\mathbb{B})$ dado por* 7.16. *Más aún, si $\mathcal{B}(C_F)$ es el álgebra de abiertos-cerrados de C_F, tenemos el diagrama conmutativo*

$$\begin{array}{ccccc} \mathbb{B} & & \longrightarrow & & \tilde{\mathbb{B}} \\ \downarrow{\scriptstyle \pi} & & & & \downarrow{\scriptstyle \tilde{\pi}} \\ \mathbb{B}/F & \longrightarrow & \widetilde{\mathbb{B}/F} & \longrightarrow & \mathcal{B}(C_F) \end{array}$$

donde $\tilde{\pi}(A) = A \cap C_F$ y las flechas horizontales son isomorfismos.

DEMOSTRACIÓN: Consideremos la proyección natural $\pi : \mathbb{B} \longrightarrow \mathbb{B}/F$, que se corresponde con una aplicación $\pi^* : S(\mathbb{B}/F) \longrightarrow S(\mathbb{B})$ inyectiva y continua. Como los espacios son compactos, $S(\mathbb{B}/F)$ es homeomorfo a su imagen K. Basta probar que $K = C_F$. Ahora bien, aplicando las definiciones se ve inmediatamente que K está formado por las antiimágenes $\pi^{-1}[y]$ de los ultrafiltros de $\mathbb{B}/F$, y es fácil ver que éstas son precisamente los ultrafiltros de $\mathbb{B}$ que contienen a F, es decir, los elementos de C_F.

Observemos que el isomorfismo natural $\widetilde{\mathbb{B}/F} \longrightarrow \mathcal{B}(C_F)$ es el dado por $A \mapsto \pi^*[A]$. Así, si $p \in B$, al recorrer el diagrama del enunciado empezando por el isomorfismo $p \mapsto C_p$ obtenemos $\tilde{\pi}(C_p) = C_p \cap C_F$, mientras que empezando por π llegamos a $\pi^*[C_{\pi(p)}]$, pero $x \in \pi^*[C_{\pi(p)}]$ si y sólo si $x = \pi^{-1}[y]$, para cierto $y \in C_{\pi(p)}$ (es decir, tal que $\pi(p) \in y$), lo cual equivale a que $x \in \pi^*[S(\mathbb{B}/F)]$ y $p \in x$, es decir, a que $x \in C_p \cap C_F$. ∎

Para terminar vamos a calcular el cardinal de $S(\mathcal{P}D)$, para cualquier conjunto infinito D, es decir, el cardinal del conjunto de los ultrafiltros en $\mathcal{P}D$. En realidad vamos a contar una familia más específica de ultrafiltros:

Definición 7.21 Si D es un conjunto infinito, un *ultrafiltro uniforme* en D es un ultrafiltro U en D tal que todos sus elementos tienen cardinal $|D|$.

Teorema 7.22 (Pospíšil) *Si D es un conjunto infinito, existen $2^{2^{|D|}}$ ultrafiltros uniformes en D.*

DEMOSTRACIÓN: Diremos que $C \subset \mathcal{P}D$ es una familia *uniformemente independiente* de subconjuntos de D si para todos los $X_1, \dots, X_m, Y_1, \dots, Y_n \in C$ distintos dos a dos se cumple que

$$X_1 \cap \cdots \cap X_m \cap (D \setminus Y_1) \cap \cdots \cap (D \setminus Y_n)$$

tiene cardinal $|D|$. Vamos a probar que existe una familia uniformemente independiente de cardinal $2^{|D|}$. Es claro que podemos sustituir D por cualquier otro conjunto del mismo cardinal, así que sustituimos D por $P = [D]^{<\omega} \times [[D]^{<\omega}]^{<\omega}$.

Para cada $u \subset D$ definimos

$$X_u = \{(A, B) \in P \mid A \cap u \in B\},$$

y llamamos $C = \{X_u \mid u \in \mathcal{P}D\}$. Vamos a probar que C cumple lo pedido. En primer lugar, si $u \neq v$ son dos subconjuntos de D, entonces $X_u \neq X_v$, pues si, por ejemplo, $d \in u \setminus v$, basta tomar $A = \{d\}$ y $B = \{A\}$, con lo que $(A, B) \in X_u$, pero $(A, B) \notin X_v$. Por lo tanto $|C| = 2^{|D|}$.

Tomemos ahora $u_1, \dots, u_m, v_1, \dots, v_n$ subconjuntos de D distintos dos a dos y fijemos elementos $d_{ij} \in (u_i \setminus v_j) \cup (v_j \setminus u_i)$ y sea $A \subset D$ finito que contenga a todos los d_{ij}. Observemos que hay $|D|$ conjuntos A posibles. Entonces tenemos que $A \cap u_i \neq A \cap v_j$ y, si llamamos $B = \{A \cap u_i \mid i = 1, \dots, m\}$, entonces $(A, B) \in X_{u_i} \setminus X_{v_j}$, luego la intersección

$$X_{u_1} \cap \cdots \cap X_{u_m} \cap (P \setminus X_{v_1}) \cap \cdots \cap (P \setminus X_{v_n})$$

contiene a todos los pares (A, B), que son $|D|$, luego la intersección tiene cardinal $|D| = |P|$.

Fijemos, pues, una familia uniformemente independiente C de subconjuntos de D con cardinal $2^{|D|}$. Para cada $f : C \longrightarrow 2$, sea

$$G_f = \{X \in \mathcal{P}D \mid |D \setminus X| < |D|\} \cup \{X \in C \mid f(X) = 1\} \cup$$
$$\{D \setminus X \mid X \in C \wedge f(X) = 0\}.$$

Observamos que G_f tiene la propiedad de la intersección finita, pues la intersección de un número finito de elementos de G_f es de la forma $X \cap Y$, donde $|D \setminus X| < |D|$ y $|Y| = |D|$ y, si fuera $X \cap Y = \varnothing$, entonces $Y \subset D \setminus X$, contradicción.

Por lo tanto, el teorema 7.8 nos da que G_f está contenido en un filtro en D que a su vez está contenido en un ultrafiltro U_f, necesariamente uniforme, pues U_f contiene a los complementarios de todos los conjuntos de cardinal menor que $|D|$, luego no puede contener a ninguno de ellos.

Por último basta observar que si $f \neq g$ entonces $U_f \neq U_g$, pues si, por ejemplo, $X \in C$ cumple $f(X) = 1$ y $g(X) = 0$, entonces $X \in U_f$ y $D \setminus X \in U_g$. ∎

Puesto que $2^{2^{|D|}}$ es también el cardinal de $\mathcal{P}\mathcal{P}D$, concluimos que el número total de ultrafiltros en D es como máximo este cardinal, y así:

Teorema 7.23 *Si D es un conjunto infinito, entonces $|S(\mathcal{P}D)| = 2^{2^{|D|}}$.*

7.3 Álgebras completas

Definición 7.24 Sea $\mathbb{B}$ un álgebra de Boole y $X \subset \mathbb{B}$. Representaremos por $\bigvee X$ y $\bigwedge X$ al supremo y al ínfimo de X en $\mathbb{B}$ (supuesto que existan). Ciertamente existen si X es finito. En particular $\bigvee \varnothing = \mathbb{0}$, $\bigwedge \varnothing = \mathbb{1}$.

También usaremos la notación

$$\bigvee_{i\in I} p_i = \bigvee\{p_i \mid i \in I\}, \qquad \bigwedge_{i\in I} p_i = \bigwedge\{p_i \mid i \in I\}.$$

Existe una relación sencilla entre los supremos e ínfimos:

Teorema 7.25 *Si $\mathbb{B}$ es un álgebra de Boole y $\{p_i\}_{i\in I}$ es una familia de elementos de $\mathbb{B}$, entonces*

$$\Big(\bigvee_{i\in I} p_i\Big)' = \bigwedge_{i\in I} p_i', \qquad \Big(\bigwedge_{i\in I} p_i\Big)' = \bigvee_{i\in I} p_i',$$

entendiendo que un miembro existe si y sólo si existe el otro.

Demostración: Supongamos que existe $\bigwedge_{i\in I} p_i'$. Entonces, para cada $i \in I$, tenemos que $\bigwedge_{i\in I} p_i' \leq p_i'$, luego $p_i \leq \big(\bigwedge_{i\in I} p_i'\big)'$, de modo que el miembro derecho es una cota superior del conjunto $\{p_i \mid i \in I\}$. Si r es cualquier cota superior, entonces $r' \leq p_i'$, luego $r' \leq \bigwedge_{i\in I} p_i'$, luego $\big(\bigwedge_{i\in I} p_i'\big)' \leq r$. Esto prueba que existe $\bigvee_{i\in I} p_i = \big(\bigwedge_{i\in I} p_i'\big)'$, luego en definitiva $\big(\bigvee_{i\in I} p_i\big)' = \bigwedge_{i\in I} p_i'$.

Si suponemos que existe el miembro izquierdo se razona análogamente que existe el miembro derecho. La segunda igualdad se obtiene de la primera aplicada a la familia $\{p'_i\}_{i\in I}$. ∎

Una formulación alternativa sin índices del teorema anterior es

$$\bigvee X' = (\bigwedge X)', \qquad \bigwedge X' = (\bigvee X)',$$

donde hay que entender que un miembro existe si y sólo si existe el otro.

Los supremos e ínfimos satisfacen la siguiente propiedad distributiva:

Teorema 7.26 *Si $\{p_{0i}\}_{i\in I}$, $\{p_{1j}\}_{j\in J}$ son dos familias de elementos de un álgebra de Boole $\mathbb{B}$, entonces*

$$\bigvee_{i\in I} p_{0i} \wedge \bigvee_{j\in J} p_{1j} = \bigvee_{(i,j)\in I\times J} (p_{0i} \wedge p_{1j}),$$

entendiendo que el miembro derecho existe si existen los dos supremos del miembro izquierdo.

Demostración: Vamos a usar varias veces la equivalencia siguiente:

$$p \wedge q \leq r \leftrightarrow q \leq r \vee p'.$$

En efecto, si $p \wedge q \leq r$, entonces

$$q = q \wedge (p \vee p') = (q \wedge p) \vee (q \wedge p') \leq r \vee p'.$$

Recíprocamente, si $q \leq r \vee p'$, entonces

$$p \wedge q \leq p \wedge (r \vee p') = (p \wedge r) \vee (p \wedge p') = p \wedge r.$$

Como

$$p_{0i} \wedge p_{1j} \leq p_{0i} \leq \bigvee_{i\in I} p_{0i} \qquad p_{0i} \wedge p_{1j} \leq p_{1j} \leq \bigvee_{j\in J} p_{1j},$$

vemos que $p_{0i} \wedge p_{1j} \leq \bigvee_{i\in I} p_{0i} \wedge \bigvee_{j\in J} p_{1j}$, luego el miembro derecho es una cota superior del conjunto $\{p_{0i} \wedge p_{1j} \mid (i,j) \in I \times J\}$. Para probar que es la mínima, tomamos una cota r arbitraria. Como $p_{0i} \wedge p_{1j} \leq r$, tenemos que $p_{0i} \leq r \vee p'_{1j}$ para todo i, luego $\bigvee_{i\in I} p_{0i} \leq r \vee p'_{1j}$, luego $\bigvee_{i\in I} p_{0i} \wedge p_{1j} \leq r$. Similarmente, $p_{1j} \leq r \vee \big(\bigvee_{i\in I} p_{0i}\big)'$, de donde $\bigvee_{j\in J} p_{1j} \leq r \vee \big(\bigvee_{i\in I} p_{0i}\big)'$, y de aquí concluimos que

$$\bigvee_{i\in I} p_{0i} \wedge \bigvee_{j\in J} p_{1j} \leq r.$$

Esto prueba que el miembro izquierdo es el supremo que en el enunciado aparece en el miembro derecho. ∎

Tomando complementos en la igualdad del teorema anterior aplicada a las familias de los complementos de las sucesiones dadas se obtiene inmediatamente la relación

$$\bigwedge_{i\in I} p_{0i} \vee \bigwedge_{j\in J} p_{1j} = \bigwedge_{(i,j)\in I\times J} (p_{0i} \vee p_{1j}).$$

En particular, si reducimos la primera familia a un único elemento, quedan las relaciones

$$p \wedge \bigvee_{i\in I} p_i = \bigvee_{i\in I} (p \wedge p_i), \qquad p \vee \bigwedge_{i\in I} p_i = \bigwedge_{i\in I} (p \vee p_i).$$

Definición 7.27 Un álgebra de Boole $\mathbb{B}$ es *completa* si todo conjunto $X \subset \mathbb{B}$ tiene supremo o, equivalentemente por las relaciones anteriores, si todo $X \subset \mathbb{B}$ tiene ínfimo.

Por ejemplo, si A es un conjunto arbitrario, es claro que $\mathcal{P}A$ es un álgebra completa, en la que, para todo $X \in \mathcal{P}A$, se cumple $\bigvee X = \bigcup X$, $\bigwedge X = \bigcap X$ (con el convenio de que $\bigcap \varnothing = A$).

Más aún, tenemos la caracterización siguiente de las álgebras de tipo $\mathcal{P}A$:

Teorema 7.28 *Un álgebra de Boole $\mathbb{B}$ es isomorfa a un álgebra $\mathcal{P}A$ si y sólo si es atómica y completa.*

Demostración: Obviamente, si $\mathbb{B} \cong \mathcal{P}A$, entonces $\mathbb{B}$ es atómica y completa. Supongamos ahora que $\mathbb{B}$ es atómica y completa y sea A el conjunto de sus átomos. Consideramos la aplicación $h : \mathbb{B} \longrightarrow \mathcal{P}A$ dada por

$$h(b) = \{a \in A \mid a \leq b\}.$$

Se cumple que h es inyectiva, pues si $b_1 \neq b_2$, podemos suponer que $b_1 \not\leq b_2$, con lo que $b_1 \wedge b_2' \neq 0$, luego existe un $a \in A$ tal que $a \leq b_1 \wedge b_2'$, luego $a \in h(b_1)$, pero $a \notin h(b_2)$, luego $h(b_1) \neq h(b_2)$.

También se cumple que h es suprayectiva, pues si $X \in \mathcal{P}A$, podemos considerar $b = \bigvee X \in \mathbb{B}$, y claramente $X \subset \{a \in A \mid a \leq b\} = h(b)$. Para probar la igualdad suponemos que $a_0 \in A$ cumple $a_0 \leq b$, pero $a_0 \notin X$. Entonces, como son átomos, $a_0 \wedge a = 0$, para todo $a \in X$, luego

$$a_0 = a_0 \wedge b = a_0 \wedge \bigvee_{a\in x} a = \bigvee_{a\in x} (a_0 \wedge a) = 0,$$

contradicción.

Es inmediato que si $b_1 \leq b_2$, entonces $h(b_1) \subset h(b_2)$, y también se da el recíproco, pues si $b_1 \not\leq b_2$, entonces $b_1 \wedge b_2' \neq 0$, luego existe $a \in A$ tal que $a \leq b_1 \wedge b_2'$, luego $a \leq b_1$ y $a \not\leq b_2$, luego $a \in h(b_1) \setminus h(b_2)$, luego $h(b_1) \not\leq h(b_2)$.

Así pues, h es una semejanza, luego un isomorfismo de álgebras. ∎

Ejercicio: Probar que toda álgebra de Boole finita es isomorfa a un álgebra $\mathcal{P}A$.

Ejemplo: Abiertos regulares Presentamos ahora una familia muy importante de álgebras de Boole completas:

Definición 7.29 Sea X un espacio topológico. Diremos que $A \subset X$ es un *abierto regular* si $A = \operatorname{int}\operatorname{cl}A$ (donde int y cl representan el interior y la clausura de un conjunto, respectivamente). Definimos $A^\perp = X \setminus \operatorname{cl}A$.

Por ejemplo, $]0,1[$ es un abierto regular en $\mathbb{R}$, mientras que $]0,1[\cup]1,2[$ no lo es.

En general, es claro que si $A \subset B \subset X$ entonces $B^\perp \subset A^\perp$ y $A^{\perp\perp} \subset B^{\perp\perp}$.

Observemos que $A^{\perp\perp} = X \setminus \operatorname{cl}A^\perp = \operatorname{int}(X \setminus A^\perp) = \operatorname{int}\operatorname{cl}A$. Así pues, A es un abierto regular si y sólo si $A = A^{\perp\perp}$.

Teorema 7.30 *Sean U y V subconjuntos de un espacio topológico X y supongamos que U es abierto. Entonces:*

1. $U^{\perp\perp\perp} = U^\perp$,
2. $V^{\perp\perp\perp\perp} = V^{\perp\perp}$,
3. $(U \cap V)^{\perp\perp} = U^{\perp\perp} \cap V^{\perp\perp}$.

Demostración: 1) Como $U \subset \operatorname{cl}U$ y U es abierto, de hecho

$$U \subset \operatorname{int}\operatorname{cl}U = U^{\perp\perp},$$

de donde $U^{\perp\perp\perp} \subset U^\perp$. Como $U^\perp \subset \operatorname{cl}U^\perp$ y $U^\perp$ es abierto, de hecho

$$U^\perp \subset \operatorname{int}\operatorname{cl}U^\perp = U^{\perp\perp\perp}.$$

Por consiguiente tenemos la igualdad.

2) Es consecuencia de 1) aplicado al abierto $U = V^\perp$.

3) Como $U \cap V \subset U$ y $U \cap V \subset V$, se cumple $(U \cap V)^{\perp\perp} \subset U^{\perp\perp} \cap V^{\perp\perp}$.

Para tener la otra inclusión basta ver que $U^{\perp\perp} \cap V^{\perp\perp} \subset \operatorname{cl}(U \cap V)$, pues como el conjunto de la izquierda es abierto, de hecho está contenido en el interior del de la derecha, es decir, en $(U \cap V)^{\perp\perp}$.

Sea, pues $x \in U^{\perp\perp} \cap V^{\perp\perp}$ y veamos que todo abierto G tal que $x \in G$ corta a $U \cap V$. Tenemos que $x \in G \cap U^{\perp\perp} \cap V^{\perp\perp}$, y este conjunto es abierto. Como $x \in U^{\perp\perp} = \operatorname{int}\operatorname{cl}U \subset \operatorname{cl}U$, ha de ser $G \cap U^{\perp\perp} \cap V^{\perp\perp} \cap U \neq \varnothing$. Sea, pues, $t \in G \cap U^{\perp\perp} \cap V^{\perp\perp} \cap U \subset V^{\perp\perp} = \operatorname{int}\operatorname{cl}V \subset \operatorname{cl}V$. Como $G \cap U$ es un abierto que contiene a t, ha de ser $G \cap U \cap V \neq \varnothing$, como teníamos que probar. ∎

Teorema 7.31 *Si X es un espacio topológico, el conjunto $R(X)$ de los abiertos regulares de X es un álgebra de Boole completa con las operaciones dadas por*

$$p \wedge q = p \cap q, \quad p \vee q = (p \cup q)^{\perp\perp}, \quad p' = p^\perp.$$

Además $\mathbb{0} = \varnothing$, $\mathbb{1} = X$, *la relación de orden es la inclusión y para todo conjunto* $A \subset R(X)$ *se cumple*

$$\bigvee A = \Big(\bigcup_{p\in A} p\Big)^{\perp\perp}, \qquad \bigwedge A = \Big(\bigcap_{p\in A} p\Big)^{\perp\perp}.$$

Demostración: Notemos que del teorema anterior apartado 3) se sigue que si p, $q \in R(X)$ entonces $p \cap q \in R(X)$, lo cual justifica la definición de $p \wedge q$. Del apartado 2) se sigue que si $p \subset X$ entonces $p^{\perp\perp} \in R(X)$, lo que justifica la definición de $p \vee q$. La definición de p' es correcta por el apartado 1).

Comprobamos las propiedades no obvias de la definición de álgebra:

1) $p'' = p^{\perp\perp} = p$ porque p es regular.

5) $p \vee (q \wedge r) = (p \cup (q \cap r))^{\perp\perp} = ((p \cup q) \cap (p \cup r))^{\perp\perp}$
$= (p \cup q)^{\perp\perp} \cap (p \cup r)^{\perp\perp} = (p \vee q) \wedge (p \vee r)$.

6) $p \vee (p \wedge q) = (p \cup (p \cap q))^{\perp\perp} = p^{\perp\perp} = p$.

7) $p' \vee q' = (p^\perp \cup q^\perp)^{\perp\perp} = (X \setminus \operatorname{cl}(p^\perp \cup q^\perp))^\perp = (X \setminus (\operatorname{cl} p^\perp \cup \operatorname{cl} q^\perp))^\perp$
$= ((X \setminus \operatorname{cl} p^\perp) \cap (X \setminus \operatorname{cl} q^\perp))^\perp = (p^{\perp\perp} \cap q^{\perp\perp})^\perp = (p \cap q)^\perp = (p \wedge q)'$.

8) $p \vee p' = p'' \vee p' = (p' \wedge p)' = ((X \setminus \operatorname{cl} p) \cap p)^\perp = \varnothing^\perp = X$, para todo p.

Así pues $R(X)$ es un álgebra de Boole. Teniendo en cuenta que $\wedge$ es la intersección, es claro que la relación de orden es la inclusión. También es claro que $\mathbb{0} = \varnothing$ y $\mathbb{1} = X$.

Si $A \subset R(X)$, sea $s = \big(\bigcup_{p\in A} p\big)^{\perp\perp} \in R(X)$. Como la unión es un abierto, se cumple que $\bigcup_{p\in A} p \subset \operatorname{int}\operatorname{cl} \bigcup_{p\in A} p = s$, luego s es una cota superior de A.

Si $r \in R(X)$ es una cota superior de A, entonces $\bigcup_{p\in A} p \subset r$, con lo que $s \subset r^{\perp\perp} = r$, es decir, $s \leq r$. Esto prueba que s es el supremo de A. Igualmente se razona con el ínfimo. ∎

Notemos que, aunque los elementos de $R(X)$ son subconjuntos de X, no es en general un álgebra de conjuntos sobre X, pues la operación $\vee$ no es la unión.

Más adelante probaremos (véase el teorema 7.49) que toda álgebra de Boole completa es isomorfa a un álgebra de abiertos regulares.

Espacios de Stone La completitud de un álgebra tiene una caracterización muy simple en términos de su espacio de Stone:

Teorema 7.32 *Un álgebra de Boole* $\mathbb{B}$ *es completa si y sólo si su espacio de Stone es extremadamente disconexo, es decir, si y sólo si las clausuras de sus abiertos son abiertas.*

DEMOSTRACIÓN: Supongamos que $\mathbb{B}$ es completa y sea A un abierto en $S(\mathbb{B})$. Entonces A es unión de una familia X de abiertos-cerrados. Sea S el supremo de X en el álgebra de abiertos cerrados. Claramente $A \subset S$ y, como S es cerrado, $\operatorname{cl} A \subset S$. El abierto $S \setminus \operatorname{cl} A$ ha de ser vacío, o de lo contrario contendría un abierto-cerrado no vacío B, y entonces $S \setminus B$ sería una cota superior de X menor que S, lo cual es imposible. Por consiguiente $\operatorname{cl} A = S$ es abierto.

Recíprocamente, si $S(\mathbb{B})$ es extremadamente disconexo y X es una familia de abiertos-cerrados en $S(\mathbb{B})$, es fácil ver que $\operatorname{cl} \bigcup_{A\in X} A$ es el supremo de X. ∎

Homomorfismos completos Un homomorfismo $h : \mathbb{B} \longrightarrow \mathbb{C}$ entre álgebras de Boole completas es *completo* si para todo $X \subset \mathbb{B}$ se cumple

$$h\Big(\bigvee_{q\in X} q\Big) = \bigvee_{q\in X} h(q)$$

(o la igualdad análoga con ínfimos, que es equivalente).

Subálgebras completas Si $\mathbb{B}$ es un álgebra de Boole completa y $\mathbb{C}$ es una subálgebra de $\mathbb{B}$, diremos que $\mathbb{C}$ es una *subálgebra completa* si para todo $X \subset \mathbb{C}$ se cumple que $\bigvee X \in \mathbb{C}$ (o, equivalentemente, $\bigwedge X \in \mathbb{C}$).

En tal caso $\mathbb{C}$ es completa con la estructura de subálgebra y si $X \subset \mathbb{C}$, el supremo de X en $\mathbb{C}$ es el mismo que el supremo en $\mathbb{B}$. Equivalentemente, $\mathbb{C}$ es una subálgebra completa de $\mathbb{B}$ si es completa como álgebra y la inclusión $i : \mathbb{C} \longrightarrow \mathbb{B}$ es un monomorfismo completo.

Nota Es importante tener presente que una subálgebra $\mathbb{C}$ de un álgebra completa $\mathbb{B}$ puede ser completa como álgebra pero no ser una subálgebra completa. Esto sucede si el supremo en $\mathbb{C}$ de un subconjunto $X \subset \mathbb{C}$ no coincide con el supremo en $\mathbb{B}$.

Por ejemplo, si $\mathbb{B}$ es un álgebra de Boole completa, entonces el álgebra $\mathbb{C}$ de abiertos-cerrados de $S(\mathbb{B})$ es una subálgebra de $\mathcal{P}S(\mathbb{B})$, y es completa, pero no es necesariamente una subálgebra completa de $\mathcal{P}S(\mathbb{B})$, pues el supremo de una familia de elementos de $\mathbb{C}$ no es necesariamente su unión (que es su supremo en $\mathcal{P}S(\mathbb{B})$), sino la clausura de su unión. ∎

Si $\mathbb{B}$ es un álgebra de Boole completa, es inmediato comprobar que la intersección de una familia de subálgebras completas de $\mathbb{B}$ es de nuevo una subálgebra completa. Por consiguiente, si $X \subset \mathbb{B}$, podemos definir la *subálgebra completa generada* por X como la intersección de todas las subálgebras completas de $\mathbb{B}$ que contienen a X. La representaremos por $\langle X\rangle_c$. Si $\mathbb{B} = \langle X\rangle_c$ diremos que $\mathbb{B}$ está *completamente generada* por X o que X es un *generador completo* de $\mathbb{B}$.

Condiciones de cadena Vamos a dar un criterio útil para probar la completitud de un álgebra de Boole. Partimos de una propiedad más débil:

Definición 7.33 Si κ es un cardinal infinito, diremos que un álgebra de Boole $\mathbb{B}$ es *κ-completa* si todo subconjunto de $\mathbb{B}$ de cardinal menor que κ tiene supremo (o, equivalentemente, ínfimo).

Y ahora vamos a dar una condición que complementa la κ-completitud para llegar a la completitud:

Dos elementos $p, q \in \mathbb{B}$ de un álgebra de Boole $\mathbb{B}$ son *incompatibles* si cumplen $p \wedge q = \mathbb{0}$. Una *anticadena* en $\mathbb{B}$ es un conjunto $A \subset \mathbb{B}$ formado por elementos incompatibles dos a dos.

Si κ es un cardinal, un c.p.o. $\mathbb{B}$ cumple la *condición de cadena κ* (c.c.κ) si toda anticadena en $\mathbb{B}$ tiene cardinal $< \kappa$. En particular, la c.c. $\aleph_1$ se llama *condición de cadena numerable.*

Teorema 7.34 (AE) *Si $\mathbb{B}$ es un álgebra de Boole κ-completa y cumple la condición de cadena κ entonces $\mathbb{B}$ es completa.*

Demostración: Tomemos $X \subset \mathbb{B}$ y veamos que X tiene supremo. Sea $Y = \{p \in \mathbb{B} \mid \bigvee q \in X\ p \leq q\}$. Sea A una anticadena maximal en Y. Claramente también es una anticadena en $\mathbb{B}$, luego por hipótesis $|A| < \kappa$ y existe $\bigvee A$. Veamos que este supremo es también el supremo de X.

Si $p \in X \subset Y$ pero $p \not\leq \bigvee A$, entonces $\mathbb{0} \neq p \wedge (\bigvee A)' \leq p$, de donde concluimos que $p \wedge (\bigvee A)' \in Y$ y es incompatible con todos los elementos de A. Esto permite extender A a una anticadena mayor, en contradicción con su maximalidad. Así pues, $\bigvee A$ es una cota superior de X.

Si t es una cota superior de X, también lo es de Y, luego de A, luego $\bigvee A \leq t$. Esto prueba que $\bigvee A$ es la menor cota superior de X. ∎

Este criterio es especialmente útil para estudiar la completitud de álgebras cociente. Para ello introducimos algunos conceptos sobre ideales o filtros:

Definición 7.35 Sea $\mathbb{B}$ un álgebra de Boole, sean I, F un ideal y un filtro en $\mathbb{B}$, respectivamente, y sea κ un cardinal infinito.

I es *κ-completo* si todo subconjunto de I de cardinal menor que κ tiene supremo y éste pertenece a I.

F es *κ-completo* si todo subconjunto de F de cardinal menor que κ tiene ínfimo y éste pertenece a F.

Obviamente un ideal es κ-completo si y sólo si lo es su filtro dual, y viceversa.

Teorema 7.36 (AE) *Sea κ un cardinal infinito, $\mathbb{B}$ un álgebra de Boole κ-completa e I un ideal κ-completo de $\mathbb{B}$. Entonces el álgebra cociente $\mathbb{B}/I$ es κ-completa. Además, para todo $X \subset \mathbb{B}$ tal que $|X| < \kappa$ se cumple*

$$\bigvee_{p\in X}[p] = \Big[\bigvee_{p\in X} p\Big].$$

DEMOSTRACIÓN: Todo subconjunto de $\mathbb{B}/I$ de cardinal menor que κ es de la forma $Y = \{[p] \mid p \in X\}$, donde $X \subset \mathbb{B}$, $|X| < \kappa$. Claramente $\big[\bigvee_{p\in X} p\big]$ es una cota superior de Y.

Si $[q]$ es otra cota superior, entonces $[p] \leq [q]$ para todo $p \in X$, es decir, $p \wedge q' \in I$. Por la completitud de I concluimos que

$$\Big(\bigvee_{p\in X} p\Big) \wedge q' = \bigvee_{p\in X} (p \wedge q') \in I,$$

luego $\big[\bigvee_{p\in X} p\big] \leq [q]$. Esto prueba que $\big[\bigvee_{p\in X} p\big]$ es el supremo de Y. ∎

Consideramos ahora la condición de cadena κ:

Definición 7.37 Sea $\mathbb{B}$ un álgebra de Boole, I un ideal de $\mathbb{B}$ y κ un cardinal infinito. Diremos que I cumple la *condición de cadena* κ o que es *κ-saturado* si el álgebra cociente $\mathbb{B}/I$ cumple la c.c. κ.

Teorema 7.38 (AE) *Sea κ un cardinal infinito, sea $\mathbb{B}$ un álgebra de Boole κ-completa e I un ideal κ-completo de $\mathbb{B}$. Entonces I cumple la c.c.κ si y sólo si toda anticadena en $\mathbb{B} \setminus I$ tiene cardinal menor que κ.*

DEMOSTRACIÓN: Una implicación es obvia. Supongamos que I cumple la condición del enunciado y sea $\{[p_\alpha]\}_{\alpha<\kappa}$ una anticadena en $\mathbb{B}/I$. Podemos suponer además que $\bigwedge\alpha < \kappa\ p_\alpha \notin I$. Así, si $\alpha < \beta < \kappa$ entonces $p_\alpha \wedge p_\beta \in I$. Definimos

$$q_\beta = p_\beta \wedge \bigwedge_{\alpha<\beta} p'_\alpha.$$

Así, si $\alpha < \beta < \kappa$ tenemos que $q_\alpha \wedge q_\beta \leq p_\alpha \wedge p'_\alpha = \mathbb{0}$, luego $\{q_\beta\}_{\beta<\kappa}$ es una anticadena en $\mathbb{B}$. Hemos de probar que está, de hecho, en $\mathbb{B} \setminus I$.

Notemos que si $\alpha < \beta$ entonces $p_\beta \wedge p_\alpha \in I$, luego por la completitud de I resulta que $p_\beta \wedge \bigvee_{\alpha<\beta} p_\alpha \in I$.

Si $q_\beta \in I$ entonces $p_\beta = (p_\beta \wedge \bigwedge_{\alpha<\beta} p'_\alpha) \vee (p_\beta \wedge \bigvee_{\alpha<\beta} p_\alpha) \in I$, contradicción, luego ciertamente tenemos una anticadena en $\mathbb{B} \setminus I$, lo que a su vez contradice la saturación de I. El recíproco es evidente. ∎

Por consiguiente, el teorema 7.34 nos da que el cociente de un álgebra κ-completa sobre un ideal κ-completo y κ-saturado es un álgebra completa.

Terminamos este apartado con un resultado elemental que es útil a menudo, según el cual todo supremo en un álgebra de Boole completa puede expresarse como el supremo de una anticadena:

Teorema 7.39 *Si $\mathbb{B}$ es un álgebra de Boole completa y $\{p_\alpha\}_{\alpha<\gamma}$ es una familia de elementos de $\mathbb{B}$ (donde γ es un ordinal), existe otra familia $\{q_\alpha\}_{\alpha<\gamma}$ tal que $\bigwedge\alpha < \gamma\ q_\alpha \leq p_\alpha$, $\bigwedge\alpha\beta < \gamma(\alpha \neq \beta \to q_\alpha \wedge q_\beta = \mathbb{0})$ y $\bigvee_{\alpha<\gamma} q_\alpha = \bigvee_{\alpha<\gamma} p_\alpha$.*

DEMOSTRACIÓN: Basta tomar $q_\alpha = p_\alpha \wedge \bigwedge_{\beta<\alpha} p'_\beta$. Obviamente $q_\alpha \leq p_\alpha$ y si $\alpha \neq \beta$, digamos $\beta < \alpha$, entonces $q_\alpha \wedge q_\beta \leq p'_\beta \wedge p_\beta = \mathbb{0}$. Veamos por inducción sobre $\alpha \leq \gamma$ que $\bigvee_{\beta<\alpha} p_\alpha = \bigvee_{\beta<\alpha} q_\beta$. Para $\alpha = \gamma$ es la tercera propiedad que teníamos que probar.

Para $\alpha = 0$ es trivial. Si vale para α, entonces

$$\bigvee_{\beta<\alpha+1} q_\beta = \bigvee_{\beta<\alpha} q_\beta \vee q_\alpha = \bigvee_{\beta<\alpha} p_\beta \vee (p_\alpha \wedge \bigwedge_{\beta<\alpha} p'_\beta) = \bigvee_{\beta<\alpha+1} p_\beta.$$

Si vale para todo $\alpha < \lambda \leq \beta$, sabemos que $\bigvee_{\beta<\lambda} q_\beta \leq \bigvee_{\beta<\lambda} p_\beta$, y, para cada $\alpha < \lambda$

$$p_\alpha \leq \bigvee_{\beta<\alpha+1} p_\beta = \bigvee_{\beta<\alpha+1} q_\beta \leq \bigvee_{\beta<\lambda} q_\beta,$$

luego $\bigvee_{\beta<\lambda} p_\beta = \bigvee_{\beta<\lambda} q_\beta$. ∎

7.4 La compleción de un álgebra de Boole

Vamos a probar que toda álgebra de Boole puede sumergirse (en un sentido que precisaremos más abajo) en un álgebra de Boole completa, pero conviene probar un resultado más general, para lo cual vamos a observar que muchos de los conceptos que hemos definido sobre álgebras de Boole son generalizables a conjuntos parcialmente ordenados arbitrarios, e incluso a una clase más general de objetos:

Definición 7.40 Un *preorden* en un conjunto $\mathbb{P}$ es una relación reflexiva y transitiva. Un *conjunto preordenado* (c.p.o.) es un par $(\mathbb{P}, \leq)$, donde $\mathbb{P}$ es un conjunto no vacío y $\leq$ es un preorden en $\mathbb{P}$.

En particular, todo conjunto parcialmente ordenado es un conjunto preordenado y, más en particular, toda álgebra de Boole es un c.p.o. Sin embargo, en lo sucesivo, cuando apliquemos a un álgebra de Boole $\mathbb{B}$ los conceptos que vamos a definir para c.p.o.s, los aplicaremos a $\mathbb{B} \setminus \{\mathbb{0}\}$. Veamos varios ejemplos:

- Si $\mathbb{P}$ es un c.p.o., diremos que dos elementos p, $q \in \mathbb{P}$ son *incompatibles* si

$$p \perp q \equiv \neg\bigvee r \in \mathbb{P}\ (r \leq p \wedge r \leq q).$$

  Entonces, si $\mathbb{B}$ es un álgebra de Boole, diremos que p, $q \in \mathbb{B} \setminus \{\mathbb{0}\}$ son incompatibles en $\mathbb{B}$ si no existe $r \in \mathbb{B} \setminus \{\mathbb{0}\}$ tal que $r \leq p \wedge r \leq q$. Puesto que $r = p \wedge q$ siempre cumple $r \leq p \wedge r \leq q$, concluimos que, en un álgebra de Boole, dos elementos p y q (no nulos) son incompatibles si y sólo si $p \wedge q = \mathbb{0}$, que es la definición de incompatibilidad que ya habíamos dado sobre álgebras de Boole, y que se extiende de forma natural al caso en que $p = \mathbb{0}$ o $q = \mathbb{0}$.

- Si $\mathbb{P}$ es un c.p.o., un elemento $p \in \mathbb{P}$ es un *átomo* si no existen q, $r \in \mathbb{P}$ tales que $q \leq p \wedge r \leq p \wedge q \perp r$.

  Si $\mathbb{B}$ es un álgebra de Boole un $a \in \mathbb{B} \setminus \{\mathbb{0}\}$ es un átomo en este sentido si y sólo si es un átomo en $\mathbb{B}$ en el sentido que ya habíamos definido, es decir, si no existe ningún $c \in \mathbb{B}$ tal que $\mathbb{0} < c < b$. En efecto, si sucede esto es obvio que b es un átomo en el sentido general que acabamos de definir, y si existe un c en estas condiciones, entonces $d = b \wedge c'$ cumple $d \neq \mathbb{0}$, $c \leq b \wedge d \leq b \wedge c \perp d$, luego b no es un átomo en el sentido general.

- Si $\mathbb{P}$ es un c.p.o. se dice que un subconjunto $F \subset \mathbb{P}$ es un *filtro* en $\mathbb{P}$ si cumple las condiciones siguientes:

  1. $F \neq \varnothing$,
  2. $\bigwedge p \in F \bigwedge q \in \mathbb{P}(p \leq q \to q \in F)$,
  3. $\bigwedge pq \in F \bigvee r \in F(r \leq p \wedge r \leq q)$.

  Nuevamente, si $\mathbb{B}$ es un álgebra de Boole, un subconjunto $F \subset \mathbb{B} \setminus \{\mathbb{0}\}$ es un filtro en $\mathbb{B}$ según la definición precedente (cambiando $\mathbb{P}$ por $\mathbb{B} \setminus \{0\}$) si y sólo si es un filtro en el sentido que ya teníamos definido.

  En efecto, si $F \subset \mathbb{B} \setminus \{\mathbb{0}\}$ es un filtro en el sentido de c.p.o.s, trivialmente tenemos que $\mathbb{0} \notin F$, por 1) existe un $p \in F$, y por 2), como $p \leq \mathbb{1}$, tenemos que $\mathbb{1} \in F$. La propiedad 2) de la definición de filtro en un álgebra es la misma que la propiedad 2) anterior y si p, $q \in F$, por 3) existe un $r \in F$ tal que $r \leq p$ y $r \leq q$, luego $r \leq p \wedge q$ y, por 2), también $p \wedge q \in F$. El recíproco se prueba más fácilmente.

Para conectar la teoría general sobre c.p.o.s con el caso de las álgebras de Boole conviene introducir el concepto siguiente:

Un c.p.o. $\mathbb{P}$ es *separativo* si $\bigwedge pq \in \mathbb{P}\ (p \not\leq q \to \bigvee r \in \mathbb{P}\ (r \leq p \wedge r \perp q))$.

Sucede que toda álgebra de Boole $\mathbb{B}$ es separativa, luego esta hipótesis sobre un c.p.o. no supone ninguna restricción a la hora de aplicar los resultados al caso de álgebras de Boole.

En efecto, cuando decimos que $\mathbb{B}$ es separativa queremos decir en realidad que lo es $\mathbb{B} \setminus \{\mathbb{0}\}$ y, ciertamente, si p, $q \in \mathbb{B} \setminus \{\mathbb{0}\}$ y $p \not\leq q$, tomamos $r = p \wedge q'$ y comprobamos que $r \neq \mathbb{0}$ pues si $p \wedge q' = \mathbb{0}$ entonces $p \to q = p' \vee q = \mathbb{1}$, luego $p \leq q$. Así, existe un $r \in \mathbb{B} \setminus \{\mathbb{0}\}$ que claramente cumple $r \leq p \wedge r \perp q$.

Una aplicación $i : \mathbb{P} \longrightarrow \mathbb{Q}$ entre dos c.p.o.s es una *inmersión* si cumple:

1. $\bigwedge p_1 p_2 \in \mathbb{P}\ (p_1 \leq p_2 \to i(p_1) \leq i(p_2))$,
2. $\bigwedge p_1 p_2 \in \mathbb{P}\ (p_1 \perp p_2 \to i(p_1) \perp i(p_2))$.

Ejemplo Consideremos el conjunto $\mathbb{P} = [\omega]^\omega$ de todos los subconjuntos infinitos de ω, con el preorden dado por $p \subset^* q$ si y sólo si $p \setminus q$ es finito.

Es claro que la relación $\subset^*$ es un preorden en $\mathbb{P}$, pero no es antisimétrica, pues de $p \subset^* q$ y $q \subset^* p$ es equivalente a que $p \triangle q$ es finito, es decir, a que $p \triangle q \in \mathrm{fin}$. Por lo tanto, si definimos

$$i : \mathbb{P} \longrightarrow \mathcal{P}\omega/\mathrm{fin}$$

mediante $i(p) = [p]$, se cumple que $p \subset^* q \wedge q \subset^* p$ si y sólo si $i(p) = i(q)$.

Observemos que dos elementos p, $q \in \mathbb{P}$ son incompatibles si y sólo si $p \cap q$ es infinito.

En efecto, en tal caso $r = p \cap q$ cumple ciertamente $r \subset^* p \wedge r \subset^* q$ y, recíprocamente, si existe $r \in \mathbb{P}$ que cumple esto, entonces $r \setminus p$ y $r \setminus q$ son finitos, pero $r = (r \setminus p) \cup (r \setminus q) \cup (r \cap p \cap q)$, luego $r \cap p \cap q$ tiene que ser infinito, y $p \cap q$ también.

Ahora es inmediato que i es una inmersión, cuya imagen es toda el álgebra $\mathcal{P}\omega/\mathrm{fin}$ excepto $\mathbb{0} = \mathrm{fin}$. Es fácil ver también que $\mathbb{P}$ es separativo. ∎

Según acabamos de ver, las inmersiones no tienen por qué ser inyectivas, pero sí que lo son entre conjuntos parcialmente ordenados separativos:

Teorema 7.41 *Si $i : \mathbb{P} \longrightarrow \mathbb{Q}$ es una inmersión entre conjuntos parcialmente ordenados separativos, entonces i es inyectiva y cumple*

$$\bigwedge p_1 p_2 \in \mathbb{P}\ (p_1 \leq p_2 \leftrightarrow i(p_1) \leq i(p_2)).$$

Demostración: Sean p_1, $p_2 \in \mathbb{P}$ tales que $i(p_1) \leq i(p_2)$. Hemos de probar que $p_1 \leq p_2$. En caso contrario, como $\mathbb{P}$ es separativo existiría $r \leq p_1$ tal que $r \perp p_2$. Entonces $i(r) \leq i(p_1) \wedge i(r) \perp i(p_2)$, contradicción. Teniendo en cuenta que, por hipótesis, la relación en $\mathbb{P}$ es antisimétrica (no es sólo un preorden), de aquí se sigue que i es inyectiva. ∎

Así pues, bajo las hipótesis del teorema (que se cumplen para álgebras de Boole) tenemos que $i : \mathbb{P} \longrightarrow i[\mathbb{P}]$ es una semejanza, con lo que podemos identificar a $\mathbb{P}$ con un subconjunto de $\mathbb{Q}$.

Es obvio que todo monomorfismo $h : \mathbb{B} \longrightarrow \mathbb{C}$ entre álgebras de Boole (o, más precisamente, su restricción $\mathbb{B} \setminus \{\mathbb{0}\} \longrightarrow \mathbb{C} \setminus \{\mathbb{0}\}$) es una inmersión, pero el recíproco no es cierto. Por ejemplo, si X es un espacio topológico, la inclusión $i : R(X) \longrightarrow \mathcal{P}X$, donde $R(X)$ es el álgebra de abiertos regulares en X (teoema 7.31), es una inmersión, pero no es un monomorfismo de álgebras, ya que $i(p \vee q) = (p \cup q)^{\perp\perp}$, que no tiene por qué coincidir con $i(p) \vee i(q) = p \cup q$. Sin embargo, añadiendo una condición técnica a la definición de inmersión, la situación cambia:

Definición 7.42 Una inmersión $i : \mathbb{P} \longrightarrow \mathbb{Q}$ es *completa* si

$$\bigwedge q \in \mathbb{Q} \bigvee p \in \mathbb{P} \bigwedge p^* \in \mathbb{P}(p^* \leq p \to \neg i(p^*) \perp q),$$

y en estas circunstancias diremos que p es una *reducción* de q a $\mathbb{P}$.

Teorema 7.43 *Toda inmersión completa $h : \mathbb{B} \longrightarrow \mathbb{C}$ entre álgebras de Boole*[2] *es un monomorfismo de álgebras tal que si un conjunto $X \subset \mathbb{B}$ tiene supremo (resp. ínfimo), entonces $h[X]$ también lo tiene y $h(\bigvee X) = \bigvee h[X]$ (resp. $h(\bigwedge X) = \bigwedge h[X]$). En particular, si $\mathbb{B}$ y $\mathbb{C}$ son álgebras completas, entonces h es un monomorfismo completo.*

Recíprocamente, todo monomorfismo completo entre álgebras de Boole completas es una inmersión completa.

Demostración: Como $\mathbb{B}$ es un conjunto totalmente ordenado separativo, el teorema anterior nos da que h es inyectiva y para todo p, $q \in \mathbb{B} \setminus \{\mathbb{0}\}$

$$p \leq q \leftrightarrow h(p) \leq h(q), \qquad p \wedge q = \mathbb{0} \leftrightarrow h(p) \wedge h(q) = \mathbb{0}.$$

Notemos además que $h(\mathbb{1}) = \mathbb{1}$. En efecto, en caso contrario $h(\mathbb{1})' \neq \mathbb{0}$, luego podemos tomar una reducción p de $h(\mathbb{1})'$ a $\mathbb{B}$. Como $p \leq p$, tenemos que $\neg h(p) \perp h(\mathbb{1})'$, luego $r = h(p) \wedge h(\mathbb{1})' \neq \mathbb{0}$, pero $p \leq \mathbb{1}$, luego $h(p) \leq h(\mathbb{1})$, y así tenemos que $r \leq h(\mathbb{1})' \wedge r \leq h(p) \leq h(\mathbb{1})$, luego $r \leq h(\mathbb{1})' \wedge h(\mathbb{1})' = \mathbb{0}$, contradicción.

Sea $p \in \mathbb{B} \setminus \{\mathbb{0}\}$ y veamos que $h(p') = h(p)'$.

Como $p \wedge p' = \mathbb{0}$, sabemos que $h(p) \wedge h(p') = \mathbb{0}$, luego $h(p') \leq h(p)'$. Si no se da la igualdad, tendrá que ser $q = h(p)' \wedge h(p')' \neq \mathbb{0}$. Sea r una reducción de q a $\mathbb{B}$. Necesariamente $r \wedge p \neq \mathbb{0}$ o $r \wedge p' \neq \mathbb{0}$. Veamos que ambos casos llevan a contradicción.

Si $r \wedge p \neq \mathbb{0}$, entonces $h(r \wedge p) \leq h(p)$, luego $h(r \wedge p) \wedge q = \mathbb{0}$, en contra de que r sea una reducción de q.

Si $r \wedge p' \neq \mathbb{0}$ entonces $h(r \wedge p') \leq h(p')$ y también $h(r \wedge p') \wedge q = \mathbb{0}$.

Así pues, h conserva complementos. Supongamos ahora que $X \subset \mathbb{B}$ tiene ínfimo y vamos a probar que existe $\bigwedge h[X] = h(\bigwedge X)$.

Al aplicar esto a conjuntos de dos elementos, concluimos que h es un monomorfismo de álgebras y, en caso de que las dos álgebras sean completas, tenemos que h es un monomorfismo completo.

Para cada $p \in X$ tenemos que

$$\bigwedge_{p\in X} p \leq p, \quad \text{luego} \quad h\Big(\bigwedge_{p\in X} p\Big) \leq h(p).$$

Sea ahora $q \in \mathbb{C}$ una cota inferior de $h[X]$ y veamos que $q \leq h\Big(\bigwedge_{p\in X} p\Big)$. Esto probará que $h\Big(\bigwedge_{p\in X} p\Big)$ es el ínfimo de $h[X]$.

En caso contrario consideramos $s = q \wedge h\Big(\bigwedge_{p\in X} p\Big)' \neq \mathbb{0}$.

Sea t una reducción de s a $\mathbb{B}$. Si $p \in X$, ha de ser $t \leq p$, pues en caso contrario $t \wedge p' \neq \mathbb{0}$ y $h(t \wedge p') \wedge s \leq h(p') \wedge h(p) = h(p)' \wedge h(p) = \mathbb{0}$,

[2]Aquí hay que entender que $h(\mathbb{0}) = \mathbb{0}$ y que la restricción $\mathbb{B} \setminus \{\mathbb{0}\} \longrightarrow \mathbb{C} \setminus \{\mathbb{0}\}$ es una inmersión completa.

en contradicción con que t es una reducción de s. Así pues, $t \leq \bigwedge_{p\in X} p$, pero entonces

$$s \wedge h(t) \leq s \wedge h\Big(\bigwedge_{p\in X} p\Big) = \mathbb{0},$$

lo que de nuevo contradice que t sea una reducción de s.

Recíprocamente, si h es un monomorfismo completo, claramente es una inmersión y si $q \in \mathbb{C} \setminus \{\mathbb{0}\}$ entonces $p = \bigwedge\{r \in \mathbb{B} \mid q \leq h(r)\}$ es una reducción de q a $\mathbb{B}$. En efecto, $h(p) = \bigwedge\{h(r) \mid r \in \mathbb{B} \wedge q \leq h(r)\} \geq q > \mathbb{0}$, luego $p > \mathbb{0}$. Si $t \leq p$ es no nulo pero $h(t) \wedge q = \mathbb{0}$, entonces $q \leq h(t')$, luego $p \leq t'$ (por definición de p), y así $t \leq p \wedge p' = \mathbb{0}$, contradicción. ∎

Necesitaremos el resultado siguiente:

Teorema 7.44 *Si $i : \mathbb{P} \longrightarrow \mathbb{Q}$ es una inmersión completa de c.p.o.s y $\mathbb{Q}$ es separativo, entonces $i[\mathbb{P}]$ también lo es.*

Demostración: Supongamos que $i(p_1) \not\leq i(p_2)$. Entonces existe un $r \in \mathbb{Q}$ tal que $r \leq i(p_1)$ y $r \perp i(p_2)$. Sea s una reducción de r a $\mathbb{P}$. Entonces $\neg i(s) \perp r$, luego $\neg i(s) \perp i(p_1)$, luego $\neg s \perp p_1$, es decir, existe $p \in \mathbb{P}$ tal que $p \leq s$ y $p \leq p_1$. Entonces $i(p) \leq i(p_1)$ y basta probar que $i(p) \perp i(p_2)$, pues esto prueba que $i[\mathbb{P}]$ es separativo. Ahora bien, en caso contrario $\neg p \perp p_2$, luego existe $p^* \leq p \leq s$, $p^* \leq p_2$, luego $\neg i(p^*) \perp r$, $i(p^*) \leq i(p_2)$, luego $\neg i(p_2) \perp r$, contradicción. ∎

En realidad nos va a interesar principalmente una clase muy particular de inmersiones completas:

Definición 7.45 Si $\mathbb{P}$ es un c.p.o. y $D \subset \mathbb{P}$, diremos que D es *denso*[3] en $\mathbb{P}$ si

$$\bigwedge p \in \mathbb{P} \bigvee d \in D\ d \leq p.$$

Una inmersión $i : \mathbb{P} \longrightarrow \mathbb{Q}$ entre dos c.p.o.s es *densa* si $i[\mathbb{P}]$ es denso en $\mathbb{Q}$.

Por ejemplo, la definición de álgebra de Boole atómica puede reformularse diciendo que $\mathbb{B}$ es atómica si el conjunto de sus átomos es denso (en $\mathbb{B} \setminus \{\mathbb{0}\}$).

Es inmediato comprobar que la composición de inmersiones (resp. inmersiones completas, resp. densas) es también una inmersión (resp. completa, densa). Además:

Teorema 7.46 *Toda inmersión densa entre c.p.o.s es una inmersión completa.*

Demostración: Si $i : \mathbb{P} \longrightarrow \mathbb{Q}$ es una inmersión densa y $q \in \mathbb{Q}$, entonces existe un $p \in \mathbb{P}$ tal que $i(p) \leq q$, y es inmediato que p es una reducción de q a $\mathbb{P}$, pues si $p^* \leq p$, entonces $i(p^*) \leq i(p) \leq q$, luego $\neg i(p^*) \perp q$. ∎

Un álgebra de Boole completa está totalmente determinada por cualquiera de sus subconjuntos densos:

[3]Si en $\mathbb{P}$ consideramos la topología que tiene por base a los conjuntos $\{q \in \mathbb{P} \mid q \leq p\}$, para todo $p \in \mathbb{P}$, los subconjuntos densos en el sentido que acabamos de definir son precisamente los subconjuntos densos en sentido topológico, es decir, los que cortan a todo abierto no vacío.

Teorema 7.47 *Sean $\mathbb{B}$ y $\mathbb{C}$ dos álgebras de Boole completas, sea $D \subset \mathbb{B}$ un subconjunto denso y sea $j : D \longrightarrow \mathbb{C}$ una inmersión completa. Entonces j se extiende a un único monomorfismo completo $j^* : \mathbb{B} \longrightarrow \mathbb{C}$, que será un isomorfismo si j es densa.*

DEMOSTRACIÓN: Notemos que al decir que D es denso en $\mathbb{B}$ hay que entender que $D \subset \mathbb{B} \setminus \{\mathbb{0}\}$ es denso en $\mathbb{B} \setminus \{\mathbb{0}\}$. La unicidad se debe a que, para todo $p \in \mathbb{B}$, se cumple que

$$p = \bigvee\{q \in D \mid q \leq p\}.$$

En efecto, si llamamos r al supremo, es claro que $r \leq p$, y si no se diera la igualdad es que $p \wedge r' \neq \mathbb{0}$, luego existe un $q \in D$ tal que $q \leq p \wedge r'$, luego $q \leq r$ por definición de r y también $q \leq r'$, luego $q \leq r \wedge r' = \mathbb{0}$, contradicción.

Por lo tanto, si existe j^*, necesariamente

$$j^*(p) = \bigvee\{j(q) \mid q \in D \wedge q \leq p\},$$

lo que nos da la unicidad.

Veamos ahora que definiendo j^* de este modo cumple lo pedido. Ante todo, si $p \in D$ entonces

$$j(p) \leq \bigvee\{j(q) \mid q \in D \wedge q \leq p\} \leq j(p),$$

luego $j^*(p) = j(p)$, es decir, j^* extiende a j.

Si $p \in \mathbb{B} \setminus \{\mathbb{0}\}$, entonces existe $q \in D$ tal que $q \leq p$ y por consiguiente $\mathbb{0} < j(q) \leq j^*(p)$. Así pues, j^* se restringe a una aplicación $\mathbb{B}\setminus\{\mathbb{0}\} \longrightarrow \mathbb{C}\setminus\{\mathbb{0}\}$. Veamos que es una inmersión.

Si p_1, $p_2 \in \mathbb{B}$ cumplen $p_1 \leq p_2$, entonces

$$\{j(q) \mid q \in D \wedge q \leq p_1\} \subset \{j(q) \mid q \in D \wedge q \leq p_2\},$$

luego $j^*(p_1) \leq j^*(p_2)$.

Si, por el contrario, $p_1 \wedge p_2 = \mathbb{0}$, entonces, para cada $q \in D$, $q \leq p_1$ tenemos que

$$j(q) \wedge j^*(p_2) = \bigvee\{j(q) \wedge j(r) \mid r \in D \wedge r \leq p_2\} = \mathbb{0},$$

pues q y r son incompatibles en D, luego $j(q)$ y $j(r)$ son incompatibles $\mathbb{C}$, porque j es una inmersión. Por consiguiente

$$j^*(p_1) \wedge j^*(p_2) = \bigvee\{j(q) \wedge j^*(p_2) \mid q \in D \wedge q \leq p_1\} = \mathbb{0}.$$

Así pues, j^* es una inmersión de c.p.o.s. Veamos que es completa. Si $q \in \mathbb{C}$, sabemos que tiene una reducción d a D, pero ésta es también una reducción a $\mathbb{B}$, pues si $p \leq d$, podemos tomar $d' \in D$ tal que $d' \leq p \leq d$, luego $\neg j(d') \perp q$, es decir, que existe un $r \in \mathbb{C} \setminus \{\mathbb{0}\}$ tal que $r \leq q$ y $r \leq j(d') = j^*(d') \leq j^*(p)$, luego $\neg j^*(p) \perp q$.

Por 7.43 sabemos que $j^* : \mathbb{B} \longrightarrow \mathbb{C}$ es un monomorfismo completo, y ya hemos visto que es la única extensión posible de j.

Supongamos ahora que j es una inmersión densa y veamos que j^* es suprayectiva. Para ello tomamos $r \in \mathbb{C}$ y definimos $s = \bigvee\{p \in D \mid j(p) \leq r\}$. Entonces, como ya sabemos que j^* conserva supremos,

$$j^*(s) = \bigvee\{j(p) \mid p \in D \wedge j(p) \leq r\} \leq r.$$

Si no se diera la igualdad existiría un $q \in \mathbb{C}$ no nulo de manera que $q \leq r$ y $q \wedge j^*(s) = 0$. Como j es densa podemos tomarlo de la forma $q = j(p)$, para cierto $p \in D$. Entonces $p \leq s$, luego $q = j(p) = j^*(p) \leq j^*(s)$, contradicción. ∎

En particular, si $j : \mathbb{B} \longrightarrow \mathbb{C}$ es una inmersión densa entre álgebras de Boole completas, se trata de hecho de un isomorfismo.

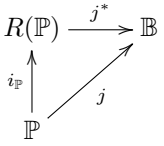
En efecto, tenemos que $j : \mathbb{B} \longrightarrow j[\mathbb{B}]$ es una semejanza, y el teorema anterior nos dice que debe extenderse a un isomorfismo $j^* : \mathbb{B} \longrightarrow \mathbb{C}$, lo cual sólo es posible si j es ya un isomorfismo.

Ahora ya estamos en condiciones de completar, no ya un álgebra de Boole, sino cualquier c.p.o.:

Definición 7.48 Sea $\mathbb{P}$ un c.p.o. Para cada $p \in \mathbb{P}$ sea $B_p = \{q \in \mathbb{P} \mid q \leq p\}$. Es inmediato comprobar que estos conjuntos son la base de una topología en $\mathbb{P}$. En particular podemos considerar el álgebra $R(\mathbb{P})$ de los abiertos regulares de $\mathbb{P}$, que por 7.31 es un álgebra de Boole completa.

Teorema 7.49 *Sea $\mathbb{P}$ un c.p.o. Entonces:*

1. *La aplicación $i_{\mathbb{P}} : \mathbb{P} \longrightarrow R(\mathbb{P})$ dada por $i(p) = B_p^{\perp\perp}$ es una inmersión densa.*
2. *Si $j : \mathbb{P} \longrightarrow \mathbb{B}$ es una inmersión completa (resp. densa) de $\mathbb{P}$ en un álgebra de Boole completa $\mathbb{B}$, entonces existe un único monomorfismo completo (resp. isomorfismo) $j^* : R(\mathbb{P}) \longrightarrow \mathbb{B}$ tal que el diagrama siguiente es conmutativo:*



En particular $R(\mathbb{P})$ es, salvo isomorfismo, la única álgebra de Boole completa en la que $\mathbb{P}$ puede sumergirse densamente. La llamaremos compleción *de $\mathbb{P}$.*

Demostración: 1) Notemos que si $p \in \mathbb{P}$, entonces

$$p \in B_p \subset B_p^{\perp\perp} \neq \varnothing = 0,$$

luego $i_{\mathbb{P}} : \mathbb{P} \longrightarrow R(\mathbb{P}) \setminus \{0\}$.

Sean p, $q \in \mathbb{P}$. Si $p \leq q$ entonces $B_p \subset B_q$, luego $B_p^{\perp\perp} \subset B_q^{\perp\perp}$, es decir, $i(p) \leq i(q)$.

Si $p \perp q$, entonces $B_p \cap B_q = \varnothing$, luego $B_p^{\perp\perp} \cap B_q^{\perp\perp} = (B_p \cap B_q)^{\perp\perp} = \varnothing$, luego $i(p) \wedge i(q) = \mathbb{0}$.

Esto prueba que i es una inmersión. Veamos que es densa. Si $A \in R(\mathbb{P})\setminus\{\mathbb{0}\}$, entonces A es un abierto no vacío, luego es unión de abiertos básicos. En particular existe un $p \in \mathbb{P}$ tal que $B_p \subset A$. Entonces $B_p^{\perp\perp} \subset A^{\perp\perp} = A$, es decir, $i(p) \leq A$.

Observemos que 2) es inmediato si $\mathbb{P}$ es un conjunto parcialmente ordenado separativo (en particular si es un álgebra de Boole), pues en tal caso $i_{\mathbb{P}}$ es una semejanza en su imagen, luego podemos definir $j' = i_{\mathbb{P}}^{-1} \circ j : i_{\mathbb{P}}[\mathbb{P}] \longrightarrow \mathbb{B}$, que es claramente una inmersión completa (resp. densa) que por el teorema anterior se extiende a un monomorfismo completo (resp. isomorfismo) $j^* : R(\mathbb{P}) \longrightarrow \mathbb{B}$ que claramente es el único que hace conmutativo el diagrama del enunciado.

Para probar el caso general veamos que si $i : \mathbb{P} \longrightarrow \mathbb{Q}$, $i' : \mathbb{P} \longrightarrow \mathbb{Q}'$ son inmersiones suprayectivas en dos conjuntos parcialmente ordenados separativos, entonces existe una única semejanza $f : \mathbb{Q} \longrightarrow \mathbb{Q}'$ tal que $i \circ f = i'$.

Admitiendo esto, como $\mathbb{Q} = i_{\mathbb{P}}[\mathbb{P}]$ y $\mathbb{Q}' = j[\mathbb{P}]$ son conjuntos parcialmente ordenados separativos (por 7.44), existe una semejanza $j' : i_{\mathbb{P}}[\mathbb{P}] \longrightarrow j[\mathbb{P}]$ tal que $i_{\mathbb{P}} \circ j' = j$, y podemos concluir igualmente.

Veamos que si r, $s \in \mathbb{Q}$, entonces

$$r \leq s \leftrightarrow \bigwedge t \in \mathbb{Q}(\neg t \perp r \to \neg t \perp s).$$

Si $r \leq s \wedge \neg t \perp r$, entonces existe $u \in \mathbb{Q}$ tal que $u \leq t \wedge u \leq r \leq s$, luego $\neg t \perp s$. Recíprocamente, si $r \not\leq s$, existe un $t \in \mathbb{Q}$ tal que $t \leq r \wedge t \perp s$ (porque $\mathbb{Q}$ es separativo), luego $\neg t \perp r$ pero $t \perp s$.

Lo mismo vale para $\mathbb{Q}'$, luego, dados p, $q \in \mathbb{P}$, se cumple

$$i(p) \perp i(q) \leftrightarrow p \perp q \leftrightarrow i'(p) \perp i'(q).$$

En consecuencia

$$i(p) \leq i(q) \leftrightarrow \bigwedge r \in \mathbb{P}(\neg i(r) \perp i(p) \to \neg i(r) \perp i(q))$$

$$\leftrightarrow \bigwedge r \in \mathbb{P}(\neg i'(r) \perp i'(p) \to \neg i'(r) \perp i'(q)) \leftrightarrow i'(p) \leq i'(q).$$

Como las relaciones en $\mathbb{Q}$ y $\mathbb{Q}'$ son antisimétricas, esto implica que

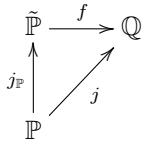
$$i(p) = i(q) \leftrightarrow i'(p) = i'(q).$$

De aquí se sigue que la aplicación $f : \mathbb{Q} \longrightarrow \mathbb{Q}'$ dada por $f(i(p)) = i'(p)$ está bien definida y es una semejanza. ∎

En particular, toda álgebra de Boole completa $\mathbb{B}$ es isomorfa al álgebra de abiertos regulares $R(\mathbb{B} \setminus \{\mathbb{0}\})$.

En la prueba del teorema anterior hemos demostrado un resultado de interés en sí mismo:

Teorema 7.50 *Si $\mathbb{P}$ es un c.p.o. y llamamos $\tilde{\mathbb{P}} = i_{\mathbb{P}}[\mathbb{P}] \subset R(\mathbb{P})$, entonces $\tilde{\mathbb{P}}$ es un conjunto parcialmente ordenado separativo, $i_{\mathbb{P}} : \mathbb{P} \longrightarrow \tilde{\mathbb{P}}$ es una inmersión suprayectiva y si $j : \mathbb{P} \longrightarrow \mathbb{Q}$ es cualquier inmersión suprayectiva en un conjunto parcialmente ordenado separativo, entonces existe una única semejanza $f : \tilde{\mathbb{P}} \longrightarrow \mathbb{Q}$ que hace conmutativo el diagrama*



Así, la inmersión densa de un c.p.o. $\mathbb{P}$ en su compleción puede descomponerse en una inmersión suprayectiva seguida de una inmersión densa inyectiva.

$$\mathbb{P} \longrightarrow \tilde{\mathbb{P}} \longrightarrow R(\mathbb{P}).$$

Vamos a dar una prueba alternativa de la existencia y unicidad de $\tilde{\mathbb{P}}$ que no dependa de la compleción de $\mathbb{P}$:

Demostración: Sea R la relación de equivalencia en $\mathbb{P}$ dada por

$$p\ R\ q \leftrightarrow \bigwedge r \in \mathbb{P}(r \perp p \leftrightarrow r \perp q).$$

Sea $\mathbb{Q} = \mathbb{P}/R$ el conjunto cociente y en él consideramos el orden dado por

$$[p] \leq [q] \leftrightarrow \bigwedge r \in \mathbb{P}(r \leq p \to \neg r \perp q).$$

Está bien definido, pues si $[p] = [p']$ y $[q] = [q']$ y $[p] \leq [q]$, entonces $[p'] \leq [q']$. En efecto, si $r \in \mathbb{P}$ cumple $r \leq p'$, entonces $\neg r \perp p'$, luego $\neg r \perp p$. Existe $s \in \mathbb{P}$ tal que $s \leq r \wedge s \leq p$. Como $[p] \leq [q]$, ha de ser $\neg s \perp q$, luego existe $t \in \mathbb{P}$ tal que $t \leq s \wedge t \leq q$. Así $t \leq r \wedge t \leq q$, es decir, $\neg r \perp q$, luego también $\neg r \perp q'$. Esto prueba que $[p'] \leq [q']$.

La relación en $\mathbb{Q}$ es claramente reflexiva. Veamos que es simétrica, para lo cual suponemos que $[p] \leq [q] \wedge [q] \leq [p]$. Si $\neg r \perp p$, existe $s \in \mathbb{P}$ tal que $s \leq r \wedge s \leq p$, luego $s \leq r \wedge \neg s \perp q$. Existe $t \in \mathbb{P}$ tal que $t \leq s \leq r \wedge t \leq q$. Por consiguiente $\neg r \perp q$. Igualmente se prueba el recíproco, luego $[p] = [q]$.

Para probar la transitividad suponemos $[p] \leq [q] \wedge [q] \leq [r]$. Si $u \leq p$ entonces $\neg u \perp q$ (porque $[p] \leq [q]$). Existe $v \in \mathbb{P}$ tal que $v \leq u \wedge v \leq q$. Entonces $\neg v \perp r$ (porque $[q] \leq [r]$). Existe $w \in \mathbb{P}$ tal que $w \leq v \leq u \wedge w \leq r$. Así pues, $\neg u \perp r$, lo que prueba que $[p] \leq [r]$.

Tenemos, por lo tanto, que $\mathbb{Q}$ es un conjunto parcialmente ordenado (con máximo $[\mathbb{1}]$). Sea $i : \mathbb{P} \longrightarrow \mathbb{Q}$ la aplicación dada por $i(p) = [p]$. Obviamente es suprayectiva y $\bigwedge pp' \in \mathbb{P}(p \leq p' \to i(p) \leq i(p'))$. Para probar que es una inmersión suponemos que $\neg i(p) \perp i(p')$ y hemos de probar que $\neg p \perp p'$. Existe $r \in \mathbb{P}$ tal que $[r] \leq [p] \wedge [r] \leq [p']$. De $[r] \leq [p]$ se sigue en particular que $\neg r \perp p$, luego existe $s \in \mathbb{P}$ tal que $s \leq r \wedge s \leq p$. Entonces $[r] \leq [p']$ implica que $\neg s \perp p'$. Existe $t \in \mathbb{P}$ tal que $t \leq s \leq p \wedge t \leq p'$. Así, ciertamente, $\neg p \perp p'$.

Veamos ahora que $\mathbb{Q}$ es separativo. Si $[p] \not\leq [q]$ esto significa que existe $r \in \mathbb{P}$ tal que $r \leq p \wedge r \perp q$. Como i es una inmersión $[r] \leq [p] \wedge [r] \perp [q]$, luego tenemos que $\bigvee r \in \mathbb{Q}(r \leq [p] \wedge r \perp [q])$.

Falta probar la unicidad de $\mathbb{Q}$. Para ello supongamos que $\mathbb{Q}'$ es otro conjunto parcialmente ordenado separativo tal que exista $j : \mathbb{P} \longrightarrow \mathbb{Q}'$ inmersión suprayectiva.

Veamos que si r, $s \in \mathbb{Q}'$ se cumple $r \leq s \leftrightarrow \bigwedge t \in \mathbb{Q}'(\neg t \perp r \to \neg t \perp s)$.

Si $r \leq s \wedge \neg t \perp r$, entonces existe $u \in \mathbb{Q}'$ tal que $u \leq t \wedge u \leq r \leq s$, luego $\neg t \perp s$. Recíprocamente, si $r \not\leq s$, existe un $t \in \mathbb{Q}'$ tal que $t \leq r \wedge t \perp s$ (porque $\mathbb{Q}'$ es separativo), luego $\neg t \perp r$ pero $t \perp s$.

Como esto vale para todo conjunto parcialmente ordenado separativo, en particular vale para $\mathbb{Q}$. Dados p, $q \in \mathbb{P}$, se cumple

$$i(p) \perp i(q) \leftrightarrow p \perp q \leftrightarrow j(p) \perp j(q).$$

En consecuencia

$$i(p) \leq i(q) \leftrightarrow \bigwedge r \in \mathbb{P}(\neg i(r) \perp i(p) \to \neg i(r) \perp i(q))$$

$$\leftrightarrow \bigwedge r \in \mathbb{P}(\neg j(r) \perp j(p) \to \neg j(r) \perp j(q)) \leftrightarrow j(p) \leq j(q).$$

Como las relaciones en $\mathbb{Q}$ y $\mathbb{Q}'$ son antisimétricas, esto implica que

$$i(p) = i(q) \leftrightarrow j(p) = j(q).$$

De aquí se sigue que la aplicación $f : \mathbb{Q} \longrightarrow \mathbb{Q}'$ dada por $f(i(p)) = j(p)$ está bien definida y es una semejanza. ∎

En particular, si aplicamos la unicidad de la prueba anterior a $\mathbb{Q}' = i_{\mathbb{P}}[\mathbb{P}]$, vemos que la condición necesaria y suficiente para que dos elementos de $\mathbb{P}$ tengan la misma imagen en su compleción es que tengan los mismos elementos incompatibles.

En particular toda álgebra de Boole $\mathbb{B}$ se puede completar, es decir, se puede sumergir como subálgebra densa en una única álgebra de Boole completa $R(\mathbb{B})$. Más en general, todo conjunto parcialmente ordenado separativo $\mathbb{P}$ es semejante a un subconjunto denso de un álgebra de Boole completa $R(\mathbb{P})$. (Si un c.p.o. no es parcialmente ordenado y separativo existe una inmersión densa, pero no es inyectiva, luego no es una semejanza en la imagen.)

Veamos algunas características de $\mathbb{P}$ que se conservan al pasar a su compleción. Por ejemplo, es claro que la definición de anticadena vale para c.p.o.s arbitrarios, e igualmente podemos definir un c.p.o. con la condición de cadena κ como un c.p.o. en el que toda anticadena tenga cardinal menor que κ.

Es inmediato que si $f : \mathbb{P} \longrightarrow \mathbb{Q}$ es una inmersión densa de c.p.o.s, entonces $\mathbb{P}$ cumple la c.c.κ si y sólo si la cumple $\mathbb{Q}$. En particular $\mathbb{P}$ cumple la c.c.κ si y sólo si la cumple su compleción $R(\mathbb{P})$.

Similarmente, diremos que un c.p.o. es *atómico* si su conjunto de átomos es denso. Diremos que es *no atómico* si no tiene átomos (de modo que "no atómico" no es la negación de "atómico").

Teorema 7.51 *Si $i : \mathbb{P} \longrightarrow \mathbb{Q}$ es una inmersión densa de c.p.o.s, se cumple que $\mathbb{P}$ es atómico (resp. no atómico) si y sólo si lo es $\mathbb{Q}$.*

Demostración: Si $a \in \mathbb{P}$ es un átomo, entonces $i(a)$ también lo es, pues si existen q, $r \in \mathbb{Q}$ tales que $q \leq i(a) \wedge r \leq i(a) \wedge p \perp r$, podemos suponer que $q = i(u) \wedge r = i(v)$. Entonces $\neg u \perp a \wedge \neg v \perp a$, luego existen u', v' de modo que $u' \leq u \wedge u' \leq a \wedge v' \leq v \wedge v' \leq a$, pero $u \perp v$, luego $u' \perp v'$, lo que contradice que a sea un átomo. El recíproco es trivial. Por lo tanto, tenemos que $\mathbb{P}$ es no atómico si y sólo si lo es $\mathbb{Q}$.

Si $\mathbb{Q}$ es no atómico y $p \in \mathbb{P}$, entonces existe un átomo $a \in \mathbb{Q}$ tal que $a \leq i(p)$, luego existe un $a' \in \mathbb{P}$ tal que $i(a') \leq a$. Entonces $\neg p \perp a'$, luego existe un $a'' \in \mathbb{P}$ tal que $a'' \leq p \wedge a'' \leq a'$. De $i(a') \leq a$ se deduce inmediatamente que $i(a')$ es un átomo, luego a' también lo es, luego a'' también lo es, y esto implica que $\mathbb{P}$ es no atómico.

Si $\mathbb{P}$ es no atómico y $q \in \mathbb{Q}$, existe un $p \in \mathbb{P}$ tal que $i(p) \leq q$ y existe un átomo $a \in \mathbb{P}$ tal que $a \leq p$, luego $i(a) \leq q$ es un átomo en $\mathbb{Q}$ que prueba que $\mathbb{Q}$ es no atómico. ∎

En particular, un c.p.o. $\mathbb{P}$ es atómico o no atómico si y sólo si lo es su compleción $R(\mathbb{P})$.

7.5 Distributividad en álgebras completas

La generalización natural del teorema 7.26 no se cumple en toda álgebra de Boole completa:

Definición 7.52 Si κ y μ son cardinales, un álgebra de Boole completa $\mathbb{B}$ es κ-μ-distributiva si cuando $\{p_{\alpha,\beta}\}_{(\alpha,\beta)\in\kappa\times\mu}$ es una familia de elementos de $\mathbb{B}$ se cumple que

$$\bigwedge_{\alpha<\kappa}\bigvee_{\beta<\mu} p_{\alpha\beta} = \bigvee_{f\in{}^{\kappa}\mu}\bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)}.$$

(o la fórmula equivalente que resulta de intercambiar supremos e ínfimos).

Se dice que $\mathbb{B}$ es κ-distributiva (o κ-∞-distributiva) si es κ-μ-distributiva para todo μ. Se dice que $\mathbb{B}$ es *completamente distributiva* si es κ distributiva para todo κ.

En estos términos, el teorema 7.26 afirma que toda álgebra de Boole completa es 2-distributiva. Las álgebras $\mathcal{P}A$ son completamente distributivas, pues esto equivale a la relación

$$\bigcap_{\alpha<\kappa}\bigcup_{\beta<\mu} A_{\alpha\beta} = \bigcup_{f\in{}^{\kappa}\mu}\bigcap_{\alpha<\kappa} A_{\alpha f(\alpha)},$$

que se comprueba sin dificultad. Sin embargo, sólo las álgebras de tipo $\mathcal{P}A$ son completamente distributivas:

Teorema 7.53 *Un álgebra de Boole completa es completamente distributiva si y sólo si es isomorfa a un álgebra $\mathcal{P}A$.*

Demostración: Sea $\mathbb{B}$ un álgebra de Boole completa y completamente distributiva.[4] Para cada $b \in \mathbb{B}$, $j \in 2$, sea

$$p_{b,j} = \begin{cases} b & \text{si } j = 1, \\ b' & \text{si } j = 0. \end{cases}$$

Entonces $\bigvee\limits_{j\in 2} p_{b,j} = \mathbb{1}$, luego $\bigwedge\limits_{b\in\mathbb{B}} \bigvee\limits_{j\in 2} p_{b,j} = \mathbb{1}$, luego la distributividad nos da que

$$\bigvee_{f\in 2^{\mathbb{B}}} \bigwedge_{b\in\mathbb{B}} p_{bf(b)} = \mathbb{1}.$$

Llamemos $a_f = \bigwedge\limits_{b\in\mathbb{B}} p_{bf(b)}$. Basta probar que cada a_f no nulo es un átomo, pues entonces, si $x \in \mathbb{B}$ es no nulo, tenemos que

$$x = x \wedge \mathbb{1} = \bigvee_{f\in 2^{\mathbb{B}}} (x \wedge a_f),$$

luego existe un $f \in 2^{\mathbb{B}}$ tal que $x \wedge a_f \neq \mathbb{0}$, luego $x \wedge a_f = a_f$, luego $\mathbb{0} < a_f \leq x$ y así $\mathbb{B}$ es atómica, y el teorema 7.28 nos da la conclusión.

Supongamos, pues, que $a_f \neq \mathbb{0}$. Dado $b \in \mathbb{B}$ no nulo, si $f(b) = 1$ entonces $a_f \leq p_{b1} = b$, mientras que si $f(b) = 0$ tenemos que $a_f \leq b'$. Esto implica que no puede existir un $c \in \mathbb{B}$ tal que $\mathbb{0} < c < a_f$, ya que entonces sería $c < a_f < c'$, contradicción. Por lo tanto a_f es un átomo. ∎

Suponiendo AE, para enunciar la κ-distributividad no es necesario que todas las sucesiones $\{p_{\alpha\beta}\}_{\beta<\mu}$ tengan el mismo conjunto de índices μ, sino que es fácil ver que equivale a que

$$\bigwedge_{\alpha<\kappa} \bigvee_{i\in I_\alpha} p_{\alpha i} = \bigvee_{f\in \prod\limits_{\alpha<\kappa} I_\alpha} \bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)}.$$

Vamos a caracterizar esta propiedad, para lo cual necesitamos algunos conceptos:

Una *partición* P de un álgebra de Boole completa $\mathbb{B}$ es una anticadena P tal que $\bigvee P = \mathbb{1}$.

Si P, Q son particiones de $\mathbb{B}$, diremos que P es un *refinamiento* de Q si $\bigwedge p \in P \bigvee q \in Q\ p \leq q$.

Observemos, por último, que respecto a la topología en $\mathbb{B}$ considerada en la definición 7.48, un conjunto $D \subset \mathbb{B}$ es un abierto denso si

$$\bigwedge b \in \mathbb{B}(b \neq \mathbb{0} \to \bigvee d \in D\ d \leq b) \wedge \bigwedge d \in D \bigwedge b \in \mathbb{B}(\mathbb{0} < b \leq d \to b \in D).$$

[4] La demostración no requiere el axioma de elección si modificamos la definición de distributividad sustituyendo los cardinales κ y μ por dos conjuntos cualesquiera I y J.

Teorema 7.54 (AE) *Si $\mathbb{B}$ es un álgebra de Boole completa y κ un cardinal, las afirmaciones siguientes son equivalentes:*

1. *$\mathbb{B}$ es κ-distributiva.*

2. *La intersección de κ abiertos densos es abierta densa.*

3. *Todo conjunto de κ particiones de $\mathbb{B}$ admite un refinamiento común.*

DEMOSTRACIÓN: 1) $\Rightarrow$ 2) Sea $\{D_\alpha\}_{\alpha<\kappa}$ una familia de abiertos densos. Es inmediato que $D = \bigcap_{\alpha<\kappa} D_\alpha$ es abierto. Para probar que es denso, tomamos $u \in \mathbb{B}$ no nulo. En la prueba de 7.47 hemos visto que $\bigvee_{d\in D_\alpha} d = \mathbb{1}$, luego $\bigvee_{d\in D_\alpha}(u \wedge d) = u$, luego

$$u = \bigwedge_{\alpha<\kappa} \bigvee_{d\in D_\alpha} (u \wedge d) = \bigvee_{f\in \prod_{\alpha<\kappa} D_\alpha} \bigwedge_{\alpha<\kappa} (u \wedge f(\alpha)).$$

Si llamamos $u_f = \bigwedge_{\alpha<\kappa} (u \wedge f(\alpha))$, alguno de ellos tiene que ser no nulo, pues el supremo de todos ellos es u. Si fijamos uno no nulo, tenemos claramente que $u_f \in D$, $u_f \le u$, lo que prueba que D es denso.

2) $\Rightarrow$ 3) Sea $\{P_\alpha\}_{\alpha<\kappa}$ una familia de particiones de $\mathbb{B}$. Para cada α, sea

$$D_\alpha = \{u \in \mathbb{B} \mid \bigvee v \in P_\alpha \ u \le v\}.$$

Entonces D_α es claramente abierto, y además es denso, pues si $b \in \mathbb{B}$ no es nulo, entonces $\bigvee_{p\in P_\alpha} p = \mathbb{1}$, luego $\bigvee_{p\in P_\alpha}(b \wedge p) = b$, luego algún $b \wedge p \neq \mathbb{0}$ y $b \wedge p \in D_\alpha$, $b \wedge p \le b$.

Sea $D = \bigcap_{\alpha<\kappa} D_\alpha$, que por hipótesis es abierto denso, y sea P una familia maximal de elementos de D incompatibles dos a dos (existe por el lema de Zorn). Basta probar que P es una partición, pues en tal caso es obvio que refina a todas las particiones dadas. Concretamente, sólo tenemos que probar que $\bigvee P = \mathbb{1}$. En caso contrario, sea $s = \bigvee P$ y sea $d \in D$ tal que $d \le s'$. Claramente, d es incompatible con todos los elementos de P, lo que contradice la maximalidad de P.

3) $\Rightarrow$ 1) Sea $\{p_{\alpha i}\}_{i\in I_\alpha}$ para $\alpha < \kappa$ una sucesión de κ familias de elementos de $\mathbb{B}$. Observemos que si $f \in \prod_{\alpha<\kappa} I_\alpha$, entonces

$$u_f = \bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)} \le p_{\alpha f(\alpha)} \le \bigvee_{i\in I_\alpha} p_{\alpha i},$$

luego $u_f \le \bigwedge_{\alpha<\kappa} \bigvee_{i\in I_\alpha} p_{\alpha i}$, luego

$$\bigvee_{f\in \prod_{\alpha<\kappa} I_\alpha} \bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)} \le \bigwedge_{\alpha<\kappa} \bigvee_{i\in I_\alpha} p_{\alpha i}.$$

Llamemos u al miembro derecho y veamos que se da la igualdad. Observemos que

$$\bigvee_{f\in\prod_{\alpha<\kappa} I_\alpha}\bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)} = \bigvee_{f\in\prod_{\alpha<\kappa} I_\alpha}\bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)}\wedge u = \bigvee_{f\in\prod_{\alpha<\kappa} I_\alpha}\bigwedge_{\alpha<\kappa} (p_{\alpha f(\alpha)}\wedge u)$$

$$\bigwedge_{\alpha<\kappa}\bigvee_{i\in I_\alpha} p_{\alpha i} = \bigwedge_{\alpha<\kappa}\bigvee_{i\in I_\alpha} p_{\alpha i}\wedge u = \bigwedge_{\alpha<\kappa}\bigvee_{i\in I_\alpha} (p_{\alpha i}\wedge u).$$

Por lo tanto, cambiando cada $p_{\alpha i}$ por $p_{\alpha i}\wedge u$, podemos suponer sin pérdida de generalidad que $p_{\alpha i}\leq u$, luego todos los elementos $p_{\alpha i}$ están en el álgebra $\mathbb{B}_u$. Esta álgebra cumple la hipótesis c), porque si $\{q_{\alpha i}\}_{i\in I_\alpha}$ son particiones de $\mathbb{B}_u$, entonces, al añadir u' a cada una de ellas, tenemos particiones de $\mathbb{B}$, y eliminando de un refinamiento común de todas ellas los elementos que no cumplan $q\leq u$ obtenemos un refinamiento común de todas las particiones dadas de $\mathbb{B}_u$. Así pues, cambiando $\mathbb{B}$ por $\mathbb{B}_u$, no perdemos generalidad si suponemos que $u=\mathbb{1}$.

Por el teorema 7.39 podemos construir anticadenas $\{q_{\alpha i}\}_{i\in I_\alpha}$ de manera que $q_{\alpha i}\leq p_{\alpha i}$ y $\bigvee_{i\in I_\alpha} q_{\alpha i} = \bigvee_{i\in I_\alpha} p_{\alpha i} = \mathbb{1}$. Sea P una partición que refine a todas las particiones $\{q_{\alpha i}\}_{i\in I_\alpha}$. Entonces, para cada $p\in P$ existe una función f tal que $w\leq q_{\alpha f(\alpha)}\leq p_{\alpha f(\alpha)}$, luego $w\leq \bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)}$, luego

$$\mathbb{1} = \bigvee P \leq \bigvee_{f\in\prod_{\alpha<\kappa} I_\alpha}\bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)},$$

luego el supremo de la derecha es $\mathbb{1}$, como había que probar. ∎

Observemos que la propiedad 2) del teorema anterior tiene sentido en c.p.o.s arbitrarios, lo que nos lleva a la definición siguiente:

Definición 7.55 Si κ es un cardinal, un c.p.o. es *κ-distributivo* si la intersección de κ abiertos densos es densa.

Notemos que $\mathbb{P}$ es $\aleph_0$-distributivo si y sólo si es un espacio de Baire, en el sentido de [T 1.64].

Teorema 7.56 *Si $i:\mathbb{P}\longrightarrow\mathbb{Q}$ es una inmersión densa de c.p.o.s separativos y κ es un cardinal, entonces $\mathbb{P}$ es κ-distributivo si y sólo si lo es $\mathbb{Q}$. En particular, un c.p.o. es κ-distributivo si y sólo si lo es su compleción.*

Demostración: Supongamos que $\mathbb{P}$ es κ-distributivo y sea $\{D_\alpha\}_{\alpha<\kappa}$ una familia de κ abiertos densos en $\mathbb{Q}$. Entonces $i^{-1}[D_\alpha]$ es un abierto denso en $\mathbb{P}$. En efecto, si $p_1\leq p_2\in i^{-1}[D_\alpha]$, entonces $i(p_1)\leq i(p_2)\in D_\alpha$, luego $i(p_1)\in D_\alpha$, luego $p_1\in i^{-1}[D_\alpha]$, lo que prueba que la antiimagen es abierta.

Si $p\in\mathbb{P}$, existe $q\in D_\alpha$ tal que $q\leq i(p)$ y, como i es densa, existe $p'\in\mathbb{P}$ tal que $i(p')\leq q\leq i(p)$. Como D_α es abierto, de hecho $i(p')\in D_\alpha$, luego $p'\in i^{-1}[D_\alpha]$ y, como los c.p.o.s son separativos, $p'\leq p$, lo que prueba que la antiimagen es densa.

Por hipótesis, la intersección $\bigcap_{\alpha<\kappa} i^{-1}[D_\alpha]$ es densa. Ahora, si $q \in \mathbb{Q}$, existe un $p \in \mathbb{P}$ tal que $i(p) \leq q$ y, reduciéndolo, podemos suponer que $p \in \bigcap_{\alpha<\kappa} i^{-1}[D_\alpha]$, luego $i(p) \in \bigcap_{\alpha<\kappa} D_\alpha$. Esto prueba que la intersección es densa y que $\mathbb{Q}$ es κ-distributivo.

Supongamos ahora que $\mathbb{Q}$ es κ-distributivo y sea $\{D_\alpha\}_{\alpha<\kappa}$ una familia de κ abiertos densos en $\mathbb{P}$. Entonces

$$D^*_\alpha = \{q \in \mathbb{Q} \mid \bigvee p \in D_\alpha\, q \leq i(p)\}$$

es abierto denso en $\mathbb{Q}$. En efecto, es obvio que es abierto y, si $q \in \mathbb{Q}$, existe un $p \in \mathbb{P}$ tal que $i(p) \leq q$, y reduciéndolo podemos suponer que $p \in D_\alpha$, con lo que $i(p) \in D^*_\alpha$, lo que prueba que D^*_α es denso. Por hipótesis la intersección $\bigcap_{\alpha<\kappa} D^*_\alpha$ es densa en $\mathbb{Q}$.

Si $p \in \mathbb{P}$, entonces existe un $q \in \bigcap_{\alpha<\kappa} D^*_\alpha$ tal que $q \leq i(p)$, luego existe un $p' \in \mathbb{P}$ tal que $i(p') \leq q \leq i(p)$. Esto implica que $p' \leq p$ y además se cumple que $p' \in \bigcap_{\alpha<\kappa} D_\alpha$. En efecto, como $q \in D^*_\alpha$, existe un $p'' \in D_\alpha$ tal que $i(p') \leq q \leq i(p'')$, luego $p' \leq p''$ y, como D_α es abierto, $p' \in D_\alpha$. Esto prueba que la intersección es densa y que $\mathbb{P}$ es κ-distributivo. ∎

7.6 Medidas

La teoría de la medida tiene sus raíces en el análisis matemático y en la estadística, más concretamente, en el cálculo de áreas y volúmenes, así como en el cálculo de probabilidades. Sin embargo, sus fundamentos son puramente conjuntistas hasta cierto punto y, yendo un poco más allá, puramente topológicos. En esta sección vamos a exponer los resultados básicos sobre medidas y álgebras de Boole.

Definición 7.57 Sea $\mathbb{B}$ un álgebra de Boole. Una *medida finitamente aditiva* en $\mathbb{B}$ es una aplicación $\mu : \mathbb{B} \longrightarrow [0, +\infty]$ tal que[5]

1. $\mu(\mathbb{0}) = 0$, $\mu(\mathbb{1}) > 0$,
2. $\bigwedge pq \in \mathbb{B}(p \wedge q = \mathbb{0} \to \mu(p \vee q) = \mu(p) + \mu(q))$.

Se dice que μ es *unitaria* si $\mu(\mathbb{1}) = 1$, se dice que μ es *finita* si $\mu(\mathbb{1}) < +\infty$, se dice que μ es *σ-finita* si existen condiciones $\{p_n\}_{n\in\omega}$ en $\mathbb{B}$ tales que $\mathbb{1} = \bigvee_{n\in\omega} p_n$ y $\bigwedge n \in \omega\ \mu(p_n) < +\infty$.

Si $\mathbb{B}$ es $\aleph_1$-completa (es decir, si los conjuntos numerables tienen supremo e ínfimo) diremos que μ es una *medida* en $\mathbb{B}$ si para toda anticadena $\{p_n\}_{n\in\omega}$ en $\mathbb{B}$ se cumple que

$$\mu\Big(\bigvee_{n\in\omega} p_n\Big) = \sum_{n\in\omega} \mu(p_n).$$

[5] Convenimos en que una suma con un sumando igual a $+\infty$ toma el valor $+\infty$.

Esta condición contiene ya la propiedad b) de la definición de medida finitamente aditiva.

Un *álgebra medida* es un par ordenado $(\mathbb{B}, \mu)$, donde $\mathbb{B}$ es un álgebra de Boole $\aleph_1$-completa y μ es una medida en $\mathbb{B}$.

Si $\mathbb{B}$ es un álgebra medida, el *ideal de los elementos nulos* de $\mathbb{B}$ se define como

$$I_\mu = \{p \in \mathbb{B} \mid \mu(p) = 0\}.$$

El teorema siguiente recoge las propiedades elementales de los conceptos que acabamos de introducir.

Teorema 7.58 *Sea $\mathbb{B}$ un álgebra medida.*

1. *Si p, $q \in \mathbb{B}$, $p \leq q$, entonces $\mu(p) \leq \mu(q)$.*
2. *Si $\{p_n\}_{n\in\omega}$ es una familia de elementos de $\mathbb{B}$, no necesariamente incompatibles entre sí, entonces*
$$\mu\Big(\bigvee_{n\in\omega} p_n\Big) \leq \sum_{n\in\omega} \mu(p_n).$$
3. *Si p, $q \in \mathbb{B}$, entonces $\mu(p \vee q) \leq \mu(p) + \mu(q)$.*
4. *Si $\{p_n\}_{n\in\omega}$ es una sucesión creciente en $\mathbb{B}$, entonces*
$$\mu\Big(\bigvee_{n\in\omega} p_n\Big) = \sup_{n\in\omega} \mu(p_n).$$
5. *Si $\{p_n\}_{n\in\omega}$ es una sucesión decreciente en $\mathbb{B}$ y $\mu(p_0) < +\infty$, entonces*
$$\mu\Big(\bigwedge_{n\in\omega} p_n\Big) = \inf_{n\in\omega} \mu(p_n).$$
6. *I_μ es un ideal $\aleph_1$-completo de $\mathbb{B}$.*
7. **(AE)** *Si μ es σ-finita entonces I_μ cumple la condición de cadena numerable.*

Demostración: 1) Es fácil ver que $q = p \vee (q \wedge p')$ y $p \wedge (q \wedge p') = \mathbb{0}$, luego $\mu(q) = \mu(p) + \mu(q \wedge p') \geq \mu(p)$.

3) $\mu(p \vee q) = \mu(p \vee (q \wedge p')) = \mu(p) \wedge \mu(q \wedge p') \leq \mu(p) + \mu(q)$.

