Carlos Ivorra Castillo

TEORÍA DE CONJUNTOS

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

Georg Cantor

Índice General

Introducción ix

Capítulo I: El lenguaje de la teoría de conjuntos 1
1.1 Clases y conjuntos . . . 1
1.2 Funciones . . . 9
1.3 Formación de conjuntos . . . 15
1.4 La teoría de conjuntos NBG* . . . 19
1.5 Relaciones . . . 20
1.6 Leyes de composición interna . . . 27

Capítulo II: Ordinales 39
2.1 La construcción de los ordinales . . . 39
2.2 Inducción y recursión transfinita . . . 48
2.3 Ordinales y buenos órdenes . . . 53
2.4 Funciones normales . . . 56
2.5 La aritmética ordinal . . . 57
2.6 Sumas finitas . . . 64
2.7 La forma normal de Cantor . . . 68

Capítulo III: La teoría de conjuntos NBG 75
3.1 Relaciones bien fundadas . . . 75
3.2 El axioma de regularidad . . . 81
3.3 El axioma de elección . . . 86

Capítulo IV: Cardinales 97
4.1 Equipotencia . . . 97
4.2 Números cardinales . . . 100
4.3 La aritmética cardinal . . . 107
4.4 Conjuntos finitos . . . 115
4.5 Sumas y productos infinitos . . . 119
4.6 Cofinalidad . . . 124
4.7 Aplicaciones sobre el axioma de elección . . . 129

Capítulo V: La exponenciación cardinal **135**
5.1 La exponenciación en NBG 135
5.2 La hipótesis de los cardinales singulares 141
5.3 Cardinales fuertemente inaccesibles 146

Capítulo VI: Conjuntos cerrados no acotados y estacionarios **153**
6.1 Conjuntos cerrados no acotados 153
6.2 Conjuntos estacionarios 159
6.3 Un teorema de Silver 163
6.4 Cardinales de Mahlo 167
6.5 Principios combinatorios 170
6.6 Puntos fijos de funciones normales 184

Capítulo VII: El sistema numérico **193**
7.1 Los números enteros 193
7.2 Los números racionales 198
7.3 Cuerpos métricos completos 201
7.4 La construcción de $\mathbb{R}$ 215
7.5 Conjuntos ordenados completos 222
7.6 Sumas infinitas 231

Capítulo VIII: Elementos de topología **237**
8.1 Espacios topológicos 238
8.2 Algunos conceptos topológicos. 249
8.3 Aplicaciones continuas 256
8.4 Condiciones de numerabilidad 263
8.5 Espacios compactos 270

Capítulo IX: Árboles **279**
9.1 El problema de Suslin 279
9.2 Conceptos básicos sobre árboles 283
9.3 Árboles de Aronszajn 287
9.4 Árboles de Suslin 291
9.5 Árboles de Kurepa 301

Capítulo X: Álgebras de Boole **305**
10.1 Conceptos básicos 305
10.2 Álgebras completas 310
10.3 Ideales y filtros 328
10.4 Espacios de Stone 333
10.5 Aplicaciones a la topología 337

Capítulo XI: Elementos de teoría de modelos **347**
11.1 Lenguajes y modelos 347
11.2 Teorías formales 355
11.3 Submodelos, inmersiones 368
11.4 Ultraproductos 375

Bibliografía **383**

Índice de Materias **384**

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 de NBG), las siglas NBG pueden ser trivial y sistemáticamente sustituidas por ZFC sin necesidad de modificar absolutamente nada de lo dicho.

Los capítulos siguientes, desde el II 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.

El capítulo VI, aunque es una prolongación natural del precedente, es bastante más avanzado y puede leerse tras los capítulos VII y VIII. El primero de éstos está dedicado a la construcción del sistema numérico, y termina de justificar así que la teoría axiomática presentada es suficiente para desarrollar a partir de ella todas las ramas de la matemática (álgebra, análisis, geometría, topología, etc.) Precisamente en el capítulo 8 introducimos los elementos básicos de la topología conjuntista como requisito para la exposición de aspectos más avanzados de la teoría de conjuntos, entre los que se cuentan varios apartados del capítulo previo VI (los relativos a principios combinatorios, cardinales inaccesibles, etc.) así como los capítulos posteriores sobre árboles y álgebras de Boole.

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 último capítulo 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. La mayor parte de los dos últimos capítulos puede verse como los preliminares necesarios (junto con LA) para abordar temas más avanzados de la teoría de conjuntos, principalmente los relativos a pruebas de consistencia, cardinales grandes, etc.

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

En este primer capítulo desarrollaremos el lenguaje necesario para hablar con precisión de conjuntos, de modo que hablaremos de conjuntos en general sin hablar de ningún conjunto en particular. En el capítulo siguiente usaremos los conceptos introducidos aquí para construir (es decir, describir) conjuntos concretos (como los números naturales) que empezarán a perfilar el objeto de estudio de la teoría.

1.1 Clases y conjuntos

El concepto matemático de "conjunto" pretende precisar el concepto informal de "colección de objetos", sin embargo hay razones profundas que harían ingenuo pensar que un conjunto (en el sentido técnico que vamos a dar a la palabra) es exactamente lo mismo que una "colección de objetos". Ciertamente, podemos pensar tranquilamente que todo conjunto es una colección de objetos sin que ello nos lleve a ninguna contradicción (que se sepa), pero pensar que cualquier colección de objetos puede identificarse con un conjunto sí que lleva inevitablemente a contradicciones. Más concretamente: al tratar de precisar el concepto informal de conjunto nos aparecen inevitablemente colecciones de objetos (muchas de las cuales tienen interés matemático) que no pueden considerarse conjuntos sin caer en contradicciones.

Por este motivo vamos a partir de un concepto más general que el de "conjunto", al que llamaremos "clase". Las clases también serán colecciones de objetos, y seguirá siendo cierto que si intentáramos identificar cualquier colección de objetos con una clase caeríamos inevitablemente en contradicciones, pero definiremos los conjuntos como un tipo particular de clases de modo que todas las colecciones de conjuntos que necesitaremos considerar, o bien serán conjuntos, o bien serán clases, y así habremos obtenido un marco conveniente para desarrollar la teoría de conjuntos.

Así pues, decimos que las clases de las que vamos a hablar serán (o podrán ser consideradas como) colecciones de objetos. Quizá el lector espere ahora que, en aras del rigor matemático, explicitemos qué colecciones de objetos vamos a considerar exactamente como clases y cuáles van a ser exactamente los objetos que podrán aparecer en las colecciones llamadas clases, pero no vamos a hacer nada parecido a esto. Por el contrario vamos a limitarnos a afirmar que las *clases* son simplemente los objetos de los que vamos a hablar (sin especificar cuáles son), y que dadas dos clases A y B, entre ellas puede darse o no la relación de *pertenencia,* que representaremos por $A \in B$ cuando se dé y por $A \notin B$ cuando no se dé. En el primer caso diremos que la clase A *pertenece a* (o *es un elemento de*) la clase B, y en el segundo caso diremos que A no pertenece a B o que no es un elemento de B.

Es en este sentido en el que podemos pensar que una clase B es la colección de todas las clases A que cumplen $A \in B$, pero ni vamos a definir qué es exactamente una clase, ni en qué consiste exactamente que una clase pertenezca o no a otra. La parte positiva es que prometemos no hacer esto nunca más, de modo que desde aquí nos obligamos a que cualquier otro concepto que introduzcamos en adelante sea definido con total precisión a partir de los conceptos de "clase" y "pertenencia". Un lógico dirá que los conceptos de "clase" y "pertenencia" son los *conceptos primitivos* (o *conceptos no definidos*) de la teoría de conjuntos.

La forma de hablar con total rigor de unos conceptos no definidos es a través de *axiomas.* Vamos a postular que las clases y la pertenencia de las que nos proponemos hablar (sean lo que sean) satisfacen unos axiomas y, del mismo modo que nos hemos comprometido a no introducir nuevos conceptos sin definirlos con todo rigor a partir de los conceptos primitivos de clase y conjunto (o, más en general, de otros conceptos previamente definidos) nos comprometemos también a no afirmar nada sobre las clases y la pertenencia (o sobre los conceptos que introduzcamos en adelante) que no pueda ser demostrado lógicamente con todo rigor a partir de los axiomas establecidos.

Para ilustrar estos propósitos empezamos dando la definición de conjunto:

Definición 1.1 Diremos que una clase es un *conjunto* si pertenece al menos a otra clase, es decir:

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

Notemos que en la formalización de esta definición hemos escrito "existe un B tal que A pertenece a B". No necesitamos especificar de ninguna forma que B es una clase, pues todos los objetos de los que vamos a hablar son clases.

El primer axioma que adoptamos es el siguiente:

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

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

Es el axioma de extensionalidad el que nos legitima a pensar en las clases como colecciones de elementos (de clases, concretamente), pues si dos clases tienen los mismos elementos (es decir, si todo elemento de una lo es de la otra y viceversa, como dice la hipótesis del axioma) entonces ambas determinan la misma colección de objetos, y lo que dice el axioma es que si dos clases determinan la misma colección de objetos, entonces son una misma clase. En otros términos: una clase no es ni más ni menos que la colección de clases que determina mediante la relación de pertenencia.

Veamos una segunda definición:

Definición 1.2 Diremos que una clase A es una *subclase* de una clase B (o un *subconjunto,* si es que A es un conjunto) si todo elemento de A es también un elemento de B, es decir,

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

Observemos que $A \subset B$ se cumple en particular si $A = B$. Cuando queramos indicar que A es una subclase de B distinta de la propia B escribiremos

$$A \subsetneq B \equiv A \subset B \land A \neq B.$$

Veamos ahora un ejemplo elemental de teorema:

Teorema 1.3 *Se cumple:*

a) $\bigwedge A\ A \subset A$,

b) $\bigwedge AB(A \subset B \land B \subset A \rightarrow A = B)$,

c) $\bigwedge ABC(A \subset B \land B \subset C \rightarrow A \subset C)$.

DEMOSTRACIÓN: Observemos que los teoremas a) y c) no requieren el axioma de extensionalidad, es decir, son teoremas lógicos que se deducen de las definiciones sin necesidad de ninguna hipótesis específica sobre las clases. Por ejemplo, para demostrar c) suponemos $A \subset B \land B \subset C$ y, para probar $A \subset C$ tomamos una clase $x \in A$, de modo que, como $A \subset B$, podemos afirmar que $x \in B$ y, como $B \subset C$, podemos afirmar que $x \in C$. Esto prueba que $x \in A \rightarrow x \in C$ y, como esto vale para toda clase x, concluimos que $A \subset C$.

En cambio, el teorema b) requiere el axioma de extensionalidad (y de hecho es equivalente a él). Si suponemos que $A \subset B \land B \subset A$, 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 $A = B$. ■

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, pero 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 segundo axioma es el más delicado desde un punto de vista técnico:

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

$$\bigvee A \bigwedge x(x \in A \leftrightarrow \operatorname{cto} x \land \phi(x)).$$

Naturalmente, aquí debemos especificar qué queremos decir por "propiedad normal". Ante todo, cuando decimos que $\phi(x)$ es una propiedad queremos decir, más concretamente, que es una propiedad definible exclusivamente a partir de los conceptos de clase y pertenencia mediante los conectores lógicos ("y", "o", "si y sólo si", etc.) y los cuantificadores ("para todo" y "existe") (o de otros conceptos definidos previamente en estas condiciones), entendiendo que pueden aparecer más variables además de la x. Enseguida veremos ejemplos. Que la propiedad sea normal significa que los 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".

Antes de discutir más a fondo las sutilezas de este axioma, vamos a poner sobre el papel ejemplos concretos, pero primero observemos que el axioma de comprensión puede ser mejorado:

Teorema 1.4 *En las condiciones del axioma de comprensión, se cumple*

$$\overset{1}{\bigvee} A \bigwedge x(x \in A \leftrightarrow \operatorname{cto} x \land \phi(x)).$$

DEMOSTRACIÓN: Se trata de probar que existe una única clase A cuyos elementos son los conjuntos que cumplen $\phi(x)$. La existencia de tal clase la proporciona el axioma de comprensión. Para probar que es única suponemos que una clase B cumple lo mismo, es decir,

$$\bigwedge x(x \in A \leftrightarrow \operatorname{cto} x \land \phi(x)) \land \bigwedge x(x \in B \leftrightarrow \operatorname{cto} x \land \phi(x)).$$

Es claro que de aquí se deduce que

$$\bigwedge x(x \in A \leftrightarrow x \in B),$$

y el axioma de extensionalidad nos da entonces que $A = B$, es decir, sólo puede haber una clase que cumpla la propiedad considerada. ■

Cuando hay una única clase que cumple una propiedad, la lógica nos permite introducir un nombre para ella. En este caso:

Definición 1.5 $\{x \mid \phi(x)\} \equiv A | \bigwedge x(x \in A \leftrightarrow \operatorname{cto} x \land \phi(x))$,

es decir, llamamos $\{x \mid \phi(x)\}$ a la única clase cuyos elementos son los conjuntos x que cumplen $\phi(x)$.

Por ejemplo, ahora podemos definir la *unión,* la *intersección,* el *complemento* y la *diferencia* de clases como

$$A \cup B \equiv \{x \mid x \in A \lor x \in B\}, \qquad A \cap B \equiv \{x \mid x \in A \land x \in B\},$$
$$\overline{A} \equiv \{x \mid x \notin A\}, \qquad A \setminus B \equiv \{x \mid x \in A \land x \notin B\},$$

respectivamente.

Tenemos así cuatro ejemplos de aplicación del axioma de comprensión. En la definición de la unión estamos tomando $\phi(x) \equiv x \in A \lor x \in B$, que es una propiedad definida exclusivamente en términos de la pertenencia y un signo lógico (la disyunción), en la que, además de la variable x, figuran las variables auxiliares A y B. Como no aparecen cuantificadores, la propiedad es normal y el axioma es aplicable. Lo mismo vale para los otros tres ejemplos.

Definimos ahora dos ejemplos concretos de clases, la *clase universal* y la *clase vacía:*

$$V \equiv \{x \mid x = x\}, \qquad \varnothing \equiv \{x \mid x \neq x\}.$$

Obviamente, como ningún conjunto es distinto de sí mismo, tenemos que $\bigwedge x\, x \notin \varnothing$. Más aún, la clase vacía es la única clase con esta propiedad, es decir:

$$\bigwedge A(\bigwedge x\, x \notin A \rightarrow A = \varnothing).$$

Esto es una consecuencia del axioma de extensionalidad, pues si una clase A no tiene elementos, entonces tiene los mismos elementos que la clase vacía (ninguno), luego ambas clases son la misma.

Respecto de la clase universal, es muy importante tener presente que, aunque toda clase A cumple $A = A$, eso no significa que toda clase A cumpla $A \in V$. Recordemos que, en general, los elementos de una clase $\{x \mid \phi(x)\}$ no son todas las clases que cumplen $\phi(x)$, sino todos los conjuntos que cumplen $\phi(x)$. Para pertenecer a $\{x \mid \phi(x)\}$ no basta con cumplir la propiedad $\phi(x)$, sino que se requiere además ser un conjunto. En nuestro caso, la clase universal está formada por todos los conjuntos que cumplen $x = x$, es decir, se trata de "la clase de todos los conjuntos" (pero no de la clase de todas las clases). Así pues:

$$\bigwedge x(x \in V \leftrightarrow \operatorname{cto} x).$$

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

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

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 $x \in \varnothing \rightarrow x \in A$ se cumple trivialmente (no es posible encontrar un conjunto x que cumpla $x \in \varnothing \land x \notin A$).

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

Nota Los conceptos que acabamos de introducir verifican 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

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

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 1.3 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 1.3 b). ■

A partir de los axiomas de extensionalidad y comprensión no es posible probar que $V \neq \varnothing$, es decir, no es posible probar que existan conjuntos. Por ello introducimos ahora un axioma que postula la existencia de un conjunto:

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 $V \neq \varnothing$.

Podemos definir unos conceptos más generales de unión e intersección:

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

Observemos que aquí usamos la notación $\bigvee y \in A\,\phi(y)$ como abreviatura de $\bigvee y(y \in A \wedge x \in y)$, es decir, "existe una clase y en A tal que $\phi(y)$". Ahora bien, la condición $y \in A$ supone implícitamente que y es un conjunto (pues estamos diciendo que pertenece a otra clase), luego esto es equivalente a $\bigvee y(\mathrm{cto}\, y \wedge y \in A \wedge \phi(y))$.

Similarmente, $\bigwedge y \in A\,\phi(y)$ es una abreviatura por $\bigwedge y(y \in A \rightarrow \phi(y))$, que a su vez es equivalente a $\bigwedge y(\mathrm{cto}\, y \wedge y \in A \rightarrow \phi(y))$, luego las cuantificaciones de la forma $\bigvee y \in A$ o $\bigwedge y \in A$ son cuantificaciones sobre conjuntos y determinan propiedades normales (supuesto que lo que vaya a continuación sea normal).

Estas consideraciones generales justifican 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 $\bigwedge y \in \varnothing\, y \in x$, pues no es posible encontrar un $y \in \varnothing$ que no cumpla $y \in x$, y esto significa que $y \in \bigcap\varnothing$, 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. ■

Veamos ahora un ejemplo que muestra la necesidad de distinguir entre clases y conjuntos. Definimos la *clase de Russell* como

$$R \equiv \{x \mid x \notin x\},$$

es decir, se trata de la clase de todos los conjuntos que no se pertenecen a sí mismos. La propiedad $x \notin x$ es normal (trivialmente, porque no tiene cuantificadores) luego el axioma de comprensión justifica la existencia de R.

Si no distinguiéramos entre clases y conjuntos, y pretendiéramos haber definido "el conjunto de todos los conjuntos que no se pertenecen a sí mismos" tendríamos una contradicción, pues cabría plantearse si el "conjunto" R se pertenece o no a sí mismo, y las dos opciones resultan contradictorias: si $R \in R$ entonces R debería ser uno de los "conjuntos que no se pertenecen a sí mismos", y concluiríamos que $R \notin R$, en contra de lo supuesto. Si, por el contrario, suponemos que $R \notin R$, entonces R sería un "conjunto que no se pertenece a sí mismo" y deberíamos concluir que $R \in R$, en contradicción con lo supuesto.

Esta paradoja se conoce como la "paradoja de Russell", y no afecta a la teoría de conjuntos en los términos que la estamos presentando, pues en nuestro contexto se reduce al teorema siguiente:

Teorema 1.6 $\neg\,\mathrm{cto}\,R$.

DEMOSTRACIÓN: Observemos que $R \notin R$, pues si se cumpliera $R \in R$ por definición de R resultaría que $R \notin R$ y tendríamos una contradicción. Si R fuera un conjunto, entonces tendríamos $\mathrm{cto}\,R \land R \notin R$, es decir, R sería un conjunto que no se pertenece a sí mismo, y esto implicaría $R \in R$, con lo que tendríamos una contradicción. Así pues, R no puede ser un conjunto. ■

Las clases que no son conjuntos se llaman *clases propias*. Acabamos de probar que la clase de Russell es una clase propia, y que además cumple $R \notin R$.

Si no fuera por la distinción entre clases y conjuntos, que hace que $R \notin R$ no obligue necesariamente a que $R \in R$, tendríamos una contradicción.

Notemos que, como $\varnothing$ es un conjunto que no se pertenece a sí mismo, se cumple que $\varnothing \in R$, luego $R \neq \varnothing$. Ahora es claro también que la noción de clase no puede identificarse con la de "colección de objetos", pues, admitiendo que existan clases que cumplen los axiomas que estamos suponiendo, tenemos que $\varnothing$ y R son dos clases que forman una "colección de dos clases", pero tal colección no se corresponde con ninguna clase, en el sentido de que no existe ninguna clase cuyos elementos sean exactamente $\varnothing$ y R, pues para que ello fuera posible R debería ser un conjunto y no lo es.

Así pues, siempre podemos pensar en colecciones de objetos (de clases, concretamente) que van más allá de las colecciones que podemos expresar mediante clases. 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.

Nota El lector se habrá preguntado sin duda por qué hemos impuesto la condición de normalidad en el axioma de comprensión o, equivalentemente, qué problema habría en admitir que cualquier propiedad, normal o no, define una clase. La respuesta es que no habría ningún problema. 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, es decir, 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 1.7 Dadas dos clases x e y, definimos el *par (desordenado)* formado por ellas como

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

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 $\bigwedge xy\ (\mathrm{cto}\, x \land \mathrm{cto}\, y \rightarrow \mathrm{cto}\{x, y\})$.

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:

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

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

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

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 1.8 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 1.9 *Si x, y, u, v son conjuntos, entonces*

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

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 $y = u \lor y = v$, pero no puede ser $y = u = x$, luego tiene que ser $y = v$. ■

Usaremos la notación

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

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

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

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

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

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 1.11 Definimos el *dominio* y el *rango* de una clase F como las clases[1]

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

Diremos que F es *unívoca* si cumple

$$\operatorname{Un} F \equiv \bigwedge xyz(\operatorname{cto} x \land \operatorname{cto} y \land \operatorname{cto} z \land (x, y) \in F \land (x, z) \in F \rightarrow y = z).$$

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

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

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

$$F : A \longrightarrow B \equiv \operatorname{Un} F \land \mathcal{D}F = A \land \mathcal{R}F \subset B.$$

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

$$F(x) \equiv y \mid (\operatorname{cto} y \land (x, y) \in F).$$

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 $F : A \longrightarrow C$.

[1]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.

Definimos:

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

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 1.12 *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 1.13 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

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

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

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

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

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

a) Si $F \circ G = I_A$ entonces F es inyectiva y G suprayectiva.

b) Si además $G \circ F = I_B$ entonces F y G son biyectivas y $G = F^{-1}$.

Demostración: a) 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 $G(y) = G(F(x)) = (F \circ G)(x) = I_A(x) = x$.

b) Aplicando a) 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 1.12 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

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

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.[2] 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

[2] 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 $\bigwedge x \in A\ \operatorname{cto} t(x)$, entonces

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

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, $t(x) \equiv \{x\}$.

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

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

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.

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.*[3]

Como primera consecuencia obtenemos:

[3]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:

$$\bigwedge FA(\operatorname{cto} A \land \operatorname{Un} F \rightarrow \bigvee B(\operatorname{cto} B \land \bigwedge v(v \in B \leftrightarrow \bigvee u \in A\,(u, v) \in F))).$$

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

Teorema 1.15 *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

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

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

Como consecuencia:

Teorema 1.16 *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:

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

En particular:

Teorema 1.17 *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 $\bigcup\limits_{i \in I} X_i$

---

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 1.15.

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 1.15. 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 1.18 *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 1.15 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 1.18 hemos usado un caso particular de la primera de las propiedades siguientes, cuya prueba no ofrece dificultad:

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

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, $\bigcap\limits_{i\in\varnothing} X_i = X$, con lo que las igualdades anteriores valen incluso si $I = \varnothing$. ■

Una consecuencia sencilla de los teoremas precedentes es la siguiente:

Teorema 1.19 *Si $R \subset V \times V$, entonces*

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

DEMOSTRACIÓN: La aplicación $R \longrightarrow \mathcal{D}R$ dada por[4] $(x, y) \mapsto x$ 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 1.20 *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:

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

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) $\bigwedge X(\operatorname{cto} X \to \operatorname{cto} \mathcal{P}X)$.

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

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

Si B es una clase propia, tenemos que $A^B = \varnothing$, pues ninguna $f : A \longrightarrow B$ 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 $f : A \longrightarrow B$, pues todas ellas son conjuntos.

[4]Más concretamente, nos referimos a

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

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.

Teorema 1.21 $\bigwedge AB(\operatorname{cto} A \land \operatorname{cto} B \rightarrow \operatorname{cto} A^B)$

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

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

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 cuyos único concepto no definido es la relación $\in$ de pertenencia (entre clases) y cuyos axiomas son los siguientes:

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

$(*)$ para toda propiedad 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.[5] 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 Relaciones

Continuamos ahora con el propósito principal de este capítulo, que es presentar el lenguaje básico de la teoría de conjuntos. Ya hemos introducido el vocabulario relacionado con las funciones, y ahora vamos a hacer lo propio con las relaciones. La definición conjuntista de "relación" es muy simple:

Definición 1.22 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.

Diremos que una relación R en una clase A es:

a) *Reflexiva* si $\bigwedge x \in A\ x\,R\,x$,

b) *Irreflexiva* si $\bigwedge x \in A\ \neg x\,R\,x$,

c) *Simétrica* si $\bigwedge xy \in A\,(x\,R\,y \rightarrow y\,R\,x)$,

d) *Antisimétrica* si $\bigwedge xy \in A\,(x\,R\,y \land y\,R\,x \rightarrow x = y)$

e) *Asimétrica* si $\bigwedge xy \in A\,(x\,R\,y \rightarrow \neg y\,R\,x)$

f) *Transitiva* si $\bigwedge xyz \in A\,(x\,R\,y \land y\,R\,z \rightarrow x\,R\,z)$

g) *Conexa* si $\bigwedge xy \in A\,(x\,R\,y \lor y\,R\,x)$

h) *Débilmente conexa* si $\bigwedge xy \in A(x\,R\,y \lor y\,R\,x \lor x = y)$

[5] 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.

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

a) $a\,R\,b \leftrightarrow [a]_R = [b]_R$,

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

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[6]

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

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).

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

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:

$$\bigwedge a \in A\, a \leq a, \quad \bigwedge ab \in A(a \leq b \land b \leq a \rightarrow a = b),$$

$$\bigwedge abc \in A(a \leq b \land b \leq c \rightarrow a \leq c).$$

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

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

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

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

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

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 $a > b \equiv b < a$.

Cuando digamos que $(A, \leq)$ es una clase total o parcialmente ordenada querremos decir[7] 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:

a) $M \in A$ es una *cota superior* de B si $\bigwedge x \in B\ x \leq M$,

b) $m \in A$ es una *cota inferior* de B si $\bigwedge x \in B\ m \leq x$,

c) $M \in A$ es un *maximal* de B si $M \in B$ y $\bigwedge x \in B(M \leq x \rightarrow M = x)$.

d) $m \in A$ es un *minimal* de B si $m \in B$ y $\bigwedge x \in B(x \leq m \rightarrow x = m)$.

[7] 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.

e) $M \in A$ es el *supremo* de B si M es una cota superior de B y $\bigwedge x \in A(x$ es una cota superior de $B \to M \leq x)$.

f) $m \in A$ es el *ínfimo* de B si m es una cota inferior de B y $\bigwedge x \in A(x$ es una cota inferior de $B \to x \leq m)$.

g) $M \in A$ es el *máximo* de B si $M \in B$ y M es una cota superior de B.

h) $m \in A$ es el *mínimo* de B si $m \in B$ y m es una cota inferior de B.

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 $X \subsetneq Y$.

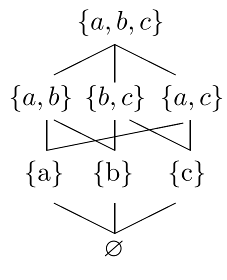
Respecto de esta relación, $\mathcal{P}A$ tiene como mínimo elemento a $\varnothing$. Si A es un conjunto, entonces $\mathcal{P}A$ tiene como máximo elemento a A, pero si A no es un conjunto, entonces $\mathcal{P}A$ no tiene máximo elemento, pues dado cualquier $X \in \mathcal{P}A$, será $X \subsetneq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

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

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

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

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:

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

b) 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.

c) 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:

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

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

c) 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[8] 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 siguiente 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.

[8]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.

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 1.24 (Principio de inducción para clases bien ordenadas) *Si* $(A, \leq)$ *es una clase bien ordenada y* $B \subset A$ *cumple* $\bigwedge x \in A(A_x^< \subset B \rightarrow x \in B)$, *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, 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 1.25 *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 1.26 *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[9] $F : (A, \leq) \longrightarrow (A_x^<, \leq)$. 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 1.27 *Si dos clases bien ordenadas son semejantes, entonces existe una única semejanza entre ellas.*

[9]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.

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 1.25 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 siguiente estaremos en condiciones de razonar más cómodamente sobre ellas.

1.6 Leyes de composición interna

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

Definición 1.28 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

a) es *asociativa* si $\bigwedge abc \in A\ (a * b) * c = a * (b * c)$

b) es *conmutativa* si $\bigwedge ab \in A\ a * b = b * a$

c) 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[10] $(A, +, \cdot)$, donde $+$ y $\cdot$ son operaciones en A (a las que llamaremos *suma* y *producto,* respectivamente, de modo que se cumplen las propiedades siguientes:

[10]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.

a) 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 $-a$.

b) 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 $a + (-b) \equiv a - b$.

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:

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

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

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

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

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

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:

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

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

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

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 además las dos siguientes *propiedades de compatibilidad:*

a) $\bigwedge abc \in A\ (a \leq b \rightarrow a + c \leq b + c)$

b) $\bigwedge ab \in A\ (a \geq 0 \land b \geq 0 \rightarrow ab \geq 0)$

Diremos que un elemento a de un anillo ordenado es

a) *positivo* si $a \geq 0$,

b) *estrictamente positivo* si $a > 0$,

c) *negativo* si $a \leq 0$,

d) *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:

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

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:

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

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:

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

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:

a) $|a| = 0 \leftrightarrow a = 0$,

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

c) $|ab| = |a||b|$,

d) $|-a| = |a|$,

e) $||a| - |b|| \leq |a - b|$.

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 $||a| - |b|| \leq |a - b|$. ■

Cuerpos de cocientes Como muestra de que NBG* es suficiente para formalizar los razonamientos conjuntistas elementales vamos a demostrar un resultado algebraico, según el cual todo dominio íntegro puede extenderse hasta un cuerpo.

En todo este apartado $(D, +, \cdot)$ será un dominio íntegro prefijado. 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.

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 1.23 a) 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,

$$+ \equiv \{((x, y), z) \in (K_D \times K_D) \times K_D \mid \bigvee abcd \in D(x = a/b \land y = c/d$$
$$\land\, z = (ad + bc)/bd)\}.$$

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

$$i_D(a+b) = i_D(a) + i_D(b), \qquad i_D(ab) = i_D(a)i_D(b).$$

Conviene introducir algunos conceptos para describir esta situación:

Definición 1.29 Una aplicación $f : A \longrightarrow B$ entre dos anillos es un *homomorfismo de anillos* si cumple[11]

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

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.

[11]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 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.

En estos términos, lo que hemos probado es que $i_D : D \longrightarrow K$ es un monomorfismo de dominios íntegros.

En general, 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.

En nuestro contexto, 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

$$x \leq y \equiv \bigvee abcd \in D(c > 0 \land d > 0 \land x = \frac{a}{b} \land y = \frac{c}{d} \land ad \leq bc).$$

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.

Definición 1.30 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

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

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.

En nuestro contexto, es claro que $i_D : D \longrightarrow K_D$ 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.

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

Definición 1.31 Sea A un anillo conmutativo y unitario. Un *ideal* de A es un conjunto $I \subset A$ tal que:

a) $0 \in I$,

b) $\bigwedge xy \in I\ x + y \in I$,

c) $\bigwedge a \in A \bigwedge b \in I\ ab \in I$.

Por ejemplo, si $x \in A$ el conjunto $(x) = \{ax \mid a \in A\}$ de los múltiplos de x es claramente un ideal[12] 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 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).

[12] 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 $I = (x)$.

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 1.32 *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.

Definición 1.33 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

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

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

Teorema 1.34 *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

Ordinales

En el capítulo precedente hemos presentado el vocabulario básico de la teoría de conjuntos, pero sin presentar realmente ningún conjunto "interesante" al que aplicar dicho vocabulario. El lector puede pensar provisionalmente a modo de motivación que el propósito de este capítulo es construir los números naturales, pero lo cierto es que el proceso de construcción que vamos a presentar nos proporcionará un concepto mucho más potente, el de número ordinal, de modo que los números naturales resultarán ser los ordinales finitos. Los ordinales representan el mismo papel respecto a conjuntos arbitrarios que los números naturales representan respecto de los conjuntos finitos y, bajo el axioma de regularidad, que presentaremos más adelante, se convierten en el "esqueleto" o el "armazón" de la clase universal V.

2.1 La construcción de los ordinales

Nos marcamos, pues, como objetivo provisional construir los números naturales en el seno de NBG*. Tienen que ser ciertos conjuntos, de modo que el problema es realmente definir una sucesión de conjuntos a los que podamos llamar 0, 1, 2, 3, etc. Hay una elección muy natural: como 0 podemos tomar un (el) conjunto con cero elementos, de modo que $0 \equiv \varnothing$, como 1 podemos tomar un conjunto con un elemento, y la elección más simple es $1 \equiv \{0\}$, como 2 podemos tomar un conjunto con dos elementos, y la elección más simple es $2 = \{0, 1\}$, y así:

$$\begin{array}{ll}
0 = \varnothing, & 6 = \{0,1,2,3,4,5\}, \\
1 = \{0\}, & 7 = \{0,1,2,3,4,5,6\}, \\
2 = \{0,1\}, & 8 = \{0,1,2,3,4,5,6,7\}, \\
3 = \{0,1,2\}, & 9 = \{0,1,2,3,4,5,6,7,8\}, \\
4 = \{0,1,2,3\}, & \quad\cdots
\end{array}$$

El primer paso para formalizar esta idea es el siguiente:

Definición 2.1 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) $\bigwedge uv(u \in v \land v \in Y \rightarrow u \in Y)$.

Una clase Y es $\in$-*conexa* si cumple

$$\in\text{-conexa } Y \equiv \bigwedge uv \in Y(u \in v \lor v \in u \lor u = v).$$

Una clase Y está *bien fundada* si cumple

$$Y \text{ bien fundada} \equiv \bigwedge X(X \subset Y \land X \neq \varnothing \rightarrow \bigvee u \in X\ u \cap X = \varnothing).$$

Un conjunto u que cumpla $u \in X \land u \cap X = \varnothing$ 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.

[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.

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 $0, 1, 2, \ldots,$ de modo que necesitamos introducir más propiedades para quedarnos únicamente con los números naturales. Como respuesta provisional damos una nueva definición:

Definición 2.2 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

$$\Omega \equiv \{\alpha \mid \operatorname{cto} \alpha \land \operatorname{ordinal} \alpha\}$$

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.

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 2.3 *Si x es una clase bien fundada entonces*[2] $x \notin x$.

[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.

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 2.4 $0 \in \Omega \wedge \bigwedge x \in \Omega\ x' \in \Omega.$

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 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 2.5 *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 $\bigwedge uv(u \in v \land v \in x \rightarrow u \in x)$.

Si $u \in v \land v \in x$, tenemos $v \in x \land x \in Y$, 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,

$$u \cap \{u, v, x\} = \varnothing \quad \lor \quad v \cap \{u, v, x\} = \varnothing \quad \lor \quad x \cap \{u, v, x\} = \varnothing,$$

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 $u \in x \lor x \in u \lor u = x$, 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

$$\bigwedge \alpha\beta(\alpha \in \beta \land \beta \in \Omega \rightarrow \alpha \in \Omega),$$

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 2.6 *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 $u \in v \lor v \in u \lor u = v$, pero el caso $v \in u$ contradice la minimalidad de u, luego nos queda $u \in v \lor u = v$, 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 2.7 *Si X, Y son ordinales, entonces $X \subset Y \leftrightarrow X \in Y \lor X = Y$.*

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 $z \in u \lor u \in z \lor z = u$. 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 2.8 *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 $u \in X \land u \in Y$, $u \subset X \land u \subset Y$, luego $u \subset X \cap Y$. ■

De aquí deducimos una propiedad nada trivial:

Teorema 2.9 *Si X e Y son ordinales, entonces $X \in Y \lor Y \in X \lor X = Y$.*

DEMOSTRACIÓN: $X \cap Y$ es un ordinal, $X \cap Y \subset X$ y $X \cap Y \subset Y$. Por el teorema 2.7 tenemos $(X \cap Y \in X \lor X \cap Y = X) \land (X \cap Y \in Y \lor X \cap Y = Y)$. Esto nos da cuatro casos:

$$(X \cap Y \in X \land X \cap Y \in Y) \lor (X \cap Y \in X \land X \cap Y = Y)$$

$$\lor (X \cap Y = X \land X \cap Y \in Y) \lor (X \cap Y = X \land X \cap Y = Y),$$

o sea $X \cap Y \in X \cap Y \quad \lor \quad Y \in X \quad \lor \quad X \in Y \quad \lor \quad X = Y$. El primer caso se descarta por el teorema 2.3. ■

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,

$$\bigwedge \alpha\beta \in \Omega\ (\alpha \in \beta \lor \beta \in \alpha \lor \alpha = \beta),$$

luego la clase Ω es $\in$-conexa (y ya habíamos probado que era transitiva). De hecho, se cumple algo más fuerte:

Teorema 2.10 *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 2.11 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 2.3. ∎

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 2.12 *Si Y es un ordinal, o bien $Y \in \Omega$, o bien $Y = \Omega$.*

DEMOSTRACIÓN: Basta aplicar el teorema 2.9, 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 2.13 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 2.6, sabemos que $(\Omega, \leq)$ es una clase bien ordenada. Así pues, $\alpha \leq \beta$ es equivalente a $\alpha \subset \beta$.

El teorema 2.7 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 2.14 *Se cumple:*

a) 0 *es el mínimo ordinal.*

b) Si α es un ordinal, entonces α' también lo es, y es el mínimo ordinal mayor que α (es decir, $\bigwedge\beta \in \Omega\ (\alpha < \beta \rightarrow \alpha' \leq \beta)$).

c) Todo conjunto de ordinales $A \subset \Omega$ tiene supremo $\sigma = \bigcup A$.

DEMOSTRACIÓN: a) ya hemos probado que 0 es un ordinal, y es el mínimo porque el conjunto vacío está contenido en cualquier conjunto.

b) 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 $\alpha' \leq \beta$.

c) 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 2.15 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

$$\alpha \text{ límite} \equiv 0 \in \alpha \land \bigwedge \delta \in \alpha\ \delta' \in \alpha.$$

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 2.16 Diremos que un conjunto n es un *número natural* si

$$n \in \Omega \land \bigwedge m \in \Omega (m \leq n \rightarrow m = 0 \lor \bigvee r \in m\ m = r').$$

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 2.17 *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 $u \in v \land v \in \omega$, 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 2.18 (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) $\bigwedge mn \in \omega\ (m' = n' \rightarrow m = n)$,

5) $\bigwedge A(A \subset \omega \wedge 0 \in A \wedge \bigwedge n \in A\ n' \in A \rightarrow A = \omega)$.

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. ∎

Está claro que los axiomas de Peano son propiedades que los matemáticos usan cuando tratan con números naturales, luego cualquier definición de número natural aceptable para un matemático debe dar lugar a un conjunto (o, al menos, a una clase) que, con un cero y una operación "siguiente" definidos adecuadamente satisfaga los axiomas de Peano. En la sección siguiente (teorema 2.24) demostraremos que los elementos de cualquier clase que satisfaga los axiomas de Peano se corresponden biunívocamente con los números naturales que hemos definido, de modo que dos definiciones alternativas de los números naturales (aceptables, en cuanto que cumplan los axiomas de Peano) corresponden simplemente a elecciones distintas de los conjuntos concretos con los que estamos representando cada número natural. Por ejemplo, en lugar de haber tomado $0 = \varnothing$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, etc., podríamos haber optado por $0 = \varnothing$, $1 = \{0\}$, $2 = \{1\}$, $3 = \{2\}$, etc. y así tendríamos otra clase de números naturales, distinta, pero equivalente a la que hemos elegido.

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 2.19 *Las afirmaciones siguientes son equivalentes:*

a) $\bigvee x(\mathrm{cto}\, x \land 0 \in x \land \bigwedge u \in x\ u' \in x)$,

b) $\mathrm{cto}\, \omega$,

c) $\omega \in \Omega$,

d) ω *es un ordinal límite,*

e) Existe un ordinal límite.

DEMOSTRACIÓN: Si x es un conjunto que cumple a), entonces $y = x \cap \omega$ está en las condiciones del quinto axioma de Peano, que nos da que $x \cap \omega = \omega$, es decir, que $\omega \subset x$, luego ω es un conjunto y tenemos b). A su vez, b) implica trivialmente c), que a su vez implica d), por el segundo axioma de peano. Obviamente d) implica e), y un ordinal límite cumple lo requerido para x en a). ■

Las afirmaciones del teorema anterior no pueden demostrarse a partir de los axiomas que hemos considerado hasta ahora, lo que nos lleva a un nuevo axioma:

Axioma de infinitud (AI) $\mathrm{cto}\, \omega$.

Naturalmente, cualquiera de las afirmaciones del teorema anterior sirve como versión alternativa del axioma de infinitud. De momento seguiremos trabajando en NBG*, es decir, sin suponer AP o AI salvo que lo indiquemos explícitamente.

2.2 Inducción y recursión transfinita

Los ordinales son una poderosa herramienta fundamental en el estudio de los conjuntos gracias a los teoremas que vamos a demostrar en esta sección. Empezamos con el principio de inducción, que no es sino un caso particular del teorema 1.24:

Teorema 2.20 (Inducción transfinita)

$$\bigwedge A(\bigwedge \alpha(\alpha \subset A \rightarrow \alpha \in A) \rightarrow \Omega \subset A).$$

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 1.24:

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 2.21 (Inducción transfinita)

$$\bigwedge A(0 \in A \wedge \bigwedge \alpha(\alpha \in A \rightarrow \alpha' \in A)$$

$$\wedge \bigwedge \lambda(\bigwedge \delta(\delta < \lambda \rightarrow \delta \in A) \rightarrow \lambda \in A) \rightarrow \Omega \subset A).$$

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 2.22 (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 $\bigwedge \delta(\delta < \lambda \rightarrow f_\delta$ 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

$$f(\delta) = f_{\delta'}(\delta) = G(f_{\delta'}|_\delta) = F(f|_\delta).$$

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 2.23 *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

$$F(\lambda) = \bigcup_{\delta<\lambda} F(\delta) = \bigcup_{\delta<\lambda} F^*(\delta) = F^*(\lambda).$$

■

Los números naturales y los axiomas de Peano Ahora estamos en condiciones de justificar que los axiomas de Peano caracterizan a los números naturales. El resultado básico es el siguiente:

Teorema 2.24 *Sea $\mathbb{N}$ una clase, sea $n_0 \in \mathbb{N}$ y sea $s : \mathbb{N} \longrightarrow \mathbb{N}$ una aplicación de modo que se cumplan los axiomas de Peano, es decir:*

1) $n_0 \in \mathbb{N}$,

2) $\bigwedge n \in \mathbb{N}\ s(n) \in \mathbb{N}$,

3) $\bigwedge n \in \mathbb{N}\ s(n) \neq n_0$,

4) $\bigwedge mn \in \mathbb{N}\ (s(m) = s(n) \rightarrow m = n)$,

5) $\bigwedge A(A \subset \mathbb{N} \wedge n_0 \in A \wedge \bigwedge n \in A\ s(n) \in A \rightarrow A = \mathbb{N})$.

Entonces existe una única aplicación $F : \omega \longrightarrow \mathbb{N}$ biyectiva tal que $F(0) = n_0$ y

$$\bigwedge n \in \omega\ F(n') = s(F(n)).$$

Demostración: La existencia de $F : \omega \longrightarrow \mathbb{N}$ viene dada por el teorema de recursión, sin más que tomar

$$G(f) = \begin{cases} n_0 & \text{si } \mathcal{D}f = 0, \\ s(f(n)) & \text{si } \mathcal{D}f = n+1. \end{cases}$$

Para probar que F es inyectiva, suponemos por reducción al absurdo que no lo es, de modo que existe un $n \in \omega$ tal que $\bigvee m < n\ F(m) = F(n)$. Tomemos el mínimo n posible y sea $m < n$ tal que $F(m) = F(n)$.

Como $0 \leq m < n$, tiene que ser $n = v'$, para cierto $u \in \omega$, con lo que $F(n) = s(F(v)) \neq n_0$, por el tercer axioma de Peano. Por lo tanto $m \neq 0$, pues $F(m) = F(n) \neq n_0$, luego $m = u'$, para cierto $u \in \omega$, luego tenemos que $s(F(u)) = F(m) = F(n) = s(F(v))$, luego $F(u) = F(v)$, por el cuarto axioma de Peano. Como $u' < v'$, también se cumple $u < v$, luego $\bigvee u < v\ F(u) = F(v)$ y por lo tanto $v < n$ cumple la misma propiedad que, supuestamente, n era el mínimo en cumplir, contradicción.

Así pues, F es inyectiva. Para probar que es suprayectiva observamos que $A = F[\omega] \subset \mathbb{N}$ cumple $n_0 \in A$ y $\bigwedge n \in A\ s(n) \in A$, pues si $n \in A$, existe un $m \in \omega$ tal que $n = F(m)$, luego $s(n) = s(F(m)) = F(m') \in A$. Por el quinto axioma de Peano (para $\mathbb{N}$), tenemos que $F[\omega] = \mathbb{N}$.

Concluimos que F es biyectiva. La unicidad la da el teorema de recursión. ■

En definitiva, lo que afirma el teorema anterior es que si $\mathbb{N}$ es cualquier clase que cumpla los axiomas de Peano, sus elementos forman una sucesión $\{n_i\}_{i\in\omega}$, donde aquí estamos llamando $n_i \equiv F(i)$, y de forma que n_0 es el "cero" de $\mathbb{N}$.

Por lo tanto, tal y como explicábamos tras el teorema 2.18, tomar una clase u otra como clase de los números naturales sólo supone elegir unos conjuntos concretos u otros como representación de los números naturales.

Otra consecuencia del teorema anterior es que el axioma de infinitud es equivalente a la existencia de un conjunto $\mathbb{N}$ que (con un cierto n_0 y una cierta función s) cumple los axiomas de Peano, pues si existe tal conjunto, el teorema anterior nos da una biyección $F : \omega \longrightarrow \mathbb{N}$ que implica, por reemplazo, que ω es un conjunto. Más aún:

Teorema 2.25 *El axioma de infinitud equivale a que exista un conjunto N con una aplicación $s : N \longrightarrow N$ inyectiva y no suprayectiva.*

Demostración: Ciertamente, si se cumple el axioma de infinitud basta tomar $N = \omega$ y $s(n) = n'$. Recíprocamente, si existe N, la no suprayectividad de s significa que existe un $n_0 \in N$ tal que $\bigwedge n \in N\ s(n) \neq n_0$. Por lo tanto N cumple claramente los cuatro primeros axiomas de Peano.

Ahora basta observar que en la prueba del teorema 2.24 sólo hemos usado que $\mathbb{N}$ cumple el quinto axioma de Peano para probar que F es suprayectiva, luego, en nuestro contexto podemos concluir que existe una aplicación inyectiva $F : \omega \longrightarrow N$, y esto implica que ω es un conjunto. ■

2.3 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 2.26 *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 1.26 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 $u < f(\gamma)$. ■

[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.

Definición 2.27 Llamaremos *ordinal* de un conjunto bien ordenado $(A, \leq)$ al único ordinal al cual es semejante. Lo representaremos por $\operatorname{ord}(A, \leq)$.

Conviene recordar que, por el teorema 1.26, si $\operatorname{ord}(A, \leq) = \alpha$, existe una única semejanza $f : (A, \leq) \longrightarrow \alpha$. Otra observación elemental es la siguiente:

Teorema 2.28 *Si B es un conjunto bien ordenado y $A \subset B$, entonces se cumple que* $\operatorname{ord} A \leq \operatorname{ord} B$.

DEMOSTRACIÓN: Sean $\alpha = \operatorname{ord} A$, $\beta = \operatorname{ord} B$ 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 1.26. ■

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:

Teorema 2.29 *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 $F = \bigcup\limits_{v \in A} F_v$, 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

---

[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.

$F(u) = f_v(u) < f_v(u') = F(u')$. Por último, F es suprayectiva, pues claramente $F[\Omega] = \bigcup\limits_{v\in A} \alpha_v$, 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). ■

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 2.30 Definimos el *orden canónico* en $\Omega \times \Omega$ como el orden dado por

$$(\alpha, \beta) \leq (\gamma, \delta) \leftrightarrow \text{máx}\{\alpha, \beta\} < \text{máx}\{\gamma, \delta\} \vee$$

$$(\text{máx}\{\alpha, \beta\} = \text{máx}\{\gamma, \delta\} \wedge \beta < \delta) \vee$$

$$(\text{máx}\{\alpha, \beta\} = \text{máx}\{\gamma, \delta\} \wedge \beta = \delta \wedge \alpha \leq \gamma).$$

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 $\text{máx}\{\gamma', \delta'\} \times \text{máx}\{\gamma', \delta'\}$. Por 2.29 existe una (única) semejanza $F : \Omega \times \Omega \longrightarrow \Omega$.

2.4 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 2.31 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 2.23 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 2.32 *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

$$\bigwedge \beta \in \Lambda (\alpha < \beta \rightarrow F(\alpha) < F(\beta))$$

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 1.26, es decir, si $F : \Lambda \longrightarrow \Lambda$ es normal, entonces $\bigwedge \alpha \in \Lambda\, \alpha \leq F(\alpha)$.

Teorema 2.33 *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 2.34 *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 $\alpha < G(F(\delta)) < G(F(\lambda))$. ■

2.5 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 $\alpha + \beta = \operatorname{ord}(\alpha \oplus \beta)$, 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 2.35 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 2.23. 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:

$$\bigwedge\alpha\beta\gamma(\beta < \gamma \rightarrow \alpha + \beta < \alpha + \gamma), \qquad \bigwedge\alpha\beta\, \beta \leq \alpha + \beta.$$

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 2.36 $\bigwedge\alpha\beta\gamma(\alpha \leq \beta \rightarrow \alpha + \gamma \leq \beta + \gamma)$.

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:

$$\bigwedge\alpha\beta\gamma\delta(\alpha \leq \beta \wedge \gamma < \delta \rightarrow \alpha + \gamma < \beta + \delta),$$

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:

$$\bigwedge \alpha\beta\gamma(\alpha + \beta = \alpha + \gamma \rightarrow \beta = \gamma).$$

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 2.37 $\bigwedge \alpha\beta\gamma\ ((\alpha + \beta) + \gamma = \alpha + (\beta + \gamma))$.

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 2.38 $\bigwedge mn \in \omega\ m + n = n + m$.

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 2.39 $\bigwedge \alpha\beta(\alpha \leq \beta \rightarrow \overset{1}{\bigvee}\gamma\ \alpha+\gamma = \beta)$.

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 2.40 $\bigwedge \alpha\beta\delta(\delta < \alpha+\beta \leftrightarrow \delta < \alpha \vee \bigvee \gamma < \beta\ \delta = \alpha+\gamma)$.

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 2.41 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:

$$\bigwedge\alpha\beta\gamma(\alpha < \beta \wedge \gamma \neq 0 \rightarrow \gamma \cdot \alpha < \gamma \cdot \beta)$$

Si multiplicamos por la derecha la desigualdad tiene que ser no estricta:

$$\bigwedge\alpha\beta\gamma(\alpha \leq \beta \rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma).$$

Esto se prueba exactamente igual que el resultado análogo para la suma. Combinando estas desigualdades tenemos:

$$\bigwedge\alpha\beta\gamma\delta(\alpha \leq \beta \wedge \gamma < \delta \wedge \beta \neq 0 \rightarrow \alpha \cdot \gamma < \beta \cdot \delta).$$

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 $\bigwedge n \in \omega(n \neq 0 \rightarrow n\omega = \omega)$.

Veamos ahora las propiedades algebraicas:

Teorema 2.42 $\bigwedge\alpha\beta\gamma\ \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

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 2.43 $\bigwedge \alpha\beta\gamma\ (\alpha\beta)\gamma = \alpha(\beta\gamma)$.

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 2.44 $\bigwedge mn \in \omega\ mn = nm$.

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 2.45 $\bigwedge \alpha\beta(\beta \neq 0 \to \overset{1}{\bigvee} \gamma\delta(\alpha = \beta\gamma + \delta \land \delta < \beta))$.

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 2.39 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 2.46 $\bigwedge \alpha\beta\epsilon\ (\epsilon < \alpha\beta \leftrightarrow \bigvee \gamma < \beta \bigvee \delta < \alpha\ \epsilon = \alpha\gamma + \delta)$

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 60, 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 Para caracterizar la exponenciación de ordinales en términos de conjuntos ordenados necesitamos el concepto de conjunto finito, que aún no hemos introducido, así que de momento nos limitaremos a dar la definición por recurrencia y más adelante (teorema 4.43) veremos la caracterización correspondiente.

[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

$$\gamma_1 < \gamma_2 \vee (\gamma_1 = \gamma_2 \wedge \delta_1 < \delta_2) \rightarrow \alpha\gamma_1 + \delta_1 < \alpha\gamma_2 + \delta_2.$$

Esto implica a su vez que $(a_1, b_1) < (a_2, b_2) \rightarrow f(a_1, b_1) < f(a_2, b_2)$.

Definición 2.47 Para cada ordinal $\alpha \neq 0$ definimos $\alpha^{(\ )} : \Omega \longrightarrow \Omega$ como la única función que cumple

$$\alpha^0 = 1 \land \bigwedge \beta\ \alpha^{\beta+1} = \alpha^\beta \cdot \alpha \land \bigwedge \lambda\ \alpha^\lambda = \bigcup_{\delta<\lambda} \alpha^\delta.$$

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 $\bigwedge \alpha\beta(\alpha \neq 0 \rightarrow \alpha^\beta \neq 0)$, 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.)

a) $\bigwedge \alpha\ 1^\alpha = 1$,

b) $\bigwedge \alpha\ \alpha^1 = \alpha$,

c) $\bigwedge \alpha\beta\gamma(\alpha < \beta \land 1 < \gamma \rightarrow \gamma^\alpha < \gamma^\beta)$,

d) $\bigwedge \alpha\beta\gamma(\alpha \leq \beta \rightarrow \alpha^\gamma \leq \beta^\gamma)$,

e) $\bigwedge \alpha\beta\gamma(\alpha \leq \beta \land 1 < \gamma \land \gamma^\alpha = \gamma^\beta \rightarrow \alpha = \beta)$,

f) $\bigwedge \alpha\beta\gamma\ \alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$,

g) $\bigwedge \alpha\beta\gamma\ (\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$.

Como siempre, una simple inducción prueba que la exponenciación de números naturales sea un número natural.

Ejercicio: (AI) Probar que $\bigwedge n \in \omega(1 < n \rightarrow n^\omega = \omega)$.

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

$$\bigwedge mnr \in \omega\ (mn)^r = m^r n^r.$$

2.6 Sumas finitas

Consideremos una clase A en la que hay definida una ley de composición interna $+ : A \times A \longrightarrow A$ con elemento neutro 0. En particular esto lo cumple $A = \Omega$ con la suma de ordinales (pero no suponemos que en general 0 sea el ordinal 0).

Para cada sucesión[6] $\{a_i\}_{i<n}$ en A, con $n \in \omega$, consideramos la única aplicación $n \longrightarrow A$ 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 $\sum\limits_{i<n} a_i \in A$.

Un poco más en general, si tenemos una sucesión $\{a_i\}_{i\in I}$ en A con $I \subset n$, para cierto $n \in \omega$, consideramos en I el orden usual de los ordinales, de modo que $\operatorname{ord} I = m \leq n$ (teorema 2.28). Tomamos entonces la (única) semejanza $s : m \longrightarrow I$ y consideramos la sucesión $\{a_{s(j)}\}_{j<m}$. Definimos

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

Es fácil ver que si $I = \varnothing$, entonces $\sum\limits_{i\in I} a_i = 0$, y si $I = J \cup \{m\}$, donde, m es el máximo de I (que existe, porque el ordinal de I es un número natural no nulo, y todo número natural no nulo tiene por máximo a su anterior), entonces

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

A partir de aquí podemos probar que si $+$ es asociativa y partimos $I = I_1 \cup I_2$ de modo que todo elemento de I_1 es menor que todo elemento de I_2, entonces

$$\sum_{i\in I} a_i = \sum_{i\in I_1} a_i + \sum_{i\in I_2} a_i.$$

En efecto, razonamos por inducción sobre el ordinal de I_2. Si es 0 es que $I_2 = \varnothing$ e $I = I_1$, con lo que la igualdad es trivial. Supuesto cierto cuando I_2 tiene ordinal k, supongamos que su ordinal es $k+1$. Entonces I_2 tiene un máximo elemento m, que será también el máximo de I. Sea $I_2' = I_2 \setminus \{m\}$. Entonces (y aquí usamos la asociatividad de $+$):

$$\sum_{i\in I} a_i = \sum_{i\in I_1\cup I_2'} a_i + a_m = \sum_{i\in I_1} a_i + \sum_{i\in I_2'} a_i + a_m = \sum_{i\in I_1} a_i + \sum_{i\in I_2} a_i.$$

A su vez podemos probar la generalización siguiente:

Teorema 2.48 (Propiedad asociativa generalizada) *Sea A una clase en la que hay definida una operación $+$ asociativa y con elemento neutro. Sea $\{I_i\}_{i<k}$ una familia de subconjuntos de un número natural n de manera que, si $i < j < k$, todo elemento de I_i es menor que todo elemento de I_j, sea $I = \bigcup\limits_{i<k} I_i$ y sea $\{a_i\}_{i\in I}$ una sucesión en A. Entonces,*

$$\sum_{j\in I} a_j = \sum_{i<k}\sum_{j\in I_i} a_j.$$

[6] Recordemos que esto significa simplemente que $a : n \longrightarrow A$.

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

$$\sum_{j\in \bigcup\limits_{i<m} I_i} a_j = \sum_{i<m}\sum_{j\in I_i} a_j.$$

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

$$\sum_{j\in \bigcup\limits_{i<m+1} I_i} a_j = \sum_{j\in \bigcup\limits_{i<m} I_i} a_j + \sum_{j\in I_m} a_j = \sum_{i<m}\sum_{j\in I_i} a_j + \sum_{j\in I_m} a_j = \sum_{i<m+1}\sum_{j\in I_i} a_j.$$

■

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

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

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.

Por ejemplo, si tenemos dos sucesiones de ordinales $\{\alpha_i\}_{i\in I}$ y $\{\beta_i\}_{i\in I}$ tales que $\bigwedge i \in I\ \alpha_i \leq \beta_i$, entonces $\sum\limits_{i\in I} \alpha_i \leq \sum\limits_{i\in I} \beta_i$. O también, si α es cualquier ordinal, se cumple $\alpha \sum\limits_{i\in I} \alpha_i = \sum\limits_{i\in I} \alpha\alpha_i$, etc.

Veamos una aplicación de estas sumas finitas:

Teorema 2.49 *Si $k > 1$ es un número natural, para cada $m \in \omega$ 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: Observemos en primer lugar que, como la función $k^{()}$ es normal (y aquí usamos que $k > 1$) se cumple que $m \leq k^m < k^{m+1}$, 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 2.50 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 $k = 9'$, donde

$$1 \equiv 0',\ 2 \equiv 1',\ 3 \equiv 2',\ 4 \equiv 3',\ 5 \equiv 4',\ 6 \equiv 5',\ 7 \equiv 6',\ 8 \equiv 7',\ 9 \equiv 8',$$

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.

2.7 La forma normal de Cantor

En esta sección probaremos un resultado análogo al teorema 2.49 tomando como base $k = \omega$ y que resulta ser válido para todos los ordinales. 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 $\omega\cdot 1$, $\omega\cdot 2$, $\omega\cdot 3$, $\omega\cdot 4, \ldots$ 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 $\omega^2\cdot 3$, $\omega^2\cdot 4, \ldots$, y por encima de todos ellos está $\omega^2\cdot\omega = \omega^3$, y si vamos formando ω^3, ω^4, $\omega^5, \ldots$, 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 2.14 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 2.51 *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 2.52 *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 2.53 *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 2.51 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 2.54 *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 2.55 (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.[7]

Si $\delta < \epsilon_0$, entonces se cumple $\delta < \omega^{(n)}$ para cierto $n \in \omega$, luego tenemos que $\omega^\delta \leq \omega^{\omega^{(n)}} = \omega^{(n+1)} \leq \epsilon_0$. Tomando el supremo en δ concluimos que $\omega^{\epsilon_0} \leq \epsilon_0$. El recíproco es obvio, luego $\omega^{\epsilon_0} = \epsilon_0$.

Definición 2.56 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 $\omega^{(n)} \leq \alpha < \omega^{(n+1)}$.

Es claro que entonces $\omega^{(n+1)} \leq \omega^\alpha < \omega^{(n+2)}$, es decir, tenemos que

$$o(\omega^\alpha) = 1 + o(\alpha).$$

En particular $\omega^\alpha \neq \alpha$, 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 2.57 *Si ξ es un ordinal, se cumple:*

a) $\bigwedge \alpha\beta < \xi\ \alpha + \beta < \xi$ *y sólo si* $\xi = 0 \vee \bigvee \eta\ \xi = \omega^\eta$.

b) $\bigwedge \alpha\beta < \xi\ \alpha \cdot \beta < \xi$ *si y sólo si* $\xi = 0, 1, 2 \vee \bigvee \eta\ \xi = \omega^{\omega^\eta}$.

c) $\bigwedge \alpha\beta < \xi\ \alpha^\beta < \xi$ *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 $\alpha + \beta < \omega^\delta < \omega^\lambda$.

[7] 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 2.53. 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 $\delta = 0 \lor \delta = \omega^\eta$ 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 $\omega < \xi \land \eta \leq \omega^\eta = \xi$, 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 2.58 *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 2.55,

$$o(\omega^{\eta_i} k_i) = o(\omega^{\eta_i}) = 1 + o(\eta_i) \leq 1 + o(\eta_0),$$

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.

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.

Ejercicio: Explicar cómo puede calcularse la suma y el producto de dos ordinales en forma normal de Cantor en función de los exponentes y coeficientes de los sumandos.