2) Sea $q_n = p_n \wedge \big(\bigvee_{m<n} p_m\big)'$. Claramente $q_n \leq p_n$, pero $\bigvee_{n\in\omega} q_n = \bigvee_{n\in\omega} p_n$, pues

$$p_n \leq \bigvee_{m\leq n} q_m \leq \bigvee_{n\in\omega} q_n.$$

La primera desigualdad se prueba por inducción:

$$p_n = \Big(p_n \wedge \big(\bigvee_{m<n} p_m\big)'\Big) \vee \Big(p_n \wedge \big(\bigvee_{m<n} p_m\big)\Big) \leq q_n \vee \big(\bigvee_{m<n} q_m\big) = \bigvee_{m\leq n} q_m.$$

Además $\{q_n\}_{n\in\omega}$ es una anticadena, luego

$$\mu\Big(\bigvee_{n\in\omega} p_n\Big) = \mu\Big(\bigvee_{n\in\omega} q_n\Big) = \sum_{n\in\omega} \mu(q_n) \le \sum_{n\in\omega} \mu(p_n).$$

4) De forma similar a como hemos hecho en el apartado anterior, podemos expresar $\bigvee_{n\in\omega} p_n = p_0 \vee \bigvee_{n\in\omega} (p_{n+1} \wedge p_n')$, de modo que

$$\mu\Big(\bigvee_{n\in\omega} p_n\Big) = \mu(p_0) + \sum_{n\in\omega} \mu(p_{n+1} \wedge p_n').$$

Si $\mu(p_0) = +\infty$ o algún $\mu(p_{n+1} \wedge p_n') = +\infty$, es claro que los dos miembros de la igualdad que hemos de probar son infinitos. En caso contrario tenemos que $\mu(p_{n+1}) = \mu(p_n) + \mu(p_{n+1} \wedge p_n')$, luego por inducción todos los p_n tienen medida finita y

$$\mu\Big(\bigvee_{n\in\omega} p_n\Big) = \mu(p_0) + \sum_{n\in\omega} (\mu(p_{n+1}) - \mu(p_n)) = \sup_{n<\omega} \mu(p_n).$$

5) La sucesión $\{p_0 \wedge p_n'\}_{n<\omega}$ está en las condiciones del apartado anterior, luego

$$\mu\big(p_0 \wedge \bigvee_{n\in\omega} p_n'\big) = \sup_{n<\omega} \mu(p_0 \wedge p_n'),$$

lo cual equivale a

$$\mu\big(p_0 \wedge \big(\bigwedge_{n\in\omega} p_n\big)'\big) = \sup_{n<\omega} (\mu(p_0) - \mu(p_n)),$$

o también a

$$\mu(p_0) - \mu\Big(\bigwedge_{n\in\omega} p_n\Big) = \mu(p_0) - \inf_{n\in\omega} \mu(p_n).$$

6) Que I_μ es un ideal $\aleph_1$-completo se sigue inmediatamente de las propiedades anteriores.

7) Para probar que cumple la condición de cadena numerable hemos de ver que no existe ninguna anticadena $\{p_\alpha\}_{\alpha<\omega_1}$ en $\mathbb{B} \setminus I_\mu$.

Estamos suponiendo que μ es σ-finita, con lo que podemos descomponer $\mathbb{1} = \bigvee_{n\in\omega} r_n$, donde $\mu(r_n) < +\infty$. Razonando como en 2) podemos suponer que las condiciones r_n son incompatibles dos a dos.

Entonces $p_\alpha = \bigvee_{n\in\omega} p_\alpha \wedge r_n$, luego $0 < \mu(p_\alpha) = \sum_{n\in\omega} \mu(p_\alpha \wedge r_n)$. Por consiguiente existe un $n \in \omega$ tal que $\mu(p_\alpha \wedge r_n) > 0$. Más aún, ha de haber una cantidad no numerable de α's para las que sirva el mismo n. Restringiendo la anticadena de partida podemos suponer que el mismo n vale para todo α. Así, si llamamos $r = r_n$, tenemos que $\mu(r_n) < +\infty$ y $\bigwedge\alpha < \omega_1\ \mu(p_\alpha \wedge r) > 0$.

Entonces $\omega_1 = \bigcup_{m\in\omega} \{\alpha < \omega_1 \mid \mu(p_\alpha \wedge r) > 1/m\}$. Alguno de estos conjuntos ha de ser no numerable, luego restringiendo de nuevo la anticadena inicial podemos suponer que $\bigwedge \alpha < \omega_1\ \mu(p_\alpha \wedge r) > 1/m$, pero esto es absurdo, pues para todo $k \in \omega$ tenemos que

$$\frac{k}{m} < \sum_{n<k} \mu(p_n \wedge r) = \mu\Big(\bigvee_{n<k} p_n \wedge r\Big) \leq \mu(r),$$

y esto obliga a que $\mu(r) = +\infty$. ∎

Así, el cociente de un álgebra de Boole respecto al ideal de elementos nulos de una medida σ-finita nos da un álgebra de Boole completa:

Teorema 7.59 *Sea $\mathbb{B}$ un álgebra medida y consideremos el cociente $\mathbb{B}_\mu = \mathbb{B}/I_\mu$.*

1. *$\mathbb{B}_\mu$ es $\aleph_1$-completa y es un álgebra medida con $\overline{\mu} : \mathbb{B}_\mu \longrightarrow \mathbb{R}$ dada por $\overline{\mu}([p]) = \mu(p)$. Además $I_{\overline{\mu}}$ es trivial. Si μ es finita, σ-finita o unitaria, entonces $\overline{\mu}$ también lo es.*

2. *Si $\{p_n\}_{n\in\omega}$ es una familia de elementos de $\mathbb{B}$, entonces*

$$\bigvee_{n\in\omega} [p_n] = \Big[\bigvee_{n\in\omega} p_n\Big], \qquad \bigwedge_{n\in\omega} [p_n] = \Big[\bigwedge_{n\in\omega} p_n\Big].$$

3. **(AE)** *Si μ es σ-finita entonces $\mathbb{B}_\mu$ es completa y cumple la condición de cadena numerable.*

Demostración: El hecho de que $\mathbb{B}_\mu$ sea $\aleph_1$-completa es el apartado 2): claramente $[p_n] \leq \big[\bigvee_{n\in\omega} p_n\big]$, y si $[r]$ es una cota superior de todos los $[p_n]$ entonces $[p_n \wedge r'] = \mathbb{0}$, luego $p_n \wedge r' \in I_\mu$ y como éste es $\aleph_1$-completo, $\bigvee_{n\in\omega} p_n \wedge r' \in I_\mu$, luego $\big[\bigvee_{n\in\omega} p_n\big] \wedge [r]' = \mathbb{0}$ y, por consiguiente $\big[\bigvee_{n\in\omega} p_n\big] \leq [r]$. Esto prueba la primera parte de b), y la segunda se sigue inmediatamente.

Tenemos, pues, que $\mathbb{B}_\mu$ es $\aleph_1$-completa. La medida $\overline{\mu}$ está bien definida, pues si $[p] = [q]$ entonces $(p \wedge q') \vee (p' \wedge q) \in I_\mu$, luego $\mu(p \wedge q') = \mu(p' \wedge q) = 0$. Consecuentemente

$$\mu(p) = \mu(p \wedge q) + \mu(p \wedge q') = \mu(p \wedge q),$$

e igualmente $\mu(q) = \mu(p \wedge q)$, luego $\mu(p) = \mu(q)$. Ahora es obvio que $\overline{\mu}$ es una medida en $\mathbb{B}_\mu$, así como que es unitaria, finita o σ-finita si μ lo es. Su ideal es trivial, pues si $\overline{\mu}([p]) = 0$ es que $\mu(p) = 0$, luego $p \in I_\mu$ y $[p] = \mathbb{0}$.

c) $\mathbb{B}_\mu$ es $\aleph_1$-completa por 7.36, cumple la condición de cadena numerable por el apartado 7) del teorema anterior, y por consiguiente es completa por 7.34. ∎

Estamos considerando medidas σ-finitas porque algunas de las medidas más importantes lo son, como es el caso de la medida de Lebesgue en $\mathbb{R}^n$, pero en

muchos casos nos interesará más el álgebra sobre la que está definida una medida y su ideal de elementos nulos que los valores concretos que toma la medida. En tal caso el teorema siguiente muestra que toda medida σ-finita se puede sustituir por una medida unitaria.

Teorema 7.60 *Si $(\mathbb{B},\mu)$ es un álgebra medida σ-finita, existe una medida unitaria μ' en $\mathbb{B}$ tal que $I_\mu = I_{\mu'}$.*

Demostración: Sean $\{p_n\}_{n\in\omega}$ elementos de $\mathbb{B}$ de medida finita y con supremo $\mathbb{1}$. Podemos suponer que $\mu(p_n) > 0$ para todo n. Entonces definimos

$$\mu'(p) = \sum_{n\in\omega} \frac{\mu(p_n \wedge p)}{\mu(p_n)} \frac{1}{2^{n+1}}.$$

Es fácil ver que μ' es una medida unitaria en $\mathbb{B}$ que cumple lo requerido. ∎

Definición 7.61 Sea $\mathbb{B}$ un álgebra medida. Se dice que $p \in \mathbb{B}$ es un *átomo* si $\mu(p) > 0$ y $\bigwedge q \in \mathbb{B}(q \le p \to \mu(q) = 0 \vee \mu(q) = \mu(p))$. La medida μ es *atómica* o *no atómica* según si tiene o no tiene átomos.

Es fácil comprobar que $p \in \mathbb{B}$ es un átomo si y sólo si $[p]$ es un átomo en el álgebra $\mathbb{B}_\mu$, por lo que μ es atómica si y sólo si lo es $\overline{\mu}$. Necesitaremos el teorema siguiente:

Teorema 7.62 (AE) *Sea μ una medida no atómica en un álgebra $\mathbb{B}$, sea $p \in \mathbb{B}$ y sea k un número real tal que $0 < k < \mu(p) < +\infty$. Entonces existe $q \in \mathbb{B}$ tal que $q \le p$ y $\mu(q) = k$.*

Demostración: Supongamos que ningún $q \le p$ tiene medida k. Veamos en primer lugar que para todo $q \in \mathbb{B}$ con $\mu(q) > 0$ y para todo natural $n > 1$ existe una anticadena $\{s_i\}_{i<n}$ en $\mathbb{B}$ tal que $q = \bigvee\limits_{i<n} s_i$ y $\bigwedge i < n\ \mu(s_i) > 0$.

Razonamos por inducción sobre n. Para $n = 2$, como q no es un átomo, existe $s_0 \le q$ tal que $0 < \mu(s_0) < \mu(q)$. Basta tomar $s_1 = q \wedge s_0'$. Claramente $q = s_0 \vee s_1$, $s_0 \wedge s_1 = \mathbb{0}$ y $\mu(q) = \mu(s_0) + \mu(s_1)$, luego ambos sumandos son positivos.

Si vale para n, por el caso 2 podemos descomponer $q = q' \vee s_n$, de modo que $q' \wedge s_n = \mathbb{0}$ y $\mu(q') > 0$, $\mu(s_n) > 0$. Basta aplicar a q' la hipótesis de inducción.

Veamos ahora que si $q \in \mathbb{B}$ cumple $k < \mu(q) < +\infty$, entonces existe $r \le q$ tal que $k < \mu(r) < \mu(q)$.

Sea n un natural tal que $\frac{1}{n}\mu(q) < \mu(q) - k$. Sea $\{s_i\}_{i<n}$ una anticadena tal que $q = \bigvee\limits_{i<n} s_i$ y $\bigwedge i < n\ \mu(s_i) > 0$. Como

$$\mu(q) = \sum_{i<n} \mu(s_i),$$

algún $i < n$ ha de cumplir que $\mu(s_i) \le \frac{1}{n}\mu(q) < \mu(q) - k$. Sea $r = q \wedge s_i' \le q$. Así $\mu(q) = \mu(s_i) + \mu(r)$, luego $\mu(r) = \mu(q) - \mu(s_i) > k$.

Vamos a construir una sucesión $\{s_\alpha\}_{\alpha<\omega_1}$ tal que

$$\bigwedge\alpha\beta(\alpha<\beta<\omega_1 \to s_\beta \le s_\alpha \wedge k<\mu(s_\beta)<\mu(s_\alpha)).$$

Partimos de $s_0 = p$. Definido s_α tal que $k<\mu(s_\alpha)$, acabamos de probar que existe $s_{\alpha+1}$ tal que $s_{\alpha+1} \le s_\alpha$ y $k<\mu(s_{\alpha+1})<\mu(s_\alpha)$. Definidos $\{s_\delta\}_{\delta<\lambda}$, para un ordinal límite $\lambda<\omega_1$, sea $s_\lambda = \bigwedge\limits_{\delta<\lambda} s_\delta$. Sea $\{\delta_n\}_{n<\omega}$ una sucesión cofinal creciente en λ. Es claro que $s_\lambda = \bigwedge\limits_{n<\omega} s_{\delta_n} = \inf\limits_{n<\omega} \mu(s_{\delta_n}) \ge k$, pero por hipótesis ha de ser $\mu(s_\lambda) > k$.

La sucesión de números reales $\{\mu(s_\alpha)\}_{\alpha<\omega_1}$ es estrictamente decreciente, y está acotada inferiormente por k, luego existe $a = \inf\limits_{\alpha<\omega_1} \mu(s_\alpha)$ y $k \le a$.

Si $0<n<\omega$, tomemos $\alpha_n<\omega_1$ tal que $\bigwedge\alpha \ge \alpha_n\ a+\frac{1}{n} > \mu(s_\alpha)$. Sea $\alpha = \sup\limits_{n<\omega} \alpha_n < \omega_1$. Entonces $\mu(s_\alpha) - a < 1/n$ para todo natural $n>0$, luego ha de ser $\mu(s_\alpha) = a$, pero entonces también $\mu(s_{\alpha+1}) = a$, contradicción, pues por construcción $\mu(s_{\alpha+1}) < \mu(s_\alpha)$. ∎

7.7 Las álgebras de medida y categoría

Vamos a aplicar la teoría que hemos presentado hasta ahora al estudio de dos importantes álgebras de Boole completas.

El álgebra de medida Sea X un espacio polaco y μ una medida de Borel en X unitaria y continua. La σ-álgebra de los conjuntos μ-medibles es la compleción $\mathcal{M}_\mu$ de la medida μ dada por el teorema [T B.15], que está formada por todos los conjuntos $A \subset X$ tales que existen conjuntos de Borel $E \subset A \subset F$ con $\mu(F \setminus E) = 0$. Esto hace que $A = E \cup N$, donde $N = A \setminus E \subset F \setminus E$ es un conjunto de Borel nulo.

La medida μ se extiende a una medida completa en $\mathcal{M}_\mu$, lo que significa que todo subconjunto de un conjunto nulo es nulo o, en otros términos, que el conjunto I_μ formado por los conjuntos nulos, no sólo es un ideal de $\mathcal{M}_\mu$, sino también de $\mathcal{P}X$.

Es claro que la inclusión $\mathcal{B}(X) \longrightarrow \mathcal{M}_\mu$ induce un isomorfismo de álgebras $\mathcal{B}(X)/(I_\mu \cap \mathcal{B}(X)) \longrightarrow \mathcal{M}_\mu/I_\mu$.

Definición 7.63 Si X es un espacio polaco y μ una medida de Borel en X unitaria y continua, llamaremos *álgebra de medida* al álgebra de Boole cociente $\mathcal{B}_m = \mathcal{M}_\mu/I_\mu$.

Según acabamos de ver, también podemos considerar que $\mathcal{B}_m = \mathcal{B}(X)/I_\mu$, donde aquí I_μ es el ideal de los conjuntos de Borel nulos.

Más precisamente, de acuerdo con las observaciones iniciales de la sección 6.5 de [T], toda clase en $\mathcal{B}_m$ admite un representante F_σ y otro G_δ.

De acuerdo con [T 6.40], existe un isomorfismo de Borel $f : X \longrightarrow \mathbb{I} = [0,1]$ tal que, para todo conjunto $A \in \mathcal{M}_\mu$, se cumple que $\mu(A) = m([f[A]])$, donde m es la medida de Lebesgue en $\mathbb{I}$.

Esto significa que f es biyectiva y que la aplicación $F : \mathcal{B}(\mathbb{I}) \longrightarrow \mathcal{B}(X)$ dada por $F(A) = f^{-1}[A]$ es un isomorfismo de álgebras de Boole, de modo que $\mu(F(A)) = m(A)$. En particular F hace corresponder los conjuntos m-nulos con los conjuntos μ-nulos, por lo que induce un isomorfismo $\mathcal{B}(\mathbb{I})/I_m \longrightarrow \mathcal{B}(X)/I_m$.

Así pues, todas las álgebras de medida $\mathcal{B}_m$ definidas por cualquier medida continua y unitaria en cualquier espacio polaco son isomorfas entre sí o, dicho de otro modo, el álgebra de medida es independiente del espacio y de la medida con la que se construye.

Según el teorema 7.59 **(AE)**, se trata de un álgebra de Boole completa con la condición de cadena numerable.

Notemos que el isomorfismo de Borel f es una biyección, luego también induce un isomorfismo de álgebras $\mathcal{P}\mathbb{I} \longrightarrow \mathcal{P}X$ que hace corresponder los ideales de conjuntos nulos para las medidas m y μ. Más aún, por el teorema 7.60, esto es cierto para medidas σ-finitas μ, no necesariamente unitarias.

El álgebra de categoría Si X es un espacio polaco, en [T 6.41] hemos definido la σ-álgebra $\mathrm{Ba}(X)$ de los subconjuntos de X con la propiedad de Baire, que está formada por los conjuntos $A \subset X$ para los que existe un abierto U tal que $A \triangle U$ es de primera categoría.

El conjunto I_c de los subconjuntos de X de primera categoría es un ideal tanto de $\mathcal{P}X$ como de $\mathrm{Ba}(X)$ y es claro que la inclusión $\mathcal{B}(X) \longrightarrow \mathrm{Ba}(X)$ induce un isomorfismo de álgebras $\mathcal{B}(X)/(I_c \cap \mathcal{B}(X)) \longrightarrow \mathrm{Ba}(X)/I_c$.

Definición 7.64 Si X es un espacio polaco, llamaremos *álgebra de categoría* al álgebra de Boole cociente $\mathcal{B}_c = \mathrm{Ba}(X)/I_c$.

Según acabamos de observar, también podemos considerar que $\mathcal{B}_c = \mathcal{B}(X)/I_c$, donde aquí I_c es el ideal de los conjuntos de Borel de primera categoria. De hecho, de la definición de la propiedad de Baire se deduce inmediatamente que toda clase de $\mathcal{B}_c$ tiene un representante abierto. Esto puede precisarse un poco más:

Teorema 7.65 *Si X es un espacio polaco y $R(X)$ es su álgebra de abiertos regulares, la aplicación $R(X) \longrightarrow \mathcal{B}_c$ dada por $A \mapsto [A]$ es un isomorfismo de álgebras de Boole. En particular, $\mathcal{B}_c$ es un álgebra de Boole completa con la condición de cadena numerable.*

Demostración: Recordemos (7.29) que si A es un abierto, entonces $\overline{\overset{\circ}{A}}$ es siempre un abierto regular. Como $A \subset \overset{\circ}{\overline{A}} \subset \overline{A}$ y $\overline{A} \setminus A$ tiene interior vacío (luego es de primera categoría), $\overset{\circ}{\overline{A}} \setminus A$ también es de primera categoría. Esto significa que A y $\overline{\overset{\circ}{A}}$ determinan la misma clase en el álgebra $\mathcal{B}_c$, luego la aplicación considerada en el enunciado es suprayectiva.

Supongamos ahora que A y B son abiertos regulares cuyas clases en $\mathcal{B}_c$ cumplen $[A] \leq [B]$. Esto significa que $A \setminus B$ es de primera categoría. Ahora bien, entonces $A \setminus \overline{B} \subset A \setminus B$ también es de primera categoría, pero $A \setminus \overline{B}$ es abierto, y el único abierto de primera categoría es $\varnothing$. Por consiguiente, $A \subset \overline{B}$, luego también $A \subset \overset{\circ}{\overline{B}} = B$. El recíproco es trivial. En definitiva, tenemos que

$$A \subset B \leftrightarrow [A] \leq [B].$$

En particular, esto implica que la aplicación del enunciado es biyectiva y que además es una semejanza para las relaciones de orden de las álgebras respectivas (pues, aunque las operaciones booleanas de $R(X)$ no sean las conjuntistas, el ínfimo sí que coincide con la intersección de conjuntos y la relación de orden es la inclusión). Por consiguiente, se trata de un isomorfismo de álgebras. ∎

Veamos ahora que, al igual que sucede con el álgebra de medida, el álgebra de categoría es única (salvo isomorfismo) para todos los espacios polacos perfectos. La condición de que no haya puntos aislados es la correspondiente a la condición de considerar medidas continuas, pues si p un punto aislado entonces $\{p\}$ es un conjunto de segunda categoría, que es el análogo a que $\{p\}$ tenga medida positiva. La condición es necesaria en el teorema siguiente, pues es fácil ver que los puntos aislados de X se corresponden biunívocamente con los átomos del álgebra $\mathcal{B}_c(X)$.

Teorema 7.66 *Si X e Y son espacios polacos perfectos, sus álgebras de categoría respectivas son isomorfas.*

Demostración: Por el teorema anterior, basta demostrar que las álgebras $R(X)$ y $R(Y)$ de abiertos regulares son isomorfas. Vamos a construir un esquema de Suslin[6] en X a partir del resultado siguiente:

> *Si U es un abierto regular no vacío en X y $\epsilon > 0$, existe una familia $\{U_n\}_{n\in\omega}$ de abiertos regulares en X contenidos en U y disjuntos dos a dos cuya unión es densa en X.*

En efecto, sea $\{d_n\}_{n\in\omega}$ un subconjunto denso de U (que ha de ser infinito, porque X no tiene puntos aislados). Tomamos una bola abierta de centro d_0 contenida en U, de diámetro $< \epsilon$ y cuya clausura no contenga a algún punto de U, y llamamos U_0 al interior de dicha clausura. Entonces $U \setminus \overline{U_0}$ es un abierto regular no vacío. Del mismo modo, podemos obtener un abierto regular $U_1 \subset U \setminus \overline{U_0}$ de diámetro $< \epsilon$ y tal que $d_2 \in U_0 \cup U_1$. Procediendo de este modo obtenemos la sucesión buscada.

Esto nos permite construir un esquema de Suslin $A : \omega^{<\omega} \longrightarrow R(X)$ con las propiedades siguientes:

1. $A(\varnothing) = X$.
2. La unión $\bigcup_{n\in\omega} A(s^\frown n)$ es disjunta y densa en $A(s)$.
3. $A(s)$ tiene diámetro menor que $1/l(s)$.

[6] Véase la sección 6.2 de [T].

Observemos ahora que si $U \subset X$ es cualquier abierto regular no vacío, existe un $s \in \omega^{<\omega}$ tal que $A(s) \subset U$. En efecto, U contendrá una bola abierta $B_{1/n}(x)$, para cierto $x \in U$ y cierto $n \in \omega$. Sea $B = B_{1/2n}(x)$. Por la propiedad 2), para $s = \varnothing$, existe un $s_1 \in \omega^1$ tal que $B \cap A(s_1) \neq \varnothing$, luego existe un $s_2 \in \omega^2$ (necesariamente $s_1 \subset s_2$) tal que $B \cap A(s_2) \neq \varnothing$ y, razonando de este modo, llegamos a un $s_{2n} \in \omega^{2n}$ tal que $B \cap A(s_{2n}) \neq \varnothing$ y, como el diámetro de $A(s_{2n})$ es menor que $1/2n$, ha de ser $A(s_{2n}) \subset B_{1/n}(x) \subset U$.

Ahora es inmediato que A es una inmersión densa, luego 7.49 nos da que $R(X) \cong R(\omega^{<\omega})$, y esto es válido para cualquier espacio polaco perfecto, luego, si Y es otro cualquiera, tenemos el isomorfismo $R(X) \cong R(Y)$. ∎

En lo sucesivo, cuando hablemos del álgebra $\mathcal{B}_c$ nos referiremos al álgebra de categoría de cualquier espacio polaco perfecto. Acabamos de probar que no importa cuál consideremos.

Usando el axioma de elección podemos dar una prueba más conceptual de la unicidad del álgebra de categoría, pues ésta es consecuencia inmediata del apartado 2) del teorema siguiente:

Teorema 7.67 (AE) *Se cumple:*

1. *Dos álgebras de Boole no atómicas numerables cualesquiera son isomorfas entres sí.*
2. *Toda álgebra de Boole completa no atómica que posea un subconjunto denso numerable es isomorfa al álgebra de categoría $\mathcal{B}_c$.*

Demostración: 1) Un álgebra de Boole $\mathbb{B}$ es no atómica y numerable si y sólo si su espacio de Stone es un espacio compacto cero-dimensional con una base numerable y sin puntos aislados. Por [T 6.6] tenemos que $S(\mathbb{B})$ es un espacio polaco, y el teorema de Brouwer [T 6.17] afirma que es homeomorfo al espacio de Cantor $\mathcal{C}$, luego $\mathbb{B}$ es isomorfa al álgebra de abiertos-cerrados de $\mathcal{C}$.

2) Un conjunto denso numerable en un álgebra de Boole no atómica genera un álgebra de Boole densa no atómica numerable, luego dos álgebras en las condiciones del enunciado tienen (por el apartado anterior) subálgebras densas isomorfas, luego ambas son isomorfas a la compleción de una misma álgebra, luego son isomorfas entre sí. Como $\mathcal{B}_c$ cumple las hipótesis, cualquier otra álgebra que las cumpla es isomorfa a $\mathcal{B}_c$. ∎

Medida y categoría Las álgebras de medida y categoría no son isomorfas:

Teorema 7.68 $\mathcal{B}_m \ncong \mathcal{B}_c$.

En la prueba del teorema 7.66 hemos visto que el álgebra de categoría tiene un subconjunto denso numerable. Basta probar que no le sucede lo mismo al álgebra de medida. En efecto, sea $\{[D_n]\}_{n\in\omega}$ un subconjunto numerable (de elementos no nulos) de $\mathcal{B}_m$ y vamos a probar que no es denso. (No importa el espacio polaco X ni la medida continua unitaria μ con la que construyamos el

álgebra.) Como $\mu(D_n) > 0$ podemos tomar un cerrado $E_n \subset D_n$ de manera que $0 < \mu(E_n) < 2^{-n-2}$. Tomemos $E = \bigcup_{n\in\omega} E_n$. Así $0 < \mu(E) < 1$, luego $\mu(X \setminus E) > 0$, luego $[X \setminus E] \neq 0$.

Además, $E_n \subset D_n \setminus (X \setminus E)$, luego $0 < [D_n] \wedge [X \setminus E]'$, luego resulta que $[D_n] \not\leq [X \setminus E]$ para todo $n \in \omega$. Esto prueba que el conjunto dado no es denso. ∎

Sin embargo, podemos mostrar una diferencia más notable entre ambas álgebras: si construimos $\mathcal{B}_m$ a partir de una medida unitaria μ, es claro que μ induce a su vez una medida $\mu : \mathcal{B}_m \longrightarrow [0,1]$ que es *estrictamente positiva,* es decir, que cumple $\mu(x) = 0$ si y sólo si $x = \mathbb{0}$. Por el contrario:

Teorema 7.69 *No existen medidas estrictamente positivas sobre el álgebra $\mathcal{B}_c$.*

Demostración: Para ello introducimos los conceptos siguientes:

Un subconjunto D de un álgebra de Boole $\mathbb{B}$ es *predenso* si su supremo es $\mathbb{1}$.

Notemos que si D es denso, entonces es predenso, pues, si $\bigvee D = b < \mathbb{1}$, no habría elementos de D por debajo de b'.

Un álgebra $\mathbb{B}$ es *débilmente $\aleph_1$-distributiva* si para toda sucesión $\{D_n\}_{n\in\omega}$ de subconjuntos predensos numerables existe un subconjunto predenso A tal que para todo $a \in A$ y todo $n \in \omega$ existe $C_n \subset A_n$ finito tal que $a \leq \bigvee C_n$.

Ahora demostramos que si un álgebra $\mathbb{B}$ admite una medida estrictamente positiva μ, entonces es débilmente $\aleph_1$-distributiva.

En efecto, sea $\{A_n\}_{n\in\omega}$ una familia de subconjuntos predensos numerables. Si $A_n = \{d^n_i\}_{i\in\omega}$ y llamamos

$$e^n_i = d^n_i \wedge \Big(\bigvee_{j<i} d^n_j\Big)',$$

se cumple que $\bigvee_{j<i} d^n_j = \bigvee_{j<i} e^n_j$, por lo que los conjuntos $A'_n = \{e^n_i\}_{i\in\omega}$ son predensos y sus elementos son incompatibles dos a dos. Además, basta probar que se cumple con ellos la definición de distributividad débil, ya que si $C'_n \subset A'_n$ es finito, existe un i tal que $\bigvee C'_n \leq \bigvee_{j<i} e^n_j = \bigvee_{j<i} d^n_j$, luego los A_n cumplen la definición con $C_n = \{d^n_j\}_{j<i}$.

Equivalentemente, podemos suponer que los elementos de A_n son incompatibles dos a dos. Vamos a probar que

$$A = \{b \in \mathbb{B} \mid \bigwedge n \in \omega \bigvee C \subset A_n(C \text{ finito} \wedge b \leq \bigvee C)\}$$

es denso en $\mathbb{B}$ y, por consiguiente, predenso.

Sea $a \in \mathbb{B}$, $a \neq \mathbb{0}$. Tenemos que $\bigvee_{x\in A_n} x = \mathbb{1}$, luego $\bigvee_{x\in A_n} x \wedge a = a$, luego, teniendo en cuenta que los elementos de A_n son disjuntos dos a dos, $0 < \mu(a) = \sum_{x\in A_n} \mu(x \wedge a)$, luego existe $C_n \subset A_n$ finito tal que

$$\mu(a \wedge \bigvee C_n) = \mu\Big(\bigvee_{x\in C_n} (x \wedge a)\Big) = \sum_{x\in C_n} \mu(x \wedge a) \geq (1 - \frac{1}{2^{n+2}})\mu(a).$$

Así

$$\mu(\bigvee_{n\in\omega}(a\wedge(\bigvee C_n)'))\le\sum_{n\in\omega}\mu(a\wedge(\bigvee C_n)')=\sum_{n\in\omega}(\mu(a)-\mu(a\wedge\bigvee C_n))$$

$$\le\sum_{n\in\omega}\frac{1}{2^{n+2}}\mu(a)=\frac{1}{2}\mu(a),$$

luego, llamando $b=a\wedge\bigwedge_{n\in\omega}\bigvee C_n$, tenemos que $\mu(b)\ge\mu(a)-\frac{1}{2}\mu(a)>0$, luego $b\neq\mathbb{0}$ y cumple $b\le a$ y $b\in A$.

Finalmente probamos que $\mathcal{B}_c$ no es débilmente $\aleph_1$-distributiva. No perdemos generalidad si consideramos, concretamente, el álgebra de categoría del espacio de Baire. Consideramos los abiertos cerrados (luego regulares)

$$D_i^n=\{x\in\mathcal{N}\mid x(n)=i\},$$

de modo que el conjunto $A_n=\{[D_i^n]\}_{i\in\omega}$ es predenso en $\mathcal{B}_c$, pues la unión de los D_i^n (para un n fijo) es $\mathcal{N}$. Vamos a probar que ningún $a\in\mathcal{B}_c$ no nulo cumple la definición de álgebra $\aleph_1$-distributiva, es decir, que si $a=[A]$, donde A es un abierto no vacío en $\mathcal{N}$, no pueden existir conjuntos finitos $C_n\subset\omega$ tales que $A\setminus\bigcup_{i\in C_n}D_i^n$ sea de primera categoría.

En tal caso, $A\setminus\bigcap_{n\in\omega}\bigcup_{i\in C_n}D_i^n$ también sería de primera categoría, luego el conjunto $C=\bigcap_{n\in\omega}\bigcup_{i\in C_n}D_i^n$ sería de segunda categoría, pero en realidad es un cerrado de interior vacío. En efecto, si contuviera un abierto, contendría un abierto básico B_s, para un cierto $s\in\omega^n$, luego $B_s\subset\bigcup_{i\in C_n}D_i^n$, pero esto es imposible, pues un $x\in\mathcal{N}$ que esté en el conjunto de la derecha sólo puede tomar un número finito de valores en n, mientras que B_s contiene puntos que toman en n cualquier valor. ∎

7.8 Cardinales medibles

Los resultados de las secciones anteriores nos permiten mostrar una relación notable entre la teoría de conjuntos y la teoría de la medida. En toda esta sección usaremos AE sin mencionarlo explícitamente. Conviene introducir algunas definiciones:

Definición 7.70 Una *medida* en un conjunto S es una medida en el álgebra $\mathcal{P}S$. Notemos que en tal caso el ideal I_μ de los conjuntos nulos es un ideal $\aleph_1$-completo en S.

Si κ es un cardinal infinito, diremos que μ es *κ-aditiva* si la unión de toda familia de menos de κ conjuntos nulos es nula. Así, toda medida en un conjunto S es $\aleph_1$-aditiva, y la κ aditividad equivale a que el ideal I_μ de los conjuntos nulos sea κ-completo.

Una *medida fuerte* en un cardinal $\kappa > \aleph_0$ es una medida unitaria, continua (es decir, tal que los puntos sean nulos) y κ-aditiva sobre κ. Un cardinal no numerable κ es $\mathbb{R}$-*medible* si existe una medida fuerte sobre κ. La $\mathbb{R}$ hace referencia a que la medida toma valores en $\mathbb{R}$, lo cual es obvio, pero se opone al caso más simple en que la medida es bivaluada:

Una medida *bivaluada* en S es una medida unitaria $\mu : \mathcal{P}S \longrightarrow \{0, 1\}$.

Un cardinal no numerable κ es *medible Ulam* si existe una medida continua bivaluada en κ. Un cardinal no numerable κ es *medible* si existe una medida fuerte bivaluada sobre κ.

Observemos que si $\mu : \mathcal{P}S \longrightarrow 2$ es una medida bivaluada, entonces el ideal I_μ de los conjuntos nulos es un ideal primo, pues es imposible que un conjunto y su complementario tengan ambos medida 0, luego su filtro dual U, formado por los conjuntos de medida 1, es un ultrafiltro en S.

Recíprocamente, todo ideal primo I (o todo ultrafiltro U) $\aleph_1$-completo en un conjunto S define una medida bivaluada en S, la dada por $\mu(A) = 1$ si y sólo si $A \in U$ (o $\mu(A) = 0$ si y sólo si $A \in I$).

Una medida bivaluada μ es continua si y sólo si todos los conjuntos $\{x\}$ están en I_μ, lo que equivale a que el ultrafiltro U sea libre. La medida μ es ν-aditiva si y sólo si el ideal I_μ es ν-completo, si y sólo si el ultrafiltro U es ν-completo.

Una *medida de Ulam* en un conjunto S es un ultrafiltro libre $\aleph_1$-completo en S. Así, un cardinal es medible Ulam si y sólo si existe una medida de Ulam en κ.

Similarmente, un cardinal no numerable κ es medible si y sólo si existe un ultrafiltro libre κ-completo en κ.

Vamos a usar a menudo el teorema siguiente, cuya prueba es trivial:

Teorema 7.71 *Sea μ una medida finita en un conjunto S y sea $f : S \longrightarrow T$. Entonces la aplicación $\sigma : \mathcal{P}T \longrightarrow [0, 1]$ dada por*

$$\sigma(Z) = \frac{\mu(f^{-1}[Z])}{\mu(S)}$$

es una medida unitaria en T, bivaluada si lo es μ. Además, si κ es un cardinal infinito y μ es κ-aditiva, también lo es σ.

El teorema B.1 asegura que no todo subconjunto de $\mathbb{R}$ es medible Lebesgue, pero no excluye que la medida de Lebesgue pueda extenderse a $\mathcal{P}\mathbb{R}$, a condición de que la extensión no sea invariante por traslaciones, pues dicha invarianza es lo único que se usa en la prueba.

Es fácil ver que la medida de Lebesgue admite una extensión a $\mathcal{P}\mathbb{R}$ si y sólo si la medida de Lebesgue en $\mathbb{I}$ admite una extensión a $\mathcal{P}\mathbb{I}$, pues en tal caso podríamos definir una medida en $\mathcal{P}\mathbb{R}$ mediante

$$\bar{\mu}(A) = \bigcup_{n\in\mathbb{Z}} \mu((A \cap [n, n + 1]) - n).$$

Por otra parte, en vista del teorema [T 6.40], que la medida de Lebesgue en $\mathbb{I}$ pueda extenderse a $\mathcal{P}\mathbb{I}$ es equivalente a que cualquier medida de Borel continua y unitaria en cualquier espacio polaco X pueda extenderse a $\mathcal{P}X$ (basta con que una cualquiera pueda extenderse para que todas puedan).

Si la medida de Lebesgue en $\mathbb{I}$ pudiera extenderse a $\mathcal{P}\mathbb{I}$, la extensión sería una medida continua, unitaria y no atómica.

En efecto, lo único que no es inmediato es que la extensión sería no atómica, pero si $A \subset \mathbb{I}$ fuera un átomo, podríamos dividir $\mathbb{I}$ en una unión finita de intervalos disjuntos de medida menor que $\mu(A)$, con lo que la intersección de A con estos intervalos tendría que ser una partición finita de A en conjuntos nulos, lo cual es absurdo.

El teorema siguiente prueba que la medida de Lebesgue es en realidad irrelevante en este asunto:

Teorema 7.72 *Si existe una medida unitaria, continua y no atómica en un conjunto S, entonces existe una medida en $\mathbb{R}$ que extiende a la medida de Lebesgue. Si κ es un cardinal infinito, esta medida será κ-aditiva si lo es la dada.*

Demostración: Sea $\mu : \mathcal{P}S \longrightarrow [0,1]$ una medida en las condiciones del enunciado. Definimos $x : 2^{<\omega} \longrightarrow \mathcal{P}S$ de modo que $x_\varnothing = S$ y si $u \in 2^{<\omega}$, entonces $\{x_{u,0}, x_{u,1}\}$ es una partición de x_u en dos conjuntos de igual medida (lo cual es posible por el teorema 7.62). Así, si $u \in {}^n2$, tenemos que $\mu(x_u) = 1/2^n$.

Consideramos ahora el espacio de Cantor $\mathcal{C} = {}^\omega 2$. Claramente, una base de $\mathcal{C}$ la forman los abiertos cerrados

$$C_n(\{s\}) = \{f \in \mathcal{C} \mid f|_n = s\},$$

para cada $n \in \omega$ y $s \in {}^n2$. Recordemos también que la medida de Haar en $\mathcal{C}$ está determinada por que $m(C_n(\{s\})) = 1/2^n$.

Para cada $u \in \mathcal{C}$, sea $x_u = \bigcap_{n<\omega} x_{u|_n}$. Es claro que $\{x_u\}_{u\in\mathcal{C}}$ es una partición de S en conjuntos nulos.

Sea $\bar{m} : \mathcal{P}\mathcal{C} \longrightarrow [0,1]$ la función dada por $\bar{m}(Z) = \mu\big(\bigcup_{u\in Z} x_u\big)$. Es inmediato comprobar que $\bar{m}$ es una medida continua unitaria κ-aditiva en $\mathcal{C}$ tal que si $s \in {}^n2$, entonces

$$\bar{m}(C_n(\{s\})) = \mu\Big(\bigcup_{u\in C_n(\{s\})} x_u\Big) = \mu(x_s) = 1/2^n.$$

Esto implica que $\bar{m}$ extiende a la medida de Haar en $\mathcal{C}$. Consideramos ahora la aplicación $\phi : \mathcal{C} \longrightarrow \mathbb{I}$ que a cada sucesión de ceros y unos le asigna el número real con dicho desarrollo binario.

Por el teorema [T 10.81], si $A \subset \mathbb{I}$ es un conjunto de Borel, la medida de Lebesgue cumple $m(A) = m[\phi^{-1}[A]] = \bar{m}[\phi^{-1}[A]]$, luego la medida en $\mathbb{I}$ dada por el teorema anterior extiende a la medida de Lebesgue (y es κ-aditiva).

Llamemos $\bar{m}_0$ a la medida en $[0,1]$ que hemos obtenido. Para cada $k \in \mathbb{Z}$, sea $\bar{m}_k : \mathcal{P}[k,k+1] \longrightarrow [0,1]$ la aplicación dada por $\bar{m}_k(X) = \bar{m}_0(X-k)$. Por el teorema anterior $\bar{m}_k$ es una medida continua unitaria κ-aditiva en $[k,k+1]$. Sea $\bar{m} : \mathcal{P}\mathbb{R} \longrightarrow [0,+\infty]$ la aplicación dada por

$$\bar{m}(X) = \sum_{k\in\mathbb{Z}} \bar{m}_k(X \cap [m,m+1]).$$

Una simple comprobación rutinaria muestra que $\bar{m}$ es una medida σ-finita, continua y κ-aditiva en $\mathbb{R}$ que extiende a la medida de Lebesgue en cada intervalo $[k,k+1]$, y de ahí se sigue fácilmente que extiende a la medida de Lebesgue en todo $\mathbb{R}$. ∎

Así pues, la existencia de una extensión de la medida de Lebesgue a $\mathcal{P}\mathbb{R}$ (o de cualquier medida de Borel continua y unitaria en cualquier espacio polaco) es equivalente a la existencia de cualquier medida unitaria, continua y no atómica en cualquier conjunto S.

Si comparamos con la larga lista de definiciones que hemos dado al principio de esta sección, veremos que el caso de una medida unitaria, continua y no atómica no se corresponde con ninguna de ellas. Pero observemos lo siguiente:

Teorema 7.73 *Si ν es el menor cardinal sobre el que existe una medida continua unitaria κ-aditiva, entonces dicha medida es ν-aditiva.*

Demostración: Sea μ la medida del enunciado. Si no fuera ν-aditiva, existen conjuntos nulos $\{X_\delta\}_{\delta<\alpha}$, con $\alpha < \nu$ cuya unión X tiene medida positiva. Cambiando X_δ por $X_\delta \setminus \bigcup_{\beta<\delta} X_\beta$ podemos suponer que los X_δ son disjuntos dos a dos.

Sea $f : X \longrightarrow \alpha$ dada por $f(x) = \delta \leftrightarrow x \in X_\delta$. Es claro que la restricción de μ a $\mathcal{P}X$ es una medida finita continua κ-aditiva en X. Por 7.71 tenemos que existe una medida unitaria κ-aditiva $\sigma : \mathcal{P}\alpha \longrightarrow [0,1]$, que claramente es continua, pues si $\delta \in \alpha$ entonces $\sigma(\{\delta\}) = \mu(f^{-1}[\{\delta\}]) = \mu(X_\delta) = 0$. Esto contradice la minimalidad de ν. ∎

Así pues, la existencia de una extensión de la medida de Lebesgue a $\mathcal{P}\mathbb{R}$ equivale a que exista un cardinal κ en el que hay definida una medida fuerte no atómica. Sin embargo, en la definición de cardinal $\mathbb{R}$-medible no hemos incluido la condición de que la medida sea no atómica. Ello se debe al teorema siguiente:

Teorema 7.74 (Ulam) *Si κ es un cardinal $\mathbb{R}$-medible, entonces se da uno de los dos casos siguientes:*

1. *Si $\kappa > 2^{\aleph_0}$, entonces κ es un cardinal medible y todas las medidas fuertes en κ son atómicas.*

2. *$\kappa \leq 2^{\aleph_0}$, entonces es débilmente inaccesible y todas las medidas fuertes en κ son no atómicas.*

DEMOSTRACIÓN: Veamos en primer lugar que todo cardinal $\mathbb{R}$-medible κ es débilmente inaccesible. Sea μ una medida fuerte en κ.

Se cumple que κ es regular, pues si κ se descompusiera en menos de κ conjuntos de cardinal menor que κ, cada uno de ellos sería nulo (pues se expresa como unión de menos de κ conjuntos puntuales, todos ellos nulos), luego κ tendría medida cero, de nuevo por la κ-aditividad.

Supongamos ahora que $\kappa = \nu^+$. Para cada $\alpha < \kappa$ sea $f_\alpha : \nu \longrightarrow \alpha$ suprayectiva y, para cada $\beta < \kappa$, $\gamma < \nu$, sea

$$A_{\beta\gamma} = \{\alpha < \kappa \mid f_\alpha(\gamma) = \beta\}.$$

Si $\beta < \kappa$, entonces para cada $\alpha \geq \beta$ existe un $\gamma < \nu$ tal que $f_\alpha(\gamma) = \beta$, luego $\alpha \in A_{\beta\gamma}$, con lo que

$$\kappa \setminus \bigcup_{\gamma<\nu} A_{\beta\gamma} \subset \beta.$$

Así, $\Big|\kappa \setminus \bigcup_{\gamma<\nu} A_{\beta\gamma}\Big| \leq \nu$, luego $\mu\Big(\kappa \setminus \bigcup_{\gamma<\nu} A_{\beta\gamma}\Big) = 0$, luego $\mu\Big(\bigcup_{\gamma<\nu} A_{\beta\gamma}\Big) > 0$.

Concluimos que para cada $\beta < \kappa$ existe un $\gamma_\beta < \nu$ tal que $\mu(A_{\beta\gamma_\beta}) > 0$. Ha de existir un conjunto $W \subset \kappa$ de cardinal κ y un $\gamma < \nu$ de modo que $\bigwedge\beta \in W\ \gamma_\beta = \gamma$. De este modo, $\{A_{\beta\gamma} \mid \beta \in W\}$ es una familia no numerable de subconjuntos de κ disjuntos dos a dos y con medida positiva, pero esto es imposible, pues el ideal de los conjuntos nulos cumple la condición de cadena numerable (teorema 7.58).

Como, por definición, κ es no numerable, concluimos que es débilmente inaccesible.

Si κ tiene una medida fuerte no atómica, la prueba del teorema 7.72 muestra que κ se descompone en $2^{\aleph_0}$ conjuntos nulos, luego la medida no puede ser $(2^{\aleph_0})^+$-aditiva. Como sí que es κ-aditiva, ha de ser $\kappa \leq 2^{\aleph_0}$.

Supongamos ahora que κ tiene una medida fuerte atómica μ. Sea $A \subset \kappa$ un átomo. Definimos $\sigma : \mathcal{P}\kappa \longrightarrow \{0, 1\}$ mediante

$$\sigma(X) = \begin{cases} 1 & \text{si } \mu(A \cap X) = \mu(A), \\ 0 & \text{si } \mu(A \cap X) = 0. \end{cases}$$

Es claro que σ es también una medida fuerte bivaluada en κ, luego κ es un cardinal medible. Si probamos que los cardinales medibles son (fuertemente) inaccesibles, en particular tendremos que $\kappa > 2^{\aleph_0}$ y el teorema quedará probado. Como el resultado tiene interés en sí mismo, lo enunciamos como un teorema aparte a continuación. ∎

Teorema 7.75 *Todo cardinal medible es inaccesible.*

DEMOSTRACIÓN: Sea κ un cardinal medible. Por el teorema anterior sabemos que es débilmente inaccesible. Sólo falta probar que es un límite fuerte. Por reducción al absurdo, supongamos que existe un cardinal $\nu < \kappa$ tal que $2^\nu \geq \kappa$.

Sea $S \subset {}^{\nu}2$ tal que $|S| = \kappa$. Sea σ una medida fuerte bivaluada en S (si hay una en κ, hay una en S). Para cada $\alpha < \nu$, sea $\epsilon_\alpha \in 2$ tal que el conjunto

$$X_\alpha = \{f \in S \mid f(\alpha) = \epsilon_\alpha\}$$

tenga medida 1. Como σ es κ-aditiva y $\nu < \kappa$, la unión de los complementarios tiene medida 0, es decir,

$$\sigma\Big(\bigcap_{\delta<\nu} X_\delta\Big) = 1.$$

Sin embargo, esta intersección contiene sólo una función, a saber, la dada por $f(\alpha) = \epsilon_\alpha$, contradicción. ∎

Ahora es inmediato el teorema siguiente:

Teorema 7.76 *Existe una extensión de la medida de Lebesgue a $\mathcal{P}\mathbb{R}$ si y sólo si existe un cardinal $\mathbb{R}$-medible $\kappa \leq 2^{\aleph_0}$.*

En particular, la hipótesis del continuo (o variantes, como $2^{\aleph_0} = \aleph_{17}$) implican que no existen tales extensiones, luego no es posible demostrar que existan.

Nota Conviene observar que sí que es posible definir medidas triviales en cualquier álgebra $\mathcal{P}X$. Por ejemplo:

1. $\mu(A) = \begin{cases} 1 & \text{si } x_0 \in A, \\ 0 & \text{si } x_0 \notin A, \end{cases}$ (para un $x_0 \in X$ prefijado),

2. $\mu(A) = \begin{cases} |A| & \text{si } A \text{ es finito}, \\ +\infty & \text{si } A \text{ es infinito}, \end{cases}$

3. $\mu(A) = \begin{cases} 0 & \text{si } A \text{ es numerable}, \\ +\infty & \text{si } A \text{ es no numerable}, \end{cases}$

Las dos últimas, cuando $X = \mathbb{R}$, son incluso invariantes por traslaciones. ∎

Puede probarse que la consistencia de que exista un cardinal $\mathbb{R}$-medible $\leq 2^{\aleph_0}$ es equivalente a la consistencia de que exista uno $> 2^{\aleph_0}$, es decir, a la consistencia de que exista un cardinal medible. Por otra parte, es fácil ver que la existencia de cardinales medibles equivale a la consistencia de que existan cardinales medibles Ulam.

En efecto, observemos en primer lugar que si κ es un cardinal medible Ulam y $\kappa \leq \mu$, entonces el teorema 7.71 aplicado a la inclusión $i : \kappa \longrightarrow \mu$ nos da una medida continua bivaluada en μ, por lo que todo cardinal mayor o igual que un cardinal medible Ulam es medible Ulam. En otras palabras, si existe un cardinal medible Ulam, entonces la clase de los cardinales se divide en dos partes: primero están todos los cardinales no medibles Ulam y por encima de ellos vienen todos los cardinales medibles Ulam.

Teorema 7.77 *Existen cardinales medibles si y sólo si existen cardinales medibles Ulam. En tal caso, el menor cardinal medible Ulam coincide con el menor cardinal medible.*

Obviamente, todo cardinal medible es medible Ulam, luego basta probar la última afirmación. Sea κ el mínimo cardinal medible Ulam y sea U una medida de Ulam en κ. Vamos a probar que es κ-completa. En caso contrario, el ideal dual de U no es κ-completo, luego existen conjuntos nulos $\{X_\alpha\}_{\alpha<\beta}$ (es decir, que no están en U) con $\beta < \kappa$, cuya unión no es nula (está en U). Quitando a cada uno la unión de los anteriores podemos suponer que son disjuntos dos a dos.

El conjunto $X_\beta = \kappa \setminus \bigcup_{\alpha<\beta} X_\alpha$ también es nulo, y así $\{X_\alpha\}_{\alpha\leq\beta}$ es una partición de κ es menos de κ conjuntos nulos. Si llamamos $\mu = |\beta| < \kappa$, reordenando los conjuntos que estamos considerando, tenemos una partición $\{X_\alpha\}_{\alpha<\mu}$, con $\mu < \kappa$, formada por conjuntos nulos. Sea $f : \kappa \longrightarrow \mu$ la función dada por $f(\alpha) = \beta \leftrightarrow \alpha \in X_\beta$.

El teorema 7.71 transforma la medida bivaluada en κ asociada a U en una medida bivaluada en μ, cuyo ultrafiltro asociado U' es libre, pues si existe un $\alpha < \mu$ tal que $\{\alpha\} \in U'$, entonces $X_\alpha = f^{-1}[\{\alpha\}] \in U$, contradicción. Por lo tanto μ es un cardinal medible Ulam, lo que contradice la minimalidad de κ.

■

Capítulo VIII

Cardinales característicos del continuo

A partir del conjunto ω de los números naturales es posible definir de forma sencilla varios conjuntos no numerables, como:

- $\mathcal{P}\omega$ (el conjunto de todos los conjuntos de números naturales),
- $[\omega]^\omega$ (el conjunto de todos los conjuntos infinitos de números naturales),
- ${}^\omega\omega$ (el conjunto de todas las sucesiones infinitas de números naturales),
- ${}^\omega 2$ (el conjunto de todas las sucesiones infinitas de ceros y unos),

y, de forma un poco más indirecta, resulta razonable añadir a esta lista el conjunto $\mathbb{R}$ de los números reales. Su construcción a partir de $\mathbb{N}$ es un poco más elaborada, pero en esencia cada número real puede determinarse mediante un elemento de cualquiera de los conjuntos anteriores fijada una codificación oportuna, y viceversa. Por ello es frecuente llamar vagamente *"reales"* a los elementos de cualquiera de los conjuntos anteriores o, más en general, de cualquier conjunto que pueda determinarse de forma sencilla y directa a partir de un subconjunto de ω u objeto equivalente.

Aunque todos estos conjuntos tienen definiciones muy simples, los axiomas de la teoría de conjuntos apenas precisan sus características, pues distan mucho de determinar qué debemos entender por "todos" los subconjuntos de ω o "todas" las sucesiones en ω, etc. Por ejemplo, es fácil probar que los cinco conjuntos que hemos mencionado tienen el mismo cardinal $2^{\aleph_0}$, pero ya hemos señalado que los axiomas de la teoría de conjuntos no determinan cuál es el valor concreto de este cardinal común. Es costumbre representarlo con la letra $\mathfrak{c}$, y lo único que podemos probar sobre él es lo que afirma el teorema de König: $\aleph_1 \leq \operatorname{cf}\mathfrak{c} \leq \mathfrak{c}$.

El *cardinal del continuo* $\mathfrak{c}$ es el más elemental de los llamados *cardinales característicos del continuo,* es decir, de cardinales definibles a partir de diversas características de los objetos "equiparables" a $\mathcal{P}\omega$ cuyo valor concreto no puede

ser determinado a partir de los axiomas de la teoría de conjuntos. En este capítulo vamos a estudiar algunos de ellos y demostraremos algunas relaciones que satisfacen. En la primera sección nos ocupamos de varios cardinales definidos en términos puramente conjuntistas, mientras que en la segunda estudiaremos otros relacionados con la topología y la teoría de la medida. Finalmente estudiaremos el llamado axioma de Martin, que es una afirmación indemostrable en (pero consistente con) los axiomas de la teoría de conjuntos que implica, entre otras cosas, que todos los cardinales que vamos a considerar son iguales a $\mathfrak{c}$.

En este capítulo usaremos el axioma de elección sin indicarlo explícitamente.

8.1 Cardinales puramente conjuntistas

8.1.1 Pseudointersecciones y torres

La estructura de $\mathcal{P}\omega$ o $[\omega]^\omega$ puede parecer muy simple, pero una forma de poner de manifiesto su complejidad consiste en considerar relaciones "módulo" conjuntos finitos. Por ejemplo:

Definición 8.1 Si A, $B \subset \omega$, diremos que A está *casi contenido* en B (y lo representaremos por $A \subset^* B$) si $A \setminus B$ es finito, es decir, si todos los elementos de A pertenecen a B salvo a lo sumo una cantidad finita de ellos.

Nota No vamos a necesitar este hecho, pero conviene observar que $A \subset^* B$ es equivalente a $[A] \leq [B]$, donde las clases de equivalencia corresponden al álgebra $\mathcal{P}\omega/\mathrm{fin}$ (donde a su vez "fin" es el ideal en $\mathcal{P}\omega$ formado por los conjuntos finitos), por lo que en el fondo vamos a estudiar algunas propiedades de esta álgebra de Boole. ∎

Si $S \subset [\omega]^\omega$, una *pseudointersección* de S es un conjunto $A \in [\omega]^\omega$ tal que $A \subset^* B$ para todo $B \in S$.

Una familia $S \subset [\omega]^\omega$ tiene la *propiedad fuerte de la intersección finita* si la intersección de cualquier conjunto finito de elementos de S es infinita.

Una *torre* es una familia $\{T_\alpha\}_{\alpha<\beta}$ de subconjuntos infinitos de ω que es casi decreciente (es decir, que si $\alpha_1 \leq \alpha_2 < \beta$ entonces $T_{\alpha_2} \subset^* T_{\alpha_1}$).

Una torre es *inextensible,* si no tiene pseudointersección, es decir, si no puede prolongarse a una torre de longitud mayor.

Notemos que en la definición de "torre" no excluimos las sucesiones constantes (o que sean constantes en un tramo arbitrariamente grande), por lo que toda torre cuya longitud sea un ordinal sucesor se puede prolongar indefinidamente sin más que repetir su último valor. Sin embargo, también es posible construir torres inextensibles:

Teorema 8.2 *Existen torres inextensibles de longitud* $\leq \mathfrak{c}$.

DEMOSTRACIÓN: En caso contrario, podríamos construir recurrentemente una sucesión $\{T_\alpha\}_{\alpha<\mathfrak{c}^+}$ en $[\omega]^\omega$ con la propiedad de que si $\alpha_1 < \alpha_2$ entonces $T_{\alpha_2} \subset^* T_{\alpha_1}$ y de modo que además $T_\alpha \setminus T_{\alpha+1}$ es infinito. En efecto, la única dificultad sería definir T_λ cuando λ es un ordinal límite, pero como, por hipótesis, la torre $\{T_\alpha\}_{\alpha<\lambda}$ no es inextensible, basta tomar como T_λ una pseudointersección. Ahora bien, la aplicación $\alpha \mapsto T_\alpha$ sería entonces inyectiva, lo cual es absurdo. En efecto, si fuera $\alpha_1 < \alpha_2$, pero $T_{\alpha_1} = T_{\alpha_2}$, entonces $T_{\alpha_1} = T_{\alpha_2} \subset^* T_{\alpha_1+1}$, luego $T_{\alpha_1} \setminus T_{\alpha_1+1}$ sería finito, contradicción. ∎

Definición 8.3 El *número de las torres* $\mathfrak{t} \leq \mathfrak{c}$ es la menor longitud de una torre inextensible. El *número de la pseudointersección* es el menor cardinal $\mathfrak{p}$ de una familia $S \subset [\omega]^\omega$ con la propiedad fuerte de la intersección finita que no admita una pseudointersección.

Es claro que $\mathfrak{t}$ es un cardinal regular, pues toda subsucesión cofinal de una torre inextensible es una torre inextensible. Como toda torre tiene la propiedad fuerte de la intersección finita, también es claro que[1] $\mathfrak{p} \leq \mathfrak{t} \leq \mathfrak{c}$.

Las definiciones de $\mathfrak{p}$ y $\mathfrak{t}$ son "negativas", pero pueden leerse "positivamente": la información que aportan estos cardinales es que toda familia con la propiedad fuerte de la intersección finita de cardinal menor que $\mathfrak{p}$ tiene una pseudointersección, y toda torre de cardinal menor que $\mathfrak{t}$ es extensible. Así, el teorema siguiente implica que $\mathfrak{p}$ es no numerable:

Teorema 8.4 *Toda familia numerable $S \subset [\omega]^\omega$ con la propiedad fuerte de la intersección finita tiene pseudointersección.*

DEMOSTRACIÓN: Sea $S = \{A_n \mid n \in \omega\}$. Tomemos $x_0 \in A_0$. Como $A_0 \cap A_1$ es infinito, podemos tomar $x_1 \in A_0 \cap A_1$ distinto de x_0. Similarmente, podemos tomar $x_2 \in A_0 \cap A_1 \cap A_2$ distinto de x_0 y x_1. De este modo construimos un conjunto infinito $X = \{x_n \mid n \in \omega\}$ que es claramente una pseudointersección de S. ∎

Ejercicio: Si $T_n = \omega \setminus n$, ¿cuál es una pseudointersección de la torre $\{T_n\}_{n\in\omega}$?

El teorema anterior y el siguiente nos dan las relaciones

$$\aleph_1 \leq \mathfrak{p} \leq \operatorname{cf} \mathfrak{t} = \mathfrak{t} \leq \operatorname{cf} \mathfrak{c} \leq \mathfrak{c}.$$

Teorema 8.5 *Si $\aleph_0 \leq \kappa < \mathfrak{t}$, entonces $2^\kappa = \mathfrak{c}$. Por lo tanto, $\mathfrak{t} \leq \operatorname{cf} \mathfrak{c}$.*

DEMOSTRACIÓN: La segunda parte se debe al teorema de König: $\operatorname{cf} \mathfrak{c} = \operatorname{cf} 2^\kappa > \kappa$, para todo $\kappa < \mathfrak{t}$, luego $\mathfrak{t} \leq \operatorname{cf} \mathfrak{c}$.

Sólo tenemos que probar que $2^\kappa \leq \mathfrak{c}$. Para ello definimos una aplicación $F : {}^{\leq\kappa}2 \longrightarrow [\omega]^\omega$ tal que si $s \subset t$ entonces $F(t) \subset^* F(s)$. Partimos de $F(\varnothing) = \omega$ y, supuesto definido $F(s)$, definimos F sobre las dos prolongaciones de s de modo que sus imágenes sean dos subconjuntos infinitos complementarios en $F(s)$. Si s tiene por longitud un ordinal límite λ definimos $F(s)$ como una pseudointersección de $\{F(s|_\delta)\}_{\delta<\lambda}$.

[1] Un resultado nada trivial sobre cardinales característicos, debido a Shelah, afirma que en realidad $\mathfrak{p} = \mathfrak{t}$.

En particular tenemos definida $F : {}^{\kappa}2 \longrightarrow [\omega]^\omega$, y es inyectiva, pues si $f, g \in {}^{\kappa}2$ son distintas, existe un mínimo $\delta < \kappa$ tal que $f(\delta) \neq g(\delta)$, luego $f|_\delta = g|_\delta$ y $F(f_{\delta+1}) \cap F(g|_{\delta+1}) = \varnothing$. Como $F(f) \subset^* F(f|_\delta)$ y $F(g) \subset^* F(g|_\delta)$, concluimos que la intersección $F(f) \cap F(g)$ es finita. ∎

En general, todos los cardinales característicos del continuo que vamos a estudiar cumplen que están situados entre $\aleph_1$ y $\mathfrak{c}$, si bien no es posible calcular su valor concreto. Obviamente, la hipótesis del continuo, $\mathfrak{c} = \aleph_1$ hace que todos sean iguales a $\mathfrak{c}$.

Por otro lado, el hecho de que sí que podamos demostrar que son no numerables aporta información relevante. Por ejemplo, en el caso del cardinal $\mathfrak{p}$, su no numerabilidad equivale al teorema 8.4, mientras que en el caso de $\mathfrak{t}$ su no numerabilidad equivale a que toda torre numerable es extensible.

8.1.2 Distributividad

El siguiente cardinal característico que vamos a estudiar indica el grado de distributividad del álgebra de Boole $\mathcal{P}\omega/\mathrm{fin}$:

Definición 8.6 Un conjunto $\mathcal{D} \subset [\omega]^\omega$ es *abierto* si cuando $A \in \mathcal{D}$ y $B \subset^* A$, entonces $B \in \mathcal{D}$. El conjunto $\mathcal{D}$ es *denso* si para todo $X \in [\omega]^\omega$ existe $D \in \mathcal{D}$ tal que $D \subset X$.

Si $A \in [\omega]^\omega$, el conjunto $\mathcal{D}_A = \{B \in [\omega]^\omega \mid B \subsetneq A \vee |B \cap A| < \aleph_0\}$ es un abierto denso y $A \notin \mathcal{D}_A$, luego $\bigcap_{A\in[\omega]^\omega} \mathcal{D}_A = \varnothing$.

El *número de distributividad* $\mathfrak{h}$ es el menor cardinal de una familia de abiertos densos en $[\omega]^\omega$ con intersección vacía. Acabamos de probar que $\mathfrak{h} \leq \mathfrak{c}$.

En realidad se cumple algo más fuerte que lo que exige la definición:

Teorema 8.7 *El número $\mathfrak{h}$ es el menor cardinal de una familia de abiertos densos en $[\omega]^\omega$ cuya intersección no es densa.*

Demostración: Sea $\mathfrak{h}'$ el cardinal descrito en el enunciado. Obviamente se cumple $\mathfrak{h}' \leq \mathfrak{h}$. Tomemos una familia $\{\mathcal{D}_\alpha\}_{\alpha<\mathfrak{h}'}$ de abiertos densos en $[\omega]^\omega$ cuya intersección no sea densa. Entonces existe un $B \in [\omega]^\omega$ tal que la intersección no contiene ningún subconjunto de B. Entonces $\mathcal{D}'_\alpha = \mathcal{D}_\alpha \cap [B]^\omega$ es abierto denso en $[B]^\omega$, pero $\bigcap_{\alpha<\mathfrak{h}'} \mathcal{D}'_\alpha = \varnothing$.

A través de una biyección entre B y ω, los $\mathcal{D}'_\alpha$ se corresponden con una familia de $\mathfrak{h}'$ abiertos densos en $[\omega]^\omega$ con intersección vacía, luego $\mathfrak{h} \leq \mathfrak{h}'$. ∎

Nota Ahora es inmediato que $\mathfrak{h}$ es el menor cardinal tal que el c.p.o. $([\omega]^\omega, \subset^*)$ no es $\mathfrak{h}$-distributivo en el sentido de la definición 7.55 y, claramente, la aplicación $i : [\omega]^\omega \longrightarrow \mathcal{P}\omega/\mathrm{fin}$ dada por $i(A) = [A]$ es una inmersión densa, por lo que el teorema 7.56 nos da que $\mathfrak{h}$ es también el menor cardinal tal que el álgebra de Boole $\mathcal{P}\omega/\mathrm{fin}$ no es $\mathfrak{h}$-distributiva. ∎

El teorema anterior implica que $\mathfrak{h}$ es regular, pues si $f : \operatorname{cf}\mathfrak{h} \longrightarrow \mathfrak{h}$ es cofinal, dada una familia $\{\mathcal{D}_\alpha\}_{\alpha<\mathfrak{h}}$ de abiertos densos en $[\omega]^\omega$ con intersección vacía, la familia $\{\mathcal{D}'_\delta\}_{\delta<\operatorname{cf}\mathfrak{h}}$ dada por $\mathcal{D}'_\delta = \bigcap_{\alpha<f(\delta)} \mathcal{D}_\alpha$ es una familia de abiertos densos con intersección vacía.

No es difícil ver que $\mathfrak{h}$ no es numerable, pero podemos probar algo más fuerte:

Teorema 8.8 *Se cumple* $\mathfrak{t} \leq \operatorname{cf}\mathfrak{h} = \mathfrak{h} \leq \mathfrak{c}$.

DEMOSTRACIÓN: Ya hemos probado que $\mathfrak{h}$ es regular. Sea $\kappa < \mathfrak{t}$ y sea $\{\mathcal{D}_\alpha\}_{\alpha<\kappa}$ una familia de abiertos densos en $[\omega]^\omega$. Definimos una torre $\{T_\alpha\}_{\alpha\leq\kappa}$ como sigue: $T_0 = \omega$, elegimos $T_{\alpha+1} \in \mathcal{D}_\alpha$ tal que $T_{\alpha+1} \subset^* T_\alpha$ (que existe porque $\mathcal{D}_\alpha$ es denso) y, si $\lambda \leq \kappa < \mathfrak{t}$, tomamos como T_λ una pseudointersección de $\{T_\alpha\}_{\alpha<\lambda}$. Así $T_\kappa \subset^* T_{\alpha+1} \in \mathcal{D}_\alpha$ para todo α y, como $\mathcal{D}_\alpha$ es abierto, de hecho $T_\kappa \in \bigcap_{\alpha<\kappa} \mathcal{D}_\alpha \neq \varnothing$, luego $\kappa < \mathfrak{h}$. ∎

8.1.3 Crecimiento de funciones

Pasamos ahora a estudiar ${}^\omega\omega$, donde podemos definir un orden parcial análogo al preorden $\subset^*$ que hemos estado considerando en $[\omega]^\omega$:

Definición 8.9 Consideramos en ${}^\omega\omega$ la relación de orden parcial $f \leq^* g$ si $f(n) \leq g(n)$ para todos los números naturales salvo a lo sumo un número finito de ellos.

Una familia $\mathcal{D} \subset {}^\omega\omega$ es *dominante* si para toda $f \in {}^\omega\omega$ existe $g \in \mathcal{D}$ tal que $f \leq^* g$.

El *número de acotación* es el menor cardinal $\mathfrak{b}$ de un subconjunto de ${}^\omega\omega$ no acotado. El *número de dominación* es el menor cardinal $\mathfrak{d}$ de un subconjunto de ${}^\omega\omega$ dominante. Obviamente una familia dominante no está acotada, luego se cumplen las desigualdades $\mathfrak{b} \leq \mathfrak{d} \leq \mathfrak{c}$.

Podemos afinar más:

Teorema 8.10 *Se cumple* $\mathfrak{h} \leq \operatorname{cf}\mathfrak{b} = \mathfrak{b} \leq \operatorname{cf}\mathfrak{d} \leq \mathfrak{d} \leq \mathfrak{c}$.

DEMOSTRACIÓN: Sea $\kappa < \mathfrak{h}$. Vamos a probar que $\kappa < \mathfrak{b}$. Para ello, consideramos una familia $\{f_\alpha\}_{\alpha<\kappa}$ de funciones en ${}^\omega\omega$ y vamos a probar que está acotada. Sea $\bar{f}_\alpha(n) = \max_{k\leq n} f_\alpha(k)$. Así $f_\alpha \leq \bar{f}_\alpha$ y $\bar{f}_\alpha$ es creciente.

Dada $f \in {}^\omega\omega$, llamamos $\mathcal{D}_f \subset [\omega]^\omega$ al conjunto de todos los $X \in [\omega]^\omega$ tales que existe $X_0 \subset^* X$ de modo que si $x \in X_0$, $y \in X$ y $x < y$, entonces $f(x) < y$.

Veamos que $\mathcal{D}_f$ es abierto denso en $[\omega]^\omega$. Si $A \in [\omega]^\omega$, definimos una sucesión $\{x_k\}_{k\in\omega}$ en A mediante

$$x_0 = \min A, \qquad x_{k+1} = \min\{a \in A \mid f(x_k) < a \wedge x_k < a\}.$$

Asi $X = \{x_k \mid k \in \omega\} \subset A$ y claramente $X \in \mathcal{D}_f$, pues si $x_k < x_l$ entonces $f(x_k) < x_{k+1} \leq x_l$. Esto prueba que $\mathcal{D}_f$ es denso. Además es abierto, pues si $X \in \mathcal{D}_f$ y $X' \subset^* X$, entonces $X' \setminus F \subset X$, para cierto conjunto finito F, y basta tomar $X'_0 = X_0 \cap X' \setminus \bigcup F$ para que X' cumpla la definición de $\mathcal{D}_f$.

Sea $\mathcal{D} = \bigcap_{\alpha<\kappa} \mathcal{D}_{\bar{f}_\alpha}$, que es un abierto denso en $[\omega]^\omega$, luego no es vacío y podemos tomar $X \in \mathcal{D}$. Sea $X = \{x_n\}_{n\in\omega}$ la única enumeración creciente de X. Como $X \in \mathcal{D}_{\bar{f}\alpha}$, existe $X_0 \subset^* X$ de modo que si $x_n \in X_0$, entonces (puesto que $n \le x_n$), se cumple $f_\alpha(n) \le \bar{f}_\alpha(x_n) < x_{n+1}$. Esto vale para todo n suficientemente grande, luego si llamamos $g(n) = x_{n+1}$, tenemos que $f_\alpha \le^* g$, luego $\{f_\alpha\}_{\alpha<\kappa}$ está acotada, luego $\kappa < \mathfrak{b}$.

Si fuera $\operatorname{cf}\mathfrak{b} < \mathfrak{b}$, podríamos descomponer una familia $\mathcal{B}$ no acotada en ${}^\omega\omega$ en unión de $\operatorname{cf}\mathfrak{b}$ familias $\mathcal{B}_\alpha$ de cardinal menor que $\mathfrak{b}$ y, por consiguiente, acotadas. Si f_α es una cota superior para $\mathcal{B}_\alpha$, la familia $\{f_\alpha \mid \alpha < \operatorname{cf}\mathfrak{b}\}$ estaría acotada, y una cota para esta familia sería una cota para $\mathcal{B}$, contradicción.

Sea $\mathcal{D}$ una familia dominante de cardinal $\mathfrak{d}$, y descompongámosla en unión de $\operatorname{cf}\mathfrak{d}$ familias $\mathcal{D}_\alpha$ de cardinal menor que $\mathfrak{d}$. Entonces, para cada $\alpha < \operatorname{cf}\mathfrak{d}$, existe una f_α que no está dominada por ninguna función de $\mathcal{D}_\alpha$. Entonces la familia $\{f_\alpha\}_{\alpha<\operatorname{cf}\mathfrak{d}}$ no está acotada, pues si existiera una cota f, podríamos tomar una cota mayor en $\mathcal{D}$, luego en un $\mathcal{D}_\alpha$, pero entonces f_α estaría dominada por una función de $\mathcal{D}_\alpha$, contradicción. Esto prueba que $\mathfrak{b} \le \operatorname{cf}\mathfrak{d}$. ∎

El teorema siguiente es elemental:

Teorema 8.11 *Existe una sucesión no acotada $\{f_\alpha\}_{\alpha<\mathfrak{b}}$ que es estrictamente creciente, es decir, tal que $\alpha < \beta \to f_\alpha <^* f_\beta$ (en el sentido de que se cumple $f_\alpha(n) < f_\beta(n)$ para todo n suficientemente grande).*

Demostración: Partimos de una familia no acotada $\{g_\alpha\}_{\alpha<\mathfrak{b}}$ y definimos recurrentemente la sucesión $\{f_\alpha\}_{\alpha<\mathfrak{b}}$: tomamos $f_0 = g_0$, supuesta definida f_α tomamos una función $f_{\alpha+1}$ que cumpla $f_\alpha <^* f_{\alpha+1}$ y $g_{\alpha+1} \le^* f_{\alpha+1}$ y, supuesta definida la sucesión $\{f_\delta\}_{\delta<\lambda}$, para $\lambda < \mathfrak{b}$, por esto mismo no puede ser no acotada, luego existe una función f_λ que acota a todos los f_δ, y podemos exigir además que $g_\lambda \le^* f_\lambda$. Claramente la sucesión $\{f_\alpha\}_{\alpha<\mathfrak{b}}$ es creciente y no puede estar acotada, pues entonces también lo estaría $\{g_\alpha\}_{\alpha<\mathfrak{b}}$. ∎

Por lo tanto, podríamos haber definido $\mathfrak{b}$ como la menor longitud de una sucesión creciente no acotada en ${}^\omega\omega$. En cambio, esto no es cierto para familias dominantes:

Definición 8.12 Una *escala* es una sucesión $\{f_\alpha\}_{\alpha<\lambda}$ estrictamente creciente y dominante.

Obviamente, si $\{f_\alpha\}_{\alpha<\lambda}$ es una escala, entonces $\mathfrak{d} \le \lambda$, y tiene una subsucesión $\{f_{\alpha_\delta}\}_{\delta<\mathfrak{d}}$ que sigue siendo una escala. En efecto, tomamos una familia dominante $\{g_\delta\}_{\delta<\mathfrak{d}}$ y definimos como sigue una sucesión estrictamente creciente de ordinales $\{\alpha_\delta\}_{\delta<\mathfrak{d}}$: si ya está definida $\{\alpha_\delta\}_{\delta<\beta}$, con $\beta < \mathfrak{d}$, no puede ocurrir que sea cofinal en λ, porque entonces la sucesión $\{f_{\alpha_\delta}\}_{\delta<\beta}$ sería dominante y tendría menos de $\mathfrak{d}$ elementos, luego existe un α_β mayor que todos los términos anteriores de la sucesión, y podemos elegirlo tal que $g_\beta \le^* f_{\alpha_\beta}$. La sucesión $\{f_{\alpha_\delta}\}_{\delta<\mathfrak{d}}$ así construida cumple lo pedido.

Por lo tanto, si hay escalas, las hay de longitud $\mathfrak{d}$. Ahora bien:

Teorema 8.13 *Existe una escala si y sólo si* $\mathfrak{b} = \mathfrak{d}$.

DEMOSTRACIÓN: Si existe una escala, acabamos de ver que existe una de longitud $\mathfrak{d}$, digamos $\{f_\alpha\}_{\alpha<\mathfrak{d}}$. Sea por otra parte $\{g_\beta\}_{\beta<\mathfrak{b}}$ una familia no acotada. Elijamos α_β tal que $g_\beta \leq^* f_{\alpha_\beta}$. Entonces la familia $\{f_{\alpha_\beta} \mid \beta < \mathfrak{b}\}$ no está acotada, pues una cota lo sería también de $\{g_\beta\}_{\beta<\mathfrak{b}}$, luego el conjunto $\{\alpha_\beta \mid \beta < \mathfrak{b}\}$ es cofinal en $\mathfrak{d}$, ya que si α fuera una cota, entonces f_α acotaría a $\{f_{\alpha_\beta} \mid \beta < \mathfrak{b}\}$, pero entonces esta familia es dominante, pues dada cualquier $h \in {}^\omega\omega$, existe $\alpha < \mathfrak{d}$ tal que $h \leq^* f_\alpha$ y existe un $\beta < \mathfrak{b}$ tal que $h \leq^* f_\alpha \leq^* f_{\alpha_\beta}$. Tenemos, pues una familia dominante de cardinal $\mathfrak{b}$, luego $\mathfrak{b} = \mathfrak{d}$.

Recíprocamente, si $\mathfrak{b} = \mathfrak{d}$ existe una familia dominante $\{g_\alpha\}_{\alpha<\mathfrak{b}}$ y definimos como sigue una sucesión $\{f_\alpha\}_{\alpha<\mathfrak{b}}$ estrictamente creciente: supuesta definida $\{f_\alpha\}_{\alpha<\beta}$, con $\beta < \mathfrak{b}$, como tiene que estar acotada, podemos tomar una cota f_β que además cumpla $g_\beta \leq^* f_\beta$. La sucesión que obtenemos es dominante, porque domina a $\{g_\alpha\}_{\alpha<\mathfrak{b}}$, luego es una escala. ∎

La igualdad $\mathfrak{b} = \mathfrak{d}$ no es demostrable en ZFC, por lo que la existencia de escalas tampoco lo es, pero se cumple, por ejemplo, bajo la hipótesis del continuo.

8.1.4 Escisión

Definición 8.14 Una *familia de escisión* $\mathcal{S} \subset \mathcal{P}\omega$ es una familia con la propiedad de que si $A \in [\omega]^\omega$, existe $I \in \mathcal{S}$ tal que $A \cap I$ y $A \setminus I$ son infinitos. Claramente $\mathcal{P}\omega$ es una familia de escisión. El *número de escisión* es el menor cardinal $\mathfrak{s}$ de una familia de escisión.

Teorema 8.15 *Se cumple que* $\mathfrak{h} \leq \operatorname{cf}\mathfrak{s} \leq \mathfrak{s} \leq \mathfrak{d}$.

DEMOSTRACIÓN: Sea $\mathcal{S}$ una familia de escisión, y descompongámosla en unión disjunta $\mathcal{S} = \bigcup_{\alpha<\operatorname{cf}\mathfrak{s}} \mathcal{S}_\alpha$, con $|\mathcal{S}_\alpha| < \mathfrak{s}$. Sea

$$\mathcal{D}_\alpha = \{A \in [\omega]^\omega \mid \bigwedge I \in \mathcal{S}_\alpha(|A \cap I| < \aleph_0 \vee |A \setminus I| < \aleph_0)\}.$$

Obviamente $\mathcal{D}_\alpha$ es abierto y $\bigcap_{\alpha<\operatorname{cf}\mathfrak{s}} \mathcal{D}_\alpha = \varnothing$, pues $\mathcal{S}$ es una familia de escisión.

Si es $\operatorname{cf}\mathfrak{s} < \mathfrak{h}$, algún $\mathcal{D}_\alpha$ no es denso, luego existe un $X \in [\omega]^\omega$ que no contiene ningún elemento de $\mathcal{D}_\alpha$, es decir, para cada $A \subset X$ infinito existe $I \in \mathcal{S}_\alpha$ tal que $A \cap I$ y $A \setminus I$ son infinitos, pero entonces, a través de una biyección entre X y ω, la familia $\mathcal{S}_\alpha$ se corresponde con una familia de escisión, lo cual es imposible, ya que $|\mathcal{S}_\alpha| < \mathfrak{s}$. Esto prueba que $\mathfrak{h} \leq \operatorname{cf}\mathfrak{s}$.

Sea $\mathcal{D} \subset {}^\omega\omega$ una familia dominante de cardinal $\mathfrak{d}$. Es claro que para toda función $f \in {}^\omega\omega$ existe otra g estrictamente creciente tal que $f < g$, por lo que, cambiando cada función de $\mathcal{D}$ por otra en estas condiciones, podemos suponer que todas las funciones de $\mathcal{D}$ son estrictamente crecientes y que, para cada $f \in {}^\omega\omega$, existe $g \in \mathcal{D}$ tal que, para todo n suficientemente grande, se cumple de hecho $f(n) < g(n)$.

Para cada $A \in [\omega]^\omega$ llamamos $f_A : \omega \longrightarrow \omega$ a la única función estrictamente creciente que enumera A. Si $f \in {}^\omega\omega$, representamos por f^n a la composición de f consigo misma n veces. Si f es estrictamente creciente, llamamos

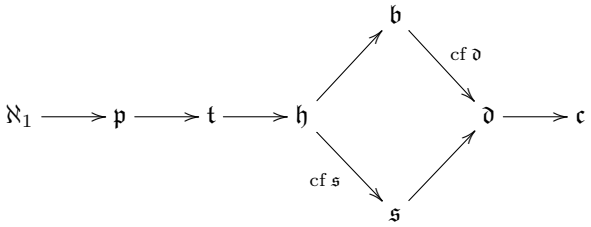
$$A_f = \bigcup_{n\in\omega} \big[f^{2n}(0), f^{2n+1}(0)\big[\,.$$

Notemos que la sucesión $\{f^n(0)\}_{n\in\omega}$ es estrictamente creciente, por lo que A_f es infinito. Basta probar que $S = \{A_f \mid f \in \mathcal{D}\}$ es una familia de escisión. Para ello tomamos $A \in [\omega]^\omega$ y a su vez tomamos $f \in \mathcal{D}$ tal que $f_A \leq^* f$. Basta ver que $A \cap A_f$ y $A \setminus A_f$ son infinitos. Fijamos $m \in \omega$ tal que, para todo $n \geq m$, se cumpla $f_A(n) < f(n)$. Como f_A es estrictamente creciente, se cumple que $n \leq f_A(n)$, y también es claro que $f^n(0) \geq n \geq m$, luego

$$f^n(0) \leq f_A(f^n(0)) < f(f^n(0)) = f^{n+1}(0).$$

Por lo tanto, $f_A(f^n(0)) \in A \cap A_f$ si n es par y $f_A(f^n(0)) \in A \setminus A_f$ si n es impar. ∎

Aquí se rompe la cadena de desigualdades que hasta ahora habíamos obtenido. En total hemos probado lo siguiente:



Ya hemos señalado que Shelah ha probado que $\mathfrak{p} = \mathfrak{t}$ y, por otra parte, Mildenberger ha probado que $\mathfrak{s} \leq \operatorname{cf}\mathfrak{d}$, pero si la teoría de conjuntos es consistente, también lo es suponer que $\mathfrak{b} < \mathfrak{s}$, que $\mathfrak{b} > \mathfrak{s}$, o que $\mathfrak{b} = \mathfrak{s}$.

8.1.5 Familias casi disjuntas

Definición 8.16 Si W es un conjunto numerable, una familia $\mathcal{C} \subset \mathcal{P}W$ es *casi disjunta* si todos sus elementos son infinitos, pero la intersección de dos cualesquiera de ellos es finita.

Notemos que cada familia casi disjunta en $\mathcal{P}\omega$ determina una anticadena en el álgebra $\mathcal{P}\omega/\mathrm{fin}$ del mismo cardinal. Obviamente, toda familia de subconjuntos disjuntos de ω tiene que ser numerable, pero si sólo pedimos que sea casi disjunta, la situación cambia:

Teorema 8.17 *Existe una familia casi disjunta en $\mathcal{P}\omega$ de cardinal $\mathfrak{c}$.*

Demostración: Basta probar que existe un conjunto numerable en el que hay una familia casi disjunta de cardinal $\mathfrak{c}$, no es necesario que sea ω. Tomamos

concretamente $2^{<\omega}$. Para cada $f \in {}^{\omega}2$, definimos $A_f = \{f|_n \mid n \in \omega\} \in \mathcal{P}2^{<\omega}$. Es claro que si $f \neq g$, entonces $A_f \cap A_g$ es finito, por lo que $\{A_f\}_{f\in{}^{\omega}2}$ es una familia casi disjunta en $\mathcal{P}\,{}^{\omega}2$ de cardinal $\mathfrak{c}$. ∎

El lema de Zorn implica que toda familia casi disjunta en $\mathcal{P}\omega$ puede extenderse a una familia casi disjunta maximal (respecto de la inclusión). Puesto que el cardinal de un subconjunto de $\mathcal{P}\omega$ no puede exceder a $\mathfrak{c}$, el teorema anterior prueba que existen familias casi disjuntas maximales de cardinal $\mathfrak{c}$, pero eso no impide que pueda haberlas de cardinal menor.

Definición 8.18 El *número de casi disjunción* es el menor cardinal $\mathfrak{a}$ de una familia casi disjunta maximal en $\mathcal{P}\omega$.

Obviamente $\mathfrak{a} \leq \mathfrak{c}$, pero lo interesante es que $\mathfrak{a}$ es no numerable, es decir, que una familia casi disjunta numerable nunca es maximal. En realidad podemos afirmar más:

Teorema 8.19 *Se cumple* $\mathfrak{b} \leq \mathfrak{a}$.

Demostración: Sea $\mathcal{A}$ una familia casi disjunta maximal de cardinal $\mathfrak{a}$. Entonces $\omega \setminus \bigcup\mathcal{A}$ es finito, o de lo contrario la familia no sería maximal. Añadiendo este resto finito a alguno de los elementos de $\mathcal{A}$, podemos suponer que $\bigcup\mathcal{A} = \omega$. Entonces podemos seleccionar una cantidad numerable $\{C_n\}_{n\in\omega}$ de elementos de $\mathcal{A}$ que cubran ω.

Cambiando C_n por $C_n \setminus \bigcup_{m<n} C_m$ estamos quitando a cada C_n un número finito de elementos, con lo que la familia completa sigue siendo casi disjunta maximal y podemos suponer que los C_n son disjuntos dos a dos (y su unión sigue siendo ω). Consideramos biyecciones $f_n : \omega \longrightarrow C_n$, que nos dan una biyección $f : \omega \times \omega \longrightarrow \omega$ dada por $f(n,k) = f_n(k)$.

A través de f, la familia $\mathcal{A}$ se transforma en una familia casi disjunta maximal en $\omega \times \omega$ de cardinal $\mathfrak{a}$ que contiene a los conjuntos $C_n = \{n\} \times \omega$. Sea $\mathcal{A}'$ el resto de la familia, que también tendrá cardinal $\mathfrak{a}$.

Cada $A \in \mathcal{A}'$ contiene un número finito de pares en C_n, luego podemos definir $f_A(n)$ como el mínimo k tal que $A \cap C_n \subset \{n\} \times k$. Tenemos así una función $f_A \in {}^{\omega}\omega$. Vamos a probar que $\{f_A\}_{A\in\mathcal{A}'}$ no está acotada en ${}^{\omega}\omega$, lo que probará que $\mathfrak{b} \leq \mathfrak{a}$.

Supongamos, por reducción al absurdo, que existe $g \in {}^{\omega}\omega$ tal que $f_A \leq^* g$, para todo $A \in \mathcal{A}'$. Entonces, considerando a g como conjunto $g \subset \omega \times \omega$, tendríamos que $g \cap A = \varnothing$, para todo $A \in \mathcal{A}'$, mientras que $|g \cap C_n| = 1$, luego $\mathcal{A} \cup \{g\}$ sería una familia casi disjunta que contradiría la maximalidad de $\mathcal{A}$. ∎

8.2 Medida y categoría

En esta sección usaremos el axioma de elección. Vamos a estudiar ahora algunas de las principales características conjuntistas de la medida de Lebesgue y sus análogas para la categoría topológica. Para ello introducimos los conceptos siguientes:

Definición 8.20 Sea I un ideal $\aleph_1$-completo en un conjunto X que contenga a los puntos. Definimos:

- La *aditividad* de I como el menor cardinal $\mathrm{ad}(I)$ de un subconjunto de I cuya unión no está en I.
- El *cubrimiento* de I como el menor cardinal $\mathrm{cub}(I)$ de un subconjunto de I cuya unión es X.
- La *uniformidad* de I como el menor cardinal $\mathrm{un}(I)$ de un subconjunto de X que no esté en I.
- La *cofinalidad* de I como el menor cardinal $\mathrm{cf}(I)$ de una base de I, es decir, de un conjunto $B \subset I$ tal que todo elemento de I esté contenido en uno de B.

Nos interesarán principalmente los casos en los que X es un espacio polaco e I es el ideal I_m de los conjuntos nulos respecto de una medida de Borel continua en X o bien el ideal I_c de los conjuntos de primera categoría (suponiendo entonces que X es perfecto, para que los puntos estén en el ideal).

Notemos que los ocho cardinales responden a otras tantas preguntas naturales sobre medida y categoría, a saber:

- *¿Cuántos conjuntos nulos / de primera categoría podemos unir sin dejar de tener un conjunto nulo / de primera categoría?* (Sabemos que como mínimo $\aleph_0$, pero, ¿pueden ser más?)
- *¿Cuántos conjuntos nulos / de primera categoría son necesarios para cubrir X?* (Obviamente bastan $\mathfrak{c}$, pero, ¿pueden ser menos?)
- ¿Cuál es el menor cardinal de un conjunto no nulo / de segunda categoría? (Tiene que ser no numerable, pero ¿tiene que ser aún mayor?)

  Notemos que el cardinal de todo conjunto medible no nulo es necesariamente $\mathfrak{c}$, por lo que la pregunta para el caso de la medida equivale a:

  ¿cuál es el menor cardinal de un conjunto no medible?
- *¿Cuántos conjuntos son necesarios para obtener con sus subconjuntos todos los conjuntos nulos / de primera categoría?* (Sirven $\mathfrak{c}$ conjuntos, pero ¿es posible usar menos?)

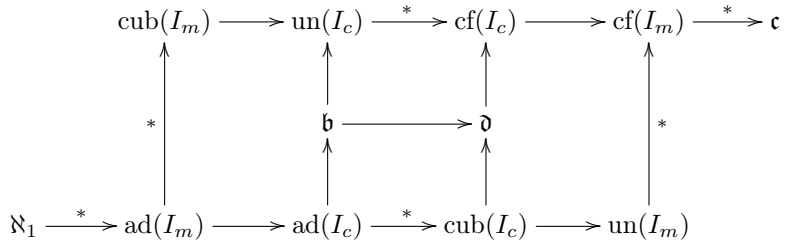
Sucede que los ocho cardinales que así obtenemos son independientes del espacio polaco considerado y, en el caso de I_m, de la medida considerada.

En efecto, al final del apartado sobre el álgebra de medida en la sección 7.7 hemos señalado que si X es cualquier espacio polaco y μ es cualquier medida de Borel σ-finita y continua en X, existe una biyección $f : X \longrightarrow [0,1]$ que hace corresponder el ideal I_m de μ con el de la medida de Lebesgue, de donde se sigue inmediatamente que los cuatro cardinales asociados a I_m son los mismos para ambas medidas.

Por otra parte, el teorema [T 6.22] afirma que todo espacio polaco perfecto no vacío X contiene un subespacio N denso y G_δ homeomorfo al espacio de Baire $\mathcal{N} = {}^\omega\omega$, y el teorema [T 1.66] afirma que un subconjunto $A \subset N$ es de primera categoría en N si y sólo si lo es en X. Más aún, como $X \setminus N$ es un F_σ de interior vacío, es unión de cerrados de interior vacío, luego es de primera categoría. Usando estos hechos, es fácil ver que los cuatro cardinales asociados a I_c son los mismos para X y para $\mathcal{N}$, luego son los mismos en todos los espacios polacos perfectos (no vacíos).

Por consiguiente, para estudiar estos cardinales podemos trabajar indistintamente en cualquier espacio polaco perfecto con cualquier medida de Borel.

Sucede que las únicas desigualdades que pueden probarse sobre estos cardinales son las contenidas en el llamado *diagrama de Cichoń:*



en el que cada flecha $A \to B$ representa la desigualdad $A \leq B$.

La desigualdad $\mathfrak{b} \leq \mathfrak{d}$ está probada en 8.10, y las marcadas con un asterisco son triviales, ya que, en general, para todo ideal $\aleph_1$-completo I que contenga a los puntos, se cumple:

- $\aleph_1 \leq \mathrm{ad}(I)$.

  Esto es inmediato por la $\aleph_1$-completitud de I.

- $\mathrm{ad}(I) \leq \mathrm{cub}(I)$.

  Una familia de elementos de I cuya unión sea X es en particular una familia de elementos de I cuya unión no está en I.

- $\mathrm{un}(I) \leq \mathrm{cf}(I)$.

  Si B es una base de I de cardinal mínimo y A resulta de elegir un punto en el complementario de cada elemento de B, entonces $|A| \leq |B|$ y $A \notin I$.

- $\mathrm{ad}(I) \leq \mathrm{un}(I)$.

  Si A es un conjunto que no está en I, sus puntos forman una familia de elementos de I cuya unión no está en I.

- $\mathrm{cub}(I) \leq \mathrm{cf}(I)$.

  Una base de I en particular es una familia de elementos de I cuya unión es X.

Por último, $\mathrm{cf}(I_m) \leq \mathfrak{c}$, pues una base de I_m la forman los conjuntos nulos que son G_δ, y es fácil ver que un espacio polaco tiene $\mathfrak{c}$ conjuntos G_δ.

Definición 8.21 Llamaremos $\mathcal{K}$ al conjunto de todos los subconjuntos de $\mathcal{N}$ contenidos en una unión numerable de compactos. Claramente es un ideal $\aleph_1$-completo en $\mathcal{N}$ que contiene a los puntos.

Observemos que $\mathcal{K} \subset I_c$, porque los compactos en $\mathcal{N}$ tienen interior vacío, luego son de primera categoría, luego las uniones numerables de compactos también.

Más detalladamente, si K es un compacto en $\mathcal{N}$, su proyección n-sima tiene que ser finita, luego tiene que estar acotada por un cierto $f(n) \in \omega$, luego $K \subset C_f$, donde

$$C_f = \{g \in \mathcal{N} \mid \bigwedge n \in \omega\ g(n) \leq f(n)\}.$$

Más aún, todo $K \in \mathcal{K}$ está contenido en una unión $\bigcup_{n\in\omega} C_{f_n}$ y, usando que $\mathfrak{b} \geq \aleph_1$, existe un $f \in \mathcal{N}$ tal que $\bigwedge n \in \omega\ f_n \leq^* f$, luego

$$K \subset C_f^* = \{g \in \mathcal{N} \mid g \leq^* f\}.$$

Recíprocamente, $C_f^* \in \mathcal{K}$, pues $C_f^* = \bigcup_{m,n\in\omega} C_{f_{n,m}}$, donde

$$f_{n,m}(i) = \begin{cases} n & \text{si } i \leq m, \\ f(i) & \text{si } i > m. \end{cases}$$

Con esto es fácil probar:

Teorema 8.22 $\mathrm{ad}(\mathcal{K}) = \mathrm{un}(\mathcal{K}) = \mathfrak{b}$, $\quad \mathrm{cub}(\mathcal{K}) = \mathrm{cf}(\mathcal{K}) = \mathfrak{d}$.

Demostración: Las observaciones precedentes nos dan que si $K \subset \mathcal{N}$ no está acotado respecto de $\leq^*$, entonces $K \notin \mathcal{K}$, luego $\mathrm{un}(\mathcal{K}) \leq \mathfrak{b}$. Por otro lado, si $A \subset \mathcal{K}$ cumple que $\bigcup A \notin \mathcal{K}$, para cada $K \in A$ podemos tomar un $f_K \in \mathcal{N}$ tal que $A \subset C_{f_K}^*$, con lo que $\bigcup_{K\in A} C_{f_K}^* \notin \mathcal{K}$, pero entonces $\{f_K \mid K \in A\}$ no está acotado en $\mathcal{N}$, luego $\mathfrak{b} \leq |A|$, luego $\mathfrak{b} \leq \mathrm{ad}(\mathcal{K})$. Ya hemos visto que, en general, $\mathrm{ad}(\mathcal{K}) \leq \mathrm{un}(\mathcal{K})$, luego $\mathrm{ad}(\mathcal{K}) = \mathrm{un}(\mathcal{K}) = \mathfrak{b}$.