Capítulo III

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.

3.1 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 3.1 Una relación R está *bien fundada* en una clase A si

$$\bigwedge X(X \subset A \land X \neq \varnothing \rightarrow \bigvee y \in X \bigwedge z \in X\, \neg x\, R\, y).$$

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 2.1 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 3.2 (Teorema general de inducción transfinita) *Sea R una relación clausurable y bien fundada en una clase A y sea B una clase cualquiera. Entonces*

$$\bigwedge x \in A(A_x^R \subset B \rightarrow x \in B) \rightarrow A \subset B.$$

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 3.3 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 3.4 Sea R una relación definida sobre una clase A. Diremos que una subclase $B \subset A$ es R-A-*transitiva* si

$$\bigwedge xy \in A(x\,R\,y \wedge y \in B \rightarrow x \in B).$$

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 2.1 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 3.5 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, $\mathrm{ct}\ x$ 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 3.6 *Sea R una relación conjuntista en una clase A y sea $x \in A$. Se cumple*

a) $A_x^R \subset \mathrm{cl}_A^R(x)$.

b) $\mathrm{cl}_A^R(x)$ *es un conjunto R-A-transitivo.*

c) Si $A_x^R \subset T$ y $T \subset A$ es una clase R-A-transitiva, entonces $\mathrm{cl}_A^R(x) \subset T$.

d) $\mathrm{cl}_A^R(x) = A_x^R \cup \bigcup\limits_{y\in A_x^R} \mathrm{cl}_A^R(y)$.

Demostración: Demostración: a) $A_x^R = \mathrm{cl}_A^R(x)[0] \subset \mathrm{cl}_A^R(x)$.

b) Supongamos que u, $y \in A$ cumplen $u\, R\, y \land y \in \mathrm{cl}_A^R(x)$. Entonces existe un $n \in \omega$ tal que $y \in \mathrm{cl}_A^R(x)[n]$, con lo que $u \in A_y^R \subset \mathrm{cl}_A^R(x)[n+1] \subset \mathrm{cl}_A^R(x)$.

c) 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 $u\, R\, y \land y \in T$. Por transitividad $u \in T$. Por definición de clausura concluimos que $\mathrm{cl}_A^R(x) \subset T$.

d) 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 b) y c) obtenemos que $\mathrm{cl}_A^R(y) \subset \mathrm{cl}_A^R(x)$. Por consiguiente el conjunto $T = A_x^R \cup \bigcup\limits_{y\in A_x^R} \mathrm{cl}_A^R(y)$ está contenido en $\mathrm{cl}_A^R(x)$.

Para demostrar la otra inclusión basta probar T es transitivo y aplicar c). Sean, pues, u, $v \in A$ tales que $u\, R\, v \land v \in T$. 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 3.7 *Sea x un conjunto arbitrario. Entonces*

a) $x \subset \operatorname{ct} x$.

b) $\operatorname{ct} x$ *es un conjunto transitivo.*

c) Si $x \subset T$ *y* T *es una clase transitiva, entonces* $\operatorname{ct} x \subset T$.

d) $\operatorname{ct} x = x \cup \bigcup_{y \in x} \operatorname{ct} y$.

e) x *es transitivo si y sólo si* $x = \operatorname{ct} x$.

La última propiedad es consecuencia inmediata de las anteriores. Como primera aplicación del concepto de clausura demostramos un resultado técnico:

Teorema 3.8 *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 $y \in B \cap \operatorname{cl}_A^R(x)$, 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, $v \in B \cap \operatorname{cl}_A^R(x)$, 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 clausurable y bien fundada, podemos definir $F(x)$ suponiendo que F está ya definida sobre los elementos de A_x^R:

Teorema 3.9 (Teorema general de recursión transfinita) *Sea R una relación conjuntista y bien fundada en una clase A y sea $G : V \longrightarrow B$ 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 $h = \bigcup\limits_{u \in A_x^R} h_u$. 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 3.6.

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 $h'|_{A_x^R} = h|_{A_x^R}$, de donde se sigue claramente que h' es una $\hat{x}$-aproximación.

3) *Definimos $F = \bigcup\limits_{x \in A} h_x$, 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 3.10 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

$$G(z) = \begin{cases} \bigcup\limits_{y \in A_x^R} (s(y) + 1) & \text{si } z = (x, s), \text{ con } x \in A \land s : A_x^R \longrightarrow \Omega, \\ 0 & \text{en otro caso.} \end{cases}$$

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 3.11 *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 3.12 (Teorema general de inducción transfinita) *Sea R una relación conjuntista y bien fundada sobre una clase A y sea B una clase cualquiera. Entonces*

$$\bigwedge x \in A(\operatorname{cl}_A^R(x) \subset B \rightarrow x \in B) \rightarrow A \subset B.$$

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 3.13 (Teorema general de recursión transfinita) *Sea R una relación conjuntista y bien fundada en una clase A y sea $G : V \longrightarrow B$ 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 3.9, salvo que el paso 1) y la unicidad de F se demuestran usando la versión fuerte del teorema general de recursión 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 clausurable y bien fundada en Ω. En efecto, como Ω es transitiva, las clases E-Ω-transitivas son simplemente las subclases transitivas de Ω y $\mathrm{cl}_\Omega^E(\alpha) = \alpha$.

3.2 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 3.14 Un conjunto x es *regular* si su clausura transitiva $\operatorname{ct} x$ 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 $\operatorname{ct} x = \operatorname{ct} y = \{x, y\}$, 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 3.15 *Se cumple:*

a) R *es una clase transitiva.*

b) $\Omega \subset R$*, luego* R *es una clase propia.*

c) La relación de pertenencia está bien fundada en R*.*

d) $\mathcal{P}R = R$*.*

e) $\bigwedge A(R \cap \mathcal{P}A \subset A \rightarrow R \subset A)$*.*
En particular, $\bigwedge A(\mathcal{P}A \subset A \rightarrow R \subset A)$*.*

Demostración: a) Se trata de probar que los elementos de los conjuntos regulares son regulares. Supongamos que $u \in v \in R$. Entonces $u \in \operatorname{ct} v$, luego $u \subset \operatorname{ct} v$, luego u está contenido en un conjunto transitivo y bien fundado, luego $u \in R$.

b) Todo ordinal es un conjunto transitivo y bien fundado, luego cumple la definición de conjunto regular.

c) 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 $x = \operatorname{ct} y \cap A$, que no es vacío, pues $u \in x$. Como $\operatorname{ct} y$ 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 $v \in u \in x \subset z$, luego $v \in z$ por la transitividad de z, luego $v \in u \cap x = \varnothing$, contradicción. Por lo tanto, $u \cap A = \varnothing$.

d) 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 $\operatorname{ct} u$ está bien fundada, luego $\operatorname{ct} u \in R$, luego $\operatorname{ct} u \subset R$. Por 3.7 d) tenemos que $\operatorname{ct} x \subset R$, y esta clausura está bien fundada por c), luego $x \in R$.

e) 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 e) 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 3.10 (para la relación de pertenencia E). Explícitamente:

Definición 3.16 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 3.17 $R_0 = \varnothing \wedge \bigwedge\alpha\ R_{\alpha+1} = \mathcal{P}R_\alpha \wedge \bigwedge\lambda\ R_\lambda = \bigcup\limits_{\delta<\lambda} R_\delta$,

$$R = \bigcup_{\alpha \in \Omega} R_\alpha.$$

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

$$\text{rang } x = \bigcup_{y \in x} (\text{rang } y + 1) \leq \alpha < \alpha + 1,$$

luego $x \in R_{\alpha+1}$. Recíprocamente, si $x \in R_{\alpha+1}$, entonces todo $y \in x$ cumple rang $y+1 \leq$ rang $x < \alpha+1$, luego 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 parte (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 3.17 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 3.18 *Se cumple:*

a) Si $\alpha \leq \beta$ son ordinales, entonces $R_\alpha \subset R_\beta$.

b) Para cada ordinal α, la clase R_α es transitiva.

c) 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

$$\operatorname{rang}\alpha = \bigcup_{\beta<\alpha}(\operatorname{rang}\beta + 1) = \bigcup_{\beta<\alpha}(\beta+1) = \alpha.$$

■

Ahora ya podemos presentar el axioma de regularidad en condiciones de que se pueda valorar su contenido:

Teorema 3.19 *Las afirmaciones siguientes son equivalentes:*

a) $\bigwedge x(\operatorname{cto} x \wedge x \neq \varnothing \rightarrow \bigvee u \in x\; u \cap x = \varnothing)$.

b) Todo conjunto está bien fundado.

c) 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) $\bigwedge x(\operatorname{cto} x \wedge x \neq \varnothing \rightarrow \bigvee u \in x\ u \cap x = \varnothing)$.

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 clara entre los conjuntos y las clases propias:

Teorema 3.20 *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. ■

3.3 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 2.22 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

$$G(s) = \begin{cases} x_0 & \text{si } \mathcal{D}s = \varnothing, \\ x & \text{si } \mathcal{D}s = n+1 \land x \in A \land x\, R\, s(n), \end{cases}$$

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:

$$G = \{(s,x) \in X_\omega \times A \mid \bigvee m \in \omega (s : m \longrightarrow A \land$$

$$((m = 0 \land x = x_0) \lor (\bigvee n \in \omega (m = n+1 \land x\, R\, s(n))))\},$$

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

$$\bigwedge X(X \subset A \land X \neq \varnothing \rightarrow E(X) \in X),$$

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

$$f(0) = x_0 \land \bigwedge n \in \omega\ f(n+1) = E(\{x \in A \mid x\,R\,f(n)\}),$$

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)

$$\bigwedge X(\operatorname{cto} X \rightarrow \bigvee f(f : X \longrightarrow V \land \bigwedge u \in X(u \neq \varnothing \rightarrow f(u) \in u)).$$

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 3.21 (AI) AE $\rightarrow$ ED.

DEMOSTRACIÓN: Consideremos un conjunto A y una relación R en las condiciones de ED. Consideremos el conjunto $X = \{A_a^R \mid a \in A\}$ 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 $g(a) = f(A_a^R)$. De este modo se cumple que $\bigwedge a \in A\,(g(a) \in A \land g(a)\,R\,a)$.

Ahora fijamos un $a_0 \in A$ y definimos por recurrencia una función $x : \omega \longrightarrow A$ mediante $x_0 = a_0 \land x_{n+1} = g(x_n)$. 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 $x : I \longrightarrow \bigcup\limits_{i\in I} X_i$.

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. Estudiaremos los conjuntos finitos en el capítulo siguiente, pero para probar esto sólo necesitamos la mera definición (y anticipamos también, de paso, la de conjunto numerable):

Definición 3.22 Un conjunto x es *finito* si $\bigvee n \in \omega \bigvee f\ f : n \longrightarrow x$ biyectiva). Diremos[2] que x es *numerable* si es finito o bien $\bigvee f\, f : \omega \longrightarrow x$ biyectiva.

Así pues, un conjunto es finito si sus elementos se pueden "contar", es decir, que se pueden emparejar con los elementos de un número natural.[3] Los conjuntos numerables son los que se pueden "contar" a expensas de agotar todos los números naturales en el proceso de cómputo.

Teorema 3.23 *Todo conjunto finito tiene una función de elección.*

DEMOSTRACIÓN: Basta probar, por inducción sobre n, que

$$\bigwedge x(\bigvee f\ f : n \longrightarrow x \text{ biyectiva} \rightarrow x \text{ tiene una función de elección}).$$

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 3.24 (AI, AP) ED $\rightarrow$ 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 $f : X_m \longrightarrow \{\varnothing\} \cup \bigcup\limits_{n<m} x_n$ cumple que $\bigwedge n < m(x_n \neq \varnothing \rightarrow f(x_n) \in x_n)$.

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

[2]No es infrecuente que se defina un conjunto numerable como un conjunto biyectable con ω (excluyendo así los conjuntos finitos). Según la definición que estamos adoptando, tales conjuntos serán para nosotros los conjuntos *infinitos numerables.*

[3]Notemos que estamos empleando una alteración técnica intrascendente de lo que normalmente se entiende por "contar". Cuando decimos que un conjunto X tiene 3 elementos es porque hemos numerado sus elementos como x_1, x_2 y x_3, mientras que, para justificar que cumple literalmente la definición que hemos dado, necesitamos una biyección $f : 3 \longrightarrow X$, lo que supone contar sus elementos como x_0, x_1 y x_2.

$\mathcal{D}f = \{x_n \mid n < m\}$, 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 $f = \bigcup\limits_{n\in\omega} f_n : X \longrightarrow V$ y es una función de elección sobre X. ■

Nota Observemos que ED no puede probarse[4] 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 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 $A_{x_n}^R$, 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 3.25 (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. ■

Hay un resultado que parece muy elemental, pero en realidad requiere el axioma de elección:

Teorema 3.26 (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.*

[4]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

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 1.14.

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 1.14 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 $E(a) = \min a$, 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 3.27 *Las afirmaciones siguientes son equivalentes:*

a) AE

b) Si $g : y \longrightarrow x$ es una aplicación suprayectiva, existe $f : x \longrightarrow y$ tal que $f \circ g = I_x$.

c) 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 $\bigwedge i \in I\ s_i \in x_i$.

d) 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: a) $\Rightarrow$ b) se sigue de la demostración del teorema anterior.

b) $\Rightarrow$ c) Consideremos la aplicación $g : \bigcup\limits_{i \in I} \{i\} \times X_i \longrightarrow I$ dada por $g(i, u) = i$. Como los conjuntos X_i son no vacíos, tenemos que g es suprayectiva. Sea $f : I \longrightarrow \bigcup\limits_{i \in I} (\{i\} \times X_i)$ según b), es decir, tal que, para cada $i \in I$, se cumple que $f(i) = (i, v)$, para cierto $v \in X_i$. Basta tomar $s = \mathcal{R}f$.

c) $\Rightarrow$ d) Podemos ver a X como una familia $\{i\}_{i \in X}$ de conjuntos no vacíos. Por c) existe $\{s_i\}_{i \in X}$ tal que $\bigwedge i \in X\ s_i \in i$. Basta tomar $a = \mathcal{R}s$.

d) $\Rightarrow$ a) 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 d) 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 $X \subset X$ para el que se cumpla $\bigwedge uv \in C(u \leq v \vee v \leq u)$. Una cota superior para un conjunto $C \subset X$ es un $u \in X$ tal que $\bigwedge v \in C\ v \leq u$. Un elemento maximal en X es un $m \in X$ tal que $\neg \bigvee u \in X\ m < u$. El teorema siguiente contiene el enunciado del lema de Zorn junto con otras afirmaciones equivalentes menos técnicas:

Teorema 3.28 (AP) *Las afirmaciones siguientes son equivalentes:*

a) **Axioma de elección** *Todo conjunto tiene una función de elección.*

b) **Principio de numerabilidad** *Todo conjunto puede biyectarse con un ordinal.*

c) **Principio de buena ordenación** *Todo conjunto puede ser bien ordenado.*

d) **Lema de Zorn** *Todo conjunto parcialmente ordenado no vacío en el que toda cadena tenga una cota superior tiene un elemento maximal.*

e) **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: a) $\Rightarrow$ b) 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 2.22 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.

b) $\Rightarrow$ c) 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.

c) $\Rightarrow$ e) 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 c), 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 2.22 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.

e) $\Rightarrow$ d) es trivial.

d) $\Rightarrow$ a) Fijemos un conjunto x, que podemos suponer no vacío y tal que $\varnothing \notin x$, y sea

$$y = \{p \in \mathcal{P}(x \times \bigcup x) \mid \bigvee a(a \subset x \land p : a \longrightarrow \bigcup x \land \bigwedge u \in a(u \neq \varnothing \to p(u) \in u))\}$$

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

$$E(u) = \begin{cases} \min u & \text{si } u \neq \varnothing, \\ \varnothing & \text{si } u = \varnothing. \end{cases}$$

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.

Terminamos con una aplicación del lema de Zorn:

Teorema 3.29 (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[5] 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 $C \subset \mathcal{M}$

[5] Se cumple que $\mathcal{M}$ es un conjunto porque $\mathcal{M} \subset \mathcal{P}A$, y estamos suponiendo AP.

es una cadena (que podemos suponer no vacía), es fácil ver que $I = \bigcup C$ es un ideal de A.

En efecto:

a) Si $J \in C$, tenemos que $0 \in J \subset I$.

b) 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 $x + y \in J \subset I$.

c) 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. ■

Capítulo IV

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. No obstante, cabe señalar que los resultados de la primera sección se demuestran en NBG*.

4.1 Equipotencia

La idea básica subyacente a toda la teoría de cardinales es que podemos decir que dos conjuntos X e Y tienen el mismo número de elementos si podemos emparejar cada elemento de X con un elemento distinto de Y, sin que falte ni sobre ninguno, pero esto se corresponde simplemente con el concepto de biyección:

Definición 4.1 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 $\overline{\overline{X}} = \overline{\overline{Y}}$.

Observaciones 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.

La notación se remonta a Cantor. Si X es un conjunto ordenado, Cantor representaba por $\overline{X}$ 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 este modo, 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 objeto (clase o conjunto) al que llamar $\overline{\overline{X}}$. Nos ocuparemos de ello en la sección siguiente, pero, de momento, la notación $\overline{\overline{X}}$ sólo tiene sentido como parte inseparable las expresiones que acabamos de definir. ■

Observemos que suponiendo AE el teorema 3.26 nos da que, para conjuntos no vacíos, $\overline{\overline{X}} \leq \overline{\overline{Y}} \leftrightarrow \bigvee g\ g : Y \longrightarrow X$ suprayectiva, pero en esta sección no vamos a necesitar este hecho.

El teorema siguiente justifica que las definiciones que hemos dado contienen realmente una noción razonable de "número de elementos" de un conjunto. Observemos que las tres primeras implican que la equipotencia define una relación de equivalencia sobre la clase universal V.

Teorema 4.2 *Sean X, Y, Z, W conjuntos cualesquiera. Se cumple:*

a) $\overline{\overline{X}} = \overline{\overline{X}}$,

b) $\overline{\overline{X}} = \overline{\overline{Y}}$ *si y sólo si* $\overline{\overline{Y}} = \overline{\overline{X}}$,

c) Si $\overline{\overline{X}} = \overline{\overline{Y}}$ *y* $\overline{\overline{Y}} = \overline{\overline{Z}}$, *entonces* $\overline{\overline{X}} = \overline{\overline{Z}}$,

d) $\overline{\overline{X}} \leq \overline{\overline{X}}$,

e) Si $\overline{\overline{X}} \leq \overline{\overline{Y}}$ *y* $\overline{\overline{Y}} \leq \overline{\overline{X}}$, *entonces* $\overline{\overline{X}} = \overline{\overline{Y}}$,

f) Si $\overline{\overline{X}} \leq \overline{\overline{Y}}$ *y* $\overline{\overline{Y}} \leq \overline{\overline{Z}}$, *entonces* $\overline{\overline{X}} \leq \overline{\overline{Z}}$,

g) 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 e) 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, b) 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 e) 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. Cantor demostró este hecho para conjuntos bien ordenados, luego su prueba sólo vale en general si aceptamos el axioma de elección. Al parecer, el primero que probó este hecho sin hacer uso del axioma de elección fue Dedekind, si bien su demostración permaneció inédita hasta 1932.

Schröder publicó en 1897 una prueba, pero resultó ser incorrecta, aunque ese mismo año F. Bernstein publicó la primera demostración válida de lo que hoy se conoce como teorema de Cantor-Bernstein. Para probarlo nos apoyaremos en un resultado previo (notemos que, pese a las apariencias, no usa AP).

Teorema 4.3 *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 $z = \bigcap\limits_{u \in A} u$. 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 4.4 (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 4.5 (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 $R = \{x \in X \mid x \notin g(x)\} \in \mathcal{P}X$. 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. ■

Por lo tanto, si suponemos también AI, resulta que ω y $\mathcal{P}\omega$ son dos conjuntos infinitos con distinto número de elementos.

Nota 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 se demuestra para conjuntos y V no lo es. 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. ■

4.2 Números cardinales

Ya hemos probado que tiene sentido hablar del número de elementos de conjuntos arbitrarios en el sentido de que podemos comparar dos conjuntos cualesquiera según su número de elementos. Ahora vamos a ver cómo construir números que midan el número de elementos de un conjunto arbitrario, es decir, que nos permitan "contar" cualquier conjunto.

Más concretamente, nos gustaría asociar a cada conjunto X un cardinal $\overline{\overline{X}}$ que nos permita considerar las relaciones de equipotencia $\overline{\overline{X}} = \overline{\overline{Y}}$ como auténticas igualdades, y las relaciones $\overline{\overline{X}} \leq \overline{\overline{Y}}$ como una relación de orden $\leq$ (que tendríamos que definir) actuando sobre los objetos $\overline{\overline{X}}$ y $\overline{\overline{Y}}$ (que de momento no tenemos definidos).

Vamos a presentar dos formas de hacerlo, 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 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 definir 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 $\operatorname{rang} : V \longrightarrow \Omega$, 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 4.6 Un *cardinal* es un conjunto no vacío $\mathfrak{p}$ tal que[1]

a) $\bigwedge xy \in \mathfrak{p}(\overline{\overline{x}} = \overline{\overline{y}}\,)$,

b) $\bigvee \alpha \bigwedge x \in \mathfrak{p} \operatorname{rang} x = \alpha$,

c) $\bigwedge xy(x \in \mathfrak{p} \land \overline{\overline{x}} = \overline{\overline{y}} \land \operatorname{rang} x = \operatorname{rang} y \rightarrow y \in \mathfrak{p})$,

d) $\neg \bigvee xy(y \in \mathfrak{p} \land \overline{\overline{x}} = \overline{\overline{y}} \land \operatorname{rang} x < \operatorname{rang} y)$.

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.

Si X es un conjunto cualquiera, definimos su *cardinal* como

$$\overline{\overline{X}} \equiv \{Y \mid \overline{\overline{X}} = \overline{\overline{Y}} \land \neg \bigvee Z(\operatorname{cto} Z \land \operatorname{rang} Z < \operatorname{rang} Y \land \overline{\overline{X}} = \overline{\overline{Z}}\,)\}.$$

[1] En lo sucesivo las letras góticas $\mathfrak{p}$, $\mathfrak{q}$, ... denotarán siempre cardinales, aunque no se indique explícitamente.

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

$$\{\alpha \in \Omega \mid \bigvee Y(\operatorname{cto} Y \wedge \overline{\overline{Y}} = \overline{\overline{X}} \wedge \operatorname{rang} Y = \alpha)\}$$

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 a) – d) 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 4.7 *Se cumple:*

a) 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 $\overline{\overline{x}} = \mathfrak{p}$.

b) 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 4.1, pero ahora son auténticas igualdades de cardinales.

Definición 4.8 Definimos la relación en $\mathfrak{C}$ dada por

$$\mathfrak{p} \leq \mathfrak{q} \equiv \bigvee xy(\operatorname{cto} x \wedge \operatorname{cto} y \wedge \mathfrak{p} = \overline{\overline{x}} \wedge \mathfrak{q} = \overline{\overline{y}} \wedge x \text{ es minuspontente a } y).$$

Esta definición no depende de la elección de x e y en virtud del último apartado del teorema 4.2, 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 4.1, pero ahora es una auténtica desigualdad entre cardinales.

El teorema 4.2 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) sí 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 4.9 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 $|x| = |y|$.

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

[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".

de von Neumann le asociamos su cardinal en el sentido de 4.6. 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.

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 ahora algunos resultados básicos sobre los cardinales de von Neumann.

Teorema 4.10 $\omega \subset K$.

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. ■

Teorema 4.11 $\omega \in K$.

DEMOSTRACIÓN: En caso contrario existiría un $n \in \omega$ tal que $\overline{\overline{n}} = \overline{\overline{\omega}}$, pero como $n \subset n+1 \subset \omega$ es claro que $\overline{\overline{n}} \leq \overline{\overline{n+1}} \leq \overline{\overline{\omega}} = \overline{\overline{n}}$, luego sería $\overline{\overline{n}} = \overline{\overline{n+1}}$ 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 4.12 $\bigwedge \kappa (\omega \leq \kappa \rightarrow \kappa$ *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 4.13 $\bigwedge \alpha \bigvee \kappa\ \alpha < \kappa$.

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 $f(R) = \operatorname{ord}(\alpha, R)$. 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 $\overline{\overline{\alpha}} = \overline{\overline{\beta}}$, 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 $\overline{\overline{\alpha}} \leq \overline{\overline{\beta}}$, ha de ser $\overline{\overline{\alpha}} < \overline{\overline{\beta}}$.

Llamemos κ al mínimo ordinal tal que $\overline{\overline{\alpha}} < \overline{\overline{\kappa}}$. Claramente $\kappa \in K$, pues si existiera un $\gamma < \kappa$ tal que $\overline{\overline{\gamma}} = \overline{\overline{\kappa}}$, también tendríamos que $\overline{\overline{\alpha}} < \overline{\overline{\gamma}}$, 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 4.14 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 4.15 *El supremo de un conjunto de cardinales es un cardinal.*

Demostración: Sea $A \subset K$ un conjunto y sea $\kappa = \bigcup\limits_{\mu \in A} \mu$. 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 4.16 Llamaremos $\aleph : \Omega \longrightarrow \Omega$ (función álef) a la única aplicación que cumple

$$\aleph_0 = \omega \quad \land \quad \bigwedge\alpha\ \aleph_{\alpha+1} = \aleph_\alpha^+ \quad \land \quad \bigwedge\lambda\ \aleph_\lambda = \bigcup_{\delta<\lambda} \aleph_\delta.$$

Es claro que se trata de una función normal. Vamos a probar que recorre todos los cardinales infinitos.

Teorema 4.17 $\aleph : \Omega \longrightarrow K \setminus \omega$ *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 4.15). 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 $\aleph_0 = \omega$, 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.

En estos términos, es claro que un conjunto es finito (resp. numerable) en el sentido de la definición 3.22 si y sólo si es bien ordenable y $|x| < \aleph_0$ (resp. $|x| \leq \aleph_0$). Las clases que no son finitas (y esto incluye obviamente a todas las clases propias) se llaman *infinitas.* Tenemos entonces que la sucesión de los cardinales (de von Neumann) infinitos 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.

4.3 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 4.18 Definimos las operaciones $+$ y $\cdot$ 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 4.19 *a) Si X e Y son conjuntos disjuntos, $\overline{\overline{X \cup Y}} = \overline{\overline{X}} + \overline{\overline{Y}}$.*
b) 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 4.20 *Para todos los cardinales $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$, $\mathfrak{s}$ se cumple:*

a) $(\mathfrak{p}+\mathfrak{q})+\mathfrak{r}=\mathfrak{p}+(\mathfrak{q}+\mathfrak{r})$,

b) $\mathfrak{p}+\mathfrak{q}=\mathfrak{q}+\mathfrak{p}$,

c) $\mathfrak{p}+0=\mathfrak{p}$,

d) $\mathfrak{p}\leq\mathfrak{q}\land\mathfrak{r}\leq\mathfrak{s}\to\mathfrak{p}+\mathfrak{r}\leq\mathfrak{q}+\mathfrak{s}$,

e) $(\mathfrak{p}\mathfrak{q})\mathfrak{r}=\mathfrak{p}(\mathfrak{q}\mathfrak{r})$,

f) $\mathfrak{p}\mathfrak{q}=\mathfrak{q}\mathfrak{p}$,

g) $\mathfrak{p}\cdot 0=0\land\mathfrak{p}\cdot 1=\mathfrak{p}$,

h) $\mathfrak{p}(\mathfrak{q}+\mathfrak{r})=\mathfrak{p}\mathfrak{q}+\mathfrak{p}\mathfrak{r}$,

i) $\mathfrak{p}\leq\mathfrak{q}\land\mathfrak{r}\leq\mathfrak{s}\to\mathfrak{p}+\mathfrak{r}\leq\mathfrak{q}+\mathfrak{s}\land\mathfrak{p}\mathfrak{r}\leq\mathfrak{q}\mathfrak{s}$.

Estas propiedades permiten operar fácilmente con cardinales. Veamos un ejemplo:

Teorema 4.21 *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 $\overline{\overline{X\cup Y}}\leq\overline{\overline{X}}+\overline{\overline{Y}}$.

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 4.22 Definimos las operaciones $+$ y $\cdot$ 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 2.5 hemos visto que si α y β son dos ordinales cualesquiera, entonces $\alpha+\beta=\operatorname{ord}(\alpha\oplus\beta)$ y $\alpha\beta=\operatorname{ord}(\alpha\times\beta)$, 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 4.18.

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 4.20 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 4.21 se traduce en que, si X e Y son conjuntos bien ordenables,

$$|X|+|Y| = |X\cup Y|+|X\cap Y|,$$

simplemente porque, precisamente por 4.21, ambos miembros se corresponden con el mismo cardinal de $\mathfrak{C}$. También hemos probado lo siguiente:

Teorema 4.23 *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 4.24 *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 4.25 *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 2.30.

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 β, $\gamma < \delta$.

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 4.26 *Se cumple:*

$$\bigwedge \kappa\mu(\kappa \leq \mu \wedge \aleph_0 \leq \mu \rightarrow \kappa + \mu = \mu),$$

$$\bigwedge \kappa\mu(\kappa \leq \mu \wedge \aleph_0 \leq \mu \wedge \kappa \neq 0 \rightarrow \kappa\mu = \mu).$$

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 4.25 hemos visto que si κ es un álef y consideramos el orden canónico en $\kappa \times \kappa$, entonces $\operatorname{ord}(\kappa \times \kappa) = \kappa$. 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 4.27 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 $\aleph(X) = \{\operatorname{ord}(\mathcal{D}R, R) \mid R \in B\}$.

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 4.28 *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 4.29 *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 4.25. 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 4.30 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 4.31 *Para todos los cardinales $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$ se cumple:*

a) $\mathfrak{p} \neq 0 \rightarrow 0^{\mathfrak{p}} = 0$,

b) $\mathfrak{p}^0 = 1, \quad 1^{\mathfrak{p}} = 1, \quad \mathfrak{p}^1 = \mathfrak{p}$,

c) $\mathfrak{q} \leq \mathfrak{r} \rightarrow \mathfrak{p}^{\mathfrak{q}} \leq \mathfrak{p}^{\mathfrak{r}}$,

d) $\mathfrak{p} \neq 0 \land \mathfrak{q} \neq 0 \land \mathfrak{q} \leq \mathfrak{r} \rightarrow \mathfrak{p}^{\mathfrak{q}} \leq \mathfrak{p}^{\mathfrak{r}}$,

e) $\mathfrak{p}^{\mathfrak{q}+\mathfrak{r}} = \mathfrak{p}^{\mathfrak{q}}\mathfrak{p}^{\mathfrak{r}}$,

f) $(\mathfrak{p}\mathfrak{q})^{\mathfrak{r}} = \mathfrak{p}^{\mathfrak{r}}\mathfrak{q}^{\mathfrak{r}}$.

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 4.32 *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. ■

Como consecuencia, el teorema de Cantor admite una formulación aritmética:

Teorema 4.33 (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 4.34 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

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

Veremos que la HCG determina completamente la exponenciación cardinal, pero dejamos esto —junto a estudio en profundidad de la exponenciación cardinal— para el capítulo siguiente.

Sucesiones y partes finitas Para completar los cálculos aritméticos básicos, dado un conjunto bien ordenable A, vamos a calcular el cardinal de los conjuntos

$$A^{<\omega} = \bigcup_{n\in\omega} A^n, \quad \text{y} \quad \mathcal{P}^f A = \{x \mid x \subset A \land |x| < \aleph_0\},$$

es decir, el conjunto de las sucesiones finitas en A y el de los subconjuntos finitos de A.

Teorema 4.35 *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 $|\mathcal{P}^f A| = |\mathcal{P}A| = 2^{|A|}$, que es un número natural, luego $\mathcal{P}A$ y $\mathcal{P}^f A$ son conjuntos finitos. Si A es infinito y bien ordenable, tenemos lo siguiente:

Teorema 4.36 *Si A es un conjunto infinito bien ordenable, entonces $\mathcal{P}^f A$ también es bien ordenable, y $|\mathcal{P}^f A| = |A|$.*

DEMOSTRACIÓN: La aplicación $A^{<\omega} \longrightarrow \mathcal{P}^f A$ dada por $s \mapsto \mathcal{R}s$ es claramente suprayectiva, luego existe una aplicación $\mathcal{P}^f A \longrightarrow A^{<\omega}$ inyectiva,[3] lo que prueba que $\mathcal{P}^f A$ es bien ordenable, y $|\mathcal{P}^f A| \leq |A^{<\omega}| = |A|$.

Por otra parte, la aplicación $A \longrightarrow \mathcal{P}^f A$ dada por $a \mapsto \{a\}$ es inyectiva, luego $|A| \leq |\mathcal{P}^f A|$ y tenemos la igualdad. ■

4.4 Conjuntos finitos

Recogemos aquí las propiedades específicas de los conjuntos finitos que no comparten los conjuntos infinitos. Recordemos que hemos definido un conjunto finito como un conjunto bien ordenable x tal que $|x| < \aleph_0$, es decir, tal que $|x|$ sea un número natural.

Obviamente, si $y \subset x$, entonces y también es bien ordenable, y $|y| \leq |x|$, luego todo subconjunto de un conjunto finito es finito. Por otra parte, como la suma y el producto de números naturales es un número natural (y las operaciones cardinales coinciden con las ordinales sobre los números naturales) concluimos que la unión y el producto cartesiano de dos conjuntos finitos es de nuevo un conjunto finito. Más aún, una simple inducción prueba que la unión de un conjunto finito de conjuntos finitos es finita.

Un ejemplo de propiedad que no es válida para conjuntos infinitos es la siguiente:

Teorema 4.37 *Si $x \subset y$ son conjuntos finitos y $|x| = |y|$, entonces $x = y$.*

DEMOSTRACIÓN: Tenemos que $y = x \cup (y - x)$, luego $|y| = |x| + |y \setminus x|$, y ahora usamos que la suma de números naturales es simplificable, por lo que $|y \setminus x| = 0$, lo que equivale a que $y \setminus x = \varnothing$, luego $x = y$. ■

A su vez esto implica:

Teorema 4.38 *Si $f : x \longrightarrow y$ es una aplicación entre conjuntos finitos tales que $|x| = |y|$, entonces f es inyectiva si y sólo si es suprayectiva, si y sólo si es biyectiva.*

DEMOSTRACIÓN: Si f es inyectiva entonces $|f[x]| = |x| = |y|$ y $f[x] \subset y$, luego por el teorema anterior $f[x] = y$, lo cual significa que f es suprayectiva.

Si f es suprayectiva, por el teorema 3.26 existe[4] $g : y \longrightarrow x$ inyectiva tal que $g \circ f = I_y$. Tenemos entonces que g es biyectiva por la parte ya probada, luego $g^{-1} \circ g \circ f = g^{-1}$, luego $f = g^{-1}$ y f es biyectiva. ■

[3]Notemos que aquí no usamos el axioma de elección porque $A^{<\omega}$ es bien ordenable.

[4]Tal y como se explica tras la prueba, como x es bien ordenable el argumento no requiere el axioma de elección.

Nota Un conjunto x con la propiedad de que existe $f : x \longrightarrow x$ inyectiva y no suprayectiva recibe el nombre de conjunto *D–infinito* (o *infinito de Dedekind*), y los conjuntos que no son D–infinitos se llaman *D–finitos.*

El teorema anterior implica que todo conjunto D–infinito es infinito, luego todo conjunto finito es D–finito. Sin embargo, el recíproco no puede probarse sin el axioma de elección.[5] 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, una implicación está probada en el teorema 2.25, pues en su demostración hemos visto que si un conjunto N es D–infinito existe una aplicación $F : \omega \longrightarrow N$ inyectiva, luego $\aleph_0 \leq \overline{\overline{N}}$.

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. ■

Otra propiedad relevante de los conjuntos finitos es la siguiente:

Teorema 4.39 *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.

[5] En realidad basta ED. Si X es un conjunto infinito, consideramos el conjunto A de todas las funciones $s : n \longrightarrow A$ 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 $f = \bigcup\limits_{n\in\omega} : \omega \longrightarrow A$ inyectiva.

En la sección 2.6 definimos sumas finitas sobre cualquier clase A dotada de una operación asociativa y con elemento neutro para sucesiones $\{a_i\}_{i\in I}$, donde I era un subconjunto de un número natural (lo cual se usaba para determinar el orden de los sumandos en la suma finita). Vamos a ver ahora que si la operación es conmutativa podemos definir sumas de sucesiones definidas sobre cualquier conjunto finito, en las que no importa el orden de los sumandos. Para ello probamos lo siguiente:

Teorema 4.40 *Sea A una clase y $+$ una operación en A asociativa, conmutativa y con elemento neutro 0. Sea $\sigma : n \longrightarrow n$ biyectiva y sea $\{a_i\}_{i\in n}$ 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 $\sigma : n+1 \longrightarrow n+1$. Si $\sigma(n) = n$, entonces, aplicando la hipótesis de inducción a $\sigma|_n : n \longrightarrow n$ 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 probada en la sección 2.6 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 $s : n \longrightarrow I$ 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 $\tau : n \longrightarrow n$ 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 I es un conjunto finito cualquiera, $\{a_i\}_{i\in I}$ es una sucesión en A y en A tenemos definida una operación en las condiciones del teorema anterior, podemos definir

$$\sum_{i\in I} a_i = \sum_{j<n} a_{s(j)},$$

donde $s : n \longrightarrow I$ es cualquier biyección. El resultado no depende de la biyección elegida porque si $t : n \longrightarrow I$ es otra biyección, podemos aplicar el teorema anterior a $\sigma = t \circ s^{-1} : n \longrightarrow n$, lo que nos da la igualdad

$$\sum_{j<n} a_{s(j)} = \sum_{j<n} a_{t(j)}.$$

Ahora podemos expresar la propiedad asociativa generalizada bajo hipótesis más generales que en 2.48:

Teorema 4.41 (Propiedad asociativa generalizada) *Sea A una clase en la que hay definida una operación $+$ asociativa y con elemento neutro. Sea $\{I_i\}_{i<k}$ una familia de conjuntos finitos, sea $I = \bigcup\limits_{i<k} I_i$ y sea $\{a_i\}_{i\in I}$ una sucesión en A. Entonces,*

$$\sum_{j\in I} a_j = \sum_{i<k}\sum_{j\in I_i} a_j.$$

Demostración: Basta observar que existe una biyección $s : n \longrightarrow I$, donde $n \in \omega$, de modo que la familia $\{s^{-1}[I_i]\}_{i<k}$ cumple las condiciones de 2.48, con lo que

$$\sum_{j\in I} a_j = \sum_{j<n} a_{s(j)} = \sum_{i<k}\sum_{j\in s^{-1}[I_i]} a_{s(j)} = \sum_{i<k}\sum_{j\in I_i} a_j.$$

■

Finalmente vamos a dar la caracterización que teníamos pendiente de la exponenciación ordinal en términos de buenos órdenes.

Definición 4.42 Sean A y B dos conjuntos bien ordenados y sea m el mínimo de A. Definimos

$$A^{(B)} = \{s \mid s : B \longrightarrow A \land |\{b \in B \mid s(b) \neq m\}| < \aleph_0\}.$$

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 4.43 *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

$$A_\delta = \{s \in \alpha^{(\lambda)} \mid \bigwedge\epsilon(\delta \leq \epsilon \rightarrow s(\epsilon) = 0)\}.$$

Es inmediato comprobar que $\alpha^{(\lambda)} = \bigcup\limits_{\delta<\lambda} A_\delta$, 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. ■

4.5 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 4.44 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 4.45 *Para cualquier familia de conjuntos $\{X_i\}_{i\in I}$ se cumple que*

$$\Big|\bigcup_{i\in I}X_i\Big| \leq \sum_{i\in I}|X_i|,$$

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

$$\Big|\bigcup_{i\in I}X_i\Big| \leq \Big|\bigcup_{i\in I}|X_i| \times \{i\}\Big| = \sum_{i\in I}|X_i|,$$

y se da la igualdad si los conjuntos son disjuntos. ■

El teorema siguiente se demuestra sin dificultad:

Teorema 4.46 *Se cumple*

a) Si $\bigwedge i \in I\ \kappa_i \leq \mu_i$, *entonces* $\sum\limits_{i\in I} \kappa_i \leq \sum\limits_{i\in I} \mu_i$,

b) $\sum\limits_{i\in I} \kappa = |I|\,\kappa$,

c) $\mu \sum\limits_{i\in I} \kappa_i = \sum\limits_{i\in I} \mu\kappa_i$.

A modo de ejemplo demostraremos la asociatividad generalizada de la suma de cardinales:

Teorema 4.47 *Si* $I = \bigcup\limits_{j\in J} I_j$ *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 4.48 *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 $1 \leq \kappa_i \leq \kappa$, luego

$$|I| = \sum_{i\in I} 1 \leq \sum_{i\in I}\kappa_i \leq \sum_{i\in I}\kappa = |I|\,\kappa.$$

Como cada $\kappa_i \leq \sum\limits_{i\in I}\kappa_i$, también $\kappa \leq \sum\limits_{i\in I}\kappa_i$.

Multiplicando las desigualdades (y teniendo en cuenta que, por las hipótesis, la suma es un cardinal infinito) obtenemos

$$|I|\,\kappa \leq \Big(\sum_{i\in I}\kappa_i\Big)^2 = \sum_{i\in I}\kappa_i.$$

■

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:

$$\prod_{i\in I} X_i = \{f \mid f : I \longrightarrow \bigcup_{i\in I} X_i \land \bigwedge i\in I\ f(i)\in X_i\}.$$

El producto cartesiano de un conjunto de conjuntos es un conjunto porque está contenido en $\mathcal{P}(I \times \bigcup\limits_{i\in I} X_i)$.

Definición 4.49 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 4.50 *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 $f : \prod\limits_{i\in I} X_i \longrightarrow \prod\limits_{i\in I}|X_i|$ 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 4.51 *Se cumple:*

a) *Si algún* $\kappa_i = 0$, *entonces* $\prod\limits_{i\in I} \kappa_i = 0$,

b) $\prod\limits_{i\in I} \kappa = \kappa^{|I|}$,

c) $\Big(\prod\limits_{i\in I} \kappa_i\Big)^\mu = \prod\limits_{i\in I} \kappa_i^\mu$,

d) $\prod\limits_{i\in I} \kappa^{\mu_i} = \kappa^{\sum\limits_{i\in I} \mu_i}$,

e) *Si* $\bigwedge i \in I\ \kappa_i \leq \mu_i$, *entonces* $\prod\limits_{i\in I} \kappa_i \leq \prod\limits_{i\in I} \mu_i$,

f) *Si* $I = \bigcup\limits_{j\in J} I_j$, *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 4.48 para el cálculo de productos infinitos, pero a menudo basta el teorema siguiente:

Teorema 4.52 *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 $\kappa = \sup\limits_{\alpha<\mu} \kappa_\alpha$. Entonces $\prod\limits_{\alpha<\mu} \kappa_\alpha \leq \prod\limits_{\alpha<\mu} \kappa = \kappa^\mu$.

Tomemos una aplicación biyectiva $f : \mu \times \mu \longrightarrow \mu$. Sea $A_\alpha = f[\mu \times \{\alpha\}]$. Así $\mu = \bigcup\limits_{\alpha<\mu} A_\alpha$ 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 $\sup\limits_{\beta\in A_\alpha} \kappa_\beta = \kappa$.

Como los κ_β son no nulos, tenemos que $\kappa_\beta \leq \prod\limits_{\beta\in A_\alpha} \kappa_\beta$, 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 $\lambda < \omega_1$. En el capítulo siguiente veremos que en general estas restricciones no pueden ser eliminadas.

Veamos ahora una desigualdad entre una suma y un producto:

Teorema 4.53 *Si* $\bigwedge i \in I\ 2 \leq \kappa_i$, *entonces* $\sum\limits_{i\in I} \kappa_i \leq \prod\limits_{i\in I} \kappa_i$.

DEMOSTRACIÓN: Claramente $|I| \leq 2^{|I|} = \prod\limits_{i\in I} 2 \leq \prod\limits_{i\in I} \kappa_i$. Por otra parte, $\kappa_i \leq \prod\limits_{i\in I} \kappa_i$, luego $\sup\limits_{i\in I} \kappa_i \leq \prod\limits_{i\in I} \kappa_i$. El teorema 4.48 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 4.54 (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 $\alpha = (\alpha_i)_{i\in I} \in \prod\limits_{i\in I} \mu_i$. 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. ■

4.6 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 4.55 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 4.56 $\bigwedge \lambda\ \omega \leq \operatorname{cf} \lambda \leq \lambda$.

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 4.57 $\bigwedge \alpha\ \operatorname{cf} \alpha \in K$.

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 4.58 $\bigwedge\lambda\bigvee f\ f : \operatorname{cf}\lambda \longrightarrow \lambda$ *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

$$\begin{aligned}
&f(0) = g(0),\\
&\textstyle\bigwedge\alpha < \operatorname{cf}\lambda\ f(\alpha+1) = \text{máx}\{g(\alpha), f(\alpha)+1\},\\
&\textstyle\bigwedge\lambda' < \operatorname{cf}\lambda\ f(\lambda') = \bigcup\limits_{\delta<\lambda'} f(\delta).
\end{aligned}$$

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 4.59 *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 4.60 *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 4.61 *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 4.58 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 4.62 *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 4.63 Sea $f : \lambda \longrightarrow \lambda$, donde λ cumple $\operatorname{cf} \lambda > \aleph_0$ o bien $\lambda = \Omega$. Para cada $\alpha \in \lambda$ definimos

$$
\begin{aligned}
f^0(\alpha) &= \alpha, \\
f^{n+1}(\alpha) &= f(f^n(\alpha)), \\
f^\omega(\alpha) &= \sup_{n \in \omega} f^n(\alpha).
\end{aligned}
$$

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 4.59), 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 4.64 *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 4.65 (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*

$$\bigwedge \alpha \in \lambda \bigvee \beta \in \lambda (\alpha \leq \beta \land f(\beta) = \beta).$$

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 4.66 (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 $\kappa = \bigcup\limits_{\alpha < \operatorname{cf} \kappa} f(\alpha)$. 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 $\kappa = \sum\limits_{\alpha<\operatorname{cf}\kappa} \nu_\alpha$. 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 4.67 (AE) *Se cumple*

a) $\operatorname{cf} \aleph_0 = \aleph_0$,

b) $\bigwedge \lambda \ \operatorname{cf} \aleph_\lambda = \operatorname{cf} \lambda$,

c) (AE) $\bigwedge \alpha \ \operatorname{cf} \aleph_{\alpha+1} = \aleph_{\alpha+1}$.

DEMOSTRACIÓN: a) es consecuencia inmediata de 4.56, b) es un caso particular de 4.62. 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 4.68 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 4.58 y 4.61 se sigue inmediatamente:

Teorema 4.69 $\bigwedge \alpha \ \operatorname{cf} \alpha$ *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 4.70 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 4.71 *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).

4.7 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,[6] una aplicación que a cada ordinal infinito α le asigne una biyección $f_\alpha : \alpha \times \alpha \longrightarrow \alpha$. Por ejemplo, la prueba de 4.25 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.

a) *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 $f_{\alpha,\beta} = g_{\alpha,\beta} \circ h_{\alpha,\beta} \circ g^{-1}_{\beta,\alpha}$.

b) *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

   $$g^i_\eta : \omega^{\eta_0} + \cdots + \omega^{\eta_i} \longrightarrow \omega^{\eta_i} + \cdots + \omega^{\eta_0}.$$

[6] 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.

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 $g_\eta = g_\eta^{n+1}$.

c) *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 2.52 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 $\omega^{\eta_0}k_0$.

d) *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 $c_\alpha : \alpha \longrightarrow \omega^{\eta_\alpha}$.

e) *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).

f) *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 $\omega^{\eta_\alpha} = \omega^{\eta_{\alpha+\alpha}}$.

g) *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 4.43. 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 $e_\eta = t_\eta^{-1} \circ t_{\eta+\eta}$.

h) *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 4.72 *Si $\mathfrak{p} \geq 5$ entonces no $2^{\mathfrak{p}} \leq \mathfrak{p}^2$.*

DEMOSTRACIÓN: Para cardinales finitos se demuestra fácilmente por inducción que $n \geq 5 \rightarrow n^2 < 2^n$: 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 4.36 tenemos que $\mathcal{P}^f\omega$ 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 $\mathcal{P}^f\omega$. 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 $U = \{G(\beta) \mid \beta < \alpha \land G(\beta) \notin g(\beta)\}$ 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 4.73 *La hipótesis del continuo generalizada implica el axioma de elección.*

Demostración: Por el teorema 4.29, 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 4.74 *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 $\kappa = \bigcup\limits_{\delta<\lambda} |V_\delta|^+$. 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:

$$x \trianglelefteq_{\delta+1} y \leftrightarrow (x, y \in V_\delta \land x \trianglelefteq_\delta y) \lor (x \in V_\delta \land y \in V_{\delta+1} \setminus V_\delta)$$

$$\lor\, (x, y \in V_{\delta+1} \setminus V_\delta \land x \trianglelefteq^*_{\delta+1} y).$$

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 4.75 *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 V

La exponenciación cardinal

Tal y como indicamos en el capítulo anterior, 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.

5.1 La exponenciación en NBG

Veamos primero lo que podemos decir sobre el cálculo de potencias de cardinales partiendo exclusivamente de los axiomas de NBG. En las secciones siguientes veremos qué más podemos añadir si suponemos axiomas adicionales como la hipótesis del continuo generalizada.

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

4.29, el teorema siguiente (enunciado para cardinales no necesariamente bien ordenables) es una forma equivalente del axioma de elección:

Teorema 5.1 *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 5.2 *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 5.3 (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 5.2, muchos de los resultados sobre exponenciación cardinal involucran la función 2^κ, la cual, ciertamente, es el esqueleto de la exponenciación cardinal. Por ello es conveniente darle un nombre:

Definición 5.4 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

$$2^{\aleph_0} = \aleph_5 \land 2^{\aleph_1} = \aleph_3.$$

Más en general, la función del continuo ha de respetar la monotonía:

$$\kappa \leq \mu \rightarrow 2^\kappa \leq 2^\mu.$$

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 4.54 y, más concretamente, del teorema siguiente:

Teorema 5.5 (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 $\kappa = \sum\limits_{\alpha < \operatorname{cf} \kappa} \mu_\alpha$. Por el teorema 4.54 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 5.2 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 5.6 (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 5.7 *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 5.8 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 4.35, nos da varias caracterizaciones interesantes de esta operación:

Teorema 5.9 *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, $\mu = \sup\limits_{\nu<\mu} \nu \leq \sup\limits_{\nu<\mu} \kappa^\nu$.

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 $\nu < \sup\limits_{\nu<\mu} \kappa^\nu$ y así $\mu = \nu^+ \leq \sup\limits_{\nu<\mu} \kappa^\nu$. 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, $\sup\limits_{\nu<\mu} \kappa^\nu \leq \kappa^{<\mu}$ 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 5.10 *Si κ es un cardinal infinito, entonces $2^\kappa = (2^{<\kappa})^{\operatorname{cf}\kappa}$.*

Demostración: Sea $\kappa = \sum\limits_{\alpha<\operatorname{cf}\kappa} \nu_\alpha$, donde $\bigwedge\alpha < \operatorname{cf}\kappa\ \nu_\alpha < \kappa$. Entonces

$$2^\kappa = 2^{\sum\limits_{\alpha<\operatorname{cf}\kappa}\nu_\alpha} = \prod_{\alpha<\operatorname{cf}\kappa} 2^{\nu_\alpha} \leq \prod_{\alpha<\operatorname{cf}\kappa} 2^{<\kappa} = (2^{<\kappa})^{\operatorname{cf}\kappa} \leq (2^\kappa)^{\operatorname{cf}\kappa} = 2^\kappa.$$

■

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 5.2). Comprenderemos mejor esta relación en la sección siguiente. De momento acabamos ésta con algunos resultados técnicos de interés:

Teorema 5.11 *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 5.12 Dado un conjunto A y un cardinal κ, llamaremos

$$\begin{aligned} [A]^\kappa &= \{x \mid x \subset A \land |x| = \kappa\}, \\ [A]^{<\kappa} &= \{x \mid x \subset A \land |x| < \kappa\}. \end{aligned}$$

La exponenciación cardinal permite calcular los cardinales de estos conjuntos. El teorema siguiente generaliza a 4.36:

Teorema 5.13 *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,

$$|[A]^{<\kappa}| = \Big|\bigcup_{\mu<\kappa} [A]^\mu\Big| = \sum_{\mu<\kappa} |[A]^\mu| = \sum_{\mu<\kappa} |A|^\mu = |A|^{<\kappa}.$$

■

5.2 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 5.14 (HCG) *Si κ y μ son cardinales y μ es infinito, entonces*

$$\kappa^\mu = \begin{cases} \kappa & \textit{si } \mu < \operatorname{cf}\kappa, \\ \kappa^+ & \textit{si } \operatorname{cf}\kappa \leq \mu \leq \kappa, \\ \mu^+ & \textit{si } \kappa \leq \mu. \end{cases}$$

DEMOSTRACIÓN: Si $\mu < \operatorname{cf}\kappa$ tenemos la inclusión ${}^\mu\kappa \subset \bigcup\limits_{\alpha<\kappa} {}^\mu\alpha$, de donde $\kappa^\mu \leq \sum\limits_{\alpha<\kappa} |\alpha|^\mu$. 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 5.15 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 $\rightarrow$ 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 $\bigwedge\alpha(\aleph_\alpha \text{ regular } \rightarrow 2^{\aleph_\alpha} = \aleph_{\alpha+\omega+5})$. Entonces, usando el teorema 5.10 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 5.16 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 5.17 *Sea κ un cardinal singular.*

a) Si la función del continuo es finalmente constante bajo κ, entonces

$$2^\kappa = 2^{<\kappa}.$$

b) En caso contrario $2^\kappa \geq (2^{<\kappa})^+$ y si suponemos la HCS *tenemos la igualdad.*

DEMOSTRACIÓN: En el caso a), sea $\mu < \kappa$ tal que si $\mu \leq \nu < \kappa$ entonces $2^\nu = 2^\mu$. Así, $2^{<\kappa} = 2^\mu$ y, por 5.10, tenemos que $2^\kappa = (2^\mu)^{\operatorname{cf}\kappa} = 2^{\mu \operatorname{cf}\kappa} = 2^\mu$.

En el caso b), 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 4.61 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 5.18 (HCS) *Sean κ y μ cardinales infinitos. Entonces*

$$\kappa^\mu = \begin{cases} \kappa & \textit{si } 2^\mu < \kappa \land \mu < \operatorname{cf}\kappa, \\ \kappa^+ & \textit{si } 2^\mu < \kappa \land \operatorname{cf}\kappa \leq \mu, \\ 2^\mu & \textit{si } \kappa \leq 2^\mu. \end{cases}$$

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 $\kappa = \sum\limits_{\alpha<\operatorname{cf}\kappa} \nu_\alpha$, 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

$$\bigwedge\alpha(\aleph_\alpha \text{ regular } \rightarrow 2^{\aleph_\alpha} = \aleph_{\alpha+\omega+5}),$$

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 5.19 *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 4.52 y conjeturó que si $\{\kappa_\alpha\}_{\alpha<\lambda}$ es una sucesión estrictamente creciente de cardinales ≥ 2 y $\kappa = \sup\limits_{\alpha<\lambda} \kappa_\alpha$, 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 4.52 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 $\kappa = \aleph_{\omega_1+\omega}$ y el producto sigue valiendo $\aleph_{\omega_1\cdot 2}^{\aleph_0} = \aleph_{\omega_1\cdot 2}$. Por otra parte la HCS implica la conjetura de Tarski:

Teorema 5.20 (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 5.18,

$$\kappa^{|\lambda|} = 2^{|\lambda|} = \prod_{\alpha<\lambda} 2 \leq \prod_{\alpha<\lambda} \kappa_\alpha \leq \kappa^{|\lambda|}.$$

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 5.18. ■

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

$$\aleph_{\omega_1}^{\aleph_1} \cdot \aleph_{\omega_1\cdot 2+\omega}^{\aleph_0} \leq 2^{\aleph_{\omega_1}} \aleph_{\omega_1\cdot 2+\omega+1} = \aleph_{\omega_1\cdot 2+\omega+1} < \aleph_{\omega_1\cdot 2+\omega}^{|\omega_1+\omega|}.$$

■

5.3 Cardinales fuertemente inaccesibles

Vamos a estudiar ahora una versión fuerte de los cardinales inaccesibles que introdujimos en el capítulo anterior.

Definición 5.21 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 μ, $\nu < \kappa$, 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 5.22 *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 ${}^\mu\kappa = \bigcup\limits_{\alpha<\kappa} {}^\mu\alpha$ 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.[1]

Definición 5.23 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:

Teorema 5.24 *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,

$$\beth_\gamma \leq \kappa < \beth_{\gamma+1} = 2^{\beth_\gamma}.$$

[1] Bet ($\beth$) es la segunda letra del alfabeto hebreo.

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 4.71:

Teorema 5.25 *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 5.26 $\bigwedge\alpha\ |\mathrm{V}_{\omega+\alpha}| = \beth_\alpha$. *En particular,* $\bigwedge\alpha(\omega^2 \leq \alpha \rightarrow |\mathrm{V}_\alpha| = \beth_\alpha)$.

(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 5.27 *Si κ es un cardinal fuertemente inaccesible se cumple que*

$$\bigwedge x(x \in V_\kappa \leftrightarrow x \subset V_\kappa \land |x| < \kappa).$$

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

$$\Omega_2 = \{\alpha \in \Omega \mid \bigwedge \delta \leq \alpha (\delta \text{ es inaccesible} \rightarrow \delta = \Omega_1)\}$$

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[2]

(AEG) $\bigvee F(F : \mathrm{V} \longrightarrow \mathrm{V} \land \bigwedge x(x \neq \varnothing \to F(x) \in X)).$

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 5.28 (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 5.26 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

$$f_\alpha : \mathrm{V}_{\omega+\alpha+1} \setminus \mathrm{V}_{\omega+\alpha} \longrightarrow \beth_{\alpha+1} \setminus \beth_\alpha \text{ biyectivas.}$$

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 2.29 concluimos que $F[A]$ es semejante a Ω (y A es equipotente a $F[A]$), luego toda clase propia es equipotente a Ω. ■

[2]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.

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. Podría decirse que si una clase no es un conjunto es “a causa” de un “exceso de tamaño”.

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 $\delta \in C$. 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 $\bigcap\limits_{\alpha<\beta} C_\alpha$ 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 $\bigcap\limits_{\alpha<\beta} C_\alpha$ no está acotado.

Sea $f_\alpha : \lambda \longrightarrow \lambda$ la función dada por $f_\alpha(\delta) = \min\{\epsilon \in C_\alpha \mid \delta < \epsilon\}$. 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 $g(\delta) = \sup\limits_{\alpha<\beta} f_\alpha(\delta)$. 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 4.63.

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 $\delta < g^\omega(\delta) \in \bigcap\limits_{\alpha<\beta} C_\alpha$, 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. 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 2.28, $\operatorname{ord} C \leq \kappa$ 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 $f(\lambda) = \bigcup\limits_{\delta<\lambda} f(\delta)$. 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 $\bigcup\limits_{\delta<\lambda} f(\delta) \in \kappa$ y como C es cerrado tenemos que $\bigcup\limits_{\delta<\lambda} f(\delta) \in C$, 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 2.28 aplicamos 2.29, 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 4.65 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 $f(\lambda) = \bigcup\limits_{\delta<\lambda} f(\delta)$. 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*

$$C = \{\alpha < \kappa \mid \bigwedge fn(f \in A \land f : {}^n\kappa \longrightarrow \kappa \to f[{}^n\alpha] \subset \alpha)\}$$

es c.n.a. en κ.

Demostración: Sea $\lambda < \kappa$ tal que $C \cap \lambda$ no esté acotado en λ, sea $f \in A$, $f :^n \kappa \longrightarrow \kappa$, tomemos ordinales $\epsilon_1, \ldots, \epsilon_n \in \lambda$ 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 $\lambda \in C$, el cual 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, para cada $f \in A$, $f : {}^n\kappa \longrightarrow \kappa$ sea β_f el mínimo ordinal tal que $f[{}^n\alpha_m] \subset \beta_f < \kappa$ (existe porque $|f[{}^n\alpha_m]| \leq |{}^n\alpha_m| < \kappa$, luego $f[{}^n\alpha_m]$ está acotado en κ).

Definimos $\alpha_{m+1} = \bigcup\limits_{f \in A} \beta_f < \kappa$, pues $|A| < \kappa$ y κ es regular. Finalmente definimos $\alpha^* = \sup\limits_{m \in \omega} \alpha_m \in \kappa$. Claramente $\alpha \leq \alpha^*$. Si probamos que $\alpha^* \in C$ tendremos que C es no acotado.

Tomemos una función $f \in A$, $f :^n \kappa \longrightarrow \kappa$ y 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

$$f(\epsilon_1, \ldots, \epsilon_n) \in f[{}^n\alpha_m] \subset \beta_f \leq \alpha_{m+1} \leq \alpha^*,$$

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. 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

$$\mathop{\triangle}_{\alpha<\kappa} X_\alpha = \{\gamma < \kappa \mid \gamma \in \bigcap_{\alpha<\gamma} X_\alpha\}.$$

Si intentamos probar algo "razonable" y "nos gustaría" que una intersección de κ conjuntos c.n.a. 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 $\mathop{\triangle}\limits_{\alpha<\kappa} C_\alpha$ 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 α, $\beta < \epsilon$. 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 α, $\delta < \epsilon$. Así $\delta < g(\epsilon) \in \lambda \cap C_\alpha$. ■

Los resultados que hemos obtenido sobre los conjuntos cerrados no acotados en un ordinal límite λ se interpretan más adecuadamente con ayuda de la noción siguiente:

Definición 6.10 Un *filtro* en un conjunto X es una familia $F \subset \mathcal{P}X$ que cumpla las propiedades siguientes:

a) $X \in F \land \varnothing \notin F$,

b) $\bigwedge y \in F \bigwedge x \in X(y \subset x \rightarrow x \in F)$,

c) $\bigwedge xy \in F\ x \cap y \in F$.