Por otra parte, si $A \subset \mathcal{N}$ es una familia dominante, es claro que el conjunto $\{C_f^* \mid f \in A\}$ es una base de $\mathcal{K}$, luego $\mathrm{cf}(\mathcal{K}) \leq \mathfrak{d}$. Si $A \subset \mathcal{K}$ cumple que $\bigcup A = \mathcal{N}$, como antes obtenemos funciones f_K tales que $\bigcup_{K\in A} C_{f_K}^* = \mathcal{N}$, y esto significa que $\{f_K \mid K \in A\}$ es dominante en $\mathcal{N}$, luego $\mathfrak{d} \leq \mathrm{cub}(\mathcal{K})$. De nuevo, la desigualdad $\mathrm{cub}(\mathcal{K}) \leq \mathrm{cf}(\mathcal{K})$ es trivial, y así $\mathrm{cub}(\mathcal{K}) = \mathrm{cf}(\mathcal{K}) = \mathfrak{d}$. ∎

De la inclusión $\mathcal{K} \subset I_c$ se siguen trivialmente dos desigualdades del diagrama de Cichoń:

Teorema 8.23 $\mathfrak{b} \leq \mathrm{un}(I_c)$ *y* $\mathrm{cub}(I_c) \leq \mathfrak{d}$.

Para cada $f \in \mathcal{N}$, definimos $f'(n) = \max f[n+1]$ y sea $\phi : \mathcal{N} \longrightarrow \mathcal{K}$ la función dada por $\phi(f) = C_{f'}^*$.

Supongamos ahora que $F = \bigcup_{n\in\omega} F_n$ es una unión de cerrados de interior vacío. Vamos a construir un $f_F \in \mathcal{N}$ tal que si $f \in \mathcal{N}$ cumple $\phi(f) \subset F$, entonces $f \leq^* f_F$.

Para ello definimos recurrentemente $\{k_n\}_{n\in\omega}$ en ω y $\{s_n\}_{n\in\omega}$ en $\omega^{<\omega}$.

Tomamos $k_0 = 0$. Supuesto definido k_n, elegimos $s_n \in \omega^{<\omega}$ de modo que para todo $t \in k_n^{\leq k_n}$ y todo $i \leq n$ se cumpla que $B_{t^\frown s_n} \cap F_i = \varnothing$.

Existe tal s_n porque cualquier t se puede prolongar hasta que el abierto básico $B_{t^\frown s}$ esté contenido en $\mathcal{N} \setminus F_i$, porque, como este conjunto es denso, corta a B_t en un punto x y, al ser abierto, existe un entorno de x de la forma $B_{t^\frown s}$ que está contenido en él.

Por último definimos $k_{n+1} = k_n + \ell(s_n) + \text{máx}\{s_n(i) \mid i < \ell(s_n)\} + 1$. A su vez, definimos

$$f_F(n) = \text{máx}\{s_n(i) \mid i < \ell(s_n)\}.$$

Tomemos ahora $f \in \mathcal{N}$ tal que $\phi(f) \subset F$ y veamos que, en efecto, $f \leq^* f_F$. En caso contrario existe $X \subset \omega$ infinito tal que $\bigwedge n \in X\ f_F(n) \leq f(n)$. Vamos a construir un $x \in \phi(f) \setminus F$ y tendremos una contradicción.

Sea $\{x_n\}_{n\in\omega}$ la enumeración creciente de X. Definimos x como la sucesión

$$\overbrace{0,\ldots,0}^{k_{x_0}}, s_{x_0}, \overbrace{0,\ldots\ldots\ldots,0}^{k_{x_1}-k_{x_0}-\ell(s_{x_0})}, s_{x_1}, 0, 0, \ldots$$

de modo que cada segmento s_{x_n} empieza exactamente en la posición k_{x_n}. La definición de la sucesión $\{k_n\}_{n\in\omega}$ garantiza que cada s_{x_n} termina siempre antes de la posición $k_{x_{n+1}}$.

De este modo $x \in B_{x|_{k_{x_n}}{}^\frown s_{x_n}}$, y, como $x|_{k_{x_n}}$ sólo toma (aparte del 0) los valores que toman los s_{x_i} con $i < n$, de nuevo la definición de la sucesión $\{k_n\}_{n\in\omega}$ garantiza que $x|_{k_{x_n}} \in k_{x_n}^{\leq k_{x_n}}$, luego, por construcción, $x \notin F_j$, para todo $j \leq x_n$ y, como esto vale para todo n, concluimos que $x \notin F$.

Para probar que $x \in \phi(f) = C^*_{f'}$ hemos de ver que $x \leq^* f'$. Ahora bien, para todo $i \in \omega$, o bien $x(i) = 0$, o bien $x(i) = s_{x_j}(l)$, para cierto j con $k_{x_j} \leq i$. En este caso $x(i) \leq f_F(x_j) \leq f(x_j) \leq f'(i)$, donde la última desigualdad se debe a que $x_j \leq k_{x_j} \leq i$.

De aquí deducimos:

Teorema 8.24 $\text{ad}(I_c) \leq \mathfrak{b}$ *y* $\mathfrak{d} \leq \text{cf}(I_c)$.

Demostración: Por 8.22 podemos tomar una familia $\{K_\alpha\}_{\alpha<\mathfrak{b}}$ de elementos de $\mathcal{K}$ cuya unión no está en $\mathcal{K}$. Para cada α podemos tomar $f_\alpha \in \mathcal{N}$ tal que $K_\alpha \subset C^*_{f_\alpha}$. Vamos a probar que $\bigcup_{\alpha<\mathfrak{b}} C^*_{\phi(f_\alpha)} \notin I_c$, lo cual implica que $\text{ad}(I_c) \leq \mathfrak{b}$.

En caso contrario existiría una unión F de cerrados de interior vacío tal que $\bigcup_{\alpha<\mathfrak{b}} C^*_{\phi(f_\alpha)} \subset F$ y, por el argumento previo al teorema, $f_\alpha \leq^* f_F$, pero entonces

$$\bigcup_{\alpha<\mathfrak{b}} K_\alpha \subset C^*_{f_F} \in \mathcal{K},$$

contradicción.

Sea $\kappa = \mathrm{cf}(I_c)$ y tomemos una base $\{F_\alpha\}_{\alpha<\kappa}$ de I_c. Podemos suponer que cada F_α es unión numerable de cerrados de interior vacío con lo que podemos considerar el conjunto $D = \{f_{F_\alpha} \mid \alpha < \kappa\}$. Entonces, para cada $f \in \mathcal{N}$, existe un α tal que $\phi(f) \subset F_\alpha$, luego, según hemos demostrado, $f \leq^* f_{F_\alpha}$, y esto prueba que D es dominante, luego $\mathfrak{d} \leq \kappa$. ∎

Falta probar las cuatro desigualdades que relacionan I_m con I_c. Dos de ellas son sencillas:

Teorema 8.25 $\mathrm{cub}(I_m) \leq \mathrm{un}(I_c)$ *y* $\mathrm{cub}(I_c) \leq \mathrm{un}(I_m)$.

Demostración: Por simplicidad trabajamos en el espacio de Cantor $\mathcal{C}$ con su medida de Haar unitaria. Según [T 6.46] podemos descomponer $\mathcal{C} = A \cup B$ en unión disjunta con $A \in I_m$ y $B \in I_c$.

Si $Z \subset \mathcal{C} \setminus I_c$, se cumple que $Z + A = \mathcal{C}$. En efecto, si existe $z \in \mathcal{C} \setminus (Z + A)$, entonces $(z+Z)\cap A = \varnothing$, pues si $a = z+x$, entonces $x = z = x+a$, contradicción. Por lo tanto, $z + Z \subset B$, luego $z + Z \in I_c$, luego $Z \in I_c$, porque la traslación $x \mapsto z + x$ es un homeomorfismo.

Podemos exigir $|Z| = \mathrm{un}(I_c)$ y, como los trasladados $x + A$ son nulos, la descomposición $\mathcal{C} = \bigcup_{x\in X} (x + A)$ prueba que $\mathrm{cub}(I_m) \leq |Z| = \mathrm{un}(I_c)$.

La segunda desigualdad se prueba análogamente. ∎

Las dos desigualdades que quedan por probar son las más complicadas, y necesitamos varios resultados previos:

Definición 8.26 Si $(X, \leq)$ es un conjunto parcialmente ordenado sin elementos maximales, definimos

$$\mathfrak{b}(X, \leq) = \mathrm{mín}\{|A| \mid A \subset X \wedge A \text{ no está acotado superiormente}\},$$

$$\mathfrak{d}(X, \leq) = \mathrm{mín}\{|A| \mid A \text{ es dominante}\},$$

donde "dominante" significa que todo elemento de X está por debajo de un elemento de A.

En estos términos es claro que $\mathfrak{b} = \mathfrak{b}(\mathcal{N}, \leq^*)$ y $\mathfrak{d} = \mathfrak{d}(\mathcal{N}, \leq^*)$, así como que

$$\mathrm{ad}(I) = \mathfrak{b}(I, \subset), \qquad \mathrm{cf}(I) = \mathfrak{d}(I, \subset).$$

También es claro que si A es dominante en X, entonces $\mathfrak{b}(X, \leq) = \mathfrak{b}(A, \leq)$ y $\mathfrak{d}(X, \leq) = \mathfrak{d}(A, \leq)$.

Si $(X, \leq)$, $(Y, \leq)$ son dos conjuntos parcialmente ordenados sin maximales, una *conexión de Tukey* entre ellos es un par (ϕ, ϕ^*) de aplicaciones $\phi : X \longrightarrow Y$, $\phi^* : Y \longrightarrow X$ con la propiedad de que

$$\bigwedge x \in X \bigwedge y \in Y (\phi(x) \leq y \to x \leq \phi^*(y)).$$

Escribiremos $(X, \leq) \preceq (Y, \leq)$ para indicar que existe una conexión de Tukey de $(X, \leq)$ en $(Y, \leq)$. El interés de estos conceptos radica en el teorema siguiente:

Teorema 8.27 *Si* $(X,\leq) \preceq (Y,\leq)$*, entonces se cumple* $\mathfrak{b}(Y,\leq) \leq \mathfrak{b}(X,\leq)$ *y* $\mathfrak{d}(X,\leq) \leq \mathfrak{d}(Y,\leq)$.

DEMOSTRACIÓN: Sea (ϕ,ϕ^*) una conexión de Tukey. Si $A \subset X$ cumple $|A| < \mathfrak{b}(Y,\leq)$, definimos $B = \phi[A]$, con lo que $|B| \leq |A|$, luego B está acotado en Y, es decir, existe $y \in Y$ tal que $\phi(x) \leq y$ para todo $x \in A$, luego $x \leq \phi^*(y)$, luego A está acotado en X. Esto prueba que $\mathfrak{b}(Y,\leq) \leq \mathfrak{b}(X,\leq)$.

Similarmente, si $B \subset Y$ es dominante en Y, entonces $A = \phi^*[B]$ es dominante en X, pues, dado $x \in X$, existe un $y \in B$ tal que $\phi(x) \leq y$, con lo que $x \leq \phi^*(y) \in B$. Por lo tanto $\mathfrak{d}(X,\leq) \leq |A| \leq |B|$, y podemos tomar $|B| = \mathfrak{d}(Y,\leq)$, tenemos la segunda desigualdad. ∎

Así pues, para demostrar las desigualdades $\mathrm{ad}(I_m) \leq \mathrm{ad}(I_c)$, $\mathrm{cf}(I_c) \leq \mathrm{cf}(I_m)$ basta probar que $(I_c,\subset) \preceq (I_m,\subset)$.

Teorema 8.28 *Si* X *es un espacio topológico* 2AN*, para cada* $n > 0$ *existe un conjunto numerable* $\mathcal{V}$ *de abiertos tal que*

1. *Si* $G \subset X$ *es un abierto denso, existe* $V \in \mathcal{V}$ *tal que* $V \subset G$.
2. *Si* $V_0,\ldots,V_n \in \mathcal{V}$*, entonces* $\bigcap_{i\leq n} V_i \neq \varnothing$.

DEMOSTRACIÓN: Sea $\{U_n\}_{n\in\omega}$ una base numerable de X que no contenga a $\varnothing$ y que podemos suponer cerrada para uniones finitas. Definimos

$$A_m = \{k \in \omega \mid k > m \wedge \textstyle\bigwedge Y \subset m+1 (\bigcap_{i\in Y} U_i \neq \varnothing \to U_k \cap \bigcap_{i\in Y} U_i \neq \varnothing)\},$$

$$\mathcal{V} = \{\textstyle\bigcup_{i\leq n} U_{s(i)} \mid s \in {}^{n+1}\omega \wedge \bigwedge i < n\ s(i+1) \in A_{s(i)}\}.$$

Veamos que $\mathcal{V}$ cumple lo requerido. Ciertamente es una familia (numerable) de abiertos básicos. Sea G un abierto denso en X.

Para cada $m \in \omega$ existe un $k \in A_m$ tal que $U_k \subset G$. En efecto, consideramos todos los conjuntos $Y \subset m+1$ tales que $\bigcap_{i\in Y} U_i \neq \varnothing$, que son un conjunto finito de abiertos no vacíos. Para cada uno de ellos tomamos un abierto básico contenido en $G \cap \bigcap_{i\in Y} U_i$ y formamos la unión de todos ellos, que será un U_k. Añadiendo más abiertos contenidos en G podemos obtener infinitos abiertos U_k que cumplen lo mismo, luego podemos elegir un $k > m$, así, $k \in A_m$.

Fijemos ahora un k_0 tal que $U_{k_0} \in G$ y definamos recurrentemente $k_{i+1} \in A_{k_i}$ tal que $U_{k_{i+1}} \subset G$. Entonces $\bigcup_{i\leq n} U_{k_i} \in \mathcal{V}$ y está contenido en G, luego se cumple la primera propiedad.

Tomemos $V_0,\ldots,V_n \in \mathcal{V}$, de modo que $V_i = \bigcup_{j\leq n} U_{k_{ij}}$, con $k_{i,j+1} \in A_{k_{ij}}$. Podemos reordenar los abiertos V_i de manera que $k_{00} = \min\{k_{i0} \mid i \leq n\}$, y luego reordenamos $V_1,\ldots,V_n$ de manera que se cumpla $k_{1,1} = \min\{k_{i,1} \mid 1 \leq i \leq n\}$, y así sucesivamente, hasta conseguir que $k_{ii} \leq k_{ji}$, para $i \leq j \leq n$. De este

modo $k_{ii} \leq k_{i+1,i} < k_{i+1,i+1}$, luego $k_{i+1,i+1} \in A_{k_{i+1,i}} \subset A_{k_{ii}}$. Por inducción obtenemos que $\bigcap_{i\leq n} U_{k_{ii}} \neq \varnothing$, y como $U_{k_{ii}} \subset V_i$, concluimos que $\bigcap_{i\leq n} V_i \neq \varnothing$. ∎

En general, dada una medida unitaria$(X, \mathcal{A}, \mu)$, una familia $G \subset \mathcal{A}$ es *independiente respecto de la medida* si todos sus elementos cumplen $0 < \mu(A) < 1$ y, para todos los $A_0, \ldots, A_n \in G$, se verifica la igualdad

$$\mu\Big(\bigcap_{i\leq n} A_i\Big) = \prod_{i\leq n} \mu(A_i).$$

Observemos que si G es una familia independiente y reemplazamos algunos de sus elementos por sus complementarios, la familia resultante es también independiente. En efecto, se cumple que

$$\mu\Big(\bigcap_{i\leq n} A_i\Big) = \mu\Big(\bigcap_{i\leq n+1} A_i\Big) + \mu\Big(\bigcap_{i\leq n} A_i \cap (X \setminus A_{n+1})\Big),$$

luego

$$\prod_{i\leq n} \mu(A_i) = \prod_{i\leq n+1} \mu(A_i) + \mu\Big(\bigcap_{i\leq n} A_i \cap (X \setminus A_{n+1})\Big),$$

luego

$$\mu\Big(\bigcap_{i\leq n} A_i \cap (X \setminus A_{n+1})\Big) = \prod_{i\leq n} \mu(A_i)\ \mu(X \setminus A_{n+1}),$$

luego la familia que resulta de cambiar A_{n+1} por su complementario es independiente, y repitiendo el razonamiento podemos realizar cualquier número finito de sustituciones, pero es claro que una familia es independiente si y sólo si lo son todas sus subfamilias finitas, por lo que la conclusión vale también si realizamos infinitas sustituciones.

Es fácil construir familias independientes en $\mathcal{C}$ respecto de la medida de Cantor. Concretamente, si $\{s_n\}_{n\in\omega}$ es una familia de funciones $d_n \longrightarrow 2$, con $d_n \subset \omega$, donde $\{d_n\}_{n\in\omega}$ es una sucesión de subconjuntos finitos de ω disjuntos dos a dos, los abiertos básicos B_{d_n} son independientes, pues

$$\mu\Big(\bigcap_{i\leq m} B_{s_{n_i}}\Big) = \mu(B_{\cup s_{n_i}}) = 2^{|\cup d_{n_i}|} = 2^{\sum_{i\leq m} |d_{n_i}|} = \prod_{i\leq m} 2^{|d_{n_i}|} = \prod_{i\leq m} \mu(B_{s_{n_i}}).$$

Específicamente, vamos a fijar una familia independiente $\{G_{nm}\}_{n,m\in\omega}$ de abiertos cerrados en $\mathcal{C}$ tal que $m(G_{nm}) = 2^{-n}$ (para lo cual sólo hay que elegir adecuadamente una familia $\{d_{nm}\}_{n,m\in\omega}$ de subconjuntos finitos de ω disjuntos dos a dos con $|d_{nm}| = n$). Por otra parte, fijemos una base numerable $\{U_n\}_{n\in\omega}$ de $\mathcal{C}$.

Para cada $A \in I_m$ elegimos un compacto $K_A \subset \mathcal{C}$ tal que $A \cap K_A = \varnothing$ y $m(K_A) > 0$. Más aún, podemos exigir además que si $U_n \cap K_A \neq \varnothing$, entonces $m(U_n \cap K_A) > 0$. En efecto, en caso contrario cambiamos K_A por

$$K_A \setminus \bigcup\{U_n \mid m(U_n \cap K_A) = 0\}.$$

Para cada par de funciones $f, g : \omega \longrightarrow \mathcal{P}\omega$, escribiremos $f \subset^* g$ para representar que $\bigvee k \in \omega \bigwedge n \geq k\ f(n) \subset g(n)$.

Similarmente, si $h \in \mathcal{N}$, usaremos la notación $h \in^* f$ para representar que $\bigvee k \in \omega \bigwedge n \geq k\ h(n) \in f(n)$.

Llamemos $L = \{h \in ([\omega]^{<\omega})^\omega \mid \bigwedge n \in \omega\ |h(n)| \leq 2^n\}$.

Teorema 8.29 *Existen funciones $\phi_1 : \mathcal{N} \longrightarrow I_m$ y $\phi_1^* : I_m \longrightarrow L$ tales que, para todo $x \in \mathcal{N}$ y todo $A \in I_m$, se cumple*

$$\phi_1(x) \subset A \to x \in^* \phi_1^*(A).$$

Demostración: Para cada $A \in I_m$ y $k, n \in \omega$, definimos

$$F(A,k,n) = \{m \in \omega \mid U_k \cap K_A \neq \varnothing \wedge U_k \cap K_A \cap G_{nm} = \varnothing\}.$$

Si $U_k \cap K_A \neq \varnothing$, como

$$0 < m(U_k \cap K_A) \leq m\Big(\bigcap_{m \in F(A,k,n)} (\mathcal{C} \setminus G_{nm})\Big)$$

y los conjuntos $\mathcal{C} \setminus G_{nm}$ son independientes, el conjunto $F(A,k,n)$ tiene que ser finito. Además

$$U_k \cap K_A \cap \bigcup\{G_{nm} \mid n \in \omega \wedge m \in F(A,k,n)\} = \varnothing,$$

luego

$$\begin{aligned} m(U_k \cap K_A) &\leq m\Big(\bigcap\{\mathcal{C} \setminus G_{nm} \mid n \in \omega \wedge m \in F(A,k,n)\}\Big) \\ &= \lim_N \prod_{n \leq N} (1 - 2^{-n})^{|F(A,k,n)|}. \end{aligned}$$

Si llamamos $L > 0$ al límite, tomando logaritmos vemos que

$$-\sum_{n \in \omega} |F(A,k,n)| \log(1 - 2^{-n}) = -\log L$$

y, usando que[2] $x \leq -\log(1-x)$, concluimos que la serie $\sum_{n \in \omega} |F(A,k,n)| 2^{-n}$ es convergente, luego su término general tiende a 0.

Sea $N(A,k)$ el menor natural tal que, para todo $n \geq N(A,k)$ se cumple que $|F(A,k,n)|2^{-n} \leq 2^{-k-1}$. Hasta aquí hemos supuesto que $U_k \cap K_A \neq \varnothing$, pero en caso contrario $F(A,k,n) = \varnothing$ y se cumple la última propiedad con $N(A,k) = 0$.

Ahora ya podemos definir $\phi_1^*(A) = h$, donde

$$h(n) = \bigcup\{F(A,k,n) \mid k \in \omega \wedge n \geq N(A,k)\}.$$

Como $|h(n)| \leq \sum_{k \in \omega} 2^n \cdot 2^{-k-1} = 2^n$, se cumple que $h \in L$.

[2]Por ejemplo, basta ver que la derivada de $x + \log(1-x)$ tiene el mismo signo que x, por lo que la función tiene su máximo en 0.

Por otra parte, si $x \in \mathcal{N}$, definimos

$$\phi_1(x) = \bigcap_{k\in\omega} \bigcup_{n\geq k} G_{n,x(n)}.$$

Como, para todo k, se cumple que

$$m(\phi_1(x)) \leq m\Big(\bigcup_{n\geq k} G_{n,x(n)}\Big) \leq 2^{-k-1},$$

concluimos que $\phi_1(x) \in I_m$.

Veamos que estas funciones cumplen lo requerido. Si $\phi_1(x) \subset A$, entonces $\bigcap_{k\in\omega} \bigcup_{n\geq k} G_{n,x(n)} \cap K_A = \varnothing$. Aplicamos el teorema de Baire a K_A (que es un espacio polaco), el cual nos da que existe un k_0 tal que $\bigcup_{n\geq k_0} G_{n,x(n)} \cap K_A$ no es denso en K_A (si todos lo fueran tendríamos una intersección numerable de abiertos densos que, en lugar de densa, sería vacía). Por lo tanto, existirá un k_1 tal que $U_{k_1} \cap K_A \neq \varnothing$, pero

$$\bigcup_{n\geq k_0} G_{n,x(n)} \cap K_A \cap U_{k_1} = \varnothing.$$

Así para todo $n \geq k_0$, $n \geq N(A, k_1)$, se cumple $K_A \cup U_{k_1} \cap G_{n,x(n)} = \varnothing$, luego $x(n) \in F(A, k_1, n) \subset h(n)$. Esto significa que $x \in^* \phi_1^*(A)$. ∎

Teorema 8.30 *Existen funciones $\phi_2 : I_c \longrightarrow \mathcal{N}$, $\phi_2^* : L \longrightarrow I_c$ tales que, para todo $B \in I_c$ y todo $h \in L$, se cumple*

$$\phi_2(B) \in^* h \to B \subset \phi_2^*(h).$$

Demostración: Por el teorema 8.28 podemos tomar familias $\{V_{n,k}\}_{k\in\omega}$ de subconjuntos abiertos de U_n tales que todo abierto denso contiene un $V_{n,k}$ y si $X \in [\omega]^{\leq 2^n}$ entonces $\bigcap_{k\in X} V_{n,k} \neq \varnothing$.

Si $B \in I_c$ existe una sucesión $\{H_n\}_{n\in\omega}$ de cerrados de interior vacío tales que $B \subset \bigcup_{n\in\omega} H_n$. Podemos suponer que $H_n \subset H_{n+1}$ para todo n. Definimos $\phi_2(B) = x$, donde $x(n)$ es el menor natural tal que $H_n \cap V_{n,x(n)} = \varnothing$ (existe, porque $\mathcal{C} \setminus H_n$ es abierto denso). Para cada $h \in L$, definimos

$$\phi_2^*(h) = \mathcal{C} \setminus \bigcap_{n\in\omega} \bigcup_{m\geq n} \bigcap_{k\in h(m)} V_{m,k}.$$

Como $\bigcap_{k\in h(m)} V_{m,k} \subset U_m$ es un abierto no vacío, la unión para $m \geq n$ es un abierto denso, luego $\phi_2^*(h) \in I_c$.

Supongamos ahora que $x = \phi_2(B) \in^* h$. Entonces existe un n_0 tal que, para $n \geq n_0$, se cumple que $x(n) \in h(n)$. Por lo tanto,

$$\bigcup_{m\geq n} \bigcap_{k\in h(m)} V_{m,k} \subset \bigcup_{m\geq n} V_{m,x(m)},$$

y el conjunto de la derecha no corta a H_n, luego $B \subset \bigcup_{n\geq n_0} H_n \subset \phi_2^*(h)$. ∎

Los dos teoremas anteriores nos dan aplicaciones $\phi = \phi_2 \circ \phi_1 : I_c \longrightarrow I_m$ y $\phi^* = \phi_1^* \circ \phi_2^* : I_m \longrightarrow I_c$ que claramente constituyen una conexión de Tukey $(I_c, \subset) \preceq (I_m, \subset)$, pues si tomaos $B \in I_c$, $A \in I_m$ tales que $\phi_1(\phi_2(B)) \subset A$, entonces $\phi_2(B) \in^* \phi_1^*(A)$, luego $B \subset \phi_2^*(\phi_1^*(A))$. Por consiguiente:

Teorema 8.31 $\mathrm{ad}(I_m) \leq \mathrm{ad}(I_c)$ *y* $\mathrm{cf}(I_c) \leq \mathrm{cf}(I_m)$.

Con esto tenemos probadas todas las desigualdades del diagrama de Cichoń. Seguidamente probamos un teorema que nos permitirá demostrar algo ligeramente más fuerte.

Consideramos de nuevo en $\mathcal{C}$ la suma definida componente a componente, con la que tiene estructura de grupo. Sea D el subgrupo denso numerable formado por las sucesiones finalmente nulas. Sea $\{V_n\}_{n\in\omega}$ una base numerable de entornos abiertos de 0, que podemos tomar decreciente y sea $D = \{r_n\}_{n\in\omega}$ una enumeración de D. Para cada $x \in \mathcal{N}$, $n \in \omega$ y $z \in \mathcal{C}$, definimos

$$D_x^n = \bigcup_{m\geq n} (r_m + V_{x(m)}), \qquad W_{x,z} = \bigcup_{m\in\omega} (\mathcal{C} \setminus (z + D_x^m)).$$

Entonces cada D_x^n es abierto denso, al igual que $z + D_x^m$, luego $W_{x,z} \in I_c$.

Teorema 8.32 *Si $H \subset \mathcal{C}$ es unión numerable de cerrados de interior vacío y $z \notin H + D$, existe un $y \in \mathcal{N}$ tal que, para todo $x \in \mathcal{N}$, se cumple*

$$y \leq^* x \to H \subset W_{x,z}.$$

Demostración: Sea $H = \bigcup_{n\in\omega} H_n$, donde cada H_n es cerrado de interior vacío, y podemos suponer que la unión es creciente. Como $z + r_n \notin H$, existe $y(n) \in \omega$ tal que $(z + r_n + V_{y(n)}) \cap H_n = \varnothing$. Supongamos ahora que $y \leq^* x$ y supongamos que existe $h \in H \setminus W_{x,z}$. Entonces existe un n_0 tal que, para todo $n \geq n_0$, se cumple $y(n) \leq x(n)$ y $h \in H_n$. Por lo tanto $h \notin z + r_n + V_{y(n)}$.

Por otra parte, $h + z \in D_x^{n_0}$. Esto significa que existe un $n \geq n_0$ tal que $h + z \in r_n + V_{x(n)} \subset r_n + V_{y(n)}$, contradicción. ∎

Teorema 8.33 $\mathrm{ad}(I_c) = \min\{\mathrm{cub}(I_c), \mathfrak{b}\}$ *y* $\mathrm{cf}(I_c) = \max\{\mathrm{un}(I_c), \mathfrak{d}\}$.

Demostración: Ya sabemos que $\mathrm{ad}(I_c) \leq \min\{\mathrm{cub}(I_c), \mathfrak{b}\}$. Tomemos ahora $A \subset I_c$ tal que $|A| < \mathrm{cub}(I_c)$ y $|A| < \mathfrak{b}$, y tenemos que probar que $\bigcup A \in I_c$. No perdemos generalidad si suponemos que cada elemento de A es unión numerable de cerrados de interior vacío. Podemos tomar

$$z \in \mathcal{C} \setminus \bigcup_{H\in A} (H + D),$$

porque los conjuntos de la derecha están en I_c y no pueden cubrir $\mathcal{C}$ (notemos que $H + D = \bigcup_{n\in\omega} (H + r_n)$).

Por el teorema anterior, para cada $H \in A$ existe $y_H \in \mathcal{N}$ tal que, para todo $x \in \mathcal{N}$ se cumple $x \leq^* y_H \to H \subset W_{x,z}$. La condición $|A| < \mathfrak{b}$ implica que existe un $y \in \mathcal{N}$ tal que $y_H \leq^* y$ para todo H, luego $\bigcup A \subset W_{x,z} \in I_c$.

Similarmente, sabemos que $\mathrm{cf}(I_c) \geq \mathrm{máx}\{\mathrm{un}(I_c), \mathfrak{d}\}$, y tomamos $A \notin I_c$ tal que $|A| = \mathrm{un}(I_c)$ y una familia dominante $F \subset \mathcal{N}$ tal que $|F| = \mathfrak{d}$. Si $H \subset \mathcal{C}$ es una unión numerable de cerrados de interior vacío, entonces $A \not\subset H + D$, luego existe un $z \in A \setminus (H + D)$. Por el teorema anterior existe un $x \in F$ tal que $H \subset W_{x,z}$. Esto prueba que la familia $\{W_{x,z} \mid x \in F \wedge z \in A\}$ es una base de I_c, luego $\mathrm{cf}(I_c) \leq \mathrm{máx}\{\mathrm{un}(I_c), \mathfrak{d}\}$. ∎

El diagrama de Cichoń incluye únicamente dos de los cardinales característicos que hemos estudiado en la sección anterior. Podemos probar algunas desigualdades que involucran a otros más:

Teorema 8.34 $\mathfrak{t} \leq \mathrm{ad}(I_c)$.

Para probarlo demostramos primero:

Teorema 8.35 *Si $\{D_\alpha\}_{\alpha<\kappa}$ es una sucesión casi decreciente de subconjuntos densos de $\mathbb{Q}$ y $\kappa < \mathfrak{t}$, entonces existe D denso en $\mathbb{Q}$ tal que $D \subset^* D_\alpha$ para todo $\alpha < \kappa$.*

Demostración: Sea $\{r_n\}_{n\in\omega}$ una enumeración de $\mathbb{Q}$. Sea $\mathcal{I}$ el conjunto de los intervalos abiertos en $\mathbb{R}$ con extremos racionales. Para cada $I \in \mathcal{I}$, la sucesión $\{I \cap D_\alpha\}_{\alpha<\kappa}$ es casi decreciente (y todos sus términos son infinitos) pero al ser $\kappa < \mathfrak{t}$ no puede ser una torre en $\mathcal{P}\mathbb{Q}$, luego existe un conjunto infinito $P_I \subset \mathbb{Q} \cap I$ tal que $P_I \subset^* I \cap D_\alpha$ para todo $\alpha < \kappa$. Llamemos $x_\alpha(I)$ al mínimo natural n tal que

$$\bigwedge m \geq n(r_m \in P_I \to r_m \in I \cap D_\alpha).$$

Como $\mathcal{I}$ es numerable y $\kappa < \mathfrak{t} \leq \mathfrak{b}$, la sucesión $\{x_\alpha\}_{\alpha<\kappa}$ está acotada, es decir, existe $y : \mathcal{I} \longrightarrow \omega$ tal que $x_\alpha <^* y$ para todo $\alpha < \kappa$, en el sentido de que $x_\alpha(I) < y(I)$ para todo I salvo un número finito de casos. Definimos

$$D = \{r_n \mid \bigvee I \in \mathcal{I}(r_n \in P_I \wedge n > y(I))\}.$$

Claramente cumple lo requerido: dados dos números racionales, consideramos el intervalo I que forman, y basta tomar un $r_n \in P_I$ con $n > y(I)$, $n > x_\alpha(I)$ para que se cumpla $r_n \in D \cap I$, luego D es denso en $\mathbb{Q}$.

Por otra parte, dado $\alpha < \kappa$, existe un número finito de intervalos $I_0, \ldots, I_k$ de modo que, para cualquier otro I, se cumple que $x_\alpha(I) < y(I)$. Si $r_n \in D$ con

$$n > \mathrm{máx}\{x_\alpha(I_0), \ldots, x_\alpha(I_k)\},$$

entonces existe un I tal que $r_n \in P_I$, $n > y(I)$. Entonces $n > x_\alpha(I)$, luego $r_n \in D_\alpha$, y esto prueba que $D \subset^* D_\alpha$. ∎

Demostración (de 8.34): Sea $\kappa < \mathfrak{t}$. Tenemos que probar que la unión de κ conjuntos de I_c (en $\mathbb{R}$) está en I_c. Podemos sustituir cada uno de ellos por

una unión numerable de cerrados de interior vacío, y a su vez podemos sustituir la familia de conjuntos dada por la de dichos cerrados de interior vacío (que tienen el mismo cardinal). Equivalentemente, basta probar que la intersección de una familia $\{G_\alpha\}_{\alpha<\kappa}$ de abiertos densos en $\mathbb{R}$ es densa.

Para ello construimos una sucesión casi decreciente $\{D_\alpha\}_{\alpha\leq\kappa}$ de abiertos densos en $\mathbb{Q}$. Partimos de $D_0 = \mathbb{Q}$, definimos $D_{\alpha+1} = D_\alpha \cap G_\alpha$ y en los límites aplicamos el teorema anterior. Observemos que los conjuntos $D_\kappa \setminus G_\alpha$ son finitos, pues $D_\kappa \setminus G_\alpha \subset D_\kappa \setminus D_{\alpha+1}$.

Definimos funciones $x_\alpha : D_\kappa \longrightarrow \omega$ de modo que $x_\alpha(r)$ es el mínimo natural $n > 0$ tal que $]r - 1/n, r + 1/n[\subset G_\alpha$ si $r \in G_\alpha$, y $x_\alpha(r) = 0$ en caso contrario. Como $\kappa < \mathfrak{b}$, existe $y : D_\kappa \longrightarrow \omega$ tal que $x_\alpha <^* y$ para todo $\alpha < \kappa$. Podemos suponer que y no toma el valor 0. Si $s \subset D_\kappa$ es finito, entonces

$$U_s = \bigcup_{r\in D_\kappa\setminus s}]r - 1/y(r), r + 1/y(r)[$$

es abierto denso en $\mathbb{R}$ y por el teorema de Baire $U = \bigcap_{s\in[D_\kappa]^{<\omega}} U_s$ también es denso en $\mathbb{R}$.

Si $\alpha < \kappa$, entonces $s = (D_\kappa \setminus G_\alpha) \cup \{r \in D_\kappa \mid y(r) < x_\alpha(r)\}$ es finito y claramente $U \subset U_s \subset G_\alpha$. Por lo tanto $U \subset \bigcap_{\alpha<\kappa} G_\alpha$, que es, por lo tanto, denso. ∎

Por otra parte:

Teorema 8.36 $\mathfrak{s} \leq \mathrm{un}(I_m), \quad \mathfrak{s} \leq \mathrm{un}(I_c)$.

Demostración: Si $x \in \mathcal{C} = {}^\omega 2$, llamamos $Z(x) = \{n \in \omega \mid x(n) = 0\}$. Para cada $A \in [\omega]^\omega$, definimos

$$S(A) = \{x \in \mathcal{C} \mid |A \cap Z(x)| < \aleph_0 \vee |A \setminus Z(x)| < \aleph_0\}.$$

Si $s \subset A$ es finito, definimos

$$N(A, s) = \{x \in \mathcal{C} \mid Z(x) \cap A = s\}.$$

Se cumple que $N(A, s)$ es un cerrado de interior vacío y medida 0. En efecto, si $x \in \mathcal{C} \setminus N(A, s)$, existe un $n \in A$ tal que $n \in s$ pero $x(n) \neq 0$, o bien $n \in A \setminus s$ y $x(n) = 0$, pero entonces $x \in \{y \in \mathcal{C} \mid y(n) = x(n)\} \subset \mathcal{C} \setminus N(A, s)$, luego $\mathcal{C} \setminus N(A, s)$ es abierto.

Si $x \in N(A, s)$, no existe ningún $n \in \omega$ tal que $\{y \in \mathcal{C} \mid y|_n = x|_n\} \subset N(A, s)$, pues siempre podemos tomar un $n \in A \setminus s$, $n > m$, y entonces tomando $y \in \mathcal{C}$ igual a x salvo por que $y(n) = 1$, tenemos que $y \in \{y \in \mathcal{C} \mid y|_n = x|_n\}$, pero $y \notin N(A, s)$. Esto prueba que $N(A, s)$ tiene interior vacío.

Por último, si $x \in N(A, s)$ y $s \subset t \subset A$, con t finito, tenemos que

$$N(A, s) \subset \{y \in \mathcal{C} \mid y|_t = x|_t\},$$

que es un abierto de medida $2^{-|t|}$, y así vemos que la medida de $N(A, s)$ es menor que 2^{-m}, para todo $m \geq |s|$, luego es nula. Por consiguiente,

$$S(A) = \bigcup\{N(A, s) \mid s \in [A]^{<\omega}\} \cup \bigcup\{N(\omega \setminus A, s) \mid s \in [\omega \setminus A]^{<\omega}\}$$

es nulo y de primera categoría.

Si $D \subset \mathcal{C}$ es un conjunto de segunda categoría de cardinal $\mathrm{un}(I_c)$, no puede suceder que $D \subset S(A)$, para ningún $A \in [\omega]^\omega$, luego, para todo $A \in [\omega]^\omega$, existe un $d \in D \setminus S(A)$, luego $A \cap Z(d)$ y $A \setminus Z(d)$ son infinitos, lo cual significa que $\{Z(d) \mid d \in D\}$ es una familia de escisión, luego $\mathfrak{s} \leq |D| = \mathrm{un}(I_c)$. La otra desigualdad se prueba análogamente. ∎

Terminamos esta sección con una propiedad adicional de $\mathrm{ad}(I_m)$ y $\mathrm{ad}(I_c)$. Conviene introducir el concepto siguiente:

Definición 8.37 Sea $(X, \mathbb{B}, \mu)$ un espacio medida, es decir, que $\mathbb{B}$ es una σ-álgebra de subconjuntos de X y $\mu : \mathbb{B} \longrightarrow [0, +\infty]$ es una medida en $\mathbb{B}$. Si κ es un cardinal infinito, diremos que la medida es κ-aditiva si cuando $\{U_\alpha\}_{\alpha<\beta}$, con $\beta < \kappa$, es una familia de elementos de $\mathbb{B}$, se cumple que $\bigcup_{\alpha<\beta} U_\alpha \in \mathbb{B}$ (con lo que $\mathbb{B}$ es un álgebra κ-completa) y, si los conjuntos son disjuntos dos a dos, entonces

$$\mu\Big(\bigcup_{\alpha<\beta} U_\alpha\Big) = \sum_{\alpha<\beta} \mu(U_\alpha).$$

La suma hay que entenderla como el supremo de las sumas finitas, entendiendo que vale ∞ si alguno de los sumandos es ∞ (aquí es importante que todos los sumandos son ≥ 0). Cuando sólo hay una cantidad numerable de sumandos no nulos, el supremo de las sumas finitas coincide con la suma de la serie en el sentido usual. Es claro que toda medida es $\aleph_1$-aditiva. El teorema siguiente prueba que esta definición generaliza a 7.70.

Teorema 8.38 *Si $(X, \mathbb{B}, \mu)$ es un espacio medida de modo que μ sea σ-finita y sea κ es un cardinal infinito, entonces μ es κ-aditiva si y sólo si $\kappa \leq \mathrm{ad}(I_\mu)$, es decir, si y sólo si la unión de menos de κ conjuntos nulos es nula.*

Demostración: Supongamos que μ es κ-aditiva y sea $\{A_\alpha\}_{\alpha<\beta}$, con $\beta < \kappa$ una familia de conjuntos nulos en X. Sea

$$B_\alpha = A_\alpha \setminus \bigcup_{\delta<\alpha} A_\delta.$$

Por la κ-aditividad, la unión es medible, luego B_α también lo es, luego es nulo. Además los conjuntos B_α son disjuntos dos a dos y su unión coincide con la de los A_α. Por la κ-aditividad la unión es nula.

Supongamos ahora que la unión de menos de κ conjuntos nulos es nula y sea $\{A_\alpha\}_{\alpha<\beta}$, con $\beta < \kappa$, una familia de conjuntos medibles tal que su unión no sea medible. Podemos suponer que β es el menor cardinal para el que esto sucede. Así, si definimos los conjuntos B_α igual que antes, tenemos que todos ellos son medibles, por la minimalidad de β, y disjuntos dos a dos, pero su unión no es medible.

Estamos suponiendo que μ es σ-finita, por lo que $X = \bigcup_{n<\omega} Y_n$, donde los conjuntos Y_n son medibles de medida finita. Sea $B_\alpha^n = B_\alpha \cap Y_n$. Así,

$$\sum_{\alpha<\beta} \mu(B_\alpha^n) \leq \mu(Y_n) < +\infty.$$

Ahora bien, si una suma de una cantidad no numerable de números reales no negativos es finita, todos sus sumandos salvo a lo sumo una cantidad numerable han de ser nulos, pues en caso contrario habría una cantidad no numerable de sumandos mayores o iguales que $1/n$ para cierto natural n, y entonces las sumas parciales finitas no estarían acotadas.

Así pues, en $\{B_\alpha\}_{\alpha<\beta}$ hay una cantidad numerable de términos con medida positiva, cuya unión es medible porque $\mathbb{B}$ es una σ-álgebra, y el resto son conjuntos nulos, cuya unión es medible por hipótesis, luego la unión total es medible, contradicción.

Con esto tenemos probado que la unión de menos de κ conjuntos medibles es medible. Supongamos ahora que $\{B_\alpha\}_{\alpha<\beta}$ son medibles y disjuntos dos a dos. Definimos B^n_α como antes, de modo que entre ellos (para un n fijo) hay una cantidad numerable de conjuntos no nulos y el resto son nulos. Descomponemos la unión de todos en la unión de los nulos, que por hipótesis es nula, y la unión de los restantes, cuya medida es la suma de las medidas. Concluimos obviamente que la medida de toda la unión es la suma de las medidas. ∎

En particular, si μ es una medida de Borel continua en un espacio polaco, entonces $\mathrm{ad}(I_m)$ es el mayor cardinal κ tal que μ es κ-aditiva. Para la categoría tenemos el teorema siguiente:

Teorema 8.39 *Si X es un espacio polaco perfecto, la σ-álgebra* $\mathrm{Ba}(X)$ *es* $\mathrm{ad}(I_c)$*-completa.*

Demostración: Sea ξ el mayor cardinal tal que $\mathrm{Ba}(X)$ es ξ-completa. Esto significa que existe una familia $\{B_\alpha\}_{\alpha<\xi}$ en $\mathrm{Ba}(X)$ cuya unión no está en $\mathrm{Ba}(X)$, pero no existe ninguna familia similar de longitud menor que ξ. En particular esto hace que los conjuntos $B'_\alpha = B_\alpha \setminus \bigcup_{\delta<\alpha} B_\delta$ estén en $\mathrm{Ba}(X)$ y tengan la misma unión. Equivalentemente, podemos suponer que los B_α son disjuntos dos a dos.

Como I_c cumple la c.c.n. (por 7.65), existe un conjunto numerable $T \subset \xi$ tal que $B_\alpha \in I_c$ para todo $\alpha \in \xi \setminus T$. Entonces $\bigcup_{\alpha\in T} B_\alpha \in \mathrm{Ba}(X)$ (porque $\mathrm{Ba}(X)$ es una σ-álgebra), y si fuera $\xi < \mathrm{ad}(I_c)$ también $\bigcup_{\alpha\in\xi\setminus T} B_\alpha \in \mathrm{Ba}(X)$, con lo que toda la unión estaría en $\mathrm{Ba}(X)$, contradicción. Así pues, $\mathrm{ad}(I_c) \le \xi$, lo que implica que $\mathrm{Ba}(X)$ es $\mathrm{ad}(I_c)$-completa. ∎

8.3 El axioma de Martin

El axioma de Martin es una afirmación técnica que tiene muchísimas implicaciones en la teoría de conjuntos, en la topología y también en otras áreas de la matemática. Su interés reside en que puede probarse que si la teoría de conjuntos es consistente, lo sigue siendo al añadir el axioma de Martin como axioma adicional. Esto hace que todas las consecuencias del axioma de Martin sean también consistentes, lo que permite obtener numerosas pruebas de consistencia sin necesidad de estar familiarizado con las técnicas de lógica y teoría

de modelos que éstas requieren (sin más que aceptar la consistencia del axioma de Martin). En esta sección supondremos el axioma de elección.

Recordemos algunas definiciones que hemos dado en la sección 7.4:

- Un conjunto preordenado (c.p.o.) es un conjunto $\mathbb{P}$ en el que hay definido un preorden (una relación reflexiva y transitiva). En este contexto, los elementos de $\mathbb{P}$ suelen llamarse *condiciones.*
- Dos condiciones de un c.p.o. $\mathbb{P}$ son incompatibles (y lo representamos con la notación $p \perp q$) si no existe un $r \in \mathbb{P}$ tal que $r \le p$, $r \le q$.
- Un conjunto $A \subset \mathbb{P}$ es una anticadena si sus elementos son incompatibles dos a dos.
- Un c.p.o. $\mathbb{P}$ cumple la *condición de cadena numerable* (c.c.n.) si todas sus anticadenas son numerables.
- Un filtro $G \subset \mathbb{P}$ en un c.p.o. $\mathbb{P}$ es un conjunto que cumple las propiedades siguientes:
  1. $G \neq \varnothing$,
  2. $\bigwedge p \in G \bigwedge q \in \mathbb{P}(p \le q \to q \in G)$,
  3. $\bigwedge pq \in G \bigvee r \in G(r \le p \wedge r \le q)$.
- Un conjunto $D \subset \mathbb{P}$ en un c.p.o. es denso si para todo $p \in \mathbb{P}$ existe $d \in D$ tal que $d \le p$.

Definición 8.40 Si κ es un cardinal infinito, llamaremos *axioma de Martin* para κ a la afirmación siguiente:

> **AM($\boldsymbol{\kappa}$)** *Si $\mathbb{P}$ es un c.p.o. que cumple la condición de cadena numerable y $\mathcal{D}$ es una familia de conjuntos densos en $\mathbb{P}$ tal que $|\mathcal{D}| \le \kappa$, entonces existe un filtro G en $\mathbb{P}$ tal que $G \cap D \neq \varnothing$, para todo $D \in \mathcal{D}$.*

El *axioma de Martin* (AM) es la afirmación $\bigwedge \kappa < \mathfrak{c}\ \mathrm{AM}(\kappa)$.

Como ya habíamos advertido, se trata de un enunciado bastante técnico, así que vamos a tratar de asimilar su contenido.

Teorema 8.41 *Se cumple:*

1. *Si $\kappa \le \mu$ son cardinales infinitos, entonces* AM(μ) *implica* AM(κ).
2. *Se cumple* AM($\aleph_0$) *incluso eliminando la restricción de que $\mathbb{P}$ cumpla la condición de cadena numerable.*
3. *Sin la restricción sobre la condición de cadena numerable,* AM($\aleph_1$) *sería falso (luego también* AM(κ) *para todo κ no numerable).*
4. AM($\mathfrak{c}$) *es falso (luego también* AM(κ) *para todo $\kappa \ge \mathfrak{c}$).*

Demostración: 1) es inmediato.

2) Sea $\mathbb{P}$ cualquier c.p.o., sin necesidad de que cumpla la c.c.n., y sea $\{D_n\}_{n=0}^{\infty}$ una familia numerable de subconjuntos densos de $\mathbb{P}$. Dado cualquier $p_0 \in \mathbb{P}$, tomamos $d_0 \in D_0$ tal que $d_0 \leq p_0$, y a su vez $d_1 \in D_1$ tal que $d_1 \leq d_0$, y así construimos una sucesión decreciente

$$\ldots \leq d_4 \leq d_3 \leq d_2 \leq d_1 \leq d_0 \leq p_0$$

tal que $d_n \in D_n$. Basta tomar $G = \{p \in \mathbb{P} \mid \bigvee n \in \omega\ d_n \leq p\}$. Es inmediato comprobar que se trata de un filtro en $\mathbb{P}$ tal que $d_n \in D_n \cap G$.

3) Sea $\mathbb{P} = \omega_1^{<\omega}$, con el orden dado por $p \leq q$ si y sólo si $q \subset p$. Notemos que no cumple la c.c.n., pues si llamamos $p_\alpha = \{(0, \alpha)\}$, entonces $A = \{p_\alpha \mid \alpha < \omega_1\}$ es una anticadena no numerable en $\mathbb{P}$. En efecto, si $\alpha < \beta < \omega_1$, no puede existir ningún $p \in \mathbb{P}$ tal que $p \leq p_\alpha$ y $p \leq p_\beta$, pues esto significaría que $\alpha = p(0) = \beta$.

Por otra parte, el conjunto D_n formado por las condiciones de longitud mayor o igual que $n < \omega$ es denso en $\mathbb{P}$, pues toda condición se puede prolongar hasta que su dominio sea mayor o igual que n.

Igualmente el conjunto E_α es el conjunto de las condiciones que toman el valor $\alpha < \omega_1$ es denso en $\mathbb{P}$, pues toda condición en ω_1 se puede prolongar a una que tome el valor α.

Si se cumpliera $\mathrm{MA}(\aleph_1)$ sin el requisito de la c.c.n., existiría un filtro $G \subset \mathbb{P}$ tal que $G \cap D_n \neq \varnothing$, para todo $n < \omega$ y $G \cap E_\alpha \neq \varnothing$, para todo $\alpha \in \omega_1$.

Si p, $q \in G$, existe un $r \in G$ tal que $r \leq p$ y $r \leq q$, lo cual significa que r es una sucesión que extiende a p y a q, lo cual sólo es posible si $p \subset q$ o $q \subset p$.

Que $G \cap D_n \neq \varnothing$ significa que G contiene condiciones de todas las longitudes y, como cada una extiende a las de longitud menor, sólo puede haber una de cada longitud, y $f_G = \bigcup G : \omega \longrightarrow \omega_1$.

Pero el hecho de que $G \cap D_\alpha \neq \varnothing$ significa que en G hay condiciones que toman cualquier valor $\alpha < \omega_1$, lo que significa que $f_G : \omega \longrightarrow \omega_1$ suprayectiva, lo cual es absurdo.

4) Sea ahora $\mathbb{P} = 2^{<\omega}$, el conjunto de las sucesiones finitas de ceros y unos, también con el orden dado por $p \leq q$ si y sólo si $q \subset p$. Como $\mathbb{P}$ es numerable, cumple trivialmente la condición de cadena numerable.

Como antes, los conjuntos D_n de las condiciones de longitud mayor o igual que n son claramente densos en $\mathbb{P}$. Además, si $f \in {}^{\omega}2$, el conjunto de las condiciones $p \in \mathbb{P}$ tales que existe $n \in \omega$ en el que están definidas de modo que $p(n) \neq f(n)$ es denso en $\mathbb{P}$, pues toda condición se puede prolongar hasta otra que discrepe de f en un número natural.

Si suponemos $\mathrm{AM}(\mathfrak{c})$, existe un filtro $G \subset \mathbb{P}$ tal que $G \cap D_n \neq \varnothing$ para todo $n < \omega$ y $G \cap E_f \neq \varnothing$ para todo $f \in {}^{\omega}2$.

Exactamente igual que en el caso anterior, que G sea un filtro implica que sus condiciones se prolongan una a otra, y el hecho de que $G \cap D_n \neq \varnothing$ implica que $f_G = \bigcup G : \omega \longrightarrow 2$ y, para toda $f \in {}^{\omega}2$, el hecho de que $D_f \cap G \neq \varnothing$ se traduce en que existe $p \in G$ que está definida en un cierto $n < \omega$ de modo que $p(n) \neq f(n)$, pero $p \subset f_G$, luego $f_G(n) \neq f(n)$ y así $f_G \neq f$ para toda $f \in {}^{\omega}2$, contradicción, lo cual es absurdo, porque implica en particular que $f_G \neq f_G$. ∎

El axioma de Martin puede expresarse en términos de lo que podríamos considerar un cardinal característico del continuo (si admitimos como tal uno con una definición tan sofisticada):

Definición 8.42 El *cardinal de Martin* es el menor cardinal $\mathfrak{m}$ tal que no se cumple AM($\mathfrak{m}$).

En virtud del teorema anterior, se cumple $\aleph_1 \leq \mathfrak{m} \leq \mathfrak{c}$, y el axioma de Martin equivale a que $\mathfrak{m} = \mathfrak{c}$.

Observemos que, trivialmente, $\mathfrak{c} = \aleph_1 \to \mathfrak{m} = \mathfrak{c}$ o, dicho de otro modo, que la hipótesis del continuo implica el axioma de Martin.

Bajo la hipótesis del continuo, AM equivale a AM($\aleph_0$), que es un teorema, por lo que el axioma de Martin no aporta nada en este caso. Pero sucede que puede demostrarse que, si la teoría de conjuntos es consistente, también lo es si le añadimos AM como axioma, *juntamente con cualquier otro axioma de la forma* $2^{\aleph_0} = \aleph_7$*, etc.,* con tal de que no pidamos que $2^{\aleph_0}$ sea singular, pues, como veremos enseguida, AM implica que $\mathfrak{c}$ es regular (teorema 8.44).

En particular, por ejemplo, si la teoría de conjuntos es consistente, también lo es tomar como axioma AM($\aleph_1$) o, lo que es lo mismo, $\mathfrak{m} > \aleph_1$, lo cual contradice la hipótesis del continuo.

Lo que hemos explicado antes es que puede demostrarse que, si la teoría de conjuntos es consistente, también lo es suponer AM o, equivalentemente, que $\mathfrak{m} = \mathfrak{c}$. Por lo tanto, cualquier afirmación que demostremos suponiendo AM será consistente con los axiomas de la teoría de conjuntos, supuesto que éstos sean consistentes. Por ejemplo:

Teorema 8.43 *Se cumple* $\mathfrak{m} \leq \mathfrak{p}$.

Vamos a tratar de usar esta primera aplicación del axioma de Martin para explicar las ideas principales subyacentes en el uso de este axioma. Ya hemos tenido ocasión de emplearlas en la prueba de 8.41, aunque de un modo un tanto atípico, porque allí suponíamos formas contradictorias de AM para llegar a contradicciones.

- En general, usar AM supone elegir un conjunto preordenado $\mathbb{P}$, cuyas condiciones serán como "piezas" de un juego de construcción con las que formaremos un determinado objeto que deseamos construir. El filtro G que proporciona AM nos dice qué "piezas" debemos usar exactamente para la construcción.

  Por ejemplo, en la prueba de 8.41 3) hemos usado como "piezas" sucesiones finitas en ω_1, pensadas para que un filtro adecuado $G \subset \mathbb{P}$ nos dé una función $f_G : \omega \longrightarrow \omega_1$ suprayectiva, y en el apartado 4) hemos usado como "piezas" sucesiones finitas en 2 pensadas para que un filtro adecuado $G \subset \mathbb{P}$ nos de una aplicación $f_G : \omega \longrightarrow 2$ distinta de todas las aplicaciones $f : \omega \longrightarrow 2$.

- Conviene pensar en cada "pieza" $p \in \mathbb{P}$ como información parcial sobre las propiedades que tendrá el objeto que queremos construir supuesto que la pieza acabe estando en el filtro G.

  Por ejemplo, cuando $\mathbb{P} = 2^{<\omega}$, una sucesión $p = (1, 1, 0, 1, 0, 0)$ nos indica que si, finalmente $p \in G$, entonces la función $f_G = \bigcup G$ cumplirá $f_G(0) = 1$, $f_G(1) = 1$, $f_G(2) = 0$, etc.

- La relación de orden debe estar pensada para que $p \leq q$ signifique que la condición p contiene más información que la condición q sobre el objeto que queremos construir, mientras que la incompatibilidad $p \perp q$ indica que las condiciones p y q contienen información contradictoria, de modo que no pueden estar las dos en el filtro G.

  Por ejemplo, si $\mathbb{P} = 2^{<\omega}$, las condiciones $p = (1, 1, 0, 1)$ y $q = (1, 0, 0, 1, 0)$ son contradictorias, porque si $p \in G$, tendría que ser $f_G(1) = 1$, mientras que si $q \in G$ tendría que ser $f_G(1) = 0$. Por eso son incompatibles.

- Una vez seleccionadas las piezas, definimos conjuntos densos adecuados que determinarán las propiedades del objeto que queremos construir.

  Por ejemplo, en los apartados 3) y 4) de 8.41, los conjuntos densos D_n estaban pensados para asegurar que la función f_G obtenida tuviera dominio ω. En el apartado 3) los conjuntos E_α estaban pensados para que f_G fuera suprayectiva, y en el apartado 4) los conjuntos E_f estaban pensados para que $f_G \neq f$.

- Una vez elegidos convenientemente los conjuntos densos, el axioma de Martin nos proporciona un filtro G que selecciona las "piezas" que debemos usar en nuestra construcción.

  En 8.41 la "construcción" consistía en tomar $f_G = \bigcup G$. En realidad, cuando elegimos el conjunto de "piezas" $\mathbb{P}$, lo hacemos pensando ya en qué objeto vamos a construir a partir de un filtro G en $\mathbb{P}$, de modo que los conjuntos densos se eligen pensando ya en el objeto que vamos a construir, aunque todavía no esté definido.

Para probar 8.43, partimos de una familia $S \subset [\omega]^\omega$ con la propiedad fuerte de la intersección finita tal que $|S| = \kappa < \mathfrak{m}$ y queremos construirle una pseudointersección X. Esto probará que $\kappa < \mathfrak{p}$, luego $\mathfrak{m} \leq \mathfrak{p}$.

Un posible conjunto de condiciones a partir de las cuales podamos obtener un $X \subset \omega$ es, como antes, $\mathbb{P} = 2^{<\omega}$, de modo que un filtro adecuado G nos dará una función $f_G : \omega \longrightarrow 2$ y podremos tomar $X_G = \{n \in \omega \mid f_G(n) = 1\}$, por ejemplo, es decir, el conjunto cuya función característica es f_G.

Así, una condición como $p = (1, 0, 1, 1, 0, 0)$ nos da información parcial sobre X_G. Concretamente, nos dice que, si $p \in G$, se cumplirá que

$$0 \in X_G, \quad 1 \notin G, \quad 2 \in G, \quad 3 \in G, \quad 4 \notin G, \quad 5 \notin G.$$

Sin embargo, para evitar los tecnicismos inherentes a que estamos construyendo una función en ${}^{\omega}2$ cuando lo que queremos es un conjunto en $[\omega]^\omega$, podemos considerar un c.p.o. que cumple la misma función de forma más directa.

Consideramos el conjunto $\mathbb{P} = [\omega]^{<\omega}$ de los subconjuntos finitos de ω con el orden dado por $p \le q$ si y sólo si q es una sección inicial de p. Por ejemplo,

$$\{2,4,5,7,10\} \le \{2,4,5\}, \qquad \text{pero} \qquad \{2,4,5,7,10\} \not\le \{2,3,4,5\}.$$

La intención es definir $X_G = \bigcup G$, de modo que $\{2,4,5,7,10\} \in G$ nos informa de que $0 \notin X_G$, $1 \notin X_G$, $2 \in X_G$, $3 \notin X_G$, $4 \in X_G$, etc.

Si hubiéramos definido $p \le q$ si y sólo si $q \subset p$, cada condición $p \in G$ contendría información sobre posibles elementos de X_G, pero no nos diría nada sobre qué elementos no están en X_G. Con la relación de orden que hemos dado, cada condición no sólo nos informa sobre que ciertos números sí que van a estar en G, sino también sobre que otros no van a estar.

Observemos ahora que el conjunto D_n de las condiciones de cardinal mayor o igual que n es denso en $\mathbb{P}$, pues toda condición se puede prolongar hasta tener al menos n elementos, y $D_n \cap G \neq \varnothing$ garantizará que $|X_G| \ge n$. Si esto sucede para todo n, tendremos garantizado que X_G será infinito.

Sólo nos falta definir, para cada $A \in S$, un conjunto denso D_A tal que $D_A \cap G \neq \varnothing$ nos asegure que $X_A \setminus A$ será finito, pues así X_G será una pseudo-intersección de S.

Por desgracia, no es posible hacer tal cosa, pues el hecho de que exista $p \in D_A \cap G$, definamos como definamos D_A, no nos permite garantizar que $X_A \setminus A$ vaya a ser finito, ya que las condiciones de G que extiendan a p pueden crecer incontroladamente, de modo que X_A acabe saliéndose infinitas veces del conjunto A.

Para resolver esta dificultad debemos reconsiderar la elección de $\mathbb{P}$. Notemos que pedir que $X_G \setminus A$ sea finito es lo mismo que pedir que exista un conjunto finito $s \subset \omega$ tal que $X_G \setminus s \subset A$. Este conjunto finito s puede ser la propia condición, pero necesitamos que vaya acompañada de la "promesa" de que sus extensiones no se saldrán de A más que el número finito de veces que ya se haya salido ella misma. Esta "promesa" tiene que incluirse en la definición de la relación de orden, para asegurarnos de que las extensiones de una condición dada no la violarán. El resultado de esta reflexión es el siguiente:

Definimos $\mathbb{P}$ como el conjunto de pares (s, F), donde $s \in [\omega]^{<\omega}$ y $F \in [S]^{<\omega}$, con el orden parcial dado por $(s', F') \le (s, F)$ si y sólo si

$$s \text{ es un segmento inicial de } s', \qquad F \subset F', \qquad s' \setminus s \subset \bigcap F.$$

La idea es que el conjunto finito $F = \{A_1, \ldots, A_n\}$ que acompaña al conjunto s es un conjunto de "promesas", de modo que cualquier extensión (s', F') de (s, F) puede tener más promesas, pero debe respetar las asumidas por (s, F), en el sentido de que los nuevos elementos añadidos a s cumplirán

$$s' \setminus s \subset A_1 \cap \cdots \cap A_n.$$

En otras palabras, (s,F) significa que el conjunto finito $s \subset \omega$ "ha prometido" que cuando crezca no se saldrá más de $A_1,\dots,A_n$, aunque hasta el momento haya podido hacerlo. Por supuesto, la idea ahora es definir igualmente

$$X_G = \bigcup_{(s,F)\in G} s,$$

pero la diferencia es que ahora, si $(s,F) \in G$ y $A \in F$, tenemos garantizado que $X_G \setminus s \subset A$, luego, para garantizar que X_G sea una pseudointersección de S sólo tenemos que asegurar que G contenga condiciones (s,F) tales que F contenga a cualquier $A \in S$, y eso sí que puede conseguirse con el conjunto denso adecuado.

Por claridad pasamos a demostrar el teorema desde cero:

Demostración (de 8.43): Sea $S \subset [\omega]^\omega$ una familia con la propiedad fuerte de la intersección finita tal que $|S| = \kappa < \mathfrak{m}$. Vamos a probar que S tiene una pseudointersección X. Definimos $\mathbb{P}$ como el conjunto de todos los pares (s,F), donde $s \in [\omega]^{<\omega}$ y $F \in [S]^{<\omega}$, con el orden parcial dado por $(s',F') \le (s,F)$ si y sólo si

$$s \text{ es un segmento inicial de } s', \qquad F \subset F', \qquad s' \setminus s \subset \bigcap F.$$

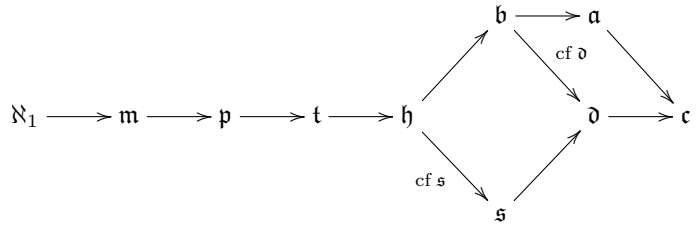
Veamos que $\mathbb{P}$ cumple la condición de cadena numerable. Basta probar que un subconjunto no numerable de $\mathbb{P}$ no puede ser una anticadena. En efecto, un subconjunto no numerable de $\mathbb{P}$ tiene que tener una cantidad no numerable de elementos con la misma primera componente, digamos (s,F) y (s,F'), pero dos condiciones así son compatibles, ya que $(s, F \cup F')$ es una extensión común.

Para cada $A \in S$, el conjunto $D_A = \{(s,F) \in \mathbb{P} \mid A \in F\}$ es denso, pues toda condición (s,F) admite como extensión $(s, F \cup \{A\}) \in D_A$. También lo es $D_n = \{(s,F) \in \mathbb{P} \mid |s| > n\}$, porque, dada una condición (s,F), tenemos que $\bigcap F$ es infinito, luego podemos extender s hasta un s' tal que $|s'| > n$ y $s' \setminus s \subset \bigcap F$ y entonces $(s',F) \in D_n$ es una extensión de (s,F).

Como se cumple $\mathrm{AM}(\kappa)$, existe un filtro G en $\mathbb{P}$ que corta a todos los conjuntos D_A. Vamos a probar que $X_G = \bigcup_{(s,F)\in G} s$ es una pseudointersección de S.

El hecho de que $G \cap D_n \neq \varnothing$ se traduce en que X_G es infinito. Dado $A \in S$, podemos tomar $(s_0,F_0) \in G \cap D_A$, con lo que $A \in F_0$. Basta probar que $X_G \setminus s_0 \subset A$. Si $k \in X_G \setminus s_0$, por definición de X_G existe un $(s,F) \in G$ tal que $k \in s \setminus s_0$. Como G es un filtro, podemos suponer que $(s,F) \le (s_0,F_0)$, y entonces $k \in \bigcap F \subset A$. ∎

Así pues, podemos completar así el esquema de los cardinales característicos que hemos estudiado en la sección 8.1:



En particular:

Teorema 8.44 (AM) $\mathfrak{p} = \mathfrak{t} = \mathfrak{h} = \mathfrak{s} = \mathfrak{b} = \mathfrak{d} = \mathfrak{a} = \mathfrak{c} = \operatorname{cf} \mathfrak{c}$.

En efecto, como $\mathfrak{t}$ o $\mathfrak{b}$ son regulares, AM implica que $\mathfrak{c}$ es regular, como ya habíamos indicado. Más aún, que si $\kappa < \mathfrak{c}$, entonces $2^\kappa = \mathfrak{c}$ (por el teorema 8.5).

Por ejemplo, esto significa que, bajo AM, una familia casi disjunta en $\mathcal{P}\omega$ tiene que tener necesariamente cardinal $\mathfrak{c}$.

Por otra parte, el teorema 8.34 muestra que AM implica que casi todos los cardinales que aparecen en el diagrama de Cichoń son iguales a $\mathfrak{c}$. Sólo se escapan $\operatorname{ad}(I_m)$ y $\operatorname{cub}(I_m)$, pero no por mucho tiempo:

Teorema 8.45 $\mathfrak{m} \leq \operatorname{ad}(I_m)$.

Demostración: Sea X un espacio polaco dotado de una medida de Borel continua y unitaria μ. Dado $\epsilon > 0$, llamamos $\mathbb{P}_\epsilon$ al conjunto de todos los abiertos de X de medida menor que ϵ, con el orden parcial dado por $U \leq V$ si y sólo si $V \subset U$. Veamos en primer lugar que $\mathbb{P}_\epsilon$ cumple la c.c.n.[3]

Observemos en primer lugar que $U \perp V$ significa que $\mu(U \cup V) < \epsilon$.

En efecto, en principio, dos abiertos son compatibles si existe un tercer abierto $W \in \mathbb{P}_\epsilon$ tal que $U \cup V \subset W$, con lo que $\mu(U \cup V) \leq \mu(W) < \epsilon$, y el recíproco es claro.

Consideramos una familia $A \subset \mathbb{P}_\epsilon$ no numerable, y vamos a probar que no es una anticadena. Si A_n es el conjunto de condiciones de A tales que $\mu(U) < \epsilon - 1/n$, como A es la unión de los A_n, tiene que existir un $n \geq 1$ tal que A_n sea no numerable. Equivelentemente, podemos suponer que todos los abiertos de A cumplen $\mu(A) < \epsilon - 1/n$.

Sea $\mathcal{B}$ una base numerable de X. Podemos suponerla cerrada para uniones finitas. Cada abierto U puede expresarse como unión creciente de abiertos de $\mathcal{B}$, luego, para cada $U \in A$, existe un $U' \in \mathcal{B}$ tal que $U' \subset U$ y $\mu(U) < \mu(U') + 1/n$. Podemos descomponer A en la unión de las condiciones que contienen a un mismo abierto $U' \in \mathcal{B}$ en estas condiciones, luego tiene que haber un $U' \in \mathcal{B}$ que aproxime la medida de una cantidad no numerable de abiertos de A. Nos basta con tomar dos de ellos: sean $U_1, U_2 \in A$ tales que existe $U' \in \mathcal{B}$ tal que $U' \subset U_1 \cap U_2$ y $\mu(U_i) < \mu(U') + 1/n$, luego $\mu(U_2 \setminus U_1) \leq \mu(U_2 \setminus U') < 1/n$. Entonces $\mu(U_1 \cup U_2) = \mu(U_1) + \mu(U_2 \setminus U_1) < \epsilon < 1/n + 1/n = \epsilon$, luego U_1 y U_2 son compatibles.

Si G es un filtro en $\mathbb{P}_\epsilon$, se cumple que $U_G = \bigcup G$ es un abierto en X que cumple $\mu(U_G) \leq \epsilon$.

En efecto, si fuera $\mu(U_G) > \epsilon$, por la regularidad de la medida, existe un compacto $K \subset U_G$ tal que $\mu(K) > \epsilon$, pero G es un cubrimiento de K, luego

[3]En general, comprobar que el c.p.o. que consideramos cumple la c.c.n. no se usa para nada en los argumentos relacionados con el axioma de Martin. Simplemente es un requisito necesario para garantizar que AM puede usarse consistentemente.

existe un subcubrimiento finito, $K \subset U_1 \cup \cdots \cup U_n$, con los $U_i \in G$. Pero como las condiciones de G son compatibles, de hecho existe $U \in G$ tal que $K \subset U_1 \cup \cdots \cup U_n \subset U$, luego $\mu(K) \leq \mu(U) < \epsilon$, contradicción.

Con esto ya podemos concluir: sea $\kappa < \mathfrak{m}$ y sea $\{N_\alpha\}_{\alpha<\kappa}$ una familia de conjuntos nulos. Dado $\epsilon > 0$, se cumple que $D_\alpha = \{U \in \mathbb{P}_\epsilon \mid N_\alpha \subset U\}$ es denso en $\mathbb{P}_\epsilon$, pues si $U \in \mathbb{P}_\epsilon$, por regularidad podemos tomar un abierto V en X tal que $N_\alpha \subset V$ y $\mu(V) < \epsilon - \mu(U)$, con lo que $\mu(U \cup V) < \epsilon$, luego $U \cup V \in D_\alpha$ y $U \cup V \leq U$.

Por AM(κ) existe un filtro G en $\mathbb{P}_\epsilon$ tal que $\mathbb{P}_\epsilon \cap D_\alpha \neq \varnothing$, para todo $\alpha < \kappa$, lo que significa que $N_\alpha \subset U_G$, para todo α, luego $\bigcup_{\alpha<\kappa} N_\alpha \subset U_G$, luego

$$\mu\Big(\bigcup_{\alpha<\kappa} N_\alpha\Big) \leq \mu(U_G) \leq \epsilon,$$

para todo $\epsilon > 0$, luego la unión de los κ conjuntos nulos es nula. Así pues, $\kappa \leq \mathrm{ad}(I_m)$, luego $\mathfrak{m} \leq \mathrm{ad}(I_m)$. ∎

Así pues, AM implica que todos los cardinales que aparecen en el diagrama de Cichoń (sin contar $\aleph_1$) son iguales a $\mathfrak{c}$.

En particular, $\mathfrak{m} \leq \mathrm{ad}(I_c)$ significa que, en un espacio polaco perfecto, la unión de $\kappa < \mathfrak{m}$ conjuntos de primera categoría es de primera categoría, luego la unión de κ cerrados de interior vacío tiene interior vacío, y la intersección de κ abiertos densos es densa. En realidad esto es válido para muchos otros espacios topológicos, incluyendo todos los espacios polacos, aunque no sean perfectos. Concretamente, podemos probarlo para todo espacio Čech-completo [T 7.81] con la condición de cadena numerable, lo cual incluye a todos los espacios polacos [T 7.83] y a todos los espacios localmente compactos con la condición de cadena numerable [7.84]:

Teorema 8.46 *Sea X un espacio topológico Čech-completo que cumpla la condición de cadena numerable (es decir, tal que toda familia de abiertos disjuntos dos a dos sea numerable). Entonces, la intersección de $\kappa < \mathfrak{m}$ abiertos densos es densa.*

Demostración: Sea $\mathbb{P}$ el conjunto de todos los abiertos no vacíos de X con el orden parcial dado por $U \leq V$ si y sólo si $U \subset V$. Claramente, dos abiertos son incompatibles en $\mathbb{P}$ si y sólo si son disjuntos, luego la hipótesis de que $\mathbb{P}$ cumple la c.c.n. como espacio topológico equivale a que $\mathbb{P}$ la cumple como c.p.o.

Sea $\{U_\alpha\}_{\alpha<\kappa}$ una familia de abiertos densos en X. Vamos a probar que su intersección es densa. Para ello tomamos un abierto no vacío U en X y vamos a probar que corta a la intersección. Sea

$$D_\alpha = \{p \in \mathbb{P} \mid \overline{p} \subset U \cap U_\alpha\}.$$

Entonces D_α es denso en $\mathbb{P}$, pues, dado $p \in \mathbb{P}$, como U_α es un abierto denso, tenemos que $p \cap U \cap U_\alpha$ es un abierto no vacío, y como X es regular, cualquier punto $x \in p \cap U \cap U_\alpha$ tiene un entorno abierto d tal que $x \in d \subset \overline{d} \subset p \cap U \cap U_\alpha$, luego $d \in D_\alpha$ y $d \leq p$.

Por otra parte, sea $\{\mathcal{U}_n\}_{n=1}^{\infty}$ una familia de cubrimientos abiertos de X que cumpla la definición de espacio Čech-completo y sea

$$E_n = \{p \in \mathbb{P} \mid \delta(\overline{p}) < \mathcal{U}_n\}.$$

También es un conjunto denso en $\mathbb{P}$, pues, si $p \in \mathbb{P}$, tiene que existir un $A \in \mathcal{U}_n$ tal que $p \cap A \neq \varnothing$, y por la regularidad de X, todo punto $x \in p \cap A$ tiene un entorno abierto d tal que $x \in d \subset \overline{d} \subset p \cap A$, con lo que $d \in E_n$ y $d \leq p$.

Por $\mathrm{AM}(\kappa)$, existe un filtro G en $\mathbb{P}$ que corta a todos los conjuntos D_α y E_n. El hecho de que corte a los conjuntos E_n se traduce en que $\{\overline{p} \mid p \in G\}$ es una familia de cerrados con la propiedad de la intersección finita (porque G es un filtro) que contiene conjuntos de diámetro menor que $\mathcal{U}_n$, para todo n, luego resulta que $K_G = \bigcap_{p \in G} \overline{p} \neq \varnothing$.

Como $G \cap D_\alpha \neq \varnothing$, existe una condición $p \in G \cap D_\alpha$, lo que significa que $K_G \subset \overline{p} \subset U \cap U_\alpha$, luego $K_G \subset U \cap \bigcap_{\alpha<\kappa} U_\alpha \neq \varnothing$. ∎

La conclusión del teorema anterior equivale claramente a que la unión de menos de $\mathfrak{m}$ cerrados de interior vacío tenga interior vacío, o a que la unión de menos de $\mathfrak{m}$ conjuntos de primera categoría sea de primera categoría, en otras palabras, a que el teorema de Baire se cumpla para uniones / intersecciones de cualquier cantidad $\kappa < \mathfrak{m}$ conjuntos.

Vamos a probar que este resultado es, de hecho, equivalente a $\mathrm{AM}(\kappa)$, con lo que tenemos una interpretación topológica del axioma de Martin:

Teorema 8.47 *Sea κ un cardinal infinito. Las afirmaciones siguientes son equivalentes:*

1. $\mathrm{AM}(\kappa)$.
2. *En un espacio topológico de Hausdorff (localmente) compacto con la c.c.n., la intersección de κ abiertos densos es densa.*
3. *En un espacio topológico de Hausdorff compacto con la c.c.n., la intersección de κ abiertos densos no vacía.*
4. *En un álgebra de Boole (completa) con la c.c.n., para toda familia de κ conjuntos densos, existe un filtro que los corta a todos.*
5. *En un c.p.o. $\mathbb{P}$ con la c.c.n. tal que $|\mathbb{P}| \leq \kappa$, para toda familia de κ conjuntos densos, existe un filtro que los corta a todos.*

Demostración: 1) ⇒ 2) es un caso particular del teorema anterior. Obviamente, 2) para espacios localmente compactos implica 2) para espacios compactos, y esto implica a su vez 3). Veamos que 3) ⇒ 4) Sea $\mathbb{B}$ un álgebra de Boole con la c.c.n. (no suponemos que sea completa) y sea $\{D_\alpha\}_{\alpha<\kappa}$ una familia de conjuntos densos en $\mathbb{B}$ (aquí hay que entender en $\mathbb{B} \setminus \{\mathbb{0}\}$).

Entonces el espacio de Stone $K = S(\mathbb{B})$ es un espacio de Hausdorff compacto que tiene por base a su álgebra de abiertos-cerrados, que es isomorfa a $\mathbb{B}$ (y por

ello a partir de aquí identificamos a $\mathbb{B}$ con la familia de abiertos-cerrados en K). El hecho de que $\mathbb{B}$ cumpla la c.c.n. como álgebra de Boole (es decir, como c.p.o.) equivale a que $S(B)$ la cumpla como espacio topológico.

Sea $E_\alpha = \bigcup D_\alpha$, que es un abierto denso en K. En efecto, basta ver que corta a todo abierto cerrado no vacío $p \in \mathbb{B}$, y esto se debe a que existe un $d \in D_\alpha$ tal que $d \leq p$, luego $\varnothing \neq d \subset E_\alpha \cap p$.

Por hipótesis existe $G \in \bigcap_{\alpha<\kappa} E_\alpha$, pero G es un ultrafiltro en $\mathbb{B}$ y claramente corta a todos los D_α.

Obviamente 4) para álgebras no necesariamente completas implica 4) para álgebras completas. Veamos ahora que 4) para álgebras completas implica 5).

Sea $\mathbb{P}$ un c.p.o. con la c.c.n. tal que $|\mathbb{P}| \leq \kappa$. Fijemos una familia $\mathcal{D}$ de a lo sumo κ subconjuntos densos de $\mathbb{P}$.

Consideramos la compleción $\mathbb{B}$ de $\mathbb{P}$, que es un álgebra de Boole completa tal que existe una inmersión densa $i : \mathbb{P} \longrightarrow \mathbb{B}$. Observemos que $\mathbb{B}$ cumple la c.c.n., pues si $C \subset \mathbb{B}$ fuera una anticadena no numerable en $\mathbb{B}$, para cada $s \in C$ podríamos tomar $p_s \in \mathbb{P}$ tal que $i(p_s) \leq s$, y entonces $\{p_s \mid s \in C\}$ sería una anticadena no numerable en $\mathbb{P}$.

También es claro que si $D \in \mathcal{D}$ entonces $i[D]$ es denso en $\mathbb{B}$, luego por hipótesis existe un filtro G en $\mathbb{B}$ que corta a todos los conjuntos $i[D]$, con $D \in \mathcal{D}$. Esto implica a su vez que $H = i^{-1}[G]$ corta a todos los elementos de $\mathcal{D}$. Sin embargo, sucede que H no es necesariamente un filtro en G. Obviamente, si $p \leq q$ con $p \in H$ también $q \in H$. El problema es que no podemos probar que dos elementos de H tienen una extensión en H.

Para resolver esto, para cada $p, q \in \mathbb{P}$, definimos

$$D_{pq} = \{r \in \mathbb{P} \mid (r \leq p \wedge r \leq q) \vee r \perp p \vee r \perp q\}.$$

Se cumple que es denso en $\mathbb{P}$. En efecto, si $s \in \mathbb{P}$, o bien tiene una extensión incompatible con p o con q (con lo que dicha extensión está en D_{pq}) o, en caso contrario, $\neg s \perp p$, luego existe $s' \in \mathbb{P}$ tal que $s' \leq s$, $s' \leq p$, pero s' tiene que ser compatible con q, luego existe $s'' \in \mathbb{P}$ tal que $s'' \leq s'$, $s'' \leq q$, luego $s'' \in D_{pq}$ y $s'' \leq s$.

Como estamos suponiendo que $|\mathbb{P}| \leq \kappa$, no perdemos generalidad si suponemos que los conjuntos D_{pq} están en $\mathcal{D}$, y así sí que podemos probar que H es un filtro en $\mathbb{P}$. En efecto, dados $p, q \in H$, tenemos que existe $r \in H \cap D_{pq}$. Si $r \perp p$, entonces $i(r) \perp i(p)$, porque i es una inmersión, lo cual es imposible porque ambos están en G, luego r es compatible con p, y por el mismo motivo con q, luego por definición de D_{pq} tiene que ser $r \leq p \wedge r \leq q$.

Veamos por último que 5) $\Rightarrow$ 1). Sea $\mathbb{P}$ un c.p.o. arbitrario con la condición de cadena numerable y sea $\mathcal{D}$ una familia de a lo sumo κ subconjuntos densos de $\mathbb{P}$. Veamos que existe $\mathbb{Q} \subset \mathbb{P}$ tal que:

1. $|\mathbb{Q}| \leq \kappa$,
2. Para todo $D \in \mathcal{D}$, se cumple que $D \cap \mathbb{Q}$ es denso en $\mathbb{Q}$,
3. Dos condiciones de $\mathbb{Q}$ son compatibles en $\mathbb{Q}$ si y sólo si lo son en $\mathbb{P}$.

Si $D \in \mathcal{D}$, sea $f_D : \mathbb{P} \longrightarrow D$ tal que

$$\bigwedge p \in \mathbb{P}\,(f_D(p) \in D \wedge f_D(p) \leq p)).$$

Sea $g : \mathbb{P} \times \mathbb{P} \longrightarrow \mathbb{P}$ tal que

$$\bigwedge pq \in \mathbb{P}(\neg p \perp q \to g(p,q) \leq p \wedge g(p,q) \leq q).$$

Tomemos cualquier $p_0 \in \mathbb{P}$ y definamos

$$\mathbb{Q}_0 = \{p_0\} \wedge \bigwedge n \in \omega\ \mathbb{Q}_{n+1} = \mathbb{Q}_n \cup g[\mathbb{Q}_n \times \mathbb{Q}_n] \cup \bigcup_{D\in\mathcal{D}} f_D[\mathbb{Q}_n].$$

Es claro que $\mathbb{Q} = \bigcup_{n\in\omega} \mathbb{Q}_n$ cumple lo pedido.

Por 3) tenemos que $\mathbb{Q}$ cumple la condición de cadena numerable, por 1), 2) tenemos que existe un filtro H en $\mathbb{Q}$ que corta a todos conjuntos $D \cap \mathbb{Q}$, con $D \in \mathcal{D}$. Definimos

$$G = \{p \in \mathbb{P} \mid \bigvee q \in H\ q \leq p\}.$$

Es fácil comprobar que G es un filtro en $\mathbb{P}$ y obviamente contiene a H, luego corta a todos los elementos de D. ∎

El teorema 8.46 permite generalizar de forma trivial argumentos basados en el teorema de Baire. Por ejemplo, un resultado clásico de Sierpiński es que $\mathbb{R}$ no puede descomponerse es unión numerable de cerrados disjuntos. La prueba siguiente es una adaptación mínima de una demostración de este hecho basada en el teorema de Baire:

Teorema 8.48 *Sea X un espacio polaco, sea $2 \leq \kappa < \mathfrak{m}$ y supongamos que X es conexo o que $\kappa \geq \aleph_1$. Entonces X no puede descomponerse en unión de κ cerrados no vacíos disjuntos dos a dos.*

Demostración: Supongamos que $X = \bigcup_{\alpha<\kappa} C_\alpha$, donde los conjuntos C_α son cerrados no vacíos disjuntos dos a dos. Sea

$$K = \bigcup_{\alpha<\kappa} \partial C_\alpha = \bigcup_{\alpha<\kappa} (C_\alpha \setminus \mathring{C}_\alpha) = I \setminus \bigcup_{\alpha<\kappa} \mathring{C}_\alpha.$$

Observemos que $K \neq \varnothing$ porque, si X es conexo, entonces todas las fronteras ∂C_α son no vacías, o de lo contrario C_α sería abierto y cerrado en X, luego sería $C_\alpha = X$ para todo α, lo cual es absurdo. Si $\kappa \geq \aleph_1$, entonces a lo sumo una cantidad numerable de cerrados C_α puede ser abierto, porque X cumple la condición de cadena numerable, luego igualmente hay κ valores de α para los que $\partial C_\alpha \neq \varnothing$, y así $K \neq \varnothing$.

Como K es cerrado en X, se trata de un espacio polaco no vacío, y la versión para espacios polacos del teorema 8.46 equivale a que la intersección de κ cerrados de interior vacío tenga interior vacío, luego concluimos que algún

∂C_β no tiene interior vacío en K. Sea U abierto en X tal que $\varnothing \neq U \cap K \subset \partial C_\beta$. Entonces

$$U = (U \cap K) \cup (U \setminus K) = (U \cap \partial C_\beta) \cup (U \cap \bigcup_{\alpha<\kappa} \mathring{C}_n).$$

Si $U \cap \mathring{C}_\alpha \neq \varnothing$, con $\alpha \neq \beta$, tenemos que $U \not\subset \mathring{C}_\alpha$, porque $U \cap \partial C_\beta \neq \varnothing$ y $\partial C_\beta \cap C_\alpha = \varnothing$. Por lo tanto, $\varnothing \neq U \cap \partial C_\alpha \subset U \cap K \subset \partial C_\beta$, pero esto es imposible, porque $\partial C_\alpha \cap \partial C_\beta = \varnothing$. Así pues,

$$U = (U \cap \partial C_\beta) \cup (U \cap \mathring{C}_\beta) = U \cap C_\beta \subset C_\beta,$$

luego $U \subset \mathring{C}_\beta$, luego $U \cap \partial C_\beta = \varnothing$, contradicción. ∎

Extensiones de medidas de Borel El teorema 7.76 afirma que la existencia de una extensión de la medida de Lebesgue a $\mathcal{P}\mathbb{R}$ equivale a la existencia de un cardinal $\mathbb{R}$-medible $\kappa \leq \mathfrak{c}$. Ahora vamos a probar que esto es incompatible con el axioma de Martin:

Teorema 8.49 (AM) *No existen cardinales $\mathbb{R}$-medibles $\leq \mathfrak{c}$.*

Demostración: Si existe un cardinal $\mathbb{R}$-medible $\leq \mathfrak{c}$, entonces existe una medida μ en $\mathbb{R}$ que extiende a la medida de Lebesgue (teorema 3.50). Como la medida de Lebesgue es $\mathfrak{c}$-aditiva (teorema 8.45) todo $x \subset \mathbb{R}$ con $|x| < \mathfrak{c}$ cumple $\mu(x) = 0$. Sea $\kappa = \mathfrak{c}$. Biyectando el intervalo $[0,1]$ con κ obtenemos una medida unitaria m en κ con esta propiedad, es decir, todo conjunto de medida positiva tiene cardinal $\mathfrak{c}$.

Como AM implica $\mathfrak{b} = \mathfrak{d}$, por 8.13 existe una escala $\{f_\alpha\}_{\alpha<\kappa}$ de longitud κ. Sea $A_{nm} = \{\alpha < \kappa \mid f_\alpha(n) = m\}$. Así $\kappa = \bigcup_{m<\omega} A_{nm}$, para todo $n < \omega$.

Para cada $n < \omega$, sea $m_n < \omega$ tal que

$$m\Big(\bigcup_{m=0}^{m_n} A_{mn}\Big) \geq 1 - \frac{1}{2^{n+2}}$$

y sea $B_n = \bigcup_{m=0}^{m_n} A_{mn}$. Sea $B = \bigcap_{n<\omega} B_n$. Así

$$m(B) = 1 - m(\kappa \setminus B) = 1 - m\Big(\bigcup_{n<\omega} \kappa \setminus B\Big) \geq 1 - \Big(\sum_{n<\omega} m(\kappa \setminus B_n)\Big)$$

$$= 1 - \Big(\sum_{n<\omega} 1 - m(B_n)\Big) \geq 1 - \sum_{n<\omega} \tfrac{1}{2^{n+2}} = 1 - \tfrac{1}{2} = \tfrac{1}{2}.$$

Sea $g : \omega \longrightarrow \omega$ la función dada por $g(n) = m_n$. De este modo, si $n \in \omega$ y $\alpha \in B$, se cumple que $\alpha \in B_n$, luego $\alpha \in A_{nm}$ para cierto $m \leq m_n$, luego $f_\alpha(n) = m \leq m_n = g(n)$. Esto significa que $g \not<^* f_\alpha$.

Por otra parte, como $m(B) > 0$, ha de ser $|B| = 2^{\aleph_0}$, luego B es cofinal en κ. Por definición de escala debe existir un $\beta < \kappa$ tal que $g <^* f_\beta$ y, como B es cofinal, existe un $\alpha \in B$, $\alpha > \beta$, pero entonces $g <^* f_\beta <^* f_\alpha$, contradicción. ∎

Ejercicio: Demostrar que si existe una escala de longitud κ entonces κ no es un cardinal $\mathbb{R}$-medible.

8.4 Condiciones de cadena en productos

Hemos visto que AM implica que la unión de menos de $\mathfrak{c}$ conjuntos nulos para la medida de Lebesgue es nula, o que la unión de menos de $\mathfrak{c}$ cerrados de interior vacío en $\mathbb{R}$ tiene interior vacío, etc. Pero todas estas propiedades se reducen a hechos conocidos si $\mathfrak{c} = \aleph_1$ (a la definición de medida o al teorema de Baire, respectivamente). Lo mismo sucede con todas las consecuencias que hemos deducido hasta ahora del axioma de Martin. En esta sección vamos a ver una consecuencia de $\mathrm{AM}(\aleph_1)$, es decir, una consecuencia que no se vuelve trivial, sino falsa, si suponemos la hipótesis del continuo.

Definición 8.50 Si $\mathbb{P}$ y $\mathbb{Q}$ son c.p.o.s, consideraremos a $\mathbb{P} \times \mathbb{Q}$ como c.p.o. con el preorden dado por

$$(p_1, q_1) \leq (p_2, q_2) \leftrightarrow p_1 \leq p_2 \wedge q_1 \leq q_2.$$

Se dice espacio topológico cumple la condición de cadena κ si toda familia de abiertos disjuntos dos a dos tiene cardinal menor que κ. Vamos a estudiar el problema de si el producto de dos espacios topológicos que cumplen la condición de cadena κ cumple necesariamente la condición de cadena κ. El teorema siguiente reduce el problema al caso de conjuntos preordenados:

Teorema 8.51 *Si κ es un cardinal infinito, las afirmaciones siguientes son equivalentes:*

1. *Existen espacios topológicos con la condición de cadena κ cuyo producto no cumple la condición de cadena κ.*
2. *Existen dos c.p.o.s con la condición de cadena κ cuyo producto no cumple la condición de cadena κ.*
3. *Existen dos espacios de Hausdorff compactos con la condición de cadena κ cuyo producto no cumple la condición de cadena κ.*

Demostración: Si X e Y son espacios topológicos que cumplen 1), tomamos como $\mathbb{P}$ y $\mathbb{Q}$ los conjuntos de abiertos no vacíos de X e Y respectivamente, ordenados con la inclusión. Así dos abiertos son incompatibles si y sólo si son disjuntos, por lo que $\mathbb{P}$ y $\mathbb{Q}$ son c.p.o.s con la condición de cadena κ. Como $X \times Y$ no cumple la condición de cadena κ, existe una anticadena de cardinal κ, que podemos tomar formada por abiertos básicos, es decir, de la forma $\{p_\alpha \times q_\alpha\}_{\alpha<\kappa}$. Entonces $\{(p_\alpha, q_\alpha)\}_{\alpha<\kappa}$ es una anticadena en $\mathbb{P} \times \mathbb{Q}$.

Supongamos ahora existen c.p.o.s $\mathbb{P}$ y $\mathbb{Q}$ que cumplen 2). Sean $\mathbb{B}_1$ y $\mathbb{B}_2$ sus respectivas compleciones, que son dos álgebras de Boole completas con la condición de cadena κ. El producto $\mathbb{B}_1 \times \mathbb{B}_2$ es un c.p.o. que no cumple la condición de cadena κ, pues si $\{(p_\alpha, q_\alpha)\}_{\alpha<\kappa}$ es una anticadena en $\mathbb{P}\times\mathbb{Q}$, es claro que $\{(i(p_\alpha), i(q_\alpha))\}_{\alpha<\kappa}$ es una anticadena en $\mathbb{B}_1 \times \mathbb{B}_2$ (donde i representa en cada componente a la inmersión densa del correspondiente c.p.o. en su compleción).

Así pues, podemos partir de dos álgebras de Boole completas. Más aún, considerando los correspondientes espacios de Stone, tenemos dos espacios compactos cerodimensionales X_1 y X_2 cuyas álgebras de abiertos cerrados $\mathbb{B}_1$ y $\mathbb{B}_2$ cumplen la condición de cadena κ, mientras que $\mathbb{B}_1 \times \mathbb{B}_2$ no la cumple.

Es obvio que X_1 y X_2 cumplen la condición de cadena κ como espacios topológicos, mientras que $X_1 \times X_2$ no la cumple, pues si $\{(U_\alpha, V_\alpha)\}_{\alpha<\kappa}$ es una anticadena en $\mathbb{B}_1 \times \mathbb{B}_2$ entonces $\{U_\alpha \times V_\alpha\}_{\alpha<\kappa}$ es una familia de abiertos disjuntos en $X_1 \times X_2$.

Obviamente 3) implica 1). ∎

Demostraremos que $\mathrm{AM}(\aleph_1)$ implica que, en efecto, el producto de dos espacios topológicos (o c.p.o.s) con la c.c.n. tiene la c.c.n. Curiosamente, esto basta para concluir que el producto de cualquier familia de espacios topológicos con la c.c.n. tiene la c.c.n.:

Teorema 8.52 (AE) *Sea κ un cardinal infinito y sea $X = \prod_{i\in I} X_i$ un producto de espacios topológicos tal que, para todo $I_0 \subset I$ finito, el producto $\prod_{i\in I_0} X_i$ cumpla la condición de cadena κ^+. Entonces X cumple la condición de cadena κ^+.*

Así, si se cumple que el producto de dos espacios con la c.c.n. cumple la c.c.n., una inducción obvia implica que lo mismo vale para productos finitos, luego el teorema anterior nos da que vale para productos arbitrarios. Demostraremos este teorema a partir de un resultado puramente conjuntista:

Definición 8.53 Un *sistema Δ,* o una *familia cuasidisjunta,* de raíz r es una familia $\mathcal{F}$ de conjuntos tal que $\bigwedge xy \in \mathcal{F}(x \neq y \to x \cap y = r)$.

Teorema 8.54 (AE) *Si κ es un cardinal regular no numerable y $\mathcal{A}$ es una familia de κ conjuntos finitos, entonces existe una familia cuasidisjunta $\mathcal{F} \subset \mathcal{A}$ con $|\mathcal{F}| = \kappa$.*

Demostración: Sea $\mathcal{A}_n = \{x \in \mathcal{A} \mid |x| = n\}$. Entonces $\mathcal{A} = \bigcup_{n\in\omega} \mathcal{A}_n$. Si $|\mathcal{A}_n| < \kappa$ para todo n, también $|\mathcal{A}| < \kappa$, luego existe un $n \in \omega$ $(n > 0)$ tal que $|\mathcal{A}_n| = \kappa$. Equivalentemente, podemos suponer que todos los elementos de $\mathcal{A}$ tienen un mismo cardinal $n > 0$. Probamos el teorema por inducción sobre n. Si $n = 1$ es obvio que la propia $\mathcal{A}$ es cuasidisjunta de raíz $r = \varnothing$. Supongamos que toda familia de κ conjuntos con n elementos tiene una subfamilia cuasidisjunta de cardinal κ y veamos que lo mismo vale para familias de conjuntos de $n + 1$ elementos.