Si κ es un cardinal infinito, un filtro F es κ-completo si para toda familia $\{x_\delta\}_{\delta<\alpha}$ de $\alpha < \kappa$ elementos de F se cumple que $\bigcap\limits_{\delta<\alpha} x_\delta \in F$.

Un *ideal* en un conjunto X es una familia $I \subset \mathcal{P}X$ que cumpla las propiedades siguientes:

a) $X \notin I \land \varnothing \in I$,

b) $\bigwedge y \in I \bigwedge x \in X(x \subset y \rightarrow x \in I)$,

c) $\bigwedge xy \in I\ x \cup y \in F$.

Un ideal I es κ-completo si para toda familia $\{x_\delta\}_{\delta<\alpha}$ de $\alpha < \kappa$ elementos de I se cumple que $\bigcup\limits_{\delta<\alpha} x_\delta \in I$.

La idea subyacente en estas definiciones es que un filtro es una familia de conjuntos que pueden ser considerados "muy grandes". La primera propiedad establece que el mayor conjunto posible es muy grande, mientras que el conjunto vacío no lo es, la segunda que todo conjunto que contiene a un conjunto muy grande es muy grande y la tercera que la intersección de dos conjuntos muy grandes, aunque es algo más pequeña, sigue siendo muy grande.

En general, todo filtro es $\aleph_0$-completo, es decir, que la intersección de un número finito de conjuntos muy grandes es muy grande. Cuanto más se pueda mejorar esto (es decir, si F es κ completo, para un cardinal mayor) más justificado está el "muy" cuando hablamos de "conjuntos muy grandes".

La definición de ideal se interpreta análogamente cambiando "muy grande" por "muy pequeño". Las dos definiciones están relacionadas del modo siguiente: para cada familia $A \subset \mathcal{P}X$, definimos su familia *dual* como

$$A' = \{X \setminus x \mid x \in A\}.$$

Es inmediato comprobar que el dual de un filtro κ-completo es un ideal κ-completo, y viceversa. Informalmente, podemos considerar como conjuntos "muy pequeños" a los que tienen complementario "muy grande" y viceversa.

Los conjuntos cerrados no acotados no forman por sí mismos un filtro, pero generan uno, en el sentido siguiente:

Sea λ un ordinal límite de cofinalidad no numerable. Definimos el *filtro de cerrados no acotados* en λ como el conjunto

$$\text{c.n.a.}(\lambda) = \{X \subset \lambda \mid \bigvee C(C \subset X \land C \text{ es c.n.a. en } \lambda\} \subset \mathcal{P}\lambda.$$

Es inmediato comprobar que realmente es un filtro $\operatorname{cf}\lambda$-completo, por lo que podemos considerar también su ideal dual $\text{c.n.a.}(\lambda)'$. Más aún, es claro que si $\delta < \lambda$ entonces $\lambda \setminus \delta$ es c.n.a. en λ, luego $\lambda \setminus \delta \in \text{c.n.a.}(\lambda)$, luego $\delta \in \text{c.n.a.}(\lambda)'$. En particular, como $\{\delta\} \subset \delta + 1 \in \lambda$, tenemos que

$$\bigwedge \delta \in \lambda \ \{\delta\} \in \text{c.n.a.}(\lambda)'$$

y por la completitud,

$$\bigwedge x(x \subset \lambda \land |x| < \operatorname{cf}\lambda \to x \in \text{c.n.a.}(\lambda)'),$$

ya que podemos expresar $x = \bigcup\limits_{\delta \in x} \{\delta\}$. Esto se interpreta como que respecto del filtro de cerrados no acotados en λ, todos los conjuntos de cardinal menor que $\operatorname{cf}\lambda$ son considerados "muy pequeños".

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 demasiado pequeño”:

Definición 6.11 Sea λ un ordinal de cofinalidad no numerable. Un conjunto $E \subset \lambda$ es *estacionario* en λ si $E \notin \text{c.n.a.}(\lambda)'$.

He aquí las propiedades elementales de los conjuntos estacionarios:

Teorema 6.12 *Sea λ un ordinal de cofinalidad no numerable y $E \subset \lambda$. Se cumple:*

a) Si E es c.n.a en λ entonces E es estacionario en λ.

b) E es estacionario en λ si y sólo si corta a todo c.n.a. en λ.

c) Si E es estacionario en λ entonces no está acotado en λ.

d) Si E es estacionario y C es c.n.a. en λ entonces $E \cap C$ es también estacionario en λ.

Demostración: a) es inmediato: si E no fuera estacionario entonces $\lambda \setminus E$ contendría un c.n.a. disjunto de E.

b) E es estacionario si y sólo si $\lambda \setminus E \notin c.n.a.(\lambda)$, 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.

c) Se sigue de b) junto con el hecho obvio de que si $\alpha \in \lambda$ entonces $\lambda \setminus \alpha$ es c.n.a.

d) 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. ∎

La propiedad b) es tal vez la más significativa: un conjunto estacionario no es necesariamente “muy grande”, pero es lo suficientemente grande como para cortar a cualquier conjunto “muy grande”.

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 el conjunto*

$$\{\alpha < \lambda \mid \operatorname{cf}\alpha = \kappa\}$$

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

$$\bigwedge \alpha \in A(\alpha \neq 0 \rightarrow f(\alpha) < \alpha).$$

Teorema 6.15 (Fodor) *Sea κ un cardinal regular no numerable y $E \subset \kappa$. Las afirmaciones siguientes son equivalentes:*

a) E es estacionario en κ,

b) 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,

c) 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: a) → b) 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 $\gamma \in \bigcap\limits_{\alpha<\gamma} C_\alpha$. Sea $\delta = f(\gamma) < \gamma$. Así $\gamma \in f^{-1}[\{\delta\}] \cap C_\delta = \varnothing$.

b) → c) es obvio.

c) → a) 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 c). 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 previo auxiliar.

Teorema 6.16 *Sea κ un cardinal regular no numerable y sea E un subconjunto estacionario en κ. Entonces el conjunto*

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

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 $\aleph_1$. 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

$f^*_\lambda(0) = \operatorname{mín} C$,

$f^*_\lambda(\alpha + 1) =$ mínimo ordinal $\epsilon \in C$ tal que $f^*_\lambda(\alpha) < \epsilon$ y $f_\lambda(\alpha) < \epsilon$.

$f^*_\lambda(\lambda') = \bigcup\limits_{\delta<\lambda'} f^*_\lambda(\delta)$.

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 $C = \mathop{\triangle}\limits_{\alpha<\kappa} C_\alpha$, 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, $D = \{\gamma \in C \mid \bigwedge \delta < \gamma\ \epsilon(\delta) < \gamma\} = \underset{\delta<\kappa}{\triangle} D_\delta$ 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:*

a) 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.

b) Si no se cumple la HCS, *entonces el mínimo cardinal que no la cumple tiene cofinalidad numerable.*

c) 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* $\bigwedge\nu < \kappa\ \nu^\mu < \kappa$, $\mathcal{F} \subset \prod\limits_{\alpha<\mu} A_\alpha$ *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* $\bigwedge\nu < \kappa\ \nu^\mu < \kappa$, $\mathcal{F} \subset \prod\limits_{\alpha<\mu} A_\alpha$ *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 $\prod\limits_{\alpha<\mu} B_\alpha$, 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

$$\mathcal{F}_f = \{g \in \mathcal{F} \mid \bigvee E \subset E_0 (E \text{ estacionario} \land \bigwedge \alpha \in E\, g(\alpha) \leq f(\alpha))\} = \bigcup_E \mathcal{F}_{f,E},$$

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 $\Big|\bigcup\limits_{\alpha<\kappa^+} \mathcal{F}_\alpha\Big| \leq \sum\limits_{\alpha<\kappa^+} \kappa = \kappa^+$, luego ha de existir una función $f \in \mathcal{F} \setminus \bigcup\limits_{\alpha<\kappa^+} \mathcal{F}_\alpha$.

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 a) 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 ν, $\mu < \kappa_\alpha$ y $2^{\kappa_\alpha} = \kappa_\alpha^+$. Entonces $\nu^\mu \leq \kappa_\alpha^{\kappa_\alpha} = 2^{\kappa_\alpha} = \kappa_\alpha^+ \leq \kappa_{\alpha+1} < \kappa$.

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 $X \neq Y$ entonces f_X y f_Y son casi disjuntas, pues ha de existir un α tal que $X \cap \kappa_\alpha \neq Y \cap \kappa_\alpha$ y entonces $\{\delta < \mu \mid f_X(\delta) = f_Y(\delta)\} \subset \alpha$. En particular, si $X \neq Y$ entonces $f_X \neq f_Y$, luego $|\mathcal{F}| = 2^\kappa$.

Por otra parte $\mathcal{F}$ es una familia casi disjunta de funciones contenida en $\prod\limits_{\alpha<\mu} \mathcal{P}\kappa_\alpha$ y el conjunto $\{\alpha < \mu \mid |\mathcal{P}\kappa_\alpha| = \kappa_\alpha^+\}$ es estacionario en μ. El teorema anterior nos da, entonces, que $2^\kappa = |\mathcal{F}| \leq \kappa^+$. ■

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* $\{\alpha < \mu \mid \kappa_\alpha^{\operatorname{cf}\kappa_\alpha} = \kappa_\alpha^+\}$ *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 $h \neq g$, entonces f_g y f_h son casi disjuntas, pues si $h(\delta) \neq g(\delta)$ y ambos son menores que κ_α, entonces

$$\{\delta < \mu \mid f_h(\delta) = f_g(\delta)\} \subset \alpha + 1.$$

En particular si $h \neq g$ se cumple $f_h \neq f_g$, luego $|\mathcal{F}| = \kappa^\mu$. Además $\mathcal{F}$ es casi disjunta y está contenida en $\prod\limits_{\alpha<\mu} {}^\mu\kappa_\alpha$.

Queremos aplicar el teorema 6.21 para concluir que $\kappa^\mu = |\mathcal{F}| \leq \kappa^+$. Necesitamos, pues, probar que el conjunto $E = \{\alpha < \mu \mid \kappa_\alpha^\mu = \kappa_\alpha^+\}$ es estacionario en μ. Para ello consideramos el conjunto

$$C = \{\lambda < \mu \mid \bigwedge \nu < \kappa_\lambda\ \nu^\mu < \kappa_\lambda\}.$$

Veamos que si $\lambda \in C$ entonces $\kappa_\lambda^{\operatorname{cf}\kappa_\lambda} = \kappa_\lambda^\mu$. De aquí se seguirá que

$$\{\alpha < \mu \mid \kappa_\alpha^{\operatorname{cf}\kappa_\alpha} = \kappa_\alpha^+\} \cap C \subset E$$

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 $\operatorname{cf}\kappa_\lambda = \operatorname{cf}\lambda \leq \lambda < \mu$. Sea $\kappa_\lambda = \sum\limits_{\alpha<\operatorname{cf}\kappa_\lambda} \nu_\alpha$, donde $\bigwedge \alpha < \operatorname{cf}\kappa_\lambda\ \nu_\alpha < \kappa_\lambda$. Así

$$\kappa_\lambda^{\operatorname{cf}\kappa_\lambda} \leq \kappa_\lambda^\mu = \Big(\sum_{\alpha<\operatorname{cf}\kappa_\lambda} \nu_\alpha\Big)^\mu \leq \prod_{\alpha<\operatorname{cf}\kappa_\lambda} \nu_\alpha^\mu \leq \prod_{\alpha<\operatorname{cf}\kappa_\lambda} \kappa_\lambda = \kappa_\lambda^{\operatorname{cf}\kappa_\lambda}.$$

Según lo dicho, ahora sólo queda probar que C es c.n.a. en μ. Para ello definimos $l : \mu \longrightarrow \mu$ mediante

$$l(\alpha) = \min\{\beta < \mu \mid \kappa_\alpha^\mu < \kappa_\beta\}.$$

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 b) del teorema de Silver, y el apartado c) es una consecuencia inmediata. Sea κ el mínimo cardinal que incumple la HCS, es decir, $\kappa > \aleph_0$, $2^{\operatorname{cf}\kappa} < \kappa$, pero $\kappa^{\operatorname{cf}\kappa} > \kappa^+$. Supongamos que $\operatorname{cf}\kappa > \aleph_0$.

Sea $\mu = \operatorname{cf}\kappa$ y $\{\kappa_\alpha\}_{\alpha<\mu}$ como en los teoremas precedentes. Tenemos que la HCS se cumple bajo κ, luego el argumento del teorema 5.18 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 $E = \{\alpha < \mu \mid \operatorname{cf}\kappa_\alpha = \aleph_0 \land 2^{\aleph_0} < \kappa_\alpha\}$. 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 $\{\lambda < \mu \mid \operatorname{cf}\lambda\ (= \operatorname{cf}\kappa_\lambda) = \aleph_0\}$, el cual es estacionario por el teorema 6.13.

Si $\alpha \in E$, entonces $2^{\operatorname{cf}\kappa_\alpha} < \kappa_\alpha$, con $\operatorname{cf}\kappa_\alpha = \aleph_0$ y, como $\kappa_\alpha < \kappa$ cumple la HCS, $\kappa_\alpha^{\operatorname{cf}\kappa_\alpha} = \kappa_\alpha^+$, de modo que $E \subset \{\alpha < \mu \mid \kappa_\alpha^{\operatorname{cf}\kappa_\alpha} = \kappa_\alpha^+\}$. Concluimos que este último conjunto es estacionario y ello nos permite aplicar el teorema anterior, según el cual $\kappa^{\operatorname{cf}\kappa} = \kappa^+$. ■

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:

$$\aleph_\lambda^{\operatorname{cf}\lambda} < \aleph_{(|\lambda|^{\operatorname{cf}\lambda})^+}.$$

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 5.10, 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 $\mu \in C \land \alpha < \mu$. 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”, de modo que si 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 + $\neg$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 $\neg$HCS es que si NBG más la existencia de ciertos cardinales grandes es consistente, también lo es NBG + $\neg$HCS. ■

6.5 Principios combinatorios

Otro contexto en el que aparecen los conjuntos c.n.a. 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:

($\Diamond$) *Existe una sucesión* $\{A_\alpha\}_{\alpha<\omega_1}$ *tal que* $\bigwedge\alpha < \omega_1\ A_\alpha \subset \alpha$ *y que verifica*

$$\bigwedge A \subset \omega_1\ \{\alpha < \omega_1 \mid A \cap \alpha = A_\alpha\} \text{ es estacionario en } \omega_1.$$

A las sucesiones $\{A_\alpha\}_{\alpha<\omega_1}$ que cumplen $\Diamond$ se las llama sucesiones $\Diamond$ (diamante).

Veamos algunas de estas generalizaciones y variantes:

[1]Más concretamente, todos son demostrables a partir del axioma de constructibilidad, $V = L$, que puede probarse que es consistente con NBG.

Definición 6.27 Sea κ un cardinal regular no numerable, para cada $E \subset \kappa$ estacionario consideramos las sentencias:

($\Diamond_E$) Existe una sucesión $\{A_\alpha\}_{\alpha\in E}$ tal que $\bigwedge\alpha \in E\ A_\alpha \subset \alpha$ y que verifica

$$\bigwedge A \subset \kappa\ \{\alpha \in E \mid A \cap \alpha = A_\alpha\} \text{ es estacionario en } \kappa.$$

($\Diamond'_E$) 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

$$\bigwedge A \subset \kappa\ \{\alpha \in E \mid A \cap \alpha \in S_\alpha\} \text{ es estacionario en } \kappa.$$

($\Diamond^*_\kappa$) 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

$$\bigwedge A \subset \kappa \bigvee C\ (C \text{ c.n.a. en } \kappa \wedge C \subset \{\alpha \in \kappa \mid A \cap \alpha \in S_\alpha\}).$$

($\Diamond^+_\kappa$) 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 $\Diamond_E$, $\Diamond'_E$, $\Diamond^*_\kappa$, $\Diamond^+_\kappa$. En particular se llama $\Diamond$, $\Diamond'$, etc. a $\Diamond_{\omega_1}$, $\Diamond'_{\omega_1}$, etc.

Podríamos haber enunciado principios $\Diamond^*_E$ y $\Diamond^+_E$, para conjuntos estacionarios $E \subset \kappa$, como hemos hecho con $\Diamond_E$ y $\Diamond'_E$, 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 $\Diamond_E$. Notemos en primer lugar que si $E \subset E'$ son estacionarios en κ entonces $\Diamond_E \to \Diamond_{E'}$, pues si completamos una sucesión $\Diamond_E$ de cualquier modo, por ejemplo, haciendo $A_\alpha = \varnothing$ para $\alpha \in E' \setminus E$, obtenemos una sucesión $\Diamond_{E'}$, luego $\Diamond_E$ es "más fuerte" cuanto menor es E y así $\Diamond_\kappa$ 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 $\Diamond_E$, pues si una sucesión cumple las condiciones de $\Diamond_E$ excepto ésa, entonces $\{A_\alpha \cap \alpha\}_{\alpha\in E}$ es una sucesión $\Diamond_E$, 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 $\Diamond_{\kappa^+} \to 2^\kappa = \kappa^+$.*

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 $\kappa > \omega$, 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 $\diamondsuit_{\kappa^+}$.

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

$$f(\alpha) = \min\{\beta < \kappa^+ \mid X_\beta = \bigcup_{j<\mu} (\{j\} \times (Z_j \cap (\kappa \times \alpha)))\}.$$

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 $C = \bigcap\limits_{i<\kappa} C_i \cap C^*$. 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 $A_0^\delta = \bigcup\limits_{i<\mu} B_i^\delta$. 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. $C_\gamma \subset \bigcap\limits_{\tau<\gamma} C_\tau$ tal que, para todo $\delta \in E \cap C_\gamma$ que cumpla

$$\sup\{\alpha < \delta \mid \bigvee \beta < \delta \ (\alpha, \beta) \in V_{\gamma+1}^\delta\} = \delta,$$

se tiene que $V_{\gamma+1}^\delta \subsetneq V_\gamma^\delta$, 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 $\diamondsuit_E \rightarrow \diamondsuit_{E'}$. 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 $E = \bigcup\limits_{\delta<\kappa} E_\delta$ 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 $\Diamond_E$ y $\Diamond'_E$: 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 $\Diamond_E$ fijada a priori. En cambio, $\Diamond'_E$ 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 $\Diamond_E \rightarrow \Diamond'_E$, pues si $\{A_\alpha\}_{\alpha\in E}$ es una sucesión $\Diamond_E$, entonces basta definir $S_\alpha = \{A_\alpha\}$ para tener una sucesión $\Diamond'_E$. 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 $\Diamond_E \leftrightarrow \Diamond'_E$.*

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 $\Diamond'_E$, 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 $\Diamond'_E$, 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 $\Diamond_E$. 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 $X = \bigcup\limits_{\delta<\kappa} (\{\delta\} \times X_\delta)$ y $C = \bigcap\limits_{\delta<\kappa} C_\delta$, 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

$$\bigwedge A \subset \kappa \bigvee C\ (C \text{ c.n.a. en } \kappa \land C \subset \{\alpha \in \kappa \mid A \cap \alpha = A_\alpha\}).$$

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* $\Box_\kappa(E)$ 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:

a) C_λ es c.n.a. en λ.

b) Si $\operatorname{cf}\lambda < \kappa$, entonces $|C_\lambda| < \kappa$.

c) 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 $\Box_\kappa(E)$. Llamaremos $\Box_\kappa \equiv \Box_\kappa(\varnothing)$.

Observemos que si $E \subset E' \subset \kappa^+$, se cumple que $\Box_\kappa(E') \to \Box_\kappa(E)$, por lo que $\Box_\kappa$ es el más débil de los cuadrados sobre κ.

Los principios $\Box_\omega(E)$ 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 $\Box_\kappa(E)$ 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, $\Box_\kappa$ implica el caso no trivial de $\Diamond_E$ 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 $\Box_\kappa \to \Diamond_W$.*

Demostración: Si $\operatorname{cf}\kappa > \aleph_0$ entonces se cumple $\Diamond_W$ 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 $\{c_\delta^\lambda\}_{\delta<\theta_\lambda}$ la semejanza $\theta_\lambda \longrightarrow C_\lambda$. Sea $\kappa = \bigcup\limits_{\beta<\kappa} A_\beta$ una partición de κ en subconjuntos de cardinal κ disjuntos dos a dos. Sea $f_\beta^\alpha : \Gamma_\alpha \longrightarrow A_\beta$ inyectiva. Para cada $\lambda < \kappa^+$ definimos $f_\lambda : \Gamma_\lambda \longrightarrow \kappa$ mediante $f_\lambda(x) = f_\delta^{c_\delta^\lambda}(x)$, donde $\delta < \theta_\lambda$ es el menor ordinal tal que $x \in \Gamma_{c_\delta^\lambda}$. 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 $c_\delta^\lambda = c_\delta^{\lambda'}$ 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 $S_\lambda = \{\bigcup f_\lambda^{-1}[x] \mid x \subset \kappa \land |x| \leq \aleph_0 \land x \text{ acotado en } \kappa\}$. 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 $\Diamond'_W$.

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

$$A = \{\lambda \in \kappa^+ \mid \bigwedge \lambda' < \lambda \; X \cap \lambda' \in \Gamma_\lambda\}.$$

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 $\gamma = \bigcup\limits_{i\in\omega} \gamma_i$ 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 $X \cap \lambda' = \bigcup\limits_{i\in\omega} X \cap b_{\gamma_i} = \bigcup f_\lambda^{-1}[x]$, 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:

a) B_λ es cerrado en λ.

b) Si $\operatorname{cf}\lambda > \aleph_0$, entonces B_λ no está acotado en λ.

c) Si $\lambda' \in B_\lambda$, entonces $B_{\lambda'} = B_\lambda \cap \lambda'$.

d) 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 $\alpha < \bigcup\limits_{n<\omega} \lambda_n \in B_\lambda$.

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 $|B_\lambda| \leq |A_\lambda| < \kappa$, luego se cumple d).

De las propiedades c) y d) se sigue que $\operatorname{ord} B_\lambda \leq \kappa$.

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:

$$\kappa = |B_{f(\kappa)}| \leq |B_{f(\kappa+\omega)}| < \kappa.$$

Llamamos $W_\delta = \{\lambda \in W \mid \operatorname{ord} B_\lambda = \delta\}$, de modo que $W = \bigcup\limits_{\delta\leq\kappa} W_\delta$. Entonces existe un $\delta \leq \kappa$ 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 $\bigcap\limits_{\delta\leq\kappa} C_\delta$ 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 $C_\lambda = \bigcup\limits_{\lambda' \in D_\lambda} C_{\lambda'}$ y en caso contrario (lo que implica que $\operatorname{cf} \lambda = \aleph_0$), definimos $C_\lambda = \bigcup\limits_{\lambda' \in D_\lambda} C_{\lambda'} \cup \{\alpha_n^\lambda \mid n \in \omega\}$, donde $\{\theta_n^\lambda\}_{n\in\omega}$ es una sucesión cofinal creciente en λ tal que $\theta_0^\lambda = \bigcup\limits_{\lambda' \in D_\lambda} C_{\lambda'}$.

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 $\bigcup\limits_{\lambda' \in D_\lambda} C_{\lambda'}$. 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 $\Box_\kappa$, existe un conjunto $E \subset \kappa^+$ estacionario tal que $\Box_\kappa(E)$ y $\Diamond_E$.*

Terminamos demostrando que $\Box_\kappa$ es equivalente esta variante:

Definición 6.37 Si κ es un cardinal infinito, llamamos $\Box'_\kappa$ a la afirmación siguiente: existe una sucesión $\{B_\lambda\}_{\lambda<\kappa^+}$ tal que:

a) B_λ es cerrado en λ y está formado por ordinales límite.

b) Si $\operatorname{cf} \lambda > \aleph_0$ entonces B_λ no está acotado en λ.

c) $\operatorname{ord} B_\lambda \leq \kappa$.

d) Si $\lambda' \in B_\lambda$, entonces $B_{\lambda'} = B_\lambda \cap \lambda'$.

A las sucesiones que cumplen esto se las llama sucesiones $\Box'_\kappa$.

Se cumple trivialmente $\Box'_\omega$, sin más que tomar todos los B_λ vacíos.

Teorema 6.38 *Para todo cardinal infinito κ, se cumple que $\Box_\kappa \leftrightarrow \Box'_\kappa$.*

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 $\Box_\kappa$, 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 $\Box'_\kappa$.)

Supongamos ahora que $\{B_\lambda\}_{\lambda<\kappa^+}$ es una sucesión $\Box'_\kappa$ y definamos C_λ como en 6.35:

Si B_λ no está acotado en λ, definimos $C_\lambda = \bigcup\limits_{\lambda'\in B_\lambda} C_{\lambda'}$ y en caso contrario (lo que implica que $\operatorname{cf}\lambda = \aleph_0$), definimos $C_\lambda = \bigcup\limits_{\lambda'\in B_\lambda} C_{\lambda'} \cup \{\alpha_n^\lambda \mid n\in\omega\}$, donde $\{\theta_n^\lambda\}_{n\in\omega}$ es una sucesión cofinal creciente en λ tal que $\theta_0^\lambda = \bigcup\limits_{\lambda'\in B_\lambda} C_{\lambda'}$.

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.
- $\operatorname{ord} C_\lambda \leq \kappa$.

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 $\geq \kappa+1$ 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 $\kappa = \operatorname{cf}\kappa \leq \operatorname{cf}\lambda$.

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 $\eta_\lambda \leq \kappa$.

Si $\theta_\alpha < \eta_\lambda \leq \theta_{\alpha+1}$ 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 $\lambda' \leq \mu$, 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 $\epsilon < \delta$,

$$f_\lambda^{(\epsilon)}\Big(\bigcup_{\alpha<\lambda'} f_\lambda^{(\delta)}(\alpha)\Big) = \bigcup_{\alpha<\lambda'} f_\lambda^{(\epsilon)}(f_\lambda^{(\delta)}(\alpha)) = \bigcup_{\alpha<\lambda'} f_\lambda^{(\delta)}(\alpha),$$

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 2.51 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 2.52 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 2.56 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 $\phi_\delta(\kappa) = \bigcup\limits_{\epsilon<\kappa} \phi_\delta(\epsilon) \leq \kappa$, 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:*

a) $\delta = \epsilon \land \alpha = \beta$,

b) $\delta < \epsilon \land \alpha = \phi_\epsilon(\beta)$,

c) $\epsilon < \delta \land \beta = \phi_\delta(\alpha)$.

Similarmente, la desigualdad $\phi_\delta(\alpha) < \phi_\epsilon(\beta)$ sólo puede darse en uno de los tres casos siguientes:

a) $\delta = \epsilon \land \alpha < \beta$,

b) $\delta < \epsilon \land \alpha < \phi_\epsilon(\beta)$,

c) $\epsilon < \delta \land \phi_\delta(\alpha) < \beta$.

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 $\alpha < \phi_\xi(0) \rightarrow \alpha < \xi$.

Para $\alpha = 0$ es trivial. Supongamos que vale para todo $\delta < \alpha < \phi_\xi(0)$. Descomponemos $\alpha = \omega^\eta + \beta$, con $\beta < \alpha$ (teorema 2.53). 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 2.54), 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 $\xi = \xi' \land \eta = \eta'$ o $\xi' < \xi \land \eta' = \phi_\xi(\eta) \geq \eta$ 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

El sistema numérico

Para terminar de perfilar a NBG como teoría capaz de formalizar todo el razonamiento matemático, veremos ahora que permite definir los conjuntos numéricos que intervienen en prácticamente todas las ramas de la matemática, y a partir de los cuales construyen la mayoría de sus objetos de estudio: ya hemos definido los números naturales y aquí presentaremos los números enteros, los números racionales y los números reales. Para completar el sistema numérico usual faltarían los números complejos, pero no entraremos en su construcción porque no los vamos a necesitar y ésta es trivial desde un punto de vista conjuntista.

Por el contrario, el conjunto $\mathbb{R}$ de los números reales representa un papel nada trivial en la teoría de conjuntos, ya que está relacionado directa o indirectamente con muchos de los problemas estudiados en ella.

Para la construcción de $\mathbb{Z}$ y $\mathbb{Q}$ bastan los axiomas de NBG* + AI, así que empezaremos trabajando en esta teoría salvo que se indique lo contrario. Para construir los números reales será necesario añadir el axioma de partes AP. Algunos resultados aislados requerirán el axioma de elección, pero sólo en su forma débil AEN (el axioma de elección numerable).

7.1 Los números enteros

En el conjunto ω 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 ω 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 $\mathbb{Z} = \omega \times \omega$ 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 7.1 Definimos en $\omega\times\omega$ 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 $\mathbb{Z}=(\omega\times\omega)/R$. 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 $n\in\omega$, definimos $+n\equiv[n,0]$. Observamos que

$$+m=+n \leftrightarrow m=n, \quad +m+(+n)=+(m+n), \quad (+m)(+n)=+(mn).$$

Definimos $\mathbb{N} \equiv \{+n \mid n \in \omega\}$. Tenemos entonces que la aplicación $i : \omega \longrightarrow \mathbb{N}$ dada por $i(n) = +n$ es biyectiva 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 ω o con los de $\mathbb{N}$, porque se suman y se multiplican igual. Si en ω 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

$$\mathbb{Z}^+ = \{+n \mid n \in \omega \setminus \{0\}\}, \qquad \mathbb{Z}^- = \{-n \mid n \in \omega \setminus \{0\}\}$$

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 ω a $\mathbb{Z}$ para formar un anillo ordenado. 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 30). Para comprobar la segunda, es decir, que

$$\bigwedge ab \in \mathbb{Z}(a \geq 0 \wedge b \geq 0 \rightarrow ab \geq 0),$$

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 $m, n \in \omega$, entonces $m \leq n \leftrightarrow +m \leq +n$, lo cual significa que ω y $\mathbb{N}$ 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

$$\bigwedge mn \in \omega\ (-m < -n \leftrightarrow n < m),$$

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 $\mathbb{N}$ y, como tiene las mismas propiedades que ω, 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.

Una última propiedad relevante de la aritmética básica de los números enteros es que admite la división euclídea en los términos siguientes:

Teorema 7.2 $\bigwedge Dd \in \mathbb{Z}(d \neq 0 \rightarrow \overset{1}{\bigvee} cr \in \mathbb{Z}\ (D = dc + r \wedge 0 \leq r < d))$

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

$$0a = 0 \land \bigwedge n \in \mathbb{N}\ (n+1)a = na + a.$$

Equivalentemente, $na = \sum\limits_{i<n} a$. 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 7.3 *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 $\bigwedge mn \in \mathbb{Z}(m < n \rightarrow i(m) < i(n))$, 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 $m < n \lor m = n$, luego $i(m) < i(n) \lor i(m) = i(n)$, 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 7.4 Diremos que un anillo ordenado A es *arquimediano* si $\mathbb{N}$ no está acotado superiormente en A, es decir, si[1] $\bigwedge a \in A \bigvee n \in \mathbb{N}\ a < n$.

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:

$$a = E[a] + F[a], \qquad E[A] \in \mathbb{Z}, \quad 0 \leq F[a] < 1.$$

7.2 Los números racionales

La construcción del cuerpo $\mathbb{Q}$ de los números racionales la hemos llevado ya a cabo en un contexto general:

Definición 7.5 Definimos el cuerpo de los *números racionales* al cuerpo de cocientes $\mathbb{Q}$ de $\mathbb{Z}$ construido en la página 34.

[1]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 $a < n$.

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 $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$. La aritmética cardinal implica trivialmente que $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$.

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 7.6 *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 7.7 Se dice que un conjunto ordenado $(A, \leq)$ es *denso* (en sí mismo) si $\bigwedge ab \in A(a < b \rightarrow \bigvee c \in A \; a < c < b)$.

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 7.8 *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

$$a < \frac{a+b}{2} < b.$$

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 entero 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 7.9 (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 $\mathbb{Q} = \{q_n \mid n \in \omega\}$ y $D = \{d_n \mid n \in \omega\}$. Definimos por recurrencia una sucesión de pares $\{(i_k, j_k)\}_{k\in\omega}$ 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 $f = \{(q_{i_k}, d_{j_k}) \mid k \in \omega\}$. 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 $\{i_k\}_{k\in\omega}$. Sea $m \in \omega$ 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).

Ejercicio: Probar que $\mathbb{Q} \oplus \mathbb{Q}$ y $\mathbb{Q} \times \mathbb{Q}$, en ambos casos con el orden lexicográfico, son semejantes a $\mathbb{Q}$.

7.3 Cuerpos métricos completos

Presentamos aquí algunos resultados preliminares a la construcción del conjunto $\mathbb{R}$ de los números reales a partir de $\mathbb{Q}$. Aunque para probar que $\mathbb{R}$ es un conjunto es imprescindible el axioma de partes, en esta sección todavía no lo necesitamos, así que seguimos trabajando en NBG* + AI.

Así como el paso de $\mathbb{N}$ a $\mathbb{Z}$ viene a "remediar" la falta de opuestos para la suma y el paso de $\mathbb{Z}$ a $\mathbb{Q}$ viene a "remediar" la falta de inversos para el producto, el paso de $\mathbb{Q}$ a $\mathbb{R}$ viene a "remediar" una incompletitud más difícil de describir en general. Empezamos presentando los conceptos necesarios para ponerla en evidencia y después veremos cómo subsanarla.

Resulta natural medir la distancia, es decir, la lejanía o proximidad, entre dos números racionales como $d(r, s) = |r - s|$. Como el concepto de distancia resulta útil en muchos otros contextos, conviene tratarlo en un contexto general:

Definición 7.10 Una *distancia* en un conjunto M es una aplicación

$$d : M \times M \longrightarrow R,$$

donde R es un cuerpo ordenado arquimediano,[2] que cumpla las propiedades siguientes:

a) $\bigwedge xy \in M \ (d(x, y) \geq 0 \land (d(x, y) = 0 \leftrightarrow x = y))$,

b) $\bigwedge xy \in M \ d(x, y) = d(y, x)$,

c) $\bigwedge xyz \in M \ d(x, z) \leq d(x, y) + d(y, z)$.

Es obvio que las tres propiedades son exigencias razonables para cualquier aplicación que realmente pueda ser considerada como medida de una distancia. La tercera recibe el nombre de *desigualdad triangular.* De ellas se deduce una cuarta:

$$\bigwedge xyz \in M \ |d(x, y) - d(x, z)| \leq d(y, z).$$

En efecto, $d(x, y) \leq d(x, z) + d(z, y)$, luego $d(x, y) - d(x, z) \leq d(y, z)$. Invirtiendo los papeles de y, z obtenemos igualmente que $d(x, z) - d(x, y) \leq d(y, z)$, luego

$$-d(y, z) \leq d(x, y) - d(x, z) \leq d(y, z),$$

y esto es equivalente a la desigualdad que queremos probar.

[2]En la definición usual se toma $R = \mathbb{R}$, cosa que no podemos hacer aquí porque todavía no hemos definido $\mathbb{R}$. Luego veremos que, en contra de lo que podría parecer, esta definición no es más general.

Un *espacio métrico* es un par (M, d), donde M es un conjunto y d es una distancia en M.

Una aplicación $f : M \longrightarrow N$ entre dos espacios métricos es una *inmersión isométrica* so cumple

$$\bigwedge xy \in M \ d(f(x), f(y)) = d(x, y).$$

Notemos que una inmersión isométrica es necesariamente inyectiva, por la primera condición de la definición de distancia. Una inmersión isométrica biyectiva entre dos espacios métricos es una *isometría.*

Dos espacios métricos son *isométricos* cuando existe una isometría entre ellos. Esto hace que ambos compartan las mismas propiedades definibles en términos de la distancia.

Sobre un cuerpo podemos considerar una clase de distancias que están bien relacionadas con la suma y el producto, a saber, las definidas en términos de valores absolutos:

Un *valor absoluto* en un cuerpo K es una aplicación $|\ \ | : K \longrightarrow R$, donde R es un cuerpo ordenado arquimediano, que cumpla las propiedades siguientes:

a) $\bigwedge x \in K \ (|x| \geq 0 \land (|x| = 0 \leftrightarrow x = 0))$,

b) $\bigwedge xy \in K \ |x + y| \leq |x| + |y|$,

c) $\bigwedge xy \in K \ |xy| = |x||y|$.

Un *cuerpo métrico* es un par $(K, |\ \ |)$, donde K es un cuerpo y $|\ \ |$ es un valor absoluto en K.

En particular, si K es un cuerpo ordenado arquimediano, sabemos que en K hay definido un valor absoluto que cumple claramente la definición anterior, pero no todo valor absoluto en un cuerpo tiene por qué derivar de una relación de orden. Veamos algunas propiedades adicionales de los valores absolutos:

- Si $0 \neq 1$, entonces $|1| = |-1| = 1$,

  pues $|1| = |1 \cdot 1| = |1| \cdot |1|$ y, como por a) $|1| \neq 0$, tiene que ser $|1| = 1$. Por otra parte, $|-1|^2 = |(-1)^2| = |1| = 1$, luego

  $$|-1|^2 - 1 = (|-1| - 1)(|-1| + 1) = 0,$$

  luego $|-1| = 1$ o $|-1| = -1$, pero la segunda opción es imposible porque los valores absolutos son positivos.

- $\bigwedge x \in K \ |x| = |-x|$,

  pues $|-x| = |-1||x| = |x|$.

- Si $x \neq 0$ tiene inverso para el producto, entonces $|x^{-1}| = |x|^{-1}$,

  pues $|x||x^{-1}| = |xx^{-1}| = |1| = 1$.

Ahora es inmediato que si K es un cuerpo métrico, entonces la aplicación $d : K \times K \longrightarrow R$ dada por $d(x, y) = |x - y|$ es una distancia en K. En lo sucesivo consideraremos siempre a cada cuerpo métrico como espacio métrico con esta distancia. Como consecuencia:

$$\bigwedge xy \in K \ ||x| - |y|| \leq |x - y|.$$

En efecto, es un caso particular de la propiedad análoga para espacios métricos, pues

$$||x| - |y|| = |d(0, x) - d(0, y)| \leq d(x, y) = |x - y|.$$

En particular, como $\mathbb{Q}$ es un cuerpo ordenado, podemos considerarlo como cuerpo métrico y a su vez como espacio métrico con la distancia definida al principio de la sección.

Una *inmersión isométrica* (resp. *isometría*) entre dos cuerpos métricos es un monomorfismo (resp. isomorfismo) $f : K \longrightarrow L$ tal que $\bigwedge x \in K \ |f(x)| = |x|$.

Es claro que las isometrías de cuerpos métricos son isometrías de espacios métricos, y hacen que dos cuerpos métricos isométricos compartan las mismas propiedades definibles en términos de la métrica, la suma y el producto.

Notemos también que todo isomorfismo de cuerpos ordenados es claramente una isometría de cuerpos métricos.

Ahora estamos en condiciones de definir los conceptos que ponen en evidencia la presencia de "agujeros microscópicos" en $\mathbb{Q}$:

Definición 7.11 Una sucesión $\{x_n\}_{n\in\omega}$ en un espacio métrico M *converge* a un *límite* $l \in M$ si[3]

$$\bigwedge \epsilon > 0 \bigvee m \in \omega \bigwedge n \geq m \ d(x_n, l) < \epsilon.$$

La sucesión es *de Cauchy* si

$$\bigwedge \epsilon > 0 \bigvee m \in \omega \bigwedge nn' \geq m \ d(x_n, x_{n'}) < \epsilon.$$

La sucesión está *acotada* si existe un $x \in M$ y un $C \in R$ de modo que

$$\bigwedge n \in \omega \ d(x_n, x) \leq C.$$

Un conjunto $D \subset M$ es *denso* en M si $\bigwedge x \in M \bigwedge \epsilon > 0 \bigvee d \in D \ d(x, d) < \epsilon$.

Vamos a analizar estos conceptos:

Que una sucesión converja a un límite l significa que sus términos se aproximan cada vez más a l hasta hacerse prácticamente indistinguibles de l. Por

[3] En lo sucesivo sobrentenderemos que la letra ϵ representa siempre un elemento del cuerpo R donde toma imágenes la distancia, mientras que m, n representarán siempre números naturales.

ejemplo, si una sucesión en $\mathbb{Q}$ converge a 1 tenemos que, para $\epsilon = 1/1\,000\,000$, existe un $m \in \omega$ tal que todos los términos posteriores a x_m se diferencian de 1 en a lo sumo una millonésima, y si esta aproximación no nos parece suficiente, siempre podemos tomar un ϵ menor, pues aumentando m si es necesario tendremos garantizada la aproximación que deseemos.

Observemos que una sucesión no puede converger a más de un límite, pues si $\{x_n\}_{n\in\omega}$ converge a dos puntos l y l' de un espacio métrico, entonces, para $\epsilon = d(l, l')$, existe un $m \in \omega$ tal que si $n \geq m$ se cumple[4] $d(x_n, l) < \epsilon/2$ y $d(x_n, l') < \epsilon/2$, y entonces tenemos una contradicción:

$$d(l, l') \leq d(l, x_n) + d(x_n, l') < \epsilon/2 + \epsilon/2 = d(l, l').$$

Así pues, si una sucesión $\{x_n\}_{n\in\omega}$ en un espacio métrico M es convergente, representaremos su único límite como

$$\lim_n x_n \in M.$$

A menudo resultará útil el resultado siguiente sobre convergencia en cuerpos ordenados:

Teorema 7.12 *Sea K un cuerpo ordenado y sea $\{x_n\}_{n\in\omega}$ una sucesión convergente en K tal que existen $a, b \in K$ y $m \in \omega$ de modo que $\bigwedge n \geq m\ a \leq x_n \leq b$. Entonces $a \leq \lim\limits_n x_n \leq b$.*

Demostración: Llamemos l al límite y supongamos, por ejemplo que $l < a$. Entonces tomamos $\epsilon = a - l$ y por la definición de convergencia existe un $n \geq m$ tal que $|x_n - l| < \epsilon$ y, como $l < a \leq x_n$, esto equivale a $x_n - l < a - l$, con lo que $x_n < a$, contradicción, luego $a \leq l$. Igualmente se razona que $l \leq b$. ■

Un subconjunto $D \subset M$ de un espacio métrico es denso si todo punto de M tiene puntos de D arbitrariamente próximos. Esto puede expresarse en términos de sucesiones:

Teorema 7.13 *Un subconjunto[5] D de un espacio métrico M es denso si y sólo si todo punto de M es el límite de una sucesión en D.*

Demostración: Si D es denso y $l \in M$, para cada $n \in \omega$ tomamos $d_n \in D$ tal que $d(d_n, l) < \frac{1}{n+1}$. Tenemos así una sucesión $\{d_n\}_{n\in\omega}$ en D que ciertamente converge a l, pues, dado $\epsilon > 0$, como R es arquimediano existe un $m \in \omega$ tal que $1/\epsilon < m$, luego $1/m < \epsilon$, y si $n \geq m$ entonces

$$d(d_n, l) < \frac{1}{n+1} < \frac{1}{m} < \epsilon.$$

[4]En principio tendríamos un m_1 tal que para $n \geq m_1$ se cumpliría la definición de convergencia a l y otro m_2 a partir del cual se cumpliría la definición de convergencia a l', pero si tomamos $m = \max\{m_1, m_2\}$, a partir de m se cumplen las dos. En lo sucesivo aplicaremos tácitamente este argumento con frecuencia.

[5]Este teorema requiere el axioma de elección (numerable) salvo que supongamos que D admite un buen orden (que nos permita tomar como d_n el mínimo elemento de D que cumple la propiedad exigida en la prueba). En realidad, todos los conjuntos densos a los que aplicaremos este teorema serán numerables, por lo que nunca necesitaremos el axioma de elección.

Recíprocamente, si D tiene la propiedad indicada, dado $x \in M$, tomamos una sucesión $\{d_n\}_{n\in\omega}$ en D que converja a x. Dado $\epsilon > 0$ existe un $m \in \omega$ tal que $d(d_m, x) < \epsilon$, y esto prueba que D es denso. ■

Este teorema es una buena ilustración del papel que representa la convergencia de sucesiones en este contexto: un punto $x \in M$ no tiene por qué estar en D, pero podemos encontrar una sucesión de elementos de D que converja a x. Una sucesión puede converger a un punto x sin necesidad de llegar nunca a x, por lo que esto no está reñido con que la sucesión esté contenida en D, un conjunto al cual x no tiene por qué pertenecer. Mediante una sucesión en D elegida oportunamente podemos especificar completamente un punto de fuera de D.

En los cuerpos ordenados los conjuntos densos tienen una caracterización más simple:

Teorema 7.14 *Un subconjunto D de un cuerpo ordenado K es denso si y sólo si $\bigwedge ab \in K\ (a < b \rightarrow \bigvee d \in D\ a < d < b)$.*

Demostración: Si D es denso y $a < b$, consideramos $c = (a + b)/2$ y $\epsilon = (b - a)/2 > 0$. Existe un $d \in D$ tal que $|d - c| < \epsilon$, pero esto quiere decir que $-\epsilon < q - c < \epsilon$, o también $a - c < d - c < b - c$, luego $a < d < b$.

Recíprocamente, si D cumple la condición del enunciado, dado $x \in K$ y $\epsilon > 0$, existe un $d \in D$ tal que $x < d < x + \epsilon$, y entonces $|d - x| = d - x < \epsilon$. ■

El concepto de sucesión acotada es un concepto técnico muy simple: una sucesión está acotada si nunca se aleja más de una distancia C de un punto fijo x. Conviene observar que el punto x podemos elegirlo, en el sentido de que si una sucesión cumple la definición de sucesión acotada con un cierto $x \in M$, entonces la cumple también con cualquier otro $y \in M$, pues

$$d(x_n, y) \leq d(x_n, x) + d(x, y) \leq C + d(x, y),$$

y basta tomar $C' = C + d(x, y)$.

En particular, una sucesión $\{x_n\}_{n\in\omega}$ está acotada en un cuerpo métrico si y sólo si existe un $C \in R$ tal que $\bigwedge n \in \omega\ |x_n| \leq C$ (donde hemos tomado $x = 0$ como punto de referencia para fijar la cota).

Pasamos ahora al concepto más delicado de todos los que hemos introducido: el de sucesión de Cauchy. Empezamos observando su relación obvia con la convergencia:

Teorema 7.15 *Toda sucesión convergente en un espacio métrico es de Cauchy, y toda sucesión de Cauchy está acotada.*

Demostración: Si $\{x_n\}_{n\in\omega}$ converge a l, dado $\epsilon > 0$ existe un $m \in \omega$ tal que si $n \geq m$ entonces $d(x_n, l) < \epsilon/2$, luego si $n, n' \geq m$ tenemos que

$$d(x_n, x_{n'}) \leq d(x_n, l) + d(l, x_{n'}) < \epsilon/2 + \epsilon/2 = \epsilon,$$

luego la sucesión es de Cauchy.

Por otra parte, si la sucesión es de Cauchy, existe un $m \in \omega$ tal que si $n \geq m$ se cumple $d(x_n, x_m) \leq 1$. Sea $C = \text{máx}(\{d(x_k, x_m) \mid k < m\} \cup \{1\})$. Es claro entonces que $\bigwedge n \in \omega\ d(x_n, x_m) \leq C$, luego la sucesión está acotada. ■

Una sucesión es de Cauchy cuando sus términos se aproximan entre sí, hasta hacerse indistinguibles unos de otros, de modo que, superado nuestro umbral de discernimiento, todos ellos se ven "en el mismo punto". Si la sucesión convergente, ese punto donde "se aglomeran" los puntos de la sucesión es el límite, pero la definición de sucesión de Cauchy no exige que exista tal límite. Si una sucesión de Cauchy no tiene límite, entonces sus términos se están "aglomerando" alrededor de "nada", alrededor de "un hueco", de "un agujero microscópico" en el espacio métrico considerado.

Si una sucesión convergente está "señalando" un punto, aunque se acerque sin llegar a él, una sucesión de Cauchy no convergente está "señalando" un agujero, acercándose a él, pero sin "caer" en él (como no puede ser de otra forma, porque la sucesión está hecha de puntos, no de agujeros). Veremos que $\mathbb{Q}$ tiene $2^{\aleph_0}$ agujeros en este sentido, así como que podemos "rellenarlos" y el resultado será el cuerpo $\mathbb{R}$ de los números reales.

Conviene observar que una sucesión de Cauchy está "a punto de converger", en el sentido que precisamos a continuación, para lo cual necesitamos el concepto de subsucesión:

Definición 7.16 Una sucesión $\{y_k\}_{k\in\omega}$ es una *subsucesión* de una sucesión $\{x_n\}_{n\in\omega}$ si existe una sucesión estrictamente creciente $\{n_k\}_{k\in\omega}$ de números naturales (es decir, tal que $k < k' \to n_k < n_{k'}$) de modo que $\bigwedge k \in \omega\ y_k = x_{n_k}$.

Así, una subsucesión avanza por los puntos de la sucesión pero dando saltos de varios a la vez, sin retroceder nunca. Observemos que, en las condiciones de la definición, se cumple que $\bigwedge k \in \omega\ k \leq n_k$, pues es un caso particular del teorema 1.25.

Por ejemplo, es inmediato que toda subsucesión de una sucesión convergente converge al mismo límite, pues si se cumple $d(x_n, l) < \epsilon$ para todo $n \geq m$, también vale $d(x_{n_k}, l) < \epsilon$ para $k \geq m$, ya que entonces $n_k \geq k \geq m$.

Para sucesiones de Cauchy se cumple un recíproco:

Teorema 7.17 *Si una sucesión de Cauchy tiene una subsucesión convergente entonces converge al mismo límite.*

Demostración: Sea $\{x_n\}_{n\in\omega}$ una sucesión de Cauchy en un espacio métrico M y sea $\{x_{n_k}\}_{k\in\omega}$ una subsucesión convergente a l. Entonces, dado $\epsilon > 0$, existe un $m \in \omega$ tal que si $n, n' \geq m$, entonces $d(x_n, x_{n'}) < \epsilon/2$ y si $k \geq m$ entonces $d(x_{n_k}, l) < \epsilon/2$. Así,

$$d(x_n, l) \leq d(x_n, x_{n_k}) + d(x_{n_k}, l) < \epsilon/2 + \epsilon/2 = \epsilon.$$ ■

Una sucesión puede ser muy caótica. Dado que la convergencia de una sucesión de Cauchy puede reducirse a estudiar la convergencia de cualquier subsucesión, resulta útil el teorema siguiente, que proporciona subsucesiones especialmente sencillas:

Teorema 7.18 *Toda sucesión en un conjunto totalmente ordenado contiene una subsucesión monótona.*

DEMOSTRACIÓN: Sea $\{a_n\}_{n=0}^{\infty}$ una sucesión en un conjunto totalmente ordenado. Sea A el conjunto de las imágenes de la sucesión. Si A es finito es obvio que A tiene una subsucesión constante, luego monótona. Supongamos que A es infinito.

Si todo subconjunto no vacío de A tiene mínimo podemos tomar x_0 igual al mínimo de A, luego x_1 igual al mínimo de $A \setminus \{x_0\}$, luego x_2 igual al mínimo de $A \setminus \{x_0, x_1\}$, y así obtenemos puntos $x_0 < x_1 < x_2 < \cdots$, es decir, obtenemos un subconjunto de A sin máximo.

Así pues, o bien existe un subconjunto de A sin mínimo o bien existe un subconjunto de A sin máximo. Los dos casos se tratan igual. Supongamos que hay un subconjunto de A sin mínimo. Llamémoslo B.

Sea a_{n_0} un elemento cualquiera de B. Como B no tiene mínimo contiene infinitos términos de la sucesión bajo a_{n_0}, pero sólo un número finito de ellos tienen índice anterior a n_0, luego existe[6] un cierto a_{n_1} en B de manera que $a_{n_1} < a_{n_0}$ y $n_0 < n_1$. Podemos repetir recurrentemente este proceso y obtener una subsucesión

$$a_{n_0} > a_{n_1} > a_{n_2} > a_{n_3} > a_{n_4} > a_{n_5} > \cdots$$

monótona decreciente. ■

La idea de que las sucesiones de Cauchy "deberían" converger nos lleva al concepto siguiente:

Definición 7.19 Un espacio métrico es *completo* si en él toda sucesión de Cauchy es convergente.

En particular podemos hablar de cuerpos métricos y cuerpos ordenados completos. Veamos en qué se traduce la completitud en el caso concreto de un cuerpo ordenado:

Teorema 7.20 *Sea K un cuerpo ordenado. Las afirmaciones siguientes son equivalentes:*

a) K es completo.

b) Si $\{a_n\}_{n\in\omega}$ y $\{b_n\}_{n\in\omega}$ son sucesiones en K tales que, para todo índice n, se cumpla $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ y $\lim\limits_n (b_n - a_n) = 0$, entonces existe un único $l \in K$ tal que $\bigwedge n \in \omega\ a_n \leq l \leq b_n$.

c) Todo subconjunto no vacío de K acotado superiormente tiene supremo.

[6] Podemos tomar siempre el mínimo número natural, n_1 en este caso, que cumple lo requerido, luego no necesitamos el axioma de elección.

Demostración: a) $\Rightarrow$ b) Supongamos que K es completo y consideremos dos sucesiones en las hipótesis de b). Observamos que $\{a_n\}_{n\in\omega}$ es de Cauchy pues, dado $\epsilon > 0$, tomamos m tal que $|b_m - a_m - 0| < \epsilon$, es decir, $b_m - a_m < \epsilon$. Entonces, si $n' \geq n \geq m$, tenemos que $a_m \leq a_n \leq a_{n'} \leq b_{n'} \leq b_m$, luego $a_{n'} - a_n \leq b_m - a_m < \epsilon$, luego $|a_{n'} - a_n| < \epsilon$ y, con el valor absoluto, la desigualdad vale igualmente si $n' \leq n$.

Por hipótesis existe $l = \lim\limits_n a_n$. Como, para cada $m \in \omega$ se cumple que si $n \geq m$ entonces $a_m \leq a_n \leq b_m$, el teorema 7.12 nos da que $a_m \leq l \leq b_m$.

Ahora supongamos que dos elementos $l, l' \in K$ cumplen $\bigwedge n \in \omega\ a_n \leq l \leq b_n$ y $\bigwedge n \in \omega\ a_n \leq l' \leq b_n$ (no suponemos que l sea el límite anterior). Entonces no perdemos generalidad si suponemos que $l \leq l'$ y, como $a_n \leq l \leq l' \leq b_n$, resulta que $l' - l \leq b_n - a_n$. Si fuera $l \neq l'$, podríamos tomar $\epsilon = l' - l > 0$ y resultaría que no se cumple la definición de convergencia para $\lim\limits_n (b_n - a_n) = 0$. Así pues, l es único.

b) $\Rightarrow$ c) Sea $A \subset K$ un subconjunto no vacío acotado superiormente. Sea $a \in A$ y sea b una cota superior. Si a es también una cota superior entonces es el máximo de A, luego también su supremo. Supongamos, pues, que a no es una cota superior de A. En particular $a < b$.

Vamos a construir recurrentemente una sucesión $\{(a_n, b_n)\}_{n\in\omega}$ en $K \times K$ de modo que $a_n < b_n$ y cada b_n sea una cota superior de A, pero ningún a_n lo sea. Tomamos $(a_0, b_0) = (a, b)$ y, supuesto definido (a_n, b_n), consideramos $c = (a_n + b_n)/2$, de modo que $a_n < c < b_n$, y distinguimos dos casos:

Si c no es cota superior de A, definimos $a_{n+1} = c$, $b_{n_1} = b_n$, mientras que si c es cota superior de A tomamos $a_{n+1} = a_n$, $b_{n+1} = c$.

Teniendo en cuenta que si $c = (a + b)/2$ entonces $b - c = c - a = (b - a)/2$, una simple inducción prueba que

$$b_n - a_n = \frac{b - a}{2^n}.$$

Esto implica que $\lim\limits_n (b_n - a_n) = 0$. En efecto, dado $\epsilon > 0$, como R es arquimediano, existe un $m \in \omega$ tal que $m > (b - a)/\epsilon$, luego si $n \geq m$ se cumple que $2^n \geq n \geq m > (b - a)/\epsilon$, luego $|b_n - a_n| < \epsilon$.

Por a) existe un $l \in K$ tal que $\bigwedge n \in \omega\ a_n \leq l \leq b_n$. Vamos a probar que l es el supremo de A. Tiene que ser una cota superior, porque si no lo fuera existiría un $x \in A$ tal que $l < x$. Pero entonces sería $a_n \leq l < x \leq b_n$ y $\epsilon = x - l$ contradiría la convergencia de $b_n - a_n$ a 0.

Por otro lado, toda cota superior c de A cumple $l \leq c$, pues si fuera $c < l$ tendríamos que $a_n \leq c < l \leq b_n$ y de nuevo tenemos una contradicción con $\epsilon = l - c$.

c) $\Rightarrow$ a) Dada una sucesión de Cauchy en K, para probar que es convergente, basta probar que lo es una cualquiera de sus subsucesiones. Por el teorema 7.18 podemos tomar una subsucesión monótona. Como toda sucesión de Cauchy es acotada y obviamente toda subsucesión de una sucesión acotada está acotada, basta probar que toda sucesión $\{x_n\}_{n\in\omega}$ monótona y acotada es convergente.

No perdemos generalidad si suponemos que es monótona creciente, ya que si es decreciente la sucesión $\{-x_n\}_{n\in\omega}$ es creciente, y si ésta converge a l, la sucesión inicial converge a $-l$ (porque la condición $|-x_n - l| < \epsilon$ es equivalente a $|x_n - (-l)| < \epsilon$).

Es claro que el conjunto $A = \{x_n \mid n \in \omega\}$ es no vacío y está acotado superiormente, luego tiene supremo l. Vamos a probar que dicho supremo es el límite de la sucesión. Dado $\epsilon > 0$, por definición de supremo se cumple que $l-\epsilon$ no es cota superior de A, luego existe un $m \in \omega$ tal que $l - \epsilon < x_m \leq l$, luego si $n \geq m$ tenemos que $l - \epsilon < x_m \leq x_n \leq l$, luego $|x_n - l| = l - x_n < l - (l - \epsilon) = \epsilon$. ■

Nota Observemos que si X es un conjunto totalmente ordenado y $A \subset X$ no es vacío y está acotado superiormente, podemos definir los conjuntos

$$X^- = \{x \in X \mid x \text{ no es cota superior de } A\},$$

$$X^+ = \{x \in X \mid x \text{ es cota superior de } A\},$$

y sucede entonces que $X = X^- \cup X^+$, la unión es disjunta y todo elemento de X^- es menor que todo elemento de X^+. Si A tiene supremo, dicho supremo será el máximo de X^- o bien el mínimo de X^+, según que esté o no en A. Pero si A no tiene supremo, entonces X^- no tiene máximo y X^+ no tiene mínimo. Podemos pensar que cada uno de ellos está a un lado de un “agujero” en X. Si X es un cuerpo ordenado, el argumento empleado en la prueba de b) $\Rightarrow$ c) en el teorema anterior permite construir sucesiones de Cauchy $\{a_n\}_{n\in\omega}$ y $\{b_n\}_{n\in\omega}$ que “se acercan al agujero”, una desde cada lado, sin converger a ningún punto. ■

Veamos ahora cómo tendría que ser un cuerpo ordenado completo:

Teorema 7.21 *Si R es un cuerpo ordenado completo, entonces es arquimediano y $\mathbb{Q}$ es denso en R.*

DEMOSTRACIÓN: Si R no es arquimediano, entonces $\mathbb{N}$ está acotado superiormente. Por el teorema anterior 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 $\mathbb{N}$.

Para probar que $\mathbb{Q}$ es denso en R tomamos un $x \in R$ cualquiera. Entonces, el conjunto $A = \{q \in \mathbb{Q} \mid q < x\}$ no es vacío (porque R es arquimediano, luego existe $n \in \mathbb{N}$ tal que $-x < n$, luego $-n \in A$) y tiene a x por cota superior. Por consiguiente tiene supremo $s \leq x$. Vamos a probar que $s = x$. En caso contrario, como R es arquimediano existe $n \in \mathbb{N}$ tal que $1/(x - s) < n$, luego $s + 1/n < x$. Como $s - 1/n$ no es cota superior de A, existe un $q \in A$ tal que

$s - 1/n < q \leq s$, luego $s < q + 1/n \leq s + 1/n < x$, pero entonces $q + 1/n \in A$, en contradicción con que s es una cota superior.

Así pues, x es el supremo de A, luego, dado $\epsilon > 0$, tenemos que $s - \epsilon$ no es cota de A, luego existe un $q \in A$ tal que $s - \epsilon < q \leq s$, luego $|s - q| < \epsilon$, y esto prueba que $\mathbb{Q}$ es denso en R. ■

Nota No vamos a necesitar este hecho, pero un cuerpo métrico se dice *arquimediano* si existe un $C \in R$ tal que $\bigwedge n \in \mathbb{N}\ |n| \leq C$. Para cuerpos ordenados esta definición coincide con la que hemos dado, pero se pueden construir cuerpos métricos completos no arquimedianos. El teorema anterior sólo asegura que no pueden ser cuerpos ordenados. ■

En un cuerpo ordenado, todos los cuadrados son positivos. Si además es completo se cumple el recíproco:

Teorema 7.22 *Si R es un cuerpo ordenado completo, para cada $x \in R$, $x \geq 0$ existe un único $y \in R$ tal que $y \geq 0 \land y^2 = x$.*

Demostración: Podemos suponer que $x > 0$. Consideremos el conjunto $A = \{u \in R \mid u > 0 \land u^2 < x\}$. Como R es arquimediano, existen números naturales $x < n < n^2$ y $1/x < m < m^2$, con lo que $1/m^2 < x$ y así $1/m \in A$ y n es una cota superior de A. Esto implica que A tiene supremo. Llamémoslo y. Claramente $y > 0$.