Aplicando el lema de Zorn igual concluimos que existe una familia maximal $\mathcal{M}$ de elementos de $\mathcal{A}$ disjuntos dos a dos. Si $|\mathcal{M}| = \kappa$, entonces es cuasidisjunta de raíz $\varnothing$ y ya hemos terminado. Supongamos que $|\mathcal{M}| < \kappa$. Entonces $A = \bigcup_{x\in\mathcal{M}} x$ tiene cardinal $< \kappa$ y todo $x \in \mathcal{A}$ corta a A, ya que en caso contrario $\mathcal{M} \cup \{x\}$ contradiría la maximalidad de $\mathcal{M}$. Para cada $a \in A$, sea $\mathcal{A}_a = \{x \in \mathcal{A} \mid a \in x\}$, de modo que $\mathcal{A} = \bigcup_{a\in A} \mathcal{A}_a$. Como $|A| < \kappa$, existe un $a \in A$ tal que $|\mathcal{A}_a| = \kappa$.

Sea $\mathcal{A}' = \{x \setminus \{a\} \mid x \in \mathcal{A}_a\}$. Entonces $\mathcal{A}'$ es una familia de κ conjuntos de cardinal n (notemos que la aplicación $\mathcal{A} \longrightarrow \mathcal{A}_a$ dada por $x \mapsto x \setminus \{a\}$ es biyectiva). Por hipótesis de inducción existe $\mathcal{F}' \subset \mathcal{A}'$ cuasidisjunta de raíz r' y cardinal κ, y entonces $\mathcal{F} = \{x \cup \{a\} \mid x \in \mathcal{F}'\} \subset \mathcal{A}$ es cuasidisjunta de raíz $r = r' \cup \{a\}$ y de cardinal κ. ∎

Demostración (de 8.52): Supongamos que $\{A_\alpha\}_{\alpha\in\kappa^+}$ es una familia de abiertos en X disjuntos dos a dos. Podemos suponer que son no vacíos (pues con ello a lo sumo suprimimos un elemento). Como cada uno contiene un abierto básico, no perdemos generalidad si suponemos que son abiertos básicos, es decir, $A_\alpha = \prod_{i\in I} A_{\alpha i}$, donde $A_{\alpha i}$ es abierto en X_i y el conjunto $I_\alpha = \{i \in I \mid A_{\alpha i} \neq X_i\}$ es finito.

Consideramos $\mathcal{A} = \{I_\alpha \mid \alpha \in \kappa^+\}$. Si $|\mathcal{A}| \leq \kappa$, existe un $r \in \mathcal{A}$ tal que $J = \{\alpha \in \kappa^+ \mid I_\alpha = r\}$ tiene cardinal κ^+. Si, por el contrario, $|\mathcal{A}| = \kappa^+$, por el teorema anterior contiene un sistema Δ de raíz r y cardinal κ^+. Equivalentemente, podemos tomar $J \subset \kappa^+$ de cardinal κ^+ tal que $\bigwedge\alpha\beta \in J(\alpha \neq \beta \to I_\alpha \cap I_\beta = r)$. Notemos que esto es trivialmente cierto en el primer caso.

En definitiva, reduciendo la familia dada si es necesario, no perdemos generalidad si suponemos que $\{A_\alpha\}_{\alpha\in\kappa^+}$ es una familia de abiertos disjuntos dos a dos de modo que $\bigwedge\alpha\beta \in \kappa^+(\alpha \neq \beta \to I_\alpha \cap I_\beta = r)$ (ya sea porque todos los conjuntos I_α sean iguales a r o bien porque forman un sistema Δ de raíz r). Notemos que no puede ser $r = \varnothing$, pues entonces los A_α no serían disjuntos dos a dos.

Consideremos ahora los abiertos $A^*_\alpha = \prod_{i\in r} A_{\alpha i} \subset \prod_{i\in r} X_i$. Basta observar que si $\alpha \neq \beta$, entonces $A^*_\alpha \cap A^*_\beta = \varnothing$, lo que contradice que el producto finito cumpla la condición de cadena κ. En efecto, tenemos que

$$\varnothing = A_\alpha \cap A_\beta = \prod_{i\in I}(A_{\alpha i} \cap A_{\beta i}),$$

luego existe un $i \in I$ tal que $A_{\alpha i} \cap A_{\beta i} = \varnothing$, pero necesariamente $i \in I_\alpha \cap I_\beta = r$, pues de lo contrario $A_{\alpha i} \cap A_{\alpha' i}$ es uno de los dos abiertos $A_{\alpha i}$ o $A_{\beta i}$, que son no vacíos. Por lo tanto $A^*_\alpha \cap A^*_\beta = \varnothing$. ∎

Condiciones de cadena y el axioma de Martin Pasamos ya a demostrar que $\mathrm{AM}(\aleph_1)$ implica que el producto de espacios topológicos (o c.p.o.s) con la condición de cadena numerable tiene la condición de cadena numerable. Para ello introducimos el concepto siguiente:

Definición 8.55 Diremos que un c.p.o. $\mathbb{P}$ cumple la *condición de cadena numerable fuerte* si todo conjunto $W \subset \mathbb{P}$ no numerable contiene un subconjunto Z no numerable con todos sus elementos compatibles dos a dos.

Obviamente, la condición de cadena numerable fuerte implica la condición de cadena numerable. Por otra parte:

Teorema 8.56 *Si $\mathbb{P}$ y $\mathbb{Q}$ son c.p.o.s de modo que $\mathbb{P}$ cumple la condición de cadena numerable fuerte y $\mathbb{Q}$ cumple la condición de cadena numerable, entonces $\mathbb{P}\times\mathbb{Q}$ cumple la condición de cadena numerable.*

DEMOSTRACIÓN: Sea $W\subset\mathbb{P}\times\mathbb{Q}$ un conjunto no numerable. Consideremos el conjunto $W_0=\{p\in\mathbb{P}\mid \bigvee q\in\mathbb{Q}\ (p,q)\in W\}$. Si W_0 es numerable existe un $p\in\mathbb{P}$ tal que $W_p=\{q\in\mathbb{Q}\mid (p,q)\in W\}$ es no numerable. Como $\mathbb{Q}$ cumple la condición de cadena numerable existen dos condiciones compatibles en W_p, digamos q_1 y q_2. Así (p,q_1) y (p,q_2) son condiciones compatibles en W.

Si, por el contrario, W_0 es no numerable, existe $Z\subset W_0$ no numerable cuyos elementos son compatibles dos a dos. Para cada $p\in Z$, sea $q_p\in\mathbb{Q}$ tal que $(p,q_p)\in W$. Si $q_{p_1}=q_{p_2}$ para ciertos p_1, $p_2\in Z$ distintos, entonces (p_1,q_{p_1}) y (p_2,q_{p_2}) son condiciones compatibles en W, mientras que si la aplicación $p\mapsto q_p$ es inyectiva entonces el conjunto $\{q_p\mid p\in Z\}$ es no numerable, luego existen p_1, $p_2\in Z$ distintos tales que q_{p_1} y q_{p_2} son compatibles. De nuevo (p_1,q_{p_1}) y (p_2,q_{p_2}) son condiciones compatibles en W.

En cualquier caso tenemos que W no puede ser una anticadena, luego $\mathbb{P}\times\mathbb{Q}$ cumple la condición de cadena numerable. ∎

Ahora ya podemos probar:

Teorema 8.57 *Suponiendo* $\mathrm{AM}(\aleph_1)$ *se cumple:*

1. *Todo c.p.o. con la condición de cadena numerable cumple la condición de cadena numerable fuerte.*
2. *Todo producto de c.p.o.s con la condición de cadena numerable cumple la condición de cadena numerable.*
3. *El producto de cualquier familia de espacios topológicos con la condición de cadena numerable cumple la condición de cadena numerable.*

DEMOSTRACIÓN: 2) es consecuencia de 1) y del teorema anterior, mientras que 3) se sigue de 2) y de los teoremas 8.51 y 8.52.

Sea $\mathbb{P}$ un c.p.o. con la condición de cadena numerable y $W=\{q_\alpha\}_{\alpha<\omega_1}$ un subconjunto de $\mathbb{P}$. Veamos que existe $p_0\in W$ tal que todo $p\le p_0$ es compatible con una cantidad no numerable de elementos de W. En caso contrario, para cada $\alpha<\omega_1$ existe $\alpha<\beta<\omega_1$ y $r_\alpha\le q_\alpha$ de modo que $r_\alpha\perp q_\gamma$ si $\beta<\gamma<\omega_1$, y esto nos permite construir por recurrencia una anticadena $\{r_\alpha\}_{\alpha<\omega_1}$, contradicción.

Fijado, pues, p_0, para cada $\alpha<\omega_1$ definimos

$$D_\alpha=\{p\in\mathbb{P}\mid p\le p_0\wedge\bigvee\gamma<\omega_1(\alpha\le\gamma\wedge p\le q_\gamma)\}.$$

Se cumple que D_α es denso bajo p_0, es decir, que para toda condición $t\le p_0$ existe $p\in D_\alpha$ tal que $p\le t$.

En efecto, si $t\le p_0$ entonces t es compatible con algún q_γ, para $\gamma\ge\alpha$, luego existe un $p\in\mathbb{P}$ tal que $p\le t$ y $p\le q_\gamma$, es decir, $p\in D_\alpha$ y $p\le t$.

El conjunto $\mathbb{P}_0 = \{p \in \mathbb{P} \mid p \leq p_0\}$ es un c.p.o. en el que los conjuntos D_α son densos, y obviamente cumple la condición de cadena numerable. Por $\mathrm{AM}(\aleph_1)$ existe un filtro G_0 en $\mathbb{P}_0$ que corta a todos los conjuntos D_α. Sea

$$G = \{p \in \mathbb{P} \mid \bigvee p' \in G_0 \; p' \leq p\}.$$

Claramente G es un filtro en $\mathbb{P}$ que contiene a p_0 y corta a todos los conjuntos D_α. Además $Z = G \cap W$ es un subconjunto de W formado por condiciones compatibles dos a dos, luego basta probar que es no numerable. En efecto, si $\alpha < \omega_1$ existe $p \in G \cap D_\alpha$, luego existe $\alpha \leq \gamma < \omega_1$ tal que $p \leq q_\gamma$, luego $q_\gamma \in G$. Así pues, el conjunto $\{\gamma < \omega_1 \mid q_\gamma \in G\}$ no está acotado, luego no es numerable. ∎

Así pues, $\mathrm{AM} + 2^{\aleph_0} > \aleph_1$ implica que el producto de espacios topológicos con la c.c.n. cumple la c.c.n.

Condiciones de cadena y la hipótesis del continuo A continuación probaremos que negar la hipótesis del continuo es necesario para probar la consistencia de que el producto de espacios con la c.c.n. cumple la c.c.n., pues la hipótesis del continuo implica justo lo contrario:

Definición 8.58 Si A y B son conjuntos cualesquiera, usaremos la notación

$$A \otimes B = \{\{a, b\} \mid a \in A \wedge b \in B\}$$

Si κ es un cardinal infinito y $K \subset [\kappa]^2$, llamaremos

$$\mathbb{P}(\kappa, K) = \{F \in [\kappa]^{<\omega} \mid [F]^2 \subset K\},$$

y lo consideraremos como conjunto parcialmente ordenado con la relación inversa de la inclusión.

Notemos que si $\alpha \in \kappa$, entonces $[\{\alpha\}]^2 = \varnothing$, por lo que se cumple trivialmente que $\{\alpha\} \in \mathbb{P}(\kappa, K)$. Si $K_1 \cap K_2 = \varnothing$, entonces $\mathbb{P}(\kappa, K_1) \times \mathbb{P}(\kappa, K_2)$ no cumple la c.c.κ, pues $\{(\{\alpha\}, \{\alpha\}) \mid \alpha \in \kappa\}$ es una anticadena.

Teorema 8.59 *Sea κ un cardinal infinito, A un conjunto, $\{I_\alpha\}_{\alpha<\kappa}$ una familia de conjuntos de cardinal κ y, para cada $\alpha < \kappa$, sea $\{E_i^\alpha\}_{i \in I_\alpha}$ una familia de subconjuntos finitos de A tal que, para todo $a \in A$, el conjunto $\{i \in I_\alpha \mid a \in E_i^\alpha\}$ es finito. Entonces existe una familia $\{A_\delta\}_{\delta<\kappa}$ de subconjuntos de A disjuntos dos a dos tal que*

$$\bigwedge \alpha\delta < \kappa \; |\{i \in I_\alpha \mid E_i^\alpha \subset A_\delta\}| = \kappa.$$

Demostración: Sea $f : \kappa^3 \longrightarrow \kappa$ biyectiva. Vamos a construir una sucesión $\{i_\eta\}_{\eta<\kappa}$ por recurrencia de modo que si $\eta = f(\alpha, \delta, \epsilon)$, entonces $i_\eta \in I_\alpha$ y, si llamamos $E_\eta = E_{i_\eta}^\alpha$, los conjuntos E_η son disjuntos dos a dos.

Supuesto definido $\{i_\beta\}_{\beta<\eta}$, tenemos que $E = \bigcup_{\beta<\eta} E_\beta$ tiene cardinal $\leq |\eta| < \kappa$ luego, si $\eta = f(\alpha, \delta, \epsilon)$, el conjunto

$$\{i \in I_\alpha \mid E_i^\alpha \cap E \neq \varnothing\}$$

tiene también cardinal $< \kappa$ (porque cada elemento de E corta a un número finito de conjuntos E_i^α). Como $|I_\alpha| = \kappa$, podemos tomar $i_\eta \in I_\alpha$ tal que $E_{i_\eta}^\alpha \cap E = \varnothing$.

Así pues, tenemos construida la sucesión indicada y, si hacemos $i^\alpha_{\delta\epsilon} = i_{f(\alpha,\delta,\epsilon)}$, tenemos que los conjuntos $E^\alpha_{i^\alpha_{\delta\epsilon}}$ son disjuntos dos a dos. Ahora basta definir

$$A_\delta = \bigcup_{\alpha,\epsilon<\kappa} E^\alpha_{i^\alpha_{\delta\epsilon}},$$

y claramente se cumple lo pedido. ∎

Teorema 8.60 (Galvin, Laver) *Si κ es un cardinal infinito tal que $2^\kappa = \kappa^+$, entonces existen conjuntos parcialmente ordenados $\mathbb{P}_1$ y $\mathbb{P}_2$ que cumplen la c.c.c.κ^+ pero $\mathbb{P}_1 \times \mathbb{P}_2$ no la cumple.*

Demostración: Por la observación previa al teorema anterior basta encontrar conjuntos disjuntos K_1, $K_2 \subset [\kappa^+]^2$ tales que $\mathbb{P}(\kappa^*, K_i)$ satisfagan la c.c.c.κ^+.

Para cada $\gamma < \kappa^+$ vamos a definir conjuntos disjuntos $K_1(\gamma), K_2(\gamma) \subset \gamma$ y luego definiremos

$$K_i = \{\{\beta,\gamma\} \in [\kappa^+]^2 \mid \beta \in K_i(\gamma)\}.$$

Sea $\{X_\eta\}_{\eta<\kappa^+}$ una enumeración de todas las sucesiones de longitud κ de subconjuntos finitos de κ^+ disjuntos dos a dos, de modo que $X_\eta = \{x^\epsilon_\eta\}_{\epsilon<\kappa}$. Notemos que el número de tales sucesiones es

$$\leq ([\kappa^+]^{<\omega})^\kappa = (\kappa^+)^\kappa = 2^\kappa\kappa^+ = \kappa^+,$$

donde hemos usado que $2^\kappa = \kappa^+$, y la otra desigualdad es cierta siempre.

Vamos a construir recurrentemente los conjuntos $K_i(\gamma)$ de modo que se cumpla lo siguiente:

(∗) Si $i \in \{1,2\}$, $\eta < \gamma$, $\bigcup_{\epsilon<\kappa} x^\epsilon_\eta \subset \gamma$, $a \in [\gamma]^{<\omega}$ y $|\{\epsilon < \kappa \mid x^\epsilon_\eta \otimes a \subset K_i\}| = \kappa$, entonces $|\{\epsilon < \kappa \mid x^\epsilon_\eta \otimes a \subset K_i \wedge x^\epsilon_\eta \subset K_i(\gamma)\}| = \kappa$ o, equivalentemente,

$$|\{\epsilon < \kappa \mid x^\epsilon_\eta \otimes (a \cup \{\gamma\}) \subset K_i\}| = \kappa.$$

Supongamos definidos $K_1(\beta)$ y $K_2(\beta)$ para todo $\beta < \gamma$ que cumplan la propiedad anterior cambiando γ por β. Aquí hay que entender que $x^\epsilon_\eta \otimes a \subset K_i$ significa que si $\{u,v\} \in x^\epsilon_\eta \otimes a$, con $u < v < \beta$, entonces $u \in K(v)$.

Sea $\{(i_\alpha, \eta_\alpha, a_\alpha)\}_{\alpha<\kappa}$ una enumeración de todas las ternas que cumplan (∗), con repeticiones, si hubiera menos de κ. Aplicamos el teorema anterior con $A = \gamma$, $I_\alpha = \{\epsilon < \kappa \mid x^\epsilon_{\eta_\alpha} \otimes a_\alpha \subset K_{i_\alpha}\}$ y $E^\alpha_\epsilon = x^\epsilon_{\eta_\alpha}$ (que para un α fijo son conjuntos disjuntos dos a dos). Obtenemos entonces κ conjuntos, aunque nos basta tomar dos de ellos, $K_1(\gamma)$ y $K_2(\gamma) \subset \gamma$, disjuntos, que cumplen (∗).

Con esto tenemos definidos K_1 y K_2. Veamos ahora que los conjuntos parcialmente ordenados $\mathbb{P}_i = \mathbb{P}(\kappa^+, K_i)$ cumplen la c.c.c.κ^+. Fijamos $i \in \{1,2\}$ y consideremos una familia $\{E_\epsilon\}_{\epsilon<\kappa^+}$ de elementos de $\mathbb{P}_i$. Tenemos que probar que existen $\epsilon < \epsilon' < \kappa^+$ tales que $E_\epsilon \cup E_{\epsilon'} \in \mathbb{P}_i$, es decir, que $[E_\epsilon \cup E_{\epsilon'}]^2 \subset K_i$.

Por el lema de los sistemas Δ (teorema 8.54) podemos suponer que existe $E \subset \kappa^+$ finito tal que $E_\epsilon \cap E_{\epsilon'} = E$ para todo $\epsilon < \epsilon' < \kappa^+$. Entonces los conjuntos $F_\epsilon = E_\epsilon \setminus E$ son disjuntos dos a dos. Como

$$[E_\epsilon \cup E_{\epsilon'}]^2 = [E_\epsilon]^2 \cup [E_{\epsilon'}]^2 \cup F_\epsilon \otimes F_{\epsilon'},$$

basta encontrar $\epsilon < \epsilon' < \kappa^+$ tales que $F_\epsilon \otimes F_{\epsilon'} \subset K_i$.

Sea $\eta < \kappa^+$ tal que $x^\epsilon_\eta = F_\epsilon$, para todo $\epsilon < \kappa$, sea $\gamma_0 < \kappa^+$ tal que $\bigcup_{\epsilon<\kappa} x^\epsilon_\eta \subset \gamma_0$ y $\eta < \gamma_0$. Como los conjuntos $\{F_\epsilon\}_{\epsilon<\kappa^+}$ son disjuntos dos a dos, existe un $\epsilon' < \kappa^+$ tal que $F_{\epsilon'} \cap \gamma_0 = \varnothing$. Digamos que $F_{\epsilon'} = \{\gamma_1 < \cdots < \gamma_n\}$. Aplicamos $(*)$ n veces, con $(\gamma, a) = (\gamma_1, \varnothing), (\gamma_2, \{\gamma_1\}), \ldots, (\gamma_n, \{\gamma_1, \ldots, \gamma_{n-1}\})$. Concluimos que $|\{\epsilon < \kappa \mid x^\epsilon_\eta \otimes F_{\epsilon'} \subset K_i\}| = \kappa$. En particular, tomando cualquier ϵ de este conjunto, tenemos que $\epsilon < \epsilon'$ y $F_\epsilon \otimes F_{\epsilon'} \subset K_i$. ∎

Así pues:

Teorema 8.61 *Si κ es un cardinal infinito y $2^\kappa = \kappa^+$, existen dos espacios topológicos compactos de Hausdorff con la c.c.κ^+ cuyo producto no cumple la c.c.κ^+.*

Condiciones de cadena sin axiomas adicionales Con el axioma de Martin sólo hemos podido probar la consistencia de que el producto de c.p.o.s con la c.c.n. cumple la c.c.n., pero no un resultado análogo general para c.p.o.s con la c.c.κ debido a que el axioma de Martin sólo se aplica a c.p.o.s con esta restricción. Ahora probaremos que esto es necesariamente así, porque existen cardinales κ para los que es posible construir c.p.o.s con la c.c.κ cuyo producto no la cumplen sin necesidad de axiomas adicionales. Vamos a probarlo concretamente para $\kappa = \operatorname{cf} \mathfrak{c}$, pero generalizando los argumentos que vamos a dar es posible probar que existe una clase propia de cardinales con esta propiedad.

Sea κ un cardinal infinito y P^n_κ el conjunto de todas las n-tuplas de elementos de κ sin componentes repetidas. Diremos que $A \subset P^n_\kappa$ es *cofinal* (en P^n_κ) si para todo $\alpha < \kappa$ existe $s \in A$ tal que $\alpha < \min_{i<n} s_i$.

Teorema 8.62 *Existe una aplicación inyectiva $r : \mathfrak{c} \longrightarrow \mathbb{R}$ tal que para todo $n < \omega$ no nulo, todo $A \subset P^n_\mathfrak{c}$ cofinal, y todo $s \in {}^n2$, existen x, $y \in A$ tales que, para todo $i < n$, se cumple*

$$r(x_i) < r(y_i) \leftrightarrow s_i = 0.$$

Demostración: Para cada $n < \omega$ no nulo, $\mathbb{R}^n$ tiene una base numerable, luego la cantidad total de abiertos es $\mathfrak{c}$, luego la cantidad total de subconjuntos G_δ es también $\mathfrak{c}$. Para cada uno de estos conjuntos G_δ, digamos G, cada aplicación continua $G \longrightarrow \mathbb{R}$ está determinada por su restricción a un subconjunto denso numerable, luego hay como máximo $\mathfrak{c}$ aplicaciones continuas, por lo que podemos considerar una enumeración $\{f_\alpha\}_{\alpha<\mathfrak{c}}$ del conjunto de todas las aplicaciones continuas $f_\alpha : G_\alpha \subset \mathbb{R}^{n_\alpha} \longrightarrow \mathbb{R}$, donde G_α es un subconjunto G_δ en un cierto $\mathbb{R}^{n_\alpha}$.

Supuesta definida $r|_\beta$, el conjunto

$$r[\beta] \cup \bigcup_{\alpha<\beta} f_\alpha[r[\beta]^{n_\alpha}]$$

es una unión de $|\beta+1|$ conjuntos de cardinal $\leq \aleph_0|\beta|$, luego tiene cardinal $\leq \aleph_0|\beta| < \mathfrak{c}$, luego podemos elegir r_β en el complementario en $\mathbb{R}$ de dicha unión. Con esto se cumple que r es inyectiva y, si $\alpha < \beta$,

$$f_\alpha[r[\beta]^{n_\alpha}] \cap r[\mathfrak{c}] \subset r[\beta].$$

Veamos que r cumple lo requerido. En caso contrario, sea n el mínimo número natural que lo incumple. Claramente $n \geq 2$. Sea $A \subset P^n_\mathfrak{c}$ cofinal y $s \in {}^n2$ tales que no existan $x, y \in A$ para los que $r(x_i) < r(y_i) \leftrightarrow s_i = 0$.

A cada $x \in A$ podemos asignarle la única permutación σ_x de n que ordena sus componentes, es decir, la que hace que $\sigma_x \circ x$ sea creciente. Si llamamos A_σ al conjunto de todos los elementos de A cuya permutación asociada es σ, tenemos una descomposición de A en unión disjunta de un número finito de subconjuntos. Necesariamente, alguno de ellos tiene que ser cofinal, luego no perdemos generalidad si suponemos que $A = A_\sigma$, para cierta permutación σ. A su vez, cambiando s por $\sigma \circ s$ podemos suponer que todas las n-tuplas de A son crecientes.

Similarmente, podemos construir un subconjunto cofinal $A_0 \subset A$ cuyas n-tuplas no tengan coordenadas en común (para cada $\beta < \mathfrak{c}$, elegimos $x_\beta \in A$ cuyas coordenadas sean mayores que β y mayores que las coordenadas de todos los x_α, con $\alpha < \beta$). Por lo tanto, también podemos suponer que las n-tuplas de A no tienen coordenadas en común.

Sea $B = \{x|_{n-1} \mid x \in A\} \subset P^{n-1}_\mathfrak{c}$ y sea $f : B \longrightarrow \mathfrak{c}$ la aplicación dada por $f(x|_{n-1}) = x(n-1)$. Esto es correcto porque las n-tuplas de A no tienen coordenadas repetidas. Notemos que B es cofinal en $P^{n-1}_\mathfrak{c}$.

En general, para cada $C \subset P^{n-1}_\mathfrak{c}$, llamaremos $\tilde{C} = \{x \circ r \mid x \in C\} \subset \mathbb{R}^{n-1}$. Como r es inyectiva, la aplicación $C \longrightarrow \tilde{C}$ dada por $x \mapsto \tilde{x} = x \circ r$ es biyectiva. Sea $\tilde{f} : \tilde{B} \longrightarrow \mathbb{R}$ la aplicación dada por $\tilde{f}(\tilde{x}) = r(f(x))$.

Para cada $p \in \mathbb{R}^{n-1}$, sea $\omega(p) = \bigcap_{p\in U} \overline{\tilde{f}[\tilde{B} \cap U]}$, donde U recorre los abiertos de $\mathbb{R}^{n-1}$ que contienen a p.

Vamos a probar que $B_0 = \{z \in B \mid |\omega(\tilde{z})| \geq 2\}$ no es cofinal en $P^{n-1}_\mathfrak{c}$. Supongamos que sí que lo es.

Si $z \in B_0$, entonces $\tilde{f}(\tilde{z}) \in \omega(\tilde{z})$, pero existe otro $r \in \omega(\tilde{z})$ distinto de $\tilde{f}(\tilde{z})$. Podemos dividir B_0 en unión de dos conjuntos, el formado por los $z \in B_0$ tales que existe un $r \in \omega(\tilde{z})$ con $\tilde{f}(\tilde{z}) < r$ y su complementario, para cuyos elementos existe un $r \in \omega(\tilde{z})$ con $r < \tilde{f}(\tilde{z})$. Uno de los dos tiene que ser cofinal. Vamos a suponer que lo es el primero, llamémoslo B_1, pues si lo es el segundo podemos razonar análogamente.

Para cada $z \in B_1$ existen un $r \in \omega(\tilde{z})$ y un $q_z \in \mathbb{Q}$ tales que $\tilde{f}(\tilde{z}) < q_z < r$. Así, podemos descomponer $B_1 = \bigcup_{q\in\mathbb{Q}} B_q$, donde B_q está formado por los $z \in B_1$ tales que $q_z = q$.

Como $\mathfrak{c}$ tiene cofinalidad no numerable, uno de los conjuntos B_q tiene que ser cofinal en $P_{\mathfrak{c}}^{n-1}$. Llamémoslo B_2. Así, para cada $z \in B_2$, existe un $r \in \omega(\tilde{z})$ tal que $\tilde{f}(\tilde{z}) < q < r$.

Vamos a suponer que $s_{m-1} = 0$. El caso opuesto se trata análogamente. Por la minimalidad de n, existen u, $v \in B_2$ tales que, para todo $i < n-1$, $r(u_i) < r(v_i) \leftrightarrow s_i = 0$. Sea

$$U = \{z \in \mathbb{R}^{n-1} \mid \bigwedge i \in n-1(\tilde{u}_i < z_i \leftrightarrow s_i = 0)\}.$$

Claramente U es abierto en $\mathbb{R}^{n-1}$ y contiene a $\tilde{v}$. Además, si $z \in B$ cumple que $\tilde{z} \in \tilde{B} \cap U$, entonces $(u_0, \ldots, u_{n-1}, f(u))$, $(z_0, \ldots, z_{n-2}, f(z)) \in A$, y no pueden cumplir la propiedad del enunciado, pero la cumplen para $i < n-1$, luego necesariamente tiene que fallar para $i = n-1$, es decir, tiene que ser $\tilde{f}(\tilde{z}) < \tilde{f}(\tilde{u})$ (donde usamos también que las n-tuplas de A no tienen coordenadas en común).

Así pues, si $z \in \tilde{B} \cap U$, se cumple que $\tilde{f}(z) < \tilde{f}(\tilde{u}) < q$, luego

$$\omega(\tilde{v}) \subset \overline{\tilde{f}[\tilde{B} \cap U]} \subset]-\infty, q]\,,$$

cuando, por otra parte, debería haber un $r \in \omega(\tilde{v})$ tal que $q < r$, contradicción.

Si $z \in B$, entonces $\tilde{f}(\tilde{z}) \in \omega(\tilde{z})$, luego $|\omega(\tilde{z})| \geq 1$, y acabamos de probar que el conjunto de los z para los que $|\omega(\tilde{z})| \geq 2$ no es cofinal, luego el conjunto $B^* = \{z \in B_0 \mid \omega(\tilde{z}) = \{\tilde{f}(\tilde{z})\}\}$ es cofinal en $P_{\mathfrak{c}}^{n-1}$.

Ahora observamos que $\tilde{f}$ es continua en $\tilde{B}^*$. En efecto, si una sucesión $\{x_i\}_{i\in\omega}$ en $\tilde{B}^*$ converge a $p \in \tilde{B}^*$, entonces, para todo entorno U de p en $\mathbb{R}^{n-1}$, existe un k tal que, si $i \geq k$, entonces $x_i \in \tilde{B} \cap U$, luego $\tilde{f}(x_i) \in \tilde{f}[\tilde{B} \cap U]$, luego

$$\operatorname{lím\,sup}_i \tilde{f}(x_i), \quad \operatorname{lím\,inf}_i \tilde{f}(x_i) \in \overline{\tilde{f}[\tilde{B} \cap U]},$$

luego ambos límites están en $\omega(p) = \{\tilde{f}(p)\}$, luego $\lim_i \tilde{f}(x_i) = \tilde{f}(p)$. Por el teorema de Lavrentieff [T 9.29], $\tilde{f}$ se extiende a una función continua en un G_δ, es decir, existe un $\alpha < \mathfrak{c}$ tal que $\tilde{B}^* \subset G_\alpha \subset \mathbb{R}^{n-1}$ y $\tilde{f}$ se extiende hasta la función continua $f_\alpha : G_\alpha \longrightarrow \mathbb{R}$.

Ahora tomamos cualquier $x \in B^*$ y llamamos $\beta = f(x)$. Así tenemos que $(x_0, \ldots, x_{n-2}, \beta) \in A$, luego $x \subset {}^{n-1}\beta$ y

$$r(\beta) = r(f(x)) = \tilde{f}(\tilde{x}) = f_\alpha(\tilde{x}) \in f_\alpha[r[\beta]^{n-1}] \cap r[\mathfrak{c}] \subset r[\beta],$$

y así tenemos una contradicción. ∎

No podemos aplicar directamente el teorema anterior debido a que $\mathfrak{c}$ puede ser singular, y necesitamos considerar un cardinal regular. Para arreglar esto basta un pequeño retoque:

Teorema 8.63 *Sea $\kappa = \operatorname{cf}\mathfrak{c}$. Existe una aplicación inyectiva $r : \kappa \longrightarrow \mathbb{R}$ tal que, para todo $n < \omega$ no nulo, toda familia $A \subset P_\kappa^n$ formada por n-tuplas sin componentes en común y con $|A| = \kappa$ y todo $s \in {}^n2$, existen x, $y \in A$ tales que, para todo $i < n$, se cumple*

$$r(x_i) < r(y_i) \leftrightarrow s_i = 0.$$

DEMOSTRACIÓN: Sea $r' : \mathfrak{c} \longrightarrow \mathbb{R}$ la aplicación dada por el teorema anterior. Basta definir $r = i \circ r'$, donde $i : \kappa \longrightarrow \mathfrak{c}$ es una aplicación cofinal creciente. En efecto, de este modo, si $A \subset P_\kappa^n$ cumple las condiciones del enunciado, es cofinal en P_κ^n, pues si existiera $\alpha < \kappa$ tal que todo $s \in A$ tuviera una componente menor que α, la aplicación $A \longrightarrow \alpha$ que a cada $s \in A$ le asigna su mínima componente sería inyectiva, lo cual es imposible. Por consiguiente, $A' = \{s \circ i \mid s \in A\}$ es cofinal en $P_\mathfrak{c}^n$, y el hecho de que A' cumpla la conclusión del teorema anterior implica que A cumple lo requerido. ∎

Teorema 8.64 (Todorčević) *Si $\kappa = \operatorname{cf} \mathfrak{c}$, existen dos c.p.o.s que cumplen la c.c.κ cuyo producto no la cumple.*

DEMOSTRACIÓN: Sea $r : \kappa \longrightarrow \mathbb{R}$ en las condiciones del teorema anterior y sea $P = \{(r(2\alpha), r(2\alpha+1)) \mid \alpha < \kappa\}$. Consideramos a P como conjunto parcialmente ordenado con el orden producto:

$$(x, y) \leq (x', y') \qquad \text{si y sólo si} \qquad x \leq x', \quad y \leq y'.$$

Llamamos $\mathbb{P}_0$ al conjunto de las cadenas finitas en P (es decir, de los subconjuntos finitos de pares comparables dos a dos), mientras que $\mathbb{P}_1$ es el conjunto de todas las anticadenas finitas en P (conjuntos finitos de pares incomparables dos a dos). Consideramos en ambos conjuntos el orden $p \leq q$ si y sólo si $q \subset p$.

Es claro que $\mathbb{P}_0 \times \mathbb{P}_1$ no cumple la condición de cadena κ, pues

$$A = \{(\{p\}, \{p\}) \mid p \in P\}$$

es una anticadena de cardinal κ. En efecto, si $p_1 \neq p_2$ son dos elementos de P, una extensión común de $(\{p_1\}, \{p_1\})$ y $(\{p_2\}, \{p_2\})$ tendría que ser de la forma (s, t), con $p_1, p_2 \in s \cap t$, con lo que p_1 y p_2 tendrían que ser comparables e incompatibles a la vez.

Falta probar que $\mathbb{P}_0$ y $\mathbb{P}_1$ cumplen la c.c.κ. Para ello tomamos un conjunto $A \subset \mathbb{P}_i$ de cardinal $\mathfrak{c}$, y vamos a ver que no es una anticadena. Los elementos de A son subconjuntos finitos de P. Por el lema de los sistemas Δ (teorema 8.54) podemos suponer que A es una familia cuasidisjunta de raíz r. El conjunto A_0 que resulta de quitar la raíz a todos los elementos de A sigue teniendo cardinal κ y sus elementos siguen estando en $\mathbb{P}_i$. Además, si probamos que A_0 no es una anticadena, tampoco lo será A.

En efecto, supongamos que a, $b \in A_0$ son compatibles. Esto significa que todos los elementos de $a \cup b$ son comparables / incomparables, pero entonces todos los elementos de $a \cup b \cup r$ también son comparables / incomparables, porque, como $a \cup r$, $b \cup r \in \mathbb{P}_i$, todo elemento de r es comparable / incomparable con todo elemento de a y de b, luego $a \cup r$ y $b \cup r$ son elementos compatibles de A.

Por lo tanto, podemos suponer que los elementos de A son disjuntos dos a dos. Si descomponemos A en unión de los conjuntos de elementos de cardinal n, para cada n, alguno de estos conjuntos tiene que tener cardinal κ, luego no perdemos generalidad si suponemos que todos los elementos de A tienen un mismo cardinal n.

Ahora, un elemento $p \in A$ está formado por n pares, cuyas componentes son $2n$ números reales distintos. Podemos asociarle $2n$ intervalos disjuntos dos a dos de extremos racionales de modo que cada uno contenga exactamente una componente de p. Esto nos divide a A en una cantidad numerable de subconjuntos, uno de los cuales tendrá cardinal κ, luego podemos suponer que existen intervalos disjuntos $I_0, \ldots, I_{2n-1}$ en $\mathbb{R}$ de modo que cada $p \in A$ tiene exactamente una coordenada en cada uno de estos intervalos.

Así, cada $p \in A$ está determinado por una $2n$-tupla de ordinales

$$\alpha_0^p < \cdots < \alpha_{2n-1}^p < \kappa,$$

con α_{2k}^p sea par y $\alpha_{2k+1}^p = \alpha_{2k}^p + 1$, de modo que

$$p = \{(r(\alpha_0^p), r(\alpha_1^p)), \ldots, (r(\alpha_{2n-2}^p), r(\alpha_{2n-1}^p))\}.$$

A cada p podemos asociarle la permutación σ_p que cumple $r(\alpha_i^p) \in I_{\sigma(i)}$ y con esto partimos A en un número finito de subconjuntos disjuntos. Uno de ellos tendrá cardinal κ, luego podemos suponer que σ_p es la misma permutación para todo $p \in A$. Renumerando los intervalos podemos suponer que $r(\alpha_i^p) \in I_i$ para todo $p \in A$ y todo $i < 2n$.

Usaremos la notación $I < J$ para indicar que todos los puntos de I son menores que todos los puntos de J. Si los intervalos pares siguen la ordenación

$$I_{2k_0} < \cdots < I_{2(k_n-1)},$$

en el caso de $\mathbb{P}_0$, para que los elementos de A estén realmente en $\mathbb{P}_0$, los intervalos impares deben seguir la misma ordenación:

$$I_{2k_0+1} < \cdots < I_{2(k_n-1)+1}.$$

Si llamamos $\tilde{A}$ al conjunto de las $2n$-tuplas de ordinales asociadas a los elementos de A, basta tomar dos de ellas (correspondientes a elementos $p, q \in A$) que cumplan $\alpha_i^p < \alpha_i^q$ para todo i, y entonces p y q son compatibles.

Similarmente, en el caso de $\mathbb{P}_1$, la ordenación de los intervalos impares debe ser la opuesta:

$$I_{2(k_n-1)+1} < \cdots < I_{2k_0+1},$$

y basta tomar $p, q \in A$ de modo que sus $2n$-tuplas asociadas cumplan

$$\alpha_{2i}^p < \alpha_{2i}^q, \qquad \alpha_{2i+1}^p > \alpha_{2i+1}^q$$

para que p y q sean compatibles. ∎

Por el teorema 8.51, tenemos también que existen dos espacios de Hausdorff compactos que cumplen la c.c.cf $\mathfrak{c}$ cuyo producto no la cumple.

8.5 Ejemplo: Intercambio de integrales

Terminamos con una aplicación al análisis matemático de los resultados sobre los cardinales relacionados con la medida de Lebesgue que hemos visto en la sección 8.2. Empezamos recordando el enunciado del teorema de Fubini[4] (particularizado a la medida de Lebesgue en $\mathbb{I} = [0, 1]$):

Teorema 8.65 (Teorema de Fubini) *Sea $f : \mathbb{I} \times \mathbb{I} \longrightarrow \mathbb{R}$ una función integrable. Entonces:*

1. *Las funciones $x \mapsto f(x, y)$, $y \mapsto f(x, y)$ son integrables para casi todo y, $x \in \mathbb{I}$, respectivamente.*

2. *Las funciones*

$$\int_0^1 f(x, y)\, dy, \qquad \int_0^1 f(x, y)\, dx$$

están definidas y son integrables para casi todo x, $y \in \mathbb{I}$, respectivamente, y se cumple

$$\int_{\mathbb{I}^2} f(x, y)\, dxdy = \int_0^1 \left(\int_0^1 f(x, y)\, dy \right) dx = \int_0^1 \left(\int_0^1 f(x, y)\, dx \right) dy.$$

Ahora vamos a plantear una variante:

¿Teorema? *Sea $f : \mathbb{I} \times \mathbb{I} \longrightarrow \mathbb{R}$ una función que cumpla:*

1. *Las funciones $x \mapsto f(x, y)$, $y \mapsto f(x, y)$ son integrables para casi todo y, $x \in \mathbb{I}$, respectivamente.*

2. *Las funciones*

$$x \mapsto \int_0^1 f(x, y)\, dy, \qquad y \mapsto \int_0^1 f(x, y)\, dx$$

son integrables en $\mathbb{I}$.

Entonces

$$\int_0^1 \left(\int_0^1 f(x, y)\, dy \right) dx = \int_0^1 \left(\int_0^1 f(x, y)\, dx \right) dy.$$

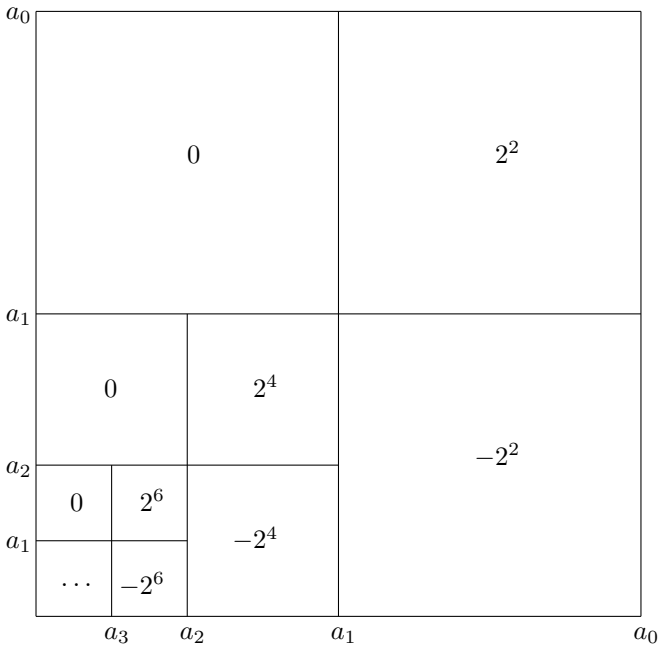
Sucede que este "resultado" es falso. Veamos un contraejemplo:

[4] Véase [T B.41].

Ejemplo Llamamos $a_n = 2^{-n}$. Para cada $n > 0$ y $x \in]a_n, a_{n-1}[$, definimos

$$f(x,y) = \begin{cases} -2^{2n} & \text{si } 0 \le y < a_n, \\ 2^{2n} & \text{si } a_n \le y < a_{n-1}, \\ 0 & \text{si } a_{n-1} \le y \le 1, \end{cases}$$

y $f(0,y) = 0$, para $0 \le y \le 1$.



Así, en los cuadrados de la figura situados sobre la diagonal, f toma los valores sucesivos 2^2, 2^4, 2^6,..., en los cuadrados situados bajo la diagonal toma esos mismos valores, pero negativos, y en los cuadrados situados sobre la diagonal vale 0.

Es obvio que cada función $y \mapsto f(x,y)$ es integrable, pues es una suma finita de funciones características de intervalos multiplicadas por coeficientes. Concretamente, si $y \in]a_n, a_{n-1}[$, tenemos que

$$\int_0^1 f(x,y)\,dx = 2^{2n}2^{-n} - (2^2 2^{-1} + 2^4 2^{-2} + \cdots + 2^{2(n-1)}2^{-(n-1)}) = 2.$$

Por otra parte, la función $x \mapsto f(x,y)$ es la suma de dos funciones características de dos intervalos de la misma longitud multiplicadas por coeficientes opuestos, luego es integrable y

$$\int_0^1 f(x,y)\,dy = 0.$$

Por consiguiente:

$$\int_0^1 \left(\int_0^1 f(x,y)\,dy \right) dx = 0, \qquad \int_0^1 \left(\int_0^1 f(x,y)\,dx \right) dy = 2.$$

Ejercicio: Probar que la función $f : \mathbb{I}^2 \longrightarrow [0,1]$ dada por:

$$f(x,y) = \begin{cases} 1/y^2 & \text{si } 0 < x < y < 1, \\ -1/x^2 & \text{si } 0 < y < x < 1, \\ 0 & \text{en otro caso,} \end{cases}$$

también es un contraejemplo (aunque requiere usar la regla de Barrow, que no hemos demostrado).

Sin embargo, se podría pensar que jugar con términos positivos y negativos que se cancelan es "jugar sucio" y, puestos a ser cautos, podemos exigir, no sólo que f sea ≥ 0, sino que esté acotada. En tal caso no perdemos generalidad si suponemos que la cota es 1, con lo que podemos replantear así el problema:

¿Teorema? *Sea $f : \mathbb{I} \times \mathbb{I} \longrightarrow [0,1]$ una función que cumpla:*

1. *Las funciones $x \mapsto f(x,y)$, $y \mapsto f(x,y)$ son medibles para casi todo y, $x \in \mathbb{I}$, respectivamente.*
2. *Las funciones*

$$x \mapsto \int_0^1 f(x,y)\,dy, \qquad y \mapsto \int_0^1 f(x,y)\,dx$$

son medibles en $\mathbb{I}$.

Entonces

$$\int_0^1 \left(\int_0^1 f(x,y)\,dy \right) dx = \int_0^1 \left(\int_0^1 f(x,y)\,dx \right) dy.$$

Hemos cambiado los requisitos de integrabilidad por medibilidad porque para una función $0 \leq f \leq 1$, ser integrable es lo mismo que ser medible.

Acabamos de encontrarnos con una afirmación que no puede demostrarse ni refutarse a partir de los axiomas de la teoría de conjuntos. Para entender por qué, introducimos el concepto siguiente:

Definición 8.66 *Un conjunto $A \subset \mathbb{I}^2$ es un conjunto de Steinhaus si, para casi todo*[5] *x, $y \in \mathbb{I}$, los conjuntos*

$$A_x = \{y \in \mathbb{I} \mid (x,y) \in A\}, \qquad A^y = \{x \in \mathbb{I} \mid (x,y) \in A\}$$

son medibles y $m(A_x) = 1$ y $m(A^y) = 0$.

[5]"Para casi todo" significa en este contexto "para todo x salvo los elementos de un cierto conjunto nulo".

Claramente, si $A \subset \mathbb{I}^2$ es un conjunto de Steinhaus, su función característica $f = \chi_A$ no cumple la afirmación, anterior, pues las funciones de 1) son χ_{A_x} y χ_{A^y}, que son medibles, y las funciones de 2) son constantes iguales a 1 y 0, respectivamente, por lo que las integrales dobles valen $1 \neq 0$.

No es evidente en absoluto que el recíproco también es cierto:

Teorema 8.67 *La existencia de un conjunto de Steinhaus es equivalente a la existencia de una función $f : \mathbb{I}^2 \longrightarrow [0,1]$ tal que:*

1. *Las funciones $x \mapsto f(x,y)$, $y \mapsto f(x,y)$ son medibles para casi todo y, $x \in \mathbb{I}$, respectivamente.*
2. *Las funciones*
$$x \mapsto \int_0^1 f(x,y)\,dy, \qquad y \mapsto \int_0^1 f(x,y)\,dx$$
son medibles en $\mathbb{I}$.
3. $\displaystyle\int_0^1 \left(\int_0^1 f(x,y)\,dy\right)dx \neq \int_0^1 \left(\int_0^1 f(x,y)\,dx\right)dy.$

Posponemos la demostración hasta el final de la sección. Ahora observamos:

Teorema 8.68 (AE) *Si $\mathrm{un}(I_m) = \mathfrak{c}$ o $\mathrm{ad}(I_m) = \mathrm{cub}(I_m)$, entonces existe un conjunto de Steinhaus.*

Demostración: La primera hipótesis es que todo subconjunto de $\mathbb{I}$ de cardinal menor que $\mathfrak{c}$ es nulo. Sea $\{x_\alpha\}_{\alpha<\mathfrak{c}}$ una enumeración de $\mathbb{I}$. Basta considerar

$$A = \{(x_\alpha, x_\beta) \mid \alpha < \beta < \mathfrak{c}\}.$$

Claramente, $|A^y| < \mathfrak{c}$, luego $m(A^y) = 0$, mientras que $|\mathbb{I} \setminus A_x| < \mathfrak{c}$, luego $m(\mathbb{I} \setminus A_x) = 0$ y, por consiguiente, $m(A_x) = 1$.

Si $\kappa = \mathrm{ad}(I_m) = \mathrm{cub}(I_m)$, estamos suponiendo que $\mathbb{I} = \bigcup_{\alpha<\kappa} B_\alpha$, donde los conjuntos B_α son nulos, y a la vez que la unión de menos de κ conjuntos nulos es nula (por lo que podemos suponer los B_α disjuntos dos a dos). En este caso tomamos

$$A = \bigcup_{\beta<\kappa}\Big(\bigcup_{\alpha<\beta} B_\alpha \times B_\beta\Big).$$

Así, si $y \in B_\beta$, tenemos que $A^y \subset \bigcup_{\alpha<\beta} A_\alpha$, luego $m(A^y) = 0$, mientras que si $x \in A_\alpha$, entonces $\mathbb{I} \setminus A_x \subset \bigcup_{\beta\leq\alpha} B_\beta$, luego $m(A_x) = 1$. ∎

En particular, la hipótesis del continuo o incluso AM implican que el "teorema" de intercambio de integrales es falso.

Teorema 8.69 *Si $\mathrm{un}(I_m) < \mathrm{cub}(I_m)$, entonces no existen conjuntos de Steinhaus.*

DEMOSTRACIÓN: Supongamos que A es un conjunto de Steinhaus. Sea B un conjunto no nulo de cardinal $\mathrm{un}(I_m)$. Veamos que $\bigcup_{y\in B} A^y = \mathbb{I}$.

Para casi todo $x \in \mathbb{I}$, tenemos que $m(A_x) = 1$, luego $B \cap A_x \neq \varnothing$, luego existe un $y \in B$ tal que $(x, y) \in A$, y así $x \in A^y$. Por lo tanto, $\mathrm{cub}(I_m) \leq |B| = \mathrm{un}(I_m)$. ∎

No estamos en condiciones de probarlo aquí, pero es consistente suponer, por ejemplo, que $\mathrm{un}(I_m) = \aleph_1$ y $\mathrm{cub}(I_m) = \mathfrak{c} > \aleph_1$. En este caso el "teorema" de intercambio de integrales resulta ser cierto.

Pasamos ya a la prueba del teorema 8.67.

Traslaciones irracionales Si $f : [0,1] \longrightarrow [0,1]$, podemos extenderla[6] a una única función $f : \mathbb{R} \longrightarrow [0,1]$ tal que $f(x+1) = f(x)$, para todo $x \in \mathbb{R}$. En lo sucesivo identificaremos tácitamente cada función f en estas condiciones con su extensión periódica a $\mathbb{R}$.

Teorema 8.70 *Si $f : [0,1] \longrightarrow [0,1]$ es una función medible y $0 < \alpha < 1$ es un número irracional tal que $f(x+\alpha) = f(x)$ para casi todo $x \in [0,1]$, entonces f es constante salvo a lo sumo en un conjunto nulo.*

DEMOSTRACIÓN: La prueba de este resultado requiere algunos hechos básicos del análisis de Fourier, lo cual queda lejos de los resultados que tenemos a nuestra disposición, así que supondremos que el lector los conoce.

Sea S^1 la circunferencia unitaria en el plano complejo. Es un grupo topológico compacto con el producto, así que podemos considerar su medida de Haar unitaria m. Tenemos un epimorfismo $\pi : \mathbb{R} \longrightarrow S^1$ dado por $\pi(x) = e^{2\pi i x}$, y es fácil ver que, a través de la restricción $\pi|_{[0,1]} : [0,1] \longrightarrow S^1$, la medida de Haar de S^1 se corresponde con la medida de Lebesgue en $[0,1]$. Esto hace que las hipótesis sobre f se traducen en que $\bar{f}$ es medible y $\bar{f}(e^{2\pi i\alpha} z) = \bar{f}(z)$, para casi todo $z \in S^1$.

Los hechos que necesitamos que el lector conozca son los siguientes: como $\bar{f}$ es medible, no negativa y acotada, se cumple que $\bar{f} \in L^2(S^1)$, y esto hace que admita un desarrollo en serie de Fourier

$$\bar{f} = \sum_{n=-\infty}^{+\infty} c_n z^n,$$

para ciertos coeficientes $c_n \in \mathbb{C}$ unívocamente determinados. Hay que tener presente que la tanto convergencia de la serie como la igualdad son únicamente válidas en L^2. En particular, los dos miembros sólo son iguales como clases de equivalencia en $L^2(S^1)$, es decir, las funciones son iguales puntualmente salvo en un conjunto nulo.

[6] En realidad sólo podemos garantizar que la extensión coincide con f en $[0,1[$ a menos que $f(0) = f(1)$, pero este hecho va a ser irrelevante.

Ahora bien, la ecuación $\bar{f}(e^{2\pi i\alpha}z) = \bar{f}(z)$ hace que, siempre como clases de $L^2(S^1)$ elementos de L^2, se cumple que

$$\bar{f} = \sum_{n=-\infty}^{+\infty} c_n e^{2\pi n i\alpha} z^n,$$

luego la unicidad de los coeficientes de Fourier implica que $c_n = c_n e^{2\pi n i\alpha}$. Así, si $c_n \neq 0$ tiene que ser $e^{2\pi n i\alpha} = 1$, lo cual equivale a que $n\alpha \in \mathbb{Z}$, pero, como α es irracional, esto implica que $n = 0$. Así pues, $\bar{f} = c_0$, luego puntualmente $\bar{f} = c_0$ salvo en un conjunto nulo, y lo mismo vale para f. ∎

El teorema ergódico Ahora vamos a probar un famoso resultado que constituye uno de los fundamentos de la llamada *teoría ergódica.* No vamos a entrar en detalles sobre su significado, sino que lo probaremos únicamente como medio para llegar al teorema 8.67.

Necesitamos algunos resultados previos. Si $a_1, \ldots, a_n$ es una sucesión finita de números reales y sea $1 \leq m \leq n$. Diremos que a_k es un *m-director* de la sucesión si existe $1 \leq p \leq m$ tal que $a_k + \cdots + a_{k+p-1} \geq 0$. (Notemos que m es el máximo número de sumandos que permitimos en la suma para que se haga positiva.)

Teorema 8.71 *Si una sucesión $a_1, \ldots, a_n$ tiene m-directores, entonces la suma de todos ellos es ≥ 0.*

Demostración: Sea a_k el primer m-director de la sucesión y sea $1 \leq p \leq m$ el menor número natural tal que $a_k + \cdots a_{k+p-1} \geq 0$. Entonces todo a_h en esta suma cumple que $a_h + \cdots + a_{k+p-1} \geq 0$, por lo que también es m-director. En caso contrario, sería $a_h + \cdots + a_{k+p-1} < 0$, con lo que $a_k + \cdots a_{h-1} > 0$, en contradicción con la minimalidad de p.

Ahora repetimos el argumento con la sucesión $a_{k+p}, \ldots, a_n$. Si tiene un m-director, tomamos el primero y obtenemos otro grupo de m-directores consecutivos con suma ≥ 0. Tras un número finito de pasos hemos descompuesto la suma de todos los m-directores en varios sumandos, todos ellos ≥ 0. ∎

Teorema 8.72 (Teorema ergódico maximal) *Sea $(X, \mathcal{M}, \mu)$ un espacio medida y sea $T : X \longrightarrow X$ una aplicación tal que, para todo $A \in \mathcal{M}$, se cumpla que $f^{-1}[A] \in \mathcal{M}$ y $\mu(f^{-1}[A]) = \mu(A)$. Sea $f : X \longrightarrow \mathbb{R}$ integrable y llamemos $f_j(x) = f(T^j(x))$. Sea E el conjunto de los puntos $x \in X$ tales que existe un natural n de modo que $f_0(x) + \cdots + f_{n-1}(x) \geq 0$. Entonces E es medible y $\int_E f(x)\,dx \geq 0$.*

Demostración: Para cada natural m, sea E_m el conjunto de los $x \in E$ que cumplen la definición con $n - 1 \leq m$. Claramente $\{E_m\}_{m=1}^{\infty}$ es una sucesión creciente cuya unión es E, luego basta probar el teorema para cada E_m.

Notemos que $x \in E_m$ si y sólo si $f_0(x)$ es un m-director de la sucesión $f_0(x), \ldots, f_{m-1}(x)$.

Fijamos ahora un $n \geq 1$ arbitrario y llamamos D_k al conjunto de los $x \in X$ tales que $f_k(x)$ es un m-director de $f_0(x), \ldots, f_{n+m-1}(x)$.

Notemos que $D_0 = E_m$, pues $f_0(x)$ será m-director de $f_0(x), \ldots, f_{m-1}(x)$ si y sólo si lo es de $f_0(x), \ldots, f_{n+m-1}(x)$ (pues en la definición sólo intervienen los primeros m términos de la sucesión).

Notemos que $D_k \in \mathcal{M}$, pues podemos descomponerlo en unión finita de los conjuntos D_k^p formados por los $x \in X$ tales que $f_k(x) + \cdots + f_{k+p-1}(x) \geq 0$. Como f y T son medibles, también lo son las funciones f_j, y también lo es la suma $f_k + \cdots + f_{k+p-1}$, luego $D_k^p \in \mathcal{M}$ y lo mismo vale para D_k. En particular tenemos que $E_m \in \mathcal{M}$.

Sea $s(x)$ la suma de los m-directores de la sucesión $f_0(x), \ldots, f_{n+m-1}(x)$. Entonces $s = \sum_{k=0}^{n+m-1} f_k \chi_{D_k}$, luego s es medible e integrable.[7]

Por el teorema anterior,

$$\sum_{k=0}^{n+m-1} \int_{D_k} f_k(x)\,dx = \int_X s(x)\,dx \geq 0. \tag{8.1}$$

Sea ahora $1 \leq k \leq n-1$ y $x \in X$. Entonces, $T(x) \in D_{k-1}$ si y sólo si existe un $p \leq m$ tal que $f_{k-1}(T(x)) + \cdots + f_{k-1+p-1}(T(x)) \geq 0$, si y sólo si existe un $p \geq m$ tal que $f_k(x) + \cdots + f_{k+p-1}(x) \geq 0$, si y sólo si $x \in D_k$. Así pues, $D_k = T^{-1}[D_{k-1}]$ y, a su vez, $D_k = T^{-k}[D_0]$. Por consiguiente,

$$\int_{D_k} f_k(x)\,dx = \int_{T^{k-1}[D_0]} f(T^k(x))\,dx = \int_{D_0} f(x)\,dx. \tag{8.2}$$

Este cambio de variable se justifica porque T conserva la medida. En efecto, si D, $A \in \mathcal{M}$, tenemos que

$$\int_D \chi_A(x)\,dx = \mu(D \cap A) = \mu(T^{-1}[D] \cap \mu(T^{-1}[A])) = \int_{T^{-1}[D]} \chi_A(T(x))\,dx,$$

de aquí se sigue la igualdad si cambiamos χ_A por una función simple, de aquí se pasa a funciones medibles no negativas y de ahí a integrables.

Por consiguiente, los primeros n términos del miembro izquierdo de (8.1) son iguales. Acotando los m restantes, tenemos que

$$n \int_{D_0} f(x)\,dx + m \int_X |f(x)|\,dx \geq 0.$$

De aquí que

$$\int_{E_m} f(x)\,dx + \frac{m}{n} \int_X |f(x)|\,dx \geq 0.$$

[7]En general, el producto de funciones integrables no es integrable, pero sí lo es si un factor está acotado. En este caso $|f_k \chi_{D_k}| \leq |f_k|$, que es integrable.

para todo $n \geq 1$, luego haciendo tender n a infinito queda que

$$\int_{E_m} f(x)\,dx \geq 0.$$

■

Finalmente podemos probar el resultado principal:

Teorema 8.73 (Teorema ergódico de Birkhoff) *Sea $(X, \mathcal{M}, \mu)$ un espacio medida finito*[8] *y sea $T : X \longrightarrow X$ una aplicación tal que, para todo $A \in \mathcal{M}$, se cumpla que $f^{-1}[A] \in \mathcal{M}$ y $\mu(f^{-1}[A]) = \mu(A)$. Sea $f : X \longrightarrow \mathbb{R}$ integrable y llamemos $f_j(x) = f(T^j(x))$. Entonces, para casi todo $x \in X$ existe*

$$f^*(x) = \lim_n \frac{1}{n} \sum_{j=0}^{n-1} f_j(x).$$

Además, para casi todo $x \in X$ se cumple que $f^*(T(x)) = f^*(x)$ y

$$\int_X f^*(x)\,dx = \int_X f(x)\,dx.$$

Demostración: Sean $a < b$ dos números reales y sea $Y = Y(a, b)$ el conjunto de todos los puntos $x \in X$ tales que

$$\liminf_n \frac{1}{n} \sum_{j=0}^{n-1} f_j(x) < a < b < \limsup_n \frac{1}{n} \sum_{j=0}^{n-1} f_j(x).$$

Claramente $Y \in \mathcal{M}$, pues las medias son funciones medibles y los límites superiores e inferiores de funciones medibles son funciones medibles. Además $Y = T^{-1}[Y]$, pues

$$\frac{1}{n} \sum_{j=0}^{n-1} f_j(T(x)) = \frac{1}{n} \sum_{j=0}^{n-1} f_{j+1}(x) = \frac{n+1}{n} \frac{1}{n+1} \sum_{j=0}^{n} f_j(x) - \frac{f(x)}{n}, \tag{8.3}$$

luego el límite superior e inferior es el mismo que el de la media para x en lugar de $T(x)$.

Así pues, $T|_Y : Y \longrightarrow Y$ es también un operador que conserva la medida, luego podemos aplicar el teorema anterior al espacio Y y a la función $f - b$. El conjunto E dado por el teorema consta de los puntos $y \in Y$ tales que existe un n tal que

$$f_0(x) + \cdots + f_{n-1}(x) - nb \geq 0,$$

es decir,

$$\frac{1}{n} \sum_{j=0}^{n-1} f_j(x) \geq b,$$

[8] La hipótesis de finitud no es necesaria, pero simplifica un poco la prueba.

pero esto lo cumplen todos los puntos de Y. Por lo tanto, la conclusión es que

$$\int_Y (f(x) - b)\, dx \geq 0.$$

Igualmente llegamos a que

$$\int_Y (a - f(x))\, dx \geq 0,$$

y sumando las dos integrales, a que $\int_Y (a-b)\, dx \geq 0$, lo cual, puesto que $a < b$, sólo es posible si $\mu(Y) = 0$.

Por lo tanto, la unión de los conjuntos $Y(a,b)$ para todos los pares de números racionales $a < b$ es un conjunto nulo N, y si $x \in X \setminus N$, tiene que darse la igualdad

$$\liminf_n \frac{1}{n} \sum_{j=0}^{n-1} f_j(x) = \limsup_n \frac{1}{n} \sum_{j=0}^{n-1} f_j(x).$$

En otras palabras, f^* está definida en $X \setminus N$. Ahora observamos que

$$\int_X \Big|\frac{1}{n} \sum_{j=0}^{n-1} f_j(x)\Big|\, dx \leq \frac{1}{n} \int_X \sum_{j=0}^{n-1} |f_j(x)|\, dx = \frac{1}{n} \int_X \sum_{j=0}^{n-1} |f(x)|\, dx = \int_X |f(x)|\, dx.$$

donde hemos hecho un cambio de variable como en la ecuación (8.2), y el lema de Fatou nos da que

$$\int_X |f^*(x)|\, dx \leq \int_X |f(x)|\, dx < +\infty,$$

por lo que f^* es integrable, en particular finita c.p.t.p. La relación (8.3) prueba que $f^*(T(x)) = f^*(x)$. Falta probar que la integral de f^* coincide con la de f.

Supongamos en primer lugar que $f^* \geq a$ y, fijado $\epsilon > 0$, aplicamos el teorema anterior a la función $f - a + \epsilon$. El conjunto E es el formado por los puntos $x \in X$ tales que existe un n que cumple

$$f_0(x) + \cdots + f_{n-1}(x) - n(a - \epsilon) \geq 0$$

o, equivalentemente,

$$\frac{1}{n} \sum_{j=0}^{n-1} f_j(x) \geq a - \epsilon,$$

pero esto pasa para casi todo x, luego la conclusión es que

$$\int_X f^*(x)\, dx \geq (a - \epsilon)\mu(X)$$

y, como ϵ es arbitrario, $\int_X f^*(x)\, dx \geq a\mu(X)$. Similarmente, si $f^* \leq b$, concluimos que $\int_X f^*(x) \leq b\mu(X)$.

Llamemos finalmente $X(k,n)$ al conjunto de todos los puntos $x \in X$ tales que $k/2^n \le f^*(x) \le (k+1)/2^n$. Claramente es un conjunto medible e invariante por T, por lo que podemos aplicar los razonamientos previos a la restricción de T y f a $X(k,n)$. La conclusión es que

$$\frac{k}{2^n}\mu(X(k,n)) \le \int_{X(k,n)} f(x)\,dx \le \frac{k+1}{2^n}\mu(X(k,n)).$$

Pero trivialmente, por la definición de $X(k,n)$, tenemos también que

$$\frac{k}{2^n}\mu(X(k,n)) \le \int_{X(k,n)} f^*(x)\,dx \le \frac{k+1}{2^n}\mu(X(k,n)).$$

Por consiguiente,

$$-\frac{1}{2^n}\mu(X(x,n)) \le \int_{X(k,n)} f(x)\,dx - \int_{X(k,n)} f^*(x)\,dx \le \frac{1}{2^n}\mu(X(k,n)),$$

Sumando para todo k,

$$\Big|\int_X f(x)\,dx - \int_X f^*(x)\,dx\Big| \le \frac{1}{2^n}\mu(X).$$

Como n es arbitrario, las integrales coinciden. ∎

Vamos a necesitar únicamente el caso particular siguiente:

Teorema 8.74 *Sea $g : [0,1] \longrightarrow \mathbb{R}$ una función integrable (extendida a $\mathbb{R}$ de forma periódica) y $\alpha \in [0,1] \setminus \mathbb{Q}$. Entonces, para casi todo $x \in [0,1]$, se cumple que*

$$\lim_n \frac{1}{n}\sum_{j=0}^{n-1} g(x+j\alpha) = \int_0^1 g(t)\,dt.$$

Demostración: Aplicamos el teorema anterior a $T : [0,1] \longrightarrow [0,1]$ dado por $T(x) = E[x+\alpha]$. Así, $g(T(x)) = g(E[x+\alpha]) = g(x+\alpha)$, si consideramos la extensión periódica de g.

Es fácil ver que T conserva la medida de Lebesgue, luego el teorema anterior nos da que la función

$$g^*(x) = \lim_n \frac{1}{n}\sum_{j=0}^{n-1} g(x+j\alpha)$$

está definida para casi todo x y cumple $g^*(x+\alpha) = g^*(x)$, luego el teorema 8.70 nos da que g^* es constante salvo en un conjunto nulo N, luego si $x \in [0,1] \setminus N$,

$$\lim_n \frac{1}{n}\sum_{j=0}^{n-1} g(x+j\alpha) = g^*(x) = \int_0^1 g^*(x)\,dt = \int_0^1 g^*(t)\,dt = \int_0^1 g(t)\,dt.$$

∎

Demostración del teorema 8.67 Ya hemos visto que si existe un conjunto de Steinhaus existe una función f con las características indicadas en el enunciado. Suponemos ahora que existe tal función f y vamos a construir un conjunto de Steinhaus.

Podemos suponer que el miembro izquierdo de 3) en el enunciado de 8.67 es menor que el derecho, y tomamos entonces un número real p tal que

$$\int_0^1 \left(\int_0^1 f(x,y)\,dy\right) dx < p < \int_0^1 \left(\int_0^1 f(x,y)\,dx\right) dy.$$

Fijamos $0 < \alpha < 1$ irracional y consideramos $T : [0,1] \longrightarrow [0,1]$ dado por $T(x) = E[x+\alpha]$. Ya hemos señalado que T conserva la medida de Lebesgue. Notemos que $T^n(x) = E[x+n\alpha]$.

Sea X el conjunto de los $x \in [0,1]$ tales que las funciones $y \mapsto f(E[x+n\alpha], y)$ son medibles, para todo natural n. Entonces $m(X) = 1$, pues por hipótesis $y \mapsto f(x,y)$ es medible salvo si $x \in N$, para cierto conjunto nulo N, luego $y \mapsto f(E[x+n\alpha], y)$ es medible salvo en $T^{-n}[N]$, que es un conjunto nulo, y $X = [0,1] \setminus \bigcup_n T^{-n}[N]$. Definimos:

$$F(x,y) = \liminf_n \frac{1}{n}\sum_{j=0}^{n-1} f(x+j\alpha, y), \quad G(x,y) = \limsup_n \frac{1}{n}\sum_{j=0}^{n-1} F(x, y+j\alpha),$$

$$A = \{(x,y) \in [0,1]^2 \mid G(x,y) < p\},$$

$$B = \left\{ x \in [0,1] \mid \lim_n \frac{1}{n}\sum_{j=0}^{n-1} \int_0^1 f(x+j\alpha, y)\,dy \neq \int_0^1 \left(\int_0^1 f(t,y)\,dy\right) dt \right\},$$

$$C = \left\{ y \in [0,1] \mid \lim_n \frac{1}{n}\sum_{j=0}^{n-1} \int_0^1 f(x, y+j\alpha)\,dx \neq \int_0^1 \left(\int_0^1 f(x,t)\,dx\right) dt \right\}.$$

Por hipótesis, la función $g(x) = \int_0^1 f(x,y)\,dy$ es medible y, al ser no negativa y acotada, es integrable, luego podemos aplicarle el teorema anterior, cuya conclusión es que $m(B) = 0$. Igualmente llegamos a que $m(C) = 0$. Vamos a probar que A es un conjunto de Steinhaus.

Si $x \in X$, las funciones $y \mapsto f(x+j\alpha, y)$ son medibles, para todo j, luego también lo es $y \mapsto F(x,y)$ y, al ser no negativa y acotada, es integrable. Le aplicamos el teorema anterior, que nos da que, para casi todo $y \in [0,1]$, se cumple que

$$G(x,y) = \int_0^1 F(x,t)\,dt.$$

Si además $x \notin B$, el lema de Fatou nos da que

$$\int_0^1 F(x,t)\,dt \leq \liminf_n \frac{1}{n}\sum_{j=0}^{n-1} \int_0^1 f(x+j\alpha, t)\,dt = \int_0^1 \left(\int_0^1 f(x,y)\,dy\right) dx < p.$$

Con esto hemos probado que si $x \in X \setminus B$, entonces casi todo $y \in [0,1]$ cumple $(x,y) \in A$ o, lo que es lo mismo, que $m(A_x) = 1$.

Por otra parte, para casi todo y, la función $x \mapsto f(x,y)$ es integrable, luego el teorema anterior nos da que

$$F(x,y) = \liminf_n \frac{1}{n} \sum_{j=0}^{n-1} f(x+j\alpha, y) = \int_0^1 f(t,y)\,dt$$

para casi todo $x \in [0,1]$.

Si además $y \notin C$, entonces

$$G(x,y) = \limsup_n \frac{1}{n} \sum_{j=0}^{n-1} F(x, y+j\alpha) = \limsup_n \frac{1}{n} \sum_{j=0}^{n-1} \int_0^1 f(t, y+j\alpha)\,dt$$

$$= \int_0^1 \left(\int_0^1 f(t,u)\,dt \right) du > p.$$

Así hemos probado que, para casi todo y, casi todo x cumple $(x,y) \notin A$, luego $m(A^y) = 0$. ∎

Capítulo IX

Árboles

El concepto de árbol aparece en contextos matemáticos muy dispares, que abarcan desde problemas combinatorios finitistas hasta problemas sobre cardinales infinitos. En la primera sección presentaremos los conceptos y resultados básicos sobre árboles y en las secciones siguientes mostraremos su conexión con la hipótesis de Suslin, que es una conjetura formulada por M. Suslin en 1920 en el primer número de la revista *Fundamenta Mathematicae*. En principio se trataba de un problema de naturaleza topológica, pero G. Kurepa mostró en 1935 que es equivalente a un problema puramente conjuntista sobre árboles.

9.1 Conceptos básicos sobre árboles

En esta sección no usaremos AE si no lo indicamos explícitamente.

Definición 9.1 Un *árbol* es un conjunto parcialmente ordenado $(A, \leq)$ tal que, para todo $x \in A$, el segmento $A^<_x = \{a \in A \mid a < x\}$ está bien ordenado.

Si $x \in A$, se llama *altura* de x a $\mathrm{alt}_A x = \mathrm{ord} A^<_x$.

Si $\alpha \in \Omega$, se llama *nivel* α-ésimo de A al conjunto

$$\mathrm{Niv}_\alpha A = \{x \in A \mid \mathrm{alt}_A x = \alpha\}.$$

Se llama *altura* de A al mínimo ordinal $\mathrm{alt} A = \alpha$ tal que $\mathrm{Niv}_\alpha A = \varnothing$. Es fácil ver que

$$\mathrm{alt} A = \bigcup_{x \in A} (\mathrm{alt}_A x + 1).$$

Dos elementos $x, y \in A$ son *compatibles* si $x \leq y \vee y \leq x$. En caso contrario se dice que son *incompatibles* y se representa por $x \perp y$.

Un subconjunto $C \subset A$ es una *cadena* si sus elementos son compatibles dos a dos, es decir, si está totalmente ordenado y, por consiguiente, bien ordenado.

Un subconjunto $R \subset A$ es una *rama* si es una cadena maximal respecto a la inclusión.

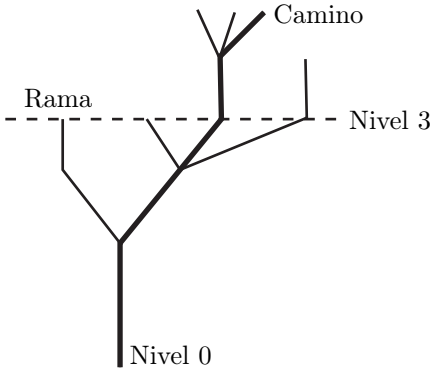
En general, el lema de Zorn asegura que toda cadena se extiende hasta una rama,[1] aunque si el árbol es finito esto mismo se prueba fácilmente sin necesidad de AE, y si el árbol es numerable basta con AEN. Llamaremos *altura* de R a

$$\mathrm{alt}_A R = \mathrm{ord} R = \bigcup_{x\in R} (\mathrm{alt}_A x + 1).$$

Un subconjunto $C \subset A$ es un *camino* si es una rama tal que $\mathrm{alt}_A C = \mathrm{alt} A$, es decir, si es una rama que corta a todos los niveles no vacíos de A.

Un subconjunto $C \subset A$ es una *anticadena* si sus elementos son incompatibles dos a dos. Claramente los niveles son anticadenas.

La figura muestra un árbol de altura 6:



Un subconjunto $A' \subset A$ es un *subárbol* de A si

$$\bigwedge x \in A \bigwedge y \in A'(x < y \to x \in A').$$

Claramente esto implica que A' también es un árbol y si $x \in A'$ entonces $\mathrm{alt}_A x = \mathrm{alt}_{A'} x$.

Si κ es un cardinal, un *κ-árbol* es un árbol de altura κ cuyos niveles tienen todos cardinal menor que κ.

Los elementos de altura 0 en un árbol se llaman *raíces*. El árbol de la figura anterior tiene una única raíz. La definición de árbol que hemos dado permite que un árbol tenga varias raíces, pero un árbol así es más bien un conjunto de varios árboles, por lo que en la práctica consideraremos siempre árboles con una única raíz. Más concretamente:

Diremos que un κ-árbol A está *bien podado* si $|\mathrm{Niv}_0 A| = 1$ y

$$\bigwedge x \in A \bigwedge \alpha < \kappa(\mathrm{alt}_A x < \alpha \to \bigvee y \in \mathrm{Niv}_\alpha A\ x < y).$$

En otras palabras, un árbol está bien podado si tiene una única raíz y desde cualquiera de sus puntos se puede ascender hasta cualquier altura. Casi siempre se puede podar bien un árbol:

[1] Basta observar que el conjunto de todas las cadenas que contienen a una dada cumple las hipótesis del lema de Zorn.

Teorema 9.2 (AE) *Si κ es un cardinal regular,*[2] *todo κ-árbol tiene un κ-subárbol bien podado.*

DEMOSTRACIÓN: Sea A un κ-árbol y $A' = \{x \in A \mid |\{z \in A \mid x < z\}| = \kappa\}$. Claramente A' es un subárbol de A. Ciertamente no es vacío, pues

$$A = \bigcup_{x \in \mathrm{Niv}_0 A} \{y \in A \mid x \leq y\},$$

y como $|\mathrm{Niv}_0 A| < \kappa$, ha de haber un $x \in \mathrm{Niv}_0 A$ tal que $|\{y \in A \mid x \leq y\}| = \kappa$, es decir, tal que $x \in A'$.

Sea $x \in A'$ y $\alpha < \kappa$ tal que $\mathrm{alt}_A x < \alpha$. Sea $Y = \{y \in \mathrm{Niv}_\alpha A \mid x < y\}$. Entonces

$$\{z \in A \mid x < z\} = \{z \in A \mid x < z \wedge \mathrm{alt}_A z \leq \alpha\} \cup \{z \in A \mid x < z \wedge \mathrm{alt}_A z > \alpha\}.$$

Por definición de A', el primer conjunto de la línea anterior tiene cardinal κ, el segundo tiene cardinal menor que κ, pues está contenido en $\bigcup_{\beta \leq \alpha} \mathrm{Niv}_\beta A$, κ es regular y los niveles tienen cardinal menor que κ.

Por consiguiente, el tercer conjunto ha de tener cardinal κ, pero

$$\{z \in A \mid x < z \wedge \mathrm{alt}_A z > \alpha\} = \bigcup_{y \in Y} \{z \in A \mid y < z \wedge \mathrm{alt}_A z > \alpha\},$$

y $|Y| \leq |\mathrm{Niv}_\alpha A| < \kappa$, por lo que ha de existir un $y \in Y$ tal que[3]

$$|\{z \in A \mid y < z \wedge \mathrm{alt}_A z > \alpha\}| = \kappa.$$

En particular $|\{z \in A \mid x < z\}| = \kappa$, con lo que $y \in A'$. Así hemos probado que

$$\bigwedge x \in A' \bigwedge \alpha < \kappa (\mathrm{alt}_A x < \alpha \to \bigvee y \in \mathrm{Niv}_\alpha A'\ x < y).$$

En particular esto implica que A' es un κ-árbol. Para estar bien podado sólo le falta tener una única raíz. Ahora bien, si $x \in \mathrm{Niv}_0 A'$, es inmediato comprobar que $B = \{y \in A' \mid x \leq y\}$ es un κ-subárbol bien podado de A', luego de A. ∎

Nota El teorema anterior es falso para cardinales singulares, pues si tenemos que $\mathrm{cf}\,\kappa = \mu < \kappa$ y $\{\alpha_\delta\}_{\delta<\mu}$ es una sucesión cofinal en κ, entonces el árbol $A = \bigcup_{\delta<\mu} \alpha_\delta \times \{\delta\}$, con el orden dado por $(\beta, \delta) \leq (\beta', \delta') \leftrightarrow \beta \leq \beta'$ cumple que $\mathrm{alt}_A(\beta, \delta) = \beta$, luego $\mathrm{alt}\, A = \kappa$, pero es fácil ver que no admite subárboles bien podados (ni tampoco el árbol que resulta de añadir a A un mínimo elemento, para que tenga una única raíz). ∎

Podría pensarse que un $\aleph_0$-árbol no tiene necesariamente un camino, es decir, una rama infinita, pues en principio podría tener únicamente ramas finitas de altura arbitrariamente grande, pero ninguna rama infinita, pese a lo cual su altura sería infinita. Sin embargo no es así:

[2]Si $\kappa = \aleph_0$ la prueba no requiere AE, pues lo único que se usa sistemáticamente es que toda unión finita de conjuntos finitos es finita.

[3]Notemos que la condición $\mathrm{alt}_A z > \alpha$ es redundante, pues se sigue de la definición de Y.

Teorema 9.3 (König) (AEN) *Todo $\aleph_0$-árbol tiene un camino.*[4]

DEMOSTRACIÓN: Sea A un $\aleph_0$-árbol y sea A' un subárbol bien podado. Entonces hay un $x_0 \in \mathrm{Niv}_0 A'$, hay un $x_1 \in \mathrm{Niv}_1 A'$ tal que $x_0 < x_1$, hay un $x_2 \in \mathrm{Niv}_2 A'$ tal que $x_1 < x_2$, y por recurrencia construimos un conjunto $C = \{x_n \mid n \in \omega\}$ que claramente es un camino en A. ∎

En general, podemos garantizar la existencia de caminos en un árbol si suponemos que sus niveles son suficientemente pequeños:

Teorema 9.4 (AE) *Si κ es un cardinal regular y $\mu < \kappa$, todo árbol de altura κ cuyos niveles tengan cardinal menor que μ tiene un camino.*

DEMOSTRACIÓN: Sea A un árbol en las condiciones del enunciado. Si $x \in A$ y $\delta < \mathrm{alt}_A x$, representaremos por $x|_\delta$ al único elemento de $\mathrm{Niv}_\delta(A)$ tal que $x|_\delta < x$.

Veamos en primer lugar que no perdemos generalidad si suponemos que A no se ramifica en niveles de altura límite, es decir, que si a, $b \in \mathrm{Niv}_\lambda(A)$, para cierto ordinal límite λ y $a \neq b$, entonces existe un $\delta < \lambda$ tal que $a|_\delta \neq b|_\delta$.

En efecto, para cada $\lambda < \kappa$, sea $\mathcal{C}_\lambda$ el conjunto de todas las cadenas de la forma $\{x \in A \mid x < a\}$, con $a \in \mathrm{Niv}_\lambda(A)$. (El problema es que diferentes elementos a pueden determinar la misma cadena C.) Podemos suponer que si $C \in \mathcal{C}_\lambda$ entonces $C \notin A$ (por ejemplo, no perdemos generalidad si suponemos que los elementos de A son pares ordenados de la forma $(a, 0)$, con lo que una cadena C no es ninguno de estos pares). Observemos que $|\mathcal{C}_\lambda| \leq |\mathrm{Niv}_\lambda(A)| < \mu$.

Consideramos ahora $A' = A \cup \bigcup_{\lambda<\kappa} \mathcal{C}_\lambda$ y definimos en A' la relación de orden que extiende a la de A de modo que si $C \in \mathcal{C}_\lambda$, sus anteriores son sus elementos y las cadenas $C' \in \mathcal{C}_{\lambda'}$ tales que $C' \subset C$ y $\lambda' < \lambda$, y sus posteriores son los elementos de A mayores que todos los elementos de C y las cadenas $C' \in \mathcal{C}_{\lambda'}$ con $\lambda < \lambda'$ y $C \subset C'$.

Es fácil ver que A' es un árbol tal que cada elemento de A de altura α tiene altura $\alpha + 1$ en A' y $\mathrm{Niv}_\lambda(A') = \mathcal{C}_\lambda$. Esto hace que A' siga siendo un κ árbol y que sus niveles siguen teniendo cardinal $< \mu$. (Lo que hemos hecho es poner un nuevo elemento por debajo de cada grupo de elementos de $\mathrm{Niv}_\lambda(A)$ con una misma cadena por debajo, de modo que la ramificación pasa de producirse en el nivel λ al nivel $\lambda + 1$).

Es claro que si demostramos que A' tiene un camino, al cortarlo con A tendremos un camino en A.

Así pues, suponemos que A no se ramifica en niveles límite. Supongamos en primer lugar que μ es regular. Para cada $\lambda < \kappa$ tal que $\mathrm{cf}\,\lambda = \mu$, elijamos un

[4]Necesitamos AEN únicamente para concluir que todo $\aleph_0$-árbol es numerable (porque es unión de una cantidad numerable de niveles finitos), pero si aplicamos el teorema de König a un árbol que ya sabemos que es numerable no necesitamos AEN, pues no hace falta el axioma de elección para elegir elementos de un conjunto numerable.

$x_\lambda \in \mathrm{Niv}_\lambda(A)$. Para cada $x \in \mathrm{Niv}_\lambda(A)$ distinto de x_λ existe un $\delta < \lambda$ tal que $x_\lambda|_\delta \neq x|_\delta$. Como $|\mathrm{Niv}_\lambda(A)| < \mu = \mathrm{cf}\,\lambda$, podemos tomar un $f(\lambda) < \lambda$ tal que para todo $x \in \mathrm{Niv}_\lambda(A) \setminus \{x_\lambda\}$ se cumple que $x_\lambda|_{f(\alpha)} \neq x|_{f(\alpha)}$.

Ahora usamos que $E = \{\lambda < \kappa \mid \mathrm{cf}\,\lambda = \mu\}$ es estacionario en κ (teorema 6.13) y, como $f : E \longrightarrow \kappa$ es regresiva, por el teorema 6.15 sabemos que es constante en un conjunto estacionario $E' \subset E$, en particular no acotado en κ. Digamos que toma el valor γ. Como $\{x_\lambda|_\gamma \mid \gamma < \lambda \in E'\}$ tiene cardinal κ, mientras que $|\mathrm{Niv}_\gamma(A)| < \mu$, tiene que existir un subconjunto $Y \subset E'$ de cardinal κ, luego no acotado, tal que todos los $x_\lambda|_\gamma$ son iguales, para $\lambda \in Y$.

Pero esto hace que si λ, $\lambda' \in Y$, digamos $\lambda < \lambda'$, necesariamente $x_\lambda < x_{\lambda'}$, pues en caso contrario $x_{\lambda'}|_\lambda \neq x_\lambda$ y, como $f(\lambda) = \gamma$, tendría que ser $x_{\lambda'}|_\gamma \neq x_\lambda|_\gamma$, por definición de f, contradicción.

Así pues, $\{x_\lambda\}_{\lambda\in Y}$ es una cadena, y $\{x \in A \mid \bigvee\lambda \in Y\ x < x_\lambda\}$ es un camino en A.

Consideremos ahora el caso en que μ es singular. Para cada $\alpha < \kappa$, tenemos que $|\mathrm{Niv}_\alpha(A)|^+ < \mu$ es un cardinal regular, luego existe un $\nu < \mu$ regular tal que el conjunto $X = \{\alpha < \kappa \mid |\mathrm{Niv}_\alpha(A)| < \nu\}$ tiene cardinal κ, luego no está acotado. Entonces $A' = \bigcup_{\alpha\in X} \mathrm{Niv}_\alpha(A)$ es un κ-árbol con todos sus niveles de cardinal $< \nu$. Por la parte ya probada tiene un camino C, y es claro que $\{x \in A \mid \bigvee y \in C\ x < y\}$ es un camino en A. ∎

Un problema conjuntista destacado en cuyo análisis resulta fundamental el concepto de árbol es la hipótesis de Suslin, que es Dedicamos la primera sección a analizar el problema de Suslin antes de presentar el concepto de árbol. En todas las secciones excepto la segunda, en la que introduciremos los conceptos básicos sobre árboles, usaremos AE sin indicarlo explícitamente.

9.2 El problema de Suslin

El teorema 2.51 prueba que un conjunto totalmente ordenado es semejante a $\mathbb{R}$ si y sólo si es un continuo sin extremos separable. Suslin conjeturó que la condición de separabilidad puede sustituirse por la condición de cadena numerable:

Hipótesis de Suslin (HS) *Todo continuo sin extremos con la condición de cadena numerable es semejante a* $\mathbb{R}$.

La condición de cadena numerable equivale a la separabilidad en espacios métricos, pero, aunque $\mathbb{R}$ es ciertamente un espacio métrico, si tenemos un continuo sin extremos con la condición de cadena numerable, no podemos asegurar que su topología de orden sea metrizable antes de saber si es o no semejante a $\mathbb{R}$, por lo que no podemos asegurar a priori que tenga que ser separable.

Definición 9.5 Una *recta de Suslin* es un continuo sin extremos con la condición de cadena numerable no separable.

En estos términos la hipótesis de Suslin equivale a la no existencia de rectas de Suslin, y lo que sucede es que no se puede demostrar ni que existan ni que no existan rectas de Suslin. De momento, lo que vamos a probar aquí es que el problema de Suslin es equivalente a un problema topológico más general, a saber:

Hipótesis de Suslin (HS) *Un conjunto totalmente ordenado cumple la c.c.n. (como espacio topológico con la topología de orden) si y sólo si es separable.*

En efecto:

Teorema 9.6 *Son equivalentes:*

1. *Existe un conjunto totalmente ordenado con la condición de cadena numerable no separable.*
2. *Existe un conjunto ordenado denso en sí mismo, sin extremos, con la condición de cadena numerable y en la que ningún intervalo es separable.*
3. *Existe una recta de Suslin en la que ningún intervalo es separable.*
4. *Existe una recta de Suslin.*

DEMOSTRACIÓN: Sólo hay que probar que 1) $\Rightarrow$ 2) y que 2) $\Rightarrow$ 3).

Sea Y un conjunto totalmente ordenado que cumpla 1) y consideremos la relación en Y dada por $x \sim y$ si y sólo si el intervalo comprendido entre ellos, $]x, y[$ o $]y, x[$, es separable. (Notemos que un intervalo vacío es separable.) Es inmediato comprobar que se trata de una relación de equivalencia. Llamamos X al conjunto cociente.

Veamos que si $[x] = [y] \in X$ y $x < z < y$, entonces $[x] = [z] = [y]$.

En efecto, tenemos que $]x, y[$ es separable, luego $]x, z[$ también lo es. (En general, todo subespacio abierto de un espacio separable es separable.)

De aquí se sigue fácilmente que si $[x_1] = [x_2] \neq [y_1] = [y_2]$, entonces

$$x_1 < y_1 \leftrightarrow x_2 < y_2.$$

Por consiguiente podemos definir la relación de orden total en X dada por

$$[x] \leq [y] \leftrightarrow x \leq y.$$

Vamos a probar que X cumple 2).

En primer lugar probamos que si $I \in X$ entonces I es un subconjunto separable de Y.

En efecto, sea M una familia maximal de intervalos abiertos no vacíos disjuntos dos a dos con extremos en I. Como Y cumple la condición de cadena numerable, tenemos que M es numerable. Digamos que $M = \{]x_n, y_n[\mid n \in \omega\}$. Como x_n, $y_n \in I$, tenemos que $x_n \sim y_n$, luego $]x_n, y_n[$ es separable. Sea D_n un subconjunto denso numerable de $]x_n, y_n[$. Sea $D = \bigcup_{n\in\omega} D_n \subset I$ numerable. Veamos que es denso en I.

Sea $]x, y[$ un intervalo abierto no vacío con $x,\ y \in I$. La maximalidad de M implica que existe un $n \in \omega$ tal que $]x_n, y_n[\cap]x, y[\neq \varnothing$. Esta intersección contiene un intervalo no vacío, luego corta a D_n, luego a D, luego $]x, y[\cap D \neq \varnothing$.

En particular concluimos que X tiene al menos dos puntos, pues en otro caso $X = \{Y\}$ y tendríamos que Y sería separable.

Veamos que X es denso en sí mismo (en particular es infinito).

Sean $[x] < [y]$ dos elementos de X y supongamos que no hay ningún otro elemento entre ambos. Supongamos que $x < z < y$. Entonces $[x] \leq [z] \leq [y]$, luego $[x] = [z]$ o $[z] = [y]$, luego $z \in [x] \cup [y]$. Así pues, $]x, y[\subset [x] \cup [y]$. Como $[x]$ e $[y]$ son subconjuntos separables de Y, también lo es su unión y también lo es $]x, y[$, luego $[x] = [y]$, contradicción.

Veamos que X cumple la condición de cadena numerable.

Supongamos que $\big\{\big][x_\alpha], [y_\alpha]\big[\big\}_{\alpha<\omega_1}$ es una familia de intervalos de X disjuntos dos a dos. Tomando intervalos estrictamente contenidos en los dados, podemos exigir que $[x_\alpha] \neq [y_\beta]$ para todo $\alpha,\ \beta < \omega_1$.

Como los intervalos de X son no vacíos, es claro que $]x_\alpha, y_\alpha[\neq \varnothing$. Más aún, son disjuntos dos a dos, pues si existe $z \in]x_\alpha, y_\alpha[\cap]x_\beta, y_\beta[$, entonces $[z] = [x_\alpha] \vee [z] = [y_\alpha]$ y, por otra parte, $[z] = [x_\beta] \vee [z] = [y_\beta]$, luego $[z] = [x_\alpha] = [x_\beta]$ o bien $[z] = [y_\alpha] = [y_\beta]$, pero esto sólo es posible si $\alpha = \beta$.

Así pues, la familia $\{]x_\alpha, y_\alpha[\}_{\alpha<\omega_1}$ contradice la condición de cadena numerable de Y.

Veamos que ningún intervalo abierto de X es separable.

Supongamos que un intervalo $\big][x], [y]\big[$ en X tiene un subconjunto denso numerable $\{d_n \mid n \in \omega\}$.

Sea $H = \bigcup_{[x]\leq L\leq[y]} L \subset Y$. Es claro que $]x, y[\subset H$, luego si probamos que H es separable tendremos que $]x, y[$ también lo será, luego $[x] = [y]$, lo cual es absurdo, pues hemos tomado $[x] < [y]$.

Observemos que el conjunto de las clases $[x] \leq L \leq [y]$ con más de dos puntos ha de ser numerable, pues de cada una de ellas obtenemos un intervalo en Y no vacío con los cuales se forma una anticadena en Y. Sea $\{L_n\}_{n<\omega}$ el conjunto de estas clases. Sabemos que L_n contiene un conjunto denso numerable D_n. Sea D la unión de todos los conjuntos D_n más un elemento de cada clase d_n. Entonces D es denso en H, pues si $u < v$ son elementos de H y $]u, v[\neq \varnothing$, o bien $[u] = [v] = L_n$ y entonces $]u, v[\cap D_n \neq \varnothing$, o bien $[u] < [v]$, en cuyo caso existe n tal que $[u] < d_n < [v]$, con lo que también $]u, v[\cap D \neq \varnothing$.

Así X cumple 2) salvo por el hecho de que puede tener máximo o mínimo elemento. Ahora bien, como X es denso en sí mismo, si eliminamos el posible máximo y mínimo, obtenemos un nuevo conjunto ordenado ya no tiene máximo ni mínimo y sigue cumpliendo las otras propiedades.

Ahora veamos que 2) implica 3). Sea X un conjunto totalmente ordenado en las condiciones de 2) y sea $W = C(X)$ la compleción de X en el sentido de 2.44, que es un continuo tal que existe una inmersión densa $i : X \longrightarrow W$.

Si hubiera en W una familia no numerable de intervalos no vacíos disjuntos dos a dos, dentro de cada uno de ellos podríamos tomar un intervalo no vacío con extremos en $i[X]$, y así obtendríamos una familia igual en X. Por lo tanto W cumple la condición de cadena numerable.

Si un intervalo $]S_1, S_2[$ en W tuviera un subconjunto denso numerable, tomamos x, $y \in X$ tales que $S_1 \leq i(x) < i(y) \leq S_2$ y podríamos tomar un conjunto denso numerable D en $]i(x), i(y)[$. Para cada intervalo $]D_1, D_2[$ con extremos en D tomamos un punto $u \in]x, y[$ tal que $i(u) \in]D_1, D_2[$. Así obtenemos un subconjunto numerable de $]x, y[$ que claramente es denso, contradicción. Así pues, W es una recta de Suslin sin intervalos separables. ∎

Por consiguiente, la hipótesis de Suslin es en realidad un problema topológico general sobre si las topologías de orden cumplen también un resultado que sabemos que es válido para las topologías metrizables: la equivalencia entre la separabilidad y la condición de cadena numerable.

A este respecto, el teorema [T 12.27] nos dice que todo espacio ordenado satisface la relación

$$c(X) \leq d(X) \leq c(X)^+,$$

donde la celularidad $c(X)$ es la menor cota del cardinal de cualquier familia de abiertos disjuntos dos a dos, y la densidad $d(X)$ es el menor cardinal de un subconjunto denso en X. En particular, un conjunto totalmente ordenado X con la c.c.n. (es decir, con $c(X) = \aleph_0$) tiene un subconjunto denso de cardinal $d(X) \leq \aleph_1$. Pero el teorema da una condición suficiente para que se dé la igualdad $d(X) = c(X)$, precisamente en términos de la no existencia de un árbol con ciertas propiedades:

Definición 9.7 Un *κ-árbol de Suslin* es un κ-árbol cuyas cadenas y anticadenas tienen todas cardinal $< \kappa$. Un *árbol de Suslin* es un $\aleph_1$-árbol de Suslin.

Antes de profundizar en la relación de los árboles de Suslin con la topología de los espacios ordenados conviene probar algunos hechos elementales.

Observemos que todo κ-subárbol bien podado de un κ-árbol de Suslin es claramente un κ-árbol de Suslin bien podado, luego, si κ es un cardinal regular y existe un κ-árbol de Suslin, también existe un κ-árbol de Suslin bien podado.

Diremos que un árbol A está *ramificado* si todo $x \in A$ tiene extensiones incompatibles, es decir, si el conjunto $\{y \in A \mid x < y\}$ no está totalmente ordenado.

Teorema 9.8 *Todo κ-árbol de Suslin bien podado está ramificado.*

Demostración: Sea A un κ-árbol de Suslin bien podado. Sea $y \in A$. Sea C una cadena maximal que contenga a y. Entonces $|C| < \kappa$, luego existe un ordinal $\alpha < \kappa$ tal que $\operatorname{alt} C < \alpha$. Como A está bien podado existe un $x \in A$ de altura α tal que $y < x$. No puede ocurrir que todos los elementos de C estén bajo x, luego tomando un $x' \in C$ con $y < x'$ que no esté bajo x, tenemos que x y x' son extensiones incompatibles de y. Por lo tanto A está ramificado. ∎

Esto tiene interés porque la condición de Suslin se simplifica un tanto sobre los árboles ramificados.

Teorema 9.9 *Si κ es un cardinal regular y A es un κ-árbol ramificado en el que toda anticadena maximal tiene cardinal $< \kappa$, entonces A es un κ-árbol de Suslin.*

DEMOSTRACIÓN: Toda anticadena está contenida en una anticadena maximal, luego todas las anticadenas de A tienen cardinal $< \kappa$. Si A tuviera una cadena de cardinal κ, podríamos tomarla maximal, llamémosla B. Entonces B corta a todos los niveles no vacíos de A. Para cada $x \in A$, sea $f(x) > x$ tal que $f(x) \notin B$ (existe porque A está ramificado).

Definimos por recurrencia una sucesión $\{x_\alpha\}_{\alpha<\kappa}$ de modo que $x_\alpha \in B$ y $\mathrm{alt}_A x_\alpha \geq \bigcup_{\beta<\alpha} \mathrm{alt}\, f(x_\alpha)$. Así $\{f(x_\alpha)\}_{\alpha<\kappa}$ es una anticadena no numerable en A, contradicción. ∎

Pasamos ya a estudiar la relación entre los árboles de Suslin y la hipótesis de Suslin. En realidad el teorema [T 12.27] nos da ya la mitad de la respuesta:

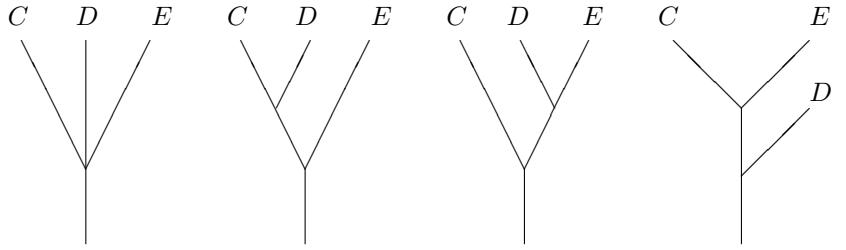
Teorema 9.10 *Si κ es un cardinal infinito, existe un espacio ordenado X tal que $c(X) = \kappa < d(X)$ si y sólo si existe un κ^+-árbol de Suslin.*

DEMOSTRACIÓN: Lo que afirma [T 12.27] es precisamente que si κ es un cardinal infinito y existe un espacio ordenado X tal que $c(X) = \kappa < d(X)$, entonces existe un κ^+-árbol de Suslin. Supongamos ahora que existe un κ^+-árbol de Suslin A y vamos a probar que existe un conjunto ordenado en las condiciones del enunciado. Podemos suponer que A está bien podado. Fijamos un orden total $\preceq$ en A y llamamos L al conjunto de todas las ramas de A.

Si $C \in L$, del hecho de que A está bien podado se sigue que $\mathrm{alt}\, C$ es un ordinal límite. Si $\alpha < \mathrm{alt}\, C$, llamaremos $C(\alpha)$ al único elemento en C de altura α. Dados C, $D \in L$, $C \neq D$, llamaremos $d(C, D)$ al mínimo ordinal α tal que $C(\alpha) \neq D(\alpha)$. Claramente $d(C, D) < \mathrm{alt}\, C \cap \mathrm{alt}\, D$. Definimos en L el orden $\leq$ dado por

$$C \leq D \leftrightarrow C = D \vee (C \neq D \wedge C(d(C, D)) \prec D(d(C, D))).$$

Es claro que la relación $\leq$ es reflexiva y antisimétrica. Veamos que es transitiva: Si $C \leq D \leq E$ y se da alguna igualdad es claro que $C \leq E$. Supongamos, pues, que $C < D < E$. Tenemos las posibilidades siguientes:



$d(D, E) = d(C, E) = d(C, D)$ $\quad$ $d(D, E) = d(C, E) < d(C, D)$ $\quad$ $d(C, E) = d(C, D) < d(D, E)$ $\quad$ $d(C, D) = d(D, E) < d(C, E)$

Sabemos que $C(d(C,D)) \prec D(d(C,D))$, $D(d(D,E)) \prec E(d(D,E))$ y hemos de probar que $C(d(C,E)) \prec E(d(C,E))$, lo cual es cierto en los tres primeros casos, mientras que el cuarto contradice las hipótesis.

Es claro que dos ramas cualesquiera son comparables, luego L es un conjunto totalmente ordenado.

Vamos a probar que $c(L) \leq \kappa$. En efecto, supongamos que $\{]C_\alpha, D_\alpha[\}_{\alpha<\kappa^+}$ es una familia de intervalos no vacíos disjuntos dos a dos. Sea $C_\alpha < E_\alpha < D_\alpha$ y sea β_α tal que

$$d(C_\alpha, E_\alpha) \cup d(E_\alpha, D_\alpha) < \beta_\alpha < \operatorname{alt} E_\alpha.$$

Vamos a probar que $\{E_\alpha(\beta_\alpha)\}_{\alpha<\kappa^+}$ es una anticadena en A, con lo que tendremos una contradicción. En caso contrario, si $E_\alpha(\beta_\alpha)$ fuera compatible con un $E_{\alpha'}(\beta_{\alpha'})$, eso significa que

$$d(E_\alpha, E_{\alpha'}) > \text{mín}\{\beta_\alpha, \beta_{\alpha'}\}.$$

No perdemos generalidad si suponemos que el mínimo es β_α. Entonces se cumple que $d(E_\alpha, E_{\alpha'}) > \beta_\alpha > d(C_\alpha, E_\alpha)$, luego $d(C_\alpha, E_{\alpha'}) = d(C_\alpha, E_\alpha)$, luego

$$C(d(C_\alpha, E_{\alpha'})) = C(d(C_\alpha, E_\alpha)) < E_\alpha(d(C_\alpha, E_\alpha))$$

$$= E_{\alpha'}(d(C_\alpha, E_\alpha)) = E_{\alpha'}(d(C_\alpha, E_{\alpha'})).$$

Esto significa que $C_\alpha < E_{\alpha'}$. Igualmente, $d(E_\alpha, E_{\alpha'}) > \beta_\alpha > d(E_\alpha, D_\alpha)$, luego $d(E_{\alpha'}, D_\alpha) = d(E_\alpha, D_\alpha)$, luego

$$E_{\alpha'}(d(E_{\alpha'}, D_\alpha)) = E_{\alpha'}(d(E_\alpha, D_\alpha)) = E_\alpha(d(E_\alpha, D_\alpha))$$

$$< D_\alpha(d(E_\alpha, D_\alpha)) = D_\alpha(d(E_{\alpha'}, D_\alpha)),$$

luego $C_\alpha < E_{\alpha'} < D_\alpha$, y así $E_{\alpha'} \in]C_\alpha, D_\alpha[\cap]C_{\alpha'}, D_{\alpha'}[= \varnothing$.

Ahora veamos que $d(L) \geq \kappa^+$. Supongamos que D es un subconjunto denso en L con $|D| \leq \kappa$. Las alturas de las ramas de D son ordinales $< \kappa^+$. Como hay a lo sumo κ alturas y κ^+ es regular, podemos tomar $\delta < \kappa^+$ mayor que cualquiera de ellas. Sea $x \in \text{Niv}_\delta A$.

Como A está ramificado, existe un ordinal $\delta < \alpha < \kappa^+$ tal que existen r, s, $t \in \text{Niv}_\alpha A$ por encima de x. Tomemos E, F, $G \in L$ tales que $r \in E$, $s \in F$, $t \in G$. Podemos suponer $E < F < G$. Así, $]E, G[$ es un intervalo no vacío, luego debería existir $C \in]E, G[\cap D$. Ahora bien, como $x \in E \cap G$, tenemos que $\delta = \operatorname{alt}_A x < d(E, G)$, y como $d(C, E) < \operatorname{alt} C < \delta$ (porque $C \in D$ y por la definición de δ), resulta que $d(C, E) = d(C, G)$, de donde se sigue que C es menor que E y G o mayor que ambos, contradicción.

Con esto hemos probado que $c(L) \leq \kappa$ y que $d(L) \geq \kappa^+$, pero como [T 12.27] afirma que $d(L) \leq c(L)^+$, tiene que ser exactamente $c(L) = \kappa$ y $d(L) = \kappa^+$. ∎

En particular, teniendo en cuenta el teorema 9.6, hemos probado lo siguiente:

Teorema 9.11 *Existe un árbol de Suslin si y sólo si existe una recta de Suslin.*

Con esto tenemos una expresión alternativa para la hipótesis de Suslin:

Hipótesis de Suslin (HS) *No existen árboles de Suslin.*

9.3 La independencia de la Hipótesis de Suslin

En esta sección vamos a demostrar que

$$\mathrm{AM}(\aleph_1) \to \mathrm{HS}, \qquad \diamondsuit \to \neg\mathrm{HS}.$$

Si el lector acepta nuestra palabra de que tanto $\mathrm{AM}(\aleph_1)$ como $\diamondsuit$ son consistentes con los axiomas de la teoría de conjuntos, con esto tendrá probado que no es posible demostrar ni refutar la existencia de rectas o árboles de Suslin.

En realidad podemos dar varias pruebas de que $\mathrm{AM}(\aleph_1) \to \mathrm{HS}$. La más sencilla y directa es ésta:

Teorema 9.12 $\mathrm{AM}(\aleph_1) \to \mathrm{HS}$.

Demostración: Supongamos $\mathrm{AM}(\aleph_1)$ y que existe un árbol de Suslin. Entonces existe uno bien podado A. Sea $\mathbb{P} = A$ con el orden inverso. Entonces $\mathbb{P}$ es un c.p.o. con la condición de cadena numerable y, para cada $\alpha < \omega_1$, el conjunto $D_\alpha = \{a \in A \mid \mathrm{alt}_A a \geq \alpha\}$ es denso en $\mathbb{P}$. Por $\mathrm{AM}(\aleph_1)$ tenemos un filtro G que corta a todos los conjuntos A_α, lo que se traduce en que G es un camino (no numerable) en A, contradicción. ∎

Otra prueba indirecta se basa en la propiedad siguiente de las rectas de Suslin:

Teorema 9.13 *Si X es un espacio ordenado con la c.c.n. pero no separable, entonces $X \times X$ no cumple la c.c.n.*

Demostración: Vamos a construir tres sucesiones $\{a_\alpha\}_{\alpha<\omega_1}$, $\{b_\alpha\}_{\alpha<\omega_1}$, $\{c_\alpha\}_{\alpha<\omega_1}$ en X tales que:

1. $a_\alpha < b_\alpha < c_\alpha$,
2. $]a_\alpha, b_\alpha[\neq \varnothing \neq]b_\alpha, c_\alpha[$
3. $]a_\alpha, c_\alpha[\cap \{b_\beta \mid \beta < \alpha\} = \varnothing$.

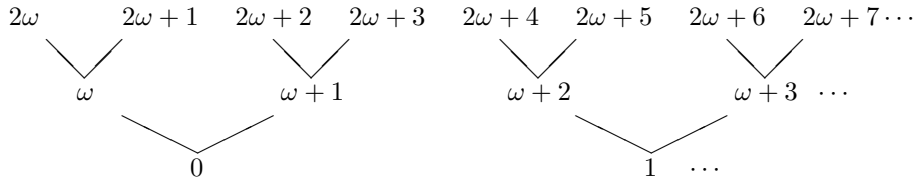
Admitiendo que tenemos tales sucesiones, definimos $U_\alpha =]a_\alpha, b_\alpha[\times]b_\alpha, c_\alpha[$ y observamos que se trata de una familia de abiertos en $X \times X$ no vacíos (por la propiedad b) y disjuntos dos a dos, pues si $\beta < \alpha$, entonces, o bien $b_\beta \leq a_\alpha$, en cuyo caso $]a_\beta, b_\beta[\cap]a_\alpha, b_\alpha[= \varnothing$, o bien $a_\alpha < b_\beta$, en cuyo caso, por c) tenemos que $c_\alpha \leq b_\beta$, luego $]b_\beta, c_\beta[\cap]b_\alpha, c_\alpha[= \varnothing$. Por lo tanto, $X \times X$ no cumple la c.c.n.

Veamos, pues, cómo construir la sucesión. Sea $A \subset X$ el conjunto de los puntos aislados de X. Si $a \in A$ entonces $\{a\}$ es abierto, luego por la c.c.n. tenemos que $|A| \leq \aleph_0$. Supongamos definidas $\{a_\alpha\}_{\alpha<\beta}$, $\{b_\alpha\}_{\alpha<\beta}$, $\{c_\alpha\}_{\alpha<\beta}$, para $\beta < \omega_1$. Entonces $D = A \cup \{a_\alpha \mid \alpha < \beta\} \cup \{b_\alpha \mid \alpha < \beta\} \cup \{c_\alpha \mid \alpha < \beta\}$ es un conjunto numerable, luego $X \setminus \overline{D} \neq \varnothing$. Como es un abierto no vacío, contendrá un intervalo abierto no vacío $]a_\beta, c_\beta[$ que, como no contiene puntos aislados, es infinito, luego contiene un b_β que lo divide en dos intervalos no vacíos. ∎

Como el teorema 8.57 afirma que si se cumple $\mathrm{AM}(\aleph_1)$ el producto de espacios con la c.c.n. cumple la c.c.n., tenemos así un argumento alternativo por el que no puede haber rectas de Suslin si se cumple $\mathrm{AM}(\aleph_1)$. Por otra parte:

Teorema 9.14 $\diamondsuit \to \neg\mathrm{HS}$.

Demostración: Vamos a definir una relación de orden $\leq^*$ en ω_1 de modo que $B = (\omega_1, \leq^*)$ sea un árbol de Suslin. Por simplificar la construcción no va a tener una única raíz, sino que todos los números naturales tendrán altura 0 (después nada nos impide podar bien el árbol resultante y obtener otro árbol de Suslin más elegante). Los primeros niveles de B serán así:



Más concretamente, $\mathrm{Niv}_\alpha B$ estará formado por los ordinales de

$$N_\alpha = \{\omega \cdot \alpha + n \mid n \in \omega\}.$$

Por las propiedades de la aritmética ordinal, los conjuntos $\{N_\alpha\}_{\alpha<\omega_1}$ forman una partición de ω_1 en $\aleph_1$ subconjuntos numerables disjuntos dos a dos.

Sea $\{A_\alpha\}_{\alpha<\omega_1}$ una sucesión $\diamondsuit$. Definiremos la relación $\leq^*$ recurrentemente sobre cada N_α de modo que se cumplan las propiedades siguientes:

1. $\bigwedge \alpha < \omega_1\ \mathrm{Niv}_\alpha B = N_\alpha$,
2. Para cada $\alpha < \omega_1$ y cada $n < \omega$ se cumple

   $$\omega \cdot \alpha + n \leq^* \omega(\alpha+1) + 2n \quad \text{y} \quad \omega \cdot \alpha + n \leq^* \omega(\alpha+1) + 2n + 1$$

   y los miembros derechos son los únicos elementos de $N_{\alpha+1}$ que extienden al miembro izquierdo.
3. Si $\beta < \alpha < \omega_1$ y $x \in N_\beta$, entonces $\bigvee y \in N_\alpha\ x \leq^* y$.
4. Si $\lambda < \omega_1$, $B_\lambda = \lambda$ (donde $B_\lambda = \{\alpha < \omega_1 \mid \mathrm{alt}_B \alpha < \lambda\}$) y A_λ es una anticadena maximal en B_λ, entonces

   $$\bigwedge x \in N_\lambda \bigvee y \in A_\lambda\ y \leq^* x.$$

La propiedad 2) afirma que el elemento n-simo del nivel α-ésimo tiene exactamente dos extensiones en el nivel $\alpha+1$-ésimo, a saber, los elementos $2n$-simo y $2n+1$-ésimo. La propiedad 3) afirma que desde cualquier punto se puede ascender hasta cualquier altura y, por último, lo que expresa la propiedad 4) es que si "da la casualidad" de que $B_\lambda = \lambda$ y "da la casualidad" de que A_λ es una anticadena maximal en B_λ, entonces A_λ será una anticadena maximal en B, es decir, no podrá prolongarse a una anticadena mayor, pues cualquier elemento $x \in B$ que esté en un nivel posterior a λ tendrá por debajo un elemento de N_λ que, por 4), tendrá por debajo un elemento de A_λ, luego x será compatible con un elemento de A_λ y, por consiguiente, no podrá estar en una anticadena que contenga a A_λ.

Así, en lugar de preocuparnos por que el árbol que vamos a construir no tenga anticadenas no numerables, sólo nos preocupamos de que, en caso de que A_λ sea una anticadena, no pueda ser prolongada, con lo que no podrá "crecer" hasta volverse no numerable. La esencia de $\diamondsuit$ es que la sucesión $\{A_\lambda\}_{\lambda<\omega_1}$ "predice" eficientemente las posibles anticadenas, de modo que al controlar las de la forma A_λ de hecho las controlamos todas, como vamos a ver.

Definiremos una sucesión de árboles

$$B_\alpha = \bigcup_{\beta<\alpha} N_\beta$$

de modo que cada cual sea un subárbol de los siguientes y cumpla las propiedades anteriores.

En $B_1 = N_0$ la relación $\leq^*$ se restringe a ser reflexiva, pues los niveles son anticadenas. Si $\lambda < \omega_1$ es un ordinal límite y $\leq^*$ está definida en B_δ, para cada $\delta < \lambda$, entonces, como

$$B_\lambda = \bigcup_{\delta<\lambda} B_\delta,$$

la relación en B_λ está completamente determinada (y cumple trivialmente todas las propiedades requeridas).

Más aún, si suponemos que $\leq^*$ está definida sobre $B_{\alpha+1}$ (es decir, hasta el nivel α), la propiedad 2) determina completamente su extensión a $B_{\alpha+2}$. Así pues, el único paso no trivial consiste en suponer definida $\leq^*$ sobre $B_\lambda = \omega\cdot\lambda$ y extenderla a $B_{\lambda+1}$, es decir, determinar qué elementos de B_λ son anteriores a cada $\omega\cdot\lambda+n \in N_\lambda$.

Numeremos los elementos de $B_\lambda = \omega\cdot\lambda = \{x_n \mid n \in \omega\}$. Vamos a probar que existen cadenas distintas $\{B(n)\}_{n<\omega}$ en B_λ tales que $x_n \in B_n$ y $B(n)$ corta a todos los niveles N_δ para todo $\delta < \lambda$.

Supongamos construidas $B(0),\dots,B(n-1)$ y vamos a construir $B(n)$. En el supuesto de que $B_\lambda = \lambda$ y que A_λ sea una anticadena maximal en B_λ, se cumple que x_n es compatible con un elemento de A_λ (bien sea porque $x_n \in A_\lambda$ y es compatible consigo mismo, bien porque $x_n \notin A_\lambda$ y entonces $A_\lambda \cup \{x_n\}$ no puede ser una anticadena, por la maximalidad de A_λ). Por consiguiente, existen un $x^* \in B_\lambda$ y un $y \in A_\lambda$ tales que $x_n \leq^* x^*$, $y \leq^* x^*$. Si no se dan las hipótesis de la propiedad 4), tomamos $x^* = x_n$.

Tenemos que $\alpha = \operatorname{alt} x^* < \lambda$ y x^* tiene 2 prolongaciones de altura $\alpha+1$, 4 de altura $\alpha+2$, etc., luego si $k > 2^n$, existe un $x^{**} \in N_{\alpha+k}$ tal que $x^* \leq x^{**}$ y que es distinto de los a lo sumo n elementos en los que cada $B(m)$ con $m < n$ corta a $N_{\alpha+k}$.

Sea $\{\beta_m(n)\}_{m\in\omega}$ una sucesión cofinal creciente en λ tal que $\operatorname{alt} x^{**} < \beta_0(n)$. Sean $\{y_m(n)\}_{m\in\omega}$ tales que $y_m(n) \in N_{\beta_m(n)}$ y $x_n <^* y_0(n) <^* y_1(n) <^* \cdots$ (existen por 3). Basta tomar $B(n) = \{z \in B_\lambda \mid \bigvee m \in \omega\ z <^* y_m(n)\}$.

Así $B(n)$ es una cadena distinta de todas las $B(m)$ anteriores, pues contiene a x^{**}, y en el caso en que se den las hipótesis de la propiedad 4) contiene un elemento $y \in A_\lambda$.

Ahora extendemos $\leq^*$ a $B_{\lambda+1}$ estableciendo que los elementos anteriores a $\omega\cdot\lambda+n$ son exactamente los de $B(n)$, con lo que ciertamente $\omega\cdot\lambda+n$ tiene exactamente λ anteriores en $B_{\lambda+1}$, luego N_λ es el nivel λ-ésimo de $B_{\lambda+1}$. Obviamente $B_{\lambda+1}$ cumple las propiedades 1), 2), 3), y también la 4), pues si $B_\lambda = \lambda$ y A_λ es una anticadena maximal en B_λ y $x \in N_\lambda$, entonces $x = \omega\cdot\lambda+n$, para cierto $n \in \omega$ y, por construcción $B(n)$ contiene un $y \in A_\lambda$, luego $y \leq^* x$.

Así pues, tenemos definido un árbol $B = (\omega_1, \leq^*)$ que cumple las propiedades 1), 2), 3) y 4). Por 1) es un $\aleph_1$-árbol y por 2) es ramificado, luego para probar que es un árbol de Suslin basta ver que todas sus anticadenas maximales son numerables (teorema 9.9).

Sea, pues, A una anticadena maximal en B. Entonces todo $\delta \in B = \omega_1$ es compatible con un elemento de A. Sea $f : \omega_1 \longrightarrow \omega_1$ una función que a cada $\delta \in \omega_1$ le asigne un $f(\delta) \in A$ compatible con δ. Consideremos también $g : \omega_1 \longrightarrow \omega_1$ dada por $g(\delta) = \omega\cdot\delta$. Entonces, el conjunto

$$C = \{\lambda < \omega_1 \mid f[\lambda] \subset \lambda, g[\lambda] \subset \lambda\}$$

es c.n.a. en ω_1, y tiene la propiedad de que si $\lambda \in C$, entonces $B_\lambda = \lambda$ y $A \cap \lambda$ es una anticadena maximal en B_λ. En efecto, si $\delta \in B_\lambda$, entonces $\delta = \omega\cdot\alpha+n$, para ciertos $\alpha < \lambda$ y $n < \omega$, luego $\omega\cdot\alpha = g(\alpha) < \lambda$, luego $\delta < \lambda$, y así $B_\lambda \subset \lambda$. La otra inclusión es $\lambda \subset \omega\lambda$, que se da siempre. Además, si $x \in B_\lambda = \lambda$, entonces $f(x) \in A\cap\lambda$ es compatible con x, luego $A\cap\lambda$ es una anticadena maximal en B_λ.

Como el conjunto $\{\alpha < \omega_1 \mid A \cap \alpha = A_\alpha\}$ es estacionario en ω_1, existe un $\lambda \in C$ tal que $A\cap\lambda = A_\lambda$, y así $B_\lambda = \lambda$ y A_λ es una anticadena maximal en A_λ. Se cumple entonces que $A = A\cap B_\lambda = A_\lambda$, pues si existiera $x \in A \setminus B_\lambda$, es decir, si A contuviera un elemento de altura $\geq \lambda$, habría un $x_0 \in N_\lambda = \operatorname{Niv}_\lambda B$ tal que $x_0 \leq x$, y por construcción existe un $y \in A_\lambda$ tal que $y \leq x_0 \leq x$, luego tiene que ser $y = x$, pues A no puede contener elementos compatibles, y así $x \in A_\lambda$. Esto prueba que $A = A_\lambda$ es numerable. ∎

El teorema anterior se generaliza sin dificultad al caso de sucesores de cardinales regulares, si bien necesitamos entonces el caso más fuerte del diamante de Jensen (el que no se sigue de la HCG):

Teorema 9.15 *Sea κ un cardinal regular tal que $2^{<\kappa} = \kappa$ y supongamos que se cumple $\diamondsuit_E$, donde $E = \{\lambda < \kappa^+ \mid \operatorname{cf}\lambda = \kappa\}$. Entonces existe un κ^+-árbol de Suslin.*

DEMOSTRACIÓN: Sea $\{A_\alpha\}_{\alpha\in E}$ una sucesión $\diamondsuit_E$. Siguiendo el esquema del teorema anterior, vamos a definir una relación de orden $\leq^*$ en κ^+ de modo que $B = (\kappa^+, \leq^*)$ sea un árbol de Suslin. Llamaremos análogamente

$$N_\alpha = \{\kappa\cdot\alpha+\delta \mid \delta\in\kappa\},$$

de modo que los conjuntos $\{N_\alpha\}_{\alpha<\kappa^+}$ forman una partición de κ^+ en κ^+ subconjuntos disjuntos dos a dos de cardinal $\leq\kappa$. La construcción garantizará que se cumplen las propiedades siguientes:

1. $\bigwedge\alpha<\kappa^+ \operatorname{Niv}_\alpha B = N_\alpha$,
2. Para cada $\alpha<\kappa^+$ y cada $\delta<\kappa$ se cumple
$$\kappa\cdot\alpha+\delta \leq^* \omega(\alpha+1)+\delta 2 \quad \text{y} \quad \kappa\cdot\alpha+\delta \leq^* \omega(\alpha+1)+\delta 2+1$$
y los miembros derechos son los únicos elementos de $N_{\alpha+1}$ que extienden al miembro izquierdo.
3. Si $\beta<\alpha<\kappa^+$ y $x\in N_\beta$, entonces $\bigvee y\in N_\alpha\ x\leq^* y$.
4. Toda cadena maximal en B tiene altura de cofinalidad κ.
5. Si $\lambda<\kappa^+$, $\operatorname{cf}\lambda=\kappa$, $B_\lambda=\lambda$ y A_λ es una anticadena maximal en B_λ, entonces
$$\bigwedge x\in N_\lambda \bigvee y\in A_\lambda\ y\leq^* x.$$

Estas condiciones implican claramente que B es un κ^+-árbol ramificado. Vamos a definir recurrentemente una estructura de árbol en cada

$$B_\alpha = \bigcup_{\beta<\alpha} N_\beta,$$

de modo que cada B_α contenga como subárboles a los B_β anteriores y cumpla las condiciones 1) – 5), entendiendo la 4) como que la altura de cada cadena maximal en B_α es α o tiene cofinalidad κ.

La definición de $\leq^*$ sobre $B_1=N_0$ es trivial (cada ordinal sólo está relacionado consigo mismo). También es trivial la definición de $\leq^*$ sobre cada B_λ y sobre cada $B_{\alpha+2}$ (en cuyo caso la extensión viene determinada por la propiedad 2). Supongamos construido B_λ y veamos cómo construir $B_{\lambda+1}$. Sea $\mu=\operatorname{cf}\lambda\leq\kappa$.

Veamos en primer lugar que todo $x\in B_\lambda$ está contenido en un camino. En efecto, podemos tomar $\{\delta_\alpha\}_{\alpha<\mu}$ una sucesión cofinal y normal en λ tal que $\operatorname{alt} x=\delta_0$. Definimos una sucesión creciente $\{x_\alpha\}_{\alpha<\mu}$ en B_λ de modo que $\operatorname{alt} x_\alpha=\delta_\alpha$ y $x_0=x$.

Para ello tomamos $x_0=x$, supuesto definido x_α, tomamos $x_{\alpha+1}\in N_{\delta_{\alpha+1}}$ tal que $x_\alpha\leq^* x_{\alpha+1}$ por la propiedad c), y si tenemos $\{x_\alpha\}_{\alpha<\lambda'}$, con $\lambda'<\mu\leq\kappa$, entonces

$$C_{\lambda'} = \{p\in B_\lambda \mid \bigvee\alpha<\lambda'\ x\leq^* x_\alpha\}$$

es una cadena en B_λ de altura $\delta_{\lambda'}$, cuya cofinalidad es $\operatorname{cf}\lambda'\leq\lambda'<\kappa$, luego por 4) no es una cadena maximal en B_λ, luego puede prolongarse a una cadena que contendrá un $x_{\lambda'}$ de altura $\delta_{\lambda'}$.

Con esto termina la construcción de la sucesión, la cual nos da a su vez una cadena C_μ de altura λ (es decir, un camino) que contiene a x.

Supongamos ahora que $\mu = \operatorname{cf}\lambda < \kappa$. Entonces, cada camino C en B_λ está determinado por

$$\{p \in C \mid \bigvee \alpha < \mu \ \operatorname{alt} p = \delta_\alpha\},$$

luego el número de caminos en B_λ es a lo sumo $|{}^\mu B_\lambda| \leq \kappa^\mu \leq \kappa^{<\kappa} = 2^{<\kappa} = \kappa$. De hecho, el número de caminos es exactamente igual a κ, pues cada elemento de N_0 pertenece a un camino distinto. Por consiguiente, podemos fijar una enumeración $\{C_\delta\}_{\delta<\kappa}$ de todos los caminos de B_λ y establecer que cada $\kappa\cdot\lambda+\delta$ está por encima de todos los elementos de C_δ y sólo de ellos. Esto hace que cada elemento de N_λ tenga altura λ en $B_{\lambda+1}$ y que no haya cadenas maximales de altura λ, pues todas ellas se extienden a cadenas de altura $\lambda+1$. Así $B_{\lambda+1}$ cumple las propiedades 1), 3), 4), y las demás se cumplen trivialmente.

Supongamos ahora que $\operatorname{cf}\lambda = \kappa$ pero no se cumple que $B_\lambda = \lambda$ y que A_λ es una cadena maximal en B_λ. Entonces repetimos la construcción anterior pero no con una enumeración de todos los caminos, sino que enumeramos los elementos de B_λ, digamos $\{x_\delta\}_{\delta<\kappa}$, y elegimos caminos $\{C_\delta\}_{\delta<\kappa}$ de modo que $x_\delta \in C_\delta$. Con esto conseguimos que se sigan cumpliendo las propiedades 1) y 3), y las demás se cumplen trivialmente.

Por último, supongamos que se cumplen las hipótesis de la propiedad e). Entonces, cada $x_\delta \in B_\lambda$ es compatible con un elemento de A_λ, lo cual significa que podemos tomar $y_\delta \in B_\lambda$ y $a_\delta \in A_\lambda$ de modo que $x_\delta <^* y_\delta$, $a_\delta <^* y_\delta$. Entonces, para cada $x_\delta \in B_\lambda$ elegimos un camino C_δ que contenga a y_δ y definimos con ellos $B_{\lambda+1}$.

Con esto tenemos construido el κ^+-árbol ramificado B. Sea A una anticadena en B, que podemos suponer maximal. Como en la prueba del teorema anterior, existe un conjunto c.n.a.

$$C \subset \{\lambda < \kappa^+ \mid B_\lambda = \lambda \wedge B_\lambda \cap A \text{ es una anticadena maximal en } B_\lambda\}$$

es c.n.a. en κ^+. Como el conjunto $\{\lambda \in E \mid A \cap \lambda = A_\lambda\}$ es estacionario en κ^+, podemos tomar $\lambda \in C$ tal que $A \cap \lambda = A_\lambda$. Así $A_\lambda \subset A$ es una anticadena maximal en B_λ. Ahora bien, todo elemento de B de altura $\geq \lambda$ tiene bajo sí un elemento de N_λ, el cual, por la propiedad 5), tiene bajo sí un elemento de A_λ, luego un elemento de A. Esto implica que $A = A_\lambda$, luego tiene cardinal $\leq \kappa$. ∎

Así pues, tenemos probado que es consistente que existan κ-árboles de Suslin (es decir, que no se puede probar que no existen) salvo si κ es inaccesible o bien es el sucesor de un cardinal singular. Vamos a probar ahora que en el último caso también es consistente la existencia de κ-árboles de Suslin:

Teorema 9.16 *Sea κ un cardinal infinito tal que existe $E \subset \kappa^+$ estacionario de modo que se cumplen $\square_\kappa(E)$ y $\diamondsuit_E$. Entonces existe un κ^+-árbol de Suslin.*

DEMOSTRACIÓN: Sea $\{A_\alpha\}_{\alpha\in E}$ una sucesión $\diamondsuit_E$ y sea $\{C_\lambda\}_{\lambda<\kappa^+}$ una sucesión $\square_\kappa(E)$. Vamos a construir un árbol sobre κ^+ siguiendo exactamente el mismo planteamiento de la demostración del teorema anterior, salvo que ahora la construcción garantizará los hechos siguientes:

1. $\bigwedge\alpha<\kappa^+\ \mathrm{Niv}_\alpha B=N_\alpha$,
2. Para cada $\alpha<\kappa^+$ y cada $\delta<\kappa$ se cumple

$$\kappa\cdot\alpha+\delta\le^*\omega(\alpha+1)+\delta 2\quad\text{y}\quad\kappa\cdot\alpha+\delta\le^*\omega(\alpha+1)+\delta 2+1$$

   y los miembros derechos son los únicos elementos de $N_{\alpha+1}$ que extienden al miembro izquierdo.
3. Si $\beta<\alpha<\kappa^+$ y $x\in N_\beta$, entonces $\bigvee y\in N_\alpha\ x\le^* y$.
4. Toda cadena de altura límite λ está bajo un único elemento de N_λ.
5. Si $\lambda\in E$, $B_\lambda=\lambda$ y A_λ es una anticadena maximal en B_λ, entonces

$$\bigwedge x\in N_\lambda\bigvee y\in A_\lambda\ y\le^* x.$$

El problema es cómo extender la relación de orden $\le^*$ de B_λ a $B_{\lambda+1}$.

Dado $x\in B_\lambda$, trataremos de encontrar un camino en B_λ que contenga a x. Sea $\{\gamma_\lambda(\alpha)\}_{\alpha<\theta_\lambda}$ la semejanza de C_λ en su ordinal θ_λ. Sea $\alpha_\lambda(x)$ el mínimo $\alpha_\lambda(x)<\theta_\lambda$ tal que $x\in B_{\gamma_\lambda(\alpha_\lambda(x))}$. Definimos una sucesión $\{p^x_\lambda(\alpha)\}_{\alpha_\lambda(x)\le\alpha<\theta_\lambda}$ como sigue:

- $p^x_\lambda(\alpha_\lambda(x))$ es el mínimo ordinal $y\in N_{\gamma_\lambda(\alpha_\lambda(x))}$ tal que $x\le^* y$.
- $p^x_\lambda(\alpha+1)$ es el mínimo ordinal $y\in B_{\gamma_\lambda(\alpha+1)}$ tal que $p^x_\lambda(\alpha)\le^* y$.
- $p^x_\lambda(\lambda')$ es el único ordinal $y\in N_{\gamma_\lambda(\lambda')}$ tal que

$$\bigwedge\alpha<\lambda'(\alpha_\lambda(x)\le\alpha\to p^x_\lambda(\alpha)\le^* y).$$

Observemos que el ordinal y requerido existe sin duda en los dos primeros casos por la propiedad 3). Sin embargo, no es evidente que exista en el tercer caso (pero si existe es único, por la propiedad 4). Supongamos de momento que existe un único y para cada x, de modo que la función p^x_λ puede ser definida. En tal caso podemos definir

$$C^x_\lambda=\{y\in B_\lambda\mid\bigvee\alpha<\theta_\lambda\ y\le^* p^x_\lambda(\alpha)\},$$

que claramente es un camino en B_λ que contiene a x. Extendemos la estructura de árbol a $B_{\lambda+1}$ distinguiendo dos casos:

Si no se cumple que $\lambda\in E$, $B_\lambda=\lambda$ y $A_\lambda\cap\lambda$ es una anticadena maximal de B_λ, numeramos todos los caminos C^x_λ que hemos construido, digamos $\{C^\delta_\lambda\}_{\delta<\kappa}$, y establecemos que por encima de cada C^δ_λ esté únicamente $\kappa\cdot\lambda+\delta$.

En caso contrario, consideramos únicamente los caminos correspondientes a ordinales $x \in B_\lambda$ que tienen por debajo un elemento de A_λ. Notemos que por la maximalidad de $A_\lambda \cap \lambda$ todo elemento de $B_\lambda = \lambda$ es compatible con un elemento de A_λ, luego está en uno de los caminos considerados, luego con esta construcción todo elemento de B_λ tiene una extensión en N_λ.

Esto termina la construcción de B, que es claramente un κ^+-árbol ramificado, supuesto que para todo λ haya sido posible construir las funciones p^x_λ. Vamos a probar que esto es así considerando, por reducción al absurdo, el mínimo λ para el que existe un $x \in B_\lambda$ que no permite construir la función p^x_λ. Esto sólo puede deberse a que existe un λ' entre $\alpha_\lambda(x)$ y θ_λ para el que no existe el y requerido.

Tenemos que $\gamma_\lambda(\lambda')$ es un punto de acumulación de C_λ. Por la definición de $\square_\kappa(E)$ tenemos que $\gamma_\lambda(\lambda') \notin E$ y que $C_{\gamma_\lambda(\lambda')} = C_\lambda \cap \gamma_\lambda(\lambda') = \{\gamma_\lambda(\alpha) \mid \alpha < \lambda'\}$.

Esto significa que la enumeración de $C_{\gamma_\lambda(\lambda')}$ es simplemente la restricción a λ' de la de C_λ, luego la función $p^x_{\gamma_\lambda(\lambda')}$ es el fragmento de p^x_λ que puede definirse hasta que la construcción falla en λ', y el problema es que el camino $C^x_{\gamma_\lambda(\lambda')}$ no tiene una extensión a $N_{\gamma_\lambda(\lambda')}$, pero eso es imposible, porque como $\gamma_\lambda(\lambda') \notin E$, la construcción al nivel $\gamma_\lambda(\lambda')$ se hace de modo que todos los caminos $C^x_{\gamma_\lambda(\lambda')}$ se prolongan hasta $N_{\gamma_\lambda(\lambda')}$.

Esto prueba que el árbol B está bien definido y sólo falta probar que toda anticadena maximal A cumple $|A| \leq \kappa$. Pero esto se prueba exactamente igual que en 9.15: existe un $\lambda \in E$ tal que $B_\lambda = \lambda$ y $A \cap \lambda = A_\lambda$ es una anticadena maximal en B_λ. Todo elemento de B de altura $\geq \lambda$ tiene bajo sí un elemento de N_λ, el cual, por la propiedad e), tiene bajo sí un elemento de A_λ, luego un elemento de A. Por lo tanto, $A = A_\lambda$ cumple $|A| \leq \kappa$. ∎

Nota El teorema 6.36 nos da una situación alternativa en la que también existen κ^+-árboles de Suslin: $2^{<\kappa} = \kappa \wedge 2^\kappa = \kappa^+ \wedge \square_\kappa$. ∎

9.4 Árboles de Aronszajn

Los teoremas 9.3 y 9.4 invitan a conjeturar si las hipótesis del segundo no podrían relajarse para obtener la generalización natural del primero, es decir, que todo κ-árbol tiene un camino. Sin embargo esto resulta ser falso si consideramos $\aleph_1$-árboles:

Definición 9.17 Un *árbol de Aronszajn* es un $\aleph_1$-árbol cuyas cadenas son todas numerables, es decir, que no tiene caminos.

Claramente, si A es un árbol de Aronszajn y A' es un subárbol bien podado, entonces A' es un árbol de Aronszajn bien podado. Todo árbol de Suslin es en particular un árbol de Aronszajn.

La situación es curiosa: Imaginemos que estamos en la raíz x_0 de un árbol de Aronszajn bien podado y nos disponemos a trepar por él lo más alto que podamos. Tenemos varias opciones para pasar al nivel 1, pero no importa cuál tomemos, pues desde cualquier punto x_1 del nivel 1 podemos llegar hasta cualquier otro nivel. Igualmente no importa a qué punto x_2 del nivel 2 saltemos, pues desde él se podrá llegar seguro a cualquier altura. Pero cuando hayamos dado ω pasos por la ruta $x_0 < x_1 < x_3 < \cdots$ podemos encontrarnos con que la rama se acaba aquí, que no hay ningún punto en el árbol mayor que todos éstos. Podemos rectificar la ruta desde cualquier paso previo para garantizar que llegamos al nivel ω. Por ejemplo, si estamos dispuestos a cambiar a partir del nivel 2 tomamos un $x_\omega > x_1$ y seguimos el camino $x_0 < x_1 < x'_2 < x'_3 < \cdots < x_\omega$ formado por los nodos anteriores a x_ω. A partir de aquí podemos pasar a un $x_{\omega+1}$ en el nivel $\omega + 1$, etc., hasta determinar una cadena

$$x_0 < x_1 < x'_2 < x'_3 < \cdots < x_\omega < x_{\omega+1} < x_{\omega+2} < \cdots$$

pero de nuevo podemos encontrarnos con que esta rama se acaba aquí, y que para llegar más arriba hubiera sido necesario desviarse en cualquiera de los pasos previos. El hecho de que A sea un árbol de Aronszajn significa precisamente que, tarde o temprano, hagamos lo que hagamos, terminaremos en una rama numerable que no puede prolongarse más. Podemos subir tan alto como queramos, pero siempre llegará un momento en que para seguir subiendo tendremos que bajar un poco y cambiar de dirección. Ésta es la característica de los árboles de Aronszajn.

La existencia de árboles tan peculiares es dudosa, pero vamos a disipar la duda construyendo uno.

Definición 9.18 Si I es un conjunto no vacío y α un ordinal, llamaremos *árbol completo I-ádico de altura α* al conjunto $I^{<\alpha}$ con el orden dado por la inclusión.

Es claro que $I^{<\alpha}$ es un árbol de altura α cuyo nivel β (para $\beta < \alpha$) es I^β.

Teorema 9.19 (Aronszajn) *Existe un árbol de Aronszajn.*

Demostración: Partiremos de $A = \{s \in \omega^{<\omega_1} \mid s \text{ es inyectiva}\}$, que es un subárbol de $\omega^{<\omega_1}$. Es claro que para cada $\alpha < \omega_1$ se cumple que

$$\mathrm{Niv}_\alpha A = \{s \in {}^\alpha\omega \mid s \text{ es inyectiva}\} \neq \varnothing,$$

luego $\mathrm{alt}A = \aleph_1$. Si C fuera una cadena no numerable en A entonces $f = \bigcup_{a\in C} a$ es una función, porque los elementos de C son compatibles, y habría de ser $f : \omega_1 \longrightarrow \omega$ inyectiva, lo cual es absurdo. Por lo tanto las cadenas de A son numerables. Sin embargo, A no es un árbol de Aronszajn porque sus niveles son no numerables.

Definimos en cada conjunto ${}^\alpha\omega$ la relación de equivalencia dada por

$$s \approx t \leftrightarrow \{\beta < \alpha \mid s(\beta) \neq t(\beta)\} \text{ es finito.}$$

Vamos a construir recurrentemente una sucesión $\{s_\alpha\}_{\alpha<\omega_1}$ tal que

1. $s_\alpha \in {}^\alpha\omega$ es inyectiva,

2. Si $\alpha < \beta < \omega_1$, entonces $s_\alpha \approx s_\beta|_\alpha$,

3. $\omega \setminus s_\alpha[\alpha]$ es infinito.

Tomamos $s_0 = \varnothing$. Definido s_α, tomamos cualquier $n \in \omega \setminus s_\alpha[\alpha]$ y es fácil ver que $s_{\alpha+1} = s_\alpha \cup \{(\alpha, n)\}$ cumple lo pedido. Supongamos definidos $\{s_\delta\}_{\delta<\lambda}$, para un límite $\lambda < \omega_1$.

Sea $\{\alpha_n\}_{n<\omega}$ una sucesión cofinal creciente en λ. Vamos a definir una sucesión de aplicaciones inyectivas $t_n : \alpha_n \longrightarrow \omega$ tales que $t_0 = s_{\alpha_0}$ y para todo $n \in \omega$ se cumpla $t_n \approx s_{\alpha_n} \wedge t_{n+1}|_{\alpha_n} = t_n$.

Supuesto que estén definidas $t_0, \ldots, t_n$, tenemos que $s_{\alpha_{n+1}}|_{\alpha_n} \approx t_n$, luego si definimos

$$t^*_{n+1}(\beta) = \begin{cases} t_n(\beta) & \text{si } \beta < \alpha_n, \\ s_{\alpha_{n+1}}(\beta) & \text{si } \alpha_n \le \beta, \end{cases}$$

la inyectividad de $s_{\alpha_{n+1}}$ se pierde a lo sumo en un número finito de ordinales $\alpha_n \le \beta < \alpha_{n+1}$. Por lo tanto, podemos definir t_{n+1} que difiera de t^*_{n+1} únicamente en dichos ordinales, haciendo que tome valores (distintos dos a dos) en el conjunto (infinito) $\omega \setminus t^*_{n+1}[\alpha_{n+1}]$. Así t_{n+1} es inyectiva y cumple lo requerido.

Sea $t = \bigcup_{n\in\omega} t_n$. Claramente $t : \lambda \longrightarrow \omega$ inyectiva. Definimos $s_\lambda : \lambda \longrightarrow \omega$ mediante

$$s_\lambda(\beta) = \begin{cases} t(\alpha_{2n}) & \text{si } \beta = \alpha_n, \\ t(\beta) & \text{en otro caso.} \end{cases}$$

De este modo, si $\alpha < \lambda$ será $\alpha < \alpha_n$ para cierto $n < \omega$, y entonces $s_\lambda|_\alpha \approx t_n|_\alpha$ (pues se diferencian a lo sumo en $\alpha_0, \ldots, \alpha_{n-1}$), luego $s_\lambda|_\alpha \approx s_{\alpha_n}|_\alpha \approx s_\alpha$.

Además $\{t(\alpha_{2n+1}) \mid n \in \omega\} \subset \omega \setminus s_\lambda[\lambda]$, con lo que este último conjunto es infinito y se cumple todo lo pedido.

Definimos $A^* = \bigcup_{\alpha<\omega_1} \{t \in \mathrm{Niv}_\alpha A \mid t \approx s_\alpha\}$. Así A^* es un subárbol de A, pues si $x \in A^*$, $y \in A$, $y < x$, digamos que $\mathrm{alt}_A x = \alpha$, $\mathrm{alt}_A y = \beta$, entonces $x \approx s_\alpha$, luego $y = x|_\beta \approx s_\alpha|_\beta \approx s_\beta$ y por consiguiente $y \in A^*$.

Para cada $\alpha < \omega_1$ se cumple que $s_\alpha \in \mathrm{Niv}_\alpha A^*$, luego $\mathrm{alt} A^* = \aleph_1$. Como en A no hay cadenas numerables, tampoco las hay en A^*. Finalmente,

$$\mathrm{Niv}_\alpha A^* = \{t \in {}^\alpha\omega \mid t \approx s_\alpha \wedge t \text{ inyectiva}\} \subset \bigcup_{\substack{x\subset\alpha \\ \text{finito}}} \{t \in {}^\alpha\omega \mid t|_{\alpha\setminus x} = s_\alpha|_{\alpha\setminus x}\},$$

y el miembro derecho es una unión numerable de conjuntos numerables. Concluimos que A^* es un árbol de Aronszajn. ∎

Más en general:

Definición 9.20 Un *κ-árbol de Aronszajn* es un κ-árbol cuyas cadenas tienen todas cardinal $< \kappa$, es decir, un κ-árbol sin caminos.

En estos términos hemos probado que no existen $\aleph_0$-árboles de Aronszajn, pero sí $\aleph_1$-árboles de Aronszajn. Por otra parte, es inmediato que si κ es un cardinal singular existen κ-árboles de Aronszajn. El árbol considerado en la nota tras el teorema 9.2 es un ejemplo. Para cardinales regulares $> \aleph_1$ la existencia o no de árboles de Aronszajn depende de la aritmética cardinal. El teorema anterior admite la generalización siguiente:

Teorema 9.21 *Sea κ un cardinal regular tal que $2^{<\kappa} = \kappa$. Entonces existe un κ^+-árbol de Aronszajn.*

DEMOSTRACIÓN: El caso en que $\kappa = \aleph_0$ se reduce al teorema 9.19, así que podemos suponer que $\kappa > \aleph_0$. Siguiendo el argumento de 9.19, partimos del árbol $A = \{s \in \kappa^{<\kappa^+} \mid s \text{ es inyectiva}\}$, que tiene claramente altura κ^+ y todas sus cadenas tienen cardinal $< \kappa^+$. Ahora definimos en cada ${}^\alpha\kappa$ la relación dada por

$$s \approx t \leftrightarrow |\{\beta < \alpha \mid s(\beta) \neq t(\beta)\}| < \kappa$$

y construimos recurrentemente una sucesión $\{s_\alpha\}_{\alpha<\kappa^+}$ tal que

1. $s_\alpha \in {}^\alpha\kappa$ es inyectiva,
2. Si $\alpha < \beta < \kappa^+$, entonces $s_\alpha \approx s_\beta|_\alpha$,
3. $s_\alpha[\alpha]$ no es estacionario en κ.

Tomamos $s_0 = \varnothing$. Definido s_α, tomamos cualquier $\delta \in \kappa \setminus s_\alpha[\alpha]$ y es fácil ver que $s_{\alpha+1} = s_\alpha \cup \{(\alpha, \delta)\}$ cumple lo pedido.

Supongamos definidos $\{s_\delta\}_{\delta<\lambda}$, para un límite $\lambda < \kappa^+$. Sea $\nu = \operatorname{cf}\lambda \leq \kappa$. Sea $\{\alpha_\eta\}_{\eta<\nu}$ una sucesión cofinal y normal en λ. Podemos suponer que $\kappa < \alpha_0$.

Para cada $\eta < \nu$, sea C_η un c.n.a. en κ tal que $s_{\alpha_\eta}[\alpha_\eta] \cap C_\eta = \varnothing$. Si $\nu < \kappa$, sea $C = \bigcap_{\eta<\nu} C_\eta$, y si $\nu = \kappa$, entonces sea $C = \triangle_{\eta<\kappa} C_\eta \setminus \{0\}$. En ambos casos C es c.n.a. en κ y $s_{\alpha_\eta}[\alpha_\eta] \cap C \subset \eta + 1 < \kappa$.

Definimos una sucesión de aplicaciones inyectivas $t_\eta : \alpha_\eta \longrightarrow \kappa \setminus C$ tales que $t_\eta \approx s_{\alpha_\eta}$ y si $\eta < \eta' < \nu$ entonces $t_{\eta'}|_{\alpha_\eta} = t_\eta$.

Como $s_{\alpha_0}[\alpha_0] \cap C = \varnothing$, podemos tomar $t_0 = s_{\alpha_0} : \alpha_0 \longrightarrow \kappa \setminus C$. Supongamos definido t_η. Como $s_{\alpha_{\eta+1}}[\alpha_{\eta+1}] \cap C \subset \eta + 2 < \kappa$, tenemos que $A = s^{-1}_{\alpha_{\eta+1}}[C]$ cumple $|A| < \kappa$, luego $|s_{\alpha_{\eta+1}}[\alpha_{\eta+1} \setminus \alpha_\eta] \setminus C| = \kappa$, luego podemos tomar un conjunto $B \subset \alpha_{\eta+1} \setminus \alpha_\eta$ tal que $|B| = |A|\aleph_0$ y $s_{\alpha_{\eta+1}}[B] \subset \kappa \setminus C$. Tomamos una biyección $g : A \cup B \longrightarrow s_{\alpha_{\eta+1}}[B]$ y definimos

$$t_{\eta+1}(\beta) = \begin{cases} t_\eta(\beta) & \text{si } \beta < \alpha_\eta, \\ s_{\alpha_{\eta+1}}(\beta) & \text{si } \beta \in \alpha_{\eta+1} \setminus (\alpha_\eta \cup A \cup B), \\ g(\beta) & \text{si } \beta \in A \cup B. \end{cases}$$

Es claro entonces que $t_{\eta+1} : \alpha_{\eta+1} \longrightarrow \kappa \setminus C$ inyectiva, extiende a t_η y además $t_{\eta+1} \approx s_{\alpha_{\eta+1}}$, pues difieren únicamente en $A \cup B$ y donde difieren t_η y s_{α_η}, lo cual es un conjunto de cardinal $< \kappa$.

En tercer lugar, si están definidos $\{t_\eta\}_{\eta<\lambda'}$, basta tomar

$$t_{\lambda'} = \bigcup_{\eta<\lambda'} t_\eta : \alpha_{\lambda'} \longrightarrow \kappa \setminus C,$$

claramente inyectiva. Se cumple que $t_{\lambda'} \approx s_{\alpha_{\lambda'}}$, pues

$$\{\beta < \alpha_{\lambda'} \mid t_{\lambda'}(\beta) \neq s_{\alpha_{\lambda'}}(\beta)\} \subset \bigcup_{\eta<\lambda'} \{\beta < \alpha_\eta \mid t_\eta(\beta) \neq s_{\alpha_{\lambda'}}(\beta)\}$$

$$\subset \bigcup_{\eta<\lambda'} \big(\{\beta < \alpha_\eta \mid t_\eta(\beta) \neq s_{\alpha_\eta}(\beta)\} \cup \{\beta < \alpha_\eta \mid s_{\alpha_\eta}(\beta) \neq s_{\alpha_{\lambda'}}(\beta)\}\big)$$

y se trata de una unión de menos de κ conjuntos de cardinal menor que κ.

Así pues, podemos definir $s_\lambda = \bigcup_{\eta<\nu} t_\eta : \lambda \longrightarrow \kappa \setminus C$ inyectiva. Trivialmente $s_\lambda[\lambda]$ no es estacionario en κ, pues no corta a C y si $\delta < \lambda$ existe un $\eta < \nu$ tal que $\delta < \alpha_\eta < \lambda$, con lo que $s_\lambda|_\delta = t_\eta|_\delta \approx s_{\alpha_\eta}|_\delta \approx s_\delta$.

Definimos $A^* = \bigcup_{\alpha<\kappa^+} \{t \in \mathrm{Niv}_\alpha A \mid t \approx s_\alpha\}$, que es un subárbol de A, luego no tiene cadenas de cardinal κ y, como $s_\alpha \in \mathrm{Niv}_\alpha A^*$, vemos que $\mathrm{alt} A^* = \kappa^+$. Finalmente,

$$\mathrm{Niv}_\alpha A^* = \{t \in {}^\alpha\kappa \mid t \approx s_\alpha \wedge t \text{ inyectiva}\} \subset \bigcup_{x\in[\alpha]^{<\kappa}} \{t \in {}^\alpha\kappa \mid t|_{\alpha\setminus x} = s_\alpha|_{\alpha\setminus x}\},$$

y bajo las hipótesis del teorema tenemos que

$$|[\alpha]^{<\kappa}| \leq \kappa^{<\kappa} = (2^{<\kappa})^{<\kappa} = 2^{<\kappa}) = \kappa,$$

$$|\{t \in {}^\alpha\kappa \mid t|_{\alpha\setminus x} = s_\alpha|_{\alpha\setminus x}\}| = |\kappa^x| \leq \kappa^{<\kappa} = \kappa,$$

luego $|\mathrm{Niv}_\alpha A^*| \leq \kappa < \kappa^+$ y concluimos que A^* es un κ^+-árbol de Aronszajn. ∎

Teniendo en cuenta que la hipótesis del continuo generalizada implica que todo cardinal infinito cumple $2^{<\kappa} = \kappa$, ahora es inmediato lo siguiente:

Teorema 9.22 (HCG) *Existen κ-árboles de Aronszajn para todo cardinal κ no numerable salvo a lo sumo si κ es inaccesible o el sucesor de un cardinal singular.*

En el caso del sucesor de un cardinal singular tenemos el teorema 9.16, que prueba que prueba la consistencia de que exista un κ^+-árbol de Suslin, luego en particular de Aronszajn, a partir de los principios combinatorios oportunos (véase también la nota posterior).

Árboles de Aronszajn especiales En el teorema 9.19 hemos construido un árbol de Aronszajn, pero sabemos que no podemos demostrar la existencia de árboles de Suslin, así que no podemos aspirar a demostrar que el árbol del teorema 9.19 no tenga anticadenas no numerables. Vamos a ver ahora que, no sólo no podemos demostrar que no las tiene, sino que podemos demostrar que las tiene. Para ello conviene dar nombre a una propiedad adicional:

Definición 9.23 Un árbol de Aronszajn es *especial* si se descompone en una unión numerable de anticadenas.

Veamos algunas caracterizaciones de estos árboles:

Teorema 9.24 *Sea A un árbol de Aronszajn. Las afirmaciones siguientes son equivalentes:*

1. *A es especial.*
2. *Existe $f : A \longrightarrow \omega$ tal que $\bigwedge pq \in A\,(p < q \to f(p) \neq f(q))$.*
3. *Existe $f : A \longrightarrow \mathbb{Q}$ estrictamente creciente.*

DEMOSTRACIÓN: 1) $\Rightarrow$ 2) es trivial: si $A = \bigcup_{n\in\omega} A_n$, donde cada A_n es una anticadena, podemos suponer que los conjuntos A_n son disjuntos dos a dos, y entonces basta definir $f(p) = n \leftrightarrow p \in A_n$.

2) $\Rightarrow$ 3) Dada $f : A \longrightarrow \omega$ según b), definimos $g : A \longrightarrow \mathbb{Q}$ mediante

$$g(p) = \sum_{n\in I_p} 2^{-n},$$

donde $I_p = \{n \leq f(p) \mid \bigvee q \leq p\ f(q) = n\}$. Veamos que es estrictamente creciente. Para ello tomamos $p_1 < p_2$. Observemos que dos elementos $\leq p_2$ son compatibles, luego no pueden tener la misma imagen por f, luego, o bien $f(p_1) < f(p_2)$ o bien $f(p_2) < f(p_1)$.

Si $f(p_1) < f(p_2)$, entonces $I_{p_1} \subsetneq I_{p_2}$ y es claro que $g(p_1) < g(p_2)$. Supongamos, pues, que $f(p_2) < f(p_1)$. Entonces $f(p_1) \in I_{p_1} \setminus I_{p_2}$, luego podemos tomar $n_0 = \min(I_{p_1} \setminus I_{p_2})$. Tiene que ser $n_0 > f(p_2)$, pues si $n_0 \leq f(p_2)$ (teniendo en cuenta que $n_0 \in I_{p_1}$) trivialmente $n_0 \in I_{p_2}$. Entonces

$$g(p_1) = \sum_{n\in I_{p_1}\cap I_{p_2}} 2^{-n} + \sum_{n\in I_{p_1}\setminus I_{p_2}} 2^{-n} \leq \sum_{n\in I_{p_1}\cap I_{p_2}} 2^{-n} + 2^{-(n_0-1)}$$

$$< \sum_{n\in I_{p_1}\cap I_{p_2}} 2^{-n} + 2^{-f(p_2)} \leq g(p_2).$$

3) $\Rightarrow$ 1) es trivial, pues cada $f^{-1}[\{q\}]$, con $q \in \mathbb{Q}$, es una anticadena en A. ∎

Conviene observar que la condición 3) del teorema anterior puede debilitarse un poco:

Teorema 9.25 *Sea A un árbol de Aronszajn y $C \subset \omega_1$ un c.n.a. Supongamos que existe $f : \bigcup_{\alpha\in C} \mathrm{Niv}_\alpha A \longrightarrow \mathbb{Q}$ estrictamente creciente. Entonces A es especial.*

Demostración: Llamemos $B = \bigcup_{\alpha\in C} \mathrm{Niv}_\alpha A$. Observemos que no perdemos generalidad si suponemos que $0 \in C$. En efecto, si $f[B]$ no estuviera acotado inferiormente en $\mathbb{Q}$, siempre podemos componer f con una aplicación estrictamente creciente que transforme $\mathbb{Q}$ en $\mathbb{Q}^+$, por ejemplo, y así "queda espacio" para extender f a $\mathrm{Niv}_0 A$ de forma que siga siendo estrictamente creciente.

Como C es c.n.a., es el rango de una función normal $C = \{\alpha_\delta\}_{\delta<\omega_1}$, con $\alpha_0 = 0$. Para cada $\beta \in \omega_1$ existe un único $\delta < \omega_1$ tal que $\alpha_\delta \le \beta < \alpha_{\delta+1}$.

Por otro lado, cada conjunto $f^{-1}[r]$, con $r \in \mathbb{Q}$ es una anticadena en B, luego enumerando las no vacías podemos expresar $B = \bigcup_{n\in\omega} B_n$ como una unión numerable de anticadenas.

Cada $s \in \mathrm{Niv}_{\alpha_\delta} A$ tiene una cantidad numerable de extensiones $\{s_{\delta,m}\}_{m<\omega}$ de altura menor que $\alpha_{\delta+1}$. Llamamos

$$B_{nm} = \{t \in A \mid \bigvee \delta < \omega_1 \bigvee s \in \mathrm{Niv}_{\alpha_\delta} A\ (t = s_{\delta,m} \wedge s \in B_n)\},$$

de modo que $A = \bigcup_{m,n} B_{mn}$, pues si $t \in A$ tiene altura β y $\alpha_\delta \le \beta < \alpha_{\delta+1}$, necesariamente $t = s_{\delta,m}$, para cierto $m \in \omega$.

Ahora basta observar que cada B_{nm} es una anticadena, pues si $t = s_{\delta,m}$, $t' = s'_{\epsilon,m}$ de modo que s, $s' \in B_n$ y $\neg t \perp t'$, entonces $\neg s \perp s'$, luego $s = s'$, luego $\delta = \epsilon$, luego $t = t'$. ∎

Una característica notable de los árboles de Aronszajn especiales es que no pueden ser de Suslin:

Teorema 9.26 *Un árbol de Aronszajn especial no es un árbol de Suslin.*

Demostración: Como un árbol de Aronszajn tiene cardinal $\aleph_1$, si se descompone en una unión numerable de anticadenas, una de ellas debe ser no numerable, luego no puede ser un árbol de Suslin. ∎

El árbol de Aronszajn construido en el teorema 9.19 no es necesariamente especial, pero contiene un árbol especial que hace que tampoco pueda ser un árbol de Suslin. En efecto, lo vemos en la prueba del teorema siguiente:

Teorema 9.27 *Existe un árbol de Aronszajn especial*

Demostración: Con la prueba del teorema 9.19 hemos obtenido un árbol de Aronszajn A^* formado por aplicaciones inyectivas $s : \alpha \longrightarrow \omega$ con $\alpha < \omega_1$ y en el que la relación de orden es la inclusión (de modo que la altura de s coincide con su dominio). Para obtener un árbol de Aronszajn especial basta definir B como el conjunto de los elementos de A^* cuyo dominio es un ordinal sucesor, también con el orden dado por la inclusión.

Es claro que B sigue siendo un $\aleph_1$-árbol. De hecho, $\mathrm{Niv}_\alpha B = \mathrm{Niv}_{\alpha+1} A^*$. Pero en B podemos definir la aplicación $f : B \longrightarrow \omega$ dada por $f(s) = s(\max \mathcal{D}s)$, y es claro que si $s < t$ son elementos de B, entonces $f(s) \neq f(t)$, ya que en caso contrario t tomaría dos veces el valor $f(t)$.

Esto implica que B es unión numerable de anticadenas, y esto a su vez implica que no tiene cadenas no numerables, pues una cadena sólo puede tener un elemento en común con una anticadena. Por lo tanto B es un árbol de Aronszajn especial. ∎

Así, el árbol B que acabamos de construir contiene una anticadena no numerable, que también será una anticadena no numerable del árbol A^*, luego éste tampoco es un árbol de Suslin.

Ahora podemos dar una tercera prueba de que $\mathrm{AM}(\aleph_1) \to \mathrm{HS}$, puesto que si todo árbol de Aronszajn es especial, no puede haber árboles de Suslin:

Teorema 9.28 $\mathrm{AM}(\aleph_1)$ *implica que todo árbol de Aronszajn es especial.*

DEMOSTRACIÓN: Sea A un árbol de Aronszajn y definimos $\mathbb{P}$ como el conjunto de todas las aplicaciones $p : a \longrightarrow \omega$ tales que $a \subset A$ es finito y $\bigwedge st \in a(s < t \to p(s) \neq p(t))$. Consideramos a $\mathbb{P}$ como c.p.o. con el orden dado por la inversa de la inclusión.

El único problema técnico es demostrar que $\mathbb{P}$ cumple la c.c.n. Aceptando esto, basta tener en cuenta que, para cada $s \in A$, el conjunto

$$D_s = \{p \in \mathbb{P} \mid s \in \mathcal{D}p\}$$

es denso en $\mathbb{P}$, y en total hay $\aleph_1$ subconjuntos de esta forma, luego $\mathrm{AM}(\aleph_1)$ implica que existe un filtro G en $\mathbb{P}$ que los corta a todos ellos. Es claro que $f = \bigcup G : A \longrightarrow \omega$ cumple el apartado 2) del teorema 9.24, lo que implica que A es especial.

Veamos, pues, que $\mathbb{P}$ cumple la c.c.n. Para ello fijamos un conjunto no numerable $C \subset \mathbb{P}$ y vamos a probar que no puede ser una anticadena. El conjunto $\{\mathcal{D}p \mid p \in C\}$ no puede ser numerable, pues entonces habría una cantidad no numerable de condiciones con el mismo dominio finito, lo cual es absurdo. Por lo tanto podemos aplicar el lema de los sistemas Δ (teorema 8.54), reduciendo C podemos suponer que $\{\mathcal{D}p \mid p \in C\}$ es una familia cuasidisjunta no numerable de raíz $r \subset A$. Más aún, como el conjunto $\{p|_r \mid p \in C\}$ tiene que ser numerable, podemos restringir C aún más y suponer que existe $p_0 : r \longrightarrow \omega$ tal que $\bigwedge p \in C\ p|_r = p_0$ (siempre sin perder la no numerabilidad de C). No obstante, esto no garantiza que las condiciones de C sean compatibles. Para concluir la prueba sólo tenemos que demostrar lo siguiente:

> *Sea A un árbol de Aronszajn y S una familia no numerable de subconjuntos finitos de A disjuntos dos a dos. Entonces existen $u, v \in S$ distintos entre sí tales que cada elemento de u es incompatible con cada elemento de v.*

En efecto, basta aplicar esto a $\{\mathcal{D}p \setminus r \mid p \in C\}$, con lo que obtenemos dos condiciones $p, q \in C$ tales que los elementos de $\mathcal{D}p \setminus r$ son incompatibles con los de $\mathcal{D}q \setminus r$, y entonces $p \cup q \in \mathbb{P}$ es una extensión común de p y q, por lo que C no es una anticadena.

Supongamos que el resultado es falso y sea S un contraejemplo. Restringiendo S podemos suponer que todos sus elementos tienen el mismo cardinal $n > 0$. Para cada $s \in S$ elegimos una enumeración $\{s_0, \ldots, s_{n-1}\}$.

Sea D un ultrafiltro uniforme sobre S, es decir, un ultrafiltro en $\mathcal{P}S$ cuyos elementos tengan todos el cardinal de S. Su existencia viene dada por 7.22. Para cada $x \in A$ y cada $k < n$, sea W_{xk} el conjunto de todos los $s \in S$ tales que x es compatible con s_k. Así, como cada $s \in S$ tiene un elemento compatible con un elemento de cualquier $s' \in S$, se cumple que

$$\bigcup_{x \in s} \bigcup_{k<n} W_{xk} = S \in D.$$

Como la unión es finita, para cada $s \in S$ podemos encontrar un $x_s \in s$ y un $k_s < n$ tales que $W_{x_s k_s} \in D$. Tomemos $k < n$ tal que $Z = \{s \in S \mid k_s = k\}$ es no numerable. Basta probar que $\{x_s \mid s \in Z\}$ es una cadena en A. Notemos que es no numerable porque los elementos de S son disjuntos dos a dos, con lo que tendremos una contradicción con que A es un árbol de Aronszajn.

En efecto, si s_1, $s_2 \in Z$, entonces $W = W_{x_{s_1} k} \cap W_{x_{s_2} k} \in D$, luego W es no numerable. Si $s \in W$, entonces su k-ésimo elemento es compatible tanto con x_{s_1} como con x_{s_2}. Como W es no numerable y sólo hay una cantidad numerable de elementos bajo x_{s_1} y x_{s_2}, tiene que existir un $s \in W$ tal que $s_k > x_{s_1} \wedge s_k > x_{s_2}$, pero entonces x_{s_1} y x_{s_2} son compatibles. ∎

9.5 Árboles de Kurepa

Hemos visto que en NBG, "con dificultad", es posible construir $\aleph_1$-árboles de Aronszajn, es decir, $\aleph_1$-árboles sin caminos, mientras que no es posible probar que existan κ-árboles sin caminos para cardinales regulares mayores. Sin embargo, sí que es posible construir κ-árboles con caminos. Por ejemplo, el propio κ es un κ-árbol con un camino, y es fácil construir κ-árboles con varios caminos. Con un poco de esfuerzo podemos probar lo siguiente:

Teorema 9.29 *Si κ es un cardinal infinito existen κ-árboles con κ caminos.*

Demostración: Vamos a construir un κ-subárbol de ${}^{<\kappa}2$ con κ caminos. Para ello construiremos recurrentemente subárboles A_α de ${}^{<\alpha}2$ de modo que cada uno sea un subárbol de los siguientes (con niveles de cardinal $< \kappa$) y una familia $\{C_\alpha^\beta\}_{\beta<\kappa}$ de caminos en A_α de modo que si $\alpha \leq \alpha'$ entonces $C_\alpha^\beta \subset C_{\alpha'}^\beta$ y además los caminos $\{C_\alpha^\beta\}_{\beta<\alpha}$ sean distintos dos a dos.

Necesariamente, $A_0 = \{\varnothing\}$ y $C_0^\beta = \{\varnothing\}$ para todo $\beta < \kappa$. Supuesto definido A_α, de modo que todos sus niveles tengan cardinal $< \kappa$, definimos $A_{\alpha+1}$ añadiendo a A_α las dos prolongaciones de cada $s \in A_\alpha$ que toman sobre α el valor 0 o 1 respectivamente. Es claro entonces que el nivel α de $A_{\alpha+1}$ sigue teniendo cardinal $< \kappa$.

Definimos $C_{\alpha+1}^\beta$ añadiendo a C_α^β la prolongación de su elemento de altura α que toma sobre α el valor 0, salvo en el caso de $C_{\alpha+1}^\alpha$, al que le añadimos la

extensión que sobre α toma el valor 1. De este modo, $C^\alpha_{\alpha+1}$ es distinto de todos los $C^\beta_{\alpha+1}$ con $\beta<\alpha$, y éstos son distintos entre sí, luego todos los $\{C^\beta_{\alpha+1}\}_{\beta<\alpha+1}$ resultan ser distintos dos a dos.

Supuestos definidos $\{A_\delta\}_{\delta<\lambda}$, para $\lambda\leq\kappa$, con sus caminos correspondientes, definimos $A_\lambda=\bigcup_{\delta<\lambda}A_\delta$ y $C^\beta_\lambda=\bigcup_{\delta<\lambda}C^\beta_\delta$, que claramente cumplen lo pedido.

Así, el κ-árbol $A=A_\kappa$ tiene κ caminos distintos $\{C^\beta_\kappa\}_{\beta<\kappa}$. ∎

Sin embargo, en principio un κ-árbol podría tener hasta 2^κ caminos. De hecho, ${}^{<\omega}2$ es un $\aleph_0$-árbol con $2^{\aleph_0}$ caminos. Kurepa conjeturo que "aguzando el ingenio" más que en la demostración del teorema anterior tendría que poder demostrarse la existencia de un $\aleph_1$-árbol con $\aleph_2$ caminos:

Definición 9.30 Si κ es un cardinal infinito, un *κ-árbol de Kurepa* es un κ-árbol con al menos κ^+ caminos. Un *árbol de Kurepa* es un $\aleph_1$-árbol de Kurepa.

La *hipótesis de Kurepa* (HK) afirma la existencia de un árbol de Kurepa. La *hipótesis de Kurepa generalizada* (HK(κ)) afirma la existencia de un κ-árbol de Kurepa.

Una vez más, resulta que la hipótesis de Kurepa es indecidible. Para analizar la situación conviene introducir un concepto relacionado:

Una *familia κ-Kurepa* es un conjunto $\mathcal{F}\subset\mathcal{P}\kappa$ tal que $|\mathcal{F}|\geq\kappa^+$ y

$$\bigwedge\alpha<\kappa\ |\{A\cap\alpha\mid A\in\mathcal{F}\}|<\kappa.$$

Teorema 9.31 *Si κ es un cardinal regular, existe un κ-árbol de Kurepa si y sólo si existe una familia κ-Kurepa.*

Demostración: Si A es un κ-árbol de Kurepa, como todo κ-árbol tiene cardinal κ, podemos suponer que $A=\kappa$ (con un orden adecuado $\leq^*$). Sea entonces $\mathcal{F}\subset\mathcal{P}\kappa$ el conjunto de todos los caminos de A. Ciertamente $|\mathcal{F}|\geq\kappa^+$. Si $\alpha<\kappa$, como κ es regular, la función $h:\alpha\longrightarrow\kappa$ que a cada $x\in\alpha$ le asigna su altura en A está acotada, luego existe un $\delta<\kappa$ tal que todos los elementos de α tienen altura $<\delta$. Así, si $A\in\mathcal{F}$, existe un único $y\in\mathrm{Niv}_\delta(A)$, y entonces $\alpha\cap A=\{x\in\alpha\mid x<^*y\}$. Por lo tanto

$$|\{A\cap\alpha\mid A\in\mathcal{F}\}|\leq|\mathrm{Niv}_\delta(A)|<\kappa.$$

Recíprocamente, si $\mathcal{F}\subset\mathcal{P}\kappa$ es una familia κ-Kurepa, para cada $\alpha<\kappa$ y cada $B\in\mathcal{F}$ sea $\chi^\alpha_B\in{}^\alpha2$ la función característica de $B\cap\alpha$ y sea

$$A=\bigcup_{\alpha<\kappa}\{\chi^\alpha_B\mid B\in\mathcal{F}\}\subset{}^{<\kappa}2.$$

Si $\beta<\alpha$, entonces $\chi^\alpha_B|_\beta=\chi^\beta_B$, luego A es un árbol con el orden dado por la inclusión y

$$\mathrm{Niv}_\alpha(A)=\{\chi^\alpha_B\mid B\in\mathcal{F}\},$$

luego es un κ-árbol, y cada $B\in\mathcal{F}$ determina un camino distinto, luego es un κ-árbol de Kurepa. ∎

La existencia de árboles de Kurepa se sigue de un principio combinatorio, pero para demostrarlo necesitamos un resultado previo:

Teorema 9.32 *Sea κ un cardinal infinito tal que $2^{<\kappa} = \kappa$. Entonces existe una familia $\mathcal{A} \subset \mathcal{P}\kappa$ tal que $\bigwedge z \in A\ |x| = \kappa$, $\bigwedge xy \in \mathcal{A}(x \neq y \to |x \cap y| < \kappa)$ y $|\mathcal{A}| = 2^\kappa$.*

Demostración: Sea I el conjunto de todos los subconjuntos acotados de κ. Por hipótesis $|I| = \kappa$. Si $X \subset \kappa$, sea $A_X = \{X \cap \alpha \mid \alpha < \kappa\}$. Si $|X| = \kappa$ es claro que $|A_X| = \kappa$ y si $X \neq Y$ entonces $|A_X \cap A_Y| < \kappa$. Por lo tanto, si llamamos $\mathcal{A}' = \{A_X \mid X \subset \kappa \wedge |X| = \kappa\}$, tenemos que $\mathcal{A}'$ cumple las condiciones del enunciado salvo que $\mathcal{A}' \subset \mathcal{P}I$ en lugar de $\mathcal{A}' \subset \mathcal{P}\kappa$, pero basta tomar una biyección $f : I \longrightarrow \kappa$ y definir $\mathcal{A} = \{f[A] \mid A \in \mathcal{A}'\}$. La familia $\mathcal{A}$ cumple lo requerido. ∎

Teorema 9.33 *Si κ es un cardinal infinito y se cumple $\diamondsuit^+_{\kappa^+}$, entonces existe un κ^+-árbol de Kurepa con 2^{κ^+} caminos.*

Demostración: Si $C \subset \kappa^+$ y $\xi < \kappa^+$, definimos

$$s(C, \xi) = \sup((C \cup \{0\}) \cap (\xi + 1)).$$

(Si C es cerrado, es el mayor elemento de $C \cup \{0\}$ menor o igual que ξ.) Si $A \subset \kappa^+$, definimos

$$X(A, C) = \{\xi \in A \mid \neg\bigvee \eta \in A\ s(C, \xi) \leq \eta < \xi\}.$$

Así $X(A, C) \subset A$ y que si $|A| = \kappa^+$ y C es c.n.a. entonces $|X(A, C)| = \kappa^+$. En efecto, dado $\alpha < \kappa^+$, podemos tomar $\beta \in C$ tal que $\beta > \alpha$ y $\gamma \in A$ tal que $\gamma > \beta$. Así $s(C, \gamma) \geq \beta > \alpha$, y entonces el mínimo $\xi \in A$ tal que $\xi \geq s(C, \gamma)$ cumple $s(C, \xi) = s(C, \gamma) > \alpha$ y $\xi \in X(A, C)$.

Sea $\{S_\alpha\}_{\alpha<\kappa^+}$ una sucesión $\diamondsuit^+_{\kappa^+}$ y sea $\mathcal{F}$ el conjunto de todos los $X(A, C)$ tales que

1. $A \subset \kappa^+$, $|A| = \kappa^+$ y C es c.n.a. en κ^+,
2. $\bigwedge \alpha \in C\ A \cap \alpha \in S_\alpha$,
3. $\bigwedge \alpha \in C\ C \cap \alpha \in S_\alpha$.

Vamos a probar que $\mathcal{F}$ es una familia κ^+-Kurepa. Veamos que si $\beta < \kappa^+$ entonces $|\{X \cap \beta \mid X \in \mathcal{F}\}| \leq \kappa$, para lo cual basta probar a su vez que si A y C cumplen las tres condiciones anteriores entonces $|X(A, C) \cap \beta| \leq 1$ o bien

$$\bigvee \alpha \leq \beta \bigvee x \subset \beta \bigvee BD \in S_\alpha (X(A, C) \cap \beta = X(B, D) \cup x \wedge |x| \leq 1).$$

De este modo, los conjuntos $X(A, C) \cap \beta$ están determinados por los a lo sumo κ elementos de β y por los a lo sumo κ pares de elementos de $\bigcup_{\alpha\leq\beta} S_\alpha$, luego como máximo habrá κ conjuntos de esta forma.

En efecto, tomamos $\alpha = s(C,\beta) \leq \beta$. Si $\alpha > 0$ entonces $\alpha \in C$. Tomamos entonces $B = A \cap \alpha$ y $D = C \cap \alpha$ y llamamos ξ al mínimo elemento de $A \setminus \alpha$. Así

$$X(A,C) \cap \beta = \begin{cases} X(B,D) & \text{si } \xi \geq \beta, \\ X(B,D) \cup \{\xi\} & \text{si } \xi < \beta. \end{cases}$$

En efecto, si $\xi' \in X(B,D)$, entonces $\xi' \in A \cap \alpha$, luego $s(D,\xi') = s(C,\xi')$ y es claro que $\xi' \in X(A,C)$. Si $\xi < \beta$ entonces $s(C,\xi) = \alpha$, luego $\xi \in X(A,C) \cap \beta$.

Recíprocamente, si $\xi' \in X(A,C) \cap \beta$ y $\xi' \neq \xi$ (caso que sólo podría darse si $\xi < \beta$) entonces entonces $\xi' \in A \cap \beta$. Además tiene que ser $\xi' < \xi$, pues si fuera $\xi < \xi'$, sería $s(C,\xi') = \alpha \leq \xi < \beta$, con $\xi \in A$, lo que equivale a que $\xi' \notin X(A,C)$. Esto implica a su vez que $\xi' \in A \cap \alpha = B$, por la elección de ξ. Es claro entonces que $s(C,\xi') = s(D,\xi')$, de donde a su vez $\xi' \in X(B,D)$.

Si $\alpha = 0$ se cumple que $|X(A,C) \cap \beta| \leq 1$, pues si existe un $\xi' \in X(A,C) \cap \beta$, entonces $s(C,\xi') = 0$ y necesariamente $\xi = \text{mín}(A \cap \beta)$.

Ahora basta probar que $|\mathcal{F}| = 2^{\kappa^+}$, pues en particular $\mathcal{F}$ será una familia κ^+-Kurepa y la prueba del teorema 9.31 muestra que existe un κ^+-árbol de Kurepa con 2^{κ^+} caminos.

Recordemos que $\diamondsuit^+_{\kappa^+} \to \diamondsuit_{\kappa^+} \to 2^\kappa = \kappa^+$. Por lo tanto $2^{<\kappa^+} = 2^\kappa = \kappa^+$, y el teorema anterior nos da una familia $\mathcal{A} \subset \mathcal{P}\kappa^+$ formada por 2^{κ^+} subconjuntos de κ^+ de cardinal κ^+, pero cuyas intersecciones tienen cardinal $\leq \kappa$.

Para cada $A \in \mathcal{A}$, por la propiedad de las sucesiones $\diamondsuit^+_{\kappa^+}$, existe un C c.n.a. en κ^+ tal que $X(A,C) \in \mathcal{F}$, pero si $A \neq A'$, entonces $X(A,C) \neq X(A',C')$, puesto que $X(A,C) \cap X(A',C') \subset A \cap A'$, luego el cardinal de la intersección es $\leq \kappa$, y si ambos conjuntos fueran el mismo sería κ^+. Así pues, $|\mathcal{F}| = 2^{\kappa^+}$. ∎

Por lo tanto, no es posible demostrar que no existan κ^+-árboles de Kurepa (pero lo cierto es que tampoco puede probarse que existan).

9.6 Álgebras de Suslin

Observemos que si $(A,\leq)$ es un árbol, el conjunto $\mathbb{P} = A$ con la relación inversa

$$p \leq^* q \leftrightarrow q \leq p$$

es un conjunto parcialmente ordenado en el que la relación de incompatibilidad es la misma que ya teníamos definida.

En efecto, si se cumple $\neg p \perp q$ en el sentido definido para árboles, tenemos que $p \leq q \vee q \leq p$, luego $q \leq^* p \vee p \leq^* q$, luego ciertamente $\neg p \perp q$ en el sentido de c.p.o.s. Si $\neg p \perp q$ en el sentido de c.p.o.s, existe un $r \in A$ tal que $r \leq^* p \wedge r \leq^* q$, es decir, $p, q \in A^{\leq}_r$, que está bien ordenado, luego p y q son comparables, luego $\neg p \perp q$ en el sentido de árboles.

De este modo, cada árbol A en estas condiciones determina un álgebra de Boole completa $R(A)$.

Es fácil ver que $\mathbb{P}$ es separativo si cuando un $p \in \mathrm{Niv}_\alpha(A)$ tiene una extensión en $\mathrm{Niv}_{\alpha+1}(A)$, de hecho tiene al menos dos, así como que $\mathbb{P}$ es no atómico si y sólo si A está ramificado.

Si $(A, \leq^*)$ es un árbol de Suslin bien podado, $(\mathbb{P}, \leq)$ es el mismo A con el orden inverso y $\mathbb{B} = R(\mathbb{P})$ es su compleción, tenemos que $\mathbb{B}$ es un álgebra de Boole completa no atómica con la condición de cadena numerable. Vamos a probar que además es $\aleph_0$-distributiva.

Observemos en primer lugar que si D es abierto denso en $\mathbb{B}$, entonces, como $\mathbb{P}$ es denso en $\mathbb{B}$, es claro que $D^* = D \cap \mathbb{P}$ es abierto denso en $\mathbb{P}$. Vamos a probar que existe un $\alpha < \omega_1$ tal que D^* contiene todos los elementos de A de altura $\geq \alpha$.

Sea C una anticadena maximal contenida en D^*. Como también es una anticadena en A, tiene ser numerable. Sea $\alpha < \omega_1$ tal que todos los elementos de C tengan altura $< \alpha$. Si $p \in A$ tiene altura $\geq \alpha$, existe $d \in D^*$ tal que $d \leq p$ y por la maximalidad de C existe un $d^* \in D^*$ compatible con d, luego con p. Ahora bien, la compatibilidad en $\mathbb{P}$ (por ser el c.p.o. asociado a un árbol) equivale a que $d^* \leq^* p \vee p \leq^* d^*$, pero el segundo caso es imposible, porque la altura de p es mayor, luego $d^* \leq^* p$, es decir, $p \leq d^*$ y, como D^* es abierto, $p \in D^*$.

Sea ahora $\{D_n\}_{n\in\omega}$ una familia de abiertos densos en $\mathbb{B}$, sea $\alpha_n < \omega_1$ tal que D_n^* contenga todos los elementos de A de altura $\geq \alpha_n$ y sea $\alpha = \bigcup_n \alpha_n < \omega_1$. Entonces $D^* = \bigcap_n D_n^*$ contiene todos los elementos de A de altura $\geq \alpha$. Como A está bien podado, es inmediato que D^* es denso en $\mathbb{P}$ y como $D^* \subset D = \bigcap_n D_n$, es claro que D es denso en $\mathbb{B}$, y obviamente es abierto. Esto prueba que $\mathbb{B}$ es $\aleph_0$-distributiva.

Definición 9.34 Un *álgebra de Suslin* es un álgebra de Boole completa, no atómica, con la condición de cadena numerable y $\aleph_0$-distributiva.

Hemos probado la mitad del teorema siguiente:

Teorema 9.35 (AE) *Existe un árbol de Suslin si y sólo si existe un álgebra de Suslin.*

Demostración: Si existe un árbol de Suslin existe uno bien podado, y hemos probado que su compleción es un álgebra de Suslin. Supongamos ahora que $\mathbb{B}$ es un álgebra de Suslin y vamos a definir recurrentemente los niveles de un ω_1-árbol $A \subset \mathbb{B} \setminus \{\mathbb{0}\}$ con el orden inverso de $\mathbb{B}$.

Más concretamente, vamos a construir una sucesión de árboles ramificados $\{A_\alpha\}_{\alpha\leq\omega_1}$ de altura α de modo que cada nivel de A_α es una partición de $\mathbb{B}$. De este modo, $A = A_{\omega_1}$ será un ω_1-árbol ramificado en el que dos elementos incompatibles en A serán también incompatibles en $\mathbb{B}$, luego todas las anticadenas en A lo serán de $\mathbb{B}$ y, por consiguiente, serán numerables, y A será un árbol de Suslin por 9.9.

Definimos $A_1 = \{\mathbb{1}\}$. Supuesto definido A_δ para todo $\delta < \lambda$, basta tomar $A_\lambda = \bigcup_{\delta<\lambda} A_\delta$. Si tenemos A_δ y $\delta = \alpha + 1$, para cada $p \in \mathrm{Niv}_\alpha(A)$, como no es un átomo, existe $\mathbb{0} < p_0 < p$, luego podemos tomar $p_1 = p \wedge p_0'$ y tenemos que $p = p_0 \vee p_1$ y $p_0 \wedge p_1 = \mathbb{0}$. Es claro entonces que si hacemos $\mathrm{Niv}_{\alpha+1}(A) = \bigcup_{p\in\mathrm{Niv}_\alpha(A)} \{p_0, p_1\}$, ciertamente los elementos de este conjunto tienen altura $\alpha+1$ en el árbol, son incompatibles dos a dos, cada elemento de $\mathrm{Niv}_\alpha(A)$ tiene dos extensiones incompatibles y además

$$\bigvee_{p\in\mathrm{Niv}_{\alpha+1}(A)} p = \mathbb{1},$$

puesto que cada $p \in \mathrm{Niv}_\alpha(A)$ cumple $p = p_0 \vee p_1 \leq \bigvee_{p\in\mathrm{Niv}_{\alpha+1}(A)} p$, y basta tomar el supremo en p.

Supongamos finalmente que tenemos definido un árbol A_λ de altura λ cuyos niveles son particiones de $\mathbb{B}$. La distributividad de $\mathbb{B}$ nos da que

$$\bigwedge_{\delta<\lambda} \bigvee_{p\in\mathrm{Niv}_\delta(A)} p = \mathbb{1} = \bigvee_f \bigwedge_{\delta<\lambda} f(\delta),$$

donde f varía en $\prod_{\delta<\lambda} \mathrm{Niv}_\delta(A)$. Claramente, $p_f = \bigwedge_{\delta<\lambda} f(\delta) = \mathbb{0}$ salvo si f recorre una cadena C_f de A_λ, en cuyo caso p_f tiene por debajo (en el árbol A, o por encima en $\mathbb{B}$) exactamente a los elementos de C_f. Por lo tanto, si definimos

$$\mathrm{Niv}_\lambda(A) = \{p_f \mid f \in \prod_{\delta<\lambda} \mathrm{Niv}_\delta(A) \wedge p_f \neq \mathbb{0}\},$$

tenemos que cada elemento de este conjunto tiene ciertamente altura λ en el árbol $A_{\lambda+1}$, y $\mathrm{Niv}_\lambda(A)$ es una partición de $\mathbb{B}$, pues ciertamente su supremo es $\mathbb{1}$ y, si $f \neq g$, entonces existe un δ tal que $f(\delta) \neq g(\delta)$, luego $f(\delta) \perp g(\delta)$, luego $p_f \perp p_g$. ∎

En particular, no es posible demostrar la existencia de álgebras de Suslin.

Capítulo X

Elementos de teoría de modelos

Hasta ahora hemos estudiado distintas "estructuras" definibles sobre un conjunto (la estructura de conjunto ordenado, la estructura de anillo, cuerpo, cuerpo ordenado, álgebra de Boole, etc.) Aquí vamos a mostrar cómo es posible estudiar hasta cierto punto todas estas estructuras dentro de un marco común, el determinado por la teoría de modelos. Notemos que hemos adoptado la costumbre de representar por $+$ y $\cdot$ las operaciones de un anillo cualquiera, si bien estos signos representan conjuntos distintos según el anillo considerado. Esto es lo que habitualmente se llama un "abuso de notación", pero ahora le daremos un sentido más profundo al mostrar que podemos considerar a $+$ y $\cdot$ como unos signos de un único "lenguaje formal" susceptibles de ser interpretados de forma distinta en cada anillo. Por ejemplo, en el contexto que vamos a presentar podremos considerar

$$\bigwedge xy\,(x+y=y+x)$$

como un único objeto matemático, una fórmula de un determinado lenguaje formal de la que podremos decir que es verdadera en el modelo que resulta de especificar que las variables x, y deben recorrer los números reales y el signo $+$ debe interpretarse como la suma usual, pero que es falsa en el modelo que resulta de especificar que las variables x, y deben recorrer los elementos de ω_1 y el signo $+$ debe interpretarse como la suma de ordinales. Pero en ambos casos estamos hablando del mismo objeto matemático "$\bigwedge xy\,(x+y=y+x)$" y no de objetos distintos que representamos por conveniencia con la misma notación.

No usaremos AE sin indicarlo explícitamente.

10.1 Lenguajes y modelos

Para enunciar las propiedades que definen una estructura como la de anillo ordenado necesitamos hacer referencia a relaciones (como $\leq$), a funciones

(como +) y a conjuntos específicos (como 0, 1), así como a elementos arbitrarios (x, y, ...) y a relaciones lógicas entre ellos. Vamos a definir ahora una familia de lenguajes cuyos signos puedan adaptarse a las estructuras que pretenden describir:

Definición 10.1 Un *lenguaje formal* (de primer orden) es una óctupla ordenada

$$\mathcal{L} = (V, F, R, r, \neg, \to, \bigwedge, =),$$

tal que

1. V es un conjunto infinito a cuyos elementos llamaremos *variables* de $\mathcal{L}$,
2. F es un conjunto arbitrario (tal vez vacío) a cuyos elementos llamaremos *funtores* de $\mathcal{L}$,
3. R es un conjunto arbitrario a cuyos elementos llamaremos *relatores* de $\mathcal{L}$,
4. Los conjuntos V, F y R son disjuntos dos a dos.
5. $r : F \cup R \longrightarrow \omega$, de modo que si $s \in F \cup R$ y $r(s) = n$ diremos que s es un relator (o funtor) n-ádico. Exigimos que no haya relatores 0-ádicos, y a los funtores 0-ádicos los llamaremos *constantes* de $\mathcal{L}$.
6. $\neg$, $\to$, $\bigwedge$, $=$ son conjuntos arbitrarios a los que llamaremos, respectivamente, *negador, implicador, generalizador* e *igualador* de $\mathcal{L}$. Exigimos que sean distintos entre sí y que no pertenezcan a $V \cup F \cup R$, salvo el igualador, que tiene que ser un relator diádico.[1]

Si $\mathcal{L}$ es un lenguaje formal, representaremos por $\mathrm{Varl}(\mathcal{L})$ al conjunto de las variables de $\mathcal{L}$, representaremos por $\mathrm{Const}(\mathcal{L})$ al conjunto de las constantes de $\mathcal{L}$, y si $n > 0$ representaremos por $\mathrm{Fn}_n(\mathcal{L})$ y $\mathrm{Rel}_n(\mathcal{L})$ los conjuntos de funtores y relatores n-ádicos de $\mathcal{L}$. Llamaremos *signos* de $\mathcal{L}$ a los elementos de

$$\mathrm{Sig}(\mathcal{L}) = \mathrm{Var}(\mathcal{L}) \cup \mathrm{Const}(\mathcal{L}) \cup \bigcup_{n\in\omega\setminus\{0\}} \mathrm{Fn}_n(\mathcal{L}) \cup \bigcup_{n\in\omega\setminus\{0\}} \mathrm{Rel}_n(\mathcal{L}) \cup \{\neg, \to, \bigwedge\}.$$

Llamaremos *cadenas de signos* de $\mathcal{L}$ a los elementos de

$$\mathrm{Cad}(\mathcal{L}) = \mathrm{Sig}(\mathcal{L})^{<\omega},$$

es decir, a las sucesiones finitas de signos de $\mathcal{L}$. Consideramos la aplicación $\ell : \mathrm{Cad}(\mathcal{L}) \longrightarrow \omega$ que a cada cadena de signos le asigna su *longitud,* es decir, su dominio.

Tenemos definida la operación $\mathrm{Cad}(\mathcal{L}) \times \mathrm{Cad}(\mathcal{L}) \longrightarrow \mathrm{Cad}(\mathcal{L})$ dada por la *yuxtaposición,* es decir, que si ζ_1, $\zeta_2 \in \mathrm{Cad}(\mathcal{L})$, definimos $\zeta_1\zeta_2$ como la sucesión de dominio $\ell(\zeta_1) + \ell(\zeta_2)$ dada por

$$(\zeta_1\zeta_2)_i = \begin{cases} (\zeta_1)_i & \text{si } i < \ell(\zeta_1), \\ (\zeta_2)_{i-\ell(\zeta_1)} & \text{si } \ell(\zeta_1) \leq 1 < \ell(\zeta_1) + \ell(\zeta_2). \end{cases}$$

[1] En ausencia de AE exigiremos además que los conjuntos V, R y F sean bien ordenables.