Supongamos que $x < y^2$. Tomemos un número natural n tal que $n > 1/y$ y $n > 2y/(y^2 - x)$. Así $2y/n < y^2 - x$ y en consecuencia

$$\left(y - \frac{1}{n}\right)^2 = y^2 - 2y\frac{1}{n} + \frac{1}{n^2} > y^2 - y^2 + x + \frac{1}{n^2} > x.$$

Así, si $u \in A$ tenemos que $u^2 < x < (y - 1/n)^2$, luego $u < y - 1/n$, pero esto significa que $y - 1/n$ es una cota superior de A, en contradicción con que y es el supremo.

Supongamos ahora que $y^2 < x$. Entonces tomamos un número natural n que cumpla $n > 4y/(x - y^2)$ y $n^2 > 2/(x - y^2)$. Así

$$\left(y + \frac{1}{n}\right)^2 = x^2 + 2y\frac{1}{n} + \frac{1}{n^2} < y^2 + \frac{x - y}{2} + \frac{x - y^2}{2} = y^2 + x - y^2 = x,$$

luego $y + 1/n \in A$, y esto supone de nuevo una contradicción. Por lo tanto ha de ser $y^2 = x$.

La unicidad es clara, pues si $z \in R$ cumple $z > 0$, $z \neq y$, entonces $z^2 < y^2$ o $z^2 > y^2$ según si $z < y$ o $z > y$. ■

Esto implica que en un cuerpo ordenado completo la relación de orden está determinada por la suma y el producto: se cumple $x \leq y \leftrightarrow \bigvee z\ y - x = z^2$. Ahora necesitamos un resultado técnico:

Teorema 7.23 *Sea K un cuerpo métrico y $\{a_n\}_{n\in\omega}$, $\{b_n\}_{n\in\omega}$, dos sucesiones convergentes (resp. de Cauchy) en K. Entonces las sucesiones $\{a_n+b_n\}_{n\in\omega}$ y $\{a_nb_n\}_{n\in\omega}$ también son convergentes (resp. de Cauchy) y, en el caso de la convergencia,*

$$\lim_n (a_n+b_n) = \lim_n a_n + \lim_n b_n, \quad \lim_n (a_nb_n) = \lim_n a_n \lim_n b_n.$$

DEMOSTRACIÓN: En el caso de la convergencia, llamaremos $l = \lim_n a_n$, $l' = \lim_n b_n$. Para la suma observamos que

$$|a_{n'}+b_{n'}-a_n-b_n| \leq |a_{n'}-a_n| + |b_{n'}-b_n|,$$

luego, dado $\epsilon > 0$, tomando un $m \in \omega$ tal que $|a_{n'}-a_n| < \epsilon/2$ y $|b_{n'}-b_n| < \epsilon/2$ siempre que $n', n \geq m$, tenemos también que $|a_{n'}+b_{n'}-a_n-b_n| < \epsilon$, luego la suma es de Cauchy. En el caso de la convergencia razonamos análogamente a partir de $|a_n+b_n-l-l'| \leq |a_n-l| + |b_n-l'|$.

Para el producto usamos que

$$|a_{n'}b_{n'}-a_nb_n| = |a_{n'}b_{n'}-a_{n'}b_n+a_{n'}b_n-a_nb_n| \leq |a_{n'}||b_{n'}-b_n| + |a_{n'}-a_n||b_n|,$$

así como que ambas sucesiones están acotadas, de modo que existe un $C \in R$ tal que $|a_n| \leq C$, $|b_n| \leq C$ para todo n. Por lo tanto, dado $\epsilon > 0$, basta tomar un $m \in \omega$ tal que $|a_{n'}-a_n| \leq \epsilon/2C$, $|b_{n'}-b_n| \leq \epsilon/2C$ siempre que $n, n' \geq m$. Obtenemos entonces que

$$|a_{n'}b_{n'}-a_nb_n| < C\epsilon/2C + C\epsilon/2C = \epsilon.$$

En el caso de la convergencia razonamos análogamente a partir de

$$|a_nb_n-ll'| = |a_nb_n-a_nl'+a_nl'-ll'| \leq |a_n||b_n-l'| + |a_n-l||l'|.$$

Notemos que podemos suponer $C \geq |l'|$. ■

Con esto podemos probar que a lo sumo hay un cuerpo ordenado completo. Probamos primero algo más general:

Teorema 7.24 *Sean M y N dos espacios métricos, sea $M_0 \subset M$ un subconjunto denso*[7]*, considerado como espacio métrico con la restricción de la distancia de M. Sea $f : M_0 \longrightarrow N$ una inmersión isométrica. Entonces existe una única inmersión isométrica $F : M \longrightarrow N$ que extiende a f (es decir, tal que $F|_{M_0} = f$). Si $f[M_0]$ es denso en N, entonces F es una isometría. Más aún, si M y N son cuerpos métricos, M_0 es un subcuerpo y f es una inmersión isométrica (resp. isometría) de cuerpos métricos, entonces F también lo es.*

[7]Necesitamos suponer que M_0 (y, por consiguiente, N_0) es bien ordenable para no requerir el axioma de elección (numerable). Esto se debe al uso del teorema 7.13.

Demostración: Sea $x \in M$. El teorema 7.13 implica que existe una sucesión $\{x_n\}_{n\in\omega}$ en M_0 convergente a x. En particular es una sucesión de Cauchy en M, pero es claro que esto es lo mismo que decir que $\{x_n\}_{n\in\omega}$ es una sucesión de Cauchy en M_0 como espacio métrico, pues la definición de sucesión de Cauchy depende sólo de los valores que toma la distancia sobre los términos de la sucesión. Como f es una inmersión isométrica, resulta que la sucesión $\{f(x_n)\}_{n\in\omega}$ es de Cauchy en $f[M_0]$, luego en N, y por la completitud de N converge en N. Definimos $F(x) = \lim_n f(x_n)$.

Para que esta definición sea correcta tenemos que comprobar que no depende de la sucesión utilizada para calcular $F(x)$. En efecto, si tomamos otra sucesión $\{y_n\}_{n\in\omega}$ en M_0 convergente a x, es fácil ver que la sucesión $\{z_k\}_{k\in\omega}$ dada por

$$z_k = \begin{cases} x_n & \text{si } k = 2n, \\ y_n & \text{si } k = 2n+1, \end{cases}$$

también converge a x. Según hemos visto, entonces $\{f(z_k)\}_{k\in\omega}$ converge a un cierto z en N, pero las sucesiones $\{f(x_n)\}_{n\in\omega}$ y $\{f(y_n)\}_{n\in\omega}$ son subsucesiones de esta sucesión, luego ambas convergen al mismo límite z.

Por lo tanto F está bien definida. Veamos ahora que es una inmersión isométrica, es decir, que cumple

$$\bigwedge xy \in M\ d(F(x), F(y)) = d(x, y).$$

Para ello observamos que si $\lim_n x_n = x$ y $\lim_n y_n = y$, donde ambas sucesiones están en M_0, entonces $\lim_n d(x_n, y_n) = d(x, y)$. En efecto,

$$\begin{aligned} |d(x,y) - d(x_n, y_n)| &\leq |d(x,y) - d(x_n, y)| + |d(x_n, y) - d(x_n, y_n)| \\ &\leq d(x_n, x) + d(y_n, y), \end{aligned}$$

luego, dado $\epsilon > 0$, podemos tomar un $m \in \omega$ tal que si $n \geq m$ se cumple $d(x_n, x) < \epsilon/2$ y $d(y_n, y) < \epsilon/2$, con lo que $|d(x,y) - d(x_n, y_n)| < \epsilon$.

Igualmente, $\lim_n d(f(x_n), f(y_n)) = d(F(x), F(y))$, pero ambas sucesiones de distancias son la misma, luego los límites son el mismo.

Si $f[M_0]$ es denso en N entonces F es suprayectiva, pues dado $y \in N$, podemos tomar una sucesión en $f[M_0]$ convergente a y y pasarla a M_0 con f, con lo que obtenemos una sucesión convergente a un cierto $x \in M$ que claramente cumplirá $F(x) = y$.

La unicidad de F es clara, pues si G fuera otra inmersión isométrica tal que $G|_{M_0} = f$, entonces, dado $x \in M$, lo expresamos como $x = \lim_n x_n$, donde la sucesión está en M_0, y entonces $d(G(x), G(x_n)) = d(x - x_n)$, de donde se sigue inmediatamente que

$$G(x) = \lim_n G(x_n) = \lim_n f(x_n) = F(x).$$

Supongamos ahora que M y N son cuerpos métricos, que M_0 es un subcuerpo y que f es una inmersión isométrica de cuerpos métricos. Entonces, dados $x = \lim\limits_n x_n$, $y = \lim\limits_n y_n$ en M, el teorema anterior nos da que $x+y = \lim\limits_n (x_n+y_n)$, luego podemos calcular F con esta sucesión y entonces

$$F(x+y) = \lim_n (f(x_n) + f(y_n)) = \lim_n f(x_n) + \lim_n f(y_n) = F(x) + F(y),$$

e igualmente se razona con el producto. Por lo tanto F es un monomorfismo de cuerpos. Como $|x| = d(x, 0)$, el hecho de que F sea una inmersión isométrica implica que $|F(x)| = |x|$. ■

En particular:

Teorema 7.25 *Dos cuerpos ordenados completos cualesquiera son isomorfos.*

Demostración: Supongamos que R y R' son cuerpos ordenados completos. Entonces ambos contienen a $\mathbb{Q}$ o, si queremos ser más precisos, existen subcuerpos densos $\mathbb{Q} \subset R$, $\mathbb{Q}' \subset R'$ y un isomorfismo de cuerpos ordenados $f : \mathbb{Q} \longrightarrow \mathbb{Q}'$.

El teorema anterior nos da que el isomorfismo f se extiende a una única isometría $F : R \longrightarrow R'$ de cuerpos métricos, pero vamos a probar que además es una semejanza, y por lo tanto un isomorfismo de cuerpos ordenados. Esto es una consecuencia inmediata del teorema 7.22: se cumple $x \leq y$ si y sólo si $\bigvee z \in R\ y - x = z^2$, si y sólo si $\bigvee z' \in R'\ F(y) - F(x) = z'^2$, si y sólo si $F(x) \leq F(y)$. ■

Así pues, el cuerpo de los números reales que construiremos en la sección siguiente será el único cuerpo ordenado completo (salvo isomorfismo).

Terminamos esta sección demostrando algunos resultados técnicos que nos harán falta en la siguiente. El primero es una caracterización de los espacios métricos completos:

Teorema 7.26 *Sea M un espacio métrico y sea $D \subset M$ un conjunto denso*[8] *tal que toda sucesión de Cauchy en D converge en M. Entonces M es un espacio métrico completo.*

Demostración: Sea $\{x_n\}_{n\in\omega}$ una sucesión de Cauchy en M. Para cada $n \in \omega$, sea $d_n \in D$ tal que $d(x_n, d_n) < 1/(n+1)$. La sucesión $\{d_n\}_{n\in\omega}$ es de Cauchy, pues

$$|d_{n'} - d_n| \leq |d_{n'} - x_{n'}| + |x_{n'} - x_n| + |x_n - d_n|,$$

luego, dado $\epsilon > 0$, existe un $m > 3/\epsilon$ tal que si $n, n' \geq m$ se cumple que $|x_{n'} - x_n| < \epsilon/3$, y entonces

$$|d_{n'} - d_n| < \frac{1}{n'+1} + \frac{\epsilon}{3} + \frac{1}{n+1} < \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon.$$

[8]Necesitamos que D sea bien ordenable si no queremos usar el axioma de elección (numerable), pues necesitamos escoger un d_n para cada n.

Por hipótesis existe $\lim_n d_n = l$ y basta probar que $\lim_n x_n = l$. En efecto:

$$|x_n - l| \leq |x_n - d_n| + |d_n - l|.$$

Dado $\epsilon > 0$, basta tomar $m \geq 2/\epsilon$ tal que si $n \geq m$ se cumpla $|d_n - l| < \epsilon/2$, y entonces $|x_n - l| < \epsilon$. ■

Teorema 7.27 *Si $\{x_n\}_{n\in\omega}$ es una sucesión acotada en un cuerpo métrico y $\{y_n\}_{n\in\omega}$ converge a 0, entonces $\{x_n y_n\}_{n\in\omega}$ converge a 0.*

DEMOSTRACIÓN: Sea $C \in R$ tal que $\bigwedge n \in \omega\ |x_n| \leq C$. Dado $\epsilon > 0$, existe un $m \in \omega$ tal que si $n \geq m$, entonces $|y_n| < \epsilon/C$, luego

$$|x_n y_n| = |x_n||y_n| < C\epsilon/X = \epsilon.$$

Esto significa que la sucesión producto tiende a 0. ■

Teorema 7.28 *Si $\{x_n\}_{n\in\omega}$ es una sucesión de Cauchy en un cuerpo métrico y no converge a 0, entonces existe un $T \in R$ y un $m \in \omega$ tal que si $n \geq m$ entonces $0 < T \leq |x_n|$. Además, la sucesión $\{y_n\}_{n\in\omega}$ dada por*

$$y_n = \begin{cases} 1/x_n & \text{si } x_n \neq 0, \\ 0 & \text{si } x_n = 0, \end{cases}$$

también es de Cauchy.

DEMOSTRACIÓN: Si no existe el T indicado, tomando $\epsilon = T$ obtenemos

$$\bigwedge \epsilon > 0 \bigwedge m \in \omega \bigvee n \in \omega (n \geq m \wedge |x_n| < \epsilon).$$

Definimos $\{n_k\}_{k\in\omega}$ por recurrencia estableciendo que n_k sea el menor número natural mayor que los ya definidos y tal que $|x_{n_k}| < 1/(k+1)$. Es claro entonces que $\{x_{n_k}\}_{k\in\omega}$ es una subsucesión de $\{x_n\}_{n\in\omega}$ convergente a 0, pero entonces, por 7.17 tenemos que la sucesión dada converge a 0, contradicción.

Para la segunda parte observamos que si $n, n' \geq m$ (el m dado por la primera parte) entonces $x_n, x_{n'} \neq 0$, luego

$$|y_{n'} - y_n| = \left| \frac{1}{x_{n'}} - \frac{1}{x_n} \right| = \frac{|x_n - x_{n'}|}{|x_{n'} x_n|} \leq \frac{|x_n - x_{n'}|}{T^2}.$$

Así, dado $\epsilon > 0$, podemos tomar un m mayor (si es preciso) que el de la primera parte de modo que si $n, n' \geq m$ se cumpla que $|x_n - x_{n'}| < T^2\epsilon$, y así concluimos que $|y_{n'} - y_n| < \epsilon$. ■

7.4 La construcción de $\mathbb{R}$

Los resultados de la sección anterior han perfilado muy bien qué estamos buscando cuando pretendemos extender el cuerpo $\mathbb{Q}$ de los números racionales. Aunque todavía no lo hemos demostrado,[9] sucede que $\mathbb{Q}$ es incompleto, y lo que queremos es encontrar un cuerpo completo $\mathbb{R}$, que necesariamente contendrá a $\mathbb{Q}$ como subcuerpo denso. Más en general vamos a ver que todo espacio métrico M puede completarse, en el sentido de que existe un espacio métrico $\overline{M}$ (único salvo isometría) que contiene a M como subconjunto denso.

El teorema 7.26 nos dice que, para que $\overline{M}$ sea completo, sólo hemos de garantizar que las sucesiones de Cauchy de M converjan en $\overline{M}$, sin necesidad de preocuparnos de que lo hagan las nuevas sucesiones de Cauchy que pueden formarse con los nuevos puntos de $\overline{M} \setminus M$.

La estrategia de construcción será la misma que hemos empleado para construir $\mathbb{Z}$ o $\mathbb{Q}$: cada punto de $\overline{M}$ debe ser el límite de una sucesión en M, que, al ser convergente en $\overline{M}$, debe ser de Cauchy en M, por lo que podríamos pensar en definir como $\overline{M}$ el conjunto de las sucesiones de Cauchy en M, pero no podemos hacerlo exactamente así porque varias sucesiones de Cauchy en M pueden estar forzadas a tener el mismo límite en $\overline{M}$, luego hay que establecer una relación de equivalencia adecuada y definir $\overline{M}$ como el conjunto cociente asociado.

A partir de este punto usaremos el axioma de partes.

Definición 7.29 Si M es un espacio métrico, llamaremos C_M al conjunto[10] de todas las sucesiones de Cauchy en M. Definimos en C_M la relación de equivalencia dada por

$$\{x_n\}_{n\in\omega} \sim \{y_n\}_{n\in\omega} \leftrightarrow \lim_n d(x_n, y_n) = 0.$$

Es fácil ver que se trata, en efecto, de una relación de equivalencia. Por ejemplo, la transitividad se debe a que si

$$\lim_n d(x_n, y_n) = \lim_n d(y_n, z_n) = 0,$$

dado $\epsilon > 0$ existe un $m \in \omega$ tal que si $n \geq m$ se cumple $d(x_n, y_n) < \epsilon/2$, $d(y_n, z_n) < \epsilon/2$, con lo que

$$d(x_n, z_n) \leq d(x_n, y_n) + d(y_n, z_n) < \epsilon/2 + \epsilon/2 = \epsilon,$$

luego $\lim_n d(x_n, z_n) = 0$.

Definimos la *compleción* de M como el conjunto cociente $\overline{M}$ de M respecto de la relación de equivalencia que acabamos de definir.

[9] En realidad el teorema 7.22 ya implica que $\mathbb{Q}$ es incompleto, si tenemos en cuenta también el resultado aritmético (que no hemos probado aquí) según el cual en $\mathbb{Q}$ no existe, por ejemplo, la raíz cuadrada de 2.

[10] Notemos que $C_M \subset M^\omega$, y el axioma AP implica que M^ω es un conjunto, luego C_M también lo es.

Definimos $i : M \longrightarrow \overline{M}$ como la aplicación que a cada $x \in M$ le asigna la clase de equivalencia de la sucesión constante $\{x\}_{n\in\omega}$. Es una aplicación inyectiva, pues si $i(x) = i(y)$, entonces la sucesión constante $\{d(x,y)\}_{n\in\omega}$ converge a 0, lo cual equivale a que $d(x,y) = 0$, luego $x = y$.

Así podemos identificar a M con un subconjunto de $\overline{M}$.

La compleción de un espacio métrico Si suponemos que el cuerpo R en el que la distancia toma sus valores es completo, entonces es fácil convertir a $\overline{M}$ en espacio métrico. Basta observar que, por una parte, si $\{x_n\}_{n\in\omega}$, $\{y_n\}_{n\in\omega}$ son sucesiones de Cauchy en M, entonces $\{d(x_n,y_n)\}_{n\in\omega}$ es una sucesión de Cauchy en R, pues

$$\begin{aligned}|d(x_n,y_n) - d(x_{n'},y_{n'})| &\leq |d(x_n,y_n) - d(x_{n'},y_n)| + |d(x_{n'},y_n) - d(x_{n'},y_{n'})|\\ &\leq d(x_n,x_{n'}) + d(y_n,y_{n'}),\end{aligned}$$

luego, dado $\epsilon > 0$, podemos tomar $m \in \omega$ tal que, para $n, n' \geq m$ se cumpla $d(x_n,x_{n'}) < \epsilon/2$ y $d(y_n,y_{n'}) < \epsilon/2$, con lo que $|d(x_n,y_n) - d(x_{n'},y_{n'})| < \epsilon$. Por lo tanto, si R es completo podemos definir

$$d([\{x_n\}_{n\in\omega}], [\{y_n\}_{n\in\omega}]) = \lim_n d(x_n,y_n).$$

En realidad, para que esta definición sea correcta hemos de comprobar que no depende de la elección de las sucesiones que tomamos en cada clase de equivalencia. Esto se debe a que si

$$[\{x_n\}_{n\in\omega}] = [\{x'_n\}_{n\in\omega}], \quad [\{y_n\}_{n\in\omega}] = [\{y'_n\}_{n\in\omega}],$$

entonces

$$\begin{aligned}|d(x_n,y_n) - d(x'_n,y'_n)| &\leq |d(x_n,y_n) - d(x_n,y'_n)| + |d(x_n,y'_n) - d(x'_n,y'_n)|\\ &\leq d(y_n,y'_n) + d(x_n,y'_n)\end{aligned}$$

y, teniendo en cuenta que los dos últimos sumandos tienden a 0, es fácil ver que

$$\lim_n (d(x_n,y_n) - d(x'_n,y'_n)) = 0,$$

de donde $\lim\limits_n d(x_n,y_n) = \lim\limits_n d(x'_n,y'_n)$.

Así pues, tenemos una aplicación $d : \overline{M} \times \overline{M} \longrightarrow R$, y es fácil comprobar que es una distancia. Por ejemplo, para probar la desigualdad triangular, dados $\alpha = [\{x_n\}_{n\in\omega}]$, $\beta = [\{y_n\}_{n\in\omega}]$, $\gamma = [\{z_n\}_{n\in\omega}]$ en $\overline{M}$, observamos que

$$0 \leq d(x_n,y_n) + d(y_n,z_n) - d(x_n,z_n),$$

luego por el teorema 7.12 (tomando como b cualquier cota de la sucesión, que es de Cauchy), obtenemos que $0 \leq d(\alpha,\beta) + d(\beta,\gamma) - d(\alpha,\gamma)$.

Además, la aplicación $i : M \longrightarrow \overline{M}$ es una inmersión isométrica. En efecto, si $x, y \in M$, es claro que la sucesión constante $\{d(x,y)\}_{n\in\omega}$ converge a $d(x,y)$, luego $d(i(x), i(y)) = d(x,y)$.

Por último, observamos que si $\{x_n\}_{n\in\omega}$ es una sucesión de Cauchy en M y $\alpha = [\{x_n\}_{n\in\omega}]$, entonces $\lim\limits_n i(x_n) = \alpha$.

En efecto, por definición $d(i(x_n), \alpha) = \lim\limits_{n'} d(x_n, x_{n'})$, luego, dado $\epsilon > 0$, existe un $m \in \omega$ tal que si $n, n' \geq m$ entonces $0 \leq d(x_n, x_{n'}) < \epsilon/2$, luego por el teorema 7.12 tenemos que $0 \leq d(i(x_n), \alpha) \leq \epsilon/2 < \epsilon$, y esto es lo que había que probar.

En definitiva, lo que sucede es que cada sucesión de Cauchy en M, identificada con una sucesión de Cauchy en $\overline{M}$ a través de i, converge a la clase de equivalencia que ella misma determina.

En particular vemos que todo elemento de $\overline{M}$ es el límite de una sucesión en $i[M]$, luego $i[M]$ es denso en $\overline{M}$, y toda sucesión de Cauchy en $i[M]$ es de la forma $\{i(x_n)\}_{n\in\omega}$, para una única sucesión de Cauchy $\{x_n\}_{n\in\omega}$ en M, luego acabamos de ver que converge en $\overline{M}$, luego el teorema 7.26 nos da que $\overline{M}$ es un espacio métrico completo.

El único problema de esta demostración es que hemos supuesto que el cuerpo R es completo, luego en principio no vale cuando $R = \mathbb{Q}$, por ejemplo.

La compleción de un cuerpo métrico Volvamos ahora al caso general en que R es un cuerpo ordenado arquimediano no necesariamente completo y veamos qué sucede en el caso en que partimos de un cuerpo métrico K.

Observamos entonces que el conjunto C_K de las sucesiones de Cauchy en K tiene estructura de anillo con la suma y el producto dadas por

$$\{x_n\}_{n\in\omega} + \{y_n\}_{n\in\omega} = \{x_n + y_n\}_{n\in\omega}, \quad \{x_n\}_{n\in\omega} \cdot \{y_n\}_{n\in\omega} = \{x_n y_n\}_{n\in\omega}.$$

Aquí usamos que la suma y el producto de sucesiones de Cauchy es una sucesión de Cauchy.

Por otra parte, el conjunto I_K de las sucesiones convergentes a 0 es un ideal de C_K, pues ciertamente contiene a la sucesión nula (que es el neutro de C_K), la suma de sucesiones convergentes a 0 converge a $0+0=0$ y si $\{x_n\}_{n\in\omega} \in C_K$ e $\{y_n\}_{n\in\omega} \in I_K$, entonces $\{x_n y_n\}_{n\in\omega} \in I_K$, porque $\{x_n\}_{n\in\omega}$ está acotada por ser de Cauchy, y basta aplicar el teorema 7.27.

Ahora observamos que la relación de equivalencia que hemos definido en C_K es la dada por

$$\{x_n\}_{n\in\omega} \sim \{y_n\}_{n\in\omega} \leftrightarrow \lim_n (x_n - y_n) = 0 \leftrightarrow \{x_n\}_{n\in\omega} - \{y_n\}_{n\in\omega} \in I_K,$$

es decir, se trata de la congruencia módulo I_K definida en 1.31, luego, según el teorema 1.32, sabemos que $\overline{K} = C_K/I_K$ tiene estructura de anillo, de modo que si tenemos dos clases $\alpha = [\{x_n\}_{n\in\omega}]$, $\beta = [\{y_n\}_{n\in\omega}]$, entonces

$$\alpha + \beta = [\{x_n + y_n\}_{n\in\omega}], \qquad \alpha\beta = [\{x_n y_n\}_{n\in\omega}].$$

Los neutros 0 y 1 de $\overline{K}$ son las clases de las sucesiones constantes correspondientes, es decir, $i(0)$ e $i(1)$.

Veamos que $\overline{K}$ es un cuerpo. Para ello tomamos un $\alpha \in \overline{K}$, $\alpha \neq 0$. Esto quiere decir que $\alpha = [\{x_n\}_{n\in\omega}]$, donde la sucesión $\{x_n\}_{n\in\omega}$ es de Cauchy en K, pero no converge a 0. Por el teorema 7.28 sabemos que la sucesión $\{1/x_n\}_{n\in\omega}$ (definida como 0 cuando $x_n = 0$, cosa que sólo puede suceder en un número finito de casos) es de Cauchy, luego define un $\beta \in K$, de modo que $\alpha\beta$ es la clase de equivalencia de una sucesión que vale 1 salvo a lo sumo en un número finito de casos. Es claro entonces que $\alpha\beta = 1$, luego α tiene inverso y $\overline{K}$ es un cuerpo.

Se comprueba trivialmente que la aplicación $i : K \longrightarrow \overline{K}$ es un monomorfismo de cuerpos.

Nuevamente, si suponemos que el cuerpo R es completo, podemos convertir a $\overline{K}$ en un cuerpo métrico. Por el caso general en que M era un espacio métrico arbitrario, sabemos que si $\{x_n\}_{n\in\omega}$ es una sucesión de Cauchy en M entonces la sucesión $\{|x_n|\}_{n\in\omega}$ es de Cauchy en R (pues $|x_n| = d(x_n, 0)$), luego podemos definir $|[\{x_n\}_{n\in\omega}]| = \lim\limits_n |x_n|$, y ya hemos visto que la definición es correcta en el sentido de que no depende de la elección de la sucesión en la clase de equivalencia.

Ahora podemos probar que $|\ \ | : \overline{K} \longrightarrow R$ es un valor absoluto en $\overline{K}$. Por ejemplo, si $\alpha = [\{x_n\}]_{n\in\omega}$, $\beta = [\{y_n\}]_{n\in\omega}$, entonces $|x_n+y_n| \leq |x_n|+|y_n|$, luego $|x_n| + |y_n| - |x_n + y_n| \geq 0$ y por 7.12 resulta que $|\alpha| + |\beta| - |\alpha + \beta| \geq 0$, luego tenemos la desigualdad triangular. Por otra parte,

$$|\alpha\beta| = \lim_n |x_n y_n| = \lim_n |x_n||y_n| = (\lim_n |x_n|)(\lim_n |y_n|) = |\alpha||\beta|.$$

La distancia en $\overline{K}$ definida a partir del valor absoluto es la misma que ya teníamos definida al considerar a K como un mero espacio métrico, luego ya sabemos que $\overline{K}$ es un cuerpo métrico completo.

La compleción de un cuerpo ordenado El problema sigue siendo que para definir el valor absoluto en $\overline{K}$ hemos tenido que suponer que R es completo. Consideremos ahora el caso de un cuerpo ordenado K y vamos a probar que $\overline{K}$ puede convertirse en un cuerpo ordenado completo sin suponer que R es completo. Sabemos que $\overline{K}$ tiene estructura de cuerpo (pues en esta parte no hemos supuesto que R fuera completo).

Para definir un orden en $\overline{K}$ diremos que $\alpha \in \overline{K}$ es *positivo* si $\alpha = [\{x_n\}_{n\in\omega}]$ y existe un $c \in K$, $c > 0$ y un $m \in \omega$ de modo que $\bigwedge n \geq m\ x_n \geq c$.

Esta propiedad no depende de la sucesión elegida en α, pues si $\alpha = [\{y_n\}_{n\in\omega}]$, entonces, para m es suficientemente grande, tenemos $x_n \geq c$ y $|x_n - y_n| < c/2$, y entonces tiene que ser $y_n \geq c/2$, pues si fuera $y_n < c/2 < c \leq x_n$, tendríamos que $|x_n - y_n| = x_n - y_n \geq c - c/2 = c/2$.

Es trivial que la suma y el producto de elementos positivos es positiva. Además, todo $\alpha \in \overline{K}$ se encuentra en uno y sólo uno de los tres casos siguientes: α es positivo, $\alpha = 0$ o bien $-\alpha$ es positivo.

En efecto, $\alpha = 0$ no es positivo, porque $\alpha = [\{0\}_{n\in\omega}]$ y la sucesión nula no cumple la definición.

Si $\alpha \neq 0$, entonces $\alpha = [\{x_n\}_{n\in\omega}]$ (y $-\alpha = [\{-x_n\}_{n\in\omega}]$) donde, por 7.28, existe un $c \in K$, $c > 0$ y un $m \in \omega$, de modo que si $n \geq m$ se cumple $|x_n| \geq c$, es decir, $x_n \geq c > 0$, o bien $x_n \leq -c < 0$.

Si se da el primer caso para todo n suficientemente grande, entonces α es positivo y $-\alpha$ no lo es. Si se da el segundo caso para todo n suficientemente grande entonces $-\alpha$ es positivo y α no lo es. Sólo falta probar que no pueden darse los dos casos para n grande, es decir, que no puede ocurrir que

$$\bigwedge m \in \omega \bigvee nn' \in \omega (n, n' \geq m \land x_n \geq c \land x_{n'} \leq -c).$$

Si ocurriera esto, entonces $|x_n - x_{n'}| \geq 2c$ y no se cumpliría la definición de sucesión de Cauchy para $\epsilon = 2c$.

Por lo tanto, si definimos en $\overline{K}$ la relación dada por

$$\alpha < \beta \leftrightarrow \beta - \alpha \text{ es positivo},$$

tenemos que se trata de una relación de orden estricto, pues no puede suceder que $\beta - \alpha$ y $\alpha - \beta$ sean ambos positivos y si $\beta - \alpha$ y $\gamma - \beta$ son positivos, también lo es la suma $\gamma - \alpha$, lo que nos da la transitividad. Además es una relación de orden total, pues o bien $\alpha - \beta$ es positivo, o bien lo es $\beta - \alpha$, o bien $\alpha - \beta = 0$, es decir, $\alpha < \beta \lor \beta < \alpha \lor \alpha = \beta$.

Más aún, $\overline{K}$ cumple las dos propiedades de la definición de cuerpo ordenado, pues si $\alpha \leq \beta$, entonces $\beta - \alpha$ es positivo o nulo, luego lo mismo vale para $(\beta + \gamma) - (\alpha + \gamma)$, luego $\alpha + \gamma \leq \beta + \gamma$, y si $\alpha, \beta \geq 0$, ambos son positivos o nulos, luego lo mismo vale para $\alpha\beta \geq 0$.

Además, la aplicación $i : K \longrightarrow \overline{K}$ conserva el orden, pues si $x < y$, es claro que la clase de la sucesión constante $\{y - x\}_{n\in\omega}$ es positiva, es decir, que $i(y) - i(x)$ es positivo y, por consiguiente, $i(x) < i(y)$.

Así pues, $\overline{K}$ es un cuerpo ordenado que tiene un subcuerpo $i[K]$ isomorfo a K como cuerpo ordenado. Veamos que si $\alpha = [\{x_n\}_{n\in\omega}]$, entonces $\lim\limits_n i(x_n) = \alpha$.

En efecto, dado $\epsilon > 0$ (ahora en $\overline{K}$, porque queremos probar una convergencia en $\overline{K}$), tenemos que $\epsilon = [\{e_n\}]_{n\in\omega}$ de modo que existe un $c > 0$ en K y un $m \in \omega$ de modo que $\bigwedge n \geq m\ e_n \geq c$.

Cambiando m por otro mayor podemos suponer que si $n, n' \geq m$, entonces $|x_n - x_{n'}| < c/2$. Así $-c/2 < x_n - x_{n'} < c/2$, luego

$$e_{n'} - x_n + x_{n'} > c - c/2 = c/2.$$

Por lo tanto, $\epsilon - i(x_n) + \alpha = [\{e_{n'} - x_n + x_{n'}\}_{n'\in\omega}]$ es positivo, luego concluimos que $i(x_n) - \alpha < \epsilon$.

Similarmente, $x_n - x_{n'} + e_{n'} > c - c/2 = c/2$, por lo que $i(x_n) - \alpha + \epsilon$ es positivo, luego $i(x_n) - \alpha > -\epsilon$. En total tenemos que $-\epsilon < i(x_n) - \alpha < \epsilon$, luego $|i(x_n) - \alpha| < \epsilon$ (siempre que $n \geq m$), luego se cumple la definición de límite.

La conclusión, como en el caso general para espacios métricos, es que $i[K]$ es denso en $\overline{K}$, que toda sucesión de Cauchy en $i[K]$ converge en $\overline{K}$ y que $\overline{K}$ es un cuerpo ordenado completo por el teorema 7.26.

A partir de aquí ya podemos recoger los frutos de todo el desarrollo que hemos realizado:

Definición 7.30 Llamaremos *cuerpo de los números reales* a la compleción $\mathbb{R} = \overline{\mathbb{Q}}$ del cuerpo $\mathbb{Q}$ de los números racionales. Hemos demostrado que es un cuerpo ordenado completo y, por 7.25 sabemos que es único salvo isomorfismo, es decir, que todo cuerpo ordenado completo es isomorfo a $\mathbb{R}$.

También sabemos que existe un monomorfismo de cuerpos $i : \mathbb{Q} \longrightarrow R$ que conserva el orden, por lo que en lo sucesivo identificaremos a $\mathbb{Q}$ con $i[\mathbb{Q}]$, de modo que podemos considerar que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Por 7.21 sabemos que $\mathbb{R}$ es arquimediano y que $\mathbb{Q}$ es denso en $\mathbb{R}$ (lo cual, según 7.14 equivale a que entre dos números reales hay siempre un número racional), por 7.22 sabemos que para cada número real $\alpha \geq 0$ existe un único $\beta \geq 0$ tal que $\beta^2 = \alpha$. Representaremos a dicho β con la notación $\sqrt{\alpha}$ y diremos que es la *raíz cuadrada* (positiva) de α (mientras que $-\sqrt{\alpha}$ es la *raíz cuadrada negativa* de α).

Cada $\alpha > 0$ tiene exactamente dos raíces cuadradas en $\mathbb{R}$ (es decir, que hay dos números β que cumplen $\beta^2 = \alpha$, pues si

$$0 = \beta^2 - \alpha = \beta^2 - \sqrt{\alpha}^{\,2} = (\beta - \sqrt{\alpha})(\beta + \sqrt{\alpha}),$$

necesariamente $\beta - \sqrt{\alpha} = 0$ o bien $\beta + \sqrt{\alpha} = 0$, luego $\beta = \pm\sqrt{\alpha}$.

Por el teorema 7.20 sabemos también que todo subconjunto de $\mathbb{R}$ no vacío y acotado superiormente tiene supremo.

Por último, si R es cualquier cuerpo ordenado arquimediano, hemos probado que su compleción $\overline{R}$ es un cuerpo ordenado completo, luego tiene que ser $\overline{R} \cong \mathbb{R}$, y entonces R resulta ser isomorfo a un subcuerpo de $\mathbb{R}$. Esto implica que no perdemos generalidad si consideramos únicamente distancias y valores absolutos de cuerpos métricos con valores en $\mathbb{R}$. Con este convenio adicional, los resultados que hemos obtenido nos permiten concluir:

Teorema 7.31 *Si M es un espacio métrico,*[11] *entonces su compleción $\overline{M}$ es un espacio métrico completo tal que existe una inmersión isométrica $i : M \longrightarrow \overline{M}$ de M en un subconjunto denso de $\overline{M}$ (la cual nos permite considerar $M \subset \overline{M}$) y toda inmersión isométrica $f : M \longrightarrow N$ de M en un cuerpo métrico completo N*

[11] Hay que suponer que M es bien ordenable para no necesitar el axioma de elección (numerable).

se extiende a una inmersión isométrica $F : \overline{M} \longrightarrow M$, que será una isometría si $f[M]$ es denso en N. Lo mismo es válido para cuerpos métricos e inmersiones isométricas de cuerpos métricos.

Podemos parafrasear este teorema diciendo que la compleción de un espacio métrico (resp. de un cuerpo métrico) es el menor espacio métrico (resp. cuerpo métrico) completo que lo contiene.

Volviendo a $\mathbb{R}$, podemos refinar el teorema 7.20:

Teorema 7.32 (de los intervalos encajados de Cantor) *Dadas dos sucesiones $\{a_n\}_{n\in\omega}$ y $\{b_n\}_{n\in\omega}$ de números reales tales que, para todo índice n, se cumple $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$, existe un $l \in \mathbb{R}$ tal que $\bigwedge n \in \omega\ a_n \leq l \leq b_n$. Si además y $\lim\limits_n (b_n - a_n) = 0$, dicho l es único.*

DEMOSTRACIÓN: El conjunto $A = \{a_n \mid n \in \omega\}$ es no vacío y está acotado superiormente por cualquier b_n, luego tiene supremo l, de modo que $a_n \leq l \leq b_n$. Si existe otro l' que cumple la condición, como es cota superior de A, tiene que ser $l \leq l'$, pero si fuera $l \neq l'$ entonces $\epsilon = l' - l > 0$ y $\bigwedge n \in \omega\ b_n - a_n \geq \epsilon$, luego no se cumple $\lim\limits_n (b_n - a_n) = 0$. ■

Los elementos de $\mathbb{R} \setminus \mathbb{Q}$ se llaman *números irracionales,* pero todavía no hemos demostrado que existan. El teorema siguiente lo prueba:

Teorema 7.33 $\overline{\overline{\mathbb{R}}} = 2^{\aleph_0}$.

DEMOSTRACIÓN: Observemos que si $\alpha < \beta$ son dos números reales, entonces

$$\alpha < \frac{2\alpha + \beta}{3} < \frac{\alpha + 2\beta}{3} < \beta,$$

y la distancia de cada uno de estos números al siguiente es $(\beta - \alpha)/3$. Sea $P = \{(\alpha, \beta) \in \mathbb{R}^2 \mid \alpha < \beta\}$. Para cada $(\alpha, \beta) \in P$, definimos

$$(\alpha, \beta)_0 = (\alpha, (2\alpha + \beta)/3), \qquad (\alpha, \beta)_1 = ((\alpha + 2\beta)/3, \beta).$$

Fijemos $(a, b) \in P$ y definamos por recurrencia una sucesión de funciones $f_n : {}^n2 \longrightarrow P$. Para $n = 0$ tenemos que ${}^02 = \{\varnothing\}$ y definimos $f_0(\varnothing) = (a, b)$. Supuesta definida f_n, definimos $f_{n+1}(s) = f_n(s|_n)_{s(n)}$.

Por ejemplo, si partimos de $(a, b) = (0, 1)$ y representamos las sucesiones finitas de ceros y unos enumerando las imágenes, de modo que

$$1101 \equiv \{(0, 1), (1, 1), (2, 0), (3, 1)\} \in {}^42,$$

tenemos que

$$f_0(\varnothing) = (0, 1), \quad f_1(1) = (0, 1)_1 = (2/3, 1),$$
$$f_2(11) = f_1(1)_1 = (2/3, 1)_1 = (8/9, 1),$$
$$f_3(110) = f_2(11)_0 = (8/9, 1)_0 = (8/9, 25/27),$$
$$f_4(1101) = f_3(110)_1 = (8/9, 25/27)_1 = (74/81, 25/27).$$

En general, para cada $s \in {}^n 2$, llamaremos a_s y b_s a los números reales que cumplen $f_n(s) = (a_s, b_s)$. En estos términos, por ejemplo, hemos visto que, si partimos de $(a, b) = (0, 1)$, se cumple $a_{110} = 8/9$, $b_{110} = 25/27$.

Si $s \in {}^\omega 2$, una simple inducción demuestra que

$$a \leq a_{s|_n} \leq a_{s|_{n+1}} < b_{s|_{n+1}} \leq b_{s|_n} \leq b,$$

así como que $b_{s|_n} - a_{s|_n} = (b-a)/3^n$. Por lo tanto $\lim_n (b_{s|_n} - a_{s|_n}) = 0$ (basta observar que, si $\epsilon > 0$, por la propiedad arquimediana existe un número natural tal que $(b-a)/\epsilon < n \leq 3^n$, luego $(b-a)/3^n < \epsilon$).

Por el teorema de los intervalos encajados, existe un único número real, que podemos llamar α_s, tal que $\bigwedge n \in \omega\ a_{s|_n} \leq \alpha_s \leq b_{s|_n}$. Tenemos, por lo tanto, una aplicación $f : {}^\omega 2 \longrightarrow \mathbb{R}$ dada por $f(s) = \alpha_s$. Vamos a probar que es inyectiva.

Si $s \neq s'$ son dos sucesiones de ${}^\omega 2$, sea $n \in \omega$ el mínimo natural tal que $s(n) \neq s'(n)$. No perdemos generalidad si suponemos que $s(n) = 0$ y $s'(n) = 1$. Entonces $s|_n = s'|_n$, luego $(a_{s|_n}, b_{s|_n}) = (a_{s'|_n}, b_{s'|_n}) = (a, b)$, pero, por construcción $(a_{s|_{n+1}}, b_{s|_{n+1}}) = f_{n+1}(s|_{n+1}) = (a, b)_0$, mientras que $(a_{s'|_{n+1}}, b_{s'|_{n+1}}) = (a, b)_1$, y entonces

$$a \leq \alpha_s \leq \frac{2a+b}{3} < \frac{a+2b}{3} \leq \alpha_{s'} \leq b,$$

lo que prueba que $\alpha_s \neq \alpha_{s'}$.

Como f es inyectiva, concluimos que $\overline{\overline{\mathbb{R}}} \geq \overline{\overline{{}^\omega 2}} = 2^{\aleph_0}$. Para la desigualdad opuesta consideramos la aplicación $g : \mathbb{R} \longrightarrow \mathcal{P}\mathbb{Q}$ dada por

$$g(\alpha) = \{q \in \mathbb{Q} \mid q \leq \alpha\}.$$

También es inyectiva, pues si $\alpha < \beta$, hemos visto que existe un $q \in \mathbb{Q}$ tal que $\alpha < q < \beta$, luego $q \in g(\beta) \setminus g(\alpha)$, luego $g(\alpha) \neq g(\beta)$. Esto prueba que $\overline{\overline{\mathbb{R}}} \leq \overline{\overline{\mathcal{P}\mathbb{Q}}} = 2^{\aleph_0}$. ■

Así pues, existen más números irracionales que racionales o, dicho de otro modo, $\mathbb{Q}$ está "lleno de agujeros". Más precisamente, el teorema anterior prueba que si $a < b$ son dos números reales cualesquiera, el conjunto $\{x \in \mathbb{R} \mid a < x < b\}$ tiene cardinal $2^{\aleph_0}$, luego contiene números irracionales. Así pues, entre dos números reales cualesquiera existen números irracionales o, lo que es lo mismo, $\mathbb{R} \setminus \mathbb{Q}$ es denso en $\mathbb{R}$.

7.5 Conjuntos ordenados completos

De las caracterizaciones de la completitud de un cuerpo ordenado dadas por el teorema 7.20, la tercera involucra exclusivamente la relación de orden (sin mencionar la suma o el producto), por lo que tiene sentido en un conjunto ordenado arbitrario. Vamos a estudiarla aquí en este contexto. Seguimos trabajando en NBG* + AI + AP. Conviene introducir algunos conceptos adicionales:

Definición 7.34 Sea X un conjunto totalmente ordenado. Llamaremos *intervalos* en X a los conjuntos siguientes, para todo a, $b \in X$:

$$\begin{aligned}]a,b[&= \{x \in X \mid a < x < b\}, & [a,b] &= \{x \in X \mid a \leq x \leq b\}, \\ ]a,b] &= \{x \in X \mid a < x \leq b\}, & [a,b[&= \{x \in X \mid a \leq x < b\}, \\ ]-\infty,b[&= \{x \in X \mid x < b\}, &]a,+\infty[&= \{x \in X \mid a < x\}, \\ ]-\infty,b] &= \{x \in X \mid x \leq b\}, & [a,+\infty[&= \{x \in X \mid a \leq x\}, \end{aligned}$$

$$]-\infty,+\infty[= X.$$

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 7.35 *Si X es un conjunto totalmente ordenado, las afirmaciones siguientes son equivalentes:*

a) Todo subconjunto de X no vacío y acotado superiormente tiene supremo.

b) Todo subconjunto de X no vacío y acotado inferiormente tiene ínfimo.

c) Un conjunto $I \subset X$ es un intervalo si y sólo si

$$\bigwedge ab \in I \bigwedge c \in X(a < c < b \rightarrow c \in I).$$

d) 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: a) $\Rightarrow$ b) 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 b) $\Rightarrow$ a). Veamos que a) y b) implican c). 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.

c) $\Rightarrow$ d) 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.

d) $\Rightarrow$ a) 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 d) 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 7.36 Diremos que un conjunto totalmente ordenado X es *completo* si cumple cualquiera de las condiciones equivalentes 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.

Es evidente que todo ordinal α es completo, pues si $A \subset \alpha$ está acotado superiormente por $\beta < \alpha$, entonces su supremo es $\bigcup A \leq \beta < \alpha$

Llamaremos *precontinuos* a los conjuntos totalmente ordenados densos en sí mismos. Un *continuo* es un precontinuo completo.

Si X es un precontinuo, diremos que un subconjunto $D \subset X$ es *denso* si

$$\bigwedge xy \in X(x < y \rightarrow \bigvee d \in D\ (x < d < y)).$$

Una aplicación $f : X \longrightarrow Y$ entre dos precontinuos es una *inmersión densa* si es estrictamente monótona creciente, es decir, si

$$\bigwedge uv \in X\ (u < v \rightarrow f(u) < f(v)),$$

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. ■

Probamos ahora un análogo al teorema 7.24 para continuos:

Teorema 7.37 *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

$$G(x) = G(\sup D_x) = \sup G[D_x] = \sup f[D_x] = F(x).$$

■

Siguiendo la analogía con los espacios métricos, vamos a ver que todo precontinuo se puede sumergir de forma única salvo semejanza como subconjunto denso de un continuo:

Definición 7.38 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:

a) $\bigwedge x \in X \bigwedge a \in \alpha (x \leq a \rightarrow x \in \alpha)$.

b) α no tiene máximo elemento.

Llamaremos $\overline{C(X)}$ al conjunto[12] 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 $C(X) = \overline{C(X)} \setminus \{-\infty, +\infty\}$.

[12]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.

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 $x \notin i(a) \neq +\infty$.

También es claro que i es estrictamente monótona creciente, es decir, que

$$\bigwedge xy \in X\ (x < y \rightarrow i(x) < i(y)).$$

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 7.39 *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 7.37, 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. ■

En particular, puesto que $\mathbb{Q}$ es un precontinuo sin máximo ni mínimo y $j : \mathbb{Q} \longrightarrow \mathbb{R}$ es una inmersión densa, el teorema anterior nos da la semejanza

$$\mathbb{R} \cong C(\mathbb{Q}).$$

En realidad es fácil obtener explícitamente la semejanza $f : \mathbb{R} \longrightarrow C(\mathbb{Q})$, ya que no es sino la dada por

$$f(\alpha) = \{q \in \mathbb{Q} \mid q < \alpha\}.$$

Teorema 7.40 *Existen unas únicas operaciones* $+, \cdot : C(\mathbb{Q}) \times C(\mathbb{Q}) \longrightarrow C(\mathbb{Q})$ *que extienden a la suma y el producto en* $\mathbb{Q}$ *y que convierten a* $C(\mathbb{Q})$ *en un cuerpo ordenado.*

Demostración: En el enunciado hay que entender que estamos identificando a $\mathbb{Q}$ con su imagen en $C(\mathbb{Q})$, pero, por claridad, en esta prueba no haremos tal identificación: llamamos $\mathbb{Q}$ al cuerpo definido en la sección 7.2, de modo que tenemos dos inmersiones densas:

$$\begin{tikzcd}
\mathbb{R} \arrow[r, "f"] & C(\mathbb{Q}) \\
\mathbb{Q} \arrow[u, "i_1"] \arrow[ur, "i_2"'] &
\end{tikzcd}$$

de modo que el diagrama es conmutativo, es decir, $i_1 \circ f = i_2$, que es lo mismo que decir que la semejanza f deja invariantes a los números racionales cuando los identificamos simultáneamente con $i_1[\mathbb{Q}]$ e $i_2[\mathbb{Q}]$. Notemos que sin las identificaciones es $f(\alpha) = \{q \in \mathbb{Q} \mid i_1(q) < \alpha\}$. Es claro entonces que si definimos en $C(\mathbb{Q})$

$$\alpha + \beta = f(f^{-1}(\alpha) + f^{-1}(\beta)), \qquad \alpha\beta = f(f^{-1}(\alpha)f^{-1}(\beta))$$

tenemos una suma y un producto en $C(\mathbb{Q})$ que convierte a f en un isomorfismo de cuerpos ordenados y a i_2 en una inmersión densa de cuerpos ordenados. Por lo tanto, tenemos probada la existencia que afirma el enunciado, y falta la unicidad. Para probarla observamos lo siguiente:

Sea K un cuerpo ordenado que contenga a $\mathbb{Q}$ como subcuerpo denso. Una sucesión $\{x_n\}_{n\in\omega}$ en K converge a $x \in K$ si y sólo si

$$\bigwedge rs \in \mathbb{Q}(r < x < s \rightarrow \bigvee m \in \omega \bigwedge n \geq m\ r < x_n < s).$$

En efecto, si se da la convergencia, tomamos $\epsilon = \min\{s - x, x - r\} > 0$, con lo que existe un m tal que si $n \geq m$ entonces $|x_n - x| < \epsilon$, luego $-\epsilon < x_n - x < \epsilon$, luego $r - x \leq -\epsilon < x_n < x < \epsilon \leq s - x$, luego $r < x_n < s$.

Recíprocamente, si se da esta condición, dado $\epsilon > 0$, podemos tomar r, $s \in \mathbb{Q}$ tales que $x - \epsilon < r < x < s < x + \epsilon$ y existe un $m \in \omega$ tal que si $n \geq m$ entonces $r < x_n < s$, luego $x - \epsilon < x_n < x + \epsilon$, luego $|x_n - x| < \epsilon$.

El interés de esta caracterización es que en ella no intervienen ni la suma ni el producto. Sólo la relación de orden. Por lo tanto, podemos concluir que si tenemos dos estructuras de cuerpo ordenado en $C(\mathbb{Q})$ (con la relación de orden de $C(\mathbb{Q})$ en común), una sucesión converge respecto de una de ellas si y sólo si lo hace respecto de la otra, y en ambos casos al mismo límite.

Por lo tanto, dados α, $\beta \in C(\mathbb{Q})$, existen sucesiones $\{q_n\}_{n\in\omega}$, $\{r_n\}_{n\in\omega}$ en $\mathbb{Q}$ tales que

$$\lim_n i_2(q_n) = \alpha, \qquad \lim_n i_2(r_n) = \beta$$

(en principio respecto de una estructura, luego también respecto de la otra). El teorema 7.23 nos da que las sucesiones $\{i_2(q_n) + i_2(r_n)\}_{n\in\omega}$ y $\{i_2(q_n)i_2(r_n)\}_{n\in\omega}$ convergen a $\alpha + \beta$ y $\alpha\beta$ respecto de ambas estructuras, es decir, que ambas tienen la misma suma y el mismo producto, luego son la misma estructura. ■

Esto nos da una definición alternativa de $\mathbb{R}$:

Definición 7.41 Llamaremos *cuerpo de los números reales* a la compleción $\mathbb{R} = C(\mathbb{Q})$ del cuerpo $\mathbb{Q}$ de los números racionales, considerado como cuerpo ordenado con las únicas operaciones que extienden a las de $\mathbb{Q}$ según el teorema anterior.

Técnicamente, no podemos llamar $\mathbb{R}$ a dos cosas a la vez,[13] pero en la práctica es del todo irrelevante que adoptemos la definición 7.30 o la anterior, pues si llamamos $\mathbb{R}_1$ al cuerpo ordenado definido en 7.30 y $\mathbb{R}_2$ al que acabamos de definir, sabemos que son isomorfos como cuerpos ordenados, luego tienen exactamente las mismas propiedades.

[13] La construcción de $\mathbb{R}$ mediante sucesiones se debe a Cantor, mientras que la construcción mediante secciones iniciales es esencialmente de Dedekind.

No obstante, en las pocas ocasiones en las que la estructura conjuntista de $\mathbb{R}$ pueda ser relevante, la definición que hace a $\mathbb{R} = C(\mathbb{Q})$ es ligeramente más práctica, porque un subconjunto de $\mathbb{Q}$ es técnicamente más sencillo que una clase de equivalencia de sucesiones de Cauchy en $\mathbb{Q}$. Por ello, en lo sucesivo nos quedaremos con esta última definición. Naturalmente, todos los hechos que hemos demostrado para $\mathbb{R}$ con la definición anterior siguen valiendo trivialmente con la nueva definición. De hecho, sólo se apoyan en que $\mathbb{R}$ es un cuerpo ordenado completo.

Llamaremos $\overline{\mathbb{R}} = \overline{C(\mathbb{Q})} = \{-\infty\} \cup \mathbb{R} \cup \{+\infty\}$, que es también un continuo. Notemos que los intervalos $]-\infty, b[$ y $]a, +\infty[$, considerados como subconjuntos de $\mathbb{R}$ coinciden con los intervalos de $\overline{\mathbb{R}}$ considerados como intervalos acotados en los que $\pm\infty$ son el máximo y el mínimo de $\overline{\mathbb{R}}$.

Nota Hemos probado la existencia de la suma y el producto en $C(\mathbb{Q})$ a partir de la construcción de $\mathbb{R}$ mediante sucesiones de Cauchy, pero es posible definirlas directamente, haciendo

$$\alpha + \beta = \sup\{r + s \mid r, s \in \mathbb{Q} \land r < \alpha \land s < \beta\},$$

y $\alpha\beta = \sup\{rs \mid r, s \in \mathbb{Q} \land 0 < r < \alpha \land 0 < s < \beta\}$ si $\alpha, \beta > 0$.

Cuando los dos factores no son positivos hay que definir el producto mediante las reglas de los signos:

$$\alpha\beta = \begin{cases} -((-\alpha)\beta) & \text{si } \alpha < 0,\ \beta > 0, \\ -(\alpha(-\beta)) & \text{si } \alpha > 0,\ \beta < 0, \\ (-\alpha)(-\beta) & \text{si } \alpha < 0,\ \beta < 0. \end{cases}$$

(y $\alpha\beta = 0$ si uno de los factores es nulo). Las comprobaciones por este camino son bastante más tediosas que las que requiere la construcción mediante sucesiones de Cauchy. No obstante, desde un punto de vista conjuntista, tiene ciertas ventajas. Además de que, como ya hemos comentado, $\mathbb{R}$ resulta ser estructuralmente más sencillo, esta construcción permite definir de la clase de los números reales, con su suma, su producto y su relación de orden, sin necesidad de suponer AP, aunque sin este axioma no se puede probar que $\mathbb{R}$ sea un conjunto. ■

Ahora tenemos una caracterización de $\mathbb{R}$ como conjunto ordenado:

Teorema 7.42 *Un conjunto ordenado es semejante a $\mathbb{R}$ si y sólo si tiene las propiedades siguientes:*

a) Está totalmente ordenado, no tiene máximo ni mínimo y es denso en sí mismo.

b) Es completo.

c) 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 7.9 nos da una semejanza $f : \mathbb{Q} \longrightarrow D$, que es una inmersión densa $f : \mathbb{Q} \longrightarrow X$. El teorema anterior 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 $]\alpha, \beta[\cong \mathbb{R}$.

7.6 Sumas infinitas

En cualquier anillo tenemos definidas las sumas de la forma $\sum\limits_{i\in I} a_i$, donde I es un conjunto finito. Veamos ahora que podemos definir sumas infinitas de números reales. Si queremos que I sea un conjunto arbitrario necesitamos restringirnos a sumandos positivos:

Definición 7.43 Si $\{a_i\}_{i\in I}$ es una familia de números reales $a_i \geq 0$, definimos

$$\sum_{i\in I} a_i = \sup\{\sum_{i\in I_0} a_i \mid I_0 \subset I \text{ finito}\}.$$

Aquí hay que entender que el supremo es en $\overline{\mathbb{R}}$, de modo que puede ser $+\infty$.

Notemos que, trivialmente, si $J \subset I$, se cumple que $\sum\limits_{i\in J} a_i \leq \sum\limits_{i\in I} a_i$. También es fácil ver que si $0 \leq a_i \leq b_i$ entonces $\sum\limits_{i\in I} a_i \leq \sum\limits_{i\in I} b_i$.

Si I es finito, el hecho de que los a_i sean positivos implica claramente que el conjunto

$$\{\sum_{i\in I_0} a_i \mid I_0 \subset I \text{ finito}\}$$

alcanza su máximo cuando $I_0 = I$, por lo que la suma que acabamos de definir coincide con la que ya teníamos definida.

Si $I = I_1 \cup I_2$ y la unión es disjunta, se cumple la relación

$$\sum_{i\in I} a_i = \sum_{i\in I_1} a_i + \sum_{i\in I_2} a_i,$$

donde hay que entender que una suma con un sumando infinito es, por definición, infinita. En efecto, si alguno de los dos sumandos de la derecha es $+\infty$, es claro que la suma de la izquierda también es infinita y se tiene la igualdad, así que suponemos que las dos sumas son finitas. Si $I_0^1 \subset I_1$, $I_0^2 \subset I_2$ son conjuntos finitos, tenemos que

$$\sum_{i\in I_0^1} a_i + \sum_{i\in I_0^2} a_i = \sum_{i\in I_0^1\cup I_0^2} a_i \leq \sum_{i\in I} a_i,$$

luego $\sum\limits_{i\in I_0^1} a_i \leq \sum\limits_{i\in I} a_i - \sum\limits_{i\in I_0^2} a_i$, luego $\sum\limits_{i\in I_1} a_i \leq \sum\limits_{i\in I} a_i - \sum\limits_{i\in I_0^2} a_i$, luego $\sum\limits_{i\in I_0^2} a_i \leq \sum\limits_{i\in I} a_i - \sum\limits_{i\in I_1} a_i$, $\sum\limits_{i\in I_2} a_i \leq \sum\limits_{i\in I} a_i - \sum\limits_{i\in I_1} a_i$, y $\sum\limits_{i\in I_1} a_i + \sum\limits_{i\in I_2} a_i \leq \sum\limits_{i\in I} a_i$.

Por otra parte, si $I_0 \subset I$ es finito, entonces

$$\sum_{i\in I_0} a_i = \sum_{i\in I_0\cap I_1} a_i + \sum_{i\in I_0\cap I_2} a_i \leq \sum_{i\in I_1} a_i + \sum_{i\in I_2} a_i,$$

luego $\sum\limits_{i\in I} a_i \leq \sum\limits_{i\in I_1} a_i + \sum\limits_{i\in I_2} a_i$ y tenemos la igualdad. Más en general, si $I = \bigcup\limits_{j\in J} I_j$ y la unión es disjunta, entonces se cumple la asociatividad generalizada:

$$\sum_{i\in I} a_i = \sum_{j\in J}\sum_{i\in I_j} a_i,$$

donde nuevamente entendemos que un sumatorio con un sumando infinito es infinito. En efecto, como antes podemos suponer que las sumas sobre los I_j son finitas. Si $J_0 \subset J$ es finito, una simple inducción sobre $|J_0|$ basada en el caso probado anteriormente implica que

$$\sum_{j\in J_0}\sum_{i\in I_j} a_i = \sum_{i\in \bigcup\limits_{j\in J_0} I_j} a_i \leq \sum_{i\in I} a_i,$$

luego $\sum\limits_{j\in J}\sum\limits_{i\in I_j} a_i \leq \sum\limits_{i\in I} a_i$. Recíprocamente, si $I_0 \subset I$ es finito, existe $J_0 \subset J$ finito tal que $I_0 \subset \bigcup\limits_{j\in J_0} I_j$, y así

$$\sum_{i\in I_0} a_i = \sum_{j\in J_0}\sum_{i\in I_j\cap I_0} a_i \leq \sum_{j\in J_0}\sum_{i\in I_j} a_i \leq \sum_{j\in J}\sum_{i\in I_j} a_i,$$

luego $\sum\limits_{i\in I_0} a_i \leq \sum\limits_{j\in J}\sum\limits_{i\in I_j} a_i$ y tenemos la igualdad.