Se comprueba sin dificultad que es una operación asociativa, por lo que podemos considerar yuxtaposiciones de la forma $\zeta_1 \cdots \zeta_n$.

En general no distinguiremos entre los signos y las cadenas de signos de longitud 1 de un lenguaje formal, es decir, por ejemplo, entre el signo $=$ y la cadena de signos $\{(0,=)\}$ (la sucesión de dominio $1 = \{0\}$ cuyo único término es $=$). Así, si x e y son dos variables de un lenguaje $\mathcal{L}$ y consideramos la cadena de signos $x = y$ que resulta de yuxtaponerlas con el signo $=$, debemos tener presente que la operación de yuxtaposición está definida sobre cadenas de signos y no sobre signos, por lo que $x = y$ es la cadena de signos

$$\{(0,x)\}\{(0,=)\}\{(0,y)\} = \{(0,x),(1,=),(2,y)\}.$$

Ejemplo: El lenguaje de la teoría de anillos Definimos el *lenguaje formal de la teoría de anillos (unitarios)* como el lenguaje formal $\mathcal{L}_a$ que tiene un conjunto numerable de variables, dos constantes 0 y 1 y dos funtores diádicos $+$ y $\cdot$ (aparte del igualador y los demás signos lógicos). Notemos que no explicitamos qué conjunto es concretamente cada signo de $\mathcal{L}_a$. Podríamos hacerlo, pero sería del todo irrelevante.[2] Si a $\mathcal{L}_a$ le añadimos un relator diádico $\leq$ tenemos el *lenguaje $\mathcal{L}_{ao}$ de la teoría de anillos ordenados.* ∎

Un *modelo* de un lenguaje formal $\mathcal{L}$ es un par (M, I), donde M es un conjunto no vacío al que llamaremos *universo* del modelo e I es una aplicación definida sobre el conjunto

$$\mathrm{Const}(\mathcal{L}) \cup \bigcup_{n\in\omega\setminus\{0\}} \mathrm{Fn}_n(\mathcal{L}) \cup \bigcup_{n\in\omega\setminus\{0\}} \mathrm{Rel}_n(\mathcal{L})$$

tal que:

1. Si $c \in \mathrm{Const}(\mathcal{L})$ entonces $I(c) \in M$.
2. Si $f \in \mathrm{Fn}_n(\mathcal{L})$ entonces $I(f) : M^n \longrightarrow M$.
3. Si $R \in \mathrm{Rel}_n(\mathcal{L})$ entonces $I(R) \subset M^n$, de modo que $I(=)$ sea la identidad en M.

En la práctica escribiremos M en lugar de (M, I) y $\bar{c}$, $\bar{f}$, $\bar{R}$ en lugar de $I(c)$, $I(f)$, $I(R)$. De este modo, especificar un modelo de un lenguaje formal $\mathcal{L}$ significa especificar un universo M (un conjunto de objetos de los que vamos a hablar con dicho lenguaje) y asociar a cada constante, cada funtor y cada relator un significado, de modo que el significado de una constante es un objeto

[2]Notemos que hasta ahora usábamos el signo $+$ para referirnos indistintamente a diversas operaciones, y era fundamental saber a cuál de ellas nos referíamos en cada momento, pues la suma de ordinales no tiene las mismas propiedades que la suma de números reales. En este contexto la situación es la opuesta. Ahora $+$ sólo pretende ser un signo de un lenguaje formal, y es totalmente irrelevante qué conjunto concreto definimos como $+$. A continuación veremos cómo asignar un significado a cada signo de un lenguaje formal, de modo que lo relevante no será nunca qué conjunto es $+$, sino qué efecto tiene asignar a un mismo (e irrelevante) signo $+$ diversos significados, como la suma de ordinales o la suma de números reales.

del universo del modelo, el significado de un funtor n-ádico es una función de n argumentos en el universo del modelo y el significado de un relator n-ádico es una relación de n argumentos en el universo del modelo.[3] Los modelos no atribuyen ningún significado a los signos $\neg$, $\to$, $\bigwedge$ porque vamos a hacer que tengan un significado fijo independiente del modelo que consideremos. A las variables no se les asigna un significado porque nuestra intención es que puedan variar de significado incluso tras haber fijado un modelo.

Ejemplo Un modelo del lenguaje de la teoría de anillos viene determinado por un conjunto A, dos objetos $\bar{0}$, $\bar{1} \in A$ y dos operaciones $\bar{+} : A \times A \longrightarrow A$, $\bar{\cdot} : A \times A \longrightarrow A$. Notemos que no es necesario que $(A, \bar{+}, \bar{\cdot})$ sea un anillo para ser un modelo del lenguaje de la teoría de anillos. Veremos enseguida que los anillos son los modelos de la teoría de anillos, pero aún no hemos definido lo que esto significa. Para tener un modelo del lenguaje de la teoría de anillos ordenados tenemos que especificar además una relación binaria $\bar{\leq}$. ∎

Observemos estos tres ejemplos de cadenas de signos de $\mathcal{L}_a$:

$$== +\neg \to, \qquad 1 \cdot 1 + 1 + 0 \qquad 1 + 1 = 0 \to 1 + 1 + 1 = 1.$$

La diferencia entre la primera y las otras dos es que a éstas les podemos asociar un significado (respecto de un modelo que fije una interpretación para los signos involucrados), y a su vez la segunda se distingue de la tercera en que el significado de la segunda debe ser un objeto del modelo considerado, mientras que el significado de la tercera debe ser un valor de verdad (verdadero o falso). A las cadenas de signos como la segunda del ejemplo anterior (las que pretenden representar objetos) las llamaremos términos y a las que pretenden ser afirmaciones, como la tercera, las llamaremos fórmulas.

Para definir con precisión los conjuntos de términos y fórmulas de un lenguaje formal $\mathcal{L}$ emplearemos el teorema de recursión sobre la relación bien fundada en $\mathrm{Cad}(\mathcal{L})$ dada por $\zeta_1 \, R \, \zeta_2 \leftrightarrow \ell(\zeta_1) < \ell(\zeta_2)$. Así, para definir el conjunto de los términos definimos una función $f : \mathrm{Cad}(\mathcal{L}) \longrightarrow 2$ de modo que los términos serán las cadenas con imagen 1. En la práctica, esto significa que podemos definir cuándo una cadena es un término supuesto que tengamos definido cuándo las cadenas de longitud menor son términos. La definición es:[4]

1. Las variables y las constantes de $\mathcal{L}$ son *términos.*
2. Si $t_1, \ldots, t_n$ son términos de $\mathcal{L}$ y f es un funtor n-ádico de $\mathcal{L}$, entonces $ft_1 \cdots t_n$ es un *término* de $\mathcal{L}$.

[3] Hasta ahora sólo habíamos trabajado con relaciones binarias, pero si tenemos $\bar{R} \subset M^n$, podemos ver a $\bar{R}$ como una relación n-ádica en M en el sentido de que, dada una n-tupla $(a_0, \ldots, a_{n-1}) \in M^n$, podemos decir que $(a_0, \ldots, a_{n-1})$ cumplen la relación $\bar{R}$ si y sólo si

$$\bar{R}(a_0, \ldots, a_{n-1}) \equiv (a_0, \ldots, a_{n-1}) \in \bar{R}.$$

[4] Mas precisamente, $f(\zeta) = 1$ si y sólo si ζ es una variable o una constante o existe un funtor n-ádico f y cadenas $t_1, \ldots, t_n$ de longitud menor que ζ de modo que $f(t_i) = 1$ para todo i y $\zeta = ft_1 \cdots t_n$.

El mismo planteamiento justifica la siguiente definición recurrente de *fórmula*:

1. Si $t_1, \ldots, t_n$ son términos de $\mathcal{L}$ y R es un relator n-ádico de $\mathcal{L}$, entonces $Rt_1 \cdots t_n$ es una fórmula de $\mathcal{L}$.

2. Si α, β son fórmulas de $\mathcal{L}$, también lo son $\neg\alpha$ y $\to \alpha\beta$.

3. Si α es una fórmula de $\mathcal{L}$ y x es una variable, también es una fórmula $\bigwedge x\alpha$.

Representaremos por $\mathrm{Term}(\mathcal{L})$ y $\mathrm{Form}(\mathcal{L})$ a los conjuntos de términos y fórmulas de $\mathcal{L}$, respectivamente.

Convenios de notación En la práctica, en lugar de escribir $= t_1t_2$ escribiremos[5] $t_1 = t_2$, en lugar de $\neg(t_1 = t_2)$ escribiremos $t_1 \neq t_2$ y en lugar de $\to \alpha\beta$ escribiremos $\alpha \to \beta$. Definimos también:

$$\alpha \vee \beta = \neg\alpha \to \beta, \quad \alpha \wedge \beta = \neg(\neg\alpha \vee \neg\beta),$$

$$\alpha \leftrightarrow \beta = (\alpha \to \beta) \wedge (\beta \to \alpha), \qquad \bigvee x\alpha = \neg\bigwedge x\neg\alpha.$$

También abreviaremos $\bigwedge xy$ en lugar de $\bigwedge x\bigwedge y$ o $\bigvee xy$ en lugar de $\bigvee x\bigvee y$. En cada lenguaje particular consideraremos también convenios de notación similares con sus signos particulares. Por ejemplo, en el lenguaje de la teoría de anillos convendremos en escribir $t_1 + t_2$ en lugar de $+t_1t_2$, e igualmente con el producto (aunque a menudo abreviaremos $t_1 \cdot t_2$ incluso a t_1t_2). Así pues, cuando hablemos de una fórmula como

$$\bigwedge xy\,(x + y = y + x)$$

nos estamos refiriendo a la cadena de signos

$$\{(0, \textstyle\bigwedge), (1, x), (2, \bigwedge), (3, y), (4, =), (5, +), (6, x), (7, y), (8, +), (9, y), (10, x)\}.$$

No obstante, la sucesión concreta de los signos de un determinado término o fórmula será siempre irrelevante. ∎

Ahora veamos cómo cada modelo determina un significado para cada término y cada fórmula de un lenguaje formal. En realidad nos falta atribuirle un significado a las variables, lo cual lo haremos mediante el concepto de valoración:

Una *valoración* de un lenguaje formal $\mathcal{L}$ en un modelo M de $\mathcal{L}$ es una aplicación $v : \mathrm{Var}(\mathcal{L}) \longrightarrow M$.

[5]Esto no significa que alteremos la cadena de signos, es decir, si x e y son variables, representamos por $x = y$ la sucesión finita cuyo primer signo es $=$, su segundo signo es x y su tercer signo es y. La razón para que "oficialmente" la fórmula $x = y$ sea la sucesión $\{(0, =), (1, x), (2, y)\}$, en este orden, es que así no necesitamos considerar los paréntesis como signos de un lenguaje formal, sino que éstos sólo hacen falta para evitar ambigüedades en los convenios de notación.

De este modo, cada valoración asigna un significado a cada variable de $\mathcal{L}$.

Si v es una valoración de $\mathcal{L}$ en M, x es una variable de $\mathcal{L}$ y $a \in M$, definimos v_x^a como la valoración que coincide con v salvo por que $v_x^a(x) = a$.

Ahora definimos por recurrencia el *objeto denotado* por un término t en un modelo M respecto de una valoración v, y que representaremos por $M(t)[v]$:

1. Si x es una variable, $M(x)[v] = v(x)$.
2. Si c es una constante, $M(c)[v] = \bar{c}$.
3. Si f es un funtor n-ádico y $t_1, \ldots, t_n$ son términos,
$$M(ft_1 \cdots t_n)[v] = \bar{f}(M(t_1)[v], \ldots, M(t_n)[v]).$$

Similarmente queremos definir la relación $M \vDash \alpha[v]$ que significa que la fórmula α es satisfecha en M respecto de la valoración v, pero no es posible hacerlo por recurrencia sobre la longitud de α, como hemos hecho hasta ahora, sino que necesitamos una relación que involucre las valoraciones en el modelo. Concretamente, en el conjunto $\mathrm{Form}(\mathcal{L}) \times \mathrm{Val}(M)$, donde $\mathrm{Val}(M)$ es el conjunto de todas las valoraciones en M, definimos la relación dada por

$$(\alpha, v)\, R\, (\beta, w) \leftrightarrow \ell(\alpha) < \ell(\beta),$$

que claramente está bien fundada. Aplicando el teorema de recursión a esta relación, podemos definir una función $F : \mathrm{Form}(\mathcal{L}) \times \mathrm{Val}(M) \longrightarrow 2$ de modo que $M \vDash \alpha[v]$ sea por definición $F(\alpha, v) = 1$, y en la práctica esto supone que podemos definir $M \vDash \alpha[v]$ supuesto definido $M \vDash \beta[w]$ para toda fórmula β de longitud menor que α y para toda valoración w. La definición es la siguiente:

1. $M \vDash Rt_1 \cdots t_n[v]$ si y sólo si $\bar{R}(M(t_1)[v], \ldots, M(t_n)[v])$.
2. $M \vDash \neg\alpha[v]$ si y sólo si no $M \vDash \alpha[v]$.
3. $M \vDash (\alpha \to \beta)[v]$ si y sólo si no $M \vDash \alpha[v]$ o bien $M \vDash \beta[v]$.
4. $M \vDash \bigwedge x\alpha[v]$ si y sólo si para todo $a \in M$ se cumple $M \vDash \alpha[v_x^a]$.

En particular, $M \vDash t_1 = t_2[v]$ si y sólo si[6] $M(t_1)[v] = M(t_2)[v]$. A partir de las definiciones que hemos dado de los signos lógicos es fácil demostrar:

1. $M \vDash (\alpha \vee \beta)[v]$ si y sólo si $M \vDash \alpha[v]$ o $M \vDash \beta[v]$.
2. $M \vDash (\alpha \wedge \beta)[v]$ si y sólo si $M \vDash \alpha[v]$ y $M \vDash \beta[v]$.
3. $M \vDash (\alpha \leftrightarrow \beta)[v]$ si y sólo si $M \vDash \alpha[v]$ y $M \vDash \beta[v]$ o bien no $M \vDash \alpha[v]$ y no $M \vDash \beta[v]$.
4. $M \vDash \bigvee x\alpha[v]$ si y sólo si existe un $a \in M$ tal que $M \vDash \alpha[v_x^a]$.

[6] No debemos confundir el signo $=$ de un lenguaje $\mathcal{L}$ (que es lo que representa $=$ en la relación $M \vDash t_1 = t_2[v]$ y es un conjunto) con el signo $=$ *metamatemático* que es el signo $=$ que venimos usando a lo largo de todo este libro (que es lo que representa $=$ en $M(t_1)[v] = M(t_2)[v]$ y que es un signo lógico, no un conjunto). Lo mismo vale para los signos $\neg$, $\to$, $\bigwedge$, $\bigvee$, etc., que ahora tienen dos interpretaciones según el contexto: bien como signos de un lenguaje formal (conjuntos) bien como signos metamatemáticos (signos lógicos, que no son conjuntos).

Nota A pesar del aspecto técnico de estas definiciones, debemos tener presente que en la práctica $M(t)[v]$ no es más que el objeto que normalmente entendemos que significa t cuando "lo leemos", e igualmente $M \vDash \alpha[v]$ significa lo que normalmente entendemos al "leer" α. Por ejemplo,

$$M \vDash \bigwedge x\,(x \cdot y = y \cdot x)[v] \text{ syss para todo } a \in M\ M \vDash (x \cdot y = y \cdot x)[v_x^a]$$

$$\text{syss para todo } a \in M\ M(x \cdot y)[v_x^a] = M(y \cdot x)[v_x^a]$$

$$\text{syss para todo } a \in M\ M(x)[v_x^a] \mathbin{\bar{\cdot}} M(y)[v_x^a] = M(y)[v_x^a] \mathbin{\bar{\cdot}} M(x)[v_x^a]$$

$$\text{syss } \bigwedge a \in M\ a \mathbin{\bar{\cdot}} v(y) = v(y) \mathbin{\bar{\cdot}} a.$$

En definitiva, al ver $\bigwedge x\,(xy = yx)$ uno "lee" que "y conmuta con todo x" y, en efecto, la interpretación de esta fórmula en un modelo M respecto de una valoración v es que el objeto $v(y)$ denotado por la variable y conmuta con todos los $a \in M$. ∎

Necesitamos un último concepto sintáctico en relación con los lenguajes formales, y es el de variable libre. El conjunto $\mathrm{Vlib}(t)$ de las *variables libres* de un término t de un lenguaje formal $\mathcal{L}$ se define como el conjunto de las variables de $\mathcal{L}$ que figuran entre los signos de t. El conjunto de las variables libres de una fórmula se define por recurrencia:

1. $\mathrm{Vlib}(Rt_1, \ldots, t_n) = \mathrm{Vlib}(t_1) \cup \cdots \cup \mathrm{Vlib}(t_n)$,
2. $\mathrm{Vlib}(\neg\alpha) = \mathrm{Vlib}(\alpha)$,
3. $\mathrm{Vlib}(\alpha \to \beta) = \mathrm{Vlib}(\alpha) \cup \mathrm{Vlib}(\beta)$,
4. $\mathrm{Vlib}(\bigwedge x\,\alpha) = \mathrm{Vlib}(\alpha) \setminus \{x\}$.

A partir de aquí se demuestra inmediatamente que

1. $\mathrm{Vlib}(\alpha \vee \beta) = \mathrm{Vlib}(\alpha) \cup \mathrm{Vlib}(\beta)$,
2. $\mathrm{Vlib}(\alpha \wedge \beta) = \mathrm{Vlib}(\alpha) \cup \mathrm{Vlib}(\beta)$,
3. $\mathrm{Vlib}(\alpha \leftrightarrow \beta) = \mathrm{Vlib}(\alpha) \cup \mathrm{Vlib}(\beta)$,
4. $\mathrm{Vlib}(\bigvee x\,\alpha) = \mathrm{Vlib}(\alpha) \setminus \{x\}$.

En la práctica, las variables libres de una fórmula son las variables que aparecen en ella sin estar afectadas por un cuantificador.

Los términos y fórmulas sin variables libres de un lenguaje formal se llaman respectivamente *designadores* y *sentencias.*

Representaremos por $\mathrm{Sent}(\mathcal{L})$ el conjunto de todas las sentencias de $\mathcal{L}$.

Un resultado básico es que $M(t)[v]$ y $M \vDash \alpha[v]$ sólo dependen de los valores que toma la valoración v sobre las variables libres en t y en α, respectivamente. En efecto:

Teorema 10.2 *Sean t y α un término y una fórmula de un lenguaje formal $\mathcal{L}$, sea M un modelo de $\mathcal{L}$ y sean v y w dos valoraciones de $\mathcal{L}$ en M.*

1. *Si v y w coinciden en* $\mathrm{Vlib}(t)$*, entonces $M(t)[v] = M(t)[w]$.*
2. *Si v y w coinciden en* $\mathrm{Vlib}(\alpha)$*, entonces $M \vDash \alpha[v]$ si y sólo si $M \vDash \alpha[w]$.*

DEMOSTRACIÓN: a) Por inducción sobre la longitud de t. Si $t = x$ es una variable, entonces $\mathrm{Vlib}(t) = \{x\}$, luego

$$M(t)[v] = v(x) = w(x) = M(t)[w].$$

Si $t = c$ es una constante, entonces $M(t)[v] = \bar{c} = M(t)[w]$.

Si $t = ft_1 \cdots t_n$ y el teorema se cumple para cada t_i, entonces v y w coinciden sobre cada conjunto $\mathrm{Vlib}(t_i)$, luego usando la hipótesis de inducción

$$M(t)[v] = \bar{f}(M(t_1)[v], \ldots, M(t_n)[v]) = \bar{f}(M(t_1)[w], \ldots, M(t_n)[w]) = M(t)[w].$$

b) Razonamos igualmente por inducción sobre la longitud de α. Si es de la forma $\alpha = Rt_1 \cdots t_n$, entonces v y w coinciden sobre todos los conjuntos $\mathrm{Vlib}(t_i)$, y podemos aplicar a):

$$M \vDash Rt_1 \cdots t_n[v] \text{ syss } \bar{R}(M(t_1)[v], \ldots, M(t_n)[v])$$

$$\text{syss } \bar{R}(M(t_1)[w], \ldots, M(t_n)[w]) \text{ syss } M \vDash Rt_1 \cdots t_n[w].$$

Si vale para α y β es inmediato que vale para $\neg\alpha$ y $\alpha \to \beta$. Supongamos finalmente que la fórmula es de tipo $\bigwedge x\, \alpha$. Entonces, por hipótesis v y w coinciden sobre las variables libres de α salvo a lo sumo en x.

$$M \vDash \bigwedge x\, \alpha[v] \text{ syss para todo } a \in M \ M \vDash \alpha[v_x^a]$$

$$\text{syss para todo } a \in M \ M \vDash \alpha[w_x^a] \text{ syss } M \vDash \bigwedge x\, \alpha[w],$$

donde hemos usado que v_x^a y w_x^a coinciden en todas las variables libres de α, por lo que hemos podido aplicar la hipótesis de inducción. ∎

Usaremos la notación $t(x_1, \ldots, x_n)$ y $\alpha(x_1, \ldots, x_n)$ para representar términos y fórmulas cuyas variables libres estén entre $x_1, \ldots, x_n$, y entonces escribiremos

$$M(t)[a_1, \ldots, a_n], \qquad M \vDash \alpha[a_1, \ldots, a_n]$$

en vez de $M(t)[v]$ o $M \vDash \alpha[v]$, donde v es cualquier valoración tal que $v(x_i) = a_i$.

Cuando consideremos fórmulas concretas, sustituiremos cada variable por su interpretación entre corchetes. Por ejemplo,

$$M \vDash [a] + [b] = [b] + [a]$$

significará $M \vDash (x + y = y + x)[v]$, donde $v(x) = a$, $v(y) = b$.

Si M es un modelo de un lenguaje formal $\mathcal{L}$ y α es una fórmula de $\mathcal{L}$, diremos que α es *verdadera* en M, y lo representaremos por $M \vDash \alpha$ si se cumple $M \vDash \alpha[v]$ para toda valoración v de $\mathcal{L}$ en M. Diremos que α es *falsa* en M si no se cumple $M \vDash \alpha[v]$ para ninguna valoración v o, equivalentemente, si $\neg\alpha$ es verdadera.

El teorema anterior implica que toda sentencia es verdadera o falsa en todo modelo.

10.2 Teorías formales

Definición 10.3 Sea $\mathcal{L}$ un lenguaje formal y sea $\Gamma \subset \mathrm{Form}(\mathcal{L})$ un conjunto de fórmulas. Diremos que M es un *modelo* de Γ (y lo representaremos por $M \vDash \Gamma$ si M es un modelo de $\mathcal{L}$ tal que $\bigwedge \alpha \in \Gamma\ M \vDash \alpha$.

Diremos que α es una *consecuencia lógica* de Γ si α es verdadera en todo modelo de Γ. Lo representaremos por $\Gamma \vDash \alpha$.

Una *teoría* sobre un lenguaje formal $\mathcal{L}$ es un conjunto T de sentencias de $\mathcal{L}$ tal que si $\alpha \in \mathrm{Sent}(\mathcal{L})$ y $T \vDash \alpha$, entonces $\alpha \in T$.

Si $\Gamma \subset \mathrm{Sent}(\mathcal{L})$ es claro que

$$T(\Gamma) = \{\alpha \in \mathrm{Sent}(\mathcal{L}) \mid \Gamma \vDash \alpha\}$$

es una teoría. Si una teoría T cumple $T = T(\Gamma)$ se dice que Γ es un conjunto de *axiomas* para la teoría T.

Si M es un modelo de $\mathcal{L}$, también es claro que

$$T(M) = \{\alpha \in \mathrm{Sent}(\mathcal{L}) \mid M \vDash \alpha\}$$

es una teoría sobre $\mathcal{L}$.

Ejemplos Ahora podemos definir la *teoría de anillos (conmutativos unitarios)* como la teoría determinada por los axiomas de la definición de anillo (conmutativo unitario), es decir:

$$\begin{array}{ll}
\bigwedge xyz((x+y)+z = x+(y+z)) & \bigwedge xy\,(x+y = y+x) \\
\bigwedge x\,(x+0 = x) & \bigwedge x \bigvee y\,(x+y = 0) \\
\bigwedge xyz\,((xy)z = x(yz)) & \bigwedge xy\,(xy = yx) \\
\bigwedge xyz\,(x(y+z) = xy+xz) & \bigwedge x\ x \cdot 1 = x.
\end{array}$$

Si a estos axioma añadimos los de la definición de anillo ordenado tendremos la *teoría de anillos ordenados,* si les añadimos $\bigwedge x(x \neq 0 \to \bigvee y\ xy = 1)$ tenemos la *teoría de cuerpos,* si añadimos ambos tenemos la *teoría de cuerpos ordenados,* etc.

Sobre un lenguaje con un único relator diádico $\leq$ podemos definir la *teoría de conjuntos parcialmente ordenados,* o la *teoría de conjuntos totalmente ordenados,* etc., sobre un lenguaje con funtores $\wedge$, $\vee$ y $'$ y constantes $\mathbb{0}$, $\mathbb{1}$ podemos definir la *teoría de álgebras de Boole,* etc.

Es claro que los modelos de la teoría de anillos (conmutativos unitarios) son precisamente los anillos conmutativos unitarios, los modelos de la teoría de álgebras de Boole son las álgebras de Boole, etc. ∎

Es inmediato que las afirmaciones siguientes son equivalentes para cualquier conjunto Γ de sentencias de un lenguaje formal $\mathcal{L}$:

1. Existe $\alpha \in \mathrm{Sent}(\mathcal{L})$ tal que $\Gamma \vDash \alpha$ y $\Gamma \vDash \neg\alpha$.
2. Γ no tiene modelos.
3. $T(\Gamma) = \mathrm{Sent}(\mathcal{L})$.

Cuando Γ cumple esto se dice que es *contradictorio,* y en caso contrario se dice que es *consistente.* Notemos que Γ es consistente o contradictorio si y sólo si lo es $T(\Gamma)$.

Diremos que Γ es *completo* si para toda $\alpha \in \mathrm{Sent}(\mathcal{L})$ se cumple $\Gamma \vDash \alpha$ o bien $\Gamma \vDash \neg\alpha$. Nuevamente, Γ es completo si y sólo si la teoría $T(\Gamma)$ es completa.

Es inmediato que si $\Delta \subset \Gamma \subset \mathrm{Sent}(\mathcal{L})$ y Γ es consistente, entonces Δ también lo es (porque todo modelo de Γ lo es también de Δ). Ahora vamos a probar que si todo $\Delta \subset \Gamma$ finito es consistente, entonces Γ también lo es. Este resultado no es trivial y requiere una forma débil del axioma de elección. Más adelante daremos una prueba conceptualmente más simple, mientras que la que vamos a ver ahora usa la forma más débil posible de AE.

Diremos que Γ es *finitamente consistente* si todo $\Delta \subset \Gamma$ finito es consistente.

Teorema 10.4 *Sea $\mathcal{L}$ un lenguaje formal y $\Gamma \subset \mathrm{Sent}(\mathcal{L})$ finitamente consistente. Entonces existe un lenguaje formal $\mathcal{L}'$ que resulta de añadir a $\mathcal{L}$ un conjunto de constantes y existe un conjunto Γ' finitamente consistente de sentencias de $\mathcal{L}'$ tal que $\Gamma \subset \Gamma'$ y para toda fórmula $\phi(x)$ de $\mathcal{L}'$ con x como única variable libre, existe una constante c tal que la sentencia*[7] $\bigvee x\, \phi(x) \to \phi(c)$ *está en Γ'.*

Demostración: Vamos a definir recurrentemente una sucesión de lenguajes formales $\{\mathcal{L}_n\}_{n\in\omega}$ y una sucesión $\{\Gamma_n\}_{n\in\omega}$ de conjuntos de sentencias de cada $\mathcal{L}_n$. Partimos de $\mathcal{L}_0 = \mathcal{L}$ y $\Gamma_0 = \Gamma$.

Supongamos definidos $\mathcal{L}_n$ y Γ_n y definimos $\mathcal{L}_{n+1}$ como el lenguaje que resulta de añadir a $\mathcal{L}_n$ una constante c_ϕ para cada fórmula $\phi(x)$ de $\mathcal{L}_n$ con una única variable libre.[8] Definimos Γ_{n+1} como la unión de Γ_n y el conjunto de todas las sentencias de la forma $\bigvee x\, \phi(x) \to \phi(c_\phi)$.

Finalmente, definimos $\mathcal{L}'$ como el lenguaje formal cuyos signos son los de $\mathcal{L}$ más las constantes de todos los lenguajes $\mathcal{L}_n$ y $\Gamma' = \bigcup_{n\in\omega} \Gamma_n$. Basta probar que cada Γ_n es finitamente consistente, pues claramente entonces lo será también Γ'. Razonamos por inducción sobre n. Para $n = 0$ se cumple por hipótesis. Supongamos que Γ_n es finitamente consistente y sea $\Delta \subset \Gamma_{n+1}$ finito. Pongamos

[7] Por $\phi(c)$ entendemos la sentencia que resulta de cambiar cada aparición de la variable x en ϕ por la constante c.

[8] No necesitamos AE para definir $\mathcal{L}_{n+1}$. Por ejemplo, podemos definir α como el rango del conjunto de los signos de $\mathcal{L}_n$ y definir $c_\phi = (\phi, \alpha)$, con lo que tenemos la garantía de que c_ϕ no es ningún signo de $\mathcal{L}$, ya que su rango es mayor que el de cualquiera de ellos.

que $\Delta = \Delta_0 \cup \Delta_1$, donde $\Delta_0 \subset \Gamma_n$ y Δ_1 está formado por sentencias de la forma $\bigvee x\, \phi(x) \to \phi(c_\phi)$, donde $\phi \in \mathrm{Form}(\mathcal{L}_n)$.

Como Γ_n es finitamente consistente, existe un modelo M de $\mathcal{L}_n$ tal que $M \vDash \Delta_0$. Extendemos M a un modelo de $\mathcal{L}_{n+1}$ del modo siguiente: si la fórmula $\bigvee x\, \phi(x) \to \phi(c_\phi)$ está en Δ_1 y $M \vDash \bigvee x\, \phi(x)$, elegimos[9] un $a \in M$ tal que $M \vDash \phi[a]$ y definimos $\bar{c}_\phi = a$. Si $\neg M \vDash \bigvee x\, \phi(x)$ o bien $\bigvee x\, \phi(x) \to \phi(c_\phi)$ no está en Δ_1, definimos $\bar{c}_\phi$ como un elemento cualquiera prefijado de M. Es claro entonces que (la extensión de) M satisface $M \vDash \Delta$, lo que prueba que Γ_{n+1} es finitamente consistente. Notemos que aquí es esencial que a fórmulas ϕ diferentes les corresponden constantes c_ϕ diferentes, por lo que no puede darse el caso de que tengamos que dar distintas interpretaciones a una misma constante.

■

Teorema 10.5 *Sea $\mathcal{L}$ un lenguaje formal y sea T una teoría $\mathcal{L}$ tal que:*

1. *T es finitamente consistente.*
2. *T es completa.*
3. *Para cada fórmula $\phi(x)$ de $\mathcal{L}$ con x como única variable libre existe una constante c tal que $\bigvee x\, \phi(x) \to \phi(c) \in T$.*

Entonces T es consistente.

Demostración: Sea C el conjunto de todas las constantes de $\mathcal{L}$ (que no puede ser vacío, por la condición c). Definimos en C la relación de equivalencia dada por $c \sim c' \leftrightarrow (c = c') \in T$.

Se trata ciertamente de una relación de equivalencia, pues $(c = c) \in T$, luego $c \sim c$, si $c \sim c'$ entonces $(c = c') \in T$, luego $T \vDash (c' = c)$, luego $(c' = c) \in T$, luego $c' \sim c$, y si $c \sim c'$ y $c' \sim c''$ entonces $(c = c') \in T$ y $(c' = c'') \in T$, luego $T \vDash c = c''$, luego $(c = c'') \in T$, luego $c \sim c''$.

Definimos M como el conjunto cociente de C respecto de la relación $\sim$. De este modo

$$[c] = [c'] \leftrightarrow (c = c') \in T.$$

Vamos a dotar a M de estructura de modelo de $\mathcal{L}$. Para cada constante c de $\mathcal{L}$ definimos $\bar{c} = [c]$. Para cada relator n-ádico R de $\mathcal{L}$ definimos

$$\bar{R}([c_1], \ldots, [c_n]) \leftrightarrow Rc_1 \cdots c_n \in T.$$

La definición es correcta, pues si $[c_i] = [c_i']$ y $\bar{R}([c_1], \ldots, [c_n])$, entonces

$$(c_i = c_i') \in T \quad \text{y} \quad Rc_1 \cdots c_n \in T,$$

luego $T \vDash Rc_1' \cdots c_n'$, luego $Rc_1' \cdots c_n' \in T$. Además, por la definición de M resulta que la relación asociada al igualador es la identidad en M.

[9] Se trata de un número finito de elecciones, por lo que no necesitamos AE.

Similarmente, si f es un funtor n-ádico en $\mathcal{L}$, definimos $\bar{f} : M^n \longrightarrow M$ mediante

$$\bar{f}([c_1], \ldots, [c_n]) = [c] \leftrightarrow (fc_1 \cdots c_n = c) \in T.$$

Esto es correcto, pues existe una constante c tal que

$$(\bigvee x\ fc_1 \cdots c_n = x \to fc_1 \cdots c_n = c) \in T$$

y trivialmente $T \vDash \bigvee x\ fc_1 \cdots c_n = x$, luego $(fc_1 \cdots c_n = c) \in T$. Por otra parte, si $(fc_1 \cdots c_n = c) \in T$ y $(fc_1 \cdots c_n = c') \in T$ entonces $(c = c') \in T$, luego $[c] = [c']$.

Veamos ahora que si $t(x_1, \ldots, x_n)$ es un término de $\mathcal{L}$, entonces

$$M \vDash t([c_1], \ldots, [c_n]) = [c] \quad \text{syss} \quad (t(c_1, \ldots, c_n) = c) \in T.$$

Razonamos por inducción sobre la longitud de t. Si $t = x_i$ es inmediato que

$$M \vDash [c_i] = [c] \quad \text{syss} \quad (c_i = c) \in T.$$

El argumento cuando $t = c'$ es casi idéntico. Si $t = ft_1 \cdots t_m$ y el resultado vale para los t_j, entonces tomamos constantes c'_j tales que T contenga la sentencia

$$\bigvee x\, t_j(c_1, \ldots, c_n) = x \to t_j(c_1, \ldots, c_n) = c'_j.$$

Como $T \vDash \bigvee x\, t_j(c_1, \ldots, c_n) = x$, resulta que $(t_j(c_1, \ldots, c_n) = c'_j) \in T$. Por hipótesis de inducción $M \vDash t_j([c_1], \ldots, [c_n]) = [c'_j]$.

Entonces $M \vDash (ft_1 \cdots t_m)([c_1], \ldots, [c_n]) = [c]$ si y sólo si

$$\bar{f}(M(t_1)[[c_1], \ldots, [c_n]], \ldots, M(t_m)[[c_1], \ldots, [c_n]]) = \bar{c}$$

si y sólo si $\bar{f}([c'_1], \ldots, [c'_m]) = \bar{c}$, si y sólo si $(fc'_1 \cdots c'_n = c) \in T$, si y sólo si

$$T \vDash t(c_1, \ldots, c_n) = c \quad \text{syss} \quad (t(c_1, \ldots, c_n) = c) \in T.$$

Seguidamente probamos que, para toda fórmula $\phi(x_1, \ldots, x_n)$ de $\mathcal{L}$, se cumple

$$M \vDash \phi[[c_1], \ldots, [c_n]] \quad \text{syss} \quad \phi(c_1, \ldots, c_n) \in T.$$

En efecto, si $\phi = Rt_1 \cdots t_m$, y $M \vDash \phi[[c_1], \ldots, [c_n]]$, tenemos que existen constantes c'_j tales que T contiene las sentencias

$$\bigvee x\ x = t_j(c_1, \ldots, c_n) \to c'_j = t_j(c_1, \ldots, c_n).$$

Claramente entonces $T \vDash c'_j = t_j(c_1, \ldots, c_n)$, luego y hemos probado que entonces $M \vDash [c'_j] = t_j([c_1], \ldots, [c_n])$. Por lo tanto, $M \vDash Rt_1 \cdots t_m([c_1], \ldots, [c_n])$ si y sólo si

$$\bar{R}(M(t_1)([c_1], \ldots, [c_n]), \ldots, M(t_m)([c_1], \ldots, [c_n])) \quad \text{syss} \quad \bar{R}([c'_1], \ldots, [c'_m])$$

syss $Rc'_1 \cdots c'_n \in T$ syss $T \vDash Rt_1 \cdots t_m([c_1], \ldots, [c_n])$ syss $\phi(c_1, \ldots, c_n) \in T$.

Si $\phi = \neg\alpha$ y el resultado vale para α, entonces

$$M \vDash \neg\alpha[[c_1,\dots,c_n]] \quad \text{syss} \quad \neg M \vDash \alpha[[c_1],\dots,[c_n]] \quad \text{syss} \quad \alpha(c_1,\dots,c_n) \notin T$$

syss $\neg\alpha(c_1,\dots,c_n) \in T$. En el último paso usamos que T es finitamente consistente y completa, pues por la completitud sabemos que $\alpha(c_1,\dots,c_n) \in T$ o $\neg\alpha(c_1,\dots,c_n) \in T$ y por la consistencia finita no se pueden dar los dos casos a la vez.

Si $\phi = (\alpha \to \beta)$, entonces (suponiendo que α y β cumplen el resultado y usando que $\neg\alpha$ también lo cumple, como ya hemos probado),

$$M \vDash \phi[[c_1],\dots,[c_n]] \quad \text{syss} \quad \neg M \vDash \alpha[[c_1],\dots,[c_n]] \vee M \vDash \beta[[c_1],\dots,[c_n]]$$

$$\text{syss} \quad \alpha(c_1,\dots,c_n) \notin T \vee \beta(c_1,\dots,c_n) \in T \quad \text{syss} \quad T \vDash \phi(c_1,\dots,c_n)$$

syss $\phi(c_1,\dots,c_n) \in T$.

Finalmente, si $\phi = \bigwedge x\, \alpha(x, x_1,\dots,x_n)$ y el resultado vale para α,

$$M \vDash \phi[[c_1],\dots,[c_n]] \quad \text{syss} \quad \bigwedge c \in \mathrm{Const}(\mathcal{L})\ M \vDash \alpha[[c],[c_1],\dots,[c_n]]$$

$$\text{syss} \quad \bigwedge c \in \mathrm{Const}(\mathcal{L})\ \alpha(c, c_1,\dots,c_n) \in T.$$

Veamos que esto implica que $\bigwedge x\, \alpha(x, c_1,\dots,c_n) \in T$. En caso contrario, como existe una constante c tal que

$$\bigvee x\, \neg\alpha(x, c_1,\dots,c_n) \to \neg\alpha(c, c_1,\dots,c_n) \in T,$$

resulta que si $\bigwedge x\, \alpha(x, c_1,\dots,c_n) \notin T$, entonces $\neg\bigwedge x\, \alpha(x, c_1,\dots,c_n) \in T$, luego $T \vDash \bigvee x\, \neg\alpha(x, c_1,\dots,c_n)$, luego $T \vDash \neg\alpha(c, c_1,\dots,c_n)$, luego $\alpha(c, c_1,\dots,c_n) \notin T$, contradicción.

Recíprocamente, si $\bigwedge x\, \alpha(x, c_1,\dots,c_n) \in T$ y $c \in \mathrm{Const}(\mathcal{L})$, entonces es claro que $T \vDash \alpha(c, c_1,\dots,c_n)$, luego $\alpha(c, c_1,\dots,c_n) \in T$.

En particular hemos probado que si ϕ es una sentencia de $\mathcal{L}$ se cumple

$$M \vDash \phi \leftrightarrow \phi \in T,$$

luego $M \vDash T$ y T es consistente. ∎

Ahora podemos probar (sin AE):

Teorema 10.6 (Teorema de compacidad (versión numerable)) *Si $\mathcal{L}$ es un lenguaje formal numerable (es decir, con una cantidad numerable de signos), un conjunto Γ de sentencias de $\mathcal{L}$ es consistente si y sólo si es finitamente consistente.*

Demostración: Razonamos en principio sin la hipótesis de numerabilidad. Si Γ es finitamente consistente, entonces, por el teorema 10.4, existe un lenguaje $\mathcal{L}'$, que resulta de añadir a $\mathcal{L}$ un conjunto de constantes, y un conjunto Γ' de

sentencias que contiene a Γ y que cumple las hipótesis a) y c) del teorema anterior. Supongamos que existe una teoría T completa y finitamente consistente tal que $\Gamma' \subset T$. Entonces T cumple las hipótesis del teorema anterior, luego T es consistente, es decir, existe un modelo M de $\mathcal{L}'$ tal que $M \models T$. En particular tenemos que $M \models \Gamma$. Pero es claro que si consideramos el modelo M_0 de $\mathcal{L}$ que se obtiene de M sin más que eliminar las interpretaciones de las constantes nuevas de $\mathcal{L}'$, entonces $M_0 \models \Gamma$, luego Γ es consistente.

Así pues, el problema es extender Γ' a una teoría completa sin perder la consistencia finita. Vamos a probar que esto es posible cuando $\mathcal{L}$ es numerable y más adelante probaremos que con AE es posible en general.

Si $\mathcal{L}$ es numerable, todos los lenguajes $\mathcal{L}_n$ que se construyen en la prueba de 10.4 son numerables también. Para probar esto basta observar que si $\mathcal{L}_n$ es numerable, entonces el conjunto de sus fórmulas con una única variable libre es también numerable, luego también lo es el conjunto de constantes que se le añaden para formar $\mathcal{L}_{n+1}$. Más aún, la prueba del teorema 5.31 muestra que podemos construir una biyección explícita entre un conjunto infinito A y $A^{<\omega}$, por lo que podemos construir recurrentemente biyecciones f_n entre los signos de $\mathcal{L}_n$ y ω, lo que a su vez permite probar que el lenguaje $\mathcal{L}'$ también es numerable. A su vez, lo es el conjunto de sus sentencias, que podemos numerar como $\{\phi_n\}_{n\in\omega}$.

Construimos ahora por recurrencia una sucesión $\{\Gamma'_n\}_{n\in\omega}$ de conjuntos finitos de sentencias de $\mathcal{L}'$. Tomamos $\Gamma'_0 = \varnothing$ y, supuesto definido Γ'_n, definimos

$$\Gamma'_{n+1} = \begin{cases} \Gamma'_n \cup \{\alpha_n\} & \text{si } \Gamma' \cup \Gamma'_n \cup \{\phi_n\} \text{ es finitamente consistente,} \\ \Gamma'_n & \text{en caso contrario.} \end{cases}$$

Es claro que $\Gamma \cup \Gamma'_n$ es finitamente consistente para todo n.

Llamamos $T = \bigcup_{n\in\omega} \Gamma'_n$. Veamos que cumple lo requerido. En primer lugar, $\Gamma' \subset T$, pues si $\phi \in \Gamma'$, entonces existe un n tal que $\phi = \phi_n$. Por construcción $\Gamma \cup \Gamma'_n$ es finitamente consistente, luego $\Gamma \cup \Gamma'_n \cup \{\phi_n\} = \Gamma \cup \Gamma'_n$ también lo es, luego tenemos que $\phi = \phi_n \in \Gamma'_{n+1} \subset T$.

También es claro que T es finitamente consistente.

Veamos ahora que si ϕ es una sentencia, entonces $\phi \in T$ o bien $\neg\phi \in T$. Esto implica claramente que T es una teoría y que es completa.

Sean m, n tales que $\phi = \phi_m$, $\neg\phi = \phi_n$. Supongamos, por ejemplo, que $m < n$ (el caso contrario es análogo). Si $\phi \notin T$, entonces $\phi_m \notin \Gamma'_{m+1}$, luego $\Gamma \cup \Gamma'_m \cup \{\phi\}$ no es finitamente consistente, luego existe $\Delta \subset \Gamma \cup \Gamma'_m \cup \{\phi\}$ finito y contradictorio. Necesariamente $\phi \in \Delta$, puesto que $\Gamma \cup \Gamma'_m$ es finitamente consistente. Por otra parte, $\Gamma \cup \Gamma'_n$ es finitamente consistente y contiene a $\Delta \setminus \{\phi\}$. Si $\Delta' \subset \Gamma \cup \Gamma'_n \cup \{\neg\phi\}$ es finito, entonces $(\Delta \cup \Delta') \setminus \{\phi, \neg\phi\}$ es un subconjunto finito de $\Gamma \cup \Gamma'_n$, luego tiene un modelo M, luego $M \models \Delta \setminus \{\phi\}$, pero no puede ser $M \models \phi$, porque Δ es contradictorio, luego $M \models \neg\phi$, luego $M \models \Delta'$, luego $\Gamma \cup \Gamma'_n$ es finitamente consistente, luego $\neg\phi \in \Gamma'_{n+1} \subset T$. ∎

En realidad hemos probado la versión numerable de un teorema importante:

Teorema 10.7 (Teorema de Löwenheim-Skolem) *Si una teoría T sobre un lenguaje formal numerable tiene un modelo, entonces tiene un modelo (de universo) numerable.*

DEMOSTRACIÓN: Si T tiene un modelo, entonces es consistente, luego es finitamente consistente, luego tiene por modelo el construido en la prueba del teorema 10.5 (a partir de un lenguaje numerable). Es claro que el universo de dicho modelo es numerable. ∎

Ejemplo Consideremos a $\mathbb{R}$ como modelo del lenguaje (numerable) de la teoría de anillos ordenados y es $T = T(\mathbb{R})$. Se trata de una teoría consistente, luego tiene un modelo numerable K, de modo que $T(K) = T(\mathbb{R})$. Es claro entonces que K es un cuerpo ordenado numerable, luego no es isomorfo a $\mathbb{R}$ (ni como cuerpo, ni como modelo, que es lo mismo), pero satisface exactamente las propiedades que $\mathbb{R}$ expresables en el lenguaje $\mathcal{L}_a$. Más adelante volveremos sobre esto. ∎

Veamos ahora cómo probar el teorema de compacidad para lenguajes arbitrarios. Vamos a probar que es equivalente a la siguiente versión débil del teorema de los ultrafiltros 7.10:

Teorema de los Ultrafiltros (TU) *Todo filtro en un conjunto puede extenderse a un ultrafiltro.*

Obviamente, este teorema es equivalente a la versión correspondiente para ideales primos: todo ideal en un conjunto puede extenderse a un ideal primo. Para probar la equivalencia incluiremos una afirmación intermedia:

Principio de coherencia *Sea A un conjunto y $\mathcal{F}$ una familia de funciones definidas sobre subconjuntos finitos de A con valores en $\{0,1\}$ de modo que toda restricción de toda función de $\mathcal{F}$ está en $\mathcal{F}$ y para todo subconjunto finito de A existe al menos una función en $\mathcal{F}$ con dicho dominio, existe una función $f : A \longrightarrow 2$ tal que, para todo $x \subset A$ finito, se cumple $f|_x \in \mathcal{F}$.*

Teorema 10.8 *Las afirmaciones siguientes son equivalentes a* (TU):

1. *Toda álgebra de Boole tiene un ultrafiltro (resp. un ideal primo).*
2. *Todo filtro (resp. ideal) en un álgebra de Boole puede extenderse a un ultrafiltro (resp. ideal primo).*
3. *El principio de coherencia.*
4. *El teorema de compacidad: Un conjunto Γ de sentencias de un lenguaje formal $\mathcal{L}$ es consistente si y sólo si es finitamente consistente.*

DEMOSTRACIÓN: Notemos que, por dualidad, las dos versiones de a) y b) son equivalentes entre sí.

a) $\Rightarrow$ b) Si F es un filtro en un álgebra de Boole $\mathbb{B}$, consideramos un ultrafiltro $\bar{U}$ del álgebra cociente $\mathbb{B}/F$ y el epimorfismo canónico $p : \mathbb{B} \longrightarrow \mathbb{B}/F$. Entonces $U = p^{-1}[\bar{U}]$ es un ultrafiltro en $\mathbb{B}$ que contiene a F.

b) $\Rightarrow$ TU es evidente.

TU $\Rightarrow$ c) Sea $\mathcal{F}$ un conjunto de funciones definidas en subconjuntos finitos de A según las condiciones del principio de coherencia, sea I el ideal formado por los subconjuntos finitos de A. Para cada $x \in I$, sea $\mathcal{F}_x$ el conjunto (finito) de todas las aplicaciones $t \in \mathcal{F}$ tales que $\mathcal{D}t = x$. Sea Z el conjunto de todas las funciones z tales que

1. $\mathcal{D}z \subset I$.
2. $\bigwedge x \in \mathcal{D}z\ z(x) \in \mathcal{F}_x$.
3. $\bigwedge xy \in \mathcal{D}z\ (z(x) \cup z(y) : x \cup y \longrightarrow 2)$.

Para cada $x \in I$, sea $Z_x = \{z \in Z \mid x \in \mathcal{D}z\} \neq \varnothing$ y notemos que si x, $y \in I$ entonces $Z_x \cap Z_y \neq \varnothing$, pues existe $t \in \mathcal{F}$ tal que $\mathcal{D}t = x \cup y$ y basta tomar $z = \{(x, t|_x), (y, t|_y)\}$, que cumple $z \in Z_x \cap Z_y$. Por lo tanto,

$$F = \{X \in \mathcal{P}Z \mid \bigvee x \in I\ Z_x \subset X\}$$

es un filtro en Z. Por hipótesis está contenido en un ultrafiltro U. Para cada $x \in I$, si $\mathcal{F}_x = \{t_1, \ldots, t_n\}$, entonces

$$Z_x = Z_{t_1} \cup \cdots \cup Z_{t_n},$$

donde, para cada $t \in \mathcal{F}$, llamamos $Z_t = \{z \in Z_x \mid z(x) = t\}$. Como la unión está en U y es disjunta, existe un único $t \in \mathcal{F}_x$ tal que $Z_t \in U$ (si $Z_{t_i} \notin U$ para todo i, entonces $Z \setminus Z_{t_i} \in U$, luego $\varnothing = Z_x \cap \bigcap_i (Z \setminus Z_{t_i}) \in U$).

Llamemos $t_x : x \longrightarrow 2$ al único elemento de $\mathcal{F}_x$ tal que $Z_{t_x} \in U$. Si x, $y \in I$, tenemos que Z_{t_x}, $Z_{t_y} \in U$, luego $Z_{t_x} \cap Z_{t_y} \in U$, luego existe $z \in Z_{t_x} \cap Z_{t_y}$, luego $z(x) = t_x$, $z(y) = t_y$, luego $t_x \cup t_y$ es una función. Esto implica que

$$f = \bigcup_{x \in I} t_x : A \longrightarrow 2$$

es una función que cumple lo requerido.

c) $\Rightarrow$ d) Según lo visto en la primera parte de la prueba del teorema 10.6, para probar el teorema de compacidad basta probar que todo conjunto finitamente consistente Γ de sentencias de un lenguaje formal $\mathcal{L}$ puede extenderse a una teoría T finitamente consistente y completa.

Sea $A = \mathrm{Sent}(\mathcal{L})$ y sea $\mathcal{F}$ el conjunto de las funciones t definidas sobre subconjuntos finitos de A de modo que existe un modelo M de $\Gamma \cap \mathcal{D}t$ tal que

$$\bigwedge \phi \in \mathcal{D}t\, (t(\phi) = 1 \leftrightarrow M \vDash \phi).$$

La consistencia finita de Γ implica que $\mathcal{F}$ para todo subconjunto finito de A existe una función en $\mathcal{F}$ que lo tiene por dominio, por lo que $\mathcal{F}$ cumple las hipótesis del principio de coherencia, y podemos concluir que existe $f : A \longrightarrow 2$ tal que $f|_x \in \mathcal{F}$ para todo $x \subset A$ finito. Definimos

$$T = \{\phi \in A \mid f(\phi) = 1\}$$

y es claro que $\Gamma \subset T$. Además T es una teoría completa, porque si $\phi \in A$, tenemos que $f|_{\{\phi,\neg\phi\}} \in \mathcal{F}$, luego existe un modelo $M \vDash \Gamma \cap \{\phi, \neg\phi\}$, y entonces

$$f(\phi) = 1 \leftrightarrow M \vDash \phi \leftrightarrow \neg M \vDash \neg\phi \leftrightarrow \neg f(\neg\phi) = 1,$$

luego $\phi \in T$ o bien $\neg\phi \in T$.

d) $\Rightarrow$ a) Sea $\mathbb{B}$ un álgebra de Boole y consideremos un lenguaje formal $\mathcal{L}$ que tenga como constantes los elementos de $\mathbb{B}$, así como un relator monádico f. Consideramos el conjunto Γ formado por las sentencias siguientes de $\mathcal{L}$:

1. $\neg f\mathbb{0}$, $f\mathbb{1}$,
2. $fb \vee fb'$, para cada $b \in \mathbb{B}$,
3. $fb_1 \wedge \cdots \wedge fb_n \to f(b_1 \wedge \cdots \wedge b_n)$, para todos los $b_1, \ldots, b_n \in \mathbb{B}$.

Observemos que Γ es finitamente consistente, pues si $\Delta \subset \Gamma$ es finito, el conjunto $X \subset \mathbb{B}$ de las constantes que aparecen en las sentencias de Δ es finito. Sea $\mathbb{C}$ la subálgebra de $\mathbb{B}$ generada por X, que por 7.6 es finita, y obviamente tiene un ultrafiltro U (basta tomar un filtro maximal respecto de la inclusión). Podemos convertir a $\mathbb{C}$ en un modelo de Δ sin más que interpretar cada constante como ella misma y el relator f como la pertenencia a U.

Por lo tanto, tenemos que Γ es consistente, es decir, que tiene un modelo M, y eso implica que el conjunto

$$U = \{b \in \mathbb{B} \mid M \vDash fb\}$$

es un ultrafiltro de $\mathbb{B}$. ∎

Es inmediato que TU es equivalente a que toda álgebra es isomorfa a un álgebra de conjuntos, pues toda álgebra de conjuntos $\mathbb{B}$ tiene un ultrafiltro: basta tomar $x \in \bigcup \mathbb{B}$ y definir $U = \{A \in \mathbb{B} \mid x \in A\}$.

Una versión equivalente del teorema de compacidad es la siguiente:

Teorema 10.9 (TU) *Si Γ es un conjunto de sentencias de un lenguaje formal $\mathcal{L}$ y ϕ es una sentencia de $\mathcal{L}$ tal que $\Gamma \vDash \phi$, entonces existe $\Delta \subset \Gamma$ finito tal que $\Delta \vDash \phi$.*

Demostración: En caso contrario, para cada $\Delta \subset \Gamma$ finito tendríamos que $\Delta \cup \{\neg\phi\}$ sería consistente, luego por el teorema de compacidad $\Gamma \cup \{\neg\phi\}$ sería consistente, pero esto contradice que $\Gamma \vDash \phi$. ∎

En particular si Γ es contradictorio (tomando como ϕ una contradicción) concluimos que tiene un subconjunto finito contradictorio, pero esto es el teorema de compacidad, que es, pues, equivalente al teorema anterior.

En la nota tras el teorema de Tychonoff [T 4.15] hemos observado que TU implica que el producto de espacios de Hausdorff compactos es compacto. Ahora podemos demostrar el recíproco:

Teorema 10.10 TU *es equivalente a que, para todo conjunto I, el espacio 2^I (con el producto de la topología discreta en 2) es compacto.*

Demostración: Sea $\mathbb{B}$ un álgebra de Boole. Para cada $b \in \mathbb{B}$, consideramos la aplicación $h_b : 2 \longrightarrow \{b, b'\}$ dada por $h_b(0) = b'$, $h_b(0) = b$. Tenemos entonces un homeomorfismo $h : 2^{\mathbb{B}} \longrightarrow X = \prod_{b\in\mathbb{B}} \{b, b'\}$ dado por $h(f)(b) = h_b(f(b))$. Por hipótesis $2^{\mathbb{B}}$ es compacto, luego X también lo es.

Sea $\mathbb{C}$ una subálgebra finita de $\mathbb{B}$ y sea I un ideal primo en $\mathbb{C}$. Definimos

$$\mathbb{C}_I = \{f \in X \mid \bigwedge c \in \mathbb{C}\ f(u) \in I\},$$

que es abierto y cerrado no vacío en X, al igual que

$$B_{\mathbb{C}} = \bigcup\{\mathbb{C}_I \mid I \text{ es un ideal primo de } \mathbb{C}\}.$$

Observemos que la familia formada por todos los $B_{\mathbb{C}}$ tiene la propiedad de la intersección finita, ya que si $\mathbb{C}_1, \ldots, \mathbb{C}_n$ son subálgebras finitas de $\mathbb{B}$, entonces la subálgebra $\mathbb{C}$ generada por la unión es finita (por 7.6) y entonces

$$B_{\mathbb{C}} \subset B_{\mathbb{C}_1} \cap \cdots \cap B_{\mathbb{C}_n},$$

ya que si $f \in B_{\mathbb{C}}$ existe un ideal primo I de $\mathbb{C}$ tal que $f \in \mathbb{C}_I$, pero entonces $I_i = I \cap \mathbb{C}_i$ es un ideal primo en $\mathbb{C}_i$ y $f \in \mathbb{C}_{I_i} \subset B_{\mathbb{C}_i}$. Como X es compacto, existe $f \in \bigcap_{\mathbb{C}} B_{\mathbb{C}}$. Sea $I_0 = \{f(b) \mid b \in \mathbb{B}\}$.

Vamos a probar que I_0 es un ideal primo en $\mathbb{B}$. Ante todo, si $b \in \mathbb{B}$ tenemos que $f(b) \in \{b, b'\} \cap I_0$, es decir, que $b \in I_0$ o bien $b' \in I_0$.

Para cada $b \in \mathbb{B}$, consideramos el álgebra $\mathbb{C}$ generada por b y sea I un ideal primo en ella tal que $f \in \mathbb{C}_I$. Entonces $\mathbb{0} = f(\mathbb{0}) \in I$, luego $\mathbb{0} \in I_0$ y $f(b) \in I_0$, luego $f(b) \neq \mathbb{1}$, luego $\mathbb{1} \notin I_0$.

Si $f(b) \in I_0$ y $c \leq f(b)$, consideramos el álgebra $\mathbb{C}$ generada por b y c y consideramos un ideal primo I en $\mathbb{C}$ tal que $f \in \mathbb{C}_I$. Entonces $f(b) \in I$, luego $c \in I$, luego $c = f(c) \in I_0$.

Finalmente, si $f(b)$, $f(c) \in I_0$, consideramos el álgebra $\mathbb{C}$ generada por b y c y tomamos un ideal primo I tal que $f \in \mathbb{C}_I$. Entonces $f(b)$, $f(c) \in I$, luego $f(b) \vee f(c) \in I$, luego $f(b) \vee f(c) = f(f(b) \vee f(c)) \in I_0$.

Con esto queda probado que I_0 es un ideal primo. ∎

Más aún:

Teorema 10.11 (TU) *Todo producto de espacios compactos de Hausdorff no vacíos es no vacío.*

DEMOSTRACIÓN: Sea $X = \prod_{i\in I} X_i$ un producto de espacios de Hausdorff compactos no vacíos.

Sea Z el conjunto de todas las funciones f tales que

$$\mathcal{D}f \subset I \wedge \bigwedge i \in \mathcal{D}f\ f(i) \in X_i.$$

Para cada $i \in I$, sea $Z_i = \{f \in Z \mid i \in \mathcal{D}f\}$. Es claro que los conjuntos Z_i forman una familia de subconjuntos de Z con la propiedad de la intersección finita, luego generan un filtro que, a su vez, está contenido en un ultrafiltro U.

Para cada $i \in I$, es fácil ver que el conjunto

$$U_i = \{A \in \mathcal{P}X_i \mid \{f \in Z \mid i \in \mathcal{D}f \wedge f(i) \in A\} \in U\}$$

es un ultrafiltro en X_i. (Aquí usamos que, como $Z_i \in U$, se cumple $X_i \in U_i$.) Pero un ultrafiltro U_i convergente en un espacio de Hausdorff tiene un único límite x_i, con lo que hemos determinado un punto $x \in X$. ∎

Álgebras de Lindenbaum Los axiomas que definen las álgebras de Boole pueden interpretarse como las propiedades de la unión, la intersección y el complemento de conjuntos, pero también como propiedades de las sentencias de una teoría formal. La relación precisa entre las álgebras de Boole y la lógica se realiza a través del concepto de álgebra de Lindenbaum, que presentamos a continuación:

Definición 10.12 Sea T una teoría sobre un lenguaje formal $\mathcal{L}$. Definimos en $\mathrm{Sent}(\mathcal{L})$ la relación de equivalencia dada por

$$\alpha \sim \beta \quad \text{syss} \quad T \vDash \alpha \leftrightarrow \beta.$$

Observemos que esto equivale también a que, en cada modelo de T, las sentencias α y β sean ambas verdaderas o ambas falsas, por lo que claramente es una relación de equivalencia.

Llamaremos $\mathbb{B}_T$ al conjunto cociente de $\mathrm{Sent}(T)$ respecto de la relación de equivalencia que acabamos de definir.

De este modo, si $p \in \mathbb{B}_T$, en cada modelo de T las sentencias de p son todas verdaderas o todas falsas, y si $p, q \in \mathbb{B}_T$ cumplen $p \neq q$, existe un modelo en el que las sentencias de p son verdaderas y las de q falsas o viceversa.

Es inmediato que las operaciones $\wedge$, $\vee$ y $'$ en $\mathbb{B}_T$ dadas por

$$[\alpha] \wedge [\beta] = [\alpha \wedge \beta], \qquad [\alpha] \vee [\beta] = [\alpha \vee \beta], \qquad [\alpha]' = [\neg\alpha]$$

están bien definidas (en el sentido de que no dependen de los representantes elegidos para calcularlas) y convierten a $\mathbb{B}_T$ en un álgebra de Boole con

$$\mathbb{1} = T, \qquad \mathbb{0} = \mathbb{1}'.$$

(Así, $\mathbb{1}$ está formado por las sentencias de T, es decir, las sentencias que son verdaderas en todo modelo de T, mientras que $\mathbb{0}$ contiene a todas las sentencias que son falsas en todo modelo de T.)

El álgebra $\mathbb{B}_T$ se llama *álgebra de Lindenbaum* de la teoría T.

Es claro que el álgebra $\mathbb{B}_T$ es degenerada si y sólo si T es contradictoria, mientras que $\mathbb{B}_T$ es trivial (es decir, cumple $\mathbb{B}_T = \{\mathbb{0}, \mathbb{1}\}$) si y sólo si T es completa.

Esto sucede, por ejemplo, con todas las teorías de la forma $T(M)$, para un modelo M.

Según las definiciones de $\to$ y $\leftrightarrow$ dadas para álgebras de Boole arbitrarias, es claro que

$$[\alpha] \to [\beta] = [\alpha \to \beta], \quad [\alpha] \leftrightarrow [\beta] = [\alpha \leftrightarrow \beta].$$

A su vez, $[\alpha] \le [\beta]$ equivale a que siempre que α es verdadera en un modelo de T sucede que β también lo es.

Teorema 10.13 (TU) *Si T es una teoría consistente sobre un lenguaje formal $\mathcal{L}$, los filtros del álgebra $\mathbb{B}_T$ se corresponden biunívocamente con las teorías consistentes que contienen a T. La correspondencia viene dada por*

$$F \mapsto T_F = \{\alpha \in \mathrm{Sent}(\mathcal{L}) \mid [\alpha] \in F\}, \qquad T' \mapsto F_{T'} = \{[\alpha] \in \mathbb{B}_T \mid \alpha \in T'\}.$$

Demostración: Observemos que T_F es una teoría, pues si $T_F \vDash \phi$ entonces existe $\Delta \subset T_F$ finito tal que $\Delta \vDash \phi$, luego, si $\Delta = \{\delta_1, \dots, \delta_n\}$, tenemos que $[\delta_1 \wedge \cdots \wedge \delta_n] \in F$ y $[\delta_1 \wedge \cdots \wedge \delta_n] \le [\phi]$, luego $[\phi] \in F$, luego $\phi \in T_F$.

Además T_F es finitamente consistente, pues si $\alpha_1, \dots, \alpha_n \in T_F$, entonces $[\alpha_1 \wedge \cdots \wedge \alpha_n] \in F$, luego $[\alpha_1 \wedge \cdots \wedge \alpha_n] \ne \mathbb{0}$, luego la conjunción tiene un modelo, que también será un modelo de $\{\alpha_1, \dots, \alpha_n\}$. Por el teorema de compacidad T_F es consistente.

El resto del teorema es inmediato. ∎

En particular, los ultrafiltros de $\mathbb{B}_T$ (es decir, los puntos del espacio de Stone $S(\mathbb{B}_T)$) se corresponden con las teorías (consistentes) completas que contienen a T o, equivalentemente, a las teorías de la forma $T(M)$, donde M es un modelo de T.

Si Γ es un conjunto de sentencias finitamente consistentes, entonces el conjunto $X = \{[\alpha] \in \mathbb{B}_T \mid \alpha \in \Gamma\}$ tiene propiedad de la intersección finita, luego genera un filtro F que se corresponde con la teoría axiomatizada por Γ.

Órdenes totales Sabemos que AE equivale a que todo conjunto puede ser bien ordenado. Con TU podemos demostrar que todo conjunto puede ser totalmente ordenado. Podemos probar un poco más:

Teorema 10.14 (TU) *Todo orden parcial en un conjunto X puede extenderse hasta un orden total.*

DEMOSTRACIÓN: Sea $\leq$ el orden parcial dado en X. Consideremos un lenguaje formal $\mathcal{L}$ que tenga como constantes a los elementos de X y además un relator diádico $\preceq$. Sea Γ el conjunto formado por las sentencias siguientes (donde p, q, r son constantes cualesquiera):

1. $p \preceq p$,
2. $p \preceq q \wedge q \leq p \to p = q$,
3. $p \preceq q \wedge q \preceq r \to p \preceq r$,
4. $p \preceq q \vee q \preceq p$,
5. $p \preceq q$ si $p \leq q$.

Si Δ es un subconjunto finito de Γ, sea $X_0 \subset X$ el conjunto (finito) de todas las constantes que aparecen en alguna sentencia de Δ. Entonces X_0 es un conjunto finito parcialmente ordenado por $\leq$, y es fácil ver que $\leq$ puede extenderse a un orden total en X_0 (por ejemplo, como la relación $<$ está bien fundada, podemos considerar su rango y definir $x \leq^* y \leftrightarrow \mathrm{rang}(x) \leq \mathrm{rang}(y)$). Con tal extensión, X_0 se convierte en un modelo de Δ, luego Γ es finitamente consistente y, por lo tanto, consistente. Si M es un modelo de Γ, entonces la relación en X dada por

$$p \leq^* q \leftrightarrow M \vDash p \preceq q$$

es un orden total en X que extiende al orden dado $\leq$. ∎

Como consecuencia inmediata:

Teorema 10.15 (TU) *Toda familia de conjuntos finitos tiene una función de elección.*

DEMOSTRACIÓN: Basta considerar un orden total $\leq$ en $\bigcup X$, de modo que cada $x \in X$ está totalmente ordenado (luego bien ordenado, al ser finito) por la restricción de $\leq$, luego si no es vacío podemos escoger en él su mínimo elemento. ∎

Observemos que el teorema anterior es un caso particular de 10.11.

Modelos infinitos Una teoría formal puede tener únicamente modelos finitos. Por ejemplo, si una teoría consistente contiene entre sus sentencias a

$$\bigvee uvwxyz \bigwedge s(s = u \vee s = u \vee s = v \vee s = x \vee s = y \vee s = z),$$

entonces todos sus modelos tendrán a lo sumo 6 elementos. Si exigimos además que u, v, w, x, y, z sean distintos dos a dos, podemos exigir que todos los modelos tengan exactamente 6 elementos. Ahora bien, el teorema de compacidad implica que ninguna teoría puede garantizar que todos sus modelos sean finitos sin imponer una cota concreta (finita) al cardinal de dichos modelos:

Teorema 10.16 (TU)[10] *Si una teoría T tiene modelos finitos de cardinal arbitrariamente grande, entonces tiene modelos infinitos.*

DEMOSTRACIÓN: Sea $\mathcal{L}$ el lenguaje de T y sea $\mathcal{L}'$ el lenguaje que resulta de añadir a $\mathcal{L}$ un conjunto numerable de constantes $\{c_n\}_{n\in\omega}$. Sea Γ el conjunto de sentencias de $\mathcal{L}'$ formado por las sentencias de T y las de la forma $c_m \neq c_n$, para todo $m \neq n$.

Entonces Γ es finitamente consistente, pues si Δ es un subconjunto finito de Γ, sea k el número de constantes c_n que aparecen en las sentencias de Δ. Por hipótesis, T tiene un modelo M de cardinal mayor que k, y dicho modelo M se convierte en un modelo de Δ sin más que interpretar las k constantes c_n que aparecen en las sentencias de Δ como k elementos distintos de M y el resto de ellas como cualquier elemento prefijado de M.

Por el teorema de compacidad Γ tiene un modelo M, que en particular es un modelo de T en el que las constantes $\{c_n \mid n \in \omega\}$ tienen interpretaciones distintas dos a dos, luego M es infinito. ∎

En la sección siguiente incidiremos en este uso del teorema de compacidad para construir modelos de cardinal grande de una teoría dada.

10.3 Submodelos, inmersiones

Estudiamos ahora las aplicaciones que relacionan dos modelos de un mismo lenguaje formal.

Definición 10.17 Una *inmersión* $i : N \longrightarrow M$ entre dos modelos de un mismo lenguaje formal $\mathcal{L}$ es una aplicación que verifica las propiedades siguientes:

1. Para toda constante c de $\mathcal{L}$ se cumple que $i(N(c)) = M(c)$.
2. Para todo relator n-ádico R de $\mathcal{L}$ se cumple que
$$\bigwedge a_1 \dots a_n \in N(N(R)(a_1, \dots, a_n) \leftrightarrow M(R)(i(a_1), \dots, i(a_n))).$$
3. Para todo funtor n-ádico f de $\mathcal{L}$ se cumple que
$$\bigwedge a_1 \dots a_n \in N(i(N(f)(a_1, \dots, a_n)) = M(f)(i(a_1), \dots, i(a_n))).$$

Observemos que la propiedad b) aplicada al igualador implica que toda inmersión es inyectiva. Una inmersión biyectiva es un *isomorfismo* de modelos. Por ejemplo, una inmersión entre dos anillos unitarios (vistos como modelos del lenguaje de la teoría de anillos) no es más que un monomorfismo de anillos unitarios en el sentido algebraico usual.

Diremos que un modelo N es un *submodelo* de un modelo M del mismo lenguaje formal si $N \subset M$ y la inclusión es una inmersión.

Supongamos que M es un modelo de un lenguaje $\mathcal{L}$ y que $N \subset M$ es un subconjunto de M con las propiedades siguientes:

[10] Si el lenguaje de la teoría es numerable, este teorema no requiere TU, pues podemos usar la versión 10.6 del teorema de compacidad.

1. $M(c) \in N$ para toda constante c de $\mathcal{L}$.

2. $M(f)|_{N^n} : N^n \longrightarrow N$, para todo funtor n-ádico f de $\mathcal{L}$.

Entonces N admite una única estructura de submodelo de M. De hecho, ésta es una definición alternativa de submodelo.

Por ejemplo, los submodelos de un anillo unitario (visto como modelo del lenguaje de la teoría de anillos) son simplemente los subanillos unitarios (es decir, con la misma unidad) en el sentido algebraico usual.

De las definiciones se sigue inmediatamente que la imagen de una inmersión es un submodelo y que, equivalentemente, una inmersión entre dos modelos es un isomorfismo de uno en un submodelo del otro.

Teorema 10.18 *Si $i : N \longrightarrow M$ es una inmersión entre dos modelos de un mismo lenguaje formal $\mathcal{L}$, $t(x_1, \ldots, x_n)$ es un término de $\mathcal{L}$ y $a_1, \ldots a_n \in N$, entonces*

$$i(N(t)[a_1, \ldots, a_n]) = M(t)[i(a_1), \ldots, i(a_n)].$$

DEMOSTRACIÓN: Por inducción sobre la longitud de t. Si $t = x_i$ es una variable tenemos simplemente que

$$i(N(x_i)[a_1, \ldots, a_n]) = i(a_i) = M(x_i)[i(a_1), \ldots, i(a_n)].$$

Si $t = c$ es una constante queda

$$i(N(c)[a_1, \ldots, a_n]) = i(N(c)) = M(c) = M(c)[i(a_1), \ldots, i(a_n)].$$

Si $t = ft_1 \cdots t_m$ y el teorema es cierto para $t_1, \ldots, t_m$ entonces

$$\begin{aligned} i(N(t)[a_1, \ldots, a_n]) &= i(N(f)(N(t_1)[a_1, \ldots, a_n], \ldots, N(t_m)[a_1, \ldots, a_n])) \\ &= M(f)(i(N(t_1)[a_1, \ldots, a_n]), \ldots, i(N(t_m)[a_1, \ldots, a_n]) \\ &= M(f)(M(t_1)[i(a_1), \ldots, i(a_n)], \ldots, M(t_m)[i(a_1), \ldots, i(a_n)]) \\ &= M(t)[i(a_1), \ldots, i(a_n)]. \end{aligned}$$

■

Con esto podemos probar que dos modelos isomorfos satisfacen las mismas sentencias:

Teorema 10.19 *Si $i : N \longrightarrow M$ es un isomorfismo entre dos modelos de un mismo lenguaje formal $\mathcal{L}$, $\phi(x_1, \ldots, x_n)$ es una fórmula de $\mathcal{L}$ y $a_1, \ldots, a_n \in N$, entonces*

$$N \vDash \phi[a_1, \ldots, a_n] \text{ syss } M \vDash \phi[i(a_1), \ldots, i(a_n)].$$

DEMOSTRACIÓN: Por inducción sobre la longitud de ϕ. Si $\phi = Rt_1 \cdots t_m$, usamos el teorema anterior:

$$N \vDash \phi[a_1, \ldots, a_n] \text{ syss } N(R)(N(t_1)[a_1, \ldots, a_n], \ldots, N(t_m)[a_1, \ldots, a_n])$$

$$\text{syss } M(R)(i(N(t_1)[a_1, \ldots, a_n]), \ldots, i(N(t_m)[a_1, \ldots, a_n]))$$

$$\text{syss } M(R)(M(t_1)[i(a_1), \ldots, i(a_n)]), \ldots, N(t_m)[i(a_1), \ldots, i(a_n)])$$

$$\text{syss } M \vDash \phi[i(a_1), \ldots, i(a_n)].$$

Si $\phi \equiv \neg\alpha$, entonces, aplicando a α la hipótesis de inducción:

$$N \vDash \phi[a_1, \ldots, a_n] \text{ syss } \neg N \vDash \alpha[a_1, \ldots, a_n] \text{ syss } \neg M \vDash \alpha[i(a_1), \ldots, i(a_n)]$$

$$\text{syss } M \vDash \phi[i(a_1), \ldots, i(a_n)].$$

El caso $\phi = \alpha \to \beta$ es similar. Supongamos por último que $\phi = \bigwedge x\alpha$. Entonces

$$N \vDash \phi[a_1, \ldots, a_n] \text{ syss } \bigwedge a \in N\ N \vDash \alpha[a, a_1, \ldots, a_n]$$

$$\text{syss } \bigwedge a \in N\ M \vDash \alpha[i(a), i(a_1), \ldots, i(a_n)]$$

$$\text{syss } \bigwedge a \in M\ M \vDash \alpha[a, i(a_1), \ldots, i(a_n)] \text{ syss } M \vDash \phi[i(a_1), \ldots, i(a_n)],$$

donde hemos usado que, como i es biyectiva, cuando a recorre N se cumple que $i(a)$ recurre M. ∎

Definición 10.20 Diremos que dos modelos M y N de un mismo lenguaje formal $\mathcal{L}$ son *elementalmente equivalentes* si satisfacen las mismas sentencias, es decir, si para toda sentencia ϕ de $\mathcal{L}$ se cumple que

$$M \vDash \phi \leftrightarrow N \vDash \phi.$$

Usaremos la notación $M \cong N$ para indicar que M y N son isomorfos (es decir, que existe un isomorfismo entre ellos), y la notación $M \equiv N$ para indicar que son elementalmente equivalentes. Acabamos de probar que si $N \cong M$ entonces $N \equiv M$. Pronto veremos ejemplos de que el recíproco no es cierto.

El teorema anterior no es válido para inmersiones arbitrarias, pero hay inmersiones que lo cumplen sin ser isomorfismos:

Definición 10.21 Una *inmersión elemental* $i : N \longrightarrow M$ entre dos modelos de un mismo lenguaje formal $\mathcal{L}$ es una aplicación tal que para toda fórmula $\phi(x_1, \ldots, x_n)$ de $\mathcal{L}$ se cumple

$$\bigwedge a_1 \cdots a_n \in N(N \vDash \phi[a_1, \ldots, a_n] \leftrightarrow M \vDash \phi[i(a_1), \ldots, i(a_n)]).$$

Observemos que esto implica que i es una inmersión. En efecto, para demostrar que conserva a una constante c basta considerar la fórmula $x = c$, para probar que conserva un relator n-ádico R basta considerar la fórmula $Rx_1 \cdots x_n$ y para probar que conserva un funtor n-ádico f basta considerar la fórmula $x = fx_1 \cdots x_n$.

Diremos que N es un *submodelo elemental* de un modelo M (y lo representaremos por $N \prec M$) si $N \subset M$ y la inclusión $i : N \longrightarrow M$ es una inmersión elemental. A su vez esto equivale a que para toda fórmula $\phi(x_1, \ldots, x_n)$ de $\mathcal{L}$ se cumple

$$\bigwedge a_1 \cdots a_n \in N(N \vDash \phi[a_1, \ldots, a_n] \leftrightarrow M \vDash \phi[a_1, \ldots, a_n]).$$

En particular, N es un submodelo de N.

Notemos que si existe una inmersión elemental $i : N \longrightarrow M$ o, en particular, si $N \prec M$, entonces $N \equiv M$.

Ejemplo Consideremos a $\mathbb{R}$ como modelo del lenguaje de la teoría de anillos. Entonces $\mathbb{Q}$ es un submodelo de $\mathbb{R}$, pero no es un submodelo elemental. Por ejemplo, si $\phi(x) = \bigvee y\, x = y \cdot y$ entonces $\mathbb{R} \vDash \phi[2]$ pero $\mathbb{Q} \vDash \neg\phi[2]$. ∎

El teorema siguiente proporciona una caracterización muy importante de los submodelos elementales. Su interés radica en que sólo involucra la noción de satisfacción en un modelo en vez de en dos.

Teorema 10.22 *Un subconjunto $N \subset M$ de un modelo M de un lenguaje formal $\mathcal{L}$ es un submodelo elemental si y sólo si para toda fórmula $\phi(x, x_1, \ldots, x_n)$ de $\mathcal{L}$ se cumple*

$$\bigwedge a_1 \cdots a_n \in N(\bigvee a \in MM \vDash \phi[a, a_1, \ldots, a_n] \to \bigvee a \in NM \vDash \phi[a, a_1, \ldots, a_n]).$$

Demostración: Veamos en primer lugar que N es un submodelo. Si c es una constante de $\mathcal{L}$ entonces $\bigvee a \in MM \vDash (x = c)[a]$, luego por hipótesis $\bigvee a \in NM \vDash (x = c)[a]$, lo que equivale a que $M(c) \in N$.

Similarmente, si f es un funtor n-ádico de $\mathcal{L}$ y $a_1, \ldots, a_n \in N$, entonces es claro que $\bigvee a \in MM \vDash x = fx_1 \cdots x_n[a, a_1, \ldots, a_n]$, luego por hipótesis también se cumple $\bigvee a \in NM \vDash x = fx_1 \cdots x_n[a, a_1, \ldots, a_n]$, lo cual equivale a que $M(f)(a_1, \ldots, a_n) \in N$. Esto prueba que N es ciertamente un submodelo de M, luego la inclusión $i : N \longrightarrow M$ es una inmersión.

Ahora probamos que para toda fórmula $\phi(x_1, \ldots, x_n)$ de $\mathcal{L}$ y todos los $a_1, \ldots, a_n \in N$ se cumple

$$N \vDash \phi[a_1, \ldots, a_n] \leftrightarrow M \vDash \phi[a_1, \ldots, a_n].$$

Lo demostramos por inducción sobre ϕ. Los primeros casos son idénticos a los de la demostración de 10.19 (teniendo en cuenta que aquí podemos omitir la inmersión i, porque es la inclusión). Sólo hay que considerar el caso en que

$\phi = \bigwedge x\alpha$ y que el teorema es válido para α. Por los casos precedentes también vale para $\neg\alpha$. Por consiguiente,

$$N \vDash \bigwedge x\alpha[a_1, \ldots, a_n] \leftrightarrow \bigwedge a \in N N \vDash \alpha[a, a_1, \ldots, a_n]$$

$$\leftrightarrow \neg\bigvee a \in N N \vDash \neg\alpha[a, a_1, \ldots, a_n] \leftrightarrow \neg\bigvee a \in N M \vDash \neg\alpha[a, a_1, \ldots, a_n]$$

$$\leftrightarrow \neg\bigvee a \in M M \vDash \neg\alpha[a, a_1, \ldots, a_n] \leftrightarrow M \vDash \bigwedge x\alpha[a_1, \ldots, a_n].$$

El recíproco es muy simple: si N es un submodelo elemental,

$$\bigvee a \in M\ M \vDash \phi[a, a_1, \ldots, a_n] \to M \vDash \bigvee x\, \phi(x)[a_1, \ldots, a_n]$$

$$\to N \vDash \bigvee x\, \phi(x)[a_1, \ldots, a_n] \to \bigvee a \in N\ N \vDash \phi[a, a_1, \ldots, a_n]$$

$$\to \bigvee a \in N\ M \vDash \phi[a, a_1, \ldots, a_n].$$

■

De aquí podemos obtener una técnica para construir submodelos elementales. Para ello necesitamos algunas definiciones:

Definición 10.23 Sea M un modelo de un lenguaje formal $\mathcal{L}$ y fijemos un orden total en el conjunto de las variables de $\mathcal{L}$. Para cada fórmula $\phi(x_0, \ldots, x_n)$ con $n+1$ variables libres (ordenadas de modo que $x_0 < x_1 < \cdots < x_n$) diremos que una función $h_\phi : M^n \longrightarrow M$ es una *función de Skolem* para ϕ si cuando $a_1, \ldots, a_n \in M$ y $\bigvee a \in M M \vDash \phi[a, a_1, \ldots, a_n]$ entonces

$$M \vDash \phi[h_\phi(a_1, \ldots, a_n), a_1, \ldots, a_n].$$

Claramente (suponiendo AE) toda fórmula ϕ con al menos dos variables libres tiene una función de Skolem, que en general no será única. Seleccionamos una función de Skolem h_ϕ para cada fórmula de $\mathcal{L}$ con al menos dos variables libres.

Si $X \subset M$ definimos $N_0(X) = X$ y $N_{k+1}(X) = N_k(X) \cup \bigcup_\phi h_\phi[N_k(X)]$, donde hay que entender que si la fórmula ϕ tiene $n+1$ variables libres entonces $h_\phi[N_k(X)]$ es en realidad $h_\phi[N_k(X)^n]$. El *núcleo de Skolem* de X en M (respecto a las funciones de Skolem escogidas) es

$$N(X) = \bigcup_{k\in\omega} N_k(X).$$

Teorema 10.24 (AE) *Si M es un modelo de un lenguaje formal $\mathcal{L}$ y $X \subset M$ es un conjunto no vacío, entonces $X \subset N(X) \prec M$ y $|N(X)| = |X| \cdot |\mathcal{L}|$ (donde $|\mathcal{L}|$ es el cardinal del conjunto de signos de $\mathcal{L}$).*

Demostración: Es claro que el cardinal del conjunto de fórmulas de $\mathcal{L}$ (con al menos dos variables libres) es exactamente $|\mathcal{L}|$. Por lo tanto hay $|\mathcal{L}|$ funciones de Skolem. De aquí se sigue fácilmente que $|N(X)| = |X| \cdot |\mathcal{L}|$. Sólo queda probar

que $N(X) \prec M$. Usaremos el teorema anterior. Para ello tomamos una fórmula $\phi(x, x_1, \ldots, x_n)$ junto con $a_1, \ldots, a_n \in N(X)$ y suponemos que

$$\bigvee a \in M M \vDash \phi[a, a_1, \ldots, a_n].$$

No perdemos generalidad si suponemos que $n \geq 1$, pues en caso contrario cambiamos $\phi(x)$ por $\phi(x) \wedge x_1 = x_1$, y tomamos cualquier $a_1 \in N(X)$, así como que las variables están ordenadas respecto del orden prefijado en el conjunto de todas ellas). Existirá un $k \in \omega$ tal que $a_1, \ldots, a_n \in N_k(X)$. Por lo tanto $a = h_\phi(a_1, \ldots, a_n) \in N(X)$ cumple $a \in N(X) \wedge M \vDash \phi[a, a_1, \ldots, a_n]$. ∎

En particular tenemos:

Teorema 10.25 (Teorema descendente de Löwenheim-Skolem) (AE) *Si M es un modelo de un lenguaje formal $\mathcal{L}$ y κ es un cardinal que cumple $|\mathcal{L}| \leq \kappa \leq |M|$, entonces M tiene un submodelo elemental de cardinal κ.*

(Basta tomar $N(X)$, donde $X \subset M$ tiene cardinal κ.)

Combinando esto con el teorema de compacidad obtenemos:

Teorema 10.26 (Teorema ascendente de Löwenheim-Skolem) (AE) *Si M es un modelo infinito de un lenguaje formal $\mathcal{L}$ y $\kappa \geq |M||\mathcal{L}|$ es un cardinal, entonces existe una inmersión elemental de M en un modelo de cardinal κ.*

Demostración: Sea $\mathcal{L}'$ un lenguaje que tenga una nueva constante c_a para cada $a \in M$, sea M' el modelo M extendido a modelo de $\mathcal{L}'$ interpretando cada constante c_a como a. Sea $T' = T(M')$. Sea $\mathcal{L}''$ el lenguaje que resulta de añadir a $\mathcal{L}'$ un conjunto de constantes $\{d_\alpha\}_{\alpha<\kappa}$. sea Γ'' el conjunto formado por las sentencias de T' más todas las de la forma $d_\alpha \neq d_\beta$, para todo par de ordinales $\alpha \neq \beta$.

Entonces Γ'' es finitamente consistente, pues si Δ es un subconjunto finito de Γ'' un modelo de Δ se obtiene extendiendo M' de modo que las constantes d_α que aparezcan en Δ se interpreten como objetos distintos en M', y las que no aparezcan en Δ como un mismo objeto cualquiera de M.

Por el teorema de compacidad existe un modelo M'' de Γ'', en el cual las constantes d_α tienen interpretaciones distintas, luego $|M''| \geq \kappa$. En particular, M'' es un modelo de T'.

Sea $i : M \longrightarrow M''$ la aplicación dada por $i(a) = M''(c_a)$. Claramente es una inmersión elemental, pues

$$M \vDash \phi[a_1, \ldots, a_n] \to M' \vDash \phi(c_{a_1}, \ldots, c_{a_n}) \to M'' \vDash \phi(c_{a_1}, \ldots, c_{a_n})$$
$$\to M'' \vDash \phi[i(a_1), \ldots, i(a_n)].$$

Sea $X \subset M''$ cualquier conjunto de cardinal κ y sea $N = N(i[M] \cup X) \preceq M''$. Entonces $|N| = \kappa$ y se cumple que $i : M \longrightarrow N$. Además es claro que i también es una inmersión elemental en N, pues

$$M \vDash \phi[a_1, \ldots, a_n] \to M'' \vDash \phi[i(a_1), \ldots, i(a_n)] \to N \vDash \phi[i(a_1), \ldots, i(a_n)].$$

∎

Combinando los dos teoremas anteriores vemos que si una teoría tiene un modelo infinito, entonces tiene modelos de todos los cardinales mayores o iguales que el cardinal de su lenguaje formal.

La definición del núcleo de Skolem no es constructiva por la elección arbitraria de las funciones de Skolem. El teorema siguiente nos da una representación de los elementos de un núcleo de Skolem que compensa en parte este inconveniente. Primero necesitamos una definición.

Definición 10.27 Sea M un modelo de un lenguaje formal $\mathcal{L}$. Supongamos escogidas unas funciones de Skolem para M. Sea $\overline{\mathcal{L}}$ el lenguaje formal que resulta de añadirle a $\mathcal{L}$ un funtor F_ϕ por cada función de Skolem h_ϕ. Es claro que M se convierte en un modelo de $\overline{\mathcal{L}}$ sin más que establecer $M(F_\phi) = h_\phi$. Los términos de $\overline{\mathcal{L}}$ construidos únicamente con variables y funtores F_ϕ se llaman *términos de Skolem.*

Teorema 10.28 *Sea M un modelo de un lenguaje formal $\mathcal{L}$ y X un subconjunto no vacío. Entonces*

$$N(X) = \{M(t)[a_1, \ldots, a_n] \mid t \text{ es un término de Skolem} \wedge a_1, \ldots, a_n \in X\}.$$

Demostración: Veamos que $M(t)[a_1, \ldots, a_n] \in N(X)$ por inducción sobre la longitud de t. Si $t = x_i$ es una variable entonces $M(t)[a_1, \ldots, a_n] = a_i \in X$. Si $t = F_\phi t_1 \cdots t_m$, donde cada t_i es un término de Skolem, entonces

$$M(t)[a_1, \ldots, a_n] = h_\phi(M(t_1)[a_1, \ldots, a_n], \ldots, M(t_m)[a_1, \ldots, a_n]).$$

Por hipótesis de inducción cada $M(t_i)[a_1, \ldots, a_n]$ está en $N(X)$, luego todos ellos están en un cierto $N_k(X)$, para un número natural k suficientemente grande, y entonces es claro que $M(t)[a_1, \ldots, a_n] \in N_{k+1}(X)$.

Recíprocamente, vamos a probar por inducción sobre k que cada $N_k(X)$ está contenido en el conjunto del enunciado. Para $k = 0$ es trivial. Si vale para k, tomamos $a \in N_{k+1}(X)$ y distinguimos dos casos: si $a \in N_k(X)$ concluimos por hipótesis de inducción; en caso contrario $a \in h_\phi[N_k(X)]$, para cierta función de Skolem h_ϕ, es decir, existen $b_1, \ldots, b_m \in N_k(X)$ tales que $a = h_\phi(b_1, \ldots, b_m)$. Por hipótesis de inducción $b_i = M(t_i)[a_1, \ldots, a_n]$, para ciertos $a_1, \ldots, a_n \in X$ y ciertos términos de Skolem t_i. Por consiguiente

$$\begin{aligned} a &= M(F_\phi)(M(t_1)[a_1, \ldots, a_n], \ldots, M(t_m)[a_1, \ldots, a_n]) \\ &= M(F_\phi t_1 \cdots t_m)[a_1, \ldots, a_n], \end{aligned}$$

luego se cumple la conclusión con el término de Skolem $t = F_\phi t_1 \cdots t_m$. ∎

Como aplicación demostramos lo siguiente:

Teorema 10.29 *Sea M un modelo de un lenguaje formal $\mathcal{L}$ y X un subconjunto no vacío. Sea $N = N(X)$. Entonces las restricciones a N de las funciones de Skolem de M son funciones de Skolem para N y el núcleo de Skolem de X en N respecto a estas restricciones es N.*

DEMOSTRACIÓN: Si $\phi(x_0, x_1, \ldots, x_n)$ es una fórmula de $\mathcal{L}$ (con una ordenación de sus variables), es claro que $h_\phi|_{N^n} : N^n \longrightarrow N$. Como $N \prec M$, si $a_1, \ldots, a_n \in N$ y

$$\bigvee a \in N N \vDash \phi[a, a_1, \ldots, a_n],$$

también

$$\bigvee a \in M M \vDash \phi[a, a_1, \ldots, a_n],$$

luego

$$M \vDash \phi[h_\phi(a_1, \ldots, a_n), a_1, \ldots, a_n],$$

y de nuevo porque $N \prec N$ concluimos que

$$N \vDash \phi[h_\phi(a_1, \ldots, a_n), a_1, \ldots, a_n].$$

Esto prueba que h_ϕ es una función de Skolem para ϕ en N. Por el teorema anterior, si $a \in N$ entonces $a = M(t)[a_1, \ldots, a_n]$, donde t es un término de Skolem y $a_1, \ldots, a_n \in X$. Ahora bien, es claro que N es un submodelo de M (no necesariamente elemental) cuando consideramos a ambos como modelos de $\overline{\mathcal{L}}$, luego por el teorema 10.18 tenemos que $a = N(t)[a_1, \ldots, a_n]$, luego el teorema anterior nos da que a está en el núcleo de Skolem de X en N. ∎

10.4 Ultraproductos

Presentamos ahora otra técnica de construcción de modelos que proporciona una demostración más natural del teorema de compacidad y, sobre todo, una descripción más útil y manejable de los modelos construidos.

Definición 10.30 Sea $\{M_i\}_{i\in I}$ una familia de modelos de un lenguaje formal $\mathcal{L}$ y sea U un ultrafiltro en I. Definimos en $\prod_{i\in I} M_i$ la relación dada por

$$f =_U g \leftrightarrow \{i \in I \mid f(i) = g(i)\} \in U.$$

Se comprueba sin dificultad que $=_U$ es una relación de equivalencia, por lo que podemos considerar el conjunto cociente, al que llamaremos *ultraproducto* de la familia dada, y lo representaremos por $\prod_{i\in I}^U M_i$.

Definimos en el ultraproducto M la siguiente estructura de modelo de $\mathcal{L}$:

- Si c es una constante de $\mathcal{L}$, definimos $M(c) = [\bar{c}]$, donde $\bar{c} \in \prod_{i\in I} M_i$ es la función dada por $\bar{c}(i) = M_i(c)$.
- Si R es un relator n-ádico de $\mathcal{L}$, entonces

$$M(R)([f_1], \ldots, [f_n]) \leftrightarrow \{i \in I \mid M_i(R)(f_1(i), \ldots, f_n(i))\} \in U.$$

- Si F es un funtor n-ádico de $\mathcal{L}$, entonces $M(F)([f_1], \ldots, [f_n]) = [f]$, donde

$$f(i) = M_i(F)(f_1(i), \ldots, f_n(i)).$$

Se comprueba sin dificultad que estas relaciones y funciones están bien definidas, así como que el igualador se interpreta como la igualdad.

Nota Observemos que si el ultrafiltro U es principal, es decir, si

$$U = \{A \in \mathcal{P}I \mid i_0 \in A\},$$

entonces $[f] = [g] \leftrightarrow f(i_0) = g(i_0)$, por lo que la aplicación $\phi : \prod_{i\in I}^U M_i \longrightarrow M_{i_0}$ dada por $\phi([f]) = f(i_0)$ es biyectiva, y claramente es un isomorfismo de modelos. Por lo tanto en este caso la construcción no aporta nada. ∎

Teorema 10.31 (Teorema fundamental de los ultraproductos) (AE) *Consideremos una familia $\{M_i\}_{i\in I}$ de modelos de un lenguaje formal $\mathcal{L}$ y sea U un ultrafiltro en I. Si $\phi(x_1,\dots,x_n) \in \mathrm{Form}(\mathcal{L})$ y $f_1,\dots,f_n \in \prod_{i\in I} M_i$, entonces*

$$\prod_{i\in I}^U M_i \vDash \phi[[f_1],\dots,[f_n]] \leftrightarrow \{i \in I \mid M_i \vDash \phi[f_1(i),\dots,f_n(i)]\} \in U.$$

En particular, si ϕ es una sentencia,

$$\prod_{i\in I}^U M_i \vDash \phi \leftrightarrow \{i \in I \mid M_i \vDash \phi\} \in U.$$

Demostración: Sea $t(x_1,\dots,x_n)$ un término de $\mathcal{L}$ y $f_1,\dots,f_n \in \prod_{i\in I} M_i$. Veamos que

$$\Big(\prod_{i\in I}^U M_i\Big)(t)[[f_1],\dots,[f_n]] = [g],$$

donde $g(i) = M_i(t)[f_1(i),\dots,f_n(i)]$.