Argumentos similares demuestran que, si $a, b > 0$,

$$\sum_{i\in I}(aa_i + bb_i) = a\sum_{i\in I} a_i + b\sum_{i\in I} b_i.$$

Sucede que el nivel de generalidad de esta definición es en parte una mera apariencia:

Teorema 7.44 (AEN) *Si $\{a_i\}_{i\in I}$ es una familia de números reales positivos tal que $\sum\limits_{i\in I} a_i < +\infty$, entonces el conjunto $I^* = \{i \in I \mid a_i \neq 0\}$ es numerable, y*

$$\sum_{i\in I} a_i = \sum_{i\in I^*} a_i.$$

DEMOSTRACIÓN: Para cada $i \in I^*$ sea n_i el menor número natural no nulo tal que $a_i > 1/n_i$. Sea $f : I \longrightarrow \mathbb{N}$ la aplicación dada por $f(i) = n_i$. Entonces $I^* = \bigcup\limits_{n\in\mathbb{N}} f^{-1}[n]$. Basta probar que todos los conjuntos $f^{-1}[n]$ son finitos, pues entonces I^* es numerable.[14] Supongamos que existe un n tal que $f^{-1}[n]$ es infinito. Entonces, dado $m \in \mathbb{N}$, existe $I_0 \subset f^{-1}[n]$ tal que $|I_0| = mn$, con lo que

$$\sum_{i\in I} a_i \geq \sum_{i\in I_0} a_i \geq \sum_{i\in I_0} \tfrac{1}{n} = m,$$

luego la suma es infinita.

Dado $\epsilon > 0$, existe $I_0 \subset I$ finito tal que $\sum\limits_{i\in I} a_i - \epsilon < \sum\limits_{i\in I_0} a_i$, pero, por las propiedades de las sumas finitas, es claro que

$$\sum_{i\in I} a_i - \epsilon < \sum_{i\in I_0} a_i = \sum_{i\in I_0\cap I^*} a_i \leq \sum_{i\in I^*} a_i \leq \sum_{i\in I} a_i.$$

Así pues, la distancia entre las sumas para I e I^* es menor que cualquier $\epsilon > 0$, luego es nula. ■

Por lo tanto, no perdemos generalidad si estudiamos únicamente sumas numerables. Cualquier resultado sobre ellas se extiende trivialmente a sumas arbitrarias mediante el teorema anterior. Cuando el conjunto de índices está contenido en $\mathbb{N}$ es costumbre usar notaciones como

$$\sum_{i=0}^{\infty} a_i, \qquad \sum_{i=k}^{\infty} a_i, \qquad \sum_{i\geq k} a_i,$$

con el sentido obvio, reducible trivialmente a la definición que hemos dado.

Teorema 7.45 *Si $\{a_i\}_{i\in\omega}$ es una sucesión de números reales positivos,*

$$\sum_{i=0}^{\infty} a_i = \lim_n \sum_{i=0}^{n} a_i.$$

DEMOSTRACIÓN: Dado $\epsilon > 0$, existe un $I \subset \omega$ finito tal que

$$\sum_{i=0}^{\infty} a_i - \epsilon < \sum_{i\in I} a_i \leq \sum_{i=0}^{\infty} a_i.$$

Sea $m \in \omega$ tal que $I \subset m$, de modo que, si $n \geq m$, se cumple

$$\sum_{i=0}^{\infty} a_i - \epsilon < \sum_{i\in I} a_i \leq \sum_{i=0}^{n} a_i \leq \sum_{i=0}^{\infty} a_i.$$

El teorema 7.12 implica entonces que $\sum\limits_{i=0}^{\infty} a_i - \epsilon \leq \lim\limits_n \sum\limits_{i=0}^{n} a_i \leq \sum\limits_{i=0}^{\infty} a_i$. Esto significa que la distancia entre el límite y la suma es menor que ϵ, para todo $\epsilon > 0$, luego es nula. ■

[14] Aquí usamos AEN, porque es necesario elegir una aplicación de cada conjunto $f^{-1}[n]$ en su cardinal para justificar que la unión es numerable.

Notemos que la igualdad del teorema anterior puede tomarse como definición de una suma infinita numerable, y en tal caso no necesitamos suponer que los términos de la serie son positivos (aunque entonces el límite puede no existir, y hay que distinguir entre series convergentes y divergentes y, en caso de convergencia, el valor de la suma puede depender del orden en que se enumeran los términos). No obstante, no vamos a necesitar tales sumas.

Vamos a calcular algunas series infinitas. Para ello empezamos observando:

Teorema 7.46 *Si* $0 < r < 1$, *entonces* $\lim_n r^n = 0$.

DEMOSTRACIÓN: Tenemos que $1/r > 1$, luego $1/r = 1 + s$, con $s > 0$. Es fácil ver[15] que $1 + ns \leq (1 + s)^n$, luego $1 + ns \leq 1/r^n$. Dado $\epsilon > 0$, podemos tomar $m \in \omega$ tal que $(1/\epsilon - 1)/s < m$, con lo que si $n \geq m$ se cumple que $1/\epsilon < 1 + ns \leq 1/r^n$, luego $r^n < \epsilon$. ■

Teorema 7.47 *Si* $0 < r < 1$, *entonces* $\displaystyle\sum_{n=k}^{\infty} r^n = \frac{r^k}{1-r}$.

DEMOSTRACIÓN: Una simple inducción prueba que, para $m \geq k$,

$$\sum_{n=k}^{m} r^n = \frac{r^k - r^{m+1}}{1-r}.$$

Si hacemos tener m a infinito, las propiedades de los límites, junto con el teorema anterior, implican trivialmente el resultado. ■

Teorema 7.48 *Sea* $b \geq 2$ *un número natural. Entonces, cada número real* $\alpha \in [0, 1[$ *se expresa de forma única como*

$$\alpha = \sum_{n=1}^{\infty} \frac{c_n}{b^n},$$

para cierta sucesión $\{c_n\}_{n=1}^{\infty}$ *de números naturales menores que* b *que no se haga constante igual a* $b - 1$ *a partir de un término.*

DEMOSTRACIÓN: Observemos en primer lugar que, si $k \geq 1$, por el teorema anterior tenemos

$$\sum_{n=k}^{\infty} \frac{c_n}{b^n} \leq \sum_{n=k}^{\infty} \frac{b-1}{b^n} = (b-1)\frac{b^{-k}}{1-b^{-1}} = (b-1)\frac{b^{-k+1}}{b-1} = \frac{1}{b^{k-1}}.$$

[15] Es consecuencia inmediata de la fórmula del binomio de Newton, pero puede probarse también por inducción sobre n, sin más que tener en cuenta que $1 \leq (1 + s)^n$, con lo que $s \leq s(1 + s)^n$, luego

$$1 + (n + 1)s \leq s + 1 + ns \leq s + (1 + s)^n \leq s(1 + s)^n + (1 + s)^n = (1 + s)^{n+1}.$$

Además, la desigualdad es estricta salvo que $\bigwedge n \geq k\ c_n = b-1$. Tomando $k = 1$, esto prueba en particular que todas las series del enunciado[16] son números en $[0, 1[$. Veamos que sucesiones distintas determinan números distintos. Si $\{c_n\}_{n=1}^{\infty} \neq \{c'_n\}_{n=1}^{\infty}$, sea k el mínimo natural en que difieren. No perdemos generalidad si suponemos que $c_k < c'_k$. Entonces

$$\sum_{n=1}^{\infty} \frac{c_n}{b^n} = \sum_{n=1}^{k-1} \frac{c_n}{b^n} + \frac{c_k}{b^k} + \sum_{n=k+1}^{\infty} \frac{c_n}{b^n} < \sum_{n=1}^{k-1} \frac{c'_n}{b^n} + \frac{c_k}{b^k} + \frac{1}{b^k}$$

$$\leq \sum_{n=1}^{k-1} \frac{c'_n}{b^n} + \frac{c'_k}{b^k} \leq \sum_{n=1}^{k-1} \frac{c'_n}{b^n} + \frac{c'_k}{b^k} + \sum_{n=k+1}^{\infty} \frac{c'_n}{b^n} = \sum_{n=1}^{\infty} \frac{c'_n}{b^n},$$

luego las series son distintas. Notemos que en la desigualdad estricta hemos usado que no todo $c_n = b-1$. En tal caso tendremos una igualdad si $c'_k = c_k+1$ y $\bigwedge n > k\ c'_n = 0$. Veamos que todo $\alpha \in [0, 1[$ admite una expresión de esta forma. Definiremos la sucesión $\{c_n\}_{\in\omega}$ por recurrencia. Puesto que $0/b \leq \alpha < b/b$, existe un único número natural $c_1 < b$ tal que $c_1/b \leq \alpha < (c_1 + 1)/b$. Supongamos definidos $\{c_n\}_{n=1}^{k}$ tales que

$$\sum_{n=1}^{k} \frac{c_n}{b^n} \leq \alpha < \sum_{n=1}^{k} \frac{c_n}{b^n} + \frac{b}{b^{k+1}}.$$

Entonces existe un único número natural $c_{k+1} < b$ tal que

$$\sum_{n=1}^{k} \frac{c_n}{b^n} + \frac{c_{k+1}}{b^{k+1}} \leq \alpha < \sum_{n=1}^{k} \frac{c_n}{b^n} + \frac{c_{k+1}+1}{b^{k+1}},$$

que es lo mismo que

$$\sum_{n=1}^{k+1} \frac{c_n}{b^n} \leq \alpha < \sum_{n=1}^{k+1} \frac{c_n}{b^n} + \frac{b}{b^{k+2}}.$$

Por lo tanto, tenemos una sucesión con la propiedad de que

$$\left| \alpha - \sum_{n=1}^{k} \frac{c_n}{b^n} \right| \leq \frac{1}{b^k}.$$

Hemos visto que la sucesión $\{(1/b)^k\}_{k\in\omega}$ tiende a 0, de donde se sigue inmediatamente que

$$\alpha = \lim_k \sum_{n=1}^{k} \frac{c_n}{b^n} = \sum_{n=1}^{\infty} \frac{c_n}{b^n}.$$

No puede ocurrir que la sucesión obtenida sea finalmente igual a $b-1$, pero en lugar de justificarlo es más fácil concluir observando que si se diera el caso hemos probado que α admite otro desarrollo en serie en el que la "cola" igual a $b-1$ se sustituye por otra igual a 0. ■

[16]Esto vale incluso si la sucesión de coeficientes es finalmente igual a $b-1$ salvo si $k = 1$ y $\bigwedge n \geq 1\ c_n = b-1$, en cuyo caso la suma es 1.

Definición 7.49 Si $\alpha \in \mathbb{R}$, la sucesión $\{c_n\}_{n=1}^{\infty}$ dada por el teorema anterior para la parte fraccionaria de α recibe el nombre de *desarrollo en base b* de la parte fraccionaria de α que, junto con el desarrollo de la parte entera dado por la definición 2.50 constituye el *desarrollo en base b* de número real α.

Cuando no se especifica la base se sobrentiende que estamos tomando $b = 10$ y hablamos entonces de la *expresión decimal* de un número real. La forma usual de representar las primeras cifras decimales de un número real es, por ejemplo: $\sqrt{1\,000} = 31.6227\ldots$ lo que significa que

$$\sqrt{1\,000} = 3 \cdot 10^1 + 1 \cdot 10^0 + \frac{6}{10^1} + \frac{2}{10^2} + \frac{2}{10^3} + \frac{7}{10^4} + \cdots$$

La existencia de desarrollos decimales proporciona otra demostración de que $\overline{\overline{\mathbb{R}}} = 2^{\aleph_0}$, pues cada elemento de ${}^{\omega}2$ constituye el desarrollo decimal (o incluso en base 3) de un número real distinto, luego $\overline{\overline{R}} \geq 2^{\aleph_0}$, y la otra desigualdad se sigue de que $\mathbb{R} \subset \mathcal{P}\mathbb{Q}$.

Observación Terminamos con una reflexión sobre lo que hemos visto a lo largo de todo el capítulo: en ningún momento hemos necesitado el axioma de regularidad (salvo a lo sumo para definir $2^{\aleph_0}$ en ausencia del axioma de elección, pero el teorema sobre el cardinal de $\mathbb{R}$ podría reformularse sin nombrarlo), pero el hecho es que todos los conjuntos numéricos que hemos definido son regulares.

Por ejemplo, todos los pares ordenados de números naturales están contenidos en V_ω, luego $\omega \times \omega \subset V_\omega$. Si $n \in \mathbb{Z}$, por definición $n \subset \omega \times \omega \subset V_\omega$, luego $n \in V_{\omega+1}$, luego $\mathbb{Z} \subset V_{\omega+1}$ y $\mathbb{Z} \in V_{\omega+2}$.

Ahora, si m, $n \in \mathbb{Z}$, entonces $\{m\}$, $\{m, n\} \in V_{\omega+2}$, luego $(m, n) \in V_{\omega+3}$, luego $\mathbb{Z} \times \mathbb{Z} \subset V_{\omega+3}$. Si $q \in \mathbb{Q}$, por definición $q \subset \mathbb{Z} \times \mathbb{Z} \subset V_{\omega+3}$, luego $q \in V_{\omega+4}$, luego $\mathbb{Q} \subset V_{\omega+4}$, luego $\mathbb{Q} \in V_{\omega+5}$.

Si definimos los números reales como secciones iniciales abiertas de $\mathbb{Q}$, entonces si $\alpha \in \mathbb{R}$ tenemos que $\alpha \subset \mathbb{Q} \subset V_{\omega+4}$, luego $\alpha \in V_{\omega+5}$, luego $\mathbb{R} \subset V_{\omega+5}$ y $\mathbb{R} \in V_{\omega+6}$. Si construimos $\mathbb{R}$ mediante sucesiones de Cauchy, su lugar en la jerarquía regular es unos peldaños más alto.

El caso es que si prosiguiéramos analizando las construcciones que manejan habitualmente los matemáticos, como los espacios $\mathbb{R}^n$, los espacios ℓ^p, los espacios de funciones holomorfas en un abierto del plano complejo, etc., análisis tan sencillos como los que acabamos de realizar mostrarían que todos ellos están en algún $V_{\omega+n}$, para cierto $n \in \omega$. En efecto, cada construcción sólo aumenta un número finito de pasos el rango de los conjuntos involucrados, por lo que nunca llegamos a $V_{\omega+\omega}$. La mayor parte de las matemáticas actuales se desarrolla de hecho en $V_{\omega+\omega}$. Por ello, resulta irrelevante plantearse si existen o no conjuntos no regulares. ■

Capítulo VIII

Elementos de topología

En el capítulo I hemos desarrollado el lenguaje básico de la teoría de conjuntos, que incluye los conceptos de "relación", "función", "operación" y todos los relacionados con ellos, y con este lenguaje hemos desarrollado los contenidos que hemos visto hasta ahora. Sin embargo, en este punto resulta conveniente enriquecer nuestro lenguaje básico con el lenguaje de la topología conjuntista. La topología es una abstracción de la geometría y, si bien una parte de esta rama de la matemática proporciona técnicas muy potentes para trabajar en contextos geométricos, otra parte desarrolla los conceptos topológicos básicos en una dirección completamente opuesta, y permite aplicar razonamientos que tienen su origen en la geometría en contextos abstractos totalmente alejados de toda base geométrica intuitiva.

El tránsito de la topología con base geométrica a la topología puramente conjuntista se realiza a través del concepto de espacio métrico, que ya conocemos. Podemos pensar que el concepto más elemental que formaliza la topología es el de "alrededor de un punto". Si pensamos en los puntos del plano, o del espacio intuitivo, vemos que sabemos dar sentido a afirmaciones sobre si todos los puntos de "alrededor" de un punto dado cumplen algo. Por ejemplo, podemos decir que una esfera contiene a todos los puntos de alrededor de su centro, y esto tiene un sentido muy preciso a pesar de que no tiene ningún sentido decir si un punto dado es o no uno de los puntos de alrededor de otro.

Más concretamente, si x es un punto de un espacio métrico M y $\epsilon > 0$ es un número real, podemos definir la bola abierta de centro x y radio ϵ como $B_\epsilon(x) = \{y \in M \mid d(x, y) < \epsilon\}$, de modo que, en el caso del plano o del espacio intuitivo con la distancia intuitiva entre puntos, se trata de el círculo o la esfera de centro x y radio ϵ. La idea básica es que, por pequeño que sea el radio ϵ, podemos decir que la bola $B_\epsilon(x)$ contiene a todos los puntos de alrededor de x, de modo que afirmar que una propiedad la cumplen todos los puntos de alrededor de x es lo mismo que afirmar que existe un $\epsilon > 0$ tal que todos los puntos de $B_\epsilon(x)$ cumplen la propiedad en cuestión.

Esto nos lleva a su vez a la noción de entorno: Un subconjunto $U \subset M$ es un entorno de un punto $x \in M$ si existe un $\epsilon > 0$ tal que $B_\epsilon(x) \subset U$, y así, los entornos de un punto son los conjuntos que contienen a todos los puntos de alrededor del punto. La noción de "entorno" captura de forma matemáticamente precisa la noción intuitiva de "alrededor". En teoría toda la topología podría formularse tomando como base la noción de entorno debidamente abstraída de su origen geométrico, pero resulta más conveniente desde un punto de vista técnico partir de un concepto relacionado que captura la misma información, el concepto de "conjunto abierto". En un espacio métrico, un conjunto A es abierto si es un entorno de todos sus puntos, es decir, si cuando contiene a un punto, contiene también a todos los puntos de su alrededor.

Por ejemplo, cuando consideramos el conjunto de los puntos de un círculo en el plano entendiendo que incluye a los de la circunferencia que lo limita, no se trata de un conjunto abierto, pues un punto de la circunferencia está en el círculo, pero tiene puntos alrededor que no están en el círculo. En cambio, si consideramos que el círculo contiene únicamente los puntos que quedan dentro de la circunferencia, pero sin contar a los de ésta, entonces tenemos un conjunto abierto.

El concepto de abierto es equivalente al de entorno en el sentido de que hemos definido "abierto" a partir de "entorno" y, recíprocamente, podemos definir "entorno" a partir de "abierto": un conjunto U es un entorno de un punto x si y sólo si existe un abierto A tal que $x \in A \subset U$. Sin embargo, como decimos, es más conveniente construir la topología sobre el concepto de abierto.

Trabajamos en NBG, aunque indicaremos explícitamente todo uso del axioma de elección (AE) o del axioma de elección numerable (AEN). Como de costumbre, el axioma de regularidad es totalmente irrelevante.

8.1 Espacios topológicos

La definición general de espacio topológico es tan abstracta y puramente conjuntista que nadie reconocería en ella su origen geométrico:

Definición 8.1 Una *topología* en un conjunto X es una familia $\mathcal{T} \subset \mathcal{P}X$ que cumpla las propiedades siguientes:

a) $\varnothing$, $X \in \mathcal{T}$,

b) Si $\{A_i\}_{i\in I}$ es una familia de elementos de $\mathcal{T}$, entonces $\bigcup\limits_{i\in I} A_i \in \mathcal{T}$,

c) Si A, $B \in \mathcal{T}$, entonces $A \cap B \in \mathcal{T}$.

Un *espacio topológico* es un par $(X, \mathcal{T})$, donde X es un conjunto y $\mathcal{T}$ es una topología en X. Los elementos de $\mathcal{T}$ se llaman *subconjuntos abiertos* de X.

Así pues, la definición de topología exige que $\varnothing$ y X sean abiertos, que la unión de cualquier familia de abiertos sea abierta y que la intersección de dos abiertos sea abierta. Una simple inducción a partir de esta última propiedad nos da que la intersección de cualquier cantidad finita de abiertos es abierta.

Notemos que la propiedad b) podría expresarse más brevemente como que $\bigwedge \mathcal{F}\ (\mathcal{F} \subset \mathcal{T} \to \bigcup \mathcal{F} \in \mathcal{T})$.

En la práctica escribiremos X en lugar de $(X, \mathcal{T})$ y sobrentenderemos que $\mathcal{T}$ es la topología del espacio topológico X, teniendo en cuenta que $\mathcal{T}$ será una topología distinta en cada caso.

Un subconjunto U de un espacio topológico X es un *entorno* de un punto $x \in X$ si existe un abierto A tal que $x \in A \subset U$.

Observemos que un conjunto A es abierto si y sólo si es entorno de todos sus puntos. En efecto, si es abierto cumple trivialmente la definición de entorno para cada uno de sus puntos, mientras que si cumple la condición sobre entornos, entonces $A = \bigcup \mathcal{F}$, donde $\mathcal{F} = \{U \in \mathcal{T} \mid U \subset A\}$, luego A es abierto porque la unión de abiertos es abierta.

Diremos que un espacio topológico X es *de Hausdorff* si

$$\bigwedge xy \in X(x \neq y \to \bigvee AB \in \mathcal{T}(x \in A \land y \in B \land A \cap B = \varnothing)).$$

Es decir, si puntos distintos pertenecen a abiertos disjuntos. (Se dice entonces que A y B *separan* a x e y.) Es inmediato ver que en la definición se puede sustituir la condición de que A y B sean abiertos por la de que sean entornos de x, de modo que un espacio es de Hausdorff si puntos distintos tienen entornos disjuntos.

Ejemplos Dado un conjunto X, la *topología discreta* en X es $\mathcal{T} = \mathcal{P}X$, y la *topología trivial* es $\mathcal{T} = \{\varnothing, X\}$.

Es inmediato comprobar que ambas son realmente topologías en X. Respecto de la topología discreta todos los subconjuntos de X son abiertos, por lo que es trivialmente una topología de Hausdorff (dados dos puntos distintos x, $y \in X$, tenemos que $\{x\}$, $\{y\}$ son abiertos disjuntos que los separan), mientras que la topología trivial tiene únicamente los abiertos exigidos por la definición de topología, y no es de Hausdorff salvo en el caso trivial en que $|X| \leq 1$, en cuyo caso coincide con la topología discreta.

Se dice también que un espacio topológico es *discreto* o *trivial* si su topología es la discreta o la trivial, respectivamente.

Observemos también que todo espacio de Hausdorff finito X es discreto. En efecto, si $x \in X$, sea U un abierto que contenga a x y que sea minimal para la inclusión (existe porque $\mathcal{P}X$ es finito). Tiene que ser $U = \{x\}$, porque si existiera $y \in U$, entonces, por la propiedad de Hausdorff, existirían abiertos disjuntos A y B tales que $x \in A$, $y \in B$, pero entonces $y \notin U \cap A$, que sería entonces un abierto tal que $x \in U \cap A \subsetneq U$, en contra de la minimalidad de U.

■

Para dar ejemplos más representativos conviene introducir primero el concepto de base de una topología:

Definición 8.2 Una *base* de un espacio topológico X es una familia de abiertos $\mathcal{B}$ (llamados *abiertos básicos*) tal que todo abierto de X se expresa como unión de abiertos básicos.

Aquí hay que entender que $\varnothing = \bigcup \varnothing$ es siempre unión de "cero" abiertos básicos, luego no hace falta que $\varnothing$ sea él mismo un abierto básico. Notemos que una definición equivalente es que $\mathcal{B} \subset \mathcal{T}$ es base de X si

$$\bigwedge A \in \mathcal{T} \bigwedge x \in A \bigvee B \in \mathcal{B}\ x \in B \subset A,$$

pues si se cumple esto y $A \in \mathcal{T}$, entonces $A = \bigcup \mathcal{F}$, donde $\mathcal{F} = \{B \in \mathcal{B} \mid B \subset A\}$.

El interés de este concepto se debe a los dos teoremas siguientes:

Teorema 8.3 *Si $\mathcal{B}$ es una base de un espacio topológico X, se cumplen las dos propiedades siguientes:*

a) $\bigcup \mathcal{B} = X$,

b) $\bigwedge AB \in \mathcal{B} \bigwedge x \in A \cap B \bigvee C \in \mathcal{B}\ x \in C \subset A \cap B$.

Demostración: Como X es abierto, debe expresarse como unión de una familia $\mathcal{F} \subset \mathcal{B}$ de abiertos básicos, luego $X = \bigcup \mathcal{F} \subset \bigcup \mathcal{B} \subset X$ y tenemos la igualdad.

Si $x \in A \cap B$, donde A y B son abiertos, entonces $A \cap B$ es también abierto, luego existe un abierto básico C que cumple lo pedido. ∎

Lo interesante es que estas propiedades bastan para que una familia de conjuntos sea la base de una topología:

Teorema 8.4 *Sea X un conjunto y $\mathcal{B} \subset \mathcal{P}X$ una familia de subconjuntos de X que tenga las propiedades siguientes:*

a) $\bigcup \mathcal{B} = X$,

b) $\bigwedge AB \in \mathcal{B} \bigwedge x \in A \cap B \bigvee C \in \mathcal{B}\ x \in C \subset A \cap B$.

Entonces existe una única topología en X que tiene a $\mathcal{B}$ por base, y es la mínima, respecto de la inclusión, para la que los elementos de $\mathcal{B}$ son abiertos.

Demostración: Definimos $\mathcal{T} = \{\bigcup \mathcal{F} \mid \mathcal{F} \subset \mathcal{B}\}$. La condición a) afirma que $X \in \mathcal{T}$ y trivialmente $\varnothing = \bigcup \varnothing \in \mathcal{T}$.

Si $\mathcal{F} \subset \mathcal{T}$, para cada $A \in \mathcal{F}$ definimos $\mathcal{F}_A = \{B \in \mathcal{B} \mid B \subset A\}$, de modo que $A = \bigcup \mathcal{F}_A$. Sea $\mathcal{F}^* = \bigcup\limits_{A \in \mathcal{F}} \mathcal{F}_A \subset \mathcal{B}$. Claramente $\bigcup \mathcal{F} = \bigcup \mathcal{F}^* \in \mathcal{T}$.

Por último, si $A,\ B \in \mathcal{T}$, sea $\mathcal{F} = \{B \in \mathcal{B} \mid B \subset A \cap B\}$. Veamos que $A \cap B = \bigcup \mathcal{F}$. Una inclusión es inmediata. Para probar la otra tomamos $x \in A \cap B$ y, por la hipótesis b) existe un $C \in \mathcal{B}$ tal que $x \in C \in \mathcal{F}$, luego $x \in \bigcup \mathcal{F}$.

La unicidad y la parte final son inmediatas: si $\mathcal{T}'$ es una topología en la que los elementos de $\mathcal{B}$ son abiertos, necesariamente $\mathcal{T} \subset \mathcal{T}'$, luego $\mathcal{T}$ es la única topología de base $\mathcal{B}$. ∎

Espacios métricos Si M es un espacio métrico, $x \in M$ y $\epsilon > 0$, definimos la *bola abierta* de centro x y radio ϵ como

$$B_\epsilon(x) = \{y \in M \mid d(x, y) < \epsilon\}.$$

Vamos a comprobar que la familia $\mathcal{B}$ formada por todas las bolas abiertas en M satisface las condiciones del teorema anterior para ser base de una topología en M:

Puesto que $x \in B_1(x)$, es obvio que $\bigcup \mathcal{B} = X$. Si $x \in B_{\epsilon_1}(u) \cap B_{\epsilon_2}(v)$, tomamos $\epsilon = \text{mín}\{\epsilon_1 - d(x, u), \epsilon_2 - d(x, v)\} > 0$ y observamos que

$$x \in B_\epsilon(x) \subset B_{\epsilon_1}(u) \cap B_{\epsilon_2}(v),$$

pues si $z \in B_\epsilon(x)$ entonces $d(z, u) \leq d(z, x) + d(x, u) < \epsilon + d(x, u) < \epsilon_1$, e igualmente $d(z, v) < \epsilon_2$.

En lo sucesivo consideraremos a todo espacio métrico M como espacio topológico con la topología que tiene por base a sus bolas abiertas.

Observemos que en el razonamiento anterior hemos visto en particular que si $x \in B_{\epsilon_1}(u)$, entonces existe un $\epsilon > 0$ tal que $x \in B_\epsilon(x) \subset B_{\epsilon_1}(u)$. Esto implica que

$$\bigwedge A \subset M(A \in \mathcal{T} \leftrightarrow \bigwedge x \in A \bigvee \epsilon > 0 \ B_\epsilon(x) \subset A).$$

(En principio sería $\bigwedge x \in A \bigvee u \in M \bigvee \epsilon_1 > 0 \ x \in B_{\epsilon_1}(u) \subset A$.)

Observemos que todo espacio métrico es un espacio de Hausdorff, pues si $x, y \in M$ son dos puntos distintos y $\epsilon = d(x, y) > 0$, entonces tenemos que $B_{\epsilon/2}(x) \cap B_{\epsilon/2}(y) = \varnothing$. ■

Definición 8.5 Si X es un espacio topológico y $x \in X$, una *base de entornos (abiertos)* de x es una familia $\mathcal{B} \subset \mathcal{T}$ de entornos (abiertos) de x tal que si U es un entorno de x existe $B \in \mathcal{B}$ tal que $x \in B \subset U$.

Por ejemplo, ahora es inmediato que, en un espacio métrico M, la familia de las bolas abiertas de centro x es una base de entornos abiertos del punto x.

En general, si en un espacio topológico X tenemos una familia $\{\mathcal{B}_x\}_{x \in X}$ de modo que cada $\mathcal{B}_x$ es una base de entornos abiertos de x, es claro que $\mathcal{B} = \bigcup\limits_{x \in X} \mathcal{B}_x$ es una base de X.

En efecto, si A es abierto y $x \in A$, entonces A es un entorno de x, luego existe un $U \in \mathcal{B}_x \subset \mathcal{B}$ tal que $x \in U \subset A$.

Por ejemplo, teniendo en cuenta que toda bola de centro x en un espacio métrico M contiene una bola de cualquiera de las familias siguientes:

$$\{B_{\epsilon_0}(x) \mid 0 < \epsilon_0 < \epsilon\}, \quad \{B_r(x) \mid r \in \mathbb{Q} \land r > 0\}, \quad \{B_{1/n}(x) \mid n \in \mathbb{N} \land n > 0\},$$

es inmediato que las tres son bases de entornos de x, luego una base de M está formada por todas las bolas abiertas en M cuyo radio sea a) menor que un $\epsilon > 0$ fijo, b) un número racional positivo o c) de la forma $1/n$ con $n \in \mathbb{N}$ no nulo.

Se dice que un espacio topológico X es *metrizable* si existe una distancia $d : X \times X \longrightarrow \mathbb{R}$ que induce la topología de X. Obviamente, todo espacio metrizable es un espacio de Hausdorff.

Por ejemplo, todo espacio discreto es metrizable, ya que la topología discreta en un conjunto X es la topología inducida por la *métrica discreta,* que es la distancia $d : X \times X \longrightarrow \mathbb{R}$ dada por

$$d(x, y) = \begin{cases} 1 & \text{si } x \neq y, \\ 0 & \text{si } x = y. \end{cases}$$

Es inmediato comprobar que es realmente una distancia, y respecto de ella $B_1(x) = \{x\}$, por lo que $\{x\}$ es abierto y, por consiguiente, todo subconjunto de X es abierto, es decir, que la topología inducida por d es la discreta.

Hay que tener presente que una misma topología puede ser inducida por métricas distintas:

Dos distancias en un conjunto X se dicen *equivalentes* si inducen la misma topología. Por ejemplo:

Teorema 8.6 *Toda distancia en un conjunto M es equivalente a una distancia acotada $d : M \times M \longrightarrow [0, 1]$.*

Demostración: Basta observar que si d' es una distancia en M entonces

$$d(x, y) = \text{mín}\{d'(x, 1), 1\}$$

también es una distancia en M y como las bolas de radio < 1 para las distancias d' y d son las mismas, y hemos visto que forman una base para las topologías inducidas por cada una de ellas, concluimos que se trata de la misma topología.

■

Presentamos ahora un concepto similar al de base que también es útil para definir topologías:

Definición 8.7 Una *subbase* de un espacio topológico X es una familia $\mathcal{S} \subset \mathcal{T}$ tal que la familia de las intersecciones finitas de elementos de $\mathcal{S}$ es una base de X.

Aquí hay que entender que, al considerar familias de subconjuntos de X, adoptamos convenio de que $\bigcap \varnothing = X$.

La diferencia respecto de las bases es que una familia de conjuntos no necesita cumplir ninguna condición para ser la subbase de una topología:

Teorema 8.8 *Sea X un conjunto y $\mathcal{S} \subset \mathcal{P}X$ una familia de subconjuntos de X. Entonces existe una única topología en X de la cual $\mathcal{S}$ es subbase, y es la mínima, respecto de la inclusión, para la que los elementos de $\mathcal{S}$ son abiertos.*

Demostración: Sea $\mathcal{B} = \{\bigcap S \mid S \subset \mathcal{S} \land S \land S \text{ finito}\}$ y veamos que cumple las condiciones del teorema 8.4. Como $X = \bigcap \varnothing \in \mathcal{B}$, la primera se cumple trivialmente. Si A, $B \in \mathcal{B}$ y $x \in A \cap B$, entonces $A = \bigcap S$, $B = \bigcap T$, para ciertos conjuntos finitos S, $T \subset \mathcal{S}$. Pero entonces $A \cap B = \bigcap (S \cup T) \in \mathcal{S}$.

Por lo tanto, $\mathcal{B}$ es la base de una topología en X, la cual tiene obviamente a $\mathcal{S}$ por subbase. Si $\mathcal{T}'$ es una topología respecto a la que los elementos de $\mathcal{S}$ son abiertos, entonces también lo son los elementos de $\mathcal{B}$, luego todos los de $\mathcal{T}$, s decir, $\mathcal{T} \subset \mathcal{T}'$, y esto nos da la unicidad. ■

La topología de orden Si X es un conjunto totalmente ordenado, la *topología de orden* en X es la topología que tiene por subbase a los intervalos de la forma

$$]-\infty, b[\qquad \text{y} \qquad]a, +\infty[\,,$$

para a, $b \in X$.

Es obvio que una intersección finita de tales intervalos es un intervalo del mismo tipo (si es que todos ellos son del mismo tipo) o bien $\varnothing$, o bien un intervalo abierto $]a, b[$, luego una base de la topología de orden la forman los intervalos abiertos

$$]-\infty, b[\,, \qquad]a, +\infty[\,, \qquad]a, b[\,.$$

Si X no tiene máximo, todo intervalo de la forma $]a, +\infty[$ es unión de intervalos $]u, v[$, pues, dado $x \in]a, +\infty[$, existe un $v > x$, luego $x \in]a, v[\subset]a, +\infty[$. Similarmente ocurre con los intervalos $]-\infty, b[$ si X no tiene mínimo. Por lo tanto, si X no tiene máximo ni mínimo, una base de X la forman por sí solos los intervalos abiertos $]a, b[$. En cambio, si X tiene máximo M, a éstos hay que añadir los intervalos $]a, M] =]a, +\infty[$, y si X tiene mínimo m, para tener una base hay que añadir también los intervalos $[m, b[=]-\infty, b[$.

En lo sucesivo consideraremos a todo conjunto totalmente ordenado como espacio topológico con la topología de orden. Notemos que son espacios de Hausdorff, pues si $x < y$ son dos elementos de X, o bien existe un $u \in X$ tal que $x < u < y$, entonces $]-\infty, u[$ y $]u, +\infty[$ son entornos disjuntos de x e y, mientras que si no existe tal u, podemos tomar $]-\infty, v[$ y $]u, +\infty[$. ■

Notemos que en $\mathbb{R}$ tenemos definida la topología inducida por la métrica y la inducida por el orden. Vamos a ver que son la misma. Ello es consecuencia de que, claramente, las bolas abiertas en $\mathbb{R}$ son intervalos $B_\epsilon(x) =]x - \epsilon, x + \epsilon[$, luego todo abierto métrico es un abierto para la topología de orden.

Recíprocamente, si $]a, b[$ es un abierto básico en $\mathbb{R}$ para la topología de orden y $x \in]a, b[$, tomamos $\epsilon = \min\{x - a, b - x\}$ y entonces es claro que

$$B_\epsilon(x) =]x - \epsilon, x + \epsilon[\subset]a, b[\,,$$

luego todos los abiertos de la topología de orden son abiertos métricos.

Llamaremos *topología usual* en $\mathbb{R}$ a la topología inducida por su distancia como cuerpo métrico, que coincide, según acabamos de ver, con su topología de orden. En lo sucesivo consideraremos siempre a $\mathbb{R}$ como espacio topológico con esta topología.

También consideraremos a los ordinales como espacios topológicos con la topología de orden.

Topología relativa Si X es un espacio topológico e $Y \subset X$, se llama *topología relativa* de Y respecto de X a la topología $\mathcal{T}_Y = \{A \cap Y \mid A \in \mathcal{T}\}$.

Veamos que es, en efecto, una topología en Y. En primer lugar tenemos que $\varnothing = \varnothing \cap Y \in \mathcal{T}_Y$, $Y = X \cap Y \in \mathcal{T}_Y$.

Si $\mathcal{F} \subset \mathcal{T}_Y$, consideramos la familia de abiertos

$$\mathcal{F}^* = \{U \in \mathcal{T} \mid U \cap Y \in \mathcal{F}\}$$

y llamamos $A = \bigcup \mathcal{F}^* \in \mathcal{T}$. Es fácil ver que $A \cap Y = \bigcup \mathcal{F}$, con lo que $\bigcup F \in \mathcal{T}_Y$.

Por último, dados $U, V \in \mathcal{T}_Y$, existen $A, B \in \mathcal{T}$ tales que $U = A \cap Y$, $V = B \cap Y$, luego $U \cap V = (A \cap B) \cap Y \in \mathcal{T}_Y$.

Observemos que si $\mathcal{B}$ es una base de X y $\mathcal{S}$ es una subbase de X, entonces

$$\mathcal{B}_Y = \{B \cap Y \mid B \in \mathcal{B}\}, \qquad \mathcal{S}_Y = \{S \cap Y \mid S \in \mathcal{S}\}$$

son, respectivamente, una base y una subbase de la topología relativa.

En efecto, un abierto de la topología relativa es de la forma $A \cap Y$, donde $A = \bigcup \mathcal{F}$, con $\mathcal{F} \subset \mathcal{B}$, luego $\mathcal{F}^* = \{U \cap Y \mid U \in \mathcal{F}\} \subset \mathcal{B}_Y$ y $A \cap Y = \bigcup \mathcal{F}^*$. Esto prueba que $\mathcal{B}_Y$ es base de la topología relativa.

Similarmente, si $\mathcal{B}$ es la base inducida por $\mathcal{S}$, es fácil ver que $\mathcal{B}_Y$ (que ya hemos probado que es una base de la topología relativa) es la base inducida por $\mathcal{S}_Y$, luego $\mathcal{S}_Y$ es subbase de la topología relativa.

En lo sucesivo consideraremos a los subconjuntos de los espacios topológicos como espacios topológicos con la topología relativa. Esto es coherente, pues es fácil ver que si X es un espacio topológico y tenemos subconjuntos $Z \subset Y \subset X$, entonces la topología relativa de Z respecto de X es la misma que la relativa respecto de Y cuando en Y consideramos la topología relativa respecto de X.

A su vez, esto es coherente con el criterio de considerar a los espacios métricos con la topología inducida por la distancia, pues si M es un espacio métrico con una distancia $d : M \times M \longrightarrow \mathbb{R}$ y $N \subset M$, entonces la topología inducida en N por la distancia $d|_{N\times N} : N \times N \longrightarrow \mathbb{R}$ es la misma que la topología relativa respecto de la topología inducida en M por la distancia d.

En efecto, es fácil ver que si $x \in N$ y $\epsilon > 0$, entonces $B^N_\epsilon(x) = B^M_\epsilon(x) \cap N$, luego los abiertos básicos de la topología métrica en N son abiertos para la topología relativa, luego todo abierto métrico es abierto para la topología relativa.

Recíprocamente, un abierto para la topología relativa es de la forma $A \cap N$, con A abierto en M, luego, para todo $x \in A \cap N$, existe un $\epsilon > 0$ tal que

$B_\epsilon^M(x) \subset A$, luego $B_\epsilon^N(x) = B_\epsilon^M(x) \cap N \subset A \cap N$, luego $A \cap N$ es abierto métrico.

En cambio, si X es un conjunto totalmente ordenado y $Y \subset X$, entonces la topología inducida en Y por la restricción del orden de X no coincide necesariamente con la topología relativa de Y respecto de la topología de orden de X.

Ejemplo Sea $X = \mathbb{R}$ con la topología usual, y sea

$$Y = \{-1\} \cup \{1/n \mid n \in \mathbb{N} \wedge n \neq 0\}.$$

Si consideramos a Y con la topología relativa, vemos que $\{-1\} = Y \cap \left]-2, 0\right[$ es abierto. Pero no es abierto para la topología de orden de Y, pues, siendo -1 el mínimo de Y, no pertenece a ningún intervalo de la forma $]a, b[$ o $]a, +\infty[$, luego tendría que existir un $b \in Y$ tal que $-1 \in \left]-\infty, b\right[\subset \{-1\}$, pero no existe tal b, pues ciertamente $b = -1$ no cumple esto y un intervalo $\left]-\infty, 1/n\right[$ no está contenido en $\{-1\}$. ■

En vista de esto, cuando consideremos subconjuntos de conjuntos ordenados los consideraremos como espacios topológicos con la topología relativa, y no con la topología de orden.

En cualquier caso, se cumple lo siguiente:

Teorema 8.9 *Si X es un conjunto totalmente ordenado y $Y \subset X$, entonces todo abierto de Y para la topología de orden es abierto para la topología relativa respecto de la topología de orden de X. Si se cumple una de las condiciones siguientes:*

a) Y es un intervalo en X,

b) $\bigwedge uv \in X(u < v \to \bigvee y \in Y\ u < y < v)$,

entonces ambas topologías coinciden.

Demostración: Es claro que si $a \in Y$ entonces $]a, +\infty[^Y =]a, \infty[^X \cap Y$, y lo mismo vale para intervalos $]-\infty, b[$, con $b \in Y$, luego todo abierto subbásico para la topología de orden de Y es abierto para la topología relativa.

Respecto a la segunda parte, es claro que si Y es un intervalo en X, entonces $Y \cap \left]a, +\infty\right[$ puede ser $\varnothing$, Y o bien $]a, +\infty[^Y$, pero en cualquier caso es abierto para la topología de orden, e igualmente sucede con los intervalos $]-\infty, b[$. Por lo tanto, los abiertos subbásicos de la topología relativa son abiertos para la topología de orden, y esto implica que lo mismo vale para todos los abiertos.

Por otra parte, si se cumple la segunda condición, entonces $Y \cap \left]a, +\infty\right[$ es igualmente abierto para la topología de orden, pues si $u \in Y \cap]a, +\infty[$, entonces $a < u$, luego existe un $y \in Y$ tal que $a < y < u$, luego

$$u \in \left]y, +\infty\right[^Y \subset Y \cap \left]a, +\infty\right[.$$

Así pues, de nuevo $Y \cap]a, +\infty[$ es abierto para la topología de orden y lo mismo vale para los intervalos $]-\infty, b[$, con lo que concluimos igualmente que la topología relativa es la topología del orden. ■

Así, consideraremos como "topología usual" en los subconjuntos de $\mathbb{R}$ a la topología relativa, y ahora sabemos que coincide con la topología de orden en los intervalos y también en los conjuntos densos, como $\mathbb{Q}$.

También podemos afirmar que la topología relativa de un ordinal respecto de otro mayor es la topología de orden.

Por último, todo subespacio de un espacio de Hausdorff es trivialmente un espacio de Hausdorff (con la topología relativa).

La topología producto Consideremos una familia de conjuntos $\{X_i\}_{i\in I}$, que nos permite formar el producto cartesiano $\prod\limits_{i\in I} X_i$. Para cada $i \in I$ tenemos la proyección $p_i : \prod\limits_{i\in I} X_i \longrightarrow X_i$.

Si cada X_i es un espacio topológico, definimos la *topología producto* en el producto cartesiano como la que tiene por subbase a los conjuntos de la forma $p_i^{-1}[A]$, donde A es un abierto en X_i.

Teorema 8.10 *Sea $\{X_i\}_{i\in I}$ una familia de espacios topológicos y sea $\{\mathcal{B}_i\}_{i\in I}$ una familia tal que $\mathcal{B}_i$ sea una base de X_i. Entonces una base de la topología producto la forman los productos $\prod\limits_{i\in I} B_i$ tales que existe $I_0 \subset I$ finito de modo que $\bigwedge i \in I_0\ B_i \in \mathcal{B}_i$ y $\bigwedge i \in I \setminus I_0\ B_i = X_i$.*

Demostración: Sea $\mathcal{T}$ la topología que tiene por subbase los conjuntos de la forma $p_i^{-1}[B]$, donde $B \in \mathcal{B}_i$. Estos abiertos son abiertos para la topología producto, luego todo abierto de $\mathcal{T}$ es abierto para la topología producto.

Recíprocamente, un abierto subbásico para la topología producto es de la forma $p_i^{-1}[A]$, donde A es abierto en X_i, pero entonces A se puede expresar como unión de conjuntos de $\mathcal{B}_i$, luego $p_i^{-1}[A]$ es unión de abiertos subbásicos de $\mathcal{T}$, luego todo abierto de la topología producto es abierto de $\mathcal{T}$. En definitiva, $\mathcal{T}$ es la topología producto.

Llamemos $\mathcal{B}$ a la familia de los conjuntos descritos en el enunciado. Todo elemento de $\mathcal{B}$ es de la forma $\bigcap\limits_{i\in I_0} p_i^{-1}[B_i]$, luego es un abierto básico de $\mathcal{T}$ (luego de la topología producto).

Si probamos que $\mathcal{B}$ es base de una topología, entonces todos los abiertos de esta topología serán abiertos para la topología producto, y como cada abierto subbásico de $\mathcal{T}$ está en $\mathcal{B}$, todo abierto de la topología producto será abierto para la topología de $\mathcal{B}$, y quedará demostrado que $\mathcal{B}$ es una base de la topología producto.

Ahora bien, la primera propiedad de 8.4 es inmediata y, si tenemos que $x \in U \cap V$, donde $U = \bigcap\limits_{i\in I_0} p_i^{-1}[B_i]$ y $V = \bigcap\limits_{i\in I_1} p_i^{-1}[B_i']$, podemos cambiar I_0 e $I^* = I_1$ por $I_0 \cup I_1$ si definimos $B_i = X_i$ para $i \in I_1 \setminus I_0$ y $B_i' = X_i$ para

$i \in I_0 \setminus I_1$. Entonces

$$U \cap V = \bigcap_{i \in I^*} p_i^{-1}[B_i] \cap \bigcap_{i \in I*} p_i^{-1}[B_i'] = \bigcap_{i \in I^*} (p_i^{-1}[B_i] \cap p_i^{-1}[B_i']) = \bigcap_{i \in I^*} p_i^{-1}[B_i \cap B_i']$$

y, como $x \in U \cap V$, tenemos que $p_i(x) \in B_i \cap B_i'$, luego existe $B_i'' \in \mathcal{B}_i$ tal que $p_i(x) \in B_i'' \subset B_i \cap B_i'$, luego

$$x \in \bigcap_{i \in I^*} p_i^{-1}[B_i''] \subset U \cap V.$$

Esto prueba que $\mathcal{B}$ es una base, y que por tanto lo es de la topología producto. ■

La situación es conceptualmente más simple si consideramos productos finitos, pues entonces el teorema anterior afirma que una base de un producto $X_1 \times \cdots \times X_n$ está formada por los conjuntos de la forma $B_1 \times \cdots \times B_n$, donde cada B_i está en una base prefijada de X_i. ■

Normalmente consideraremos los productos de espacios topológicos como espacios topológicos con la topología producto. Al tomar subespacios de productos tenemos el resultado siguiente de coherencia:

Teorema 8.11 *Sea $\{X_i\}_{i \in I}$ una familia de espacios topológicos y sea $\{Y_i\}_{i \in I}$ una familia de conjuntos, de modo que cada $Y_i \subset X_i$. Entonces $Y = \prod_{i \in I} Y_i$ es un subconjunto de $X = \prod_{i \in I} X_i$. Si consideramos a cada Y_i como espacio topológico con la topología relativa, entonces la topología producto de Y es la misma que la topología relativa respecto de X.*

Demostración: Un abierto básico para la topología relativa de Y es

$$\prod_{i \in I} Y_i \cap \prod_{i \in I} A_i = \prod_{i \in I} (Y_i \cap A_i),$$

donde cada A_i es abierto en X_i y todos salvo una cantidad finita coinciden con X_i, pero es claro que el miembro derecho es un abierto básico para la topología producto de Y, y viceversa. Por lo tanto, ambas topologías coinciden. ■

Llamaremos *topología usual* de $\mathbb{R}^n$ a la topología producto, cuando consideramos en $\mathbb{R}$ la topología usual.

Teorema 8.12 *Todo producto de espacios topológicos de Hausdorff es un espacio de Hausdorff.*

Demostración: Sea $X = \prod_{i \in I} X_i$ un producto de espacios topológicos de Hausdorff y sean $x, y \in X$ dos puntos distintos. Entonces existe un $i \in I$ tal que $x_i \neq y_i$, luego existen abiertos disjuntos U, $V \in X_i$ tales que $x_i \in U$, $y_i \in V$, y entonces $p_i^{-1}[U]$ y $p_i^{-1}[V]$ son abiertos disjuntos en X que separan a los puntos dados. ■

Si $\{M_i\}_{i=1}^n$ es una familia de espacios topológicos metrizables, entonces el producto $M = \prod\limits_{i=1}^n M_i$ es metrizable, es decir, existe una distancia en el producto que induce la topología producto. De hecho, hay varias opciones. Por ejemplo, podemos considerar $d : M \times M \longrightarrow \mathbb{R}$ dada por

$$d(x, y) = \sum_{i=1}^n d(x_i, y_i).$$

Se comprueba sin dificultad que d es una distancia en M. Vamos a ver que induce la topología producto. Un abierto básico para la topología producto es de la forma $B = B_{\epsilon_1}(x_1) \times \cdots \times B_{\epsilon_n}(x_n)$. Veamos que B es abierto para la distancia d. Para ello tomamos $y \in B$ y observamos que $B_\epsilon(y) \subset B$, donde $\epsilon = \min\{\epsilon_i - d(y_i, x_i) \mid 1 \leq i \leq n\}$, pues si $z \in B_\epsilon(y)$, entonces

$$d(z_i, x_i) \leq d(z_i, y_i) + d(y_i, x_i) \leq d(z, y) + d(y_i, x_i) < \epsilon + d(y_i, x_i) \leq \epsilon_i,$$

luego $z_i \in B_{\epsilon_i}(x_i)$, luego $z \in B$. Así pues, todo abierto para la topología producto es abierto para d.

Recíprocamente, un abierto básico para d es $B_\epsilon(x)$, y tenemos que probar que es abierto para la topología producto. Para ello tomamos $y \in B_\epsilon(x)$ y probamos que $y \in B_\delta(y_1) \times \cdots \times B_\delta(y_n) \subset B_\epsilon(x)$, donde $\delta = (\epsilon - d(x, y))/n$. En efecto, si z pertenece al producto de bolas, entonces

$$d(z, x) \leq d(z, y) + d(y, x) = \sum_{i=1}^n d(z_i, y_i) + d(y, x) < n\delta + d(y, x) = \epsilon.$$

luego $y \in B_\epsilon(x)$. Con esto queda probado que la topología métrica es la topología producto.

Una mínima variante del argumento anterior prueba que lo mismo vale para la distancia dada por

$$d'(x, y) = \max_i d(x_i, y_i).$$

Por lo tanto, d y d' son distancias equivalentes en el producto.

Este resultado se puede generalizar ligeramente:

Teorema 8.13 *Si $\{M_n\}_{n\in\omega}$ es una familia numerable de espacios métricos, entonces el producto $M = \prod\limits_{i\in\omega} M_i$ admite una distancia que induce la topología producto.*

Demostración: Por el teorema 8.6 podemos tomar una distancia d_i en M_i que tome valores en $[0, 1]$. Definimos $d : M \times M \longrightarrow M$ mediante

$$d(x, y) = \sum_{i\in\omega} \frac{d_i(x_i, y_i)}{2^i} \leq \sum_{i\in\omega} \frac{1}{2^i} = 2.$$

La prueba de que d es una distancia no ofrece dificultad. Veamos que induce la topología producto. Consideremos un abierto básico para la topología producto, que es de la forma

$$B = \bigcap_{i<n} p_i^{-1}[B_{\epsilon_i}(x_i)].$$

Para probar que es abierto para d tomamos $y \in B$ y vamos a ver que $B_\epsilon(y) \subset B$, donde $\epsilon = \text{mín}\{\epsilon_i - d(y_i, x_i) \mid i < n\}/2^n$. En efecto, si $z \in B_\epsilon(y)$, entonces, para $i < n$,

$$\frac{d(z_i, y_i)}{2^n} \leq \frac{d(z_i, y_i)}{2^i} \leq d(z, y) < \epsilon < \frac{\epsilon_i - d(y_i, x_i)}{2^n}$$

luego

$$d(z_i, x_i) \leq d(z_i, y_i) + d(y_i, x_i) < \epsilon_i,$$

luego $z_i \in B_{\epsilon_i}(x_i)$, luego $z \in B$. Por lo tanto, los abiertos para la topología producto son abiertos para d. Recíprocamente, consideramos un abierto básico para d, es decir, $B_\epsilon(x)$ y veamos que es abierto para la topología producto. Para ello tomamos $y \in B_\epsilon(x)$ y vamos a encontrar un abierto básico B para la topología producto tal que $y \in B \subset B_\epsilon(x)$.

Tomamos $n \in \omega$ tal que

$$\sum_{i \geq n} \frac{1}{2^i} = \frac{1}{2^{n-1}} < \frac{\epsilon - d(y, x)}{2}$$

y sea $\delta = (\epsilon - d(y, x))/(2n)$, $B = \bigcap_{i<n} p_i^{-1}[B_\delta(y_i)]$. Así, si $z \in B$, tenemos que

$$d(z, x) \leq d(z, y) + d(y, x) \leq \sum_{i \in \omega} \frac{d_i(z_i, y_i)}{2^i} + d(y, x)$$

$$= \sum_{i<n} \frac{d_i(z_i, y_i)}{2^i} + \sum_{i \geq n} \frac{d_i(z_i, y_i)}{2^i} + d(y, x) < n\delta + \sum_{i \geq n} \frac{1}{2^i} + d(y, x)$$

$$\leq \frac{\epsilon - d(y, x)}{2} + \frac{\epsilon - d(y, x)}{2} + d(y, x) = \epsilon.$$

Por lo tanto $z \in B_\epsilon(x)$, luego $B \subset B_\epsilon(x)$ y la bola es abierta para la topología producto. ■

8.2 Algunos conceptos topológicos.

Veamos ahora cómo el concepto de espacio topológico permite introducir numerosos conceptos de gran utilidad para describir su estructura. Empezaremos mostrando que la noción de convergencia de sucesiones que ya hemos manejado en el capítulo anterior en el contexto de espacios métricos es en realidad topológica.

Definición 8.14 Diremos que una sucesión $\{x_n\}_{n\in\omega}$ en un espacio topológico X *converge* a un *límite* $l \in X$ si para todo entorno U de l

$$\bigvee m \in \omega \bigwedge n \geq m \; x_n \in U,$$

es decir, si la sucesión entra en todo entorno de l a partir de un término y ya no vuelve a salir.

Notemos que en un espacio trivial, el único entorno de cualquier punto es todo el espacio, que trivialmente contiene a cualquier sucesión, luego en un espacio trivial toda sucesión converge a cualquier punto. En cambio, en un espacio de Hausdorff, si una sucesión tiene límite, éste es único. En efecto, si $\{x_n\}_{n\in\omega}$ convergiera a dos límites $l \neq l'$, entonces existirían abiertos disjuntos U, V tales que $l \in U$, $l' \in V$, pero entonces debería haber un $m \in \omega$ tal que si $n \geq m$, entonces $x_n \in U \cap V$, contradicción.

Por ello, si una sucesión $\{x_n\}_{n\in\omega}$ converge en un espacio de Hausdorff, representaremos su límite como $\lim\limits_n x_n \in X$.

Es inmediato comprobar que para que se cumpla la definición de límite basta considerar los entornos de l pertenecientes a una base de entornos prefijada. Por ejemplo, en un espacio métrico basta considerar las bolas abiertas $B_\epsilon(l)$, pero entonces la condición $x_n \in B_\epsilon(l)$ equivale a $d(x_n, l) < \epsilon$, de donde se sigue que la noción de convergencia que acabamos de introducir coincide con la definida en 7.11.

Es inmediato comprobar que si tenemos espacios $Y \subset X$, la convergencia de una sucesión $\{x_n\}_{n\in\omega}$ contenida en Y a un límite $y \in Y$ se cumple respecto de la topología de X si y sólo si se cumple respecto de la topología de Y. (Aunque, naturalmente, una sucesión en Y puede converger en X a un límite que no esté en Y. Para productos tenemos el teorema siguiente:

Teorema 8.15 *Sea $X = \prod\limits_{i\in I} X_i$ un producto de espacios topológicos. Una sucesión $\{x_n\}_{n\in\omega}$ en X converge a un punto $x \in X$ si y sólo si cada una de las sucesiones $\{x_{ni}\}_{n\in\omega}$ converge a x_i.*

DEMOSTRACIÓN: Si converge la sucesión en el producto, fijado $i \in I$ y un entorno U de x_i, tenemos que $p_i^{-1}[U]$ es un entorno de x, luego existe un $m \in \omega$ tal que para $n \geq m$ se cumple $x_n \in p_i^{-1}[U]$, luego $x_{ni} \in U$, luego $\{x_{ni}\}_{n\in\omega}$ converge a x_i.

Recíprocamente, si todas las sucesiones de coordenadas convergen, dado un entorno U de x, podemos suponer que es un abierto básico

$$U = \prod_{i\in I} A_i,$$

donde cada A_i es abierto en X_i y existe $I_0 \subset I$ finito tal que si $i \in I \setminus I_0$ entonces $A_i = X_i$. Para cada $i \in I_0$, tenemos que A_i es un entorno de x_i, luego existe un m_i tal que si $n \geq m_i$, entonces $x_{ni} \in A_i$. Tomamos $m = \max\{m_i \mid i \in I_0\}$, con lo que si $n \geq m$, se cumple $x_{ni} \in A_i$ para todo $i \in I_0$, y trivialmente si $i \in I \setminus I_0$, luego $x_n \in U$, y esto prueba que la sucesión converge a x. ■

Un subconjunto C de un espacio topológico X es *cerrado* si y sólo si $X \setminus C$ es abierto. Obviamente, los cerrados tienen las propiedades análogas a las de los abiertos cambiando uniones por intersecciones:

Teorema 8.16 *Si X es un espacio topológico, se cumple:*

a) $\varnothing$, X son cerrados.

b) Si $\{A_i\}_{i\in I}$ es una familia de elementos de cerrados en X, entonces $\bigcap\limits_{i\in I} A_i$ es cerrado.

c) Si A, B son cerrados, entonces $A \cup B$ es cerrado.

Observemos que si $Y \subset X$, los cerrados de Y son los conjuntos de la forma $C \cap Y$, donde C es cerrado en X. En efecto, en principio son los conjuntos de la forma $Y \setminus (A \cap Y)$, donde A es abierto en X, pero obviamente

$$Y \setminus (A \cap Y) = Y \cap (X \setminus A).$$

Hay una caracterización útil de los espacios de Hausdorff:

Teorema 8.17 *Un espacio topológico X es de Hausdorff si y sólo si la diagonal $\Delta = \{(x, x) \mid x \in X\}$ es cerrada en $X \times X$.*

Demostración: Si X es de Hausdorff y $(x, y) \in (X \times X) \setminus \Delta$, entonces $x \neq y$, luego x e y pueden ser separados por abiertos disjuntos U y V. Entonces $(x, y) \in U \times V \subset (X \times X) \setminus \Delta$, luego el complemento de la diagonal es entorno de todos sus puntos, es decir, es abierto, y la diagonal es cerrada.

Recíprocamente, si la diagonal es cerrada, dados dos puntos distintos x, $y \in X$, entonces $(x, y) \in (X \times X) \setminus \Delta$, que es un abierto, luego existe un abierto básico $(x, y) \in U \times V \subset (X \times X) \setminus \Delta$, donde U y V son abiertos, necesariamente disjuntos, con lo que separan a x e y. ■

Las propiedades de los abiertos y los cerrados nos permiten definir dos conceptos asociados:

Definición 8.18 Si X es un espacio topológico y $A \subset X$, definimos el *interior* $\mathring{A}$ y la *clausura* $\overline{A}$ de A como los conjuntos

$$\mathring{A} = \bigcup\{U \mid U \subset A \land U \text{ abierto}\}, \qquad \overline{A} = \bigcap\{C \mid A \subset C \land C \text{ cerrado}\}.$$

Es obvio que $\mathring{A}$ es el mayor abierto contenido en A (respecto de la inclusión) y que $\overline{C}$ es el menor cerrado que contiene a A. En particular $\mathring{A} \subset A \subset \overline{A}$. Además, A es abierto si y sólo si $A = \mathring{A}$ y A es cerrado si y sólo si $A = \overline{A}$.

Cuando sea más conveniente por razones tipográficas representaremos el interior y la clausura mediante $\operatorname{int} A$ y $\operatorname{cl} A$, respectivamente.