Lo probamos por inducción sobre la longitud de t. Si $t(x_1,\dots,x_n) = x_i$, entonces el miembro izquierdo es $[f_i]$, y $g = f_i$, luego se cumple la igualdad.

Si $t(x_1,\dots,x_n) = c$, donde c es una constante de $\mathcal{L}$, entonces el miembro izquierdo es $[\bar{c}]$ y $g = \bar{c}$, luego se cumple la igualdad.

Si $t(x_1,\dots,x_n) = Ft_1(x_1,\dots,x_n)\cdots t_r(x_1,\dots,x_n)$, donde F es un funtor r-ádico de $\mathcal{L}$, entonces

$$\Big(\prod_{i\in I}^U M_i\Big)(t)[[f_1],\dots,[f_n]]$$

$$= \Big(\prod_{i\in I}^U M_i\Big)(F)\Big(\Big(\prod_{i\in I}^U M_i\Big)(t_1)[[f_1],\dots,[f_n]],\dots,\Big(\prod_{i\in I}^U M_i\Big)(t_r)[[f_1],\dots,[f_n]]\Big)$$

$$= \Big(\prod_{i\in I}^U M_i\Big)(F)([g_1],\dots,[g_r]) = [g],$$

donde $g_j(i) = M_i(t_j)[f_1(i),\dots,f_n(i)]$ (por hipótesis de inducción) y

$$g(i) = M_i(F)(g_1(i),\dots,g_r(i)) = M_i(t)[f_1(i),\dots,f_n(i)].$$

Veamos ahora el teorema por inducción sobre la longitud de ϕ.

Si $\phi(x_1,\dots,x_n) = Rt_1(x_1,\dots,x_n)\cdots t_r(x_1,\dots,x_n)$, donde R es un relator r-ádico de $\mathcal{L}$, entonces

$$\prod_{i\in I}^U M_i \vDash \phi[[f_1],\dots,[f_n]]$$

$$\leftrightarrow \Big(\prod_{i\in I}^U M_i\Big)(R)\Big(\Big(\prod_{i\in I}^U M_i\Big)(t_1)[[f_1],\dots,[f_n]],\dots,\Big(\prod_{i\in I}^U M_i\Big)(t_r)[[f_1],\dots,[f_n]]\Big)$$

$$\leftrightarrow \Big(\prod_{i\in I}^U M_i\Big)(R)([g_1],\dots,[g_r]),$$

donde, según hemos probado, $g_j(i) = M_i(t_j)[f_1(i),\dots,f_n(i)]$. Esto equivale a

$$\{i\in I \mid M_i(R)[g_1(i),\dots,g_r(i)]\}\in U \leftrightarrow \{i\in I \mid M_i\vDash\phi[f_1(i),\dots,f_n(i)]\}\in U.$$

Si $\phi(x_1,\dots,x_n) = \neg\psi(x_1,\dots,x_n)$ y el teorema vale para ψ, entonces

$$\prod_{i\in I}^U M_i \vDash \phi[[f_1],\dots,[f_n]] \leftrightarrow \neg\prod_{i\in I}^U M_i \vDash \psi[[f_1],\dots,[f_n]]$$

$$\leftrightarrow \{i\in I \mid M_i\vDash\psi[f_1(i),\dots,f_n(i)]\}\notin U$$

$$\leftrightarrow \{i\in I \mid M_i\vDash\phi[f_1(i),\dots,f_n(i)]\}\in U.$$

Si $\phi(x_1,\dots,x_n) = \psi(x_1,\dots,x_n)\to\chi(x_1,\dots,x_n)$ y el teorema vale para ψ y χ, probaremos la coimplicación de las negaciones, es decir, que

$$\neg\prod_{i\in I}^U M_i \vDash (\psi\to\chi)[[f_1],\dots,[f_n]]$$

$$\leftrightarrow \{i\in I \mid M_i\vDash(\psi\to\chi)[f_1(i),\dots,f_n(i)]\}\notin U$$

En efecto,

$$\neg\prod_{i\in I}^U M_i \vDash (\psi\to\chi)[[f_1],\dots,[f_n]]$$

$$\leftrightarrow \prod_{i\in I}^U M_i \vDash \psi[[f_1],\dots,[f_n]] \wedge \neg\prod_{i\in I}^U M_i \vDash \chi[[f_1],\dots,[f_n]]$$

$$\leftrightarrow \{i\in I \mid M_i\vDash\psi[f_1(i),\dots,f_n(i)]\}\in U$$

$$\wedge \{i\in I \mid M_i\vDash\neg\chi[f_1(i),\dots,f_n(i)]\}\in U$$

$$\leftrightarrow \{i\in I \mid M_i\vDash\psi[f_1(i),\dots,f_n(i)]\}\cap\{i\in I \mid M_i\vDash\neg\chi[f_1(i),\dots,f_n(i)]\}\in U$$

$$\leftrightarrow \{i\in I \mid \neg M_i\vDash(\psi\to\chi)[f_1(i),\dots,f_n(i)]\}\in U$$

$$\leftrightarrow \{i\in I \mid M_i\vDash(\psi\to\chi)[f_1(i),\dots,f_n(i)]\}\notin U.$$

Si $\phi(x_1,\dots,x_n) = \bigwedge x\psi(x,x_1,\dots,x_n)$ y el teorema vale para ψ, probaremos también la coimplicación de las negaciones:

$$\neg\prod_{i\in I}^U M_i \vDash \bigwedge x\,\psi[[f_1],\dots,[f_n]]$$

$$\leftrightarrow \{i\in I \mid M_i\vDash\bigwedge x\,\psi[f_1(i),\dots,f_n(i)]\}\notin U.$$

En efecto:

$$\neg\prod_{i\in I}^{U} M_i \vDash \bigwedge x\,\psi[[f_1],\dots,[f_n]] \leftrightarrow \bigvee f \in \prod_{i\in I} M_i \neg\prod_{i\in I}^{U} M_i \vDash \psi[[f],[f_1],\dots,[f_n]]$$

$$\leftrightarrow \bigvee f \in \prod_{i\in I} M_i\ \{i\in I \mid M_i \vDash \psi[f(i),f_1(i),\dots,f_n(i)]\} \notin U$$

$$\leftrightarrow \bigvee f \in \prod_{i\in I} M_i\ \{i\in I \mid M_i \vDash \neg\psi[f(i),f_1(i),\dots,f_n(i)]\} \in U. \tag{10.1}$$

Basta probar que esto equivale a

$$\{i\in I \mid M_i \vDash \bigvee x\neg\psi[f_1(i),\dots,f_n(i)]\} \in U, \tag{10.2}$$

pues claramente esto equivale a $\{i\in I \mid M_i \vDash \bigwedge x\psi[f_1(i),\dots,f_n(i)]\} \notin U$.

Si f cumple (10.1), es claro que el conjunto de (10.1) está contenido en el conjunto de (10.2). Como el primero está en U el segundo también. Recíprocamente, si se cumple (10.2), para cada i en el conjunto de (10.2) sea[11] $f(i) \in M_i$ tal que $M_i \vDash \neg\psi[f(i),f_1(i),\dots,f_n(i)]$ y para los demás $i \in I$ tomamos $f(i) \in M_i$ arbitrario. Es claro que f cumple (10.1). ∎

Hay un caso particular del teorema anterior que tiene especial interés:

Definición 10.32 Si M es un modelo de un lenguaje formal $\mathcal{L}$, I es un conjunto y U es un ultrafiltro en I, se define la *ultrapotencia* $\mathrm{Ult}_U(M)$ como el ultraproducto $\prod_{i\in I}^{U} M$, que es también[12] un modelo de $\mathcal{L}$.

Definimos además $j_U : M \longrightarrow \mathrm{Ult}_U(M)$ mediante $j_U(a) = [c_a]$, donde c_a es la función constante dada por $\bigwedge i \in I\ c_a(i) = a$.

Del teorema anterior se sigue inmediatamente:

Teorema 10.33 *Sea M un modelo (que admita un buen orden) de un lenguaje formal $\mathcal{L}$ y U un ultrafiltro en un conjunto I. Entonces $j_U : M \longrightarrow \mathrm{Ult}_U(M)$ es una inmersión elemental.*

Demostración: Si $\phi(x_1,\dots,x_n) \in \mathrm{Form}(\mathcal{L})$ y $a_1,\dots,a_n \in M$, entonces

$$M \vDash \phi[a_1,\dots,a_n] \leftrightarrow \{i\in I \mid M \vDash \phi[c_{a_1}(i),\dots,c_{a_n}(i)]\} \in U$$

$$\leftrightarrow \mathrm{Ult}_U(M) \vDash \phi[j_U(a_1),\dots,j_U(a_n)].$$

∎

Como aplicación del teorema de los ultraproductos demostramos el teorema de compacidad:

[11] Éste es el único punto de la prueba donde se usa AE.

[12] El teorema fundamental restringido a ultrapotencias se cumple sin suponer AE, pues la función f en la parte final de la prueba se puede tomar constante.

Teorema 10.34 (Teorema de compacidad) (AE)[13] *Un conjunto* Γ *de sentencias de un lenguaje formal* $\mathcal{L}$ *es consistente si y sólo si es finitamente consistente.*

DEMOSTRACIÓN: Sea I el conjunto de todos los subconjuntos finitos de Γ. Para cada $\Delta \in I$ sea M_Δ un modelo de $\mathcal{L}$ tal que $M_\Delta \vDash \Delta$ y sea

$$I_\Delta = \{E \in I \mid M_E \vDash \Delta\}.$$

Sea $S = \{I_\Delta \mid \Delta \in I\}$. Claramente S cumple la propiedad de la intersección finita, pues si $\Delta_1, \ldots, \Delta_n \in I$ y $\Delta = \Delta_1 \cup \cdots \cup \Delta_n$, entonces

$$I_\Delta \subset I_{\Delta_1} \cap \cdots \cap I_{\Delta_n},$$

y además $\Delta \in I_\Delta \neq \varnothing$. Por consiguiente S genera un filtro en I, que a su vez está contenido en un ultrafiltro U. Si $\phi \in \Gamma$, entonces

$$\{\Delta \in I \mid M_\Delta \vDash \phi\} = I_{\{\phi\}} \in S \subset U,$$

luego por el teorema fundamental $\prod_{\Delta\in I}^U M_\Delta \vDash \phi$, es decir, $\prod_{\Delta\in I}^U M_\Delta \vDash \Gamma$. ∎

Admitiendo que TU no implica AE (esto puede ser probado), el teorema siguiente tiene como consecuencia que TU no implica el teorema fundamental sobre ultraproductos, ni siquiera su restricción a ultrapotencias.

Teorema 10.35 (TU) *El axioma de elección es equivalente a que, para todo modelo* M *de un lenguaje formal y todo ultrafiltro* U *en un conjunto* I*, la ultrapotencia* $\mathrm{Ult}_U(M)$ *es elementalmente equivalente a* M*.*

DEMOSTRACIÓN: Sea X un conjunto y vamos a probar que tiene una función de elección. Si llamamos $X' = \{a \times \{a\} \mid a \in X\}$, basta encontrar una función de elección en X'. Alternativamente, podemos suponer que los elementos de X son disjuntos dos a dos y disjuntos de X. Tampoco perdemos generalidad si suponemos que todos los elementos de X son no vacíos. Sea $M = X \cup \bigcup X$.

Consideramos un lenguaje formal $\mathcal{L}$ con un relator diádico R y dotamos a M de estructura de modelo de $\mathcal{L}$ interpretando R como la relación $\bar{R}$ tal que $a\,R\,x$ se cumple cuando $a \in x \wedge x \in X$ o bien $a = x \in \bigcup X$.

Supongamos que X no admite una función de elección y sea I el conjunto de los $Y \subset X$ que sí que admiten una función de elección. Obviamente I es un ideal en X (aquí usamos que X no admite una función de elección). Sea $F = I'$ el filtro dual y sea U un ultrafiltro que lo contenga.

Por hipótesis $\mathrm{Ult}_U(M)$ es elementalmente equivalente a M. Claramente

$$M \vDash \bigwedge x \bigvee a\ a\,R\,x,$$

[13] Marcamos la prueba con AE porque esta prueba usa AE, pero ya hemos visto que puede demostrarse suponiendo sólo TU.

luego lo mismo vale en $\mathrm{Ult}_U(M)$. Sea $d : X \longrightarrow X$ la identidad y sea consideremos la clase $[d] \in \mathrm{Ult}_U(M)$. Tenemos que existe una $f : X \longrightarrow M$ tal que $[f]\,\bar{R}\,[d]$, es decir, que

$$\{a \in X \mid f(a)\,\bar{R}\,d(a)\} \in U$$

o, lo que es lo mismo,

$$A = \{a \in X \mid f(a) \in a\} \in U,$$

pero A tiene una función de elección, luego $A \in I \subset U'$, contradicción. ∎

Modelos no estándar de la aritmética de Peano La *aritmética de Peano* (de primer orden) es la teoría formal AP construida sobre el lenguaje $\mathcal{L}_{\mathrm{ap}}$ cuyos signos eventuales son una constante 0, un funtor monádico $'$ y dos funtores diádicos $+$ y $\cdot$, y cuyos axiomas son las sentencias:

$$\begin{array}{ll}
(\mathrm{AP1}) & \bigwedge x\ x' \neq 0 \\
(\mathrm{AP2}) & \bigwedge xy(x' = y' \to x = y) \\
(\mathrm{AP3}) & \bigwedge x\ x + 0 = x \\
(\mathrm{AP4}) & \bigwedge xy(x + y' = (x + y)') \\
(\mathrm{AP5}) & \bigwedge x\ x \cdot 0 = 0 \\
(\mathrm{AP6}) & \bigwedge xy(xy' = xy + x) \\
(\mathrm{AP7}) & \bigwedge x_1 \cdots x_n(\phi(0) \wedge \bigwedge x(\phi(x) \to \phi(x')) \to \bigwedge x\phi(x)),
\end{array}$$

donde ϕ es cualquier fórmula con variables libres $x_1, \ldots, x_n$.

Es inmediato que el conjunto $\mathbb{N}$ de los números naturales es un modelo de AP cuando la constante 0 se interpreta como el número natural cero, el funtor $'$ se interpreta como la función $n \mapsto n+1$ y los funtores $+$ y $\cdot$ se interpretan como la suma y el producto de números naturales.

Para cada $n \in \mathbb{N}$, podemos definir recurrentemente el término $0^{(n)}$ de $\mathcal{L}_{\mathrm{ap}}$ mediante $0^{(0)} = 0$ y $0^{(n+1)} = (0^{(n)})'$, de modo que

$$0^{(0)} = 0, \quad 0^{(1)} = 0', \quad 0^{(2)} = 0'', \quad \ldots$$

Es claro entonces que $\mathbb{N}(0^{(n)}) = n$. Un modelo M de AP se dice *no estándar* si existe un $c \in M$ que no es de la forma $M(0^{(n)})$, para ningún $n \in \mathbb{N}$.

El teorema de compacidad implica la existencia de modelos no estándar de AP, pues basta extender $\mathcal{L}_{\mathrm{ap}}$ con una constante c y considerar el conjunto de sentencias $\Gamma = \mathrm{AP} \cup \{c \neq 0^{(n)} \mid n \in \mathbb{N}\}$, que es finitamente consistente, pues todo subconjunto finito de Γ tiene por modelo a $\mathbb{N}$ sin más que interpretar c como un número natural suficientemente grande, y un modelo de Γ es un modelo no estándar de AP.

Podemos construir un modelo no estándar (relativamente) explícito de AP mediante una ultrapotencia de $\mathbb{N}$: si U es un ultrafiltro no principal en ω, entonces $M = \mathrm{Ult}_U(\mathbb{N})$ es un modelo no estándar de AP, pues un ejemplo de

número natural no estándar es $[d]$, donde $d : \mathbb{N} \longrightarrow \mathbb{N}$ es la identidad. En efecto, para cada $n \in \mathbb{N}$ tenemos que $M(0^{(n)}) = [c_n]$, y como

$$\{i \in \mathbb{N} \mid c_n(i) \neq d(i)\} = \mathbb{N} \setminus \{n\} \in U,$$

concluimos que $M \vDash 0^{(n)} \neq [d]$.

En AP podemos definir la fórmula $x \leq y = \bigvee z\ y = z + x$, de modo que

$$\mathbb{N} \vDash 0^{(m)} \leq 0^{(n)} \quad \text{syss} \quad m \leq n.$$

En la ultrapotencia M se cumple que $M \vDash 0^{(n)} \leq [d]$ para todo $n \in \mathbb{N}$, ya que

$$\{i \in \mathbb{N} \mid \mathbb{N} \vDash c_n(i) \leq d(i)\} = \mathbb{N} \setminus n \in U.$$

Por lo tanto, en M se cumple que $[d]$ es un número natural infinitamente grande. (De hecho, no es difícil probar que en cualquier modelo no estándar de AP los números naturales no estándar son mayores que los números estándar.) ∎

Análisis no estándar Similarmente, si fijamos un ultrafiltro U en $\mathbb{N}$ y definimos $\mathbb{R}^* = \mathrm{Ult}_U(\mathbb{R})$ (considerando a $\mathbb{R}$ como modelo de la teoría de anillos ordenados), obtenemos un cuerpo ordenado elementalmente equivalente a $\mathbb{R}$ que contiene números naturales infinitamente grandes, pero también a sus inversos, que son números reales infinitamente pequeños, o infinitésimos, que se comportan como los infinitésimos que manejaban los analistas de los siglos XVII y XVIII.

Más precisamente, consideramos a $\mathbb{R}$ como modelo del lenguaje $\mathcal{L}_{ao}$ de la teoría de anillos ordenados y, fijado cualquier ultrafiltro U en cualquier conjunto I, llamamos $\mathbb{R}^* = \mathrm{Ult}_U(\mathbb{R})$ y $j : \mathbb{R} \longrightarrow \mathbb{R}^*$ a la inmersión elemental natural.

Las condiciones de la definición de cuerpo ordenado pueden expresarse como fórmulas de $\mathcal{L}_{ao}$, de modo que el hecho de que $\mathbb{R}$ sea un cuerpo ordenado equivale a que es un modelo de la teoría que tiene a dichas fórmulas como axiomas, lo que implica que $\mathbb{R}^*$ también lo es, luego $\mathbb{R}^*$ es un cuerpo ordenado. Además, j es un monomorfismo de cuerpos ordenados, pues

$$[f] = j(\alpha + \beta) \leftrightarrow \{i \in I \mid f(i) = \alpha + \beta\} \in U \leftrightarrow$$

$$\{i \in I \mid \mathbb{R} \vDash (z = x + y)[c_\alpha(i), c_\beta(i), f(i)]\} \in U \leftrightarrow$$

$$\mathbb{R}^* \vDash (z = x + y)[j(\alpha), j(\beta), [f]] \leftrightarrow [f] = j(\alpha) + j(\beta),$$

luego $j(\alpha + \beta) = j(\alpha) + j(\beta)$, e igualmente se prueba que $j(\alpha\beta) = j(\alpha)j(\beta)$, así como que $\alpha \leq \beta \leftrightarrow j(\alpha) \leq j(\beta)$.

A partir de aquí podemos considerar que $\mathbb{R} \subset \mathbb{R}^*$. A los elementos de $\mathbb{R}^*$ los llamaremos *números hiperreales*. Definimos los hiperreales *finitos* como los elementos del conjunto

$$\mathcal{O} = \{\alpha \in \mathbb{R}^* \mid \bigvee M \in \mathbb{R}\ |\alpha| \leq M\}.$$

Es inmediato comprobar que $\mathbb{R} \subset \mathcal{O} \subset \mathbb{R}^*$ es un subanillo ordenado de $\mathbb{R}^*$. Los hiperreales *infinitesimales* son los elementos de

$$o = \{\delta \in \mathbb{R}^* \mid \bigwedge \epsilon > 0 \ |\delta| < \epsilon\}$$

(donde hay que entender que ϵ varía en $\mathbb{R}$, no en $\mathbb{R}^*$).

Es muy sencillo comprobar, a partir de las meras definiciones, que o es un ideal de $\mathcal{O}$, con la propiedad adicional de que si $\alpha \in \mathbb{R}^*$ y $\delta \in o$ cumplen $|\alpha| \leq \delta$, entonces $\delta \in o$.

Vamos a probar que la inmersión natural $\pi : \mathbb{R} \longrightarrow \mathcal{O}/o$ es un isomorfismo de cuerpos. Es inyectiva porque, claramente, el único número real infinitesimal es 0. Tomemos $\alpha \in \mathcal{O}$ y veamos que la clase $[\alpha] \in \mathcal{O}/o$ tiene una antiimagen en $\mathbb{R}$. No perdemos generalidad si suponemos que $\alpha > 0$.

Consideramos el conjunto $S_\alpha = \{r \in \mathbb{R} \mid r < \alpha\}$, que es no vacío y acotado superiormente en $\mathbb{R}$ (porque α es finito, luego existe un $M \in \mathbb{R}$ tal que $\alpha < M$ y M es una cota de S_α). Sea $\hat{\alpha} = \sup S_\alpha \in \mathbb{R}$. Vamos a probar[14] que $\alpha - \hat{\alpha} \in o$, con lo que tendremos que $[\alpha] = \pi(\hat{\alpha})$.

Tomamos $\epsilon > 0$ y supongamos que $|\alpha - \hat{\alpha}| > \epsilon$. Si $\alpha < \hat{\alpha}$, tenemos que $\alpha < \hat{\alpha} - \epsilon < \hat{\alpha}$, luego por definición de supremo tiene que haber un $r \in S_\alpha$ tal que $\alpha < \hat{\alpha} - \epsilon \leq r < \alpha$, contradicción. Si, por el contrario $\hat{\alpha} < \alpha$, entonces $\hat{\alpha} + \epsilon < \alpha$, luego $\hat{\alpha} + \epsilon \in S_\alpha$ y $\hat{\alpha} + \epsilon \leq \hat{\alpha}$, que es otra contradicción. Así pues $|\alpha - \hat{\alpha}| \leq \epsilon$ para todo $\epsilon > 0$, luego $\alpha - \hat{\alpha} \in o$.

Lo que hemos probado es que cada clase de $\mathcal{O}/o$ contiene un único número real. Un enunciado alternativo es el siguiente:

Teorema 10.36 *Sea $\mathbb{R}^*$ una ultrapotencia de $\mathbb{R}$. Para cada número hiperreal finito $\alpha \in \mathcal{O}$ existe un único número real $\operatorname{st}\alpha$ tal que $\alpha - \operatorname{st}\alpha$ es infinitesimal. Además, la aplicación $\operatorname{st} : \mathcal{O} \longrightarrow \mathbb{R}$ es un homomorfismo de anillos ordenados.*

Demostración: La aplicación $\operatorname{st} : \mathcal{O} \longrightarrow \mathcal{O}/o \xrightarrow{\pi^{-1}} \mathbb{R}$ es simplemente la composición de la proyección natural en el cociente con el isomorfismo inverso de π. Sólo falta probar que st conserva el orden.

En efecto, si $\alpha \leq \beta$ son hiperreales finitos, tenemos que

$$\alpha = \operatorname{st}\alpha + \delta, \qquad \beta = \operatorname{st}\beta + \epsilon,$$

con δ, $\epsilon \in o$. Entonces $\operatorname{st}\alpha + \delta \leq \operatorname{st}\beta + \epsilon$, luego si fuera $\operatorname{st}\beta < \operatorname{st}\alpha$ tendríamos que

$$0 < \operatorname{st}\alpha - \operatorname{st}\beta \leq \epsilon - \delta \in o,$$

contradicción, pues un número real positivo no puede ser menor que un infinitésimo, luego $\operatorname{st}\alpha \leq \operatorname{st}\beta$. ∎

El número $\operatorname{st}\alpha$ recibe el nombre de *parte estándar* de α.

[14] Notemos que el supremo se toma en $\mathbb{R}$, por lo que no podemos decir que α sea una cota superior de S_α (en $\mathbb{R}$) y, por consiguiente, no podemos concluir que $\hat{\alpha} \leq \alpha$.

En principio, nada impide que $\mathbb{R}^* = \mathbb{R}$ y que todas las consideraciones precedentes sean triviales. No obstante, basta con que exista un $\alpha \in \mathbb{R}^* \setminus \mathbb{R}$ para que existan infinitésimos no nulos. En efecto, si α es finito, entonces $\alpha - \operatorname{st}\alpha$ es un infinitésimo no nulo, mientras que si α es infinito, es fácil ver que $1/\alpha$ es un infinitésimo no nulo.

Podemos garantizar que $\mathbb{R}^* \neq \mathbb{R}$ tomando $I = \omega$ y un ultrafiltro U en ω no principal. En tal caso $d(n) = n$ determina un hiperreal $\alpha = [d] \in \mathbb{R}^*$ que es infinito, pues, para todo $M \in \mathbb{R}$

$$\{i \in \omega \mid c_M(i) \leq d(i)\} = \omega \setminus \{i \in \omega \mid i < M\} \in U,$$

porque el último conjunto es finito, luego no está en U. Por consiguiente, tenemos que $M = [c_M] \leq [d] = \alpha$ para todo $M \in \mathbb{R}$, luego α es infinito. (Alternativamente, la función $f(i) = 1/(i+1)$ determina un infinitésimo no nulo.)

Observemos que toda función $f : \mathbb{R} \longrightarrow \mathbb{R}$ puede extenderse a $f^* : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ mediante $f^*([h]) = [h \circ f]$. Por ejemplo, si $f(x) = x^2$ y $\alpha = [h]$, tenemos que

$$\{i \in I \mid (h \circ f)(i) = h(i)^2\} = I \in U,$$

luego $f^*(\alpha) = [h \circ f] = [h]^2 = \alpha^2$. En general, cada función definible en $\mathbb{R}^*$ puede extenderse a su "análoga no estándar" en $\mathbb{R}$, y es posible definir o caracterizar los conceptos de límite, derivada, integral, etc. de funciones reales en términos de sus extensiones usando infinitésimos.[15] En realidad, con un uso sistemático de las ultrapotencias es posible abordar en términos infinitesimales todo el cálculo diferencial, incluso en variedades diferenciales o en espacios topológicos arbitrarios.

En B.14 daremos una demostración no estándar de la existencia de subconjuntos de $\mathbb{R}$ no medibles Lebesgue. Aquí vamos a dar una demostración no estándar del teorema de Hahn-Banach [T 11.50], que tiene el interés de que permite sustituir el uso del lema de Zorn por el teorema de los ultrafiltros:

Teorema 10.37 (Hahn-Banach) (TU) *Sea V un espacio vectorial sobre $\mathbb{R}$, sea $p : V \longrightarrow \mathbb{R}$ una aplicación que cumpla*

$$p(v+w) \leq p(v) + p(w), \qquad p(\alpha v) = \alpha p(v)$$

para $\alpha > 0$. Sea $W \subset V$ un subespacio vectorial y $f : W \longrightarrow \mathbb{R}$ un funcional lineal tal que $f(w) \leq p(w)$ para todo $w \in W$. Entonces existe un funcional lineal $\bar{f} : V \longrightarrow \mathbb{R}$ que extiende a f y tal que $\bar{f}(v) \leq p(v)$ para todo $v \in V$.

[15] Por ejemplo, no es difícil demostrar que una función $f : \mathbb{R} \longrightarrow \mathbb{R}$ es derivable en un punto $a \in \mathbb{R}$ si y sólo si, para todo infinitésimo no nulo δ, la expresión

$$f'(a) = \operatorname{st}\frac{f^*(a+\delta) - f^*(a)}{\delta}$$

es independiente de δ. Por ejemplo, para calcular la derivada de la función $f(x) = x^2$ basta observar que

$$f'(x^2) = \operatorname{st}\frac{(x+\delta)^2 - x^2}{\delta} = \operatorname{st}(2x+\delta) = 2x.$$

Como el resultado es independiente de δ, la función es derivable y su derivada es $2x$.

DEMOSTRACIÓN: Llamemos I al conjunto de todos los funcionales lineales $f_1 : W_1 \longrightarrow \mathbb{R}$ definidos en subespacios vectoriales $W \subset W_1 \subset V$ y tales que $f_1(w) \leq p(w)$ para todo $w \in W_1$.

Para cada $v \in V$, llamamos I_v al conjunto de los $f_1 \in I$ tales que $v \in W_1$. En la prueba del teorema [T 11.50] mostramos que todo funcional $f_1 \in$ puede extenderse a otro $f_2 \in I$ que tenga a cualquier vector dado en su dominio. Por lo tanto, la familia $\{I_v \mid v \in V\}$ tiene la propiedad de la intersección finita, luego genera un filtro en I, que por TU puede extenderse a un ultrafiltro U. Llamemos $\mathbb{R}^* = \mathrm{Ult}_U(\mathbb{R})$.

Definimos $f^* : V \longrightarrow \mathbb{R}^*$ como sigue: para cada $v \in V$ y $f_1 \in I$, llamamos $t_v : I \longrightarrow \mathbb{R}$ a la aplicación dada por

$$t_v(h) = \begin{cases} h(v) & \text{si } h \in D_v, \\ 0 & \text{si } h \notin D_v, \end{cases}$$

y llamamos $f^*(v) = [t_v] \in \mathbb{R}^*$. Se trata de una aplicación lineal, pues, dados v_1, $v_2 \in V$ y α, $\beta \in \mathbb{R}$, para todo $h \in I_{v_1} \cap I_{v_2}$ tenemos que

$$t_{\alpha v_1+\beta v_2}(h) = h(\alpha v_1 + \beta v_2) = \alpha h(v_1) + \beta h(v_2) = c_\alpha(h)t_{v_1}(h) + c_\beta(h)t_{v_2}(h)$$

y, como $I_{v_1} \cap I_{v_2} \in U$, se cumple que

$$f^*(\alpha v_1 + \beta v_2) = [t_{\alpha v_1+\beta v_2}] = [c_\alpha][t_{v_1}] + [c_\beta][t_{v_2}] = \alpha f^*(v_1) + \beta f^*(v_2).$$

Si $w \in W$, entonces $\{h \in I \mid t_w(h) = c_{f(w)}(h)\} = I \in U$, luego se cumple que $f^*(w) = f(w)$.

Además, si $v \in V$ y $h \in I_v$, tenemos que $t_h(v) = h(v) \leq p(v) = c_{p(v)}(h)$ y, como $I_v \in U$, concluimos que $f^*(v) = [t_h] \leq [c_{p(v)}] = p(v)$.

En particular, $-f^*(v) = f^*(-v) \leq p(-v)$, luego $-p(-v) \leq f^*(v) \leq p(v)$, y esto prueba que $f^*(v) \in \mathcal{O}$. Por consiguiente, podemos definir $\bar{f}(v) = \mathrm{st}\, f^*(v)$, con lo que tenemos un funcional lineal $\bar{f} : V \longrightarrow \mathbb{R}$ que cumple lo requerido, pues $f^*(v) \leq p(v)$ implica que $\mathrm{st}\, f^*(v) \leq p(v)$. ∎

Puede probarse que el teorema de Hahn-Banach no implica el teorema de los ultrafiltros.

Capítulo XI

El cálculo de particiones

El cálculo de particiones proporciona teoremas de existencia muy generales que pueden aplicarse en los contextos más diversos y a la vez determina afirmaciones indecidibles que pueden usarse en pruebas de consistencia.

Las ideas de este capítulo provienen de la llamada teoría de Ramsey. En su formulación más abstracta afirma que en muchos casos podemos garantizar que una muestra satisface ciertas peculiaridades sin más que exigir que sea lo suficientemente grande. Por ejemplo, para garantizar la "coincidencia" de encontrar dos personas que celebren su cumpleaños el mismo día, basta tomar una muestra de al menos 367 personas. Un ejemplo más sofisticado es el siguiente: en toda muestra de al menos 6 personas, siempre hay tres que se conocen dos a dos o bien tres que no se conocen dos a dos. Esto es un caso particular del teorema siguiente:

Teorema de Ramsey *Para cada natural m existe un número natural n de modo que todo grafo con al menos n vértices posee m vértices conectados dos a dos, o bien m vértices desconectados dos a dos.*

El mínimo n posible se conoce como el *número de Ramsey* de m. El número de Ramsey de 3 es 6, pero en general los números de Ramsey no son fáciles de calcular.

No vamos a probar este teorema porque aquí estamos interesados en versiones análogas que involucran cardinales infinitos.

11.1 Particiones

Vamos a introducir una notación conveniente para formular teoremas de tipo Ramsey:

Definición 11.1 Una *partición* de un conjunto X es una familia $\{X_i\}_{i\in I}$ de subconjuntos de X disjuntos dos a dos tales que $X = \bigcup_{i\in I} X_i$.

Por conveniencia, y en contra de lo habitual, no exigimos que los conjuntos X_i sean no vacíos.

A cada partición $\{X_i\}_{i\in I}$ podemos asociarle una aplicación $F : X \longrightarrow I$ dada por $F(x) = i \leftrightarrow x \in X_i$. Recíprocamente, cada aplicación $F : X \longrightarrow I$ determina una partición $\{F^{-1}[\{i\}]\}_{i\in I}$, de modo que podemos identificar las particiones de X con las aplicaciones de dominio X.

Recordemos que si A es un conjunto y n es un cardinal, podemos considerar el conjunto $[A]^n = \{x \subset A \mid |x| = n\}$. En el caso en que A sea un conjunto de ordinales y $n < \omega$ identificaremos $[A]^n$ con el conjunto

$$\{(\alpha_1, \ldots, \alpha_n) \in A^n \mid \alpha_1 < \cdots < \alpha_n\} \subset A^n.$$

Aunque formalmente no necesitaremos este concepto, podemos definir un *grafo* con vértices en un conjunto A como un subconjunto F de $[A]^2$. Los elementos de F son las *aristas* del grafo. Dos vértices distintos están *conectados* por F si forman una arista. Equivalentemente, podemos definir un grafo como una partición $F : [A]^2 \longrightarrow 2$, de modo que las aristas de F son los pares $\{a, b\}$ tales que $F(\{a, b\}) = 1$. A su vez, una partición $F : [A]^2 \longrightarrow n$ puede verse como un *grafo coloreado,* es decir, un grafo con aristas de color 0, 1, 2, etc.

Si $\{X_i\}_{i\in I}$ es una partición de $[A]^n$, diremos que un subconjunto $H \subset A$ es *homogéneo* para la partición si existe un $i \in I$ tal que $[H]^n \subset X_i$. Si pensamos en la partición como una aplicación F, entonces H es homogéneo si F es constante en $[H]^n$.

En términos de grafos (cuando $n = 2$) un conjunto de vértices H es homogéneo para un grafo (coloreado) si todos sus puntos están conectados dos a dos o bien todos están desconectados dos a dos (resp. todos están conectados por aristas del mismo color).

Por último, si μ, κ, m y n son cardinales, llamaremos

$$\mu \longrightarrow (\kappa)^n_m$$

a la fórmula siguiente:

> *Para toda partición de $[\mu]^n$ en m partes existe un subconjunto homogéneo H de μ con cardinal κ.*

La notación sugiere que μ elementos son suficientes para garantizar un conjunto homogéneo con los requisitos $(\kappa)^n_m$.

Si $m = 1$ la relación $\mu \longrightarrow (\kappa)^n_m$ se cumple trivialmente, luego supondremos siempre que $m \geq 2$. Más aún, para $m = 2$ escribiremos simplemente $\mu \longrightarrow (\kappa)^n$.

Para evitar casos triviales podemos suponer $n \leq \mu$ (o si no $[\mu]^n = \varnothing$), $\kappa \leq \mu$ (pues en caso contrario no puede existir H) y $n \leq \kappa$ (o si no $[H]^n = \varnothing$).

Por ejemplo, en estos términos $6 \longrightarrow (3)^2$ (bastan 6 vértices para que un grafo tenga un subconjunto homogéneo de 3 vértices) y el teorema de Ramsey afirma que si $2 \leq \kappa < \aleph_0$ existe un $\mu < \aleph_0$ tal que $\mu \longrightarrow (\kappa)^2$.

Una primera relación elemental es la siguiente:

Teorema 11.2 *Si $\mu \le \mu'$, $\kappa' \le \kappa$, $m' \le m$ y $n' \le n$ y $\mu \longrightarrow (\kappa)^n_m$, entonces también $\mu' \longrightarrow (\kappa')^{n'}_{m'}$.*

En otras palabras, las relaciones de partición se conservan si se aumenta el cardinal de la izquierda o se reduce cualquiera de los de la derecha.

DEMOSTRACIÓN: Sea $\{X_i\}_{i<m'}$ una partición de $[\mu']^{n'}$. Definimos

$$Y_i = \{(\alpha_1, \dots, \alpha_n) \in [\mu]^n \mid (\alpha_1, \dots, \alpha_{n'}) \in X_i\}, \qquad \text{para } i < m'$$

y sea $Y_i = \varnothing$ si $m' \le i < m$. Es claro que $\{Y_i\}_{i<m}$ es una partición de $[\mu]^n$. Por hipótesis existe un conjunto homogéneo $H \subset \mu$ de cardinal κ. Sea $H' \subset H$ un subconjunto de cardinal κ' (que sigue siendo homogéneo). Quitando a H' un número finito de elementos podemos exigir que no tenga máximo. Sea $i < m$ tal que $[H']^n \subset Y_i$. Necesariamente $i < m'$.

Dado $(\alpha_1, \dots, \alpha_{n'}) \in [H']^{n'}$, tomemos ordinales $\alpha_{n'} < \alpha_{n'+1} < \cdots < \alpha_n$ en H' (existen porque H' no tiene máximo). Así $(\alpha_1, \dots, \alpha_n) \in [H']^n \subset Y_i$, luego $(\alpha_1, \dots, \alpha_{n'}) \in X_i$. Así pues, $[H']^{n'} \subset X_i$, luego H' es homogéneo para la partición dada. ∎

Veamos ahora que no perdemos generalidad al exigir que n sea un cardinal finito:

Teorema 11.3 *Consideremos cardinales tales que $\aleph_0 \le n \le \kappa \le \mu$. Entonces $\mu \not\longrightarrow (\kappa)^n$.*

DEMOSTRACIÓN: Podemos identificar $[\mu]^n$ con el conjunto de las funciones crecientes $f : n \longrightarrow \mu$. Definimos en $[\mu]^n$ la relación de equivalencia dada por

$$f \,R\, g \leftrightarrow \{i \in n \mid f(i) \neq g(i)\} \text{ es finito.}$$

Sea $S \subset [\mu]^n$ un conjunto formado por un elemento de cada clase de equivalencia. Para cada $f \in [\mu]^n$ llamemos $r(f)$ al único elemento de S relacionado con f. Definimos $F : [\mu]^n \longrightarrow 2$ mediante

$$F(f) = \begin{cases} 0 & \text{si } \{i \in n \mid f(i) \neq r(f)(i)\} \text{ tiene cardinal par,} \\ 1 & \text{si } \{i \in n \mid f(i) \neq r(f)(i)\} \text{ tiene cardinal impar.} \end{cases}$$

Si se cumpliera $\mu \longrightarrow (\kappa)^n$ existiría $H \subset \mu$ homogéneo para F. Es claro que podemos construir $f \in [H]^n$ tal que $\bigwedge i \in n \bigvee h \in H\ f(i) < h < f(i+1)$. Digamos que el conjunto $\{i \in n \mid f(i) \neq r(f)(i)\}$ tiene cardinal par. Tomemos $i \in n$ fuera de este conjunto y $h \in H$ tal que $f(i) < h < f(i+1)$. Definimos $g \in [H]^n$ que coincida con f salvo en que $g(i) = h$. Entonces $r(g) = r(f)$, pero el conjunto $\{i \in n \mid g(i) \neq r(g)(i)\}$ tiene cardinal impar, luego $F(f) \neq F(g)$, lo cual contradice la homogeneidad de H. ∎

Los dos teoremas anteriores implican que en realidad $\mu \not\longrightarrow (\kappa)^n_m$ para ningún cardinal $m \ge 2$, por lo que en lo sucesivo supondremos siempre que n es finito. También podemos suponer que $m < \mu$, pues la partición $\{\{x\}\}_{x \in [\mu]^n}$ prueba que $\mu \not\longrightarrow (\kappa)^n_\mu$.

Así pues, en lo sucesivo supondremos siempre que

$$2 \leq n < \aleph_0 \leq \kappa \leq \mu \quad \text{y} \quad 2 \leq m < \mu.$$

La razón para descartar el caso $n = 1$ es la siguiente:

Ejercicio: Probar que si $\kappa \leq \mu$ y $2 \leq m < \mu$, entonces $\mu \longrightarrow (\kappa)^1_m$ si y sólo si $\kappa < \mu$ o bien $\kappa = \mu \wedge m < \operatorname{cf} \mu$.

El primer resultado no trivial sobre particiones es la versión infinita del teorema de Ramsey:

Teorema 11.4 (Teorema de Ramsey) *Si m, $n < \omega$, entonces*

$$\aleph_0 \longrightarrow (\aleph_0)^n_m.$$

Demostración: Por inducción sobre n. Para $n = 1$ es trivial. Supongamos $\aleph_0 \longrightarrow (\aleph_0)^n_m$ y veamos $\aleph_0 \longrightarrow (\aleph_0)^{n+1}_m$. Para ello consideramos una partición $F : [\omega]^{n+1} \longrightarrow m$. Definimos $H_0 = \omega$, $a_0 = 0$ y $F_0 : [H_0 \setminus \{a_0\}]^n \longrightarrow m$ dada por $F_0(x) = F(\{a_0\} \cup x)$. Por hipótesis de inducción existe un conjunto infinito $H_1 \subset H_0 \setminus \{a_0\}$ tal que F_0 es constante en $[H_1]^n$.

Supongamos definidos $a_0 < a_1 < \cdots < a_j \in \omega$ y $H_0 \supset H_1 \supset \cdots \supset H_{j+1}$ infinitos de manera que $a_i \in H_i$ y las particiones $F_i : [H_i \setminus \{a_i\}]^n \longrightarrow m$ dadas por $F_i(x) = F(\{a_i\} \cup x)$ sean constantes en sus respectivos conjuntos $[H_{i+1}]^n$. Entonces tomamos $a_{j+1} \in H_{j+1}$ mayor que a_j y aplicamos la hipótesis de inducción a la partición F_{j+1}, con lo que obtenemos un conjunto infinito $H_{j+2} \subset H_{j+1}$ homogéneo para F_{j+1}.

De este modo obtenemos un conjunto infinito $A = \{a_j \mid j \in \omega\}$. Dado $i \in \omega$, tenemos que $a_j \in H_i$ para todo $j > i$, luego F_i es constante en $[\{a_j \mid j > i\}]^n$. Sea $G(a_i) \in m$ el valor que toma F_i en dicho conjunto. Como G toma un número finito de valores, ha de existir $H \subset A$ infinito donde G sea constante igual a un cierto $k < m$. Así, si $x_1 < \cdots < x_{n+1} \in H$ resulta que

$$F(\{x_1, \ldots, x_{n+1}\}) = F_{x_1}(\{x_2, \ldots, x_{n+1}\}) = G(x_1) = k.$$

Así pues, H es homogéneo para F. ∎

Ante esto, podríamos conjeturar que el cálculo de particiones infinito es trivial, en el sentido de que se vaya a cumplir algo así como $\kappa \longrightarrow (\kappa)^n_m$, para todo cardinal infinito κ. El teorema siguiente muestra que no es así:

Teorema 11.5 *Sea κ un cardinal infinito. Entonces $2^\kappa \not\longrightarrow (\kappa^+)^2$.*

Demostración: Para probar este teorema conviene demostrar antes un resultado general: si $\mu \longrightarrow (\kappa)^2$ entonces todo conjunto totalmente ordenado L de cardinal μ tiene una sucesión $\{x_\alpha\}_{\alpha<\kappa}$ estrictamente creciente o decreciente.

En efecto, basta considerar una enumeración $\{y_\alpha\}_{\alpha<\mu}$ de L y la partición $F : [\mu]^2 \longrightarrow 2$ dada por $F(\alpha, \beta) = 1 \leftrightarrow y_\alpha < y_\beta$ (donde se entiende que $\alpha < \beta$). Si $H \subset \mu$ es un subconjunto homogéneo de cardinal κ, tomando un subconjunto

podemos suponer que tiene ordinal κ, digamos $H = \{\alpha_\beta\}_{\beta<\kappa}$, de modo que $\beta < \gamma \to \alpha_\beta < \alpha_\gamma$. Entonces la sucesión $x_\beta = y_{\alpha_\beta}$ es monótona creciente si F vale 1 sobre $[H]^2$ o monótona decreciente si vale 0.

Según esto, para probar el teorema basta ver que ${}^\kappa 2$ con el orden lexicográfico no admite sucesiones monótonas de longitud κ^+. El orden lexicográfico es el dado por

$$f < g \leftrightarrow f(\alpha) < g(\alpha), \text{ donde } \alpha = \text{mín}\{\beta < \kappa \mid f(\beta) \neq g(\beta)\}.$$

Supongamos que $\{f_\alpha\}_{\alpha<\kappa^+}$ es una sucesión monótona creciente (el caso decreciente es análogo). Sea $\gamma \leq \kappa$ el menor ordinal tal que el conjunto $\{f_\alpha|_\gamma \mid \alpha < \kappa^+\}$ tiene cardinal κ^+. Eliminando de la sucesión original aquellas funciones que al restringirlas a γ coinciden con la restricción de funciones precedentes (y renumerando) podemos suponer que si $\alpha < \beta < \kappa^+$ entonces $f_\alpha|_\gamma \neq f_\beta|_\gamma$.

Para cada $\alpha < \kappa^+$, sea $\delta_\alpha < \gamma$ tal que

$$f_\alpha|_{\delta_\alpha} = f_{\alpha+1}|_{\delta_\alpha}, \qquad f_\alpha(\delta_\alpha) = 0, \qquad f_{\alpha+1}(\delta_\alpha) = 1.$$

Considerando la aplicación $\kappa^+ \longrightarrow \kappa$ dada por $\alpha \mapsto \delta_\alpha$ concluimos que ha de existir un $\delta < \gamma$ tal que el conjunto $\{\alpha < \kappa^+ \mid \delta = \delta_\alpha\}$ tenga cardinal κ^+. Ahora bien, si $\delta_\alpha = \delta_\beta = \delta$ y $f_\alpha|_\delta = f_\beta|_\delta$, entonces $f_\alpha < f_{\beta+1}$ y $f_\beta < f_{\alpha+1}$, luego $f_\alpha = f_\beta$. Por consiguiente, el conjunto $\{f_\alpha|_\delta \mid \alpha < \kappa^+\}$ tiene cardinal κ^+, pero $\delta < \gamma$, lo que contradice la elección de γ. ∎

En particular vemos que $\kappa^+ \not\longrightarrow (\kappa^+)^2$ para todo cardinal infinito κ. No obstante, un refinamiento de la prueba del teorema de Ramsey 11.4 muestra que el teorema de Ramsey finito es válido también para cardinales infinitos, es decir, que dados cardinales κ, m y n tales que $2 \leq m$ y $2 \leq n < \aleph_0 \leq \kappa$, se cumple $\mu \longrightarrow (\kappa)^n_m$ para todo μ suficientemente grande.

Para enunciar adecuadamente este resultado necesitamos la exponencial iterada:

$$\exp_0(\kappa) = \kappa \wedge \bigwedge n \in \omega \ \exp_{n+1}(\kappa) = 2^{\exp_n(\kappa)}.$$

Teorema 11.6 (Erdős-Rado) *Si κ es un cardinal infinito y $n < \omega$, entonces*

$$\exp_n(\kappa)^+ \longrightarrow (\kappa^+)^{n+1}_\kappa.$$

En particular $\beth_n^+ \longrightarrow (\aleph_1)^{n+1}_{\aleph_0}$, y también $(2^\kappa)^+ \longrightarrow (\kappa^+)^2_\kappa$.

Demostración: Razonamos por inducción sobre n. Para $n = 0$ es uno de los casos triviales que ya hemos discutido. Supongamos $\exp_n(\kappa)^+ \longrightarrow (\kappa^+)^{n+1}_\kappa$. Sea $\mu = \exp_{n+1}(\kappa)^+$ y consideremos una partición $f : [\mu]^{n+2} \longrightarrow \kappa$. Para cada $a \in \mu$ sea $F_a : [\mu \setminus \{a\}]^{n+1} \longrightarrow \kappa$ dada por $F_a(x) = F(x \cup \{a\})$.

Veamos que existe un conjunto $A \subset \mu$ tal que $|A| = \exp_{n+1}(\kappa)$ y para todo $C \subset A$ con $|C| \leq \exp_n(\kappa)$ y todo $u \in \mu \setminus C$ existe un $v \in A \setminus C$ tal que F_v y F_u coinciden en $[C]^{n+1}$.

Definimos $A_0 = \exp_{n+1}(\kappa)$, $A_\lambda = \bigcup_{\delta<\lambda} A_\delta$ y, dado $A_\alpha \subset \mu$ con cardinal $\exp_{n+1}(\kappa)$, construimos $A_{\alpha+1}$ tal que $A_\alpha \subset A_{\alpha+1}$, $|A_{\alpha+1}| = \exp_{n+1}(\kappa)$ y para todo subconjunto $C \subset A_\alpha$ con $|C| \leq \exp_n(\kappa)$ y todo $u \in \mu \setminus C$, existe un $v \in A_{\alpha+1} \setminus C$ tal que F_v y F_u coinciden en $[C]^{n+1}$.

Existe tal conjunto porque hay $\exp_{n+1}(\kappa)^{\exp_n(\kappa)} = \exp_{n+1}(\kappa)$ conjuntos C posibles y para cada uno de ellos hay a lo sumo $\kappa^{\exp_n(\kappa)} = 2^{\exp_n(\kappa)} = \exp_{n+1}(\kappa)$ funciones $F_u|_{[C]^{n+1}}$ posibles. Por lo tanto basta añadir $\exp_{n+1}(\kappa)$ elementos a A_α para recorrerlas todas.

El conjunto $A = \bigcup_{\alpha<\exp_{n+1}(\kappa)} A_\alpha$ cumple lo pedido. Notemos que, por el teorema de König, $\operatorname{cf}\exp_{n+1}(\kappa) > \exp_n(\kappa)$, luego todo $C \subset A$ con $|C| \leq \exp_n(\kappa)$ cumple $C \subset A_\alpha$ para cierto $\alpha < \exp_{n+1}(\kappa)$.

Dado $a \in \mu \setminus A$, definimos inductivamente $X = \{x_\alpha \mid \alpha < \exp_n(\kappa)^+\} \subset A$ de manera que para todo $\alpha < \exp_n(\kappa)^+$, la función F_{x_α} coincide con F_a en $[\{x_\beta \mid \beta < \alpha\}]^{n+1}$. Sea $G : [X]^{n+1} \longrightarrow \kappa$ dada por $G(x) = F_a(x)$. Por hipótesis de inducción existe $H \subset X$ tal que $|H| = \kappa^+$ y G es constante en $[H]^{n+1}$.

Si $\alpha_1 < \cdots < \alpha_{n+2} < \exp_n(\kappa)^+$, entonces

$$F(\{x_{\alpha_1}, \ldots, x_{\alpha_{n+2}}\}) = F_{x_{\alpha_{n+2}}}(\{x_{\alpha_1}, \ldots, x_{\alpha_{n+1}}\})$$

$$= F_a(\{x_{\alpha_1}, \ldots, x_{\alpha_{n+1}}\}) = G(\{x_{\alpha_1}, \ldots, x_{\alpha_{n+1}}\}).$$

Por lo tanto F es constante en $[H]^{n+2}$. Las otras afirmaciones del enunciado son los casos particulares $\kappa = \aleph_0$ y $n = 1$. ∎

En particular, si $m < \kappa$ se cumple $\exp_n(\kappa)^+ \longrightarrow (\kappa)^{n+1}_m$, luego ciertamente podemos conseguir conjuntos homogéneos de cualquier cardinal prefijado si el conjunto que partimos tiene suficientes elementos.

El teorema 11.5 muestra que la relación $(2^\kappa)^+ \longrightarrow (\kappa^+)^2_\kappa$ que proporciona el teorema de Erdős-Rado tiene a la izquierda el menor cardinal posible. Puede probarse que esto es cierto en general, es decir, que para un cardinal sucesor κ^+, el menor cardinal μ que cumple $\mu \longrightarrow (\kappa^+)^n$ es precisamente $\mu = \exp_n(\kappa)^+$. Vemos así que el análogo infinito a los números de Ramsey es fácil de calcular para cardinales sucesores. No sucede lo mismo con los cardinales límite, como se verá en la sección siguiente.

Hay otro resultado negativo muy simple que conviene señalar:

Teorema 11.7 *Para todo cardinal infinito κ, se cumple $2^\kappa \not\longrightarrow (3)^2_\kappa$.*

Demostración: Sea $\{f_\alpha\}_{\alpha<2^\kappa}$ una enumeración de ${}^\kappa 2$. Sea $F[2^\kappa]^2 \longrightarrow \kappa$ dada por $F(\alpha,\beta) = \min\{\delta < \kappa \mid f_\alpha(\delta) \neq f_\beta(\delta)\}$. Claramente F no tiene un conjunto homogéneo $\{\alpha,\beta,\gamma\}$, pues si $F(\alpha,\beta) = F(\alpha,\gamma) = F(\beta,\gamma) = \delta$, entonces $f_\alpha(\delta)$, $f_\beta(\delta)$, $f_\gamma(\delta) \in 2$ deberían ser distintos entre sí. ∎

11.2 Cardinales débilmente compactos

Hemos visto que la "conjetura" $\kappa \longrightarrow (\kappa)^2$ es falsa en general. Más concretamente, sabemos que es falsa para todo cardinal sucesor, mientras que el teorema de Ramsey afirma que es cierta para $\aleph_0$. Es natural preguntarse si la cumple algún otro cardinal límite, pero sucede que esto nos lleva a cardinales grandes:

Definición 11.8 Un cardinal no numerable κ es *débilmente compacto* si cumple la relación $\kappa \longrightarrow (\kappa)^2$.

El nombre de "débilmente compacto" proviene de la teoría de modelos, y lo explicaremos dentro de poco. Los cardinales débilmente compactos son grandes. El teorema siguiente es sólo una primera muestra:

Teorema 11.9 *Todo cardinal débilmente compacto es inaccesible.*

DEMOSTRACIÓN: Sea κ un cardinal débilmente compacto. Del teorema 11.5 se sigue que κ es un cardinal límite. Más aún, ha de ser un límite fuerte, pues si existe $\mu < \kappa$ tal que $\kappa \leq 2^\mu$, entonces $2^\mu \not\longrightarrow (\mu^+)^2$, luego también $\kappa \not\longrightarrow (\kappa)^2$.

Falta probar que κ es regular. En caso contrario sea $\mu = \operatorname{cf}\kappa < \kappa$. Sea $\kappa = \bigcup_{\alpha<\mu} A_\alpha$ una partición de κ en conjuntos disjuntos de cardinal menor que κ.

Definimos $F : [\kappa]^2 \longrightarrow 2$ dada por $F(\{\alpha,\beta\}) = 0 \leftrightarrow \bigvee\gamma < \mu\ \{\alpha,\beta\} \subset A_\gamma$.

Por hipótesis existe un conjunto $H \subset \kappa$ homogéneo para F de cardinal κ. Ahora bien, si F toma el valor 0 sobre $[H]^2$ entonces algún A_γ tiene cardinal κ, mientras que si F toma el valor 1 ha de ser $\kappa = \mu$. ∎

A continuación probamos una caracterización muy útil de la compacidad débil en términos de árboles. Recordemos de 9.22 que la HCG implica la existencia de κ-árboles de Aronszajn para todo cardinal κ salvo a lo sumo si κ es inaccesible o el sucesor de un cardinal singular. Si κ es singular y además de la HCG se cumple $\square_\kappa$, entonces también hay κ^+-árboles de Aronszajn (véase la nota tras el teorema 9.16). Finalmente, la existencia de κ-árboles de Aronszajn cuando κ es inaccesible no depende de la función del continuo o del axioma de constructibilidad, sino de la compacidad débil:

Teorema 11.10 *Sea κ un cardinal inaccesible. Las afirmaciones siguientes son equivalentes:*

1. *κ es débilmente compacto.*
2. *No existen κ-árboles de Aronszajn.*
3. *κ cumple $\kappa \longrightarrow (\kappa)^n_m$ para todo $n \in \omega$ y todo cardinal $m < \kappa$.*

DEMOSTRACIÓN: 1) → 2). Supongamos que κ es débilmente compacto y sea $(A, \leq_A)$ un κ-árbol. Como A es la unión de κ niveles de cardinal menor que κ, tenemos que $|A| = \kappa$, luego podemos suponer que $A = \kappa$.

Definimos sobre A el orden total R dado por $\alpha\, R\, \beta$ si y sólo si $\alpha \leq_A \beta$ o bien $\alpha \perp \beta$ y, si δ es el mínimo nivel en que los predecesores de α y β (digamos α' y β') son distintos, se cumple $\alpha' < \beta'$ (como ordinales).

Sea $F : [\kappa]^2 \longrightarrow 2$ dada por $F(\alpha, \beta) = 1$ si y sólo si $\alpha\, R\, \beta$ (donde se entiende que $\alpha < \beta$). Por la compacidad débil existe un conjunto $H \subset \kappa$ de cardinal κ homogéneo para F.

Sea C el conjunto de todos los $\alpha < \kappa$ tales que el conjunto $\{\beta \in H \mid \alpha <_A \beta\}$ tiene cardinal κ. Para cada $\delta < \kappa$ tenemos que

$$H = \bigcup_{\alpha \in \mathrm{Niv}_\delta A} \{\beta \in H \mid \beta \leq_A \alpha\} \cup \bigcup_{\alpha \in \mathrm{Niv}_\delta A} \{\beta \in H \mid \alpha <_A \beta\}.$$

Como κ es regular, la primera unión tiene cardinal menor que κ, luego la segunda tiene que tener cardinal κ y, más concretamente, uno de sus conjuntos ha de tener cardinal κ. Esto significa que C corta a todos los niveles de A. Si probamos que C está totalmente ordenado por $<_A$ concluiremos que C es un camino en A, luego A no será un κ-árbol de Aronszajn.

Supongamos que $\alpha,\ \beta \in C$ no son comparables por $<_A$. Digamos, por ejemplo, que $\alpha\, R\, \beta$. Como ambos tienen κ sucesores en H, existen $\gamma < \delta < \epsilon$ en H tales que $\alpha <_A \gamma$, $\beta <_A \delta$, $\alpha <_A \epsilon$. Por definición de R tenemos que $\gamma\, R\, \delta$ y $\epsilon\, R\, \delta$ (pues el primer nivel en que difieren los anteriores de γ y δ es el mismo en que difieren los anteriores de α y β). Por lo tanto $F(\gamma, \delta) = 1$ y $F(\delta, \epsilon) = 0$, en contra de la homogeneidad de H.

2) $\to$ 3). Veamos $\kappa \longrightarrow (\kappa)^n_m$ por inducción sobre n. Para $n = 1$ la propiedad se se sigue de la regularidad de κ. Supongamos $\kappa \longrightarrow (\kappa)^n_m$ y consideremos una partición $F : [\kappa]^{n+1} \longrightarrow m$. Para cada $\alpha < \kappa$ sea $S_\alpha = \{s \mid s : [\alpha]^n \longrightarrow m\}$ y sea $S = \bigcup_{\alpha<\kappa} S_\alpha$. Claramente S es un árbol con el orden dado por la inclusión. Además el nivel α-ésimo es S_α, de cardinal $m^{|\alpha|} < \kappa$, luego S es un κ-árbol.

Para cada $s \in S$ definimos $h(s) \in \kappa$ y $A(s) \subset \kappa$ de modo que:

1. $A(\varnothing) = \kappa$,
2. $h(s) = \min A(s)$ (salvo si $A(s) = \varnothing$, en cuyo caso $h(s) = 0$),
3. si $s \in S_\lambda$, entonces $A(s) = \bigcap_{\delta<\lambda} A(s|_{[\delta]^n})$,
4. Si $s \in S_\alpha$, $t \in S_{\alpha+1}$, $s \leq t$, entonces

$$A(t) = A(s) \cap \{\gamma > h(s) \mid \textstyle\bigwedge B \in [\alpha+1]^n\ t(B) = F(h(B) \cup \{\gamma\})\},$$

donde $h(B)$ significa $\{h(s|_{[\beta_1]^n}), \ldots, h(s|_{[\beta_n]^n})\}$, con $B = \{\beta_1, \ldots, \beta_n\}$.

Como $A(s)$ es decreciente, es claro que $T = \{s \in S \mid A(s) \neq \varnothing\}$ es un subárbol de S. Veamos que T tiene altura κ, y así será un κ-árbol. Sea $\alpha < \kappa$. Podemos tomar $\gamma < \kappa$ mayor que todos los elementos de $h[S_\beta]$ para $\beta \leq \alpha$. Sea $s_0 = \varnothing \in T$. Obviamente $\gamma \in A(s_0)$. Si $s_\beta \in T$ tiene altura $\beta < \alpha$ y $\gamma \in A(s_\beta)$, podemos extender s_β a $s_{\beta+1} \in S_{\beta+1}$ de acuerdo con la condición 4) para que $\gamma \in A(s_{\beta+1})$ y por lo tanto $s_{\beta+1} \in T$. Definidos $\{s_\delta\}_{\delta<\lambda}$ en T tales que cada s_δ tenga altura δ y $\gamma \in A(s_\delta)$ (y que cada uno extienda a los anteriores), es claro que su unión s_λ cumple $\gamma \in A(s_\lambda)$, luego $s_\lambda \in T$ y tiene altura λ. De este modo llegamos a un $s_\alpha \in T$ de altura α.

Por hipótesis T tiene un camino C, la unión de cuyos elementos es una aplicación $f : [\kappa]^n \longrightarrow m$ tal que $\bigwedge \alpha < \kappa\ f|_{[\alpha]^n} \in T$, luego

$$\bigwedge \alpha < \kappa\ h(f|_{[\alpha]^n}) \in A(f|_{[\alpha]^n}).$$

Sea $\alpha_1 < \cdots < \alpha_{n+1} < \kappa$. Sea $B = \{\alpha_1 + 1, \ldots, \alpha_n + 1\} \in [\alpha_{n+1} + 1]^n$. Como $h(f|_{[\alpha_{n+1}+1]^n}) \in A(f|_{[\alpha_{n+1}+1]^n})$, por la condición d) se cumple que

$$f(\{\alpha_1 + 1, \ldots, \alpha_n + 1\}) = F(\{h(f|_{[\alpha_1+1]^n}), \ldots, h(f|_{[\alpha_n+1]^n}), h(f|_{[\alpha_{n+1}+1]^n})\}).$$

En otros términos, si llamamos $X = \{h(f|_{[\alpha+1]^n}) \mid \alpha < \kappa\}$, acabamos de probar que si tomamos $\alpha_1 < \cdots < \alpha_{n+1}$ en X, entonces $F(\{\alpha_1, \ldots, \alpha_{n+1}\})$ no depende de α_{n+1}, luego podemos definir una partición $G : [X]^n \longrightarrow m$ mediante $G(\{\alpha_1, \ldots, \alpha_n\}) = F(\{\alpha_1, \ldots, \alpha_{n+1}\})$, donde α_{n+1} es cualquier elemento de X mayor que $\alpha_1, \ldots, \alpha_n$. Por hipótesis de inducción G tiene un conjunto homogéneo H de cardinal κ (notemos que $|X| = \kappa$), el cual es obviamente homogéneo para F.

3) $\to$ 1) es trivial. ∎

Vamos a usar este teorema para probar que los cardinales débilmente compactos son más que inaccesibles. Necesitamos un resultado técnico:

Teorema 11.11 *Sea E un conjunto de cardinales infinitos tal que para todo cardinal regular μ, el conjunto $E \cap \mu$ no es estacionario en μ. Entonces existe $g : E \longrightarrow \Omega$ inyectiva tal que $\bigwedge \nu \in E\ g(\nu) < \nu$.*

Demostración: Razonamos por inducción sobre $\kappa = \sup E$. Si $\kappa = \aleph_0$, entonces $E = \{\aleph_0\}$ y la conclusión es trivial.

Si $\kappa = \xi^+$, entonces $\xi^+ \in E$. Si llamamos $E' = E \setminus \{\xi^+\} \subset \xi + 1$, para todo cardinal regular μ, se cumple que $E' \cap \mu$ no es estacionario en μ, luego por hipótesis de inducción existe $g' : E' \longrightarrow \xi$ inyectiva tal que $\bigwedge \nu \in E'\ g'(\nu) < \nu$. Basta extender g' a una función g tal que $\xi < g(\xi^+) < \xi^+$.

Supongamos ahora que $\kappa > \aleph_0$ es un cardinal límite y sea $\xi = \operatorname{cf} \kappa$. Sea $\{\mu_\alpha\}_{\alpha<\xi}$ una sucesión cofinal y normal formada por cardinales infinitos. Si $\xi < \kappa$ podemos exigir además que $\xi < \mu_0$, mientras que si κ es regular, por hipótesis $E \cap \kappa = E$ no es estacionario en κ, luego podemos tomar como $\{\mu_\alpha\}_{\alpha<\xi}$ la enumeración de un c.n.a. en κ que no corte a E, es decir, que podemos exigir que $\bigwedge \alpha < \xi\ \mu_\alpha \notin E$.

Observamos ahora que $E_\alpha = E \cap \mu_\alpha$ cumple la hipótesis del enunciado, luego por hipótesis de inducción existe $g_\alpha : E \cap \mu_\alpha \longrightarrow \mu_\alpha$ inyectiva tal que $\bigwedge \nu \in E \cap \mu_\alpha\ g_\alpha(\nu) < \nu$. Definimos $g : E \longrightarrow \kappa$ mediante

$$g(\nu) = \begin{cases} g_0(\nu) + 1 & \text{si } \nu < \mu_0, \\ \mu_\alpha + g_{\alpha+1}(\nu) & \text{si } \mu_\alpha < \nu < \mu_{\alpha+1}, \\ \omega \cdot \alpha & \text{si } \nu = \mu_\alpha. \end{cases}$$

Observemos que si $\xi < \kappa$, entonces en el tercer caso tenemos que $\alpha < \xi < \mu_0$, luego $\omega \cdot \alpha < \mu_0 \leq \nu$, y además es un ordinal límite, luego no puede coincidir con $g(\nu)$ para $\nu < \mu_0$, que está definido como un ordinal sucesor. En el caso en que $\xi = \kappa$ el tercer caso no puede darse, porque $\nu \in E$ y $\mu_\alpha \notin E$. Teniendo esto en cuenta, es fácil ver que g cumple lo requerido. ∎

Teorema 11.12 *Si κ es un cardinal débilmente compacto y $E \subset \kappa$ es estacionario, entonces existe un cardinal regular $\mu < \kappa$ tal que $E \cap \mu$ es estacionario en μ.*

DEMOSTRACIÓN: Como κ es un cardinal límite, los cardinales infinitos menores que κ forman un conjunto c.n.a. en κ, luego podemos suponer que E consta únicamente de cardinales infinitos. Consideramos la semejanza $f : \kappa \longrightarrow E$ y sea

$$A = \{s \in {}^{<\kappa}\kappa \mid s \text{ es inyectiva} \wedge \bigwedge \alpha < \ell(s)\ s(\alpha) < f(\alpha)\}.$$

Claramente A es un árbol con el orden dado por la inclusión. Si para todo cardinal regular $\mu < \kappa$ se cumple que $E \cap \mu$ no es estacionario en μ, entonces $E \cap \mu$ cumple las hipótesis del teorema anterior, luego existe $g_\mu : E \cap \mu \longrightarrow \mu$ inyectiva tal que $\bigwedge \nu \in E \cap \mu\ g_\mu(\nu) < \nu$, luego $f \circ g_\mu \in A$ tiene altura μ. Por lo tanto, A es un κ-árbol (notemos que los niveles tienen cardinal menor que κ porque κ es inaccesible).

Como κ es fuertemente compacto, A no puede ser un κ-árbol de Aronszajn, luego tiene un camino, el cual determina una aplicación inyectiva $g : \kappa \longrightarrow \kappa$ tal que $\bigwedge \alpha < \kappa\ g(\alpha) < f(\alpha)$, pero entonces $h = f^{-1} \circ g : E \longrightarrow \kappa$ sería regresiva e inyectiva, en contradicción con 6.15. ∎

Teorema 11.13 *Todo cadinal débilmente compacto es ω-Mahlo.*

DEMOSTRACIÓN: El conjunto $C_0 \subset \kappa$ formado por los cardinales límite fuerte menores que κ es c.n.a. en κ, luego si $C \subset \kappa$ es cualquier c.n.a., el teorema anterior nos da que existe un cardinal regular $\mu < \kappa$ tal que $\mu \cap C \cap C_0$ es estacionario en μ, luego $\mu \in C \cap C_0$, luego μ es fuertemente inaccesible, y hemos probado que $\{\mu < \kappa \mid \mu \text{ es fuertemente inaccesible}\}$ es estacionario en κ, es decir, que κ es un cardinal de Mahlo.

En general, si κ es $\alpha + 1$-Mahlo, es decir, si el conjunto

$$E = \{\mu < \kappa \mid \mu \text{ es } \alpha\text{-Mahlo}\}$$

es estacionario en κ, para cada c.n.a. $C \subset \kappa$ tenemos que $C \cap E$ también es estacionario luego existe $\mu < \kappa$ regular tal que $\mu \cap E \cap C$ es estacionario en μ, luego $\mu \in C$ y μ es $\alpha + 1$-Mahlo, luego κ es $\alpha + 2$-Mahlo. Esto implica obviamente que κ es ω-Mahlo. ∎

En realidad puede probar que que un cardinal débilmente compacto κ es de hecho κ-Mahlo y, más aún, que el conjunto $\{\mu < \kappa \mid \mu \text{ es } \mu\text{-Mahlo}\}$ es estacionario en κ.

Fórmulas de longitud infinita Los resultados siguientes explican el nombre de "cardinales débilmente compactos". Para ello definimos fórmulas de longitud infinita en un lenguaje formal.

Definición 11.14 Sea $\mathcal{L}$ un lenguaje formal y sean κ, μ dos cardinales infinitos. Definimos como sigue las fórmulas de $\mathcal{L}$ de tipo (κ, μ):

$$\begin{aligned}
F(0) &= \{Rt_0\cdots t_{n-1} \mid 0<n<\omega \wedge R\in \mathrm{Rel}_n\mathcal{L} \wedge \{t_i\}_{i<n}\in(\mathrm{Term}\,\mathcal{L})^n\},\\
F(\alpha+1) &= F(\alpha)\cup\{(\neg,\phi)\mid \phi\in F(\alpha)\}\\
&\quad \cup\{(\textstyle\bigwedge,\{\phi_\delta\}_{\delta<\beta})\mid \beta<\kappa\wedge\{\phi_\delta\}_{\delta<\beta}\in F(\alpha)^\beta\}\\
&\quad \cup\{(\textstyle\bigwedge,\{x_\delta\}_{\delta<\beta},\phi)\mid \beta<\mu\wedge\{x_\delta\}_{\delta<\beta}\in(\mathrm{Var}\,\mathcal{L})^\beta\wedge\phi\in F(\alpha)\},\\
F(\lambda) &= \bigcup_{\delta<\lambda} F(\delta),
\end{aligned}$$

$$\mathrm{Form}_{\kappa\mu}(\mathcal{L}) = \bigcup_{\alpha<\kappa^+\cup\mu^+} F(\alpha).$$

En la práctica usaremos la notación siguiente:

Escribiremos	$\neg\phi$	en lugar de	$(\neg,\phi)$,
"	$\bigwedge\limits_{\delta<\beta}\phi_\delta$	"	$(\bigwedge,\{\phi_\delta\}_{\delta<\beta})$,
"	$\bigvee\limits_{\delta<\beta}\phi_\delta$	"	$\neg\bigwedge\limits_{\delta<\beta}\neg\phi_\delta$,
"	$\bigwedge\limits_{\delta<\beta}x_\delta\ \phi$	"	$(\bigwedge,\{x_\delta\}_{\delta<\beta},\phi)$,
"	$\bigvee\limits_{\delta<\beta}x_\delta\ \phi$	"	$\neg\bigvee\limits_{\delta<\beta}x_\delta\ \neg\phi$,
"	$\phi\wedge\psi$	"	$\bigwedge\limits_{\delta<2}\{(0,\phi),(1,\psi)\}$,
"	$\phi\vee\psi$	"	$\bigvee\limits_{\delta<2}\{(0,\phi),(1,\psi)\}$,

y de aquí definimos $\phi\to\psi$ como $\neg\phi\vee\psi$, etc.

En definitiva, las fórmulas de tipo (κ,μ) de $\mathcal{L}$ son formalmente como las fórmulas usuales salvo por que admitimos conjunciones (y, por consiguiente, disyunciones) infinitas sobre menos de κ fórmulas y cuantificaciones infinitas sobre menos de μ variables. Notemos que técnicamente estamos usando el mismo signo como conjuntor infinito y como cuantificador infinito, pero la estructura de cada fórmula determina cuándo hay que considerarlo como conjuntor y cuándo como cuantificador.

De la definición se sigue que toda fórmula de tipo (κ,μ) es elemental (o sea, un relator y términos) o bien es una negación, o una implicación, o una conjunción o una generalización.

Los conceptos de "variable libre", "variable ligada", sentencia, etc. se definen de forma obvia para fórmulas de tipo (κ,μ). Por razones técnicas no hemos definido las fórmulas como sucesiones de signos, sino como pares o ternas, por lo que no tiene sentido hablar de la longitud de una fórmula (podría definirse de todos modos, pero no lo vamos a necesitar). No obstante, la inducción o recursión sobre la longitud de una fórmula se sustituye por inducción o recursión sobre el rango, y el resultado es formalmente el mismo.

Por ejemplo, si M es un modelo de $\mathcal{L}$, $v:\mathrm{Var}(\mathcal{L})\longrightarrow M$ y ϕ es una fórmula de tipo (κ,μ), podemos definir $M\vDash\phi[v]$ de forma natural. Las únicas condiciones

que difieren respecto a la definición usual son:

$$\begin{aligned} M \vDash \bigwedge_{\delta<\beta} \phi_\delta[v] &\leftrightarrow \bigwedge \delta < \beta\ M \vDash \phi_\delta[v], \\ M \vDash \bigwedge_{\delta<\beta} x_\delta\, \phi[v] &\leftrightarrow \text{para toda } w : \mathrm{Var}(\mathcal{L}) \longrightarrow M \text{ que coincida con } v \text{ sobre} \\ &\quad \text{las variables de } \mathcal{L} \text{ distintas de las } x_\delta \text{ se cumple} \\ &\quad M \vDash \phi[w]. \end{aligned}$$

A su vez, de aquí se deducen propiedades análogas para las disyunciones y las particularizaciones infinitas. Concretamente:

$$\begin{aligned} M \vDash \bigvee_{\delta<\beta} \phi_\delta[v] &\leftrightarrow \bigvee \delta < \beta\ M \vDash \phi_\delta[v], \\ M \vDash \bigvee_{\delta<\beta} x_\delta\, \phi[v] &\leftrightarrow \text{existe } w : \mathrm{Var}(\mathcal{L}) \longrightarrow M \text{ que coincide con } v \text{ sobre las} \\ &\quad \text{variables de } \mathcal{L} \text{ distintas de las } x_\delta \text{ y } M \vDash \phi[w]. \end{aligned}$$

Podemos identificar las fórmulas usuales (finitas) de $\mathcal{L}$ con las fórmulas de tipo $(\aleph_0, \aleph_0)$. No hay una biyección natural entre ellas, pero a cualquier fórmula finita le podemos asociar de forma natural una fórmula de tipo $(\aleph_0, \aleph_0)$ con el mismo significado y viceversa.

Admitiremos expresiones de la forma $\bigwedge_{i\in I} \phi_i$, con $|I| < \kappa$, aunque en la definición hemos exigido que las conjunciones estén subindicadas con ordinales. Para ello identificaremos esta fórmula con la construida a partir de una biyección $i : |I| \longrightarrow I$, es decir, con $\bigwedge_{\delta<|I|} \phi_{i_\delta}$. Esta fórmula depende de la biyección escogida, pero su interpretación en un modelo es la misma en cualquier caso. (En la definición no podíamos admitir conjuntos de índices arbitrarios porque entonces la clase de las fórmulas no sería un conjunto). Similarmente admitiremos generalizaciones con conjuntos de índices arbitrarios (de cardinal menor que μ).

En la práctica es más cómodo hablar de lenguajes de tipo (κ, μ) que de fórmulas de tipo (κ, μ). Cuando digamos que $\mathcal{L}$ es un lenguaje formal de tipo (κ, μ) querremos decir que es un lenguaje formal en el sentido usual, pero que al hablar de fórmulas de $\mathcal{L}$ habrá que entender que son fórmulas de tipo (κ, μ).

Recordemos que el teorema de compacidad (para la lógica usual, finita) afirma que si Σ es un conjunto de sentencias tal que todo subconjunto finito tiene un modelo, entonces Σ tiene un modelo.

Diremos que un lenguaje $\mathcal{L}$ de tipo (κ, μ) cumple el *teorema de compacidad (débil)* si para todo conjunto de sentencias Σ (con $|\Sigma| \le \kappa$) tal que todo $S \subset \Sigma$ con $|S| < \kappa$ tiene un modelo, se cumple que Σ tiene un modelo.

A pesar de los términos que estamos empleando, debemos tener presente que el "teorema de compacidad (débil)" es una propiedad que puede satisfacer o no un lenguaje formal, es decir, que no es realmente un teorema.

Teorema 11.15 *Sea κ un cardinal fuertemente inaccesible. Las afirmaciones siguientes son equivalentes:*

1. *κ es débilmente compacto.*
2. *Todo lenguaje formal de tipo (κ,κ) cumple el teorema de compacidad débil.*
3. *Todo lenguaje formal de tipo $(\kappa,\aleph_0)$ cumple el teorema de compacidad débil.*

DEMOSTRACIÓN: 1) $\to$ 2). Sea Σ un conjunto de sentencias de un lenguaje $\mathcal{L}$ de tipo (κ,κ) tal que $|\Sigma|\le\kappa$ y todo $S\subset\Sigma$ con $|S|<\kappa$ tiene un modelo. Podemos suponer que $|\mathcal{L}|\le\kappa$, pues sólo importan los signos que de hecho aparecen en las sentencias de Σ. Si encontramos un modelo de Σ para el lenguaje formado por dichos signos, los demás signos de $\mathcal{L}$ pueden interpretarse arbitrariamente.

Sea $\mathcal{L}^1$ el lenguaje formal que resulta de añadir a $\mathcal{L}$ una sucesión de constantes $\{c^\phi_\alpha\}_{\alpha<\beta}$ para cada fórmula ϕ de $\mathcal{L}$ con variables libres $\{x_\alpha\}_{\alpha<\beta}$. Con estas nuevas constantes se pueden construir nuevas fórmulas de $\mathcal{L}^1$, lo que nos permite definir del mismo modo un lenguaje $\mathcal{L}^2$, y así sucesivamente. Llamamos $\mathcal{L}^\infty$ al lenguaje formado por todos los signos de todos los lenguajes $\mathcal{L}^n$, con $n<\omega$. De este modo, cada fórmula ϕ de $\mathcal{L}^\infty$ tiene asociada una sucesión de constantes $\{c^\phi_\alpha\}_{\alpha<\beta}$ en correspondencia con sus variables libres y que no aparecen en ϕ.

Llamaremos $\tilde\phi$ a la sentencia que resulta de sustituir cada variable libre de ϕ por su constante asociada. Por otra parte, llamaremos ϕ' a la sentencia

$$\bigvee_{\delta<\beta} x_\delta\,\phi\to\tilde\phi.$$

Es inmediato que $|\mathcal{L}^\infty|\le\kappa$ y como κ es inaccesible se cumple también que $|\mathrm{Form}(\mathcal{L}^\infty)|\le\kappa$. Llamemos $\Sigma'=\Sigma\cup\{\phi'\mid\phi\in\mathrm{Form}(\mathcal{L}^\infty)\}$. Si $S\subset\Sigma'$ cumple $|S|<\kappa$, entonces S tiene un modelo, pues un modelo de $S\cap\Sigma$ para $\mathcal{L}$ se extiende a un modelo de S sin más que interpretar adecuadamente las constantes añadidas.

Sea $\{\sigma_\alpha\}_{\alpha<\kappa}$ una enumeración de las sentencias de $\mathcal{L}^\infty$. Sea A el conjunto formado por todas las aplicaciones $s:\gamma\longrightarrow 2$ tales que $\gamma<\kappa$ y existe un modelo M de $\Sigma'\cap\{\sigma_\alpha\mid\alpha<\gamma\}$ de modo que

$$\bigwedge\alpha<\gamma(s(\alpha)=1\leftrightarrow M\vDash\sigma_\alpha). \tag{11.1}$$

Claramente A es un árbol con la inclusión. La altura de un elemento de A es su dominio, y por la propiedad de Σ' resulta que A tiene altura κ. Al ser κ inaccesible, los niveles tienen cardinal menor que κ, luego A es un κ-árbol.

Como estamos suponiendo que κ es débilmente compacto, A tiene un camino, cuyos elementos determinan una aplicación $s:\kappa\longrightarrow 2$ con la propiedad de que $\bigwedge\gamma<\kappa\, s|_\gamma\in A$.

Sea $\Delta=\{\sigma_\alpha\mid\alpha<\kappa\wedge s(\alpha)=1\}$. Por construcción $\Sigma'\subset\Delta$, luego basta encontrar un modelo para Δ.

Sea U el conjunto de todos los designadores de $\mathcal{L}^\infty$. Definimos en U la relación dada por $t_1\,R\,t_2$ si y sólo si $(t_1=t_2)\in\Delta$.

Veamos que R es una relación de equivalencia. Probaremos la simetría, pues la reflexividad y la transitividad se demuestran análogamente.

Dados t_1, $t_2 \in U$, sea $\gamma < \kappa$ suficientemente grande como para que las sentencias $t_1 = t_2$ y $t_2 = t_1$ estén en $\{\sigma_\alpha \mid \alpha < \gamma\}$. Supongamos que $t_1\, R\, t_2$, es decir, que $(t_1 = t_2) \in \Delta$. Como $s|_\gamma \in A$, existe un modelo M que cumple (11.1). Por definición de Δ tenemos que $M \vDash t_1 = t_2$, luego $M \vDash t_2 = t_1$, luego $(t_2 = t_1) \in \Delta$, es decir, $t_2\, R\, t_1$.

Sea N el modelo de $\mathcal{L}^\infty$ cuyo universo es el cociente U/R y donde los signos de $\mathcal{L}^\infty$ se interpretan como sigue:

$N(c) = [c]$, para toda constante c de $\mathcal{L}^\infty$,

$N(f)([t_1], \ldots, [t_n]) = [ft_1 \cdots t_n]$, para todo funtor n-ádico f de $\mathcal{L}^\infty$,

$N(R)([t_1], \ldots, [t_n]) \leftrightarrow Rt_1 \cdots t_n \in \Delta$, para todo relator n-ádico R de $\mathcal{L}^\infty$.

Veamos que N está bien definido. Por ejemplo, probemos que las interpretaciones de los funtores son funciones bien definidas (el caso de los relatores es análogo).

Sea f un funtor n-ádico de $\mathcal{L}^\infty$ y sean $t_1, \ldots, t_n, t'_1, \ldots, t'_n \in U$ tales que $[t_i] = [t'_i]$ para $i = 1, \ldots, n$. Sea $\gamma < \kappa$ suficientemente grande como para que las sentencias $t_i = t'_i$ y $ft_1 \cdots t_n = ft'_1 \cdots t'_n$ estén en $\{\sigma_\alpha \mid \alpha < \gamma\}$.

Como $s|_\gamma \in A$, existe un modelo M de $\mathcal{L}^\infty$ que cumple (11.1). Por definición de Δ tenemos que $M \vDash t_i = t'_i$, para $i = 1, \ldots, n$, luego también se cumple que $M \vDash ft_1 \cdots t_n = ft'_1 \cdots t'_n$, con lo que esta sentencia está en Δ y por consiguiente $[ft_1 \cdots t_n] = [ft'_1 \cdots t'_n]$.

Para que N esté bien definido también hemos de comprobar que la interpretación del igualador es la igualdad, pero esto es inmediato.

Una simple inducción sobre la longitud de t (los términos son sucesiones finitas de signos, y tienen definida su longitud) prueba que si t es un designador de $\mathcal{L}^\infty$ entonces $N(t) = [t]$. Ahora basta probar que para toda sentencia σ de $\mathcal{L}^\infty$ se cumple

$$N \vDash \sigma \leftrightarrow \sigma \in \Delta.$$

Lo probamos por inducción sobre el mínimo α tal que $\sigma \in F(\alpha)$ en la definición 11.14. Para las sentencias de la forma $Rt_1 \cdots t_n$ es inmediato, por la definición de $N(R)$.

Supongámoslo para σ y veámoslo para $\neg\sigma$. Sea $\gamma < \kappa$ suficientemente grande como para que σ y $\neg\sigma$ estén en $\{\sigma_\alpha \mid \alpha < \gamma\}$. Sea M un modelo de $\mathcal{L}^\infty$ que cumpla (11.1). Entonces

$$N \vDash \neg\sigma \leftrightarrow \neg N \vDash \sigma \leftrightarrow \sigma \notin \Delta \leftrightarrow \neg M \vDash \sigma \leftrightarrow M \vDash \neg\sigma \leftrightarrow \neg\sigma \in \Delta.$$

Supongamos ahora que $\sigma = \bigwedge_{\delta<\beta} \phi_\delta$. Sea $\gamma < \kappa$ suficientemente grande como para que σ y todas las sentencias ϕ_δ estén en $\{\sigma_\alpha \mid \alpha < \gamma\}$. Sea M un modelo de $\mathcal{L}^\infty$ que cumpla (11.1).

Así, por la hipótesis de inducción para las ϕ_δ,

$$N \vDash \sigma \leftrightarrow \bigwedge \delta < \beta\, N \vDash \phi_\delta \leftrightarrow \bigwedge \delta < \beta\, \phi_\delta \in \Delta$$

$$\leftrightarrow \bigwedge \beta < \delta\, M \vDash \phi_\delta \leftrightarrow M \vDash \sigma \leftrightarrow \sigma \in \Delta.$$

Supongamos ahora que $\sigma = \bigwedge\limits_{\delta<\beta} x_\delta\ \phi$. Si $\neg N \vDash \sigma$, teniendo en cuenta quién es el universo de N, esto significa que existen designadores de $\mathcal{L}^\infty$ tales que $\neg N \vDash \phi^*$, donde ϕ^* es la sentencia que resulta de sustituir las variables x_δ en ϕ por tales designadores. La sentencia ϕ^* se construye en los mismos pasos que ϕ, luego en menos pasos que σ, luego podemos aplicarle la hipótesis de inducción y concluir que $\phi^* \notin \Delta$.

Sea $\gamma < \kappa$ suficientemente grande como para que las sentencias ϕ^* y σ estén en $\{\sigma_\alpha \mid \alpha < \gamma\}$. Sea M un modelo de $\mathcal{L}^\infty$ que cumpla (11.1). Entonces $\neg M \vDash \phi^*$, luego $\neg M \vDash \sigma$, luego $\sigma \notin \Delta$.

Supongamos ahora $\sigma \notin \Delta$ y sea $\gamma < \kappa$ suficientemente grande como para que las sentencias σ, $\tilde\phi$ y $\phi' = \bigvee\limits_{\delta<\beta} x_\delta\ \phi \to \tilde\phi$ estén en $\{\sigma_\alpha \mid \alpha < \gamma\}$. Sea M un modelo de $\mathcal{L}^\infty$ que cumpla (11.1). Entonces $\neg M \vDash \sigma$, luego $M \vDash \bigvee\limits_{\delta<\beta} x_\delta\ \phi$. Por otra parte, como $\phi' \in \Sigma' \cap \{\sigma_\alpha \mid \alpha < \gamma\}$, tenemos que $M \vDash \phi'$, de donde llegamos a que $M \vDash \tilde\phi$, y en consecuencia $\tilde\phi \in \Delta$.

Ahora bien, $\tilde\phi$ se construye en los mismos pasos que ϕ, luego en uno menos que σ, luego podemos aplicarle la hipótesis de inducción y concluir que $N \vDash \tilde\phi$, de donde claramente $\neg N \vDash \sigma$.

2) $\to$ 3) es evidente.

3) $\to$ 1). Veamos que no hay κ-árboles de Aronszajn. Sea A un κ-árbol y sea $\mathcal{L}$ un lenguaje formal con un relator diádico R, un relator monádico T y κ constantes $\{c_a\}_{a\in A}$. Sea Σ el siguiente conjunto de sentencias $(\kappa, \aleph_0)$ de $\mathcal{L}$:

$c_x\, R\, c_y$	para cada x, $y \in A$ tales que $x \le y$,
$\neg c_x\, R\, c_y$	para cada x, $y \in A$ tales que $x \not\le y$,
$\neg(Tc_x \wedge Tc_y)$	para cada x, $y \in A$ tales que $x \perp y$,
$\bigvee\limits_{x\in \mathrm{Niv}_\alpha(A)} Tc_x$	para todo $\alpha < \kappa$.

Es claro que $|\Sigma| = \kappa$ y si $S \subset \Sigma$ cumple $|S| < \kappa$, entonces S tiene como modelo a $M = A$ con $M(c_x) = x$, $M(R) = \le_A$ y tomando como $M(T)$ la pertenencia a una cadena de altura suficientemente grande como para que cumpla todas las fórmulas del cuarto tipo que haya en S.

Por hipótesis Σ tiene un modelo M, del cual obtenemos un camino en A, a saber, $C = \{x \in A \mid M \vDash Tc_x\}$. ∎

Los cardinales regulares no numerables que cumplen el teorema de compacidad (fuerte) se llaman (fuertemente) compactos, pero no vamos a estudiarlos aquí.

De la prueba del teorema anterior se desprende que un cardinal inaccesible κ es débilmente compacto si y sólo si el árbol $2^{<\kappa}$ no contiene κ-subárboles de

Aronszajn, pues en la prueba de 1) $\to$ 2) sólo se ha usado que un cierto subárbol de $2^{<\kappa}$ tenía un camino.

Apéndice A

Bases de espacios vectoriales

Este apéndice consta de tres secciones: en la primera demostramos que todo espacio vectorial tiene una base, que es un ejemplo típico de aplicación del lema de Zorn, junto con algunos resultados relacionados, como el hecho de que todas las bases de un espacio vectorial tienen el mismo cardinal, que es una aplicación típica de la aritmética cardinal; en la segunda sección probamos que, recíprocamente, la existencia de bases implica el axioma de elección y, finalmente, en la tercera sección probamos un resultado no trivial sobre la dimensión del espacio dual de un espacio vectorial.

A.1 Existencia y equicardinalidad de bases

Definición A.1 Si K es un cuerpo, un *espacio vectorial* sobre K es una terna $(V, +, \cdot)$, donde $+ : V \times V \longrightarrow V$ es una ley de composición interna en V y $\cdot : K \times V \longrightarrow V$ es lo que se denomina una *ley de composición externa*, de modo que se cumplan las propiedades siguientes:

1. $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$,
2. $v_1 + v_2 = v_2 + v_1$,
3. Existe un elemento $0 \in V$ tal que $v + 0 = v$ para todo $v \in V$,
4. Para todo $v \in V$ existe $-v \in V$ tal que $v + (-v) = 0$,
5. $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$,
6. $(\alpha + \beta)v = \alpha v + \beta v$,
7. $\alpha(\beta v) = (\alpha\beta)v$,
8. $1 \cdot v = v$,

donde v, v_1, etc. son vectores arbitrarios (elementos de V) y α, β, etc. son escalares arbitrarios (elementos de K).

La estructura de espacio vectorial, que definimos a continuación, es otra de las estructuras algebraicas fundamentales, junto con la de anillo o la de cuerpo:

De la definición se siguen fácilmente propiedades adicionales, como que el vector 0 es único, que $0 \cdot v = 0$, $\alpha \cdot 0 = 0$ y, más aún, que $\alpha v = 0$ si y sólo si $\alpha = 0$ o $v = 0$, y que $-v = (-1) \cdot v$.

Ejemplo Si K es un cuerpo e I es un conjunto arbitrario, el conjunto K^I adquiere estructura de K-espacio vectorial con las operaciones definidas puntualmente, es decir,

$$(f + g)(v) = f(v) + g(v), \qquad (\alpha f)(v) = \alpha f(v).$$

■

Un *subespacio vectorial* W de un K-espacio vectorial V es un subconjunto que cumple:

1. $0 \in W$.
2. Si w_1, $w_2 \in W$, $w_1 + w_2 \in W$.
3. Si $w \in W$ y $\alpha \in K$, $\alpha w \in W$.

De aquí se sigue inmediatamente que W admite una estructura de espacio vectorial con las restricciones de las operaciones de V. Siempre consideraremos a los subespacios vectoriales como espacios vectoriales con dicha estructura.

Es fácil ver que la intersección de cualquier familia de subespacios vectoriales de V es un subespacio vectorial de V. Esto justifica la definición siguiente:

Si V es un K-espacio vectorial y $X \subset V$, se llama *subespacio generado* por X a la intersección de todos los subespacios vectoriales de V que contienen a X. Se representa por $\langle X \rangle$. Si $V = \langle X \rangle$ se dice que X es un *sistema generador* de V.

Teorema A.2 *Si V es un K-espacio vectorial y $X \subset V$, el subespacio $\langle X \rangle$ está formado por todos los vectores de la forma $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ con $v_1, \ldots, v_n \in X$ y $\alpha_1, \ldots, \alpha_n \in K$.*

Demostración: Si llamamos W al conjunto formado por todos los vectores de la forma indicada, es inmediato que se trata de un subespacio vectorial de V que contiene a X, luego $\langle X \rangle \subset W$, pero, como $\langle X \rangle$ es un subespacio vectorial de V que contiene a X, es claro que también tiene que contener a todos los elementos de W, luego $W = \langle X \rangle$. ■

Definición A.3 Si V es un K-espacio vectorial, un conjunto $X \subset V$ es *linealmente independiente* si cuando $v_1, \ldots, v_n$ son elementos de X distintos dos a dos y $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$, para ciertos escalares $\alpha_i \in K$, entonces todos los α_i son necesariamente nulos. Una *base* de un espacio vectorial V es un sistema generador linealmente independiente.

Notemos que, por definición, $\varnothing$ es linealmente independiente y $\langle\varnothing\rangle = \{0\}$, por lo que $\varnothing$ es trivialmente una base del espacio vectorial nulo. También es claro que todo subconjunto de un conjunto linealmente independiente es linealmente independiente.

Teorema A.4 *Si B es una base de un Kespacio vectorial V, entonces todo vector $v \in V$ se expresa de forma única como combinación lineal de elementos de B.*

DEMOSTRACIÓN: Como B es un sistema generador, todo $v \in V$ se expresa como combinación lineal de elementos de B. Si admitiera dos expresiones distintas, completándolas con términos con coeficientes nulos, podríamos obtener dos expresiones de la forma

$$v = \alpha_1 v_1 + \cdots \alpha_n v_n = \beta_1 v_1 + \cdots + \beta_n v_n,$$

para ciertos vectores $v_1, \ldots, v_n \in B$ distintos dos a dos y con $\alpha_i \neq \beta_i$ para algún índice i. Sin embargo, esto es imposible, pues entonces tenemos que $(\alpha_1 - \beta_1)v_1 + \cdots + (\alpha_n - \beta_n)v_n = 0$ con algún coeficiente no nulo, en contra de la definición de independencia lineal. ∎

Con esto ya podemos probar los dos resultados fundamentales sobre bases en espacios vectoriales:

Teorema A.5 (Teorema de existencia de base) *Sea V un espacio vectorial, sean $A \subset X \subset V$ de modo que A es linealmente independiente y X es un sistema generador de V. Entonces existe una base de V tal que $A \subset B \subset V$.*

DEMOSTRACIÓN: Por el lema de Zorn, la familia de todos los subconjuntos $A \subset Y \subset X$ linealmente independientes tiene un elemento B maximal respecto de la inclusión. Basta probar que B es una base de V. Como es linealmente independiente, si no fuera base no sería un sistema generador. A su vez, esto implica que $X \not\subset B$, pues es inmediato que todo conjunto que contiene un sistema generador es generador.

Sea, pues, $v \in X \setminus \langle B\rangle$, pero entonces $B \cup \{v\}$ es linealmente independiente y contradice la maximalidad de B. En efecto, si $\alpha v + \alpha_1 v_1 + \cdots \alpha_n v_n = 0$, con $v_1, \ldots, v_n \in B$ con algún coeficiente no nulo, tiene que ser $\alpha \neq 0$ (ya que en caso contrario B no sería linealmente independiente), y entonces podemos despejar v de la ecuación anterior para concluir que $v \in \langle B\rangle$, contradicción. ∎

Teorema A.6 (Teorema de equicardinalidad de bases) *Todas las bases de un mismo espacio vectorial tienen el mismo cardinal.*

DEMOSTRACIÓN: Sea V un espacio vectorial y supongamos en primer lugar que V tiene una base finita. Entonces podemos tomar una base $B = \langle v_1, \ldots, v_n\rangle$ del menor cardinal posible. Podemos suponer que $n \geq 1$, pues si V tiene por base al conjunto vacío es que $V = 0$ y la conclusión es trivial.

Sea B' cualquier otra base (en principio, tal vez infinita). Dado $v'_1 \in B'$, podemos expresar

$$v'_1 = \alpha_1 v_1 + \cdots + \alpha_n v_n,$$

para ciertos escalares α_j. No pueden ser todos nulos, pues una base no puede contener el vector nulo (en tal caso $1 \cdot 0 = 0$ contradiría la definición de independencia lineal). Sin pérdida de generalidad, podemos suponer que $\alpha_1 \neq 0$. En tal caso

$$v_1 = -(1/\alpha_1)v'_1 - \alpha_2/\alpha_1 v_2 - \cdots - \alpha_n/\alpha_1 v_n.$$

Por consiguiente, si llamamos $B_1 = \{v'_1, v_2, \ldots, v_n\}$, tenemos que $v_1 \in \langle B_1\rangle$, luego $B \subset \langle B_1\rangle$, luego $V = \langle B\rangle \subset \langle B_1\rangle$, luego $\langle B_1\rangle = V$. Así pues, B_1 es un sistema generador, luego contiene una base, pero como el cardinal n de B es el menor posible, y B_1 tiene (a lo sumo) n vectores, de hecho tiene que tener exactamente n vectores y es ya una base.

Si $n > 1$, tomamos otro vector $v'_2 \in B'$ distinto de v'_1 (tiene que haberlo, porque B' tiene que tener al menos n vectores). Expresamos de nuevo

$$v'_2 = \alpha_1 v'_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n,$$

No puede ser que $\alpha_2 = \cdots = \alpha_n = 0$, pues entonces $\alpha_1 v'_1 - v'_2 = 0$ contradiría la independencia lineal de B'. Sin pérdida de generalidad podemos suponer que $\alpha_2 \neq 0$, y el mismo razonamiento anterior nos da que $B_2 = \{v'_1, v'_2, v_3, \ldots, v_n\}$ es una base de V.

Repitiendo el proceso n veces llegamos a una base $B_n \subset B'$ con n vectores. Pero entonces $B_n = B'$, pues si hubiera un vector $v' \in B' \setminus B_n$, tendría que poder expresarse como combinación lineal de los vectores de B_n, y ello contradiría la independencia lineal de B'. Así pues, B' tiene también n vectores.

Supongamos ahora que V no tiene bases finitas y sean B y B' dos bases cualesquiera de V. Cada $v \in B$ se expresa de forma única como combinación lineal $x = \alpha_1 w_1 + \cdots + \alpha_n w_n$, donde los escalares son no nulos y $w_1, \ldots, w_n \in B'$. Por lo tanto, tenemos definida una aplicación $f : B \longrightarrow [B']^{<\aleph_0}$ determinada por la relación $f(v) = \{w_1, \ldots, w_n\}$.

Así, para todo $v \in B$, se cumple que $x \in \langle f(x)\rangle$. Equivalentemente, tenemos que si $A \in [B']^{<\aleph_0}$ y $x \in B$ cumple que $f(x) = A$, entonces $x \in \langle A\rangle$, luego $f^{-1}[\{A\}] \subset \langle A\rangle$.

Ahora bien, A es una base finita de $\langle A\rangle$, y por la parte ya probada todas las bases de $\langle A\rangle$ son finitas, y todos los conjuntos linealmente independientes también, pues cada uno de ellos está contenido en una base. Puesto que $f^{-1}[\{A\}] \subset B$ es linealmente independiente, es finito.

Por otra parte, $X = \bigcup_{A \in [B']^{<\aleph_0}} f^{-1}[\{A\}]$, luego

$$|B| \leq \sum_{A \in [B']^{<\aleph_0}} |f^{-1}[\{A\}] \leq \sum_{A \in [B']^{<\aleph_0}} \aleph_0 = |B'|^{<\aleph_0} = |B'|,$$

e igualmente se cumple que $|B'| \leq |B|$, luego $|B| = |B'|$. ∎

Definición A.7 Si V es un K-espacio vectorial, se llama *dimensión* de V al cardinal de cualquier base de V y se representa por $\dim V$.

Por ejemplo, es fácil ver que $\dim K^n = n$, para todo $n \in \omega$, pues una base de K^n es la *base canónica,* $e_1, \ldots, e_n$ dada por

$$e_{ij} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Si V es un K-espacio vectorial de dimensión finita, es claro que

$$|V| = |K|^{\dim V},$$

pues cada elemento de V se expresa de forma única como combinación lineal de los $\dim V$ vectores de una base, luego está unívocamente determinado por los $\dim V$ coeficientes de la combinación lineal. Para espacios de dimensión infinita tenemos el teorema siguiente:

Teorema A.8 *Si V es un K-espacio vectorial de dimensión infinita, entonces*

$$|V| = |K| \dim V.$$

Demostración: Si B es una base de V, tenemos que $\dim V = |B| \leq |V|$. Por otra parte, si $v \in V$ no es nulo, la aplicación $K \longrightarrow V$ dada por $\alpha \mapsto \alpha v$ es inyectiva, luego $|K| \leq |V|$ y, como la dimensión de V es infinita, concluimos que $|K| \dim V \leq |V|$.

Ahora consideramos la aplicación $f : V \longrightarrow \bigcup_{n\in\omega} (K^n \times B^n)$ que a cada $v \in V$ le asigna un par $((\alpha_1, \ldots, \alpha_n), (v_1, \ldots, v_n))$ tal que $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ con los α_i no nulos (dicho par es único salvo por el orden de $v_1, \ldots, v_n$, entendiendo además que $f(0) = (\varnothing, \varnothing)$). Claramente f es inyectiva, luego

$$|V| \leq \sum_{n\in\omega} |K|^n |B|^n = |K|^{<\aleph_0} \dim V = |K| \dim V,$$

donde en la última igualdad hay que distinguir si el cuerpo K es finito o infinito. ∎

A.2 Equivalencia con el axioma de elección

En esta sección probaremos que la afirmación *"Todo espacio vectorial tiene una base"* es equivalente al axioma de elección. Para ello supondremos que el lector conoce algunos resultados algebraicos que van más allá de los demostrados en este libro.[1]

[1] Las referencias [A] remiten a mi libro de Álgebra.

Si k es un cuerpo y X es un conjunto arbitrario, podemos considerar [A 2.28] el anillo $k[X]$ de los polinomios con indeterminadas en X y coeficientes en k. Cada $p \in k[X]$ se expresa de forma única [A 2.34] en la forma

$$p = \sum_{i=1}^{n} a_i x_1^{k_1} \cdots x_n^{k_{in}},$$

donde las indeterminadas $x_1, \ldots, x_n \in X$ son distintas dos a dos y las n-tuplas de naturales $(k_{i1}, \ldots, k_{in})$ son también distintas dos a dos. Además $k[X]$ es un dominio íntegro [A 2.41]. Esto nos permite considerar a su vez el cuerpo de cocientes $k(X)$, cuyos elementos son fracciones p/q de polinomios, con $q \neq 0$.

Según [A 2.42], las unidades de $k[X]$ son los elementos de k, es decir, los polinomios constantes. El teorema de Gauss [A 3.28] nos asegura que $k[X]$ es un dominio de factorización única, es decir, que todo polinomio $p \in k[X]$ se descompone de forma única en factores primos, los cuales están determinados salvo producto por una constante.

Esto implica que todo elemento de $k(X)$ admite una expresión en fracción irreducible p/q, en el sentido de que p y q no tienen factores primos comunes, lo cual hace que estén unívocamente determinados salvo producto por constantes.

De cara a probar el axioma de elección, partimos de una familia de conjuntos no vacíos $\{X_i\}_{i\in I}$, que podemos suponer disjuntos dos a dos (en caso contrario los cambiamos por $X_i \times \{i\}$). Sea $X = \bigcup_{i\in I} X_i$.

Fijamos un cuerpo cualquiera k y consideramos el cuerpo $k(X)$. Para cada monomio

$$m = a x_1^{k_1} \cdots x_n^{k_n} \in k[X],$$

definimos su grado i-ésimo como $\operatorname{grad}_i(m) = \sum_{x_j \in X_i} k_j$, es decir, como la suma de los exponentes de todas las indeterminadas de X_i que aparecen en m.

Diremos que un polinomio $p \in k[X]$ es i-homogéneo de grado n si todos sus monomios cumplen $\operatorname{grad}_i(m) = n$.

Ahora observamos lo siguiente:

Si p, $q \in k[X]$, el producto pq es i-homogéneo si y sólo si los factores p y q son i-homogéneos, y en tal caso $\operatorname{grad}_i(pq) = \operatorname{grad}_i(p) + \operatorname{grad}_i(q)$.

Para probarlo observamos en primer lugar que es inmediato que si p y q son i-homogéneos, entonces pq también lo es y $\operatorname{grad}_i(pq) = \operatorname{grad}_i(p) + \operatorname{grad}_i(q)$ (se prueba primero para monomios, y de ahí se sigue para polinomios homogéneos cualesquiera). Por otra parte, todo polinomio $p \in k[X]$ se descompone de forma única como

$$p = p_{n_1} + \cdots + p_{n_r},$$

donde cada p_{n_j} es i-homogéneo de grado n_j y $n_1 < \cdots < n_r$. Sólo hay que agrupar todos los monomios con el mismo grado de i-homogeneidad. El polinomio p será homogéneo si y sólo si $r = 1$.

Descomponemos igualmente $q = q_{m_1} + \cdots + q_{m_s}$, y observamos que

$$pq = \sum_{u,v} p_{n_u} q_{m_v},$$

donde $\mathrm{grad}_i(p_{n_u} q_{m_v}) = n_u + m_v$, por lo que el término de menor grado en la descomposición de pq en sumandos homogéneos es $p_{n_1} q_{m_1}$, mientras que el de mayor grado es $p_{n_r} q_{m_s}$. Por lo tanto, el producto pq será homogéneo si y sólo si $n_1 + m_1 = n_r + m_s$, si y sólo si $n_1 = n_r$ y $m_1 = m_s$ (porque $n_1 \leq n_r$ y $m_1 \leq m_s$), si y sólo si p y q son i-homogéneos.

Como consecuencia, los factores primos de un polinomio i-homogéneo son i-homogéneos y, a su vez, esto se traduce en que si $f \in k(X)$ es cociente de polinomios i-homogéneos, en su expresión como fracción irreducible el numerador y el denominador son i-homogéneos.

Si p, $q \in k[X]$ son polinomios i-homogéneos, podamos definir

$$\mathrm{grad}_i(p/q) = \mathrm{grad}_i(p) - \mathrm{grad}_i(q),$$

y este grado está bien definido sin que importe la expresión de $f = p/q$ como cociente de polinomios i-homogéneos, pues si $f = p/q = p'/q'$, entonces $pq' = qp'$ y al tomar grados en ambos miembros llegamos a que

$$\mathrm{grad}_i(p) - \mathrm{grad}_i(q) = \mathrm{grad}_i(p') - \mathrm{grad}_i(q').$$

Llamamos K al conjunto de los $f \in k(X)$ que, para todo $i \in I$, se expresan como cociente de polinomios i-homogéneos y $\mathrm{grad}_i(f) = 0$.

Se comprueba inmediatamente que K es un subcuerpo de $k(X)$, lo que nos permite considerar a $k(X)$ como K-espacio vectorial. Llamamos $V \subset k(X)$ al K-espacio vectorial generado por X. Por hipótesis, podemos tomar una K-base B de V.

Si $i \in I$ y $x \in X_i$, podemos expresar

$$x = \sum_{b \in B(x)} a_b(x) \cdot b,$$

donde $B(x) \subset B$ es un conjunto finito y $0 \neq a_b(x) \in K$. Aquí es crucial que la unicidad de la expresión de un vector como combinación lineal de los vectores de una base implica que tanto $B(x)$ como $\{a_b(x)\}_{b \in B(x)}$ están unívocamente determinados por x, es decir, que no hemos usado el axioma de elección para justificar su existencia.

Ahora bien, si $y \in X_i$, tenemos que

$$y = \sum_{b \in B(x)} \tfrac{y}{x}\, a_b(x) \cdot b,$$

y el cociente y/x está en K, pues es i-homogéneo de grado 0 y trivialmente también es j-homogéneo para cualquier $j \neq i$. La unicidad de la expresión nos

da que $B(y) = B(x)$ y que $a_b(y) = (y/x)a_b(x)$. Equivalentemente, tenemos que el conjunto finito $B_i = B(x)$ es independiente de la elección de $x \in X_i$, al igual que los coeficientes $a_{ib} = a_b(x)/x$.

Ahora observamos que $a_{ib} \in k(X)$ es i-homogéneo de grado -1, lo cual significa que en el denominador de cualquier expresión en forma de fracción tienen que aparecer necesariamente variables de X_i. Llamamos $A(b,i) \subset X_i$ al conjunto (finito) de las variables de X_i que aparecen en el denominador de la expresión irreducible de a_{ib} como cociente de polinomios i-homogéneos. Notemos que $A(b,i)$ está unívocamente determinado por b, i, sin depender de ninguna elección arbitraria.

Para eliminar la dependencia de b definimos $F(i) = \bigcup_{b\in B_i} A(b,i)$, que sigue siendo un subconjunto finito no vacío de X_i.

En resumen, bajo la hipótesis de que todo espacio vectorial tiene una base, hemos demostrado lo siguiente:

> **Principio de elección múltiple** *Si A es una familia de conjuntos no vacíos, existe una función $f : A \longrightarrow [\bigcup A]^{<\omega}$ tal que, para todo $x \in A$, se cumple que $\varnothing \neq f(x) \subset x$.*

En otras palabras, que si tenemos una familia de conjuntos no vacíos, podemos seleccionar un subconjunto finito no vacío de cada uno de ellos.

De aquí se deduce a su vez que si X es un conjunto totalmente ordenado, entonces existe una función de elección en $\mathcal{P}X$.

En efecto, tenemos una función de elección múltiple $f : \mathcal{P}X \setminus \{\varnothing\} \longrightarrow [X]^{<\omega}$ y, como todo conjunto finito totalmente ordenado está bien ordenado, para cada $A \in \mathcal{P}X \setminus \{\varnothing\}$, podemos definir $g(A) = \min f(A) \in A$.

De aquí se sigue a su vez que todo conjunto totalmente ordenado puede biyectarse con un ordinal y, por consiguiente, puede ser bien ordenado.

En efecto, basta observar que en la prueba de la implicación 1) $\Rightarrow$ 2) del teorema 4.28, para ver que un conjunto X es biyectable con un ordinal, sólo se usa una función de elección en $\mathcal{P}X$.

A su vez, esto implica que, para todo ordinal α, el conjunto $\mathcal{P}\alpha$ puede ser bien ordenado, ya que tenemos una biyección natural $\mathcal{P}\alpha \longrightarrow {}^{\alpha}2$ y el conjunto ${}^{\alpha}2$ está totalmente ordenado por la relación según la cual $u < v$ si y sólo si $u \neq v$ y el mínimo ordinal $\beta < \alpha$ que cumple $u(\beta) \neq v(\beta)$ cumple, de hecho, $u(\beta) < v(\beta)$.

Por último, el teorema 4.33 nos da que se cumple el axioma de elección.

A.3 La dimensión del espacio dual

Aquí probaremos un resultado nada trivial que determina la dimensión de lo que se conoce como espacio dual de un espacio vectorial dado:

Definición A.9 Una aplicación $f : V \longrightarrow W$ entre dos K-espacios vectoriales es *lineal* si:

1. $f(v_1 + v_2) = f(v_1) + f(v_2)$, para $v_1, v_2 \in V$.
2. $f(\alpha v) = \alpha f(v)$, para $v \in V$ y $\alpha \in K$.

Teorema A.10 *Sea $f : B \longrightarrow W$ una aplicación de una base B de un K-espacio vectorial V en otro K-espacio vectorial W. Entonces existe una única aplicación lineal $\bar{f} : V \longrightarrow W$ que extiende a f.*

DEMOSTRACIÓN: Como todo vector $v \in V$ se expresa de forma única como combinación lineal $v = \alpha_1 v_1 + \cdots \alpha_n v_n$, con $v_1, \ldots, v_n \in B$, podemos definir $\bar{f}(v) = \alpha_1 f(v_1) + \cdots \alpha_n f(v_n) \in W$. No ofrece ninguna dificultad comprobar que $\bar{f}$ así definida es una aplicación lineal y que es la única que extiende a f. ∎

Notemos ahora que un cuerpo K es un K-espacio vectorial con la suma y el producto de su estructura de cuerpo, por lo que podemos considerar el conjunto V^* de todas las aplicaciones lineales $f : V \longrightarrow K$.

Es inmediato comprobar que V^* es un subespacio vectorial de K^V, es decir, que la suma de aplicaciones lineales y el producto producto de un escalar por una aplicación lineal son aplicaciones lineales. El espacio vectorial V^* se llama *espacio dual* de V.

Si V tiene dimensión finita, es fácil calcular la dimensión de V^*. De hecho, en la prueba del teorema siguiente determinamos explícitamente una base:

Teorema A.11 *Si V es un espacio vectorial de dimensión finita, entonces*

$$\dim V^* = \dim V.$$

DEMOSTRACIÓN: Sea $v_1, \ldots, v_n$ una base de V. Definimos su *base dual* como la base $v_1^*, \ldots, v_n^*$ de V^* dada por

$$v_i^*(v_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

(Aquí usamos el teorema anterior para definir v_i^* a través de su restricción a una base.) Basta probar que la base dual es realmente una base de V^*. En efecto, si

$$\alpha_1 v_1^* + \cdots + \alpha_n v_n^* = 0,$$

evaluando en v_i obtenemos que $\alpha_i = 0$, luego la base dual es linealmente independiente. Por otra parte, si $f \in V^*$, se cumple que

$$f = f(v_1)v_1^* + \cdots + f(v_n)v_n^*,$$

pues ambos miembros son aplicaciones lineales que coinciden sobre la base dada $v_1, \ldots, v_n$. ∎

Para espacios de dimensión infinita, el cálculo de la dimensión del espacio dual es más complicado:

Teorema A.12 *Si V es un K-espacio vectorial de dimensión infinita, entonces*

$$\dim V^* = |K|^{\dim V} > \dim V.$$

DEMOSTRACIÓN: Si B es una base de V, el teorema A.10 nos da una biyección $K^B \longrightarrow V^*$ que a cada aplicación $B \longrightarrow K$ le asigna su única extensión lineal a V. Por lo tanto $|V^*| = |K|^{\dim V}$. Por otra parte, el teorema A.8 nos da que $|V^*| = |K| \dim V^*$. Así pues,

$$|K| \dim V^* = |K|^{\dim V}$$

y el teorema quedará probado si demostramos que $|K| \leq \dim V^*$. Esto es obvio si K es finito, así que podemos suponer que K es infinito.

Diremos que una familia $F \subset K^\omega$ es *fuertemente independiente* si para todo $n \geq 1$, todos los $f_1, \ldots, f_n \in F$ distintos y todo $I \subset \omega$ con $|I| = n$, se cumple que $f_1|_I, \ldots, f_n|_I$ es una familia linealmente independiente en el espacio K^I. Hay que entender que $\varnothing$ es trivialmente fuertemente independiente.

El lema de Zorn nos garantiza la existencia de una familia $\mathcal{M} \subset K^\omega$ fuertemente independiente y maximal respecto de la inclusión. Vamos a probar que

$$|K| \leq |\mathcal{M}| \leq \dim V^*.$$

Empezamos con la segunda desigualdad. Para ello fijamos una base B^* de V^* (necesariamente infinita) y fijamos en ella un subconjunto numerable $\{v_n\}_{n\in\omega}$. Para cada $f \in \mathcal{M}$, consideramos la aplicación lineal $w_f : V \longrightarrow K$ que sobre B^* viene dada por

$$w_f(v) = \begin{cases} f(n) & \text{si existe un } n \text{ tal que } v = v_n, \\ 0 & \text{si } v \neq v_n \text{ para todo } n. \end{cases}$$

Basta probar que si $f_1, \ldots, f_n \in \mathcal{M}$ son distintos dos a dos y los escalares $\alpha_1, \ldots, \alpha_n \in K$ cumplen $\alpha_1 w_{f_1} + \cdots + \alpha_n w_{f_n} = 0$, entonces todos los α_i son nulos, pues esto prueba a la vez que los w_f son distintos dos a dos y que son linealmente independientes en V^*. Como todo conjunto linealmente independiente está contenido en una base, de aquí concluimos que $|\mathcal{M}| \leq \dim V^*$, como queremos probar.

Ahora bien, tenemos que, para todo $j \in \omega$, se cumple que

$$\alpha_1 w_{f_1}(v_j) + \cdots + \alpha_n w_{f_n}(v_j) = 0,$$

es decir, que

$$\alpha_1 f_1(j) + \cdots + \alpha_n f_n(j) = 0.$$

luego si $I \subset \omega$ cumple $|I| = n$, tenemos que

$$\alpha_1 f_1|_I + \cdots + \alpha_n f_n|_I = 0,$$

pero por definición de familia fuertemente independiente tenemos que las restricciones $f_1|_I, \ldots, f_n|_I$ son linealmente independientes en K^I, luego todos los escalares α_i son nulos.

Pasamos ahora a probar que $|K| \leq |\mathcal{M}|$. Para ello suponemos que $|\mathcal{M}| < |K|$. Vamos a definir recurrentemente una sucesión $\{\xi_i\}_{i\in\omega} \in K^\omega$ de manera que si $n \leq p$, $f_1, \ldots, f_n \in \mathcal{M} \cup \{\{\xi_i\}_{i<p}\}$ son distintos dos a dos e $I \subset p$ cumple que $|I| = n$, entonces $f_1|_I, \ldots, f_n|_I$ son linealmente independientes en K^I.

Tomamos $\xi_0 = 1$, que cumple trivialmente lo requerido para $p = 1$. Supongamos definida $\{\xi_i\}_{i<p}$ y vamos a definir ξ_p. Para cada $\alpha \in K$, consideremos $\xi^\alpha = (\xi_0, \ldots, \xi_{p-1}, \alpha) \in K^{p+1}$.

Si tomando $\xi_p = \alpha$ no se cumple lo requerido, eso significa que existen $f_1, \ldots, f_n \in \mathcal{M} \cup \{\xi^\alpha\}$ distintos dos a dos, para $n \leq p+1$ y existe un conjunto $I \subset p+1$ de modo que $|I| = n$ y $f_1|_I, \ldots, f_n|_I$ son linealmente dependientes (incluyendo la posibilidad de que dos de ellos coincidan). Pongamos que los elementos de I son $i_1 < \cdots < i_n$.

Algún f_j tiene que ser ξ^α, pues lo contrario contradiría la independencia fuerte de $\mathcal{M}$. No perdemos generalidad si suponemos que $f_n = \xi^\alpha$. Además $p \in I$, pues en caso contrario $f_n|_I = \{\xi_i\}_{i<p}|_I$ y $f_1, \ldots, f_{n-1}$ contradiría la hipótesis de inducción. Más concretamente, tiene que ser $i_n = p$. Sean

$$\begin{aligned} f_1|_I &= (a_{11}, \ \ldots, a_{1m}, \ b_1) \\ &\vdots \qquad\qquad \vdots \\ f_m|_I &= (a_{m1}, \ldots, a_{mm}, b_m) \\ f_n|_I &= (\xi_{i_1}, \ \ldots, \xi_{i_m}, \ \alpha), \end{aligned}$$

donde $m = n - 1$.

La independencia fuerte de $\mathcal{M}$ implica que los m vectores $(a_{j1}, \ldots, a_{jm})$ son linealmente independientes en K^m y, como $\dim K^m = m$ y todo conjunto independiente está contenido en una base, concluimos que estos vectores son una base de K^m. Por consiguiente, existen unos únicos escalares $\alpha_1, \ldots, \alpha_m$ tales que

$$(\xi_{i_1}, \ldots, \xi_{i_m}) = \sum_{k=1}^{m} \alpha_k (a_{k1}, \ldots, a_{km}).$$

Por otra parte, es obvio que $f_1|_I, \ldots, f_m|_I$ son linealmente independientes (porque lo son al quitarles la última componente), luego para que $f_1|_I, \ldots, f_n|_I$ sean linealmente dependientes es necesario que $f_n|_I$ sea combinación lineal de $f_1|_I, \ldots, f_m|_I$, y por la unicidad de los α_k tiene que ser

$$f_n|_I = \sum_{k=1}^{m} \alpha_k f_k|_I.$$

En particular,

$$\alpha = \sum_{k=1}^{m} \alpha_k f_k(p).$$

Con esto hemos probado que para cada elección posible $f_1, \dots, f_m \in \mathcal{M}$, con $m \leq p$, y cada $J \subset p$ con $|J| = m$, existe a lo sumo un $\alpha \in K$ para el que la asignación $\xi_p = \alpha$ no cumpliría lo requerido. Como $|\mathcal{M}^{\leq p} \times \mathcal{P}p| < |K|$, vemos que el cardinal del conjunto de todos los α que no podemos tomar como ξ_p es menor que el cardinal de K, luego existe un $\alpha \in K$ fuera de este conjunto, y tomando $\xi_p = \alpha$ se cumple lo requerido.

Con esto tenemos definida la sucesión $\xi = \{\xi_i\}_{i<\omega} \in K^\omega$. Observemos que $\xi \notin \mathcal{M}$, pues, dado cualquier $f \in \mathcal{M}$, tomando $p = 2$, $I = \{0, 1\}$, por construcción tenemos que $(f(0), f(1))$, (ξ_0, ξ_1) son linealmente independientes, luego $\xi \neq f$.

Vamos a probar que $\mathcal{M} \cup \{\xi\}$ es fuertemente independiente, lo que contradirá la maximalidad de $\mathcal{M}$ y el teorema quedará probado.

En efecto, si $f_1, \dots, f_n \in \mathcal{M} \cup \{\xi\}$ son distintos dos a dos e $I \subset \omega$ cumple $|I| = n$, podemos tomar $p \in \omega$ tal que $p \geq n$, $I \subset p$.

Si $f_1, \dots, f_n \in \mathcal{M}$, entonces $f_1|_I, \dots, f_n|_I$ son linealmente independientes por la independencia fuerte de $\mathcal{M}$. En caso contrario podemos suponer que $f_n = \xi$, con lo que $f_n|_p = \{\xi_i\}_{i<p}$ y $f_1|_I, \dots, f_n|_I$ son linealmente independientes por la construcción de ξ. ∎

Apéndice B

Subconjuntos de $\mathbb{R}$ y el axioma de elección

En el capítulo VI de [T] hemos probado que todo subconjunto de Borel de un espacio polaco cumple las tres propiedades siguientes (la primera de las cuales es trivial):

- Son medibles (para cualquier medida de Borel).
- Tienen la propiedad de Baire [T 6.42].
- Son numerables o bien contienen un subconjunto perfecto (y en este caso su cardinal es $\mathfrak{c}$) [T 6.28].

Cabe preguntarse si en realidad estas propiedades no serán mucho más generales: ¿existe un subconjunto de $\mathbb{R}$ que no sea medible Lebesgue? ¿Y sin la propiedad de Baire? ¿Existe un subconjunto de $\mathbb{R}$ no numerable que no contenga un subconjunto perfecto? Las tres preguntas tienen respuesta afirmativa, pero la respuesta en todos los casos requiere de forma esencial el uso del axioma de elección.

Es interesante observar que se trata de tres preguntas que basta responder en un espacio polaco cualquiera para que la respuesta sea válida en cualquier otro. Por ejemplo, si en un espacio polaco X tenemos una medida de Borel unitaria continua μ y existe un subconjunto A que no es μ-medible, aplicando dos veces el teorema [T 6.40], concluimos que cualquier medida de Borel unitaria continua en cualquier espacio polaco tiene conjuntos no medibles, y el teorema 7.60 nos permite extender la conclusión a medidas de Borel continuas arbitrarias.

Similarmente, si en un espacio polaco perfecto X existe un subconjunto A sin la propiedad de Baire, el teorema [T 6.22] nos da que X tiene un subconjunto G_δ denso Y homeomorfo a $\mathcal{N}$ y $A \cap Y$ no tiene la propiedad de Baire en Y, ya que en caso contrario $A \cap Y = U \cup C$, donde U es de Borel en Y (luego en X) y C es de primera categoría en Y (luego en X por [T 1.66]). Concluimos que $\mathcal{N}$

contiene un subconjunto sin la propiedad de Baire. A su vez, invirtiendo los razonamientos precedentes, llegamos a que todo espacio polaco perfecto tiene un subconjunto sin la propiedad de Baire.

Por último, si X es un espacio polaco con un subconjunto no numerable A que no contiene un subconjunto perfecto, el teorema [T 6.9] nos da una biyección continua $f : C \longrightarrow X$, donde C es cerrado en $\mathcal{N}$. Así $f^{-1}[A]$ es no numerable y, si contuviera un subconjunto perfecto K, podríamos tomarlo compacto, con lo que $f|_K : K \longrightarrow A$ es un homeomorfismo en su imagen, luego A contiene un subconjunto perfecto. Concluimos que $\mathcal{N}$ contiene un subconjunto no numerable sin subconjuntos perfectos, y de aquí se sigue inmediatamente que lo mismo vale para todo espacio polaco.

B.1 El ejemplo de Vitali

El ejemplo clásico de conjunto no medible Lebesgue se debe a Vitali, y aprovecha también para la propiedad de Baire:

Teorema B.1 (AE) *Existe un subconjunto de $\mathbb{R}$ no medible Lebesgue y sin la propiedad de Baire.*

Demostración: Consideramos en $\mathbb{I} = [0, 1]$ la relación de equivalencia R dada por $a\,R\,b \leftrightarrow b - a \in \mathbb{Q}$, y sea $V \subset \mathbb{I}$ un conjunto que posea exactamente un punto en cada clase de equivalencia.[1] Vamos a probar que V no es medible Lebesgue ni tiene la propiedad de Baire.

En realidad demostraremos algo más general: el conjunto de Vitali V no es medible para ninguna medida de Borel $\mu \neq 0$ definida en $\mathbb{R}$ respecto a la que los intervalos acotados tengan medida finita y que sea invariante por traslaciones, es decir, tal que si $A \in \mathcal{M}_\mu$ y $a \in \mathbb{R}$, entonces $a+A \in \mathcal{M}_\mu$ y $\mu(a+A) = \mu(A)$. En particular, no sólo existe un subconjunto de $\mathbb{R}$ no medible Lebesgue, sino que la medida de Lebesgue no puede extenderse a una medida definida sobre toda el álgebra $\mathcal{P}\mathbb{R}$ de modo que la extensión siga siendo invariante por traslaciones.

Sea $\{r_n\}_{n\in\omega}$ una enumeración de $\mathbb{Q} \cap \mathbb{I}$ y sea $V_n = r_n + V$. La definición de V hace que los conjuntos V_n sean disjuntos dos a dos y además

$$[0, 1] \subset \bigcup_{n\in\omega} V_n \subset [-1, 2].$$

Si V fuera medible para la medida μ, como suponemos que es invariante por traslaciones, resulta que $\mu(V_n) = \mu(V)$ y, como la unión es disjunta,

$$\mu([0, 1]) \leq \sum_{n\in\omega} \mu(V) \leq \mu([-1, 2]) < +\infty.$$

[1] Notemos que el conjunto cociente $\mathbb{I}/R$ es no numerable, por lo que esta elección no puede justificarse (o, por lo menos, no es evidente que pueda justificarse —y puede probarse que no se puede—) a partir de ED. Más concretamente, para construirlo basta suponer que $\mathbb{R}$ puede ser bien ordenado.

La segunda desigualdad implica que $\mu(V) = 0$, y la primera nos da entonces que $\mu([0,1]) = 0$. La invarianza por traslaciones implica entonces que $\mu = 0$.

Supongamos ahora que V tiene la propiedad de Baire, y sea $A \subset \mathbb{R}$ un abierto tal que $V \triangle A$ sea de primera categoría. Si $A = \varnothing$, entonces $V \triangle A = V$ es de primera categoría. Si, por el contrario $A \neq \varnothing$, tomamos un intervalo no vacío $]a,b[\subset A$. Si $q \in \mathbb{Q}$ es cualquier número racional no nulo, por construcción de V tenemos que $V \cap (q+V) = \varnothing$, luego

$$]a,b[\cap (q+V) \subset]a,b[\setminus V \subset A \setminus V \subset V \triangle A,$$

luego $]a,b[\cap(q+V)$ es de primera categoría y, como la traslación $x \mapsto x-q$ es un homeomorfismo, también lo será su imagen por ésta, es decir, $]a-q, b-q[\cap V$ es de primera categoría.

Ahora bien, es claro que $V = \bigcup_{q \in \mathbb{Q}\setminus\{0\}}]a,b[\cap (q+V)$, luego concluimos que, en cualquier caso, V es de primera categoría. Ahora bien,

$$[0,1] \subset \bigcup_{q \in \mathbb{Q}} (q+V),$$

y todos los trasladados $q+V$ son de primera categoría, luego $[0,1]$ también lo es, y eso es absurdo. ∎

En lugar de un ejemplo que carezca a la vez de las dos propiedades, podemos encontrar ejemplos separados:

Teorema B.2 (AE) *Existen conjuntos con la propiedad de Baire que no son medibles Lebesgue y conjuntos medibles Lebesgue que no tienen la propiedad de Baire.*

Demostración: Basta considerar el conjunto de Vitali V construido en la demostración del teorema anterior y los conjuntos A y B dados por [T 6.46] (para $\mathbb{R}$). Así $V = (V \cap A) \cup (V \cap B) = A' \cup B'$, donde A' es nulo y B' es de primera categoría. Como la unión de ambos no es medible ni tiene la propiedad de Baire, A' ha de ser medible sin la propiedad de Baire y B' ha de ser no medible con la propiedad de Baire. ∎

B.2 Conjuntos finales

Veamos ahora que la existencia de conjuntos no medibles Lebesgue y sin la propiedad de Baire se sigue de hecho del teorema de los ultrafiltros.

Definición B.3 Un conjunto $A \subset \mathcal{C}$ es un *conjunto final* si cuando $x \in A$ e $y \in \mathcal{C}$ cumple $x|_n = y|_n$ para cierto $n \in \omega$, entonces $y \in A$.

Consideramos en $\mathcal{C}$ la medida de Haar unitaria (véase el final de la sección 10.8 de [T]), determinada por que sobre los abiertos básicos $B_s = \{x \in \mathcal{C} \mid x|_{\ell(s)} = s\}$ (donde $s \in 2^{<\omega}$) viene dada por

$$m(B_s) = 2^{-\ell(s)}. \tag{B.1}$$

La unicidad implica que si $i \in \omega$ y $T_i : \mathcal{C} \longrightarrow \mathcal{C}$ es el homeomorfismo dado por

$$T_i(x)(n) = \begin{cases} x(n) & \text{si } n \neq i, \\ 1 - x(n) & \text{si } n = i, \end{cases}$$

se cumple que $m(T_i[A]) = m(A)$ para todo $A \subset \mathcal{C}$ medible. En efecto, la aplicación dada por $m'(A) = m(T_i[A])$ es una medida de Borel en $\mathcal{C}$ que cumple la condición (B.1), luego es $m' = m$.

Teorema B.4 *Si $A \subset \mathcal{C}$ es un conjunto final con la propiedad de Baire, o bien A o bien $\mathcal{C} \setminus A$ es de primera categoría.*

Demostración: Supongamos que A no es de primera categoría. Entonces existe un abierto no vacío U tal que $U \triangle A$ es de primera categoría. Sea $s \in 2^n$ tal que $B_s \subset U$, con lo que $B_s \setminus A$ es de primera categoría. Para cada $t \in 2^n$, una composición de a lo sumo n homeomorfismos T_i transforma B_s en B_t y, como A es final, resulta invariante por todos ellos, luego existe un homeomorfismo de $\mathcal{C}$ que transforma $B_s \setminus A$ en $B_t \setminus A$, luego este conjunto es de primera categoría. Por consiguiente,

$$\mathcal{C} \setminus A = \bigcup_{t \in 2^n} (B_t \setminus A)$$

también es de primera categoría. ∎

Teorema B.5 *Si $A \subset \mathcal{C}$ es un conjunto final medible, entonces $m(A) = 0$ o bien $m(A) = 1$.*

Demostración: Al igual que hemos visto en la prueba del teorema anterior, dados $s, t \in 2^n$, existe una composición T de homeomorfismos T_i que transforma B_s en B_t. Dichos homeomorfismos conservan la medida y, como A es final, queda invariante por ellos. Así pues,

$$m(A \cap B_t) = m(T[A \cap B_s]) = m(A \cap B_s).$$

Puesto que $A = \bigcup_{s \in 2^n} (A \cap B_s)$ y la unión es disjunta, tenemos que

$$m(A) = \sum_{t \in 2^n} m(A \cap B_t) = 2^n\, m(A \cap B_s).$$

Así pues, para todo $s \in 2^n$,

$$m(A \cap B_s) = 2^{-n}\, m(A) = m(B_s)\, m(A).$$

Si $m(A) > 0$, la medida en $\mathcal{C}$ dada por

$$m'(X) = \frac{m(X \cap A)}{m(A)}$$

cumple la condición de unicidad (B.1), luego $m(X \cap A) = m(X)\, m(A)$ para todo $X \subset \mathcal{C}$ medible (y esto es cierto igualmente si $m(A) = 0$). Tomando en particular $X = A$ tenemos que $m(A) = m^2(A)$, luego $m(A) = 0, 1$. ∎

En particular, si $\mathcal{F}$ es un filtro en ω, podemos considerar el conjunto

$$\tilde{\mathcal{F}} = \{\chi_F \mid F \in \mathcal{F}\} \subset \mathcal{C}$$

y, si $\mathcal{F}$ contiene a los conjuntos cofinitos, $\tilde{\mathcal{F}}$ es claramente final.

Teorema B.6 *Si $\mathcal{F}$ es un ultrafiltro no principal en ω, entonces $\tilde{\mathcal{F}}$ es un subconjunto no medible de $\mathcal{C}$ y sin la propiedad de Baire.*

DEMOSTRACIÓN: Consideremos el homeomorfismo $T : \mathcal{C} \longrightarrow \mathcal{C}$ dado por $T(x)(i) = 1 - x(i)$. Es inmediato que $T[\tilde{\mathcal{F}}] = \mathcal{C} \setminus \tilde{\mathcal{F}}$. Por lo tanto, $\tilde{\mathcal{F}}$ no puede tener la propiedad de Baire, ya que, al ser un conjunto final, o bien $\tilde{\mathcal{F}}$ o bien $T[\tilde{\mathcal{F}}]$ tendría que ser de primera categoría, pero, como T es un homeomorfismo, de hecho ambos tendrían que serlo y $\mathcal{C}$ también lo sería.

Similarmente, si $\tilde{\mathcal{F}}$ fuera medible, $T[\tilde{\mathcal{F}}]$ también lo sería y con la misma medida, pues T conserva la medida (es inmediato que $m'(X) = m(T[X])$ es una medida de Borel en $\mathcal{C}$ que cumple (B.1), luego $m' = m$). Por consiguiente, tendríamos que $m(\tilde{\mathcal{F}}) = m(T[\tilde{\mathcal{F}}]) = 1 - m(\tilde{\mathcal{F}})$, luego $m(\tilde{\mathcal{F}}) = 1/2$, cuando, al ser $\tilde{\mathcal{F}}$ un conjunto final, hemos visto que su medida ha de ser 0 o 1, contradicción. ∎

B.3 Conjuntos de Bernstein

En cuanto a la propiedad de poseer subconjuntos perfectos, es evidente que si $2^{\aleph_0} > \aleph_1$ entonces cualquier subconjunto B de un espacio polaco X tal que $|B| = \aleph_1$ es un subconjunto no numerable de X que no tiene subconjuntos perfectos, pero podemos encontrar ejemplos sin necesidad de negar la hipótesis del continuo:

Definición B.7 Un subconjunto B de un espacio polaco X es un *conjunto de Bernstein* si tanto B como $X \setminus B$ cortan a todo subconjunto perfecto de X y ambos tienen cardinal $\mathfrak{c} = 2^{\aleph_0}$.

Teorema B.8 *Todo espacio polaco no numerable que admita un buen orden contiene un conjunto de Bernstein.*

DEMOSTRACIÓN: Sea X un espacio polaco no numerable que pueda ser bien ordenado. Esto implica en particular que su cardinal $\mathfrak{c} = 2^{\aleph_0}$ puede identificarse con un ordinal. Sea $\{P_\alpha\}_{\alpha<\mathfrak{c}}$ una enumeración[2] (con repeticiones, si es preciso) de los subconjuntos perfectos de X. Definimos por recurrencia dos sucesiones $\{p_\alpha\}_{\alpha<\mathfrak{c}}$ y $\{q_\alpha\}_{\alpha<\mathfrak{c}}$ de modo que p_α, q_α sean dos elementos de P_α distintos entre sí y distintos de todos los $\{p_\delta\}_{\delta<\alpha}$ y $\{q_\delta\}_{\delta<\alpha}$. Esta elección es posible[3] porque $|P_\alpha| = \mathfrak{c}$. Así, basta tomar $B = \{p_\alpha \mid \alpha \in \mathfrak{c}\}$, de modo que $\{q_\alpha \mid \alpha \in \mathfrak{c}\} \subset X \setminus B$. Es claro que B es un conjunto de Bernstein. ∎

[2]Como X tiene una base numerable, es claro que tiene a lo sumo $\mathfrak{c}$ abiertos, luego también a lo sumo $\mathfrak{c}$ cerrados.

[3]Aquí es donde usamos que X puede ser bien ordenado.

Los conjuntos de Bernstein también son ejemplos de conjuntos no medibles Lebesgue y sin la propiedad de Baire. Al contrario de lo que sucede con los ejemplos considerados anteriormente, este hecho es válido en cualquier espacio polaco:

Teorema B.9 *Sea X un espacio polaco no numerable y sea $\mu \neq 0$ una medida de Borel continua en X. Si $B \subset X$ es un conjunto de Bernstein, entonces todo subconjunto de B que sea μ-medible es nulo, y si tiene la propiedad de Baire es de primera categoría. En particular, los conjuntos de Bernstein no son medibles ni tienen la propiedad de Baire.*

DEMOSTRACIÓN: Si $A \subset B$ es un conjunto medible con medida no nula (resp. con la propiedad de Baire y de segunda categoría), entonces A contiene un subconjunto de Borel también con medida no nula (resp. de segunda categoría, por [T 6.43]), el cual, al ser no numerable (porque la medida es continua), contiene a su vez un subconjunto perfecto, lo cual es imposible.

Así, si B fuera medible, su complementario también lo sería y tendríamos que $\mu(X) = 0$. Igualmente, si B tuviera la propiedad de Baire X sería de primera categoría. ∎

La existencia de conjuntos no numerables sin subconjuntos perfectos puede demostrarse a partir de una consecuencia muy concreta de AE:

Teorema B.10 *Si $\aleph_1 \leq 2^{\aleph_0}$, entonces todo espacio polaco no numerable contiene un subconjunto no numerable sin subconjuntos perfectos.*

DEMOSTRACIÓN: Si $2^{\aleph_0} \leq \aleph_1$, entonces $2^{\aleph_0} = \aleph_1$, luego todo espacio polaco no numerable tiene cardinal $\aleph_1$ y, en particular, admite un buen orden. Por lo tanto, la conclusión se sigue de B.8. Si $2^{\aleph_0} \not\leq \aleph_1$, entonces, por hipótesis, todo espacio polaco no numerable (que tiene cardinal $2^{\aleph_0}$) tiene un subconjunto de cardinal $\aleph_1$, el cual no puede tener un subconjunto perfecto, ya que entonces sería $2^{\aleph_0} \leq \aleph_1$. ∎

B.3.1 Bases de Hamel

Una *base de Hamel*[4] es simplemente una base de $\mathbb{R}$ como espacio vectorial sobre $\mathbb{Q}$. El teorema A.5 prueba (a través del lema de Zorn) que todo espacio vectorial tiene una base. Ahora vamos a probar que la mera existencia de una base de Hamel implica la existencia de un conjunto no medible Lebesgue. Nos basamos en el teorema siguiente:

Teorema B.11 (Steinhaus) *Si $A \subset \mathbb{R}^n$ es un conjunto medible Lebesgue de medida no nula, entonces el conjunto $A - A = \{a - b \mid a, b \in A\}$ contiene un entorno de 0.*

[4]En algunos contextos la expresión "base de Hamel" se usa más en general, incluso para referirse a cualquier base de cualquier espacio vectorial, pero aquí la usaremos en este sentido específico.

DEMOSTRACIÓN: Tomando un subconjunto, no perdemos generalidad si suponemos que $0 < m(A) < \infty$. Como $m(A) < 2m(A)$, existen $K \subset A \subset V$ tales que K es compacto, V es abierto y $m(V) < 2m(K)$. La distancia de K a $\mathbb{R}^n \setminus V$ no es nula, luego, tomando una bola U de centro cero y radio dicha distancia, tenemos que $K+U \subset V$. Así, si $u \in U$, no puede ser $K \cap (u+K) = \varnothing$, pues en tal caso $2m(K) = m(K) + m(u+K) \leq m(V)$, contradicción. Por lo tanto, existen $k, k' \in K \subset A$ tales que $k = u + k'$, luego $U \subset A - A$. ∎

Teorema B.12 *Si existe una base de Hamel, entonces existe un subconjunto de $\mathbb{R}$ no medible Lebesgue.*

DEMOSTRACIÓN: Si $B \subset \mathbb{R}$ es una base de Hamel, sea $b \in B$ y consideremos el subespacio vectorial $A = \langle B \setminus \{b\}\rangle$ generado por $B \setminus \{b\}$ sobre $\mathbb{Q}$. Veamos que A no es medible Lebesgue. Claramente

$$\mathbb{R} = \bigcup_{q\in\mathbb{Q}} (qb + A),$$

luego si A es medible, como $m(qb + A) = m(A)$, tiene que ser $m(A) > 0$. Por el teorema anterior existe un entorno U de 0 tal que $U \subset A - A$. Podemos tomar $q \in \mathbb{Q} \setminus \{0\}$ suficientemente pequeño para que $qb \in U$, y entonces existen $x, y \in A$ tales que $qb = x - y$, luego $b \in A$, lo que contradice la independencia lineal de B. Esto prueba que A no es medible Lebesgue. ∎

En contra de lo que podría parecer a la vista del teorema precedente, no es cierto que una base de Hamel B sea necesariamente no medible Lebesgue. Lo que sí podemos decir a partir de la prueba es que si es medible Lebesgue, entonces su medida es nula. En efecto, si $m(B) > 0$ entonces $A_0 = B \setminus \{b\}$ también tiene medida positiva, luego por el teorema de Steinhaus $A_0 - A_0$ contiene un entorno de 0, luego lo mismo le sucede a $A - A \supset A_0 - A_0$ (donde A es el espacio vectorial definido en el teorema anterior), y este hecho es lo único que realmente se usa en el teorema para llegar a una contradicción.

Para probar (AE) que existe una base de Hamel medible Lebesgue basta tener en cuenta el teorema [T 6.20], según el cual el conjunto de Cantor C cumple $C + C = [0, 2]$. Esto implica que C es un sistema generador de $\mathbb{R}$ sobre $\mathbb{Q}$, pues para cada $x \in \mathbb{R}$ existe un $q \in \mathbb{Q}$ no nulo tal que $\frac{1}{q}x \in [0, 2]$, luego $x = qc_1 + qc_2$, con $c_1, c_2 \in C$. Por A.5, todo sistema generador de un espacio vectorial contiene una base, luego C contiene una base de Hamel, y como C es medible Lebesgue y tiene medida nula (teorema [T 6.38]), concluimos que lo mismo vale para la base que contiene. Reunimos estos hechos y algunos más en el teorema siguiente:

Teorema B.13 (AE) *Se cumple:*

1. *Existen bases de Hamel, todas ellas tienen cardinal $2^{\aleph_0}$ y, si son medibles Lebesgue, entonces tienen medida nula.*
2. *Existen bases de Hamel medibles Lebesgue y bases de Hamel no medibles Lebesgue.*

DEMOSTRACIÓN: La existencia de bases de Hamel nos la da A.5. Todas ellas tienen cardinal $2^{\aleph_0}$ por el teorema A.8 (notemos que $\mathbb{R}$ no puede tener dimensión finita n como $\mathbb{Q}$-espacio vectorial, pues en tal caso tendríamos que $|\mathbb{R}| = |\mathbb{Q}^n|$ y $\mathbb{R}$ sería numerable).

Sólo falta probar que existen bases de Hamel no medibles Lebesgue. Para ello modificaremos ligeramente la prueba del teorema B.8. El planteamiento es el mismo: partimos de una enumeración $\{P_\alpha\}_{\alpha<\mathfrak{c}}$ de los subconjuntos perfectos de $\mathbb{R}$. Definimos por recurrencia una sucesiones $\{p_\alpha\}_{\alpha<\mathfrak{c}}$ de modo que $p_\alpha \in P_\alpha$ no pertenezca al subespacio vectorial generado (sobre $\mathbb{Q}$) por todos los $\{p_\delta\}_{\delta<\alpha}$. Esta elección es posible porque $|P_\alpha| = \mathfrak{c}$, mientras que (por el mismo argumento con el que hemos calculado el cardinal de una base de Hamel) el cardinal del espacio generado por las dos sucesiones es $\leq \aleph_0|\alpha| < \mathfrak{c}$.

El conjunto $B_0 = \{p_\alpha \mid \alpha \in \mathfrak{c}\}$ es así un conjunto linealmente independiente que corta a todos los subconjuntos perfectos de $\mathbb{R}$. Ahora usamos que, según A.5, todo conjunto linealmente independiente en un espacio vectorial está contenido en una base. Esto nos da en nuestro caso una base de Hamel B que contiene a B_0, luego sigue cortando a todos los subconjuntos perfectos de $\mathbb{R}$. Esta base B es necesariamente no medible Lebesgue, pues si lo fuera tendría medida 0, luego $\mathbb{R} \setminus B$ sería un conjunto medible no nulo, luego contendría un subconjunto de Borel, y a su vez un subconjunto perfecto, contradicción. ∎

B.4 Números hiperreales

El teorema B.6 muestra que para probar la existencia de conjuntos no medibles no es necesario todo el axioma de elección, sino que basta el teorema de los ultrafiltros, que es ligeramente más débil. Vamos a ver aquí otra construcción basada en este teorema a través de la teoría de modelos.

Teorema B.14 (TU) *Existe un subconjunto de $\mathbb{R}$ no medible Lebesgue.*

DEMOSTRACIÓN: Sea U un ultrafiltro no principal sobre ω y consideremos la ultrapotencia $\mathbb{R}^* = \mathrm{Ult}_U(\mathbb{R})$. De acuerdo con las observaciones previas al teorema 10.37, tenemos que $\mathbb{R}^*$ es un cuerpo ordenado no arquimediano que extiende a $\mathbb{R}$.

Observemos que la construcción de la ultrapotencia no depende del lenguaje formal del cual consideramos a $\mathbb{R}$ como modelo, luego podemos añadirle más signos sin cambiar $\mathbb{R}^*$. Por ejemplo, si le añadimos dos relatores monádicos que se interpreten en $\mathbb{R}$ como la pertenencia a $\mathbb{N}$ y a $\mathbb{Q}$, respectivamente, entonces en $\mathbb{R}^*$ se interpretan como la pertenencia a dos subconjuntos que podemos representar por $\mathbb{N}^*$ y $\mathbb{Q}^*$, a cuyos elementos podemos llamar *hipernaturales* e *hiperracionales,* respectivamente.

La equivalencia elemental se traduce en que todas las propiedades —expresables como sentencias del lenguaje de la teoría de anillos con las extensiones que estamos considerando— que valen para $\mathbb{R}$, $\mathbb{Q}$ y $\mathbb{N}$ valen también en $\mathbb{R}^*$.

Por ejemplo, como $\mathbb{R} \vDash \bigwedge xy \in \mathbb{N}\ x + y \in \mathbb{N}$, lo mismo vale para $\mathbb{R}^*$, lo cual significa que la suma de hipernaturales es hipernatural, etc.

Añadimos también al lenguaje formal un funtor monádico que se interprete en $\mathbb{R}$ como la función $x \mapsto 2^x$, que en $\mathbb{R}^*$ se interpretará como una función que representaremos igualmente por 2^x. Como $\mathbb{R} \vDash \bigwedge n \in \mathbb{N}\ 2^n \in \mathbb{N}$, se cumple que $\bigwedge n \in \mathbb{N}^*\ 2^n \in \mathbb{N}^*$, etc.

Fijamos ahora un hipernatural N infinitamente grande. Por ejemplo, basta considerar $N = [d]$, donde $d(n) = n$, y así $N \in \mathbb{N}^*$ y $\bigwedge n \in \mathbb{N}\ n < N$.

Definimos

$$E_0 = \{x \in [0,1]^* \setminus \mathbb{Q} \mid \bigvee k \in \mathbb{N}^* \left(\frac{2k}{2^N} < x < \frac{2k+1}{2^N}\right)\},$$

$$E_1 = \{x \in [0,1]^* \setminus \mathbb{Q} \mid \bigvee k \in \mathbb{N}^* \left(\frac{2k+1}{2^N} < x < \frac{2k+2}{2^N}\right)\},$$

donde $[0,1]^*$ representa el intervalo correspondiente en $\mathbb{R}^*$. Podemos pensar que E_i es el conjunto de los números irracionales cuya N-sima cifra en su desarrollo binario es i.

Ahora usamos que

$$\mathbb{R} \vDash \bigwedge n \in \mathbb{N} \bigwedge x(0 < x < 1 \wedge x \notin \mathbb{Q} \to \overset{1}{\bigvee} r \in \mathbb{N} \left(\frac{r}{2^n} < x < \frac{r+1}{2^n}\right)),$$

así como que

$$\mathbb{R} \vDash \bigwedge r \in \mathbb{N} \bigvee k(r = 2k \vee r = 2k+1),$$

con lo que lo mismo es válido en $\mathbb{R}^*$, lo que se traduce en que $[0,1]^* \setminus \mathbb{Q}^* = E_0 \cup E_1$ y $E_0 \cap E_1 = \varnothing$, (aquí usamos también la traducción a $\mathbb{R}^*$ de que un mismo número natural no puede ser par e impar a la vez).

Definimos $A_i = [0,1] \cap E_i$, de modo que $[0,1] \setminus \mathbb{Q} = A_0 \cup A_1$ y $A_0 \cap A_1 = \varnothing$. Vamos a probar que A_0 y A_1 no son medibles Lebesgue.

Para ello consideramos $I_n^k = \left[\frac{k}{2^n}, \frac{k+1}{2^n}\right] \setminus \mathbb{Q}$ y observamos que la función $f_n^k : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f_n^k(x) = \frac{2k+1}{2^n} - x$ cumple $f_n^k[I_n^k] = I_n^k$ (le aplica una simetría). Por otra parte:

$$\frac{R}{2^N} < x < \frac{R+1}{2^N} \quad \Rightarrow \quad \frac{2k+1}{2^n} - \frac{R+1}{2^N} < f_n^k(x) < \frac{2k+1}{2^n} - \frac{R}{2^N},$$

es decir,

$$\frac{(2k+1)2^{N-n} - R - 1}{2^N} < f_n^k(x) < \frac{(2k+1)2^{N-n} - R}{2^N},$$

y resulta que $(2k+1)2^{N-n} - R - 1$ es par si y sólo si R es impar. (Aquí usamos que en ${}^*\mathbb{N}$ se cumplen las propiedades obvias sobre números pares e impares.) Por lo tanto, $x \in A_i \leftrightarrow f_n^k(x) \in A_{1-i}$. Equivalentemente:

$$f_n^k[I_n^k \cap A_i] = I_n^k \cap A_{1-i}.$$

Si los conjuntos A_i son medibles, entonces, como f_n^k conserva la medida de Lebesgue (porque es una simetría, luego conserva las medidas de los intervalos), concluimos que

$$m(I_n^k \cap A_0) = m(I_n^k \cap A_1) = m(I_n^k)/2.$$

(La última igualdad se debe a que I_n^k es unión disjunta de los dos primeros conjuntos.) En particular, $m(A_0) = m(I_0^0 \cap A_0) = 1/2$.

Consideramos entonces la medida que a cada conjunto medible Lebesgue en $[0,1]$ le asigna $\mu(X) = 2m(X \cap A_0)$. Ciertamente es una medida con la propiedad de que $\mu(I_n^k) = m(I_n^k)$. De aquí se sigue fácilmente que μ y m coinciden sobre todos los intervalos abiertos, luego, de hecho, $\mu = m$. Ahora bien, haciendo $X = A_0$ en la definición de μ, tenemos que $m(A_0) = 2m(A_0)$, es decir, $1/2 = 1$. ∎

B.5 Filtros rápidos

El propósito de esta sección es demostrar un teorema análogo a B.10 para conjuntos medibles, lo cual es mucho más delicado. Para ello demostraremos una versión de B.6 con una hipótesis más débil. Vamos a necesitar varios resultados técnicos, el primero de los cuales es el siguiente (consideramos en $\mathcal{C}$ la medida de Haar unitaria m, como en la sección B.2):

Teorema B.15 *Sea $A \subset \mathcal{C}$ un cerrado de medida positiva. Entonces existe un cerrado $B \subset A$ de medida positiva y una sucesión creciente $\{n_k\}_{k\in\omega}$ de números naturales tal que*

$$\bigwedge s \in 2^{n_k}(B_s \cap B \neq \varnothing \to m(B_s \cap B) \geq (1 - 2^{-k})m(B_s)).$$

Demostración: Vamos a construir una sucesión creciente $\{n_k\}_{k\in\omega}$ de números naturales y una sucesión decreciente $\{C_k\}_{k\in\omega}$ de cerrados tales que

$$m(C_k \setminus C_{k+1}) \leq m(A)2^{-n_k-k-2} \tag{B.2}$$

y

$$C_k = \bigcup_{s\in T_k} (B_s \cap C_{k-1}), \tag{B.3}$$

donde

$$T_k = \{s \in 2^{n_k} \mid m(B_s \cap C_{k-1}) \geq (1 - 2^{-k-1})\, m(B_s)\}. \tag{B.4}$$

Tomamos $C_0 = A$ y $n_0 = 1$. Supongamos construidos C_ky n_k, y veamos que existe $n_{k+1} > n_k$ tal que

$$N = |\{s \in 2^{n_{k+1}} \mid B_s \cap C_k \neq \varnothing\}| \leq 2^{n_{k+1}}(m(C_k) + m(A)\, 2^{-n_k-2k-4}).$$

Para ello tomamos un abierto G tal que $C_k \subset G$ y

$$m(G) \leq m(C_k) + m(A)\, 2^{-n_k-2k-4}.$$

Como C_k es compacto, podemos exigir que G sea unión de un número finito de abiertos básicos, así como que todos ellos corten a C_k. También podemos suponer que todos ellos son de la forma B_s con $s \in 2^{n_{k+1}}$, para un $n_{k+1} > n_k$. Como los abiertos de este tipo son disjuntos dos a dos, G será, más precisamente, la unión de todos los abiertos básicos B_s con $s \in 2^{n_k+1}$ tales que $B_s \cap C_k \neq \varnothing$, y el numero de tales abiertos es el que hemos llamado N.

Así pues, $m(G) = N/2^{n_{k+1}}$, luego

$$N = 2^{n_{k+1}}\, m(G) \leq 2^{n_{k+1}}(m(C_k) + m(A)\, 2^{-n_k-2k-4}), \tag{B.5}$$

como había que probar. Definimos C_{k+1} mediante (B.3), con lo que claramente es cerrado, $C_{k+1} \subset C_k$ y

$$m(C_{k+1}) \leq |T_{k+1}|2^{-n_{k+1}}. \tag{B.6}$$

Además

$$C_k \setminus C_{k+1} \subset \bigcup\{B_s \cap C_k \mid s \in 2^{n_{k+1}} \setminus T_{k+1} \wedge B_s \cap C_k \neq \varnothing\}.$$

Entonces

$$m(C_k) = m(C_{k+1}) + m(C_k \setminus C_{k+1}) \leq [\text{por } (B.4)]$$

$$m(C_{k+1}) + \sum\{(1-2^{-k-2})2^{-n_{k+1}} \mid s \in 2^{n_{k+1}} \setminus T_{k+1} \wedge B_s \cap C_k \neq \varnothing\}$$

$$\leq m(C_{k+1}) + (1-2^{-k-2})2^{-n_{k+1}}(N - |T_{k+1}|) \leq [\text{por } (B.6)]$$

$$m(C_{k+1}) + (1-2^{-k-2})2^{-n_{k+1}}(N - 2^{n_{k+1}} m(C_{k+1}))$$

$$= m(C_{k+1}) + (1-2^{-k-2})(N2^{-n_{k+1}} - m(C_{k+1}))$$

$$= 2^{-k-2}m(C_{k+1}) + (1-2^{-k-2})N2^{-n_{k+1}}.$$

Por lo tanto

$$2^{-k-2}m(C_{k+1}) \geq m(C_k) - N2^{-n_{k+1}}(1-2^{-k-2}) \geq [\text{por } (B.5)]$$

$$m(C_k) - 2^{n_{k+1}}(m(C_k) + m(A)\, 2^{-n_k-2k-4})2^{-n_{k+1}}(1-2^{-k-2})$$

$$= -m(A)\, 2^{-n_k-2k-4} + 2^{-k-2}m(C_k),$$

luego

$$m(C_{k+1}) \geq m(C_k) - m(A)\, 2^{-n_k-k-2}$$

de donde se sigue (B.2).

Ahora definimos $B = \bigcap_{k\in\omega} C_k$, que obviamente es cerrado. Así

$$C_k \setminus B = \bigcup_{r\geq k} (C_r \setminus C_{r+1}) \to m(C_k \setminus B) = \sum_{r\geq k} m(C_r \setminus C_{r+1})$$

$$\leq \sum_{r\geq k} m(A)\, 2^{-n_r-r-2} = m(A)\, 2^{-n_k-k-1} \sum_{r\geq k} 2^{-(n_r-n_k)-(r-k)-1}$$

$$= m(A)\, 2^{-n_k-k-1} \sum_{r\geq 0} 2^{-(n_{r+k}-n_k)-r-1} \leq m(A)\, 2^{-n_k-k-1} \sum_{r\geq 0} 2^{-r-1}$$

$$= m(A)\, 2^{-n_k-k-1}.$$

Así pues,

$$m(B) = m(C_k) - m(C_k \setminus B) \geq m(C_k) - m(A)\,2^{-n_k-k-1}.$$

Para $k = 0$ queda $m(B) \geq m(A) - m(A)2^{-2} > 0$.

Si $s \in 2^{n_k}$ y $B_s \cap B \neq \varnothing$, entonces $B_z \cap C_k \neq \varnothing$, luego $s \in T_k$, luego

$$m(B_s \cap C_k) = m(B_s \cap \bigcup_{s' \in T_k} (B_{s'} \cap C_{k-1})) = m(B_s \cap C_{k-1})$$

$$[\text{por } (B.4)] \geq (1 - 2^{-k-1})\, m(B_s) \geq (1 - 2^{-k})\, m(B_s),$$

como había que probar. ∎

Definición B.16 Un filtro $\mathcal{F}$ en ω es *rápido* si para toda $\phi : \omega \longrightarrow \omega$ creciente existe $F \in \mathcal{F}$ tal que $\bigwedge k \in \omega\ |F \cap \phi(k)| \leq k$.

En primer lugar demostramos que el teorema B.6 es válido para filtros rápidos en lugar de ultrafiltros no principales:

Teorema B.17 *Si $\mathcal{F}$ es un filtro rápido, entonces $\tilde{\mathcal{F}}$ no es medible.*

Demostración: Supongamos que $\tilde{\mathcal{F}}$ es medible. Sea $T : \mathcal{C} \longrightarrow \mathcal{C}$ el homeomorfismo definido al principio de la prueba del teorema B.6. Es inmediato que $\tilde{\mathcal{F}} \cap T[\tilde{\mathcal{F}}] = \varnothing$ y, si $\tilde{F}$ es medible, ambos conjuntos tienen la misma medida, luego $m(\tilde{F}) \leq 1/2$.

Existe un abierto G tal que $\tilde{\mathcal{F}} \subset G$ y $m(G) < 1$, luego $A = \mathcal{C} \setminus G$ es un cerrado de medida positiva tal que $\tilde{\mathcal{F}} \cap A = \varnothing$. Sea $B \subset A$ y $\{n_k\}_{k\in\omega}$ según el teorema anterior. Sea $\phi : \omega \longrightarrow \omega$ la aplicación (creciente) dada por $\phi(k) = n_{k+2}$. Como $\mathcal{F}$ es rápido existe $F \in \mathcal{F}$ tal que $\bigwedge k \in \omega\ |F \cap n_{k+2}| \leq k$.

Vamos a construir $s_k \in 2^{n_k}$ tal que, para todo $k \in \omega$,

$$s_k = s_{k+1}|_{s_k}, \qquad \chi_F|_{n_k} \leq s_k, \qquad B_{s_k} \cap B \neq \varnothing.$$

Por la propiedad de F tenemos $|F \cap n_2| \leq 0$, luego $\chi_F|_{n_0} = 0$, luego basta tomar $z_0 \in 2^{n_0}$ tal que $B_{z_0} \cap B \neq \varnothing$ y s_0 cumple lo pedido.

Supongamos construido s_k. Como $B_{s_k} \cap B \neq \varnothing$, tenemos que

$$m(B_{s_k} \cap B) \geq (1 - 2^{-k}) m(B_{s_k}).$$

Sea $P = \{s \in 2^{n_{k+1}} \mid s|_{n_k} = s_k \wedge \bigwedge m \in F \cap n_{k+1}\ s(m) = 1\}$. Así

$$|P| = 2^{n_{k+1}-n_k-|(n_{k+1}\setminus n_k)\cap F|}, \qquad \text{luego}$$

$$m(\{u \in B_{s_k} \mid \chi_F|_{n_{k+1}} \leq u|_{n_{k+1}}\}) = m(\{u \in B_{s_k} \mid u|_{n_{k+1}} \in P\})$$

$$= 2^{n_{k+1}-n_k-|(n_{k+1}\setminus n_k)\cap F|-n_{k+1}} = 2^{-n_k-|(n_{k+1}\setminus n_k)\cap F|}$$

$$= m(B_{s_k}) 2^{-|(n_{k+1}\setminus n_k)\cap F|} \geq m(B_{s_k})\, 2^{-|n_{k+1}\cap F|} \geq m(B_{s_k})\, 2^{-k+1}.$$

Si este conjunto fuera disjunto con $B_{s_k} \cap B$, su unión tendría medida

$$\geq (1 - 2^{-k})\, m(B_{s_k}) + m(B_{s_k})\, 2^{-k+1} > m(B_{s_k}),$$

pero esto es imposible, pues se trata de un subconjunto de B_{s_k}. Así pues, existe un $u \in B_{s_k} \cap B$ tal que $\chi_F|_{n_{k+1}} \leq u|_{n_{k+1}}$. Tomamos $s_{k+1} = u|_{n_{k+1}}$, con lo que $u \in B_{s_{k+1}} \cap B \neq \varnothing$ y s_{k+1} cumple lo pedido.

Sea $x = \bigcup_{k\in\omega} s_k \in \mathcal{C}$. Como $B_{s_k} \cap B \neq \varnothing$ y $\{B_{s_k}\}_{k\in\omega}$ es una base de entornos de x, tenemos que $x \in \overline{B} = B \subset A$.

Como $\chi_F|_{n_k} \leq s_k$, resulta que $\chi_F \leq x$, luego $F \subset x^{-1}[\{1\}]$, con lo que $x^{-1}[\{1\}] \in \mathcal{F}$, luego $x \in \tilde{\mathcal{F}} \cap A = \varnothing$, contradicción. ∎

Ahora vamos a ver cómo construir un filtro rápido. Necesitamos otro hecho técnico:

Teorema B.18 *Sea $E \subset \mathcal{C}$ un conjunto nulo. Entonces existe un subconjunto cerrado $B \subset \mathcal{C}$ tal que $B \cap E = \varnothing$, $m(B) > 0$ y para todo $n \in \omega$ y todo $s \in 2^n$, si $B \cap B_s \neq \varnothing$ entonces $m(B \cap B_2) \geq 8^{-n-1}$.*

Demostración: Por regularidad existe un cerrado $C_0 \subset \mathcal{C}$ de manera que $C_0 \cap E = \varnothing$ y $m(C_0) \geq 1/2$. Supuesto definido C_k, sea

$$C_{k+1} = \bigcup\{B_s \cap C_k \mid s \in 2^{k+1} \wedge m(B_s \cap C_k) \geq 1/8^{k+1}\},$$

que claramente es cerrado, al igual que $B = \bigcap_{k\in\omega} C_k$.

Tomemos $n \leq k$ y $s \in 2^n$. Entonces

$$\begin{aligned} m(B_s \cap (C_k \setminus C_{k+1})) &= m(B_s \cap \bigcup\{B_{s'} \cap C_k \mid s' \in 2^{k+1} \wedge m(B_s \cap C_k) < 1/8^{k+1}\}) \\ &= m(\bigcup\{B_{s'} \cap C_k \mid s' \in 2^{k+1} \wedge m(B_s \cap C_k) < 1/8^{k+1} \wedge s'|_n = s\}) \\ &\leq 2^{k+1-n}(1/8^{k+1}). \end{aligned}$$

En particular, si $s = \varnothing$, tenemos que $m(C_k \setminus C_{k+1}) \leq 1/4^{k+1}$. Así

$$m(B) = m(C_0) - m(C_0 \setminus B) = \frac{1}{2} - m(\bigcup_{k\in\omega}(C_k \setminus C_{k+1}))$$

$$= \frac{1}{2} - \sum_{k\in\omega} m(C_k \setminus C_{k+1}) \geq \tfrac{1}{2} - \sum_{k\in\omega} \tfrac{1}{4^{k+1}} = \tfrac{1}{2} - \tfrac{1}{3} > 0.$$

Ahora, si $s \in 2^n$, con $n > 0$ y $B \cap B_s \neq \varnothing$, entonces $B_s \cap C_n \neq \varnothing$, luego, por definición de C_n ha de ser $m(B_s \cap C_{n-1}) \geq 1/8^n$ y además $B_s \cap C_n = B_s \cap C_{n-1}$, luego $m(B_s \cap C_n) \geq 1/8^n$. Entonces

$$m(B_s \cap B) \geq m(B_s \cap C_n) - \sum_{k\geq n} m(B_s \cap (C_k \setminus C_{k+1}))$$

$$\geq \frac{1}{8^n} - \sum_{k\geq n} \frac{2^{k+1-n}}{8^{k+1}} = \frac{1}{8^n} - \frac{1}{2^n}\sum_{k\geq n} \frac{1}{4^{k+1}} = \frac{2}{3\cdot 8^n} \geq \frac{1}{8^n} \geq \frac{1}{8^{n+1}}.$$

∎

Puede probarse que los filtros rápidos tampoco tienen la propiedad de Baire.

Definición B.19 Supongamos que existe $X \subset \mathcal{C}$ tal que $|X| = \aleph_1$. Para cada $x, y \in \mathcal{C}$, $x \neq y$, definimos $h(x,y) = \min\{n \in \omega \mid x(n) \neq y(n)\}$. Si $R \subset \mathcal{C} \times \mathcal{C}$ es una relación de equivalencia, definimos

$$Z_R = \{h(x,y) \mid x \in X \wedge y \in X \wedge x \neq y \wedge x\,R\,y\} \subset \omega.$$

Teorema B.20 *Los conjuntos Z_R, donde R recorre las relaciones de equivalencia en $\mathcal{C}$ que sean de Borel como subconjunto de $\mathcal{C} \times \mathcal{C}$ y tales que $|\mathcal{C}/R| \leq \aleph_0$, generan un filtro $\mathcal{F}_X$ en ω que contiene a los conjuntos cofinitos.*

Demostración: Veamos que cada Z_R es infinito. Como $|X| = \aleph_1$ y $|C/R| \leq \aleph_0$, alguna clase de equivalencia ha de ser infinita, sea Y una de ellas. Sea $h : [Y]^2 \longrightarrow Z_R$ la aplicación dada por $h(\{x,y\}) = h(x,y)$. Si Z_R fuera finito, por el teorema de Ramsey 11.4, Y contendría un conjunto infinito homogéneo H y, si $x, y, z \in H$, entonces $h(x,y) = h(x,z) = h(y,z) = n$, pero eso es imposible.

Obviamente $Z_{R_1 \cap R_2} \subset Z_{R_1} \cap Z_{R_2}$, por lo que los conjuntos Z_R generan un filtro $\mathcal{F}_X$. Para probar que contiene a los conjuntos cofinitos tomamos $n \in \omega$ y consideramos la relación de equivalencia en $\mathcal{C}$ dada por

$$x\,R_n\,y \leftrightarrow x|_n = y|_n.$$

Obviamente es de Borel, determina 2^n clases de equivalencia y $Z_R \subset \omega \setminus n$, luego $\omega \setminus n \in \mathcal{F}_X$, lo que implica que $\mathcal{F}_X$ contiene a los conjuntos cofinitos. ∎

Definición B.21 Si $X \subset \mathcal{C}$ cumple $|X| = \aleph_1$, el filtro $\mathcal{F}_X$ dado por el teorema anterior recibe el nombre de *filtro de Raisonnier* asociado a X.

Vamos a dar una condición suficiente para que $\mathcal{F}_X$ sea un filtro rápido.

Para ello, para cada $H \subset \mathcal{C} \times \mathcal{C}$ llamamos $H_x = \{y \in \mathcal{C} \mid (x,y) \in H\}$ y

$$H(X) = \bigcup_{x \in X} H_x.$$

Teorema B.22 *Supongamos que se cumple la condición:*

(N) *Si $H \subset \mathcal{C} \times \mathcal{C}$ es un G_δ con secciones nulas, entonces $H(X)$ es nulo.*

Entonces $\mathcal{F}_X$ es un filtro rápido.

Demostración: Consideramos aquí la base de $\mathcal{C}$ formada por los abiertos de la forma

$$B_s = \{x \in \mathcal{C} \mid x|_{\mathcal{D}s} = s\},$$

donde, en lugar de restringir $s \in 2^n$ para $n \in \omega$, consideramos más en general $s \in 2^I$, para cualquier $I \subset \omega$ finito. Diremos que $I = \mathcal{D}s$ es el *soporte* de D_s.

Observemos que podemos construir una sucesión $\{A(s,i,j)\}_{s\in 2^{<\omega},i,j\in\omega}$ de abiertos básicos tales que $m(A(s,i,j)) = 2^{-i-j}$ y los abiertos $\{A(s,i,j)\}_{s\in 2^{<\omega}}$ tengan soportes disjuntos dos a dos.

En efecto, basta partir ω en infinitos conjuntos disjuntos de cardinal $i+j$ y asignamos uno a cada $s \in 2^{<\omega}$, tomando un abierto básico cualquiera con dicho soporte.

Sea $\phi : \omega \longrightarrow \omega$ creciente y sea $H^\phi \subset \mathcal{C}\times\mathcal{C}$ la relación dada por

$$x\, H^\phi\, y \leftrightarrow \bigwedge j \in \omega \bigvee j' l \in \omega(j \le j' \le l \wedge y \in A(x|_{\phi(l)}, l, j')).$$

Así

$$H^\phi = \bigcap_{j\in\omega} \bigcup_{j\le j'\le l} \{(x,y) \in \mathcal{C}\times\mathcal{C} \mid y \in A(x|_{\phi(l)}, l, j')\},$$

y los conjuntos de la izquierda son antiimágenes de abiertos por la proyección en la segunda componente, luego son abiertos en $\mathcal{C}\times\mathcal{C}$, luego H^ϕ es un G_δ.

Para cada $x \in \mathcal{C}$,

$$H^\phi_x = \bigcap_{j\in\omega} \bigcup_{j\le j'\le l} A(x|_{\phi(l)}, l, j')$$

y

$$m\Big(\bigcup_{j\le j'\le l} A(x|_{\phi(l)}, l, j')\Big) \le \sum_{j\le j'\le l} \frac{1}{2^{l+j'}} = \sum_{j\le j'} \frac{1}{2^{j'}} \sum_{j'\le l} \frac{1}{2^l} = \sum_{j\le j'} \frac{1}{2^{j'}} \frac{1}{2^{j'-1}}$$

$$= \sum_{j\le j'} \frac{1}{2^{2j'-1}} = \frac{1}{2^{2j-2}} = \frac{1}{4^{j-2}},$$

luego $m(H^\phi_x) = 0$.

Por (N) podemos afirmar que $H^\phi(X)$ es un conjunto nulo. Sea B^ϕ según el teorema B.18, es decir, B^ϕ es cerrado en $\mathcal{C}$, $B^\phi \cap H^\phi(X) = \varnothing$, $m(B^\phi) > 0$ y, para todo $s \in 2^{<\omega}$, si $B^\phi \cap B_s \ne \varnothing$, entonces $m(B^\phi \cap B_2) \ge 8^{-n-1}$, donde $n = \ell(s)$.

Dado $x \in \mathcal{C}$, sea $O^x_j = \bigcup_{j\le j'\le l} A(x|_{\phi(l)}, l, j') \cap B^\phi$, que es un abierto en B^ϕ y, si $x \in X$, entonces $\bigcap_j O^x_j = H^\phi_x \cap B^\phi = \varnothing$, luego, por el teorema de Baire, algún O^x_j no es denso en B^ϕ, es decir, para cierto $j \in \omega$ y $s \in 2^{<\omega}$, se cumple que $B^\phi \cap B_s \ne \varnothing$ y $B^\phi \cap B_s \cap O_j = \varnothing$.

Fijemos una biyección $\langle\ ,\ \rangle : \omega \times 2^{<\omega} \longrightarrow \omega$. Podemos suponer que cumple $\max\{\ell(s), j\} \le \langle j, s\rangle$.

Para cada $x \in \mathcal{C}$, sea $F(x)$ el mínimo $\langle j_0, s_0\rangle$ tal que $B^\phi \cap B_{s_0} \ne \varnothing$ y $B^\phi \cap B_{s_0} \cap O_{j_0} \ne \varnothing$ si existe algún par (j_0, s_0) en estas condiciones, y $F(x) = \infty$ en otro caso. (Acabamos de probar que $F(x)$ es finito siempre que $x \in X$.) Sea R^ϕ la relación en $\mathcal{C}\times\mathcal{C}$ dada por

$$x\, R^\phi\, y \leftrightarrow (F(x) = F(y) = \infty) \vee (F(x) = F(y) \ne \infty \wedge x|_{\phi(F(x))} = y|_{\phi(F(y))}).$$

Claramente R^ϕ es una relación de equivalencia. Vamos a probar que es de Borel. Para ello empezamos descomponiéndola como

$$R^\phi = \{x \in \mathcal{C} \mid F(x) = \infty\} \times \{y \in \mathcal{C} \mid F(y) = \infty\} \cup$$

$$\{(x,y) \in \mathcal{C} \times \mathcal{C} \mid F(x) = F(y) \neq \infty \wedge x|_{\phi(F(x))} = y|_{\phi(F(y))}\}.$$

Por una parte:

$$\{x \in \mathcal{C} \mid F(x) = \infty\} = \{x \in \mathcal{C} \mid \neg\bigvee js(B^\phi \cap B_s \neq \varnothing \wedge B^\phi \cap B_s \cap O_j^x = \varnothing)\}$$

$$= \mathcal{C} \setminus \bigcup_{(j,s)} \{x \in \mathcal{C} \mid B^\phi \cap B_s \cap O_j^x = \varnothing\},$$

donde en la última unión (j,s) recorren los pares tales que $B^\phi \cap B_s \neq \varnothing$.

A su vez,

$$\{x \in \mathcal{C} \mid B^\phi \cap B_s \cap O_j^x = \varnothing\} = \bigcap_{j \leq j' \leq l} \{x \in \mathcal{C} \mid A(x|_{\phi(l)}, l, j') \cap B^\phi \cap B_s = \varnothing\}$$

y el último conjunto es claramente abierto, pues la condición depende únicamente de $x|_{\phi(l)}$. Concluimos que $\{x \in \mathcal{C} \mid F(x) = \infty\}$ es un conjunto de Borel.

Por otra parte:

$$\{(x,y) \in \mathcal{C} \times \mathcal{C} \mid F(x) = F(y) \neq \infty \wedge x|_{\phi(F(x))} = y|_{\phi(F(y))}\}$$

$$= \bigcup_{n \in \omega} \{(x,y) \in \mathcal{C} \times \mathcal{C} \mid F(x) = F(y) = n \wedge x|_{\phi(n)} = y|_{\phi(n)}\}$$

$$= \bigcup_{n \in \omega} (\{(x,y) \in \mathcal{C} \times \mathcal{C} \mid F(x) = F(y) = n\} \cap \{(x,y) \in \mathcal{C} \times \mathcal{C} \mid x|_{\phi(n)} = y|_{\phi(n)}\}).$$

El conjunto a la derecha de $\cap$ es abierto, luego sólo falta probar que el de la izquierda también lo es. Pongamos que $n = \langle j, s\rangle$. Si $B^\phi \cap B_s = \varnothing$, el conjunto es vacío, luego es de Borel. Supongamos que $B^\phi \cap B_s \neq \varnothing$. Entonces

$$\{(x,y) \in \mathcal{C} \times \mathcal{C} \mid F(x) = F(y) = \langle j, s\rangle\} =$$

$$\{(x,y) \in \mathcal{C} \times \mathcal{C} \mid F(x) = \langle j, s\rangle\} \times \{(x,y) \in \mathcal{C} \times \mathcal{C} \mid F(y) = \langle j, s\rangle\},$$

luego basta ver que el conjunto $\{(x,y) \in \mathcal{C} \times \mathcal{C} \mid F(x) = \langle j, s\rangle\}$ es de Borel. Ahora bien,

$$\{(x,y) \in \mathcal{C} \times \mathcal{C} \mid F(x) = \langle j, s\rangle\} = \{(x,y) \in \mathcal{C} \times \mathcal{C} \mid B^\phi \cap B_s \cap O_j^x = \varnothing\} \cap$$

$$\bigcap_{j',s'} \{x \in \mathcal{C} \mid B^\phi \cap B_{s'} \cap O_{j'}^x \neq \varnothing\}, \tag{B.7}$$

donde la última intersección recorre los j', s' tales que

$$\langle j', s'\rangle < \langle j, s\rangle \quad \text{y} \quad B^\phi \cap B_{s'} \neq \varnothing.$$

El primer conjunto del miembro derecho de (B.7) es de Borel porque así lo hemos demostrado antes, y los que aparecen tras la intersección son de Borel porque son complementarios de conjuntos como el primero. Esto termina la prueba de que R^ϕ es de Borel.

Por otra parte, es evidente que R^ϕ determina una cantidad numerable de clases de equivalencia (una para cada valor posible de F).

Por consiguiente, podemos considerar $Z_\phi = Z_{R^\phi} \in \mathcal{F}_X$. Veamos que

$$\bigwedge k \in \omega\ |Z_\phi \cap \phi(k)| \le k(3k+3)^2 2^{4k}.$$

En principio:

$$Z_\phi \cap \phi(k) = \{h(x,y) \mid x,y \in X \wedge x \neq y \wedge x\, R^\phi\, y \wedge h(x,y) < \phi(k)\}.$$

Si $x,y \in X \wedge x\, R^\phi\, y$, existen $j \in \omega$ y $s \in 2^{<\omega}$ tales que $F(x) = F(y) = \langle j,s\rangle$ y $x|_{\phi(\langle j,s\rangle)} = y|_{\phi(\langle j,s\rangle)}$, luego $h(x,y) \ge \phi(\langle j,s\rangle)$.

Si $h(x,y) < \phi(k)$, entonces $\langle j,s\rangle < k$, pues si fuera $k \le \langle j,s\rangle$, entonces $\phi(k) \le \phi(\langle j,s\rangle) \le h(x,y)$.

Por definición de F, tenemos además que $B^\phi \cap B_s \neq \varnothing$ y $B^\phi \cap B_s \cap O^x_j = \varnothing$, luego, como $j < k$, por definición de O^x_j, $B^\phi \cap B_s \cap A(x|_{\phi(k)}, k, j) = \varnothing$, e igualmente para y.

Sea $\Delta(s,j) = \{t \in 2^{\phi(k)} \mid B^\phi \cap B_s \cap A(t,k,j) = \varnothing\}$, $\delta(s,j) = |\Delta(s,j)|$.

Así, si $n \in Z_\phi \cap \phi(k)$, entonces $n = h(x,y)$, para ciertos $x,y \in X$ tales que existen s,j de modo que

$$\langle s,j\rangle < k, \quad B^\phi \cap B_s \neq \varnothing, \quad x|_{\phi(k)} \in \Delta(s,j), \quad y|_{\phi(k)} \in \Delta(s,j).$$

Además, por la definición de h, si $h(x,y) \neq h(x',y') < \phi(k)$ entonces $(x|_{\phi(k)}, y|_{\phi(k)}) \neq (x'|_{\phi(k)}, y'|_{\phi(k)})$, luego $Z_\phi \cap \phi(k)$ está completamente determinado por el conjunto $\bigcup_{s,j} \Delta(s,j) \times \Delta(s,j)$, donde s,j recorre los pares tales que $\langle s,j\rangle < k$ y $B^\phi \cap B_s \neq \varnothing$, luego

$$|Z_\phi \cap \phi(k)| \le \sum_{s,j} \delta(s,j)^2. \tag{B.8}$$

Por definición de Δ, tenemos que

$$B^\phi \cap B_s \subset \bigcap_{t \in \Delta(s,j)} (\mathcal{C} \setminus A(t,k,j)),$$

luego

$$m(B^\phi \cap B_s) \le m\Big(\bigcap_{t \in \Delta(s,j)} (\mathcal{C} \setminus A(t,k,j))\Big) \le (1 - 2^{-k-j})^{\delta(s,j)}.$$

Vamos a probar la última igualdad. Pongamos que, para cada $t \in \Delta(s,j)$, $A(t,k,j) = B_{s_t}$, donde $s_t \in 2^{I_t}$ y los soportes I_t son conjuntos disjuntos de cardinal $k+j$. Así

$$\bigcap_{t \in \Delta(s,j)} (\mathcal{C} \setminus A(t,k,j)) = \{x \in \mathcal{C} \mid \bigwedge t \in \Delta(s,j)\ x|_{I_t} \neq s_t\}$$

$$= \{x \in \mathcal{C} \mid x|_I \in D\},$$

donde $I = \bigcup_{t \in \Delta(s,j)} I_t$ y $D = \{u \in 2^I \mid \bigwedge t \in \Delta(S,j)\ u|_{I_t} \neq s_t\}$.

El hecho de que los soportes sean disjuntos implica que $|D| = (2^{k+j}-1)^{\delta(s,j)}$. Así

$$m\Big(\bigcap_{t\in\Delta(s,j)}(\mathcal{C}\setminus A(t,k,j))\Big) = \frac{(2^{k+j}-1)^{\delta(s,j)}}{2^{(k+j)\delta(s,j)}} = \left(1-\frac{1}{2^{k+j}}\right)^{\delta(s,j)}.$$

Por otra parte, por construcción de B^ϕ, si $B^\phi \cap B_s \neq \varnothing$, entonces

$$m(B^\phi \cap B_s) \geq 8^{-\ell(s)-1}.$$

Así,

$$2^{-3\ell(s)-3} \leq (1-2^{-k-j})^{\delta(s,j)} \to -(3\ell(s)+3) \leq \delta(s,j)\log_2(1-2^{-k-j})$$

$$\to \delta(s,j) \leq \frac{3n+3}{\log_2(\frac{2^{k+j}}{2^{k+j}-1})} \leq (3\ell(s)+3)\,2^{k+j}.$$

Para probar la última desigualdad basta ver (llamando $t = 2^{k+j}$) que

$$\frac{1}{\log_2(\frac{t}{t-1})} \leq t \leftrightarrow \frac{1}{t} \leq \log_2(\frac{t}{t-1}) \leftrightarrow 2^{1/t} \leq \frac{t}{t-1} \leftrightarrow 2 \leq \frac{t^t}{(t-1)^t}$$

$$\leftrightarrow t^t \geq 2(t-1)^t,$$

y esto es cierto, pues

$$t^t = ((t-1)+1)^t \geq (t-1)^t + t(t-1)^{t-1} \geq 2(t-1)^t.$$

Así, continuando con (B.8) y teniendo en cuenta que $j \leq \langle s,j\rangle < k$, $\ell(s) \leq k$,

$$|Z_\phi \cap \phi(k)| \leq \sum_{s,j}((3\ell(s)+3)2^{k+j})^2 \leq \sum_{s,j}(3k+3)^2 2^{4k} \leq k(3k+3)^2 2^{4k}.$$

Finalmente, sea $\psi(k) = k(3k+3)^2 2^{4k}$ y consideremos $\phi' : \omega \longrightarrow \omega$ dada por $\phi'(k) = \phi(\psi(k+1))$. Se trata de una aplicación creciente, luego todo lo que hemos probado para ϕ es válido también para ϕ'. Así, está definido $Z_{\phi'}$ y para todo $k \in \omega$

$$|Z_{\phi'} \cap \phi(\psi(k+1))| \leq \psi(k).$$

Si $p \geq \psi(0)$, existe un k tal que $\psi(k) \leq p \leq \psi(k+1)$, con lo que

$$|Z_{\phi'} \cap \phi(p)| \leq |Z_{\phi'} \cap \phi(\psi(k+1))| \leq \psi(k) \leq p.$$

Por lo tanto, si llamamos $A = Z_{\phi'} \setminus \phi(\psi(0)) \in \mathcal{F}_X$ (aquí usamos que $\mathcal{F}_X$ contiene a los conjuntos cofinitos), se cumple que

$$|A \cap \phi(p)| \leq |Z_{\phi'} \cap \phi(p)| \leq p,$$

para todo $p \geq \psi(0)$, pero si $p < \psi(0)$, entonces $\phi(p) < \phi(\psi(0))$, luego también

$$|A \cap \phi(p)| = 0 \leq p.$$

Con esto hemos probado que $\bigwedge p \in \omega\ |A \cap \phi(p)| \leq p$, luego $\mathcal{F}_X$ es un filtro rápido. ∎

Finalmente podemos probar:

Teorema B.23 *Si $\aleph_1 \leq 2^{\aleph_0}$ toda medida de Borel continua en un espacio polaco tiene conjuntos no medibles.*

DEMOSTRACIÓN: En la prueba del teorema [T 6.36] se ve que para cada medida de Borel continua existe otra medida de Borel unitaria con los mismos conjuntos medibles, y por el teorema [T 6.40] no perdemos generalidad si consideramos concretamente la medida m en $\mathcal{C}$ que estamos considerando hasta ahora.

Supongamos que todo subconjunto de $\mathcal{C}$ es medible y llegaremos a una contradicción. Por [T 6.40], podemos suponer también que todo subconjunto de $\mathcal{C} \times \mathcal{C}$ es medible para la medida producto.

Por hipótesis existe un conjunto $X \subset \mathcal{C}$ de cardinal $\aleph_1$. Sea $\leq_X$ un buen orden en X de ordinal $\aleph_1$.

Vamos a demostrar que X cumple la condición (N) del teorema B.22, con lo que el teorema anterior nos dará un conjunto no medible y tendremos la contradicción buscada.

Así pues, sea $H \subset \mathcal{C} \times \mathcal{C}$ un conjunto G_δ con secciones nulas. Hemos de probar que $H(X)$ es nulo.

Para cada $x \in H(X)$, sea $\lambda(x)$ el menor $y \in X$ tal que $x \in H_y$. Sea

$$\tilde{H}(X) = \{(x, y) \in H(X) \times H(X) \mid \lambda(x) <_X \lambda(y)\}.$$

Si $y \in H(X)$, entonces

$$\tilde{H}(X)_y = \{y \in \mathcal{C} \mid (x, y) \in \tilde{H}(X)\} = \{x \in H(X) \mid \lambda(x) <_X \lambda(y)\}$$

$$= \bigcup_{z \in X^<_{\lambda(y)}} \{x \in H(X) \mid \lambda(x) = z\} \subset \bigcup_{z \in X^<_{\lambda(y)}} H_z,$$

luego $\tilde{H}(X)_y$ es nulo por ser unión numerable de conjuntos nulos. Puesto que estamos suponiendo que $\tilde{H}(X)$ es medible, el teorema de Fubini implica que $\tilde{H}(X)$ es nulo. Sea ahora

$$D = (H(X) \times H(X)) \setminus \tilde{H}(X) = \{(x, y) \in H(X) \times H(X) \mid \lambda(y) \leq_X \lambda(x)\}.$$

Exactamente el mismo argumento demuestra que D es nulo, luego el conjunto $H(X) \times H(X)$ es nulo, luego $H(X)$ también. ∎

Bibliografía

[1] Barwise, J. (editor), *Handbook of Mathematical Logic,* North Holland, Amsterdam, 1977.

[2] Blass, A. *Combinatorial Cardinal Characteristics of the Continuum,* en [6].

[3] Bukovský, L. *The Structure of the Real Line,* Birkhäuser (2011)

[4] Devlin, K.J. *Constructibility,* Springer, Berlín (1984)

[5] Engelking, R. *General Topology,* Helderman, Berlín (1989)

[6] Foreman, M., Kanamori, A. (eds.) *Handbook of Set Theory* Springer, (2010)

[7] Galvin, F. *Chain conditions and products, Fund. Math,* **108,** 1 (1980), 33–48.

[8] Givant, S., Halmos, P., *Introduction to Boolean algebras,* Springer, (2009)

[9] Halmos, P.R. *Lectures on Ergodic Theory,* Chelsea, (1956)

[10] Howard, P.E., Ł*os' theorem and the Boolean prime ideal theorem imply the axiom of choice,* Proc. Amer. Math. Soc. **49,** 2 (1975).

[11] Jech, T.J. *The Axiom of Choice,* North Holand, Amsterdam, 1973.

[12] — *Set Theory,* Academic Press, New York, 1978.

[13] Koppelberg, S. *Handbook of Boolean Algebras,* (Vol I), North Holland (1989)

[14] Kunen, K. *Combinatorics,* (en Barwise).

[15] — *Set Theory. An Introduction to Independence Proofs,* North Holland, Amsterdam, 1985.

[16] Luxemburg, W.A.J., *Two applications of the method of construction by ultrapowers to analysis,* Bull. Amer. Math. Soc. **68**, 4 (1962), 416–419.

[17] Pohlers, W. *Proof Theory, The first step to impredicativity,* Springer, Berlin (2009).

[18] Sikorski, R. *Boolean Algebras.* Springer Verlag, Berlin, 1969.

[19] Talagrand, M. *Compacts de fonctions mesurables et filtres non mesurables.* Studia Mathematica 67 (1980) 13–43.

[20] Todorčević, S. *Remarks on Chain Conditions in Products,* Compositio Mathematica, 55 (3) (1985) 295–302.

Índice de Materias