Los puntos de $\mathring{A}$ se llaman *puntos interiores* de A, mientras que los de $\overline{A}$ se llaman *puntos adherentes* de A.

El interior y la clausura verifican una relación fundamental:

Teorema 8.19 *Si A es un subconjunto de un espacio topológico X, entonces*

$$\operatorname{int}(X \setminus A) = X \setminus \operatorname{cl} A, \qquad \operatorname{cl}(X \setminus A) = X \setminus \operatorname{int} A.$$

Demostración: Como $A \subset \operatorname{cl} A$, también $X \setminus \operatorname{cl} A \subset X \setminus A$, y el término de la izquierda es abierto, luego $X \setminus \operatorname{cl} A \subset \operatorname{int}(X \setminus A)$.

Por otra parte, $\operatorname{int}(X \setminus A) \subset X \setminus A$, luego $A \subset X \setminus \operatorname{int}(X \setminus A)$, y el término de la derecha es cerrado, luego $\operatorname{cl} A \subset X \setminus \operatorname{int}(X \setminus A)$, luego $\operatorname{int}(X \setminus A) \subset X \setminus \operatorname{cl} A$.

La otra igualdad se prueba análogamente. ■

La interpretación de los puntos interiores es muy simple: un punto x es interior a A si y sólo si A es un entorno de x. Los puntos adherentes también tienen su interpretación:

Teorema 8.20 *Si A es un subconjunto de un espacio topológico X, entonces un punto $x \in X$ es adherente a A si y sólo si todo entorno de x corta a A.*

Demostración: Supongamos que x es adherente a A. Sea U un entorno de x. Existe un abierto G tal que $x \in G \subset U$. Basta probar que $G \cap A \neq \varnothing$. Ahora bien, en caso contrario $X \setminus G$ sería un cerrado que contiene a A, luego $\overline{A} \subset X \setminus G$, mientras que $x \in \overline{A} \cap G$.

Recíprocamente, si x tiene esta propiedad entonces $x \in \overline{A}$, ya que de lo contrario $X \setminus \overline{A}$ sería un entorno de x que no corta a A. ■

Por lo tanto, podemos decir que los puntos interiores de A son los puntos que tienen todos los puntos de su alrededor en A, mientras que los puntos adherentes de A son los puntos que tienen en A al menos parte de los puntos de su alrededor. En este sentido, los puntos de $\overline{A} \setminus A$ son puntos que, sin estar en A, están "pegados a" o "en contacto con" A.

Es espacios métricos tenemos una caracterización muy descriptiva de los puntos adherentes. Necesitamos la definición siguiente:

Definición 8.21 *Sea M un espacio métrico, sea $\varnothing \neq A \subset M$ y sea $x \in M$, definimos la distancia de x a A como*

$$d(x, A) = \operatorname{ínf}\{d(x, y) \mid y \in A\}.$$

Teorema 8.22 *Sea X un espacio métrico y $A \subset M$ un conjunto no vacío. Entonces $\overline{A} = \{x \in M \mid d(x, A) = 0\}$.*

Demostración: Si $d(x, A) = 0$, para probar que es adherente basta ver que toda bola abierta de centro x corta a A. Dado $\epsilon > 0$ tenemos que $d(x, A) < \epsilon$, lo que significa que existe un $y \in A$ tal que $d(x, y) < \epsilon$, es decir, $y \in B_\epsilon(x) \cap A$. El recíproco se prueba igualmente. ■

Conviene distinguir los puntos adherentes que no son interiores:

Definición 8.23 Si A es un subconjunto de un espacio topológico X, se llama *frontera* de A al conjunto

$$\partial A = \overline{A} \cap \overline{X \setminus A}.$$

Así, un punto está en la frontera de A si una parte de sus puntos de alrededor están en A y otra parte está en $X \setminus A$. Por el teorema anterior:

$$\partial A = \overline{A} \cap (X \setminus \mathring{A}) = \overline{A} \setminus \mathring{A},$$

de modo que los puntos de la frontera de A son los puntos adherentes que no son interiores.

De esta última expresión para la frontera resulta inmediatamente que un conjunto A es abierto si y sólo si $A \cap \partial A = \varnothing$, y es cerrado si y sólo si $\partial A \subset A$, es decir, los abiertos son los conjuntos que no contienen a "su borde" y los cerrados son los conjuntos que contienen a todo "su borde".

Observemos que la inclusión $A \subset \overline{A}$ se puede interpretar como que todo punto $x \in A$ tiene trivialmente algún punto de su alrededor en A, a saber, el propio x, pero a veces es relevante que un punto tenga puntos de alrededor en A sin contarlo a él mismo. Esto nos lleva al concepto de punto de acumulación:

Si A es un subconjunto de un espacio topológico X, un punto $x \in X$ es un *punto de acumulación* de A si todo entorno U de x cumple $(U \setminus \{x\}) \cap A \neq \varnothing$. El conjunto de todos los puntos de acumulación de A se llama *conjunto derivado* de A, y se representa por A'.

Los puntos de $A \setminus A'$ se llaman *puntos aislados* de A.

En otras palabras, $x \in A$ es un punto aislado si tiene un entorno U tal que $U \cap A = \{x\}$ o, lo que es lo mismo, si es abierto en la topología relativa de A.

Un punto aislado en A no tiene ningún punto de su alrededor en A salvo él mismo. Por eso está trivialmente en $\overline{A}$, pero no está en A'. Obviamente $A' \subset \overline{A}$.

También es inmediato que un espacio topológico es discreto si y sólo si todos sus puntos son aislados.

Para completar el vocabulario topológico básico añadimos una última definición:

Un subconjunto D de un espacio topológico X es *denso* si $\overline{D} = X$.

Esto significa que todo punto de X tiene su alrededor puntos de D. Más concretamente, que todo entorno de cualquier punto de X corta a D, pero esto equivale claramente a que todo abierto no vacío de X corte a D, y la condición se puede restringir a todo abierto básico no vacío.

En particular, un subconjunto D de un espacio métrico M es denso si y sólo si toda bola $B_\epsilon(x)$ corta a D, lo cual equivale a que para todo $x \in M$ y todo $\epsilon > 0$ exista un $d \in D$ tal que $d(x, d) < \epsilon$, con lo que la definición de conjunto denso que acabamos de dar es equivalente, en el caso de espacios métricos, a la que dimos en en 7.11. También es claro que sobre precontinuos equivale a la dada en 7.36.

De todas estas definiciones se siguen muchas propiedades inmediatas. Por ejemplo, es claro que si $A \subset B$ entonces $\mathring{A} \subset \mathring{B}$ y $\overline{A} \subset \overline{B}$. (Tenemos que $\mathring{A} \subset A \subset B$ y, como $\mathring{A}$ es un abierto contenido en B, se cumple $\mathring{A} \subset \mathring{B}$.)

También es fácil ver que $\operatorname{int}(A \cap B) = \operatorname{int} A \cap \operatorname{int} B$, y que $\overline{A \cup B} = \overline{A} \cup \overline{B}$, así como que si $A \subset B \subset X$, entonces $\overline{A}^B = \overline{A}^X \cap B$ (pero la igualdad análoga con interiores es falsa en general).

En un espacio de Hausdorff, los conjuntos finitos son cerrados. En efecto, basta probar que los puntos son cerrados, pero si x, y son dos puntos distintos, hay abiertos disjuntos tales que $x \in U$, $y \in V$, luego $\{x\} \subset X \setminus V$, luego $\overline{\{x\}} \subset X \setminus V$, luego $y \notin \overline{\{x\}}$, y esto vale para todo $y \neq x$, luego $\overline{\{x\}} = \{x\}$.

Para productos tenemos:

Teorema 8.24 *Sea $\{X_i\}_{i \in I}$ una familia de espacios topológicos y sea $\{Y_i\}_{i \in I}$ una familia tal que cada $Y_i \subset X_i$. Entonces*

$$\overline{\prod_{i \in I} Y_i} = \prod_{i \in I} \overline{Y_i}.$$

En particular, el producto de cerrados es cerrado.

Demostración: Si llamamos X al espacio producto, se cumple que

$$X \setminus p_i^{-1}[\overline{Y}_i] = p_i^{-1}[X_i \setminus \overline{Y}_i]$$

de donde $p_i^{-1}[\overline{Y_i}]$ es cerrado, y $\prod\limits_{i \in I} \overline{Y_i} = \bigcap\limits_{i \in I} p_i^{-1}[\overline{Y}_i]$ es cerrado por ser intersección de cerrados. Esto implica que $\overline{\prod\limits_{i \in I} Y_i} \subset \prod\limits_{i \in I} \overline{Y_i}$.

Recíprocamente, si $y \in \prod\limits_{i \in I} \overline{Y_i}$, vamos a probar que está en la clausura del producto viendo que todo entorno de y corta al producto. Podemos tomar como entorno un abierto básico $U = \prod\limits_{i \in I} A_i$, donde cada A_i es abierto en X_i y existe $I_0 \subset I$ finito tal que si $i \in I \setminus I_0$ entonces $A_i = X_i$. Para cada $i \in I_0$ tenemos que $y_i \in A_i \cap \overline{Y_i}$, luego existe $y_i' \in A_i \cap Y_i$. Definimos

$$y_i' = \begin{cases} y_i' & \text{si } i \in I_0, \\ y_i & \text{si } i \in I \setminus I_0, \end{cases}$$

Así $y' \in U \cap \prod\limits_{i \in I} Y_i \neq \varnothing$, luego y es un punto adherente del producto y tenemos la igualdad requerida. ∎

Caracterizaciones con sucesiones Todos los conceptos que hemos introducido en esta sección admiten caracterizaciones en términos de sucesiones en una clase de espacios topológicos que incluye a todos los espacios métricos:

Definición 8.25 Un espacio topológico cumple el *primer axioma de numerabilidad* (1AN) si cada uno de sus puntos tiene una base numerable de entornos.

Notemos que si $\{U_n\}_{n\in\omega}$ es una base de entornos de x, entonces $\{\mathring{U}_n\}_{n\in\omega}$ es una base de entornos abiertos de x y, si llamamos $V_m = \bigcap\limits_{n\leq m} \mathring{U}_n$, entonces $\{V_m\}_{m\in\omega}$ es una base numerable de entornos abiertos de x con la propiedad adicional de que $\bigwedge mn \in \omega\ (m \leq n \rightarrow V_n \subset V_m)$. A las bases en estas condiciones las llamaremos *bases de entornos decrecientes.*

Por ejemplo, todo espacio métrico M cumple 1AN, pues cada punto $x \in M$ tiene por base decreciente de entornos abiertos a la familia de bolas abiertas $\{B_{1/n}(x)\}_{n=1}^{\infty}$.

Teorema 8.26 (AEN) *Sea X un espacio que cumpla* 1AN*, sea $A \subset X$ y sea $x \in X$. Entonces:*

a) x es un punto interior de A si y sólo si para toda sucesión $\{x_n\}_{n\in\omega}$ que converja a x se cumple $\bigvee m \in \omega \bigwedge n \geq m\ x_n \in A$.

b) x es un punto adherente de A si y sólo si existe una sucesión $\{x_n\}_{n\in\omega}$ convergente a x contenida en A.

c) x es un punto de acumulación de A si y sólo si existe una sucesión $\{x_n\}_{n\in\omega}$ convergente a x contenida en $A \setminus \{x\}$.

d) A es denso si y sólo si para todo $x \in X$ existe una sucesión $\{x_n\}_{n\in\omega}$ convergente a x contenida en A.

DEMOSTRACIÓN: b) Sea $\{U_n\}_{n\in\omega}$ una base decreciente de entornos abiertos de x. Si $x \in \overline{A}$, entonces $U_n \cap A \neq \varnothing$, luego podemos elegir un punto $x_n \in U_n \cap A$. Es inmediato que la sucesión $\{x_n\}_{n\in\omega}$ está contenida en A y converge a x.

El recíproco es trivial: si existe la sucesión y U es un entorno de x, entonces existe un n tal que $x_n \in U \cap A \neq \varnothing$, luego x es adherente a A.

a) Si x no es un punto interior de A, entonces $x \in X \setminus \mathring{A} = \overline{X \setminus A}$, luego por b) existe una sucesión en $X \setminus A$ que converge a x. El recíproco es consecuencia inmediata de la definición de convergencia.

La prueba de c) es análoga a la de b) y el apartado d) es un caso particular de b). ■

Vemos, pues, que en este contexto un conjunto A es cerrado cuando es imposible que el límite de una sucesión contenida en A se salga de A.

La topología de orden en los ordinales Consideremos un ordinal $\alpha > 0$ como espacio topológico con la topología de orden. Observamos en primer lugar que los puntos aislados de α son el 0 y los ordinales sucesores.

En efecto, por una parte tenemos que $\{0\} =]-\infty, 1[$ (o bien $\{0\} = \alpha$, si es que $\alpha = 1$) y, si $\beta+1 < \alpha$, entonces $\{\beta+1\} =]\beta, \beta+2[$ (o bien $\{\beta+1\} =]\beta, +\infty[$ si es que $\beta + 2 = \alpha$). Por lo tanto, 0 y los ordinales sucesores en α son puntos aislados.

En cuanto a los ordinales límite, veamos que si $\lambda \in \alpha$, entonces una base de entornos abiertos de λ es $\{]\delta, \lambda]\}_{\delta<\lambda}$. Es claro entonces que λ es un punto de acumulación de α, pues todos sus entornos contienen ordinales $< \lambda$.

Ante todo, $]\delta, \lambda]$ es abierto, pues coincide con $]\delta, \lambda + 1[$ si $\lambda+1 < \alpha$ o bien con $]\delta, +\infty[$ en caso contrario. Si $U \subset \alpha$ es un entorno de λ, entonces existen δ, β tales que $\lambda \in]u, v[\subset U$, donde u, v son ordinales de α o bien $\pm\infty$. Ahora bien, si $u = -\infty$, siempre podemos tomar $\delta < \lambda$ y se cumple que $]\delta, \lambda] \subset]u, v[\subset U$.

En particular, α es discreto si y sólo si $\alpha \leq \omega$, y α es 1AN si y sólo si[1] $\alpha \leq \omega_1$. En efecto, si $\alpha > \omega_1$ entonces $\omega_1 \in \alpha$ no admite una base numerable de entornos, pues si $\{U_n\}_{n\in\omega}$ es cualquier familia numerable de entornos de ω_1, podemos tomar el menor ordinal $\delta_n < \omega_1$ tal que $]\delta_n, \lambda] \subset U_n$. Entonces $\delta = \bigcup\limits_n \delta_n < \omega_1$, y cumple que $\bigwedge n \in \omega \ \ ]\delta, \lambda] \subset U_n$, luego $]\delta + 1, \lambda]$ es un entorno de λ que no puede contener ningún entorno U_n, luego la familia dada no es una base de entornos.

Así pues, los ordinales $> \omega_1$ son ejemplos de espacios topológicos no metrizables.

Observemos por último que si λ es un ordinal límite, un conjunto $C \subset \lambda$ es cerrado en λ en el sentido de la definición 6.1 si y sólo si es cerrado respecto de la topología de orden en λ.

En efecto, si C es cerrado para la topología de orden y $\lambda' < \lambda$ cumple que $C \cap \lambda'$ no está acotado en λ', entonces C corta a todo conjunto $]\delta, \lambda']$, luego corta a todo entorno de λ', luego $\lambda' \in \overline{C} = C$. Así pues, C es cerrado en el sentido de 6.1.

Recíprocamente, si C es cerrado según 6.1 y $\beta \in \overline{C}$, entonces todo entorno de β corta a C. Si β es un punto aislado, entonces $\{\beta\} \cap C \neq \varnothing$, luego $\beta \in C$, y si β es un ordinal límite, entonces, para todo $\delta < \beta$ tenemos que $]\delta, \beta] \cap C \neq \varnothing$, lo cual significa que $\beta \cap C$ no está acotado en β, luego $\beta \in C$ igualmente. Concluimos que $\overline{C} = C$, luego C es cerrado para la topología.

8.3 Aplicaciones continuas

Uno de los conceptos más relevantes que permite formalizar la topología es el de aplicación continua, entendida como una aplicación que "no desgarra" un

[1]Una implicación usa AEN, al afirmar que $\delta < \omega_1$.

conjunto, en el sentido de que transforma los puntos de alrededor de un punto x en los puntos de alrededor de $f(x)$. Con precisión:

Definición 8.27 Una aplicación $f : X \longrightarrow Y$ entre dos espacios topológicos es *continua* en un punto $x \in X$ si para todo entorno U de $f(x)$ se cumple que $f^{-1}[U]$ es un entorno de x. Diremos que f es *continua* en un conjunto $A \subset X$ si es continua en todos los puntos de A. Diremos que f es *continua* si lo es en todos los puntos de su dominio X.

En otras palabras, f es continua en x si entre los puntos de alrededor de $f(x)$ están las imágenes de todos los puntos de alrededor de x. La definición puede expresarse en términos de una base de entornos de x y otra de $f(x)$: dado un entorno básico U de $f(x)$, debe cumplirse que $f^{-1}[U]$ contenga un entorno básico de x. Si aplicamos esto a una aplicación entre dos espacios métricos tomando un entorno básico de $f(x)$ de la forma $B_\epsilon(f(x))$ y un entorno básico de x de la forma $B_\delta(x)$, tenemos la caracterización siguiente:

Teorema 8.28 *Una aplicación $f : M \longrightarrow N$ entre dos espacios métricos es continua en un punto $x \in M$ si y sólo si*

$$\bigwedge \epsilon > 0 \bigvee \delta > 0 \bigwedge u \in M(d(x, u) < \delta \rightarrow d(f(x), f(u)) < \epsilon).$$

Es decir, que si queremos que $f(u)$ diste de $f(x)$ menos que ϵ, sólo tenemos que tomar u a una distancia de x menor que δ, o también, que puntos suficientemente próximos a x tienen imágenes arbitrariamente próximas a $f(x)$.

En espacios 1AN podemos caracterizar la continuidad en términos de sucesiones:

Teorema 8.29 (AEN) *Sea $f : X \longrightarrow Y$ una aplicación entre espacios topológicos y sea $x \in X$ un punto con una base numerable de entornos. Entonces f es continua en x si y sólo si para toda sucesión $\{x_n\}_{n\in\omega}$ en X convergente a x se cumple que $\{f(x_n)\}_{n\in\omega}$ converge a $f(x)$.*

DEMOSTRACIÓN: Si f es continua en x y $\{x_n\}_{n\in\omega}$ converge a x, entonces, dado un entorno U de $f(x)$, tenemos que $f^{-1}[U]$ es un entorno de x, luego existe un $m \in \omega$ tal que para $n \geq m$ se cumple $x_n \in f^{-1}[U]$, luego $f(x_n) \in U$, luego $\{f(x_n)\}_{n\in\omega}$ converge a $f(x)$.

Recíprocamente, si se cumple la propiedad sobre las sucesiones pero f no es continua en x, entonces existe un entorno U de $f(x)$ tal que $f^{-1}[U]$ no es entorno de x, es decir, que x no es interior a $f^{-1}[U]$. Por el teorema 8.26 (en cuya prueba sólo se usa que x tiene una base numerable de entornos) existe una sucesión $\{x_n\}_{n\in\omega}$ convergente a x contenida en $X \setminus f^{-1}[U]$ (en la prueba se ve que es así), luego $\{f(x_n)\}_{n\in\omega}$ está contenida en $Y \setminus U$, luego no puede converger a $f(x)$. ∎

El teorema siguiente es una consecuencia inmediata de la definición de continuidad:

Teorema 8.30 *Si $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ son aplicaciones entre espacios topológicos, f es continua en un punto $x \in X$ y g es continua en $f(x)$, entonces $f \circ g$ es continua en x. En particular, si f y g son continuas, también lo es $f \circ g$.*

Ahora observamos que la continuidad global tiene una caracterización global:

Teorema 8.31 *Una aplicación $f : X \longrightarrow Y$ entre espacios topológicos es continua si y sólo si para todo abierto A de Y se cumple que $f^{-1}[A]$ es abierto en X.*

DEMOSTRACIÓN: Si f es continua y A es abierto en Y, para probar que $f^{-1}[A]$ es abierto en X veamos que es entorno de todos sus puntos. Sea, pues, $x \in f^{-1}[A]$. Entonces $f(x) \in A$, luego A es un entorno de $f(x)$, luego $f^{-1}[A]$ es un entorno de x. Así pues, $f^{-1}[A]$ es abierto.

Recíprocamente, si U es un entorno de $f(x)$, entonces existe un abierto A tal que $f(x) \in A \subset U$, luego $x \in f^{-1}[A] \subset f^{-1}[U]$, luego $f^{-1}[U]$ es un entorno de x. ■

Es claro que para que f sea continua basta con pedir que $f^{-1}[A]$ sea abierto en X para todo abierto de una base o subbase prefijada de Y.

Ahora es inmediato que si X es discreto o Y es trivial, toda aplicación $f : X \longrightarrow Y$ es continua. Más en general, notemos que una aplicación f es siempre continua en los puntos aislados de su dominio, pues si U es un entorno de $f(x)$, entonces $f^{-1}[U]$ es entorno de x, ya que $\{x\}$ es abierto.

Por otra parte, toda función constante es continua, ya que la antiimagen de un conjunto por una función constante es vacía o todo el espacio.

El teorema siguiente relaciona la continuidad con la topología relativa:

Teorema 8.32 *Sea $f : X \longrightarrow Y$ una aplicación entre espacios topológicos.*

a) Si $Z \subset X$, la inclusión $i : Z \longrightarrow X$ es continua, luego si f es continua también lo es la restricción $f|_Z : Z \longrightarrow Y$ es continua.

b) Si $f[X] \subset W \subset Y$, entonces f es continua (en un punto) como aplicación $f : X \longrightarrow Y$ si y sólo si lo es como aplicación $f : X \longrightarrow W$.

DEMOSTRACIÓN: a) Si $A \subset X$ es abierto, entonces $i^{-1}[A] = A \cap Z$ es abierto en Z, luego i es continua. Entonces $f|_Z = i \circ f$ es continua por ser composición de funciones continuas.

Si $f : X \longrightarrow W$ es continua, entonces $f : X \longrightarrow Y$ lo es porque es la composición de f con la inclusión $W \longrightarrow Y$. Si $f : X \longrightarrow Y$ es continua, un abierto de W es de la forma $A \cap W$, donde A es abierto en Y, pero claramente $f^{-1}[A \cap W] = f^{-1}[A]$, luego f es continua como aplicación en W. ■

Respecto a productos, observemos que de la propia definición de la topología producto se sigue que ésta es la mínima topología para la que las proyecciones son funciones continuas. Más aún:

Teorema 8.33 *Sea* $X = \prod_i X_i$ *un producto de espacios topológicos. Entonces cada proyección* $p_i : X \longrightarrow X_i$ *es continua y una aplicación* $f : Y \longrightarrow X$ *entre espacios topológicos es continua si y sólo si lo es cada función coordenada* $f_i = f \circ p_i$.

Demostración: Si f es continua las funciones $f \circ p_i$ también lo son por ser composición de funciones continuas.

Si cada $f \circ p_i$ es continua, sea $A = \prod_{i \in I} A_i$ un abierto básico de X. Sean $i_1, \ldots, i_n$ los índices tales que $A_{i_j} \neq X_{i_j}$. Entonces tenemos que cada antiimagen $f^{-1}\big[p_{i_j}^{-1}[A_{i_j}]\big] = (f \circ p_{i_j})^{-1}[A_{i_j}]$ es abierta en Y, pero

$$A = \bigcap_{j=1}^{n} p_{i_j}^{-1}[A_{i_j}] \quad \text{y} \quad f^{-1}[A] = \bigcap_{j=1}^{n} f^{-1}\big[p_{i_j}^{-1}[A_{i_j}]\big]$$

es abierto en Y. ■

Teorema 8.34 *Sean* $X = \prod_{i \in I} X_i$, $Y = \prod_{i \in I} Y_i$ *dos productos de espacios topológicos y sea* $\{f_i\}_{i \in I}$ *una familia de aplicaciones continuas* $f_i : X_i \longrightarrow Y_i$. *Entonces la aplicación* $f = \prod_{i \in I} f_i : X \longrightarrow Y$ *dada por* $f(x) = \{f_i(x_i)\}_{i \in I}$ *es continua.*

Demostración: Basta observar que $f \circ p_i^Y = p_i^X \circ f_i$, luego la composición es continua, luego f también, por el teorema anterior. ■

Una propiedad que se usa con frecuencia es la siguiente:

Teorema 8.35 *Si* $f, g : X \longrightarrow Y$ *son funciones continuas entre espacios topológicos e* Y *es un espacio de Hausdorff, entonces el conjunto*

$$\{x \in X \mid f(x) = g(x)\}$$

es cerrado en X. *En particular, si* f *y* g *coinciden en un conjunto denso, entonces* $f = g$.

Demostración: Llamemos A al conjunto del enunciado. La aplicación $h : X \longrightarrow Y \times Y$ dada por $h(x) = (f(x), g(x))$ es continua, porque lo son sus funciones coordenadas, y por 8.17 la diagonal $\Delta \subset Y \times Y$ es cerrada. Basta observar que $A = h^{-1}[\Delta]$.

Si existe $D \subset X$ denso tal que $f|_D = g|_D$, entonces $D \subset A$, de modo que $X = \overline{D} \subset \overline{A} = A \subset X$, lo que significa que $f = g$. ■

El teorema siguiente es útil a menudo para probar que una aplicación es continua cuando tiene definiciones diferentes sobre conjuntos diferentes:

Teorema 8.36 *Sea* $f : X \longrightarrow Y$ *una aplicación entre espacios topológicos. Sean* $C_1, \ldots, C_n$ *subconjuntos cerrados de* X *tales que* $X = C_1 \cup \cdots \cup C_n$. *Entonces* f *es continua si y sólo si cada* $f|_{C_i}$ *es continua.*

Demostración: Una implicación es obvia. Si las restricciones son continuas, entonces dado un cerrado C de Y, se cumple que

$$f^{-1}[C] = (f^{-1}[C] \cap C_1) \cup \cdots \cup (f^{-1}[C] \cap C_n) = (f|_{C_1})^{-1}[C] \cup \cdots \cup (f|_{C_n})^{-1}[C].$$

Ahora, cada $(f|_{C_i})^{-1}[C]$ es cerrado en C_i, luego es la intersección con C_i de un cerrado de X, luego es la intersección de dos cerrados en X, luego es cerrado en X. Así pues, $f^{-1}[C]$ es la unión de un número finito de cerrados de X, luego es cerrado en X. Esto prueba que f es continua. ■

Veamos algunos ejemplos concretos de funciones continuas:

Teorema 8.37 *Si M es un espacio métrico y $\varnothing \neq A \subset M$, entonces la distancia $d : M \times M \longrightarrow \mathbb{R}$ y la aplicación $d(\ \ , A) : M \longrightarrow \mathbb{R}$ son continuas.*

Demostración: Consideramos en $M \times M$ la distancia dada por

$$d((x, y), (x', y')) = d(x, x') + d(y, y'),$$

que hemos probado que induce la topología producto en $M \times M$. Entonces

$$|d(x, y) - d(x', y')| \leq |d(x, y) - d(x', y)| + |d(x', y) - d(x', y')|$$

$$\leq d(x, x') + d(y, y') = d((x, y), (x', y')),$$

es decir, si llamamos $P = (x, y)$ y $P' = (x', y')$, acabamos de probar que $d(d(P), d(P')) \leq d(P, P')$, lo que permite aplicar el teorema 8.28 con $\delta = \epsilon$.

La continuidad de $d(\ \ , A)$ en un punto x es consecuencia inmediata de la relación:

$$|d(x, A) - d(y, A)| \leq d(x, y).$$

Para probarla observamos que si $z \in A$, se cumple $d(x, z) \leq d(x, y) + d(y, z)$. De aquí se sigue claramente $d(x, A) \leq d(x, y) + d(y, z)$, y tomando el ínfimo en z vemos que $d(x, A) \leq d(x, y) + d(y, A)$. Análogamente, $d(y, A) \leq d(x, y) + d(x, A)$, de donde se sigue la relación con valores absolutos. ■

En particular, el valor absoluto es una aplicación continua $K \longrightarrow \mathbb{R}$ en todo cuerpo métrico, pues $|x| = d(x, 0)$ (luego es la composición de la aplicación $K \longrightarrow K \times K$ dada por $x \mapsto (x, 0)$, que es continua porque lo son sus funciones coordenadas, con la distancia d).

Los teoremas 7.23, 8.29 y 8.15 implican que la suma y el producto en todo cuerpo métrico K (en particular en $\mathbb{R}$) son aplicaciones continuas $K \times K \longrightarrow K$. También es continua la aplicación $K \setminus \{0\} \longrightarrow K \setminus \{0\}$ dada por $x \mapsto 1/x$.

Para probarlo consideramos una sucesión $\{x_n\}_{n \in \omega}$ en $K \setminus \{0\}$ convergente a $x \in K \setminus \{0\}$ y observamos que

$$\left|\frac{1}{x_n} - \frac{1}{x}\right| = \frac{|x - x_n|}{|x_n||x|}.$$

Sabemos que la sucesión $\{1/x_n\}_{n\in\omega}$ es de Cauchy (teorema 7.28), luego está acotada, luego también lo está $\{1/|x_n||x|\}_{n\in\omega}$, y tenemos que $\{|x_n-x|\}_{n\in\omega}$ converge a 0, luego su producto converge a 0 por 7.27. Esto implica que $\{1/x_n\}_{n\in\omega}$ converge a $1/x$.

Por ejemplo, por el teorema 8.24 sabemos que $\mathbb{Q}\times\mathbb{Q}$ es denso en $\mathbb{R}\times\mathbb{R}$, luego el teorema 8.35 implica que la suma y el producto de $\mathbb{R}$ son las únicas extensiones posibles de la suma y el producto en $\mathbb{Q}$ que convierten a $\mathbb{R}$ en un cuerpo métrico.

Es obvio que toda semejanza entre dos conjuntos totalmente ordenados es continua respecto de las topologías de orden, pues la antiimagen de un intervalo abierto es también un intervalo abierto.

Lo mismo vale si $f : X \longrightarrow Y$ es una biyección monótona decreciente, pues entonces

$$f^{-1}\big[\,]a,+\infty[\,\big] = \,]-\infty, f^{-1}(a)[\,, \qquad f^{-1}\big[\,]-\infty,b[\,\big] = \,]f^{-1}(b),+\infty[\,.$$

En particular, la aplicación $[0,+\infty] \longrightarrow [0,+\infty]$ dada por $x\mapsto 1/x$, con el convenio de que $1/0=+\infty$ y $1/+\infty = 0$ es continua, pues es inmediato que se trata de una biyección monótona decreciente.

También es continua la aplicación $\sqrt{} : [0,+\infty[\, \longrightarrow [0,+\infty[$, pues se trata de una semejanza. Incluso sigue siendo continua si la extendemos a $[0,+\infty]$ mediante $\sqrt{+\infty}=+\infty$, pues sigue siendo una semejanza.

Teorema 8.38 *Una aplicación $f:\alpha\longrightarrow\beta$ creciente entre dos ordinales es continua si y sólo si para todo ordinal límite $\lambda\in\alpha$ se cumple que $f(\lambda)=\bigcup\limits_{\delta<\lambda} f(\delta)$. En particular, toda función normal es continua.*

DEMOSTRACIÓN: Toda función es continua en los puntos aislados, luego f será continua si y sólo si lo es en los ordinales límite. Vamos a probar que la condición del enunciado equivale a la continuidad de f en λ.

Observemos que la monotonía de f implica en cualquier caso la desigualdad $\gamma=\bigcup\limits_{\delta<\lambda} f(\delta)\leq f(\lambda)$. Supongamos que f es continua en λ pero $\gamma<f(\lambda)$. Como $]\gamma,f(\lambda)]$ es un entorno de $f(\lambda)$, existe $\delta_0<\lambda$ tal que $]\delta_0,\lambda]\subset f^{-1}\big[]\gamma,f(\lambda)]\big]$, pero entonces, si $\delta_0<\delta<\lambda$, tenemos que $f(\delta_0)\leq\gamma<f(\delta_0)$, contradicción. Así pues, $f(\lambda)=\gamma$, como había que probar.

Si se cumple la condición del enunciado, un entorno básico de $f(\lambda)$ es de la forma $]\gamma,f(\lambda)]$, para cierto $\gamma<f(\lambda)$, pero por hipótesis $\gamma<f(\delta_0)$, para cierto ordinal $\delta_0<\lambda$, y esto implica que $]\delta_0,\lambda[\,\subset f^{-1}\big[]\gamma,f(\lambda)]\big]$, pues si $\delta_0<\delta<\lambda$ entonces $\gamma<f(\delta_0)\leq f(\delta)\leq f(\lambda)$, luego $f(\delta)\in\,]\gamma,f(\lambda)]$. ■

Para terminar introducimos las aplicaciones que conservan todas las propiedades topológicas:

Definición 8.39 Una aplicación $f : X \longrightarrow Y$ entre dos espacios topológicos es un *homeomorfismo* si es biyectiva y tanto f como f^{-1} son continuas. Se dice que X e Y son *homeomorfos* si existe un homeomorfismo entre ellos, y se representa por $X \cong Y$.

Claramente, f es un homeomorfismo si cumple que $A \subset X$ es un abierto en X si y sólo si $f[A]$ es un abierto en Y, y viceversa. Las propiedades topológicas son las que se definen en última instancia a partir de los conjuntos abiertos, luego es claro que dos espacios homeomorfos tienen las mismas propiedades topológicas.

Es claro que la isometrías entre espacios métricos y las semejanzas entre conjuntos totalmente ordenados son homeomorfismos.

Equivalentemente, un homeomorfismo es una aplicación biyectiva, continua y abierta entre espacios topológicos, donde una aplicación $f : X \longrightarrow Y$ se dice *abierta* si cuando $U \subset X$ es abierto entonces $f[U]$ también lo es.

Un ejemplo de aplicaciones abiertas que no son homeomorfismos lo constituyen las proyecciones de los productos cartesianos:

Teorema 8.40 *Las proyecciones* $p_i : \prod\limits_{i\in I} X_i \longrightarrow X_i$ *son aplicaciones abiertas.*

DEMOSTRACIÓN: Si $U = \prod\limits_{i\in I} U_i$ es un abierto básico, entonces $p_i[U] = U_i$ es abierto en X_i, y si $G = \bigcup\limits_{j\in J} U_j$ es una unión de abiertos básicos, entonces $p_i[G] = \bigcup\limits_{j\in J} p_i[U_j]$ también es abierto. ■

El producto cartesiano de espacios topológicos es asociativo:

Teorema 8.41 *Si* $\{X_i\}_{i\in I}$ *es una familia de espacios topológicos y* $I = \bigcup\limits_{j\in J} I_j$ *es una descomposición de* I *en conjuntos disjuntos dos a dos, entonces la aplicación* $f : \prod\limits_{i\in I} X_i \longrightarrow \prod\limits_{j\in J} \prod\limits_{i\in I_j} X_i$ *dada por* $f(x)_j = x|_{I_j}$ *es un homeomorfismo.*

DEMOSTRACIÓN: Claramente f es biyectiva, y es continua, pues si $j \in J$ la función coordenada $f \circ p_j : \prod\limits_{i\in I} X_i \longrightarrow \prod\limits_{i\in I_j} X_i$ es continua, pues, para cada $i \in I_j$ tenemos que $f \circ p_j \circ p_i = p_i$, que es continua.

Teniendo en cuenta que $f^{-1}(x) = \bigcup\limits_{j\in j} x_j$, se comprueba igualmente que, si $i \in I_j$, entonces $f^{-1} \circ p_i = p_j \circ p_i$, luego f^{-1} es continua. ■

Nota El teorema 7.42 nos da que $\mathbb{R}$ es semejante a $]0,1[$, luego son espacios homeomorfos con la topología del orden (la usual). La topología de ambos espacios está inducida por la distancia usual en $\mathbb{R}$, pero $\mathbb{R}$ es un espacio métrico completo, mientras que es fácil ver que $]0,1[$ no lo es. Basta considerar la sucesión $\{1/n\}_{n=1}^{\infty}$, que converge en $\mathbb{R}$, luego es de Cauchy en $\mathbb{R}$, luego también lo es en $]0,1[$, pero no converge en $]0,1[$.

Esto significa que la completitud de un espacio métrico no es una propiedad topológica, ni tampoco lo es el concepto de sucesión de Cauchy. Un homeomorfismo entre $]0,1[$ y $\mathbb{R}$ tiene que transformar la sucesión de Cauchy no convergente $\{1/n\}_{n=1}^{\infty}$ en una sucesión no convergente en $\mathbb{R}$, pero como $\mathbb{R}$ es completo, la sucesión imagen no puede ser de Cauchy. Por lo tanto, "ser una sucesión de Cauchy" no es una propiedad que se conserve necesariamente a través de un homeomorfismo.

Esto no contradice nada de lo dicho anteriormente, porque lo que sucede es que, al contrario de lo que sucede con el concepto de sucesión convergente, no es posible definir el concepto de sucesión de Cauchy en un espacio métrico a partir de la topología inducida por la distancia, sino que es imprescindible hacer referencia a la distancia en sí. De este modo, dos distancias en un mismo conjunto pueden inducir la misma topología, pero de modo que una determine un espacio métrico completo y la otra no. Esto sucede, por ejemplo, si transportamos la distancia de $\mathbb{R}$ a $]0,1[$ a través de un homeomorfismo. Con ello obtenemos una distancia que induce la topología usual en $]0,1[$, pero que lo convierte en un espacio métrico completo.

Lo que sí que es una propiedad topológica es "ser metrizable" o "ser completamente metrizable". El espacio topológico $]0,1[$ es completamente metrizable, en el sentido de que su topología es la topología inducida por una cierta distancia que lo convierte en un espacio métrico completo (sólo que esa distancia no es la usual, sino la deducida de un homeomorfismo entre $]0,1[$ y $\mathbb{R}$). ■

8.4 Condiciones de numerabilidad

La mayor parte de los espacios topológicos que surgen de forma natural al estudiar la topología de los espacios $\mathbb{R}^n$ satisfacen condiciones de numerabilidad que simplifican en gran medida su estudio, a la vez que proporcionan criterios de elección que hacen innecesario el axioma de elección o bien hacen que sólo se requieran las formas débiles, como AEN o ED.

Ya hemos visto una de estas condiciones: el primer axioma de numerabilidad 1AN, que satisfacen todos los espacios métricos y que permite caracterizar mediante sucesiones los conceptos topológicos. Otra condición más fuerte es el segundo axioma de numerabilidad:

Definición 8.42 Un espacio topológico cumple el *segundo axioma de numerabilidad* (2AN) si tiene una base numerable.

Es inmediato que, en todo espacio topológico, 2AN $\rightarrow$ 1AN, pues si $\mathcal{B}$ es una base numerable de un espacio X y $x \in X$, entonces $\mathcal{B}_x = \{B \in \mathcal{B} \mid x \in B\}$ es una base numerable de entornos de X.

Por otra parte, un espacio discreto no numerable es un ejemplo de espacio 1AN que no es 2AN.

También es inmediato que todo subespacio Y de un espacio X que sea 1AN o 2AN es también 1AN o 2AN, pues si $\mathcal{B}$ es una base numerable de X (o una base numerable de entornos en X de un punto $y \in Y$) entonces $\{B \cap Y \mid B \in \mathcal{B}\}$ es una base numerable de Y (o una base numerable de entornos de y en Y).

Observemos que $\mathbb{R}$ cumple el segundo axioma de numerabilidad, pues el conjunto de todos los intervalos $]a, b[$ con extremos a, $b \in \mathbb{Q}$ es una base numerable.

Este hecho se extiende a los espacios $\mathbb{R}^n$ y a todos sus subespacios. Más en general:

Teorema 8.43 (AEN) *Si $\{X_i\}_{i\in I}$ es una familia de espacios topológicos que cumplen* 1AN *(resp.* 2AN*) e I es numerable, entonces $X = \prod\limits_{i\in I} X_i$ cumple también* 1AN *(resp.* 2AN*).*

Demostración: Consideremos un punto $x \in X$ y, para cada $i \in I$, sea $\mathcal{B}_i$ una base numerable de entornos (abiertos) de x_i (resp. una base de X_i). Es claro entonces que el conjunto $\mathcal{B}$ formado por todos los conjuntos de la forma $\bigcap\limits_{i\in I_0} p_i^{-1}[B_i]$ con $B_i \in \mathcal{B}_i$ forman una base de entornos de x (resp. una base de X). Basta probar que $\mathcal{B}$ es numerable. Ahora bien, tenemos una aplicación suprayectiva

$$\bigcup_{I_0 \in \mathcal{P}^f I} \prod_{i\in I_0} \mathcal{B}_i \longrightarrow \mathcal{B},$$

la dada por $\{B_i\}_{i\in I_0} \mapsto \bigcap\limits_{i\in I_0} p_i^{-1}[B_i]$, y es fácil ver que[2] el conjunto de la izquierda es numerable, luego $\mathcal{B}$ también lo es. ■

En cambio estas condiciones de numerabilidad no se conservan con productos no numerables:

Teorema 8.44 (AE) *Si un producto $X = \prod\limits_{i\in I} X_i$ cumple* 1AN *y ningún factor X_i tiene la topología trivial (lo que en particular supone que tiene más de un punto), entonces I es numerable.*

Demostración: Para cada $i \in I$ elegimos un abierto $U_i \subsetneq X_i$ no vacío, y un punto $x_i \in U_i$. Con esto formamos un punto $x \in X$. Si $\mathcal{B}$ es una base numerable de entornos de x, para cada $i \in I$ existe un $B_i \in \mathcal{B}$ tal que $x \in B_i \subset p_i^{-1}[U_i]$. Consideramos la aplicación $f : I \longrightarrow \mathcal{B}$ dada por $f(i) = B_i$. Así

$$I = \bigcup_{B\in\mathcal{B}} f^{-1}[B],$$

Basta probar que cada conjunto $f^{-1}[B]$ es finito, pues entonces I será una unión numerable de conjuntos finitos, luego será numerable. Ahora bien, dado $B \in \mathcal{B}$,

[2] Aquí usamos que un producto finito de conjuntos numerables es numerable (lo que no requiere AE), y que la unión numerable de conjuntos numerables es numerable (lo que sólo requiere AEN para elegir una biyección de cada conjunto en ω), lo cual implica en particular que $\mathcal{P}^f I$ es numerable.

entonces $x \in \bigcap\limits_{i \in I_0} p_i^{-1}[A_i] \subset B$, donde $I_0 \subset I$ es finito y A_i es abierto en X_i. Si $i \in f^{-1}[B]$ entonces $B \subset p_i^{-1}[U_i]$, y esto implica que $i \in I_0$, pues en caso contrario podemos tomar $y \in X_i \setminus U_i$ y el punto $x' \in X$ que coincide con x salvo que $x'_i = y$ cumpliría $x' \in B \setminus p_i^{-1}[U_i]$. Así pues, $f^{-1}[B] \subset I_0$ es finito. ■

Nota Los únicos usos de AE en la prueba del teorema anterior que no pueden reducirse a AEN son las elecciones de los abiertos U_i y de los puntos x_i. Por ello, el caso particular siguiente sólo requiere AEN:

> *Si X es un espacio topológico no trivial y el producto X^I cumple* 1AN*, entonces I es numerable.*

En particular (bajo AEN), espacios como ${}^{\omega_1}2$ son ejemplos de espacios que no cumplen 1AN y que, en particular, no son metrizables. ■

Una condición de numerabilidad más débil es la separabilidad:

Definición 8.45 Un espacio topológico es *separable* si tiene un conjunto denso numerable.

Es inmediato que 2AN implica la separabilidad, pues si $\mathcal{B} = \{B_n \mid n \in \omega\}$ es una base numerable de un espacio X y elegimos un punto $d_n \in B_n$, el conjunto $D = \{d_n \mid n \in \omega\}$ corta a cada abierto básico, luego corta a cada abierto, luego es un conjunto denso numerable.

En el contexto de los espacios métricos la separabilidad equivale a 2AN:

Teorema 8.46 *Un espacio métrico cumple* 2AN *si y sólo si es separable.*

Demostración: Si M es un espacio métrico separable, tomamos un conjunto denso $D = \{d_n \mid n \in \omega\}$. Entonces el conjunto $\mathcal{B}$ formado por las bolas $B_{1/m}(d_n)$ es una base de M, pues si A es un abierto en M y $x \in A$, entonces existe un $\epsilon > 0$ tal que $B_\epsilon(x) \subset A$ y, tomando $k \in \omega$ tal que $1/k < \epsilon/2$, podemos tomar un n tal que $d(d_n, x) < 1/k$, con lo que $x \in B_{1/k}(d_n) \subset B_\epsilon(x) \subset A$, ya que si $y \in B_{1/k}(d_n)$ entonces $d(y, x) \leq d(y, d_n) + d(d_n, x) < 1/k < \epsilon$. ■

Ejemplo La *recta de Sorgenfrey* S es el conjunto $\mathbb{R}$ de los números reales con la topología que tiene por base a los intervalos $[a, b[$, con $a < b$. Es fácil comprobar que se cumplen las condiciones del teorema 8.4, por lo que S es ciertamente un espacio topológico.

Se comprueba inmediatamente que es de Hausdorff, que cumple 1AN (porque $\{[a, 1/n[\}_{n \in \omega \setminus \{0\}}$ es una base de entornos de a) y es separable, pues $\mathbb{Q}$ es denso en S. En cambio, no cumple 2AN.

En efecto, si tuviera una base numerable $\mathcal{B}$, para cada $x \in \mathbb{R} \setminus \mathbb{Q}$ tomamos[3] $B_x \in \mathcal{B}$ tal que $x \in B_x \subset [x, x + 1[$, pero sucede entonces que la aplicación $f : \mathbb{R} \setminus \mathbb{Q} \longrightarrow \mathcal{B}$ dada por $f(x) = B_x$ es inyectiva, pues si $x < y$ son dos números irracionales, entonces $x \in B_x \setminus B_y$, y así tenemos una contradicción.

[3] Aquí no usamos AE porque estamos eligiendo en un conjunto numerable.

En particular vemos que S es un espacio 1AN separable no metrizable. ■

La separabilidad se conserva por productos mejor que 1AN y 2AN:

Teorema 8.47 (AE) *El producto de a lo sumo $2^{\aleph_0}$ espacios topológicos separables es separable.*

Demostración: Sea $X = \prod\limits_{i\in I} X_i$ un producto de espacios separables, donde $|I| \leq 2^{\aleph_0}$. Sea $D_i \subset X_i$ un subconjunto denso numerable. Entonces sabemos que $D = \prod\limits_{i\in I} D_i$ es denso en X, luego basta probar[4] que D contiene un subconjunto denso numerable. Equivalentemente, podemos suponer que cada X_i es numerable. Tomamos biyecciones $g_i : \omega \longrightarrow X_i$, que son trivialmente continuas, y determinan una biyección continua $\omega^I \longrightarrow X$.

Consideremos el espacio $Y = {}^\omega 2$. A partir de una aplicación $j : I \longrightarrow Y$ inyectiva podemos construir una aplicación continua y suprayectiva $h : \omega^Y \longrightarrow \omega^I$ (la dada por $h(y)(i) = y(j(i))$). Componiendo ambas obtenemos una aplicación continua y suprayectiva $f : \omega^Y \longrightarrow X$.

Si encontramos $D \subset \omega^Y$ denso numerable, entonces $f[D]$ será un subconjunto denso numerable de X (si $A \subset X$ es abierto no vacío, entonces $f^{-1}[A]$ es un abierto no vacío, luego corta a D, luego A corta a $f[D]$). Así pues, basta probar que ω^Y es separable.

Por 8.43 sabemos que Y es un espacio topológico que cumple 2AN. Sea $\mathcal{B}$ una base numerable. Sea $\mathcal{F}$ el conjunto de todos los subconjuntos finitos de $\mathcal{B}$ formados por abiertos disjuntos dos a dos. Claramente $\mathcal{F}$ es numerable. Sea $D \subset \omega^Y$ el conjunto de todas las funciones $f : Y \longrightarrow \omega$ tales que existe $B = \{B_i \mid i < n\} \in \mathcal{F}$ de modo que cada $f|_{B_i}$ es constante, al igual que $f|_{Y\setminus\bigcup B}$.

Si llamamos D_B al conjunto de los $f \in D$ determinados por $B \in \mathcal{F}$, tenemos que $D = \bigcup\limits_{B\in\mathcal{F}} D_B$ y cada D_B es numerable, pues si $B = \{B_i \mid i < n\}$, la aplicación ${}^{n+1}\omega \longrightarrow D_B$ que a cada $s \in {}^{n+1}\omega$ le asigna la función

$$\bigcup_{i<n} (B_i \times \{s(i)\}) \cup ((Y \setminus \bigcup B) \times \{s(n)\})$$

es suprayectiva. Concluimos que D es numerable, y basta probar que es denso en ω^Y.

Una base de ω es $\{\{n\}\}_{n\in\omega}$, la cual determina la base de ω^Y formada por los abiertos de la forma $\bigcap\limits_{i\leq k} p_{y_i}^{-1}[n_i]$, donde $y_0, \ldots, y_k$ son puntos de Y distintos dos a dos y $n_i \in \omega$.

Basta probar que D corta a todos estos abiertos básicos. Esto equivale a encontrar un $f \in D$ tal que $\bigwedge i \leq k\ f(y_i) = n_i$. Pero, como Y es un espacio de Hausdorff, existen abiertos básicos disjuntos dos a dos $B_0, \ldots, B_n$ tales que $y_i \in B_i$. Ahora basta tomar $f = \bigcup\limits_{i\leq n} (B_i \times \{n_i\}) \cup ((Y \setminus \bigcup B) \times \{y_0\}) \in D$. ■

[4]En general, si $E \subset D \subset X$, E es denso en D y D es denso en X, entonces E es también denso en X, pues tenemos que $D = \overline{E}^D = \overline{E} \cap D$, luego $D \subset \overline{E} \subset X$, luego $X = \overline{D} \subset \overline{E} \subset X$ y $\overline{E} = X$.

Nota La prueba de que ω^Y es separable sólo usa AEN, y la reducción a este caso requiere únicamente AEN si I es numerable y no requiere AE en absoluto si todos los espacios son el mismo. Por lo tanto, con AEN puede probarse que un producto numerable de espacios separables es separable y que X^I es separable siempre que X es separable y $\overline{\overline{I}} \leq 2^{\aleph_0}$. ■

En particular vemos que $\omega^{\omega 2}$ es un espacio separable que no cumple 1AN, ni por tanto 2AN.

Veamos una última condición de numerabilidad:

Definición 8.48 Un espacio topológico X cumple la *condición de cadena numerable* (ccn) si toda familia de abiertos de X disjuntos dos a dos es numerable.

Las familias de abiertos disjuntos dos a dos en un espacio topológico se llaman *anticadenas* de abiertos.[5]

Todo espacio separable X cumple la ccn, pues si D es denso en X y es numerable, y $\mathcal{F}$ es una familia de abiertos disjuntos dos a dos, podemos definir una aplicación $\mathcal{F} \setminus \{\varnothing\} \longrightarrow D$ inyectiva asignando a abierto $U \in \mathcal{F}$ no vacío un punto de $U \cap D$.

Nuevamente, en espacios métricos la condición es equivalente a la separabilidad y a 2AN:

Teorema 8.49 (AE) *Un espacio métrico es* 2AN *si y sólo si cumple la condición de cadena numerable.*

DEMOSTRACIÓN: Sea M un espacio métrico ccn y, para cada $n \in \omega \setminus \{0\}$, sea A_n el conjunto de todas las familias de bolas abiertas disjuntas dos a dos de radio $1/n$. Podemos considerar a A_n como conjunto parcialmente ordenado por la inclusión, y es claro que cumple las hipótesis del lema de Zorn, pues si tenemos una cadena en A_n, la unión de sus elementos es una cota superior. Por lo tanto, existe una anticadena maximal C_n de bolas abiertas de radio $1/n$. Que sea maximal significa que si $B \notin C_n$ es una bola abierta de radio n, no puede ocurrir que sea disjunta de todos los elementos de C_n, pues entonces $C_n \cup \{B\}$ sería una anticadena mayor, en contra de la maximalidad de C_n, luego en cualquier caso (tanto si está en C_n como si no) toda bola abierta de radio $1/n$ corta a algún elemento de C_n.

Por hipótesis C_n es numerable, al igual que $\mathcal{B} = \bigcup\limits_{n\in\omega\setminus\{0\}} C_n$. Vamos a probar que $\mathcal{B}$ es una base de M.

Dado un abierto U en M y un punto $x \in U$, existe un $\epsilon > 0$ tal que $x \in B_\epsilon(x) \subset U$. Sea $n \in \omega$ tal que $1/n < \epsilon/3$. Entonces la bola $B_{1/n}(x)$ corta a una bola $B_{1/n}(y) \in \mathcal{B}$. Veamos que $x \in B_{2/n}(y) \subset B_\epsilon(x) \subset U$.

[5] Según esto, la condición de cadena numerable debería llamarse "condición de anticadena numerable". Su nombre se debe a que admite una formulación equivalente en términos de cadenas crecientes de abiertos, pero es más útil la formulación que hemos adoptado.

Si $u \in B_{1/n}(x) \cap B_{1/n}(y)$, entonces $d(x, y) \leq d(x, u) + d(u, y) < 2/n$, luego $x \in B_{2/n}(y)$. Por otra parte, si $z \in B_{2/n}(y)$, entonces

$$d(z, x) \leq d(z, y) + d(y, x) < 1/n + 2/n = 3/n < \epsilon,$$

luego $B_{2/n}(y) \subset B_\epsilon(x)$. ■

Sin embargo, la relación de la condición de cadena numerable con los productos es muy peculiar: no es posible demostrar en NBG (supuesto que sea consistente) que el producto de dos espacios topológicos que cumplan la ccn cumpla necesariamente la ccn, (véase el teorema 10.58) pero tampoco es posible demostrar que sea falso. Y además se cumple un teorema muy peculiar:

Teorema 8.50 (AE) *Sea* $X = \prod\limits_{i \in I} X_i$ *un producto de espacios topológicos tal que, para todo* $I_0 \subset I$ *finito, el producto* $\prod\limits_{i \in I_0} X_i$ *cumpla la condición de cadena numerable. Entonces* X *cumple la condición de cadena numerable. En particular, todo producto de espacios separables cumple la condición de cadena numerable.*

La segunda parte del teorema es inmediata: si los factores son separables, cualquier producto finito de ellos es separable por 8.47, luego cumple la ccn.

Una consecuencia de este teorema es que si tomamos como axioma que el producto de dos espacios topológicos con la ccn cumple también la ccn (lo cual es consistente, pues, como hemos indicado, no se puede demostrar lo contrario), entonces una simple inducción prueba que lo mismo vale para productos con cualquier número finito de factores, y el teorema anterior implica entonces que el producto de espacios ccn (sin restricción alguna sobre el número de factores) cumple también la ccn. Demostraremos este teorema a partir de un resultado puramente conjuntista:

Definición 8.51 Un *sistema* Δ o una *familia cuasidisjunta* de raíz r es una familia $\mathcal{F}$ de conjuntos tal que $\bigwedge xy \in \mathcal{F}(x \neq y \rightarrow x \cap y = r)$.

Teorema 8.52 (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 $\mathcal{A} = \bigcup\limits_{n \in \omega} \mathcal{A}_n$. Si $|\mathcal{A}_n| < \kappa$ para todo n, también $|\mathcal{A}| < \kappa$, luego existe un $n \in \omega$ (obviamente $n > 0$) 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 que en la prueba de 8.49, 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 $A = \bigcup\limits_{x\in\mathcal{M}} x$ 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 $\mathcal{A} = \bigcup\limits_{a\in A} \mathcal{A}_a$. 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 8.50): Supongamos que $\{A_j\}_{j\in J}$ es una familia no numerable 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, $A_j = \bigcap\limits_{i\in I_j} p_i^{-1}[U_{ij}]$, donde $I_j \subset I$ es finito y cada U_{ij} es abierto en X_i.

Consideramos la familia $\mathcal{A} = \{I_j \mid j \in J\}$. Si es numerable, como J no lo es, existe un $r \in \mathcal{A}$ tal que $J_0 = \{j \in J \mid I_j = r\}$ es no numerable. Si, por el contrario, $\mathcal{A}$ es no numerable, por el teorema anterior contiene un sistema Δ no numerable de raíz r. Equivalentemente, podemos tomar $J_0 \subset J$ no numerable tal que $\bigwedge jj' \in J_0(j \neq j' \to I_j \cap I_{j'} = r)$. 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 $\{A_j\}_{j\in J}$ es una familia de abiertos disjuntos dos a dos de modo que $\bigwedge jj' \in J(j \neq j' \to I_j \cap I_{j'} = r)$ (ya sea porque todos los conjuntos I_j 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_j no serían disjuntos dos a dos.

Consideremos ahora los abiertos $A_j^* = \prod\limits_{i\in r} U_{ij} \subset \prod\limits_{i\in r} X_i$. Vamos a probar que son disjuntos dos a dos, y con ello tendremos una contradicción pues estamos suponiendo que el producto finito cumple la ccn. En efecto, si $s^* \in A_j^* \cap A_{j'}^*$, podemos construir un $s \in A_i \cap A_j$ sin más que tomar:

$$\begin{array}{ll} s_i = s_i^* \in U_{ij} \cap U_{ij'} & \text{si } i \in r = I_j \cap I_{j'}, \\ s_i \in U_{ij} & \text{si } i \in I_j \setminus r, \\ s_i \in U_{ij'} & \text{si } i \in I_{j'} \setminus r, \\ s_i \in X_i & \text{si } i \in I \setminus (I_j \cup I_{j'}). \end{array}$$

Como $A_j \cap A_{j'} = \varnothing$, concluimos que también $A_j^* \cap A_{j'}^* = \varnothing$ y tenemos la contradicción. ■

8.5 Espacios compactos

La compacidad es el más abstracto de los conceptos topológicos básicos y a la vez el más potente. Se trata de una condición de finitud, en el sentido de que los espacios que la cumplen presentan muchas características en común con los espacios finitos sin limitar por ello el tamaño que puede tener el espacio.

Definición 8.53 Sea X un espacio topológico. Un *cubrimiento abierto* de X es una familia $\mathcal{C}$ de abiertos de X tal que $X = \bigcup \mathcal{C}$. Un *subcubrimiento* de un cubrimiento $\mathcal{C}$ es un cubrimiento contenido en $\mathcal{C}$.

Un espacio topológico K es *compacto*[6] si de todo cubrimiento abierto de K se puede extraer un subcubrimiento finito.

Es obvio que si X es un espacio finito, de todo cubrimiento abierto se puede extraer un subcubrimiento finito. Basta tomar un abierto que contenga a cada uno de los puntos del espacio. Así pues, todo espacio topológico finito es compacto.

Observemos que si $\mathcal{B}$ es una base de un espacio topológico K, se cumple que K es compacto si y sólo si todo cubrimiento de K por abiertos básicos admite un subcubrimiento finito. En efecto, si $\mathcal{C}$ es un cubrimiento arbitrario, consideramos el conjunto $\mathcal{C}_0 = \{B \in \mathcal{B} \mid \bigvee U \in \mathcal{C}\ B \subset U\}$, que es también un cubrimiento abierto de K, pues para cada $x \in K$ existe un $U \in \mathcal{C}$ tal que $x \in U$, y entonces existe un $B \in \mathcal{B}$ tal que $x \in B \subset U$, luego $x \in B \in \mathcal{C}_0$. Por hipótesis $\mathcal{C}_0$ admite un subcubrimiento finito $\{B_1, \ldots, B_n\}$ y para cada $j = 1, \ldots, n$ existe un $U_j \in \mathcal{C}$ tal que $B_j \subset U_j$, con lo que $\{U_1, \ldots, U_n\}$ es un subcubrimiento finito del cubrimiento dado.

La compacidad puede caracterizarse en términos de cerrados en lugar de abiertos:

Una familia $\mathcal{F}$ de subconjuntos de un conjunto X tiene la *propiedad de la intersección finita* si para todo $F \subset \mathcal{F}$ finito se cumple que $\bigcap F \neq \varnothing$.

Teorema 8.54 *Un espacio topológico K es compacto si y sólo si toda familia de cerrados de K con la propiedad de la intersección finita tiene intersección no vacía.*

Demostración: A cada familia $\mathcal{F}$ de cerrados de K le corresponde la familia de abiertos $\mathcal{F}' = \{K \setminus A \mid A \in \mathcal{F}\}$. La condición $\bigcap \mathcal{F} \neq \varnothing$ equivale a que $\mathcal{F}'$ no sea un cubrimiento abierto, mientras que la propiedad de la intersección finita equivale a que $\mathcal{F}'$ no admita subcubrimientos finitos, luego la condición del enunciado equivale a que toda familia de abiertos que no contenga cubrimientos finitos no es un cubrimiento, es decir, a la compacidad de K. ■

Hay muchos espacios que no son compactos pero tienen subespacios compactos. Por ello resulta útil caracterizar la compacidad de un subespacio en

[6] No es raro que se exija la propiedad de Hausdorff en la definición de compacidad. Aquí no lo hacemos.

términos de la topología de todo el espacio y no de la topología relativa. Concretamente:

Teorema 8.55 *Sea X un espacio topológico y K un subespacio de X. Entonces K es compacto si y sólo si para toda familia $\mathcal{C}$ de abiertos (básicos) de X tal que $K \subset \bigcup \mathcal{C}$ se puede extraer una subfamilia finita que cumpla lo mismo.*

DEMOSTRACIÓN: Supongamos que K es compacto. Entonces

$$\{U \cap K \mid U \in \mathcal{C}\}$$

es claramente un cubrimiento abierto de K, del que podemos extraer un subcubrimiento finito de modo que

$$K = (U_1 \cap K) \cup \cdots \cup (U_n \cap K),$$

luego $K \subset U_1 \cup \cdots \cup U_n$.

Recíprocamente, si K cumple esta propiedad y $\mathcal{C}$ es un cubrimiento abierto de K, entonces para cada $U \in \mathcal{C}$ consideramos

$$U^* = \bigcup \{B \subset X \mid B \text{ abierto} \land B \cap K = U\},$$

de modo que U^* es abierto en X y $U^* \cap K = U$. Sea $\mathcal{C}^* = \{U^* \mid U \in \mathcal{C}\}$. Entonces $K = \bigcup \mathcal{C} \subset \bigcup \mathcal{C}^*$, luego por hipótesis existe un subcubrimiento finito tal que $K \subset U_1^* \cup \cdots \cup U_n^*$, luego $K = (U_1^* \cap K) \cup \cdots \cup (U_n^* \cap K) = U_1 \cup \cdots \cup U_n$. Así pues, K es compacto. ■

Si la unión de una familia de abiertos de un espacio X contiene a un subespacio K, diremos que forma un *cubrimiento abierto* de K en X. Así pues, un subespacio K de X es compacto si y sólo si de todo cubrimiento abierto de K en X puede extraerse un subcubrimiento finito (en X también). Aquí estamos considerando la topología de X, pero deberemos tener siempre presente que la compacidad es una propiedad absoluta, es decir, que depende exclusivamente de la topología del propio espacio K.

La compacidad tiene una caracterización muy simple en el caso de la topología de orden:

Teorema 8.56 *Sea X un conjunto totalmente ordenado no vacío, considerado como espacio topológico con la topología de orden. Entonces X es compacto si y sólo si es completo y tiene máximo y mínimo.*

DEMOSTRACIÓN: Si X no tiene máximo, entonces $\{]-\infty, x[\}_{x \in X}$ es un cubrimiento abierto que no admite un subcubrimiento finito, luego X no es compacto. Por lo tanto, si X es compacto tiene máximo, y análogamente se concluye que tiene mínimo.

Si X no fuera completo el teorema 7.35 nos permite descomponerlo como $X = A \cup B$, donde A y B son no vacíos, todo elemento de A es menor que todo elemento de B, y además A no tiene máximo y B no tiene mínimo. Entonces

$$A = \bigcup_{a \in A}]-\infty, a[\,, \qquad B = \bigcup_{b \in B}]b, +\infty[\,,$$

lo que prueba que A y B son abiertos. Además los intervalos considerados forman un cubrimiento abierto de X que no tiene un subcubrimiento finito. Por lo tanto, si X es compacto, es completo.

Recíprocamente, supongamos que X es completo y que tiene máximo M y mínimo m. Podemos suponer que $m < M$, pues si $m = M$ entonces $X = \{m\}$ es obviamente compacto. Sea $\mathcal{C}$ un cubrimiento abierto de X y sea A el conjunto de los $x \in X$ tales que el intervalo $[m, x]$ admite un subcubrimiento finito, es decir:

$$A = \{x \in X \mid \bigvee C \subset \mathcal{C}(C \text{ finito} \wedge [m, x] \subset \bigcup C)\}.$$

Sea $s = \sup A$ y sea $U \in \mathcal{C}$ tal que $s \in U$. No puede ser $s = m$, porque entonces existiría un $v \in X$ tal que $s \in [m, v[\subset U$, y podríamos tomar un $U' \in \mathcal{C}$ tal que $v \in U'$, y entonces $[m, v] \subset U \cup U'$ implicaría que $s < v \in A$, en contradicción con que s es cota superior de A.

Así pues, $m < s$, luego existe un $u < s$ tal que $]u, s] \subset U$. Por definición de supremo existe un $a \in A$ tal que $u < a \leq s$, luego existe $C \subset \mathcal{C}$ finito tal que $[m, a] \subset \bigcup C$, pero cambiando C por $C \cup \{U\}$ tenemos, de hecho, que $[m, s] \subset \bigcup C$, luego $s \in A$.

Ahora basta probar que $s = M$, pero si fuera $s < M$ existiría un $v \in X$ tal que $s \in]u, v[\subset U$ y, tomando $U' \in \mathcal{C}$ tal que $v \in U'$ y añadiéndolo al conjunto finito C, obtendríamos que $[m, v] \subset \bigcup C$, con lo que $v \in A$, lo que contradice de nuevo a que s es cota superior de A. ■

En particular, un ordinal es compacto si y sólo si no es un ordinal límite (puesto que todo ordinal es completo como conjunto ordenado, si no es vacío tiene mínimo y tiene máximo si y sólo si no es un ordinal límite).

Los teoremas siguientes muestran la anunciada similitud entre los espacios compactos y los espacios finitos. Por lo pronto, todo espacio finito es cerrado en un espacio de Hausdorff. El análogo con compactos es el siguiente:

Teorema 8.57 *Se cumplen las propiedades siguientes:*

a) Si X es un espacio de Hausdorff y $K \subset X$ es compacto, entonces K es cerrado en X.

b) Si K es un compacto y $C \subset K$ es un cerrado, entonces C es compacto.

Demostración: a) Veamos que $X \setminus K$ es abierto. Para ello tomamos $x \in X \setminus K$ y vamos a probar que $X \setminus K$ es entorno de x. Sea

$$\mathcal{C} = \{V \subset X \mid V \text{ abierto} \wedge \bigvee U(U \subset X \wedge U \text{ abierto} \wedge U \cap V = \varnothing \wedge x \in U)\}.$$

Tenemos que $\mathcal{C}$ es un cubrimiento abierto de K, pues si $v \in K$ existen abiertos disjuntos U, V en X que separan a x y v, lo que implica que $v \in V \in \mathcal{C}$. Como K es compacto, $\mathcal{C}$ admite un subcubrimiento finito $\{V_1, \ldots, V_n\}$, de modo que $K \subset V_1 \cup \cdots \cup V_n$. Para cada i, existe un abierto U_i tal que $x \in U_i$ y $U_i \cap V_i = \varnothing$. Pero entonces $x \in \bigcap_{i=1}^{n} U_i \subset X \setminus K$, luego K es cerrado.

b) Si $\{A_i\}_{i\in I}$ es un cubrimiento abierto de C, entonces $\{A_i\}_{i\in I} \cup \{K \setminus C\}$ es un cubrimiento abierto de K, luego existe un subcubrimiento finito

$$K = A_{i_1} \cup \cdots \cup A_{i_n} \cup (K \setminus C).$$

Claramente entonces $C \subset A_{i_1} \cup \cdots \cup A_{i_n}$, luego C es compacto. ■

En un conjunto totalmente ordenado, todo subconjunto finito tiene máximo y mínimo. Análogamente:

Teorema 8.58 *Si X es un conjunto totalmente ordenado completo, considerado como espacio topológico con la topología de orden, entonces un subconjunto de X es compacto (con la topología relativa) si y sólo si es cerrado y acotado (superior e inferiormente), y en tal caso tiene máximo y mínimo.*

DEMOSTRACIÓN: Supongamos que $C \subset X$ es cerrado y acotado. Si a es una cota inferior y b es una cota superior, entonces $C \subset [a, b]$. La topología relativa de $[a, b]$ es la topología de orden y, como conjunto ordenado, $[a, b]$ es claramente completo. Por el 8.56 tenemos que $[a, b]$ es compacto, y C también lo es por ser cerrado en $[a, b]$.

Recíprocamente, si C es compacto, entonces sabemos que es cerrado. Si no tuviera máximo $\{]-\infty, x[\}_{x\in X}$ sería un cubrimiento de C que no admitiría un subcubrimiento finito, luego C sí que tiene máximo, e igualmente se prueba que tiene mínimo. ■

En particular, los subconjuntos compactos de $\mathbb{R}$ son los cerrados y acotados. El propio $\mathbb{R}$ no es compacto, pero es lo que se llama un espacio *localmente compacto,* es decir, un espacio en el que todo punto x tiene una base de entornos compactos (por ejemplo, los intervalos $[x - \epsilon, x + \epsilon]$). Por otra parte, $\overline{\mathbb{R}}$ es compacto y, más en general, si X es un precontinuo, entonces $\overline{C(X)}$ es un continuo compacto que tiene a X como subconjunto denso.

Si $f : A \longrightarrow B$ y A es finito, entonces $f[A]$ también es finito. La versión topológica es:

Teorema 8.59 *Si $f : K \longrightarrow X$ es una aplicación continua, K es compacto, entonces $f[K]$ es compacto.*

DEMOSTRACIÓN: Si $\{U_i\}_{i\in I}$ es un cubrimiento abierto de $f[K]$ en X, entonces $\{f^{-1}[U_i]\}_{i\in I}$ es un cubrimiento abierto de K, luego admite un subcubrimiento finito $\{f^{-1}[U_{i_k}]\}_{k=1}^n$, pero entonces es claro que $\{U_{i_k}\}_{k=1}^n$ es un subcubrimiento finito del cubrimiento dado. ■

Como consecuencia:

Teorema 8.60 *Si $f : K \longrightarrow X$ es una aplicación biyectiva y continua, K es compacto y X es un espacio de Hausdorff, entonces f es un homeomorfismo.*

Demostración: Falta probar que f^{-1} es continua, pero eso equivale a que si A es abierto en K, entonces $f[A]$ es abierto en X, o también, tomando complementos, a que si C es cerrado en K, entonces $f[C]$ es cerrado en X, pero si C es cerrado en K, entonces es compacto, luego $f[C]$ es compacto por el teorema anterior, luego $f[C]$ es cerrado en X. ■

Una aplicación de un conjunto finito en un conjunto totalmente ordenado alcanza un valor máximo y un valor mínimo. Igualmente:

Teorema 8.61 *Si $F : K \longrightarrow X$ es una aplicación continua de un compacto K en un conjunto totalmente ordenado, entonces f toma un valor máximo y un valor mínimo.*

Demostración: Tenemos que $f[K]$ es compacto en X, luego tiene máximo y mínimo por el teorema 8.58. ■

En un espacio 1AN, podemos caracterizar mediante sucesiones una propiedad más débil que la compacidad:

Definición 8.62 Un espacio topológico es *numerablemente compacto* si todo cubrimiento abierto numerable admite un subcubrimiento finito.

Obviamente esto equivale a que toda familia numerable de cerrados con la propiedad de la intersección finita tenga intersección no vacía.

Teorema 8.63 (AEN) *Un espacio* 1AN *es numerablemente compacto si y sólo si toda sucesión tiene una subsucesión convergente.*

Demostración: Sea X un espacio numerablemente compacto y sea $\{a_n\}_{n\in\omega}$ una sucesión en K. Sea $A_n = \{a_m \mid m \geq n\}$. Obviamente

$$A_0 \supset A_1 \supset A_2 \supset A_3 \supset A_4 \supset \cdots \quad ,$$

luego también

$$\overline{A}_0 \supset \overline{A}_1 \supset \overline{A}_2 \supset \overline{A}_3 \supset \overline{A}_4 \supset \cdots \quad ,$$

y así tenemos una familia de cerrados con la propiedad de la intersección finita. Por la compacidad numerable existe un punto $x \in \bigcap\limits_{n\in\omega} \overline{A}_n$. Sea $\{U_k\}_{k\in\omega}$ una base decreciente de entornos abiertos de x. Para cada k, $m \in \omega$, tenemos que $U_k \cap A_m \neq \varnothing$, es decir, existe un $n \geq m$ tal que $a_n \in U_k$. Esto nos permite construir por recurrencia una subsucesión de $\{a_n\}_{n\in\omega}$. Tomamos n_0 como el mínimo número natural tal que $a_{n_0} \in U_0$ y definimos n_{k+1} como el menor número natural $n_{k+1} > n_k$ tal que $a_{n_{k+1}} \in U_{k+1}$. Es claro entonces que $\{a_{n_k}\}_{k\in\omega}$ converge a x.

Supongamos ahora que X tiene la propiedad del enunciado y veamos que es numerablemente compacto. Sea $\{U_n\}_{n\in\omega}$ un cubrimiento abierto de X. Queremos probar que admite un subcubrimiento finito. Cambiando cada U_n por $\bigcup\limits_{i\leq n} U_i$ obtenemos un cubrimiento creciente respecto de la inclusión y basta probar que $U_n = X$ para algún n. Si no fuera así, eliminando términos repetidos podríamos suponer además que $U_n \subsetneq U_{n+1}$, para todo n. Entonces podemos tomar $x_n \in U_{n+1} \setminus U_n$, y tenemos así una sucesión $\{x_n\}_{n\in\omega}$ que debería tener una subsucesión convergente a un cierto $x \in X$. Existe entonces un $m \in \omega$ tal que $x \in U_m$, pero entonces la convergencia implica que existe un $k \geq m$ tal que $x_k \in U_m$, pero eso es imposible. ■

Las sucesiones caracterizan la compacidad en los espacios 2AN:

Teorema 8.64 (AEN) *Un espacio* 2AN *es compacto si y sólo si toda sucesión tiene una subsucesión convergente.*

Demostración: Basta probar que si X es numerablemente compacto, entonces es compacto. Pero si $\mathcal{C}$ es un cubrimiento abierto de X y $\mathcal{B}$ es una base numerable, para cada $x \in X$ podemos tomar[7] $B_x \in \mathcal{B}$ tal que existe un $U \in \mathcal{C}$ de modo que $x \in B_x \subset U$. Sea $\mathcal{B}^* = \{B_x \mid x \in X\}$, que es un cubrimiento numerable de X, luego tiene un subcubrimiento finito $B_1, \ldots, B_n$. Para cada B_i podemos tomar un $U_i \in \mathcal{F}$ tal que $B_i \subset U_i$, y así tenemos un subcubrimiento finito del cubrimiento dado. ■

Ejemplo (AEN) El espacio ω_1 es 1AN y es numerablemente compacto por el teorema 8.63, ya que una sucesión en ω_1 no puede ser cofinal, luego está contenida en un intervalo $[0, \alpha]$, que es compacto, luego tiene una subsucesión convergente. Sin embargo ω_1 no es compacto, por el teorema 8.56. ■

Para terminar nos ocupamos del producto de espacios compactos:

Teorema 8.65 (Tychonoff) (AE) *Todo producto de espacios compactos es compacto.*

Nota Este teorema no sólo requiere el axioma de elección, sino que de hecho es equivalente a él. En efecto, tomemos una familia $\{X_i\}_{i\in I}$ de conjuntos no vacíos. Aceptando el teorema de Tychonoff vamos a probar que $\prod\limits_{i\in I} X_i \neq \varnothing$, lo que, por la observación tras 3.27, equivale al axioma de elección.

Sea $p \in V \setminus \bigcup\limits_{i\in I} X_i$ y sea $Y_i = X_i \cup \{p\}$. Consideramos a cada Y_i como espacio topológico con la topología que tiene por cerrados a Y_i, X_i y los conjuntos finitos. Se comprueba sin dificultad que realmente es una topología (no de Hausdorff, pues p está en todo entorno de todo punto de X_i). Además Y_i es un espacio compacto, pues, dado un cubrimiento abierto $\mathcal{C}$ de Y_i, tomamos un punto $x \in X_i$ y un abierto $U \in \mathcal{C}$ tal que $x \in U$, pero entonces U contiene todos los puntos de Y_i salvo a lo sumo un número finito de ellos, luego tomando un abierto de $\mathcal{C}$ para cada uno de los puntos de $Y_i \setminus U$ obtenemos un subcubrimiento finito.

Por lo tanto, tenemos que $Y = \prod\limits_{i\in I} Y_i$ es compacto. Para cada $i \in I$, sea

$$Z_i = \{f \in Y \mid f(i) \in X_i\}.$$

[7]Para elegir en un conjunto numerable n se necesita el axioma de elección.

Se trata de un cerrado, pues $Y \setminus Z_i = \bigcup_{i \in I} p_i^{-1}[\{p\}]$ y $\{p\}$ es abierto en Y_i. Además, la familia $\{Z_i \mid i \in I\}$ tiene la propiedad de la intersección finita, pues si $I_0 \subset I$ es finito, podemos tomar $s \in \prod_{i \in I_0} X_i$ (porque los conjuntos finitos siempre tienen funciones de elección) y extenderlo a Y mediante $s(i) = p$ para $i \in I \setminus I_0$, con lo que obtenemos un $s \in \bigcap_{i \in I_0} Z_i$. Por la compacidad existe $f \in \bigcap_{i \in I} Z_i$, con lo que $f \in \prod_{i \in I} X_i \neq \varnothing$. ■

En 10.53 daremos una prueba conceptualmente simple del teorema de Tychonoff. Aquí daremos un argumento que muestra explícitamente cómo interviene en la prueba el axioma de elección, de modo que veremos que en muchos casos particulares de interés no se necesita realmente. Por ejemplo, veremos que la prueba de que el producto de un número finito de espacios compactos es compacto no requiere AE, y esto es lo único que requiere la consecuencia siguiente:

Teorema 8.66 *Un subconjunto de $\mathbb{R}^n$ es compacto si y sólo si es cerrado y acotado.*

Aquí entendemos que un subconjunto de $\mathbb{R}^n$ está *acotado* si está contenido en un cubo $[-M, M]^n$, para cierto $M > 0$.

Demostración: Si C es cerrado y $C \subset [-M, M]^n$ para cierto $M > 0$, por el teorema de Tychonoff el cubo es compacto, y C también lo es por ser cerrado en un compacto.

Recíprocamente, si $C \subset \mathbb{R}^n$ es compacto, sabemos que tiene que ser cerrado, y los cubos $\{]-k, k[^n\}_{k \in \omega}$ forman un cubrimiento abierto de C, luego tiene que tener un subcubrimiento finito, y si tomamos el máximo k que aparece en dicho subcubrimiento, resulta que $C \subset]-k, k[^n \subset [-k, k]^n$, luego está acotado. ■

El teorema de Tychonoff es consecuencia inmediata del teorema siguiente:

Teorema 8.67 *Sea $\{X_i\}_{i \in I}$ una familia de espacios topológicos compactos. Supongamos que I admite un buen orden y que, si I es infinito, existe una función de elección sobre el conjunto de todos los cerrados en todos los espacios X_i. Entonces el producto $X = \prod_{i \in I} X_i$ es compacto.*

Demostración: No perdemos generalidad si sustituimos I por un ordinal α. Podemos suponer que $X \neq \varnothing$, pues si no la conclusión es trivial.

Sea $\mathbb{P} = \bigcup_{\beta \leq \alpha} X^\beta$, considerado como conjunto parcialmente ordenado por la inclusión. Definimos la *altura* de un $p \in \mathbb{P}$ como $\operatorname{alt} p = \mathcal{D}p$, es decir, el único ordinal $\beta \leq \alpha$ tal que $p \in X^\beta$. Así, los elementos de X son los elementos de $\mathbb{P}$ de altura α.

Para cada $p \in \mathbb{P}$ llamaremos $M(p) = \{x \in X \mid p \subset x\}$. Notemos que $M(p) \neq \varnothing$, pues, como estamos suponiendo que X no es vacío, podemos tomar $x \in X$ y, si $\operatorname{alt} p = \beta$, basta considerar $p' = p \cup (x|_{\lambda \setminus \beta}) \in M(p)$.

Fijemos un cubrimiento abierto $\mathcal{C}$ de X. No perdemos generalidad si suponemos que sus elementos son abiertos básicos del producto.

Sea A el conjunto de todos los $p \in \mathbb{P}$ tales que $M(p)$ no está contenido en ninguna unión finita de abiertos de $\mathcal{C}$. Basta probar que $A = \varnothing$, pues entonces $X = M(\varnothing)$ está contenido en una unión finita de abiertos de $\mathcal{C}$. Suponemos, pues, que $A \neq \varnothing$. Notemos que si $p \in A$ y $q \subset p$ entonces $M(p) \subset M(q)$, luego $q \in A$.

Llamaremos $A^\beta = A \cap X^\beta$, el conjunto de los elementos de A de altura β. Veamos que si $\beta < \alpha$ y $s \in A^\beta$, entonces $C(s) = \{t(\beta) \mid t \in A \land s \subsetneq t\}$ es cerrado en X_β. Para ello tomamos un $a \in X_\beta \setminus C(s)$ y vamos a encontrar un abierto $a \in U \subset X_\beta \setminus C(s)$.

Sea $t = s \cup \{(\beta, a)\} \in X^{\beta+1}$. Como t no puede justificar que $a \in C(s)$, necesariamente $t \notin A$, luego $M(t) \subset \bigcup G$, para cierto $G \subset \mathcal{C}$ finito. Reduciendo G si es preciso podemos suponer que todo $V \in G$ corta a $M(t)$.

Cada $V \in G$ es un abierto básico, de la forma $\bigcap\limits_{\delta \in J_V} p_\delta^{-1}[W_{V\delta}]$, donde $J_V \subset \alpha$ es finito y $W_{V\delta}$ es abierto en X_δ. Podemos suponer que $\beta \in J_V$ añadiendo si es preciso $W_{V\beta} = X_\beta$. Como $V \cap M(t) \neq \varnothing$, existe un $x \in V$ tal que $x|_{\beta+1} = t$, luego $a = x(\beta) \in W_{V\beta}$. Sea $U = \bigcap\limits_{V \in G} W_{V\beta}$, que es un entorno abierto de a.

Veamos que $\{x \in X \mid s \subset x \land x(\beta) \in U\} \subset \bigcup G$.

En efecto, si $x \in X$ cumple que $s \subset x \land x(\beta) \in U$, sea $y \in X$ la aplicación que coincide con x salvo por que $y(\beta) = a$. Entonces $t \subset y$, luego $y \in M(t)$, luego existe un $V \in G$ tal que $y \in V = \bigcap\limits_{\delta \in J_V} p_\delta^{-1}[W_{V\delta}]$. Como $x(\beta) \in U \subset W_{V\beta}$, es claro entonces que $x \in V$, luego $x \in \bigcup G$. Por consiguiente $U \subset X_\beta \setminus C(s)$, como había que probar.

Veamos ahora que $C(s) \neq \varnothing$. En caso contrario, el paso anterior prueba que la familia de todos los abiertos U en X_i tales que $\{x \in X \mid s \subset x \land x(\beta) \in U\}$ está contenido en una unión finita de elementos de $\mathcal{C}$ es un cubrimiento abierto de X_β (pues hemos probado que cubre a $X_\beta \setminus C(s)$). Por la compacidad de X_β podríamos extraer un subcubrimiento finito $X_\beta = \bigcup\limits_{k<n} U_k$, pero entonces

$$M(s) = \bigcup_{k<n} \{x \in X \mid s \subset x \land x(\beta) \in U_k\}$$

estaría contenido en una unión finita de elementos de $\mathcal{C}$, en contra de que $s \in A$.

En particular tenemos que si $s \in A$ tiene altura $\beta < \alpha$, entonces existe un $t \in A$ tal que $s \subsetneq t$. Si α es finito, esto basta para concluir que existe un $p \in A$ de altura α (pues podemos considerar la máxima altura de un elemento de A y acabamos de probar que no puede ser menor que α), pero esto es absurdo, porque entonces $p \in X$ y $M(p) = \{p\}$ no debería estar contenido en una unión finita de elementos de $\mathcal{C}$, y esto contradice que $\mathcal{C}$ sea un cubrimiento de X. Así pues, si α es finito tenemos que $A = \varnothing$ y X es compacto.

A partir de aquí suponemos que α es un ordinal infinito y por hipótesis contamos con una función de elección e que a cada cerrado $C \neq \varnothing$ de cada X_i le asigna un elemento $e(C) \in C$. Vamos a definir recurrentemente una sucesión $\{s_\delta\}_{\delta\leq\alpha}$ de modo que $s_\delta \in A^\delta$ y $\bigwedge\delta\epsilon(\delta \leq \epsilon < \alpha \rightarrow s_\delta \subset s_\epsilon)$.

Tomamos $s_0 = \varnothing$. Si $\delta < \alpha$, definimos $s_{\delta+1} \in A^{\delta+1}$ como el único elemento que cumple $s_\delta \subset s_{\delta+1} \wedge s_{\delta+1}(\delta) = e(C(s_\delta))$. Por último, si $\lambda < \alpha$, definimos $s_\lambda = \bigcup\limits_{\delta<\lambda} s_\delta$ y veamos que $s_\lambda \in A^\lambda$. En principio tenemos que $s_\lambda \in X^\lambda$, pero falta probar que $s_\lambda \in A$. En caso contrario, existe $G \subset \mathcal{C}$ finito tal que $M(s_\lambda) \subset \bigcup G$. Podemos suponer que todo $V \in G$ corta a $M(s_\lambda)$.

Como antes, cada $V \in G$ es de la forma $\bigcap\limits_{\delta\in J_V} p_\delta^{-1}[W_{V\delta}]$, donde $J_V \subset \alpha$ es finito y $W_{V\delta}$ es abierto en X_δ. Sea $J = \bigcup\limits_{V\in G} J_V$, que es un subconjunto finito de α. Sea $\beta < \lambda$ una cota superior de $J \cap \lambda$. Vamos a ver que $M(s_\beta) \subset \bigcup G$, en contradicción con que $s_\beta \in A$. En efecto, observemos en primer lugar que, para todo $V \in G$, como existe un $y \in V \cap M(s_\lambda)$, para cada $\delta \in J_V \cap \lambda$ tenemos que $s_\lambda(\delta) = y(\delta) \in W_{V\delta}$.

Si $x \in M(s_\beta)$, sea $y = s_\lambda \cup x|_{\alpha\setminus\lambda}$. Entonces $y \in M(s_\lambda)$, luego existe un $V \in G$ tal que $y \in V = \bigcap\limits_{\delta\in J_V} p_\delta^{-1}[W_{V\delta}]$, pero entonces $x \in V$, porque x e y sólo se distinguen bajo λ y $x(\delta) \in W_{V\delta}$ para todo $\delta \in J_V \cap \lambda$. Esto prueba que $M(s_\beta) \subset \bigcup G$, como había que probar.

Con esto concluimos que $s_\lambda \in A^\lambda$, luego tenemos definida la sucesión $\{s_\delta\}_{\delta\leq\alpha}$, y en particular s_α, que es un elemento de A de altura α, lo que nos lleva a la misma contradicción que el caso en que α era finito. ■

Así pues, no se necesita AE para demostrar que el producto de una familia finita de espacios topológicos compactos es compacto, ni tampoco para el caso en que I admite un buen orden y cada X_i es un subespacio compacto de $\mathbb{R}$. En efecto, en tal caso, en virtud de 8.58, podemos definir una función de elección sobre los cerrados de los espacios X_i sin más que tomar $e(C) = \min C$, luego es aplicable el teorema anterior. En particular, podemos afirmar sin AE la compacidad de los espacios $[0,1]^\alpha$ o 2^α, para cualquier ordinal α.

Por último, para probar que el producto de una familia numerable de compactos es compacto sólo necesitamos el principio ED de elecciones dependientes. Esto no se sigue del teorema anterior, sino de una ligera modificación de la parte final de la demostración. En este caso podemos tomar $\alpha = \omega$ y basta observar que no necesitamos la función de elección e para construir la sucesión $\{s_n\}_{n\in\omega}$, sino que basta considerar en A la relación dada por

$$t\,R\,s \leftrightarrow s \subset t \wedge \operatorname{alt} t = \operatorname{alt} s + 1.$$

Como $C(s) \neq \varnothing$, tenemos que $\bigwedge s \in A \bigvee t \in A\; t\,R\,s$, y ED es aplicable. A partir de ahí se define $s_\omega = \bigcup\limits_{n\in\omega} s_n$ y el argumento de la prueba vale sin cambio alguno para concluir que $s_\omega \in A$, lo que nos lleva a a contradicción.

Capítulo IX

Árboles

El concepto de árbol aparece en contextos matemáticos muy dispares, que abarcan desde problemas combinatorios finitistas hasta problemas sobre cardinales infinitos. De hecho, nosotros nos lo hemos encontrado ya, aunque de forma implícita, en la demostración que hemos dado en el capítulo anterior del teorema de Tychonoff.

Un problema conjuntista destacado en cuyo análisis resulta fundamental el concepto de árbol es 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. 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.

9.1 El problema de Suslin

El teorema 7.42 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* $\mathbb{R}$.

Sabemos que 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 9.1 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.*[1]

En efecto:

Teorema 9.2 *Son equivalentes:*

a) Existe un conjunto totalmente ordenado con la condición de cadena numerable no separable.

b) Existe un conjunto ordenado denso en sí mismo, sin extremos, con la condición de cadena numerable y en la que ningún intervalo es separable.

c) Existe una recta de Suslin en la que ningún intervalo es separable.

d) Existe una recta de Suslin.

Demostración: Sólo hay que probar que a) $\Rightarrow$ b) y que b) $\Rightarrow$ c).

Sea Y un conjunto totalmente ordenado que cumpla a) 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 b).

[1]Notemos que un subconjunto D de un precontinuo X es denso (en el sentido topológico) si y sólo si $\bigwedge xy \in X(x < y \rightarrow \bigvee d \in D\ x < d < y)$, pero esto no es cierto en conjuntos totalmente ordenados cualesquiera. En este contexto hay que entender la densidad en el sentido topológico general.

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 $D = \bigcup\limits_{n \in \omega} D_n \subset I$ 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 α, $\beta < \omega_1$.

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 $H = \bigcup\limits_{[x] \leq L \leq [y]} L \subset Y$. 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 b) salvo por el hecho de que puede tener máximo o mínimo elemento. Ahora bien, como X es denso en sí mismo, si eliminamos los posibles máximo y mínimo, obtenemos un nuevo conjunto ordenado ya no tiene máximo ni mínimo y sigue cumpliendo las otras propiedades.

Ahora veamos que b) implica c). Sea X un conjunto totalmente ordenado en las condiciones de b) y sea $W = C(X)$ la compleción de X en el sentido de 7.38, 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. ■

Así pues, 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. Este problema está relacionado con otro que ya hemos planteado:[2] si el producto de espacios topológicos (o, más en particular, de continuos) con la condición de cadena numerable tiene la condición de cadena numerable, entonces se cumple HS. En efecto:

Teorema 9.3 *Si X es un conjunto totalmente 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:

a) $a_\alpha < b_\alpha < c_\alpha$,

b) $]a_\alpha, b_\alpha[\, \neq \varnothing \neq\,]b_\alpha, c_\alpha[$

c) $]a_\alpha, c_\alpha[\, \cap \{b_\beta \mid \beta < \alpha\} = \varnothing$.

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.

[2]Véase las observaciones anteriores y posteriores al teorema 8.50.

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 $D = W \cup \{a_\alpha \mid \alpha < \beta\} \cup \{b_\alpha \mid \alpha < \beta\} \cup \{c_\alpha \mid \alpha < \beta\}$ es un conjunto numerable, luego $X \setminus \overline{D} \neq \varnothing$. Como es un abierto no vacío, contiene un intervalo abierto no vacío, contendrá un intervalo abierto no vacío $]a_\alpha, c_\alpha[$ que, como no contiene puntos aislados, es infinito, luego contiene un b_α que lo divide en dos intervalos no vacíos. ■

9.2 Conceptos básicos sobre árboles

En esta sección no usaremos AE si no lo indicamos explícitamente.

Definición 9.4 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 $\operatorname{alt}_A x = \operatorname{ord} A_x^<$.

Si $\alpha \in \Omega$, se llama *nivel* α-ésimo de A al conjunto

$$\operatorname{Niv}_\alpha A = \{x \in A \mid \operatorname{alt}_A x = \alpha\}.$$

Se llama *altura* de A al mínimo ordinal $\operatorname{alt} A = \alpha$ tal que $\operatorname{Niv}_\alpha A = \varnothing$. Es fácil ver que

$$\operatorname{alt} A = \bigcup_{x \in A} (\operatorname{alt}_A x + 1).$$

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,[3] 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

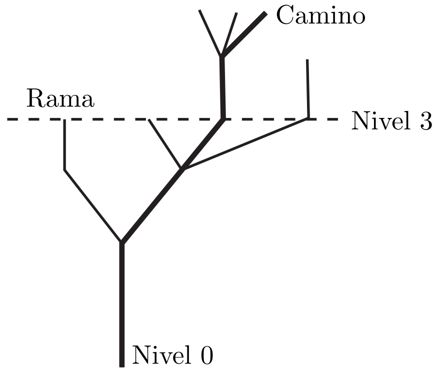
$$\operatorname{alt}_A R = \operatorname{ord} R = \bigcup_{x \in R} (\operatorname{alt}_A x + 1).$$

Un subconjunto $C \subset A$ es un *camino* si es una rama tal que $\operatorname{alt}_A C = \operatorname{alt} A$, 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:

[3]Basta observar que el conjunto de todas las cadenas que contienen a una dada cumple las hipótesis del lema de Zorn.



Un subconjunto $A' \subset A$ es un *subárbol* de A si

$$\bigwedge x \in A \bigwedge y \in A'(x < y \rightarrow x \in A').$$

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

$$\bigwedge x \in A \bigwedge \alpha < \kappa(\mathrm{alt}_A x < \alpha \rightarrow \bigvee y \in \mathrm{Niv}_\alpha A\ x < y).$$

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:

Teorema 9.5 (AE) *Si κ es un cardinal regular,*[4] *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 $x \in A'$.

[4] 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.

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

$$\{z \in A \mid x < z\} = \{z \in A \mid x < z \land \mathrm{alt}_A z \leq \alpha\} \cup \{z \in A \mid x < z \land \mathrm{alt}_A z > \alpha\}.$$

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 $\bigcup\limits_{\beta \leq \alpha} \mathrm{Niv}_\beta A$, κ es regular y los niveles tienen cardinal menor que κ.

Por consiguiente, el tercer conjunto ha de tener cardinal κ, pero

$$\{z \in A \mid x < z \land \mathrm{alt}_A z > \alpha\} = \bigcup_{y \in Y} \{z \in A \mid y < z \land \mathrm{alt}_A z > \alpha\},$$

y $|Y| \leq |\mathrm{Niv}_\alpha A| < \kappa$, por lo que ha de existir un $y \in Y$ tal que[5]

$$|\{z \in A \mid y < z \land \mathrm{alt}_A z > \alpha\}| = \kappa.$$

En particular $|\{z \in A \mid x < z\}| = \kappa$, con lo que $y \in A'$. Así hemos probado que

$$\bigwedge x \in A' \bigwedge \alpha < \kappa (\mathrm{alt}_A x < \alpha \rightarrow \bigvee y \in \mathrm{Niv}_\alpha A' \; x < y).$$

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 $A = \bigcup\limits_{\delta<\mu} \alpha_\delta \times \{\delta\}$, 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:

Teorema 9.6 (König) (AEN) *Todo $\aleph_0$-árbol tiene un camino.*[6]

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:

[5] Notemos que la condición $\mathrm{alt}_A z > \alpha$ es redundante, pues se sigue de la definición de Y.

[6] 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.

Teorema 9.7 (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 $\delta < \operatorname{alt}_A x$, representaremos por $x|_\delta$ al único elemento de $\operatorname{Niv}_\delta(A)$ 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, $b \in \operatorname{Niv}_\lambda(A)$, 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 $a \in \operatorname{Niv}_\lambda(A)$. (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 $|\mathcal{C}_\lambda| \leq |\operatorname{Niv}_\lambda(A)| < \mu$.

Consideramos ahora $A' = A \cup \bigcup\limits_{\lambda<\kappa} \mathcal{C}_\lambda$ 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 $\operatorname{Niv}_\lambda(A') = \mathcal{C}_\lambda$. 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 $\operatorname{Niv}_\lambda(A)$ 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 $\operatorname{cf} \lambda = \mu$, elijamos un $x_\lambda \in \operatorname{Niv}_\lambda(A)$. Para cada $x \in \operatorname{Niv}_\lambda(A)$ distinto de x_λ existe un $\delta < \lambda$ tal que $x_\lambda|_\delta \neq x|_\delta$. Como $|\operatorname{Niv}_\lambda(A)| < \mu = \operatorname{cf} \lambda$, podemos tomar un $f(\lambda) < \lambda$ tal que para todo $x \in \operatorname{Niv}_\lambda(A) \setminus \{x_\lambda\}$ se cumple que $x_\lambda|_{f(\alpha)} \neq x|_{f(\alpha)}$.

Ahora usamos que $E = \{\lambda < \kappa \mid \operatorname{cf} \lambda = \mu\}$ 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 $|\operatorname{Niv}_\gamma(A)| < \mu$, 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 $A' = \bigcup\limits_{\alpha\in X} \mathrm{Niv}_\alpha(A)$ 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. ■

9.3 Árboles de Aronszajn

Los dos últimos teoremas 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 9.8 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.

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 9.9 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 9.10 (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 $f = \bigcup\limits_{a\in C} a$ 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

a) $s_\alpha \in {}^\alpha\omega$ es inyectiva,

b) Si $\alpha < \beta < \omega_1$, entonces $s_\alpha \approx s_\beta|_\alpha$,

c) $\omega \setminus s_\alpha[\alpha]$ 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 $t_n \approx s_{\alpha_n} \land t_{n+1}|_{\alpha_n} = t_n$.

Supuesto que estén definidas $t_0, \ldots, t_n$, definimos $t_{n+1} : \alpha_{n+1} \longrightarrow \omega$ mediante

$$t_{n+1}(\beta) = \begin{cases} t_n(\beta) & \text{si } \beta < \alpha_n, \\ s_{\alpha_{n+1}}(\beta) & \text{si } \alpha_n \leq \beta \text{ y } s_{\alpha_{n+1}}(\beta) \notin t_n[\alpha_n], \\ \min(\omega \setminus (t_n[\alpha_n] \cup s_{\alpha_{n+1}}[\alpha_{n+1}])) & \text{si } \alpha_n \leq \beta \text{ y } s_{\alpha_{n+1}}(\beta) \in t_n[\alpha_n]. \end{cases}$$

Como s_{α_n} coincide con t_n salvo en un número finito de casos, sólo puede ocurrir $s_{\alpha_{n+1}}(\beta) \in t_n[\alpha_n]$ en un número finito de casos. Por lo tanto se cumple $s_{\alpha_{n+1}} \approx t_{n+1}$.

Sea $t = \bigcup\limits_{n\in\omega} t_n$. 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 $A^* = \bigcup\limits_{\alpha<\omega_1} \{t \in \mathrm{Niv}_\alpha A \mid t \approx s_\alpha\}$. 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,

$$\mathrm{Niv}_\alpha A^* = \{t \in {}^\alpha\omega \mid t \approx s_\alpha \land t \text{ inyectiva}\} \subset \bigcup_{\substack{x\subset\alpha \\ \text{finito}}} \{t \in {}^\alpha\omega \mid t|_{\alpha\setminus x} = s_\alpha|_{\alpha\setminus x}\},$$

y el miembro derecho es una unión numerable de conjuntos numerables. Concluimos que A^* es un árbol de Aronszajn. ■

Más en general:

Definición 9.11 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 9.5 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 9.12 *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 9.10, así que podemos suponer que $\kappa > \aleph_0$. Siguiendo el argumento de 9.10, 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

a) $s_\alpha \in {}^\alpha\kappa$ es inyectiva,

b) Si $\alpha < \beta < \kappa^+$, entonces $s_\alpha \approx s_\beta|_\alpha$,

c) $s_\alpha[\alpha]$ 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 $C = \bigcap\limits_{\eta<\nu} C_\eta$, y si $\nu = \kappa$, entonces sea $C = \mathop{\triangle}\limits_{\eta<\kappa} C_\eta \setminus \{0\}$. 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 $s_\lambda = \bigcup\limits_{\eta<\nu} t_\eta : \lambda \longrightarrow \kappa \setminus C$ 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 $A^* = \bigcup\limits_{\alpha<\kappa^+} \{t \in \operatorname{Niv}_\alpha A \mid t \approx s_\alpha\}$, que es un subárbol de A, luego no tiene cadenas de cardinal κ y, como $s_\alpha \in \operatorname{Niv}_\alpha A^*$, vemos que $\operatorname{alt} A^* = \kappa^+$. Finalmente,

$$\operatorname{Niv}_\alpha A^* = \{t \in {}^\alpha\kappa \mid t \approx s_\alpha \wedge t \text{ inyectiva}\} \subset \bigcup_{x\in[\alpha]^{<\kappa}} \{t \in {}^\alpha\kappa \mid t|_{\alpha\setminus x} = s_\alpha|_{\alpha\setminus x}\},$$

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 9.13 (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.*

El caso del sucesor de un cardinal singular lo consideraremos de nuevo en la sección siguiente (véase el teorema 9.21 y la nota posterior).

9.4 Árboles de Suslin

Vamos a probar que la existencia de rectas de Suslin es equivalente a la existencia de un árbol de Suslin:

Definición 9.14 Un *κ-árbol de Suslin* es un κ-árbol cuyas cadenas y anticadenas tienen todas cardinal $< \kappa$. En particular, todo κ-árbol de Suslin es un κ-árbol de Aronszajn. Un *árbol de Suslin* es un $\aleph_1$-árbol de Suslin.

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 9.15 *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 $\mathrm{alt}\, C < \alpha$. 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 9.16 *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 $\operatorname{alt}_A x_\alpha \geq \bigcup\limits_{\beta<\alpha} \operatorname{alt} f(x_\alpha)$. Así $\{f(x_\alpha)\}_{\alpha<\kappa}$ es una anticadena no numerable en A, contradicción. ■

Finalmente obtenemos la caracterización anunciada de la hipótesis de Suslin:

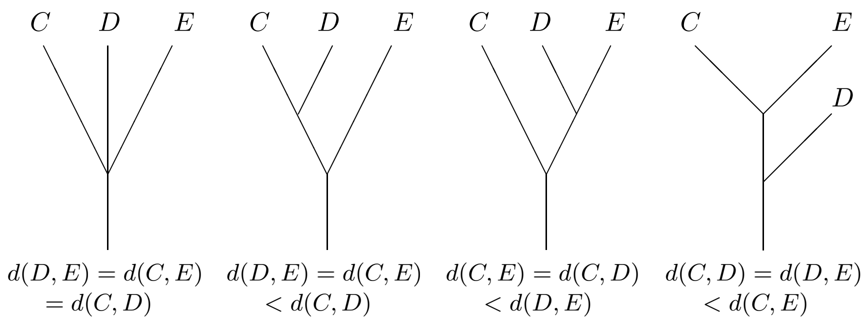
Teorema 9.17 *Existe un árbol de Suslin si y sólo si existe una recta de Suslin.*

Demostración: Supongamos que A es un árbol de Suslin. Podemos suponer que está bien podado. Sea L el conjunto de todas las ramas de A. Si $C \in L$, del hecho de que A está bien podado se sigue que $\operatorname{alt} C$ es un ordinal límite. Si $\alpha < \operatorname{alt} C$, llamaremos $C(\alpha)$ al único elemento en C de altura α. Si C, $D \in L$, $C \neq D$, llamaremos $d(C, D)$ al mínimo ordinal α tal que $C(\alpha) \neq D(\alpha)$. Claramente $d(C, D) < \operatorname{alt} C \cap \operatorname{alt} D$.

Fijemos un orden total $\preceq$ en A y definamos 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 que $C < D < E$. Tenemos las posibilidades siguientes:



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. Veamos que cumple la condición de cadena numerable. Supongamos que $\{]C_\alpha, D_\alpha[\}_{\alpha<\omega_1}$ 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 $\{E_\alpha(\beta_\alpha)\}_{\alpha<\omega_1}$ es una anticadena en A, en contradicción con la definición de árbol de Suslin.

En caso contrario $E_\alpha(\beta_\alpha) \leq E_{\alpha'}(\beta_{\alpha'})$, para ciertos α, $\alpha' < \omega_1$. Claramente entonces, $E_\alpha(\beta_\alpha) = E_{\alpha'}(\beta_\alpha)$ y así

$$d(E_\alpha, E_{\alpha'}) > \beta_\alpha > d(C_\alpha, E_\alpha) \cup d(E_\alpha, D_\alpha),$$

luego $d(C_\alpha, E_{\alpha'}) = d(C_\alpha, E_\alpha)$ y $d(E_\alpha, D_\alpha) = d(E_{\alpha'}, D_\alpha)$. Pero entonces las desigualdades $C_\alpha < E_\alpha < D_\alpha$ implican $C_\alpha < E_{\alpha'} < D_\alpha$, con lo que

$$E_{\alpha'} \in \,]C_\alpha, D_\alpha[\, \cap \,]C_{\alpha'}, D_{\alpha'}[\, = \varnothing,$$

contradicción.

Veamos, por último, que L no es separable. Supongamos que D es un subconjunto denso numerable en L. Las alturas de las ramas de D son ordinales numerables. Sea $\delta < \omega_1$ mayor que cualquiera de ellas y sea $x \in \operatorname{Niv}_\delta A$. Como A está ramificado, existe un ordinal $\delta < \alpha < \omega$ tal que existen r, s, $t \in \operatorname{Niv}_\alpha A$ 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.

Por consiguiente, L cumple 9.2 a), lo que implica que existe una recta de Suslin.

Supongamos ahora que existe una recta de Suslin L. Por 9.2 podemos suponer que no tiene intervalos separables. Llamemos B al conjunto de los intervalos abiertos no vacíos de L. Vamos a construir una sucesión $\{B_\alpha\}_{\alpha<\omega_1}$ que cumpla lo siguiente:

a) $B_\alpha \subset B$ y está formado por intervalos disjuntos dos a dos,

b) $\bigcup\limits_{x \in B_\alpha} x$ es denso en L,

c) Si $\alpha < \beta < \omega_1$, $I \in B_\alpha$, $J \in B_\beta$, entonces o bien $I \cap J = \varnothing$ o bien $J \subsetneq I$.

Para empezar tomamos como B_0 una familia maximal de intervalos disjuntos dos a dos. Por ser maximal $\bigcup\limits_{x \in B_0} x$ es denso en L.

Supongamos definido B_α. Para cada $I \in B_\alpha$, sea H_I una familia maximal de elementos disjuntos del conjunto $\{K \in B \mid K \subsetneq I\}$. Sea $B_{\alpha+1} = \bigcup\limits_{I \in B_\alpha} H_I$.

Es claro que $B_{\alpha+1}$ cumple a) y c). Veamos b). Para ello tomamos un intervalo abierto no vacío $J \in B$ y hemos de probar que corta a algún intervalo de $B_{\alpha+1}$. Sabemos que corta a un $I \in B_\alpha$. Como L es denso en sí mismo, dentro de $J \cap I$ podemos tomar un intervalo no vacío estrictamente contenido en I. De hecho, podemos suponer que $J \subsetneq I$. Entonces J ha de cortar a algún intervalo de $H_I \subset B_{\alpha+1}$, o si no podríamos añadirlo a H_I contradiciendo la maximalidad de éste.

Supongamos definidos $\{B_\alpha\}_{\alpha<\lambda}$, para un límite $\lambda < \omega_1$. Sea

$$H = \{K \in B \mid \bigwedge \delta < \lambda \bigwedge I \in B_\delta (I \cap K = \varnothing \vee H \subsetneq I)\}.$$

Tomamos como B_λ una familia maximal de intervalos disjuntos en H. En realidad hemos de probar que $H \neq \varnothing$, pero esto está implícito en la prueba de que B_λ cumple b). Sea $J \in B$ y veamos que corta a un intervalo de B_λ.

Como L cumple la condición de cadena numerable, cada B_α es numerable, luego $\bigcup\limits_{\delta<\lambda} B_\delta$ también lo es. Sea E el conjunto de los extremos de los intervalos de esta unión, numerable también. Como J no es separable $E \cap J$ no es denso en J, luego existe un intervalo $K_1 \in B$, $K_1 \subset J$, $K_1 \cap E = \varnothing$.

Como L es denso en sí mismo, podemos tomar $K_2 \in B$, $K_2 \subsetneq K_1$. Entonces $K_2 \in H$, pues si $\delta < \lambda$ e $I \in B_\delta$, los extremos de I están en E, luego no están en K_1, luego $K_1 \cap I = \varnothing$ o bien $K_1 \subset I$. Consecuentemente, $K_2 \cap I = \varnothing$ o bien $K_2 \subsetneq I$. Por la maximalidad de B_λ, el intervalo K_2 ha de cortar a alguno de sus intervalos, luego J también. Obviamente B_λ cumple a) y c).

Llamemos $A = \bigcup\limits_{\alpha<\omega_1} B_\alpha$ con el orden dado por la inversa de la inclusión. Vamos a probar que es un árbol. Tomamos $x \in A$ y hemos de ver que $A_x^<$ está bien ordenado. En primer lugar probaremos que está totalmente ordenado. Tomemos u, $v \in A_x^<$. Esto significa que $x \subset u \cap v \neq \varnothing$. Es claro entonces que $u \subset v$ o $v \subset u$.

Tomemos ahora $C \subset A_x^<$ no vacío y veamos que tiene mínimo. Sea α el mínimo ordinal tal que $C \cap B_\alpha \neq \varnothing$. Sea $u \in C \cap B_\alpha$. Veamos que u es el mínimo de C. En caso contrario (puesto que C está totalmente ordenado) existiría $v \in C$ tal que $v < u$, o sea, $u \subsetneq v$. Digamos que $v \in B_\beta$, donde $\beta \geq \alpha$ por la minimalidad de α. Ahora bien, si $\beta = \alpha$ entonces u y v tendrían que ser disjuntos, luego $\beta > \alpha$, pero entonces tendría que ser $v \subsetneq u$, contradicción.

Tenemos, pues, que A es un árbol. Una anticadena en A está formada por intervalos de L disjuntos dos a dos, luego ha de ser numerable.

Si $\{I_\alpha\}_{\alpha<\omega_1}$ fuera una cadena en A, para $\alpha < \omega_1$ se cumpliría que $I_{\alpha+1} \subsetneq I_\alpha$, y como L es denso en sí mismo $I_\alpha \setminus I_{\alpha+1}$ contendría un intervalo abierto no vacío J_α. Entonces $\{J_\alpha\}_{\alpha<\omega_1}$ sería una familia de intervalos en L disjuntos dos a dos, contradicción. Por lo tanto A es un árbol de Suslin. ■

Así pues, ahora tenemos una expresión alternativa para la hipótesis de Suslin:

Hipótesis de Suslin (HS) *No existen árboles de Suslin*

Según ya hemos advertido, en NBG no puede probarse la existencia de árboles de Suslin, pero sí podemos construir uno si suponemos el diamante. Con su ayuda construiremos un árbol de Suslin definiendo un orden adecuado sobre ω_1. Primeramente demostramos un hecho técnico.

Teorema 9.18 *Sea κ un cardinal regular y $B = (\kappa, \leq^*)$ un κ-árbol. Para cada $\alpha < \kappa$ sea $B_\alpha = \{x \in \kappa \mid \mathrm{alt}_B x < \alpha\}$ y sea A una anticadena maximal de B. Entonces el conjunto*

$$\{\lambda < \kappa \mid B_\lambda = \lambda \wedge B_\lambda \cap A \text{ es una anticadena maximal en } B_\lambda\}$$

es c.n.a. en κ.

DEMOSTRACIÓN: Sea C el conjunto del enunciado. Supongamos que $\lambda < \kappa$ es un ordinal límite tal que $C \cap \lambda$ no está acotado en λ. Entonces para todo $x \in B$ se cumple que

$$x \in B_\lambda \leftrightarrow \mathrm{alt}_B x < \lambda \leftrightarrow \bigvee \delta \in C \cap \lambda\ \mathrm{alt}_B x < \delta$$
$$\leftrightarrow \bigvee \delta \in C \cap \lambda\ x \in B_\delta = \delta \leftrightarrow x \in \lambda,$$

luego $B_\lambda = \lambda$.

Claramente $B_\lambda \cap A$ es una anticadena en B_λ. Si no es maximal existe un $x \in B_\lambda \setminus A$ incompatible con todos los elementos de $B_\lambda \cap A$. Entonces $\mathrm{alt}_B x < \lambda$, luego existe $\delta \in C \cap \lambda$ tal que $\mathrm{alt}_B x < \delta$. Así $x \in B_\delta \setminus A$ y es incompatible con todos los elementos de B_δ, y esto contradice que $B_\delta \cap A$ es una anticadena maximal de B_δ. Así pues, $\lambda \in C$ y C es cerrado.

Llamemos $f(\alpha) = \mathrm{alt}_B \alpha$, $g(\alpha) = \bigcup\limits_{\beta \in \mathrm{Niv}_\alpha B} \beta$ y sea $h(\alpha)$ un elemento de A compatible con α. De este modo $f, g, h : \kappa \longrightarrow \kappa$, el conjunto

$$D = \{\lambda < \kappa \mid f[\lambda] \subset \lambda \wedge g[\lambda] \subset \lambda \wedge h[\lambda] \subset \lambda\}$$

es c.n.a. y es fácil ver que $D \subset C$, luego C no está acotado. ■

Teorema 9.19 $\Diamond \rightarrow \neg\mathrm{HS}$.

DEMOSTRACIÓN: Sea $\{A_\alpha\}_{\alpha<\omega_1}$ una sucesión $\Diamond$. Vamos a definir una relación de orden $\leq^*$ en ω_1 de modo que $B = (\omega_1, \leq^*)$ sea un árbol de Suslin. Llamaremos

$$N_\alpha = \{\omega \cdot \alpha + n \mid n \in \omega\}.$$

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. Definiremos $\leq^*$ de modo que N_α sea el nivel α-ésimo de B. De este modo tendremos garantizado que B será un $\aleph_1$-árbol. Más concretamente, vamos construir un árbol B que cumpla las propiedades siguientes:

a) $\bigwedge \alpha < \omega_1\ \mathrm{Niv}_\alpha B = N_\alpha$,

b) 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.

c) Si $\beta < \alpha < \omega_1$ y $x \in N_\beta$, entonces $\bigvee y \in N_\alpha\ x \leq^* y$.

d) 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 b) 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 c) afirma que desde cualquier punto se puede ascender hasta cualquier altura. La propiedad d) es la que nos dará la propiedad de Suslin.

Razonamos por recurrencia. 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 b) 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 para cada $n \in \omega$ existe una cadena $B(n)$ en B_λ tal que $x_n \in B_n$ y $B(n)$ corta a todos los niveles N_δ para todo $\delta < \lambda$.

Sea $\{\beta_m(n)\}_{m\in\omega}$ una sucesión cofinal creciente en λ tal que $\mathrm{alt}\, x_n < \beta_0(n)$. 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 c). Basta tomar $B(n) = \{z \in B_\lambda \mid \bigvee m \in \omega \; z <^* y_m(n)\}$.

Supongamos momentáneamente que $B_\lambda = \lambda$ y que A_λ (de la sucesión $\Diamond$) sea una anticadena maximal en B_λ. Entonces cada x_n es compatible en B_λ con algún elemento de A_λ, es decir, existe un $a(n) \in A_\lambda$ anterior o posterior a x_n. En cualquier caso existe un $y \in B_\lambda$ tal que $x_n <^* y \wedge a(n) <^* y$. Podemos escoger la sucesión $\{y_m(n)\}_{m\in\omega}$ de modo que $y_0(n) = y$, con lo que $a(n) \in B(n)$.

Volviendo al caso general, 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 a), b) y c). La propiedad

d) también se cumple, 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 $a(n) \in A_\lambda$ cumple $a(n) \in B_n$, es decir, $a(n) <^* x$.

Así pues, tenemos definido un árbol $B = (\omega_1, \leq^*)$ que cumple las propiedades a), b), c) y d). Por a) es un $\aleph_1$-árbol. Por b) es ramificado, luego para probar que es un árbol de Suslin basta ver que todas sus anticadenas maximales son numerables (teorema 9.16). Sea, pues, A una anticadena maximal en B. Por el teorema anterior, el conjunto

$$C = \{\lambda < \omega_1 \mid B_\lambda = \lambda \wedge B_\lambda \cap A \text{ es una anticadena maximal en } B_\lambda\}$$

es c.n.a. en ω_1. Por $\diamondsuit$, el conjunto $\{\alpha < \omega_1 \mid A \cap \alpha = A_\alpha\}$ es estacionario en ω_1, luego existe un $\lambda \in C$ tal que $A \cap \lambda = A_\lambda$. Tenemos entonces que $A_\lambda \subset A$ es una anticadena maximal en B_λ. Ahora bien, por construcción, todos los elementos de N_λ tienen por debajo un elemento de A_λ, pero de hecho todo elemento de B de altura $\geq \lambda$ tiene bajo sí un elemento de N_λ, luego un elemento de A. Esto significa que $A \subset B_\lambda$ (más concretamente, $A = A_\lambda$), y en particular es numerable. ■

Si meditamos sobre la construcción anterior veremos que esencialmente consiste en garantizar que una cierta anticadena A_λ no puede extenderse más allá del nivel λ, haciendo que todos los elementos del nivel λ sean compatibles con ella. El diamante hace falta para garantizar que una anticadena maximal arbitraria del árbol que resulte de la construcción coincidirá hasta un cierto nivel λ con A_λ.

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 9.20 *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:

a) $\bigwedge \alpha < \kappa^+ \ \mathrm{Niv}_\alpha B = N_\alpha$,

b) 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.

c) Si $\beta < \alpha < \kappa^+$ y $x \in N_\beta$, entonces $\bigvee y \in N_\alpha\ x \leq^* y$.

d) Toda cadena maximal en B tiene altura de cofinalidad κ.

e) 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 a) – e), entendiendo la d) 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 b). 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 d) 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 a), c), d), 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 a) y c), 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. Por el teorema 9.18, el conjunto

$$C = \{\lambda < \kappa^+ \mid B_\lambda = \lambda \land B_\lambda \cap A \text{ es una anticadena maximal en } B_\lambda\}$$

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 e), 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, como en el caso de los κ-árboles de Aronszajn, 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 y, en particular, de κ-árboles de Aronszajn:

Teorema 9.21 *Sea κ un cardinal infinito tal que existe $E \subset \kappa^+$ estacionario de modo que se cumplen $\Box_\kappa(E)$ y $\Diamond_E$. Entonces existe un κ^+-árbol de Suslin.*

Demostración: Sea $\{A_\alpha\}_{\alpha\in E}$ una sucesión $\Diamond_E$ y sea $\{C_\lambda\}_{\lambda<\kappa^+}$ una sucesión $\Box_\kappa(E)$. 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:

a) $\bigwedge\alpha < \kappa^+ \ \mathrm{Niv}_\alpha B = N_\alpha$,

b) 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.

c) Si $\beta < \alpha < \kappa^+$ y $x \in N_\beta$, entonces $\bigvee y \in N_\alpha \ x \leq^* y$.

d) Toda cadena de altura límite λ está bajo un único elemento de N_λ.

e) Si $\lambda \in E$, $B_\lambda = \lambda$ y A_λ es una anticadena maximal en B_λ, entonces

$$\bigwedge x \in N_\lambda \bigvee y \in A_\lambda \; y \leq^* x.$$

El problema es cómo extender la relación de orden $\leq^*$ 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 $\{p_\lambda^x(\alpha)\}_{\alpha_\lambda(x)\leq\alpha<\theta_\lambda}$ como sigue:

- $p_\lambda^x(\alpha_\lambda(x))$ es el mínimo ordinal $y \in N_{\gamma_\lambda(\alpha_\lambda(x))}$ tal que $x \leq^* y$.
- $p_\lambda^x(\alpha+1)$ es el mínimo ordinal $y \in B_{\gamma_\lambda(\alpha+1)}$ tal que $p_\lambda^x(\alpha) \leq^* y$.
- $p_\lambda^x(\lambda')$ es el único ordinal $y \in N_{\gamma_\lambda(\lambda')}$ tal que

$$\bigwedge \alpha < \lambda' (\alpha_\lambda(x) \leq \alpha \to p_\lambda^x(\alpha) \leq^* y).$$

Observemos que el ordinal y requerido existe sin duda en los dos primeros casos por la propiedad c). Sin embargo, no es evidente que exista en el tercer caso (pero si existe es único, por la propiedad d). Supongamos de momento que existe un único y para cada x, de modo que la función p_λ^x puede ser definida. En tal caso podemos definir

$$C_\lambda^x = \{y \in B_\lambda \mid \bigvee \alpha < \theta_\lambda \; y \leq^* p_\lambda^x(\alpha)\},$$

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_λ^x que hemos construido, digamos $\{C_\lambda^\delta\}_{\delta<\kappa}$, y establecemos que por encima de cada C_λ^δ 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_λ^x. 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_λ^x. 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 $\Box_\kappa(E)$ 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 $p_{\gamma_\lambda(\lambda')}^x$ es el fragmento de p_λ^x 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 9.20: 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 (luego de Aronszajn): $2^{<\kappa} = \kappa \wedge 2^\kappa = \kappa^+ \wedge \Box_\kappa$. ■

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 9.22 *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 $\{C^\beta_\alpha\}_{\beta<\kappa}$ de caminos en A_α de modo que si $\alpha \leq \alpha'$ entonces $C^\beta_\alpha \subset C^\beta_{\alpha'}$ y además los caminos $\{C^\beta_\alpha\}_{\beta<\alpha}$ sean distintos dos a dos.

Necesariamente, $A_0 = \{\varnothing\}$ y $C^\beta_0 = \{\varnothing\}$ 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 $C^\beta_{\alpha+1}$ añadiendo a C^β_α la prolongación de su elemento de altura α que toma sobre α el valor 0, salvo en el caso de $C^\alpha_{\alpha+1}$, 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 $A_\lambda = \bigcup\limits_{\delta<\lambda} A_\delta$ y $C^\beta_\lambda = \bigcup\limits_{\delta<\lambda} C^\beta_\delta$, que claramente cumplen lo pedido.

Así, el κ-árbol $A = A_\kappa$ tiene κ caminos distintos $\{C_\kappa^\beta\}_{\beta<\kappa}$. ■

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 9.23 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 en NBG. 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 9.24 *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 $\chi_B^\alpha \in {}^\alpha 2$ la función característica de $B \cap \alpha$ y sea

$$A = \bigcup_{\alpha<\kappa} \{\chi_B^\alpha \mid B \in \mathcal{F}\} \subset {}^{<\kappa}2.$$

Si $\beta < \alpha$, entonces $\chi_B^\alpha|_\beta = \chi_B^\beta$, luego A es un árbol con el orden dado por la inclusión y

$$\mathrm{Niv}_\alpha(A) = \{\chi_B^\alpha \mid B \in \mathcal{F}\},$$

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 9.25 *Sea κ un cardinal infinito tal que $2^{<\kappa} = \kappa$. Entonces existe una familia $\mathcal{A} \subset \mathcal{P}\kappa$ tal que $\bigwedge z \in A\ |x| = \kappa$, $\bigwedge xy \in \mathcal{A}(x \neq y \rightarrow |x \cap y| < \kappa)$ 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 9.26 *Si κ es un cardinal infinito y se cumple $\Diamond^+_{\kappa^+}$, 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 $\Diamond^+_{\kappa^+}$ y sea $\mathcal{F}$ el conjunto de todos los $X(A, C)$ tales que

a) $A \subset \kappa^+$, $|A| = \kappa^+$ y C es c.n.a. en κ^+,

b) $\bigwedge \alpha \in C\ A \cap \alpha \in S_\alpha$,

c) $\bigwedge \alpha \in C\ C \cap \alpha \in S_\alpha$.

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 $\bigcup\limits_{\alpha\leq\beta} S_\alpha$, 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 $\xi = \mathrm{mín}(A \cap \beta)$.

Ahora basta probar que $|\mathcal{F}| = 2^{\kappa^+}$, pues en particular $\mathcal{F}$ será una familia κ^+-Kurepa y la prueba del teorema 9.24 muestra que existe un κ^+-árbol de Kurepa con 2^{κ^+} caminos.

Recordemos que $\Diamond^+_{\kappa^+} \to \Diamond_{\kappa^+} \to 2^\kappa = \kappa^+$. 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 $\Diamond^+_{\kappa^+}$, 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 en NBG que no existan κ^+-árboles de Kurepa (pero lo cierto es que tampoco puede probarse que existan).

Capítulo X

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, como de topología, de análisis matemático o de estadística. Trabajamos en NBG sin el axioma de elección.

10.1 Conceptos básicos

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 10.1 Un *álgebra de Boole* es una cuádrupla $(\mathbb{B}, \wedge, \vee, ')$, donde $\mathbb{B}$ es un conjunto no vacío, $\wedge : \mathbb{B} \times \mathbb{B} \longrightarrow \mathbb{B}$, $\vee : \mathbb{B} \times \mathbb{B} \longrightarrow \mathbb{B}$ y $' : \mathbb{B} \longrightarrow \mathbb{B}$ de modo que se cumplen las propiedades siguientes:

1) $p'' = p$,	5) $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$,
2) $p \wedge q = q \wedge p$,	6) $p \vee (p \wedge q) = p$,
3) $(p \wedge q) \wedge r = p \wedge (q \wedge r)$,	7) $(p \wedge q)' = p' \vee q'$,
4) $p \wedge p = p$,	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 $p \in B$ se cumple $p \wedge p' = \mathbb{0}$, $p \vee p' = \mathbb{1}$. Las propiedades siguientes se 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, $p \vee \mathbb{1} = p \vee (p \vee p') = (p \vee p) \vee p' = p \vee p' = \mathbb{1}$.

Definimos además las operaciones

$$p \rightarrow q = p' \vee q, \qquad p \leftrightarrow q = (p \rightarrow q) \wedge (q \rightarrow p).$$

Teorema 10.2 *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:

a) $p \wedge q$ es el ínfimo del conjunto $\{p, q\}$,

b) $p \vee q$ es el supremo del conjunto $\{p, q\}$,

c) $p \leq q$ syss $q' \leq p'$.

d) $\mathbb{0}$ y $\mathbb{1}$ son el mínimo y el máximo de $\mathbb{B}$ respectivamente.

e) $p \leq q$ syss $p \rightarrow q = \mathbb{1}$, y $(p \leftrightarrow q) = \mathbb{1}$ syss $p = q$.

f) $p = q'$ 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). 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 $p \leq r$.

a) 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 $\{p, q\}$.

b) es análogo a a).

c) Si $p \leq q$ entonces $p \wedge q = p$, luego $p' \vee q' = p'$, luego $q' \leq p'$.

d) es trivial.

e) Si $p \leq q$ entonces $(p \rightarrow q) = p' \vee q = p' \vee p \vee q = \mathbb{1} \vee q = \mathbb{1}$.

Si $(p \rightarrow q) = \mathbb{1}$, 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 $(p \rightarrow q) = (q \rightarrow p) = \mathbb{1}$, syss $p \leq q \wedge q \leq p$, syss $p = q$.

f) Tenemos que

$$\begin{aligned} q &= \mathbb{1} \wedge q = (p \vee p') \wedge q = (p \wedge q) \vee (p' \wedge q) = \mathbb{0} \vee (p' \wedge q) \\ &= (p' \wedge p) \vee (p' \wedge q) = p' \wedge (p \vee q) = p' \wedge \mathbb{1} = p'. \end{aligned}$$

■

Definición 10.3 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, en lo sucesivo entenderemos que "álgebra de Boole" significa "álgebra de Boole no degenerada".

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 $\mathbb{C}$ es la restricción de la de $\mathbb{B}$.

Obviamente $\mathbb{B}$ es una subálgebra de $\mathbb{B}$, las subálgebras de $\mathbb{B}$ distintas de la propia $\mathbb{B}$ se llaman subálgebras *propias.* Así mismo, $\{\mathbb{0}, \mathbb{1}\}$ 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 $\mathbb{B} = \{\mathbb{0}, \mathbb{1}\}$.

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 $\mathbb{B}$.

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

$$\mathbb{O} = \varnothing, \quad \mathbb{1} = X, \quad x \leq y \text{ syss } x \subset y.$$

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 y además $\mathbb{O} = \varnothing$, $\mathbb{1} = X$.

Por ejemplo, si X es un espacio topológico, el conjunto $\mathbb{B}$ de los subconjuntos de X que son a la vez abiertos y cerrados es un álgebra de conjuntos[1] sobre X. ■

Ejemplo 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 $\mathbb{O}$ 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 $a = \mathbb{1}$). ■

Definición 10.4 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 cumple $h(\mathbb{O}) = \mathbb{O}$, $h(\mathbb{1}) = \mathbb{1}$ y si $p \leq q$ entonces $h(p) \leq h(q)$. Además $h[\mathbb{B}]$ es una subálgebra de $\mathbb{C}$.

[1]Los espacios topológicos cuya álgebra de abiertos cerrados es trivial, es decir, los que no tienen más abiertos cerrados que $\varnothing$ y X, se llaman *espacios conexos*. Por ejemplo, puede probarse que los conjuntos totalmente ordenados conexos con la topología de orden son precisamente los continuos. En particular $\mathbb{R}$ es conexo.

Un *monomorfismo, epimorfismo, isomorfismo de álgebras* 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, p' está caracterizado como el único elemento q que cumple $p \wedge q = \mathbb{O}$, $p \vee q = \mathbb{1}$.

Terminamos esta sección con el teorema siguiente:

Teorema 10.5 *Toda álgebra de Boole finitamente generada es finita.*

Demostración: Sea $\mathbb{B}$ un álgebra de Boole y sea $\{c_i\}_{i<n}$ una familia finita de elementos de $\mathbb{B}$. Para cada $b \in \mathbb{B}$ llamamos $p(b,0) = b'$ y $p(b,1) = b$. Para cada $f \in {}^n2$ llamaremos

$$a_f = \bigwedge_{i\in n} p(c_i, f(i)) \in \mathbb{B}.$$

Sea $X = \{f \in {}^n2 \mid a_f \neq \mathbb{O}\}$ y para cada $x \subset X$ sea $b_x = \bigvee\limits_{f\in x} a_f$. Por último, llamemos $\mathbb{C} = \{b_x \mid x \in \mathcal{P}X\} \subset \mathbb{B}$.

Observemos en primer lugar que si $f \neq g$ entonces $a_f \wedge a_g = \mathbb{O}$, pues existe un i tal que $f(i) \neq g(i)$, luego $a_f \wedge a_g \leq x_i \wedge x_i' = \mathbb{O}$.

Veamos ahora que $b_X = \mathbb{1}$. En efecto:

$$\mathbb{1} = \bigwedge_{i<n} (c_i \vee c_i') = \bigvee_{f\in {}^n2} \bigwedge_{i<n} p(c_i, f(i)) = \bigvee_{f\in {}^n2} a_f = \bigvee_{f\in X} a_f = b_X.$$

Por otra parte, es trivial que $b_\varnothing = \mathbb{O}$, así como que $b_{x\cup y} = b_x \vee b_y$. Veamos ahora que $b_{x\cap y} = b_x \wedge b_y$. En efecto:

$$b_x \wedge b_y = \bigvee_{f\in x} a_f \wedge \bigvee_{f\in y} a_f = \bigvee_{(f,g)\in x\times y} (a_f \wedge a_g).$$

Como $a_f \wedge a_g = \mathbb{O}$ salvo si $f = g$, esto implica que

$$b_x \wedge b_y = \bigvee_{f\in x\cap y} a_f = b_{x\cap y}.$$

Por último, si llamamos $x' = X \setminus x$, tenemos que $b_{x'} = b_x'$. En efecto,

$$b_{x'} \wedge b_x = b_{x'\cap x} = \mathbb{O}, \qquad b_{x'} \vee b_x = b_{x'\cup x} = \mathbb{1}.$$

Con esto hemos probado que $\mathbb{C}$ es una subálgebra de $\mathbb{B}$ y que la aplicación $h : \mathcal{P}X \longrightarrow \mathbb{C}$ dada por $h(x) = b_x$ es un epimorfismo de álgebras. De hecho es un isomorfismo, pues si $h(x) = h(y)$ entonces $b_{x\cap y'} = b_x \wedge b_y' = b_x \wedge b_x' = \mathbb{O}$, luego $x \cap y' = \varnothing$ (porque si $f \in x \cap y'$ entonces $\mathbb{O} < a_f \leq b_{x\cap y'}$), luego $x \subset y$, e igualmente $y \subset x$.

Para cada $i < n$, sea $x_i = \{f \in X \mid f(i) = 1\}$. Veamos que $b_{x_i} = c_i$. En efecto, si $f \in x_i$ tenemos que $a_f \leq c_i$, luego $b_{x_i} \leq c_i$.

Por otra parte, si $f \in x_i'$, entonces $a_f \wedge c_i = \mathbb{O}$, luego $b_{c_i'} \wedge c_i = \mathbb{O}$, es decir, $b_{x_i}' \wedge c_i = \mathbb{O}$, luego $\mathbb{1} = c_i' \vee b_{c_i} = c_i \rightarrow b_{x_i}$, luego $c_i \leq b_{x_i}$, luego $c_i = b_{x_i} \in \mathbb{C}$.

Concluimos que $\mathbb{C}$ es el álgebra generada por el conjunto $\{x_i \mid i < n\}$, luego es un álgebra finita isomorfa a $\mathcal{P}X$, donde X es un conjunto tal que $|X| \leq 2^n$. ■

10.2 Álgebras completas

Definición 10.6 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 $\bigvee \varnothing = \mathbb{O}$, $\bigwedge \varnothing = \mathbb{1}$.

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 10.7 *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 $\bigwedge\limits_{i \in I} p_i'$. Entonces, para cada $i \in I$, tenemos que $\bigwedge\limits_{i \in I} p_i' \leq p_i'$, luego $p_i \leq \big(\bigwedge\limits_{i \in I} p_i'\big)'$, 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 $r' \leq \bigwedge\limits_{i \in I} p_i'$, luego $\big(\bigwedge\limits_{i \in I} p_i'\big)' \leq r$. Esto prueba que existe $\bigvee\limits_{i \in I} p_i = \big(\bigwedge\limits_{i \in I} p_i'\big)'$, luego en definitiva $\big(\bigvee\limits_{i \in I} p_i\big)' = \bigwedge\limits_{i \in I} p_i'$.

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 $\{p_i'\}_{i \in I}$. ■

Equivalentemente, si definimos el *conjunto dual* de un conjunto $X \subset \mathbb{B}$ como

$$X' = \{p' \mid p \in X\},$$

el teorema anterior se expresa mediante las igualdades

$$\bigvee X' = (\bigwedge X)', \qquad \bigwedge X' = (\bigvee X)',$$

en las que hay que entender que un miembro existe si y sólo si existe el otro.

Definición 10.8 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 $\bigcap \varnothing = A$).

Los supremos e ínfimos satisfacen la siguiente propiedad distributiva:

Teorema 10.9 *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 $p_{0i} \wedge p_{1j} \leq \bigvee\limits_{i\in I} p_{0i} \wedge \bigvee\limits_{j\in J} p_{1j}$, 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 $\bigvee\limits_{i\in I} p_{0i} \leq r \vee p'_{1j}$, luego $\bigvee\limits_{i\in I} p_{0i} \wedge p_{1j} \leq r$. Similarmente, $p_{1j} \leq r \vee \big(\bigvee\limits_{i\in I} p_{0i}\big)'$, de donde $\bigvee\limits_{j\in J} p_{1j} \leq r \vee \big(\bigvee\limits_{i\in I} p_{0i}\big)'$, 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

$$p \wedge \bigvee_{i\in I} p_i = \bigvee_{i\in I} (p \wedge p_i), \qquad p \vee \bigwedge_{i\in I} p_i = \bigwedge_{i\in I} (p \vee p_i).$$

Probamos ahora un resultado elemental que es útil a menudo:

Teorema 10.10 *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 $\bigwedge \alpha < \gamma\ q_\alpha \leq p_\alpha$, $\bigwedge \alpha\beta < \gamma(\alpha \neq \beta \rightarrow q_\alpha \wedge q_\beta = \mathbb{O})$ y $\bigvee\limits_{\alpha<\gamma} q_\alpha = \bigvee\limits_{\alpha<\gamma} p_\alpha$.*

Demostración: Basta tomar $q_\alpha = p_\alpha \wedge \bigwedge\limits_{\beta<\alpha} p'_\beta$. Obviamente $q_\alpha \leq p_\alpha$ y si $\alpha \neq \beta$, digamos $\beta < \alpha$, entonces $q_\alpha \wedge q_\beta \leq p'_\beta \wedge p_\beta = \mathbb{O}$. Veamos por inducción sobre $\alpha \leq \gamma$ que $\bigvee\limits_{\beta<\alpha} p_\alpha = \bigvee\limits_{\beta<\alpha} q_\beta$. 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 $\bigvee\limits_{\beta<\lambda} q_\beta \leq \bigvee\limits_{\beta<\lambda} p_\beta$, 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 $\bigvee\limits_{\beta<\lambda} p_\beta = \bigvee\limits_{\beta<\lambda} q_\beta$. ■

Definición 10.11 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).

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.

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 $\mathbb{B}$. (Véase la nota tras el teorema 10.49).

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 $\mathbb{B}$.

Presentamos ahora una familia muy importante de álgebras completas:

Definición 10.12 Sea X un espacio topológico. Diremos que $A \subset X$ es un *abierto regular* si $A = \operatorname{int}\operatorname{cl} A$. 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 10.13 *Sean U y V subconjuntos de un espacio topológico X y supongamos que U es abierto. Entonces:*

a) $U^{\perp\perp\perp} = U^\perp$,

b) $V^{\perp\perp\perp\perp} = V^{\perp\perp}$,

c) $(U \cap V)^{\perp\perp} = U^{\perp\perp} \cap V^{\perp\perp}$.

DEMOSTRACIÓN: a) 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.

b) Es consecuencia de a) aplicado al abierto $U = V^\perp$.

c) 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 10.14 *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 c) 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 b) 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 a).

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 $s = \big(\bigcup\limits_{p\in A} p\big)^{\perp\perp} \in R(X)$. Como la unión es un abierto, se cumple que $\bigcup\limits_{p\in A} p \subset \operatorname{int}\operatorname{cl} \bigcup\limits_{p\in A} p = s$, luego s es una cota superior de A. Si $r \in R(X)$ es una cota superior de A, entonces $\bigcup\limits_{p\in A} p \subset r$, luego $s \subset r^{\perp\perp} = r$, 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.

Compleción de un álgebra de Boole Toda álgebra de Boole se puede sumergir en un álgebra de Boole completa, que es única salvo isomorfismo si exigimos que la inmersión sea "densa" en un sentido que hemos de especificar. Vamos a demostrar una generalización de este hecho.

Definición 10.15 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 $\mathbb{B} \setminus \{\mathbb{O}\}$. Por ejemplo:

Si $\mathbb{P}$ es un c.p.o., diremos que dos elementos p, $q \in \mathbb{P}$ son *incompatibles* si

$$p \perp q \equiv \neg \bigvee r \in \mathbb{P}\ (r \leq p \land r \leq q).$$

Entonces, si $\mathbb{B}$ es un álgebra de Boole, diremos que p, $q \in \mathbb{B} \setminus \{\mathbb{O}\}$ son incompatibles si no existe $r \in \mathbb{B} \setminus \{\mathbb{O}\}$ tal que $r \leq p \land r \leq q$. Puesto que $r = p \land q$ siempre cumple $r \leq p \land r \leq q$, concluimos que, en un álgebra de Boole, dos elementos p y q (no nulos) son incompatibles si y sólo si[2] $p \land q = \mathbb{O}$.

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 $\bigwedge pq \in \mathbb{P}\ (p \not\leq q \rightarrow \bigvee r \in \mathbb{P}\ (r \leq p \land r \perp q))$.

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 $\mathbb{B} \setminus \{\mathbb{O}\}$ y, ciertamente, si p, $q \in \mathbb{B} \setminus \{\mathbb{O}\}$ y $p \not\leq q$, tomamos $r = p \land q'$ y comprobamos que $r \neq \mathbb{O}$ pues si $p \land q' = \mathbb{O}$ entonces $p \rightarrow q = p' \lor q = \mathbb{1}$, luego $p \leq q$. Así, existe un $r \in \mathbb{B} \setminus \{\mathbb{O}\}$ que claramente cumple $r \leq p \land r \perp q$.

Si $\mathbb{P}$ es un c.p.o. y $D \subset \mathbb{P}$, diremos que D es *denso* en $\mathbb{P}$ si

$$\bigwedge p \in \mathbb{P} \bigvee d \in D\ d \leq p.$$

Una aplicación $i : \mathbb{P} \longrightarrow \mathbb{Q}$ entre dos c.p.o.s es una *inmersión* si cumple:

a) $\bigwedge p_1 p_2 \in \mathbb{P}\ (p_1 \leq p_2 \rightarrow i(p_1) \leq i(p_2))$,

b) $\bigwedge p_1 p_2 \in \mathbb{P}\ (p_1 \perp p_2 \rightarrow i(p_1) \perp i(p_2))$.
Diremos que i es una *inmersión completa* si además cumple

c) $\bigwedge q \in \mathbb{Q} \bigvee p \in \mathbb{P} \bigwedge p^* \in \mathbb{P}(p^* \leq p \rightarrow \neg i(p^*) \perp q)$,
y en estas circunstancias diremos que p es una *reducción* de q a $\mathbb{P}$.

[2]Obviamente, si $p = \mathbb{O} \lor q = \mathbb{O}$ se cumple también que $p \land q = \mathbb{O}$. En tal caso diremos también que p y q son incompatibles, es decir, extendemos así a $\mathbb{B}$ la relación de incompatibilidad, que en principio se aplica a $\mathbb{B} \setminus \{\mathbb{O}\}$.

Una inmersión $i : \mathbb{P} \longrightarrow \mathbb{Q}$ es *densa* si $i[\mathbb{P}]$ es denso en $\mathbb{Q}$.

Es inmediato comprobar que la composición de inmersiones (resp. inmersiones completas, resp. densas) es también una inmersión (resp. completa, densa).

Vamos a ver cómo se particularizan estos conceptos al caso de álgebras de Boole. Para empezar observamos lo siguiente:

Teorema 10.16 *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 $\mathbb{Q}$.

La definición de inmersión completa es algo técnica, pero captura exclusivamente en términos de la relación de orden el concepto de monomorfismo completo entre álgebras de Boole completas:

Teorema 10.17 *Sean $\mathbb{B}$ y $\mathbb{C}$ dos álgebras de Boole completas. Entonces, una aplicación $h : \mathbb{B} \longrightarrow \mathbb{C}$ es un monomorfismo completo (en el sentido de conservar supremos) si y sólo si $h(\mathbb{O}) = \mathbb{O}$ y su restricción a $\mathbb{B} \setminus \{\mathbb{O}\}$ es una inmersión completa $\mathbb{B} \setminus \{\mathbb{O}\} \longrightarrow \mathbb{C} \setminus \{\mathbb{O}\}$ en el sentido de c.p.o.s.*

Demostración: Si h es un monomorfismo completo, claramente es una inmersión y si $q \in \mathbb{C} \setminus \{\mathbb{O}\}$ entonces $p = \bigwedge\{r \in \mathbb{B} \mid q \leq h(r)\}$ es una reducción de q a $\mathbb{B}$. En efecto, $h(p) = \bigwedge\{h(r) \mid r \in \mathbb{B} \wedge q \leq h(r)\} \geq q > \mathbb{O}$, luego $p > \mathbb{O}$. Si $t \leq p$ es no nulo pero $h(t) \wedge q = \mathbb{O}$, entonces $q \leq h(t')$, luego $p \leq t'$ (por definición de p), y así $t \leq p \wedge p' = \mathbb{O}$, contradicción.

Supongamos ahora que h es una inmersión completa en el sentido de c.p.o.s. Como $\mathbb{B}$ es un c.p.o. separativo, el teorema anterior nos da que h es inyectiva y para todo p, $q \in \mathbb{B} \setminus \{\mathbb{O}\}$

$$p \leq q \leftrightarrow h(p) \leq h(q), \qquad p \wedge q = \mathbb{O} \leftrightarrow h(p) \wedge h(q) = \mathbb{O}.$$

Notemos además que $h(\mathbb{1}) = \mathbb{1}$. En efecto, en caso contrario $h(\mathbb{1})' \neq \mathbb{O}$, 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 $r = h(p) \wedge h(\mathbb{1})' \neq \mathbb{O}$, 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 $r \leq h(\mathbb{1})' \wedge h(\mathbb{1})' = \mathbb{O}$, contradicción.

Sea $p \in \mathbb{B} \setminus \{\mathbb{O}\}$ y veamos que $h(p') = h(p)'$. Como $p \wedge p' = \mathbb{O}$, sabemos que $h(p) \wedge h(p') = \mathbb{O}$, luego $h(p') \leq h(p)'$. Si no se da la igualdad, tendrá que ser $q = h(p)' \wedge h(p')' \neq \mathbb{O}$. Sea r una reducción de q a $\mathbb{B}$. Necesariamente $r \wedge p \neq \mathbb{O}$ o $r \wedge p' \neq \mathbb{O}$. Veamos que ambos casos llevan a contradicción.

Si $r \wedge p \neq \mathbb{O}$, entonces $h(r \wedge p) \leq h(p)$, luego $h(r \wedge p) \wedge q = \mathbb{O}$, en contra de que r sea una reducción de q.

Si $r \wedge p' \neq \mathbb{O}$ entonces $h(r \wedge p') \leq h(p')$ y también $h(r \wedge p') \wedge q = \mathbb{O}$.

Así pues, h conserva complementos. Si probamos que h conserva ínfimos de conjuntos arbitrarios tendremos en particular que conserva ínfimos de pares, luego h será un monomorfismo completo. Sea, pues, $X \subset \mathbb{B}$. Para cada $p \in X$ tenemos que

$$\bigwedge_{p\in X} p \leq p, \quad \text{luego} \quad h\Big(\bigwedge_{p\in X} p\Big) \leq h(p), \quad \text{luego} \quad h\Big(\bigwedge_{p\in X} p\Big) \leq \bigwedge_{p\in X} h(p).$$

Si se diera la desigualdad estricta existiría un $s \in \mathbb{C} \setminus \{\mathbb{O}\}$ tal que

$$s \leq \bigwedge_{p\in X} h(p) \quad \text{y} \quad s \wedge h\Big(\bigwedge_{p\in X} p\Big) = \mathbb{O}.$$

Sea t una reducción de s a $\mathbb{B}$. Si $p \in X$ ha de ser $t \leq p$, pues en caso contrario $t \wedge p' \neq \mathbb{O}$ y $h(t \wedge p') \wedge s \leq h(p') \wedge h(p) = h(p)' \wedge h(p) = \mathbb{O}$, en contradicción con que t es una reducción de s. Así pues, $t \leq \bigwedge\limits_{p\in X} p$, pero entonces

$$s \wedge h(t) \leq s \wedge h\Big(\bigwedge_{p\in X} p\Big) = \mathbb{O},$$

lo que de nuevo contradice que t sea una reducción de s. ■

Necesitaremos el resultado siguiente:

Teorema 10.18 *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. ■

Nos ocupamos ahora de las inmersiones densas y empezamos con un hecho elemental:

Teorema 10.19 *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 $\neg i(p^*) \perp q$. ■

Veamos ahora que un álgebra de Boole completa está totalmente determinada por cualquiera de sus subconjuntos densos:

Teorema 10.20 *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 $D \subset \mathbb{B} \setminus \{\mathbb{O}\}$ es denso en $\mathbb{B} \setminus \{\mathbb{O}\}$. 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 $p \wedge r' \neq \mathbb{O}$, 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 $q \leq r \wedge r' = \mathbb{O}$, 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 $p \in \mathbb{B} \setminus \{\mathbb{O}\}$, entonces existe $q \in D$ tal que $q \leq p$ y por consiguiente $\mathbb{O} < j(q) \leq j^*(p)$. Así pues, j^* se restringe a una aplicación $\mathbb{B}\setminus\{\mathbb{O}\} \longrightarrow \mathbb{C}\setminus\{\mathbb{O}\}$. 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, $p_1 \wedge p_2 = \mathbb{O}$, entonces, para cada $q \in D$, $q \leq p_1$ tenemos que

$$j(q) \wedge j^*(p_2) = \bigvee\{j(q) \wedge j(r) \mid r \in D \wedge r \leq p_2\} = \mathbb{O},$$

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

$$j^*(p_1) \wedge j^*(p_2) = \bigvee\{j(q) \wedge j^*(p_2) \mid q \in D \wedge q \leq p_1\} = \mathbb{O}.$$

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 $r \in \mathbb{C} \setminus \{\mathbb{O}\}$ tal que $r \leq q$ y $r \leq j(d') = j^*(d') \leq j^*(p)$, luego $\neg j^*(p) \perp q$.

Por 10.17 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 $q \wedge j^*(s) = \mathbb{O}$. 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 10.21 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 10.14 es un álgebra de Boole completa.

El claro que los subconjuntos de $\mathbb{P}$ densos para la topología que acabamos de definir son precisamente los que hemos definido como tales.

Teorema 10.22 *Sea $\mathbb{P}$ un c.p.o. Entonces:*

a) La aplicación $i_{\mathbb{P}} : \mathbb{P} \longrightarrow R(\mathbb{P})$ dada por $i(p) = B_p^{\perp\perp}$ es una inmersión densa.

b) 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:

$$\begin{tikzcd} R(\mathbb{P}) \arrow[r, "j^*"] & \mathbb{B} \\ \mathbb{P} \arrow[u, "i_{\mathbb{P}}"] \arrow[ur, "j"'] & \end{tikzcd}$$

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: a) Notemos que si $p \in \mathbb{P}$, entonces

$$p \in B_p \subset B_p^{\perp\perp} \neq \varnothing = \mathbb{O},$$

luego $i_{\mathbb{P}} : \mathbb{P} \longrightarrow R(\mathbb{P}) \setminus \{\mathbb{O}\}$.

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 $i(p) \wedge i(q) = \mathbb{O}$.

Esto prueba que i es una inmersión. Veamos que es densa. Si $A \in R(\mathbb{P})\setminus\{\mathbb{O}\}$, 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 b) 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 10.18), 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

$$r \leq s \leftrightarrow \bigwedge t \in \mathbb{Q}(\neg t \perp r \rightarrow \neg t \perp s).$$

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

$$i(p) \leq i(q) \leftrightarrow \bigwedge r \in \mathbb{P}(\neg i(r) \perp i(p) \rightarrow \neg i(r) \perp i(q))$$

$$\leftrightarrow \bigwedge r \in \mathbb{P}(\neg i'(r) \perp i'(p) \rightarrow \neg i'(r) \perp i'(q)) \leftrightarrow i'(p) \leq i'(q).$$

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 $\mathbb{B}$ 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 c.p.o. separativo $\mathbb{P}$ es semejante a un subconjunto denso de un álgebra de Boole completa $R(\mathbb{P})$. (Si no es separativo existe una inmersión densa, pero no es inyectiva, luego no es una semejanza en la imagen.)

Álgebras atómicas Ahora podemos dar una caracterización algebraica de las álgebras de la forma $\mathcal{P}A$.

Definición 10.23 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 $q \leq p \wedge r \leq p \wedge q \perp r$.

Diremos que $\mathbb{P}$ es *no atómico* si no tiene átomos. Diremos que $\mathbb{P}$ es *atómico* si el conjunto de sus átomos es denso.

Si $\mathbb{B}$ es un álgebra de Boole, un elemento $b \in \mathbb{B}$ no nulo es un átomo si no existe ningún $c \in \mathbb{B}$ tal que $\mathbb{O} < c < b$. En efecto, si sucede esto es obvio que b es un átomo, y si existe un c en estas condiciones, entonces $d = b \wedge c'$ cumple $d \neq \mathbb{O}$, $c \leq b \wedge d \leq b \wedge c \perp d$, luego b no es un átomo.

En particular, los átomos de un álgebra $\mathcal{P}A$ son los conjuntos de la forma $\{a\}$, con $a \in A$, y es claro que $\mathcal{P}A$ es un álgebra atómica.

Teorema 10.24 *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 comprueba inmediatamente que si $b \leq c$ entonces $h(b) \subset h(c)$, así como que si $b \perp c$ entonces $h(b) \cap h(c) = \varnothing$. Por lo tanto, h es una inmersión. Además, como $h(a) = \{a\}$, se trata de una inmersión densa, y una inmersión densa entre álgebras de Boole completas es un isomorfismo. ■

Ejercicio: Probar que toda álgebra de Boole finita es isomorfa a un álgebra $\mathcal{P}A$.

Teorema 10.25 *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 $q \leq i(a) \land r \leq i(a) \land p \perp r$, podemos suponer que $q = i(u) \land r = i(v)$. Entonces $\neg u \perp a \land \neg v \perp a$, luego existen u', v' de modo que $u' \leq u \land u' \leq a \land v' \leq v \land v' \leq a$, 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 $a'' \leq p \land a'' \leq a'$. 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 $R(\mathbb{P})$.

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 10.26 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. Conviene definirla para c.p.o.s arbitrarios:

Una *anticadena* en un c.p.o. $\mathbb{P}$ es un conjunto $A \subset \mathbb{P}$ formado por elementos incompatibles dos a dos.

Si κ es un cardinal, un c.p.o. $\mathbb{P}$ cumple la *condición de cadena* κ (c.c.κ) si toda anticadena en $\mathbb{P}$ tiene cardinal $< \kappa$. En particular, la c.c.$\aleph_1$ se llama *condición de cadena numerable.*

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 $R(\mathbb{P})$.

Teorema 10.27 (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 $\mathbb{O} \neq p \land (\bigvee A)' \leq p$, de donde concluimos que $p \land (\bigvee A)' \in Y$ 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. ■

Distributividad en álgebras completas La generalización natural del teorema 10.9 no se cumple en toda álgebra de Boole completa:

Definición 10.28 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 10.9 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 10.29 *Un álgebra de Boole completa es totalmente distributiva si y sólo si es isomorfa a un álgebra $\mathcal{P}A$.*

Demostración: Sea $\mathbb{B}$ un álgebra de Boole completa y totalmente distributiva.[3] 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_b 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 $\mathbb{0} < a_f \leq x$.

[3] 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.

Supongamos, pues, que $a_f \neq \mathbb{O}$. 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 $\mathbb{O} < c < a_f$, 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 10.21, un conjunto $D \subset \mathbb{B}$ es un abierto denso si

$$\bigwedge b \in \mathbb{B}(b \neq \mathbb{O} \to \bigvee d \in D\ d \leq b) \land \bigwedge d \in D \bigwedge b \in \mathbb{B}(\mathbb{O} < b \leq d \to b \in D).$$

Teorema 10.30 (AE) *Si $\mathbb{B}$ es un álgebra de Boole completa y κ un cardinal, las afirmaciones siguientes son equivalentes:*

a) B es κ-distributiva.

b) La intersección de κ abiertos densos es abierta densa.

c) Todo conjunto de κ particiones de $\mathbb{B}$ admite un refinamiento común.

Demostración: a) $\Rightarrow$ b) Sea $\{D_\alpha\}_{\alpha<\kappa}$ una familia de abiertos densos. Es inmediato que $D = \bigcap\limits_{\alpha<\kappa} D_\alpha$ es abierto. Para probar que es denso, tomamos $u \in \mathbb{B}$ no nulo. En la prueba de 10.20 hemos visto que $\bigvee\limits_{d\in D_\alpha} d = \mathbb{1}$, luego $\bigvee\limits_{d\in D_\alpha} (u \land d) = u$, luego

$$u = \bigwedge_{\alpha<\kappa} \bigvee_{d\in D_\alpha} (u \land d) = \bigvee_{f\in \prod\limits_{\alpha<\kappa} D_\alpha} \bigwedge_{\alpha<\kappa} (u \land f(\alpha)).$$

Si llamamos $u_f = \bigwedge\limits_{\alpha<\kappa} (u \land f(\alpha))$, alguno de ellos tiene que ser no nulo, pues el supremo de todos ellos es u. Si fijamos uno no nulo, tenemos claramente que $u_f \in D$, $u_f \leq u$, lo que prueba que D es denso.

b) $\Rightarrow$ c) Sea $\{P_\alpha\}_{\alpha<\kappa}$ una familia de particiones de $\mathbb{B}$. Para cada α, sea

$$D_\alpha = \{u \in \mathbb{B} \mid \bigvee v \in P_\alpha\ u \leq v\}.$$

Entonces D_α es claramente abierto, y además es denso, pues si $b \in \mathbb{B}$ no es nulo, entonces $\bigvee\limits_{p\in P_\alpha} p = \mathbb{1}$, luego $\bigvee\limits_{p\in P_\alpha} (b \wedge p) = b$, luego algún $b \wedge p \neq \mathbb{0}$ y $b \wedge p \in D_\alpha$, $b \wedge p \leq b$.

Sea $D = \bigcap\limits_{\alpha<\kappa} D_\alpha$, 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 $d \leq s'$. Claramente, d es incompatible con todos los elementos de P, lo que contradice la maximalidad de P.

c) $\Rightarrow$ a) Sea $\{p_{\alpha i}\}_{i\in I_\alpha}$ para $\alpha < \kappa$ una sucesión de κ familias de elementos de $\mathbb{B}$. Observemos que si $f \in \prod\limits_{\alpha<\kappa} I_\alpha$, entonces

$$u_f = \bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)} \leq p_{\alpha f(\alpha)} \leq \bigvee_{i\in I_\alpha} p_{\alpha i},$$

luego $u_f \leq \bigwedge\limits_{\alpha<\kappa} \bigvee\limits_{i\in I_\alpha} p_{\alpha i}$, luego

$$\bigvee_{f\in \prod\limits_{\alpha<\kappa} I_\alpha} \bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)} \leq \bigwedge_{\alpha<\kappa} \bigvee_{i\in I_\alpha} p_{\alpha i}.$$

Llamemos u al miembro derecho y veamos que se da la igualdad. Observemos que

$$\bigvee_{f\in \prod\limits_{\alpha<\kappa} I_\alpha} \bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)} = \bigvee_{f\in \prod\limits_{\alpha<\kappa} I_\alpha} \bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)} \wedge u = \bigvee_{f\in \prod\limits_{\alpha<\kappa} I_\alpha} \bigwedge_{\alpha<\kappa} (p_{\alpha f(\alpha)} \wedge u)$$

$$\bigwedge_{\alpha<\kappa} \bigvee_{i\in I_\alpha} p_{\alpha i} = \bigwedge_{\alpha<\kappa} \bigvee_{i\in I_\alpha} p_{\alpha i} \wedge u = \bigwedge_{\alpha<\kappa} \bigvee_{i\in I_\alpha} (p_{\alpha i} \wedge u).$$

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 10.10 podemos construir anticadenas $\{q_{\alpha i}\}_{i\in I_\alpha}$ de manera que $q_{\alpha i} \leq p_{\alpha i}$ y $\bigvee\limits_{i\in I_\alpha} q_{\alpha i} = \bigvee\limits_{i\in I_\alpha} p_{\alpha i} = \mathbb{1}$. 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 $w \leq \bigwedge\limits_{\alpha<\kappa} p_{\alpha f(\alpha)}$, luego

$$\mathbb{1} = \bigvee P \leq \bigvee_{f\in \prod\limits_{\alpha<\kappa} I_\alpha} \bigwedge_{\alpha<\kappa} p_{\alpha f(\alpha)},$$

luego el supremo de la derecha es $\mathbb{1}$, como había que probar. ■

Árboles como c.p.o.s 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 $p \leq q \lor q \leq p$, luego $q \leq^* p \lor p \leq^* q$, 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 $r \leq^* p \land r \leq^* q$, es decir, $p, q \in A_r^{\leq}$, 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 (usando AE) 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 $d^* \leq^* p \lor p \leq^* d^*$, 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 $\alpha = \bigcup\limits_n \alpha_n < \omega_1$. Entonces $D^* = \bigcap\limits_n D_n^*$ 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 $D^* \subset D = \bigcap\limits_n D_n$, es claro que D es denso en $\mathbb{B}$, y obviamente es abierto. Esto prueba que $\mathbb{B}$ es $\aleph_0$-distributiva.

Definición 10.31 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 10.32 (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 $A \subset \mathbb{B} \setminus \{\mathbb{O}\}$ 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 9.16.

Definimos $A_1 = \{\mathbb{1}\}$. Supuesto definido A_δ para todo $\delta < \lambda$, basta tomar $A_\lambda = \bigcup\limits_{\delta<\lambda} A_\delta$. Si tenemos A_δ y $\delta = \alpha + 1$, para cada $p \in \mathrm{Niv}_\alpha(A)$, como no es un átomo, existe $\mathbb{O} < p_0 < p$, luego podemos tomar $p_1 = p \wedge p_0'$ y tenemos que $p = p_0 \vee p_1$ y $p_0 \wedge p_1 = \mathbb{O}$. Es claro entonces que si hacemos $\mathrm{Niv}_{\alpha+1}(A) = \bigcup\limits_{p \in \mathrm{Niv}_\alpha(A)} \{p_0, p_1\}$, 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 $p = p_0 \vee p_1 \leq \bigvee\limits_{p \in \mathrm{Niv}_{\alpha+1}(A)} p$, 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 $\prod\limits_{\delta<\lambda} \mathrm{Niv}_\delta(A)$. Claramente, $p_f = \bigwedge\limits_{\delta<\lambda} f(\delta) = \mathbb{O}$ 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

$$\mathrm{Niv}_\lambda(A) = \{p_f \mid f \in \prod_{\delta<\lambda} \mathrm{Niv}_\delta(A) \wedge p_f \neq \mathbb{O}\},$$

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 en NBG la existencia de árboles de Suslin.

10.3 Ideales y filtros

Veamos ahora que toda álgebra de Boole admite una estructura de anillo:

Teorema 10.33 *toda álgebra de Boole $\mathbb{B}$ tiene estructura de anillo conmutativo y unitario con las operaciones dadas por*

$$p+q=(p\land q')\lor(p'\land q)=(p\lor q)\land(p\land q)'=(p\leftrightarrow q)',\quad p\cdot q=p\land q.$$

El elemento neutro de la suma es $\mathbb{O}$ 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:

$$(p+q)+r=((p+q)\land r')\lor((p+q)'\land r)$$

$$=(((p\land q')\lor(p'\land q))\land r')\lor(((p\lor q)\land(p'\lor q'))'\land r)$$

$$=(p\land q'\land r')\lor(p'\land q\land r')\lor(((p\lor q)'\lor(p'\lor q')')\land r)$$

$$=(p\land q'\land r')\lor(p'\land q\land r')\lor(((p'\land q')\lor(p\land q))\land r)$$

$$=(p\land q'\land r')\lor(p'\land q\land r')\lor(p'\land q'\land r)\lor(p\land q\land r),$$

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. En las álgebras de conjuntos la suma que acabamos de introducir se corresponde con la operación conjuntista conocida como *diferencia simétrica:*

$$X\mathbin{\triangle}Y=(X\setminus Y)\cup(Y\setminus X)=(X\cup Y)\setminus(X\cap Y).$$

Observemos que, al igual que hemos definido la suma y el producto a partir de las operaciones booleanas $\land$, $\lor$ y $'$, también podemos definir las operaciones booleanas a partir de la suma y el producto:

$$x\land y=xy,\quad x\lor y=x+y+xy,\quad x'=x+\mathbb{1}.$$

Esto se traduce en que una aplicación $f:\mathbb{B}\longrightarrow\mathbb{C}$ es un homomorfismo de álgebras si y sólo si es un homomorfismo de anillos.

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 $\land$, $\lor$ y $'$ dadas por las relaciones precedentes.

Los ideales de las álgebras de Boole tienen una caracterización muy simple en términos de las operaciones del álgebra, una caracterización que ya hemos considerado en el caso particular de las álgebras $\mathcal{P}X$:

Definición 10.34 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:

a) $\mathbb{O} \in I \land \mathbb{1} \notin I$,

b) $\bigwedge p \in I \bigwedge q \in \mathbb{B}\ (q \leq p \to q \in I)$,

c) $\bigwedge pq \in I\ p \lor q \in I$.

Diremos que es un *ideal primo* si además cumple

d) $\bigwedge p \in \mathbb{B}\ p \in I \lor p' \in I$.

Un *filtro* de $\mathbb{B}$ es un conjunto $F \subset \mathbb{B}$ que cumpla las propiedades siguientes:

a) $\mathbb{O} \notin F \land \mathbb{1} \in F$,

b) $\bigwedge p \in F \bigwedge q \in \mathbb{B}\ (p \leq q \to q \in F)$,

c) $\bigwedge pq \in F\ p \land q \in F$.

Diremos que es un *ultrafiltro* si además cumple

d) $\bigwedge p \in \mathbb{B}\ p \in F \lor p' \in F$.

Es claro entonces 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).

Notemos también que los ideales y los filtros definidos en 6.10 son los ideales y los filtros de las álgebras $\mathcal{P}X$.

Hemos definido así el concepto de ideal de un álgebra para que la definición no dependa del teorema 10.33, 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 $x + y \leq x \lor y$, luego $x + y \in I$, y si $x \in \mathbb{B} \land y \in I$, 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 $\mathbb{O} \in I \land \mathbb{1} \notin I$, si $p \in I \land q \in \mathbb{B} \land q \leq p$, entonces $q = qp \in I$, y si $p, q \in I$, entonces $p \lor q = p + q + pq \in I$, 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 $\mathbb{B}$, representaremos por $\mathbb{B}/I$ al anillo cociente correspondiente, que tiene estructura de álgebra de Boole con las operaciones dadas por

$$[p] \land [q] = [p \land q], \quad [p] \lor [q] = [p \lor q], \quad [p]' = [p'].$$

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 que $\mathbb{1} \notin I$, 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 1.34 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 $F \subsetneq G \subsetneq \mathbb{B}$.

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 10.35 *Sea $\mathbb{B}$ un álgebra de Boole.*

a) La intersección de una familia de ideales/filtros de $\mathbb{B}$ es un ideal/filtro.

b) 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.*

c) Si $X \subset \mathbb{B}$ no contiene cubrimientos finitos, entonces el conjunto

$$(X)_i = \{p \in \mathbb{B} \mid \textit{existen } n \in \omega \textit{ y } x_1, \ldots, x_n \in X \textit{ tales que } p \leq x_1 \vee \cdots \vee x_n\}$$

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.*

d) 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 el 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

$$\mathcal{I} = \{X \in \mathcal{P}A \mid X \text{ es finito}\}$$

es un ideal en $\mathcal{P}A$, cuyo filtro dual es el formado por los conjuntos cofinitos:

$$\mathcal{F} = \{X \in \mathcal{P}A \mid A \setminus X \text{ es finito}\}.$$

Acabamos de justificar que un ultrafiltro F es libre si y sólo si $\mathcal{F} \subset F$. ■

La existencia de ultrafiltros libres no puede demostrarse sin AE, pero una aplicación elemental del lema de Zorn (compárese con 3.29) nos da los teoremas siguientes:

Teorema 10.36 (de los ideales primos) (AE) *Todo ideal en un álgebra de Boole puede extenderse hasta un ideal primo.*

Teorema 10.37 (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.

Dedicaremos la sección siguiente a estudiar los ultrafiltros de un álgebra de Boole. Terminamos esta sección dando condiciones suficientes para que un álgebra cociente sea completa basándonos en el teorema 10.27:

Definición 10.38 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 10.39 (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 $\big[\bigvee\limits_{p\in X} p\big]$ 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 $\big[\bigvee\limits_{p\in X} p\big] \leq [q]$. Esto prueba que $\big[\bigvee\limits_{p\in X} p\big]$ es el supremo de Y. ■

Consideramos ahora la condición de cadena κ:

Definición 10.40 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 toda anticadena en $\mathbb{B} \setminus I$ tiene cardinal menor que κ.

Teorema 10.41 (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 el álgebra $\mathbb{B}/I$ cumple la c.c.κ.*

DEMOSTRACIÓN: Supongamos que I cumple la c.c.κ 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 $p_\beta \wedge \bigvee\limits_{\alpha<\beta} p_\alpha \in I$.

Si $q_\beta \in I$ entonces $p_\beta = (p_\beta \wedge \bigwedge\limits_{\alpha<\beta} p'_\alpha) \vee (p_\beta \wedge \bigvee\limits_{\alpha<\beta} p_\alpha) \in I$, 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 10.27 nos da que el cociente de un álgebra κ-completa sobre un ideal κ-completo y κ-saturado es un álgebra completa.

10.4 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 10.33, 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 10.36, o de 10.37, que es equivalente.

Definición 10.42 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 10.43 (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[4] $p = \mathbb{O}$. 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 10.37, está contenido en un ultrafiltro. Por consiguiente $p = \mathbb{O}$. ■

Veamos ahora que el teorema de Stone se puede refinar notablemente:

[4]Esto es cierto para todo homomorfismo de anillos: si $h(u) = 0 \rightarrow u = 0$ entonces h es un monomorfismo, pues si $h(u) = h(v)$, entonces $h(u - v) = 0$, luego $u - v = 0$, luego $u = v$.

Definición 10.44 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 10.45 *Sea $\mathbb{B}$ un álgebra de Boole. Entonces $S(\mathbb{B})$ es un espacio de Hausdorff compacto cero-dimensional*[5] *y $\tilde{B}$ 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 $x \in C_p \land y \in C_{p'}$, 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, por las observaciones tras la definición 8.53, podemos considerarlo 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 $p_1 \lor \cdots \lor p_n \neq \mathbb{1}$, 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 teoremas siguientes demuestran que hay una correspondencia natural entre las álgebras de Boole y los espacios compactos cero-dimensionales.

Teorema 10.46 *Sea K un espacio compacto cero-dimensional 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. ∎

[5] Un espacio topológico compacto es *cero-dimensional* si tiene una base formada por abiertos-cerrados.

Teorema 10.47 *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

$$\bigwedge x \in S(\mathbb{C})(x \in C_q \leftrightarrow f^*(x) \in C_p),$$

luego

$$\bigwedge x \in S(\mathbb{C})(x \in C_q \leftrightarrow p \in f^*(x)),$$

luego

$$\bigwedge x \in S(\mathbb{C})(x \in C_q \leftrightarrow f(p) \in x),$$

luego

$$\bigwedge x \in S(\mathbb{C})(x \in C_q \leftrightarrow c \in C_{f(p)}),$$

y esto significa que $C_q = C_{f(p)}$, por lo que $f(p) = q$. Así pues, f es suprayectiva.

■

Teorema 10.48 *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 las fórmulas siguientes:

$(g^*)^{-1}[C_p] = C_q$

$\bigwedge x \in S(\mathbb{C})(p \in g^*(x) \leftrightarrow q \in x)$

$\bigwedge x \in S(\mathbb{C})(g(p) \in x \leftrightarrow q \in x)$

$\bigwedge x \in S(\mathbb{C})(x \in C_{g(p)} \leftrightarrow x \in C_q)$,

$C_{g(p)} = C_q$,

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 cero-dimensional (su espacio de Stone) y a cada espacio compacto cero-dimensional 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 10.5: 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. ■

Existe una correspondencia biunívoca entre los filtros de un álgebra de Boole $\mathbb{B}$ y los cerrados de su espacio de Stone. Concretamente, para cada filtro F, el epimorfismo canónico $p : \mathbb{B} \longrightarrow \mathbb{B}/F$ se corresponde con una aplicación inyectiva y continua $p^* : S(\mathbb{B}/F) \longrightarrow S(\mathbb{B})$ que determina el cerrado $C_F = p^*[S(\mathbb{B}/F)]$. Recíprocamente, si $C \subset S(\mathbb{B})$ es un cerrado, la inclusión $i : C \longrightarrow S(\mathbb{B})$ se corresponde con un epimorfismo $i^* : \mathbb{B} \longrightarrow \mathbb{C}$, donde $\mathbb{C}$ es el álgebra de abiertos-cerrados de C. Entonces $F_C = (i^*)^{-1}[\{\mathbb{1}\}]$ es un filtro en $\mathbb{B}$ y es fácil ver que estas dos correspondencias que hemos definido son mutuamente inversas.

Observemos para terminar 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 el conjunto de sus átomos es denso, lo cual equivale a que los puntos aislados en $S(\mathbb{B})$ sean un conjunto denso.

Teorema 10.49 *Un álgebra de Boole $\mathbb{B}$ es completa si y sólo si su espacio de Stone es extremadamente disconexo, es decir, 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 $\operatorname{cl} \bigcup\limits_{A \in X} A$ es el supremo de X. ■

Nota Observemos que 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 los supremos coincidieran con las uniones (luego los ínfimos con las intersecciones), entonces $\mathbb{C}$ sería completamente distributiva y $\mathbb{B}$ también. Por lo tanto, si partimos de un álgebra $\mathbb{B}$ que no sea completamente distributiva, tenemos un ejemplo de subálgebra de un álgebra completa que es completa pero no es una subálgebra completa. ■

10.5 Aplicaciones a la topología

Terminamos el capítulo con algunas aplicaciones a la topología de los conceptos que acabamos de introducir. No usaremos el axioma de elección si no lo especificamos.

Convergencia de filtros En primer lugar mostraremos que los filtros pueden sustituir a las sucesiones en las caracterizaciones de algunos conceptos topológicos en espacios no necesariamente 1AN.

Definición 10.50 Un filtro en un espacio topológico X es un filtro en el álgebra $\mathcal{P}X$. Diremos que un filtro F *converge* a un punto $x \in X$ si contiene a todos los entornos de x. Diremos que $x \in X$ es un *punto de acumulación* de un filtro F si $x \in \bigcap\limits_{A \in F} \overline{A}$.

Veamos algunas propiedades elementales:

a) Si F converge a x entonces x es un punto de acumulación de F, pues si $A \in F$ y U es un entorno de x, tenemos que $U \in F$, luego $A \cap U \in F$, luego $A \cap U \neq \varnothing$, luego $x \in \overline{A}$.

b) Si F es un ultrafiltro y x es un punto de acumulación de F, entonces F converge a x. En efecto, si U es un entorno de x pero $U \notin F$, entonces $X \setminus U \in F$, luego $x \in \overline{X \setminus U} = X \setminus \mathring{U}$, pero esto contradice que U sea un entorno de X.

c) Si X es un espacio de Hausdorff, cada filtro tiene a lo sumo un límite, pues si $x \neq y$ son dos puntos de X, tienen entornos disjuntos U y V, y no pueden estar ambos en un mismo filtro.

d) Un espacio X es compacto si y sólo si todo filtro tiene un punto de acumulación.

   En efecto, si X es compacto y F es un filtro, la familia $\{\overline{A} \mid A \in F\}$ tiene la propiedad de la intersección finita, luego existe $x \in \bigcap\limits_{A \in F} \overline{A}$, y x es un punto de acumulación de F.

   Si los filtros tienen puntos de acumulación y $\mathcal{F}$ es una familia de cerrados con la propiedad de la intersección finita, entonces $\mathcal{F}$ está contenida en un filtro $F = (\mathcal{F})_f$, y si x es un punto de acumulación de F, tenemos que $x \in \bigcap\limits_{A \in \mathcal{F}} A \neq \varnothing$, luego X es compacto.

   La propiedad siguiente se apoya en AE en la forma del teorema de los ultrafiltros (TU):

e) **[TU]** Un espacio X es compacto si y sólo si todo ultrafiltro converge a un punto.

   En efecto, si X es compacto, entonces todo ultrafiltro tiene un punto de acumulación, y hemos visto que converge a él. Recíprocamente, si F es un filtro en X, por el teorema de los ultrafiltros está contenido en un ultrafiltro U, y si U converge a x, sabemos que es un punto de acumulación de U, y trivialmente también lo es de F.

Si $f : X \longrightarrow Y$ es una aplicación, sabemos que induce un homomorfismo de álgebras $f^* : \mathcal{P}Y \longrightarrow \mathcal{P}X$ dado por $f^*(A) = f^{-1}[A]$, luego para cada filtro F en X tenemos definida su imagen

$$f(F) = (f^*)^{-1}[F] = \{A \in \mathcal{P}Y \mid f^{-1}[A] \in F\},$$

que sabemos que es un filtro, y de hecho un ultrafiltro si F lo es.

Teorema 10.51 *Una función $f : X \longrightarrow Y$ entre espacios topológicos es continua en un punto $x \in X$ si y sólo si para todo filtro F en X que converge a x se cumple que $f(F)$ converge a $f(x)$.*

DEMOSTRACIÓN: Si f es continua en X y F converge a x dado un entorno U de $f(x)$ sabemos que $f^{-1}[U]$ es un entorno de X, luego $f^{-1}[U] \in F$, luego $U \in f(F)$, luego F converge a $f(x)$.

Recíprocamente, si se cumple esta propiedad y sea F el conjunto de los entornos de x, que claramente es un filtro y converge a x, luego $f(F)$ converge a $f(x)$. Si U es un entorno de $f(x)$, entonces $U \in f(F)$, luego $f^{-1}[U] \in F$, luego $f^{-1}[U]$ es un entorno de x y f es continua. ■

Teorema 10.52 *Sea* $X = \prod\limits_{i \in I} X_i$ *un producto de espacios topológicos y sea* $x \in X$. *Un filtro* F *en* X *converge a* x *si y sólo si cada filtro* $p_i(X)$ *converge a* x_i, *donde* $p_i : X \longrightarrow X_i$ *es la proyección i-ésima.*

DEMOSTRACIÓN: Si F converge a x, el teorema anterior nos da que cada $p_i(F)$ converge a x_i. Si convergen las proyecciones, basta probar que cada abierto básico $B = \bigcap\limits_{i \in I} p_i^{-1}[A_i]$ que contenga a x está en F. Ahora bien, si $x \in B$, entonces $x_i \in A_i$, luego A_i es un entorno de x_i, luego $A_i \in p_i(F)$, luego $p_i^{-1}[A_i] \in F$, luego $B \in F$, porque la intersección finita de elementos de F está en F. Por lo tanto, F converge a x. ■

Con esto ya podemos dar una prueba sencilla del teorema de Tychonoff:

Teorema 10.53 (Tychonoff) (AE) *Todo producto* $X = \prod\limits_{i \in I} X_i$ *de espacios compactos es compacto.*

DEMOSTRACIÓN: Basta probar que todo ultrafiltro F en X converge. Para ello consideramos las proyecciones $p_i(F)$, que son ultrafiltros en cada X_i, luego convergen. Elijamos un $x_i \in X_i$ tal que $p_i(F)$ converja a x_i. Entonces F converge a x. ■

Nota En la prueba del teorema anterior hemos usado AE en dos ocasiones: primero al elegir un x_i al que converja cada $p_i(X)$ y luego al aplicar la caracterización de los compactos en términos de ultrafiltros. Ahora bien, si los espacios X_i son de Hausdorff, entonces cada $p_i(F)$ tiene un único límite, luego podemos suprimir el primer uso de AE, y el segundo requiere únicamente el teorema de los ultrafiltros, luego tenemos que (TU) implica que el producto de espacios de Hausdorff compactos es compacto. ■

Condiciones de cadena en productos La segunda aplicación que vamos a ver está relacionada con la conservación de las condiciones de cadena en productos de espacios topológicos.

En general, diremos que un espacio X cumple la *condición de cadena* κ si toda familia de abiertos disjuntos dos a dos tiene cardinal $< \kappa$ (de modo que la condición de cadena numerable es la condición de cadena $\aleph_1$).

Vamos a probar que el problema de si la condición de cadena κ se conserva en productos equivale a que se conserve en c.p.o.s.

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

$$(p, q) \leq (p', q') \leftrightarrow p \leq p' \land q \leq q'.$$

Teorema 10.54 (AE) *Si κ es un cardinal infinito, las afirmaciones siguientes son equivalentes:*

a) Existen espacios topológicos con la condición de cadena κ cuyo producto no cumple la condición de cadena κ.

b) Existen dos c.p.o.s con la condición de cadena κ cuyo producto no cumple la condición de cadena κ.

c) 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 a), 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 b). 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 cero-dimensionales 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 $X_1 \times X_2$. ■

En 9.3 demostramos que el producto de una recta de Suslin por sí misma no tiene la c.c.n., luego en particular $\diamondsuit$ implica que el producto de espacios topológicos no conserva en general la c.n.n. Ahora estamos en condiciones de probar esto mismo suponiendo únicamente la hipótesis del continuo:

Definición 10.55 Si A y B son conjuntos cualesquiera, usaremos la notación

$$A \otimes B = \{\{a, b\} \mid a \in A \land b \in B\}$$

Si κ es un cardinal infinito y $K \subset [\kappa]^2$, llamaremos

$$\mathbb{P}(\kappa, K) = \{F \in \mathcal{P}^f\kappa \mid [F]^2 \subset K\},$$

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 10.56 (AE) *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 elemento $a \in A$, 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 $E = \bigcup\limits_{\beta<\eta} E_\beta$ 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 $i_{\delta\epsilon}^\alpha = i_{f(\alpha,\delta,\epsilon)}$, tenemos que los conjuntos $E_{i_{\delta\epsilon}^\alpha}^\alpha$ son disjuntos dos a dos. Ahora basta definir

$$A_\delta = \bigcup_{\alpha,\epsilon<\kappa} E_{i_{\delta\epsilon}^\alpha}^\alpha,$$

y claramente se cumple lo pedido. ■

Teorema 10.57 (Galvin, Laver) (AE) *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.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.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 $X_\eta = \{x_\eta^\epsilon\}_{\epsilon<\kappa}$. Notemos que el número de tales sucesiones es

$$\leq (\mathcal{P}^f\kappa^+)^\kappa = (\kappa^+)^\kappa = 2^\kappa\kappa^+ = \kappa^+,$$

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 $i \in \{1,2\}$, $\eta < \gamma$, $\bigcup\limits_{\epsilon<\kappa} x_\eta^\epsilon \subset \gamma$, $a \in \mathcal{P}^f\gamma$ y $|\{\epsilon < \kappa \mid x_\eta^\epsilon \otimes a \subset K_i\}| = \kappa$, entonces $|\{\epsilon < \kappa \mid x_\eta^\epsilon \otimes a \subset K_i \land x_\eta^\epsilon \subset K_i(\gamma)\}| = \kappa$ o, equivalentemente,

$$|\{\epsilon < \kappa \mid x_\eta^\epsilon \otimes (a \cup \{\gamma\}) \subset K_i\}| = \kappa.$$

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 $x_\eta^\epsilon \otimes a \subset K_i$ significa que si $\{u, v\} \in x_\eta^\epsilon \otimes a$, 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 $A = \gamma$, $I_\alpha = \{\epsilon < \kappa \mid x_{\eta_\alpha}^\epsilon \otimes a_\alpha \subset K_{i_\alpha}\}$ y $E_\epsilon^\alpha = x_{\eta_\alpha}^\epsilon$ (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.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 8.52) 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 $x_\eta^\epsilon = F_\epsilon$, para todo $\epsilon < \kappa$, sea $\gamma_0 < \kappa^+$ tal que $\bigcup\limits_{\epsilon<\kappa} x_\eta^\epsilon \subset \gamma_0$ 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 $|\{\epsilon < \kappa \mid x_\eta^\epsilon \otimes F_{\epsilon'} \subset K_i\}| = \kappa$. En particular, tomando cualquier ϵ de este conjunto, tenemos que $\epsilon < \epsilon'$ y $F_\epsilon \otimes F_{\epsilon'} \subset K_i$. ■

Así pues:

Teorema 10.58 (AE) *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^+.*

Los espacios βD Terminamos describiendo brevemente los espacios de Stone más sencillos, los de las álgebras $\mathcal{P}D$, para un conjunto arbitrario $D \neq \varnothing$. En toda esta sección usaremos tácitamente el axioma de elección o, más concretamente, el teorema de los ultrafiltros.

Definición 10.59 Representaremos por βD el espacio de Stone del álgebra de Boole $\mathcal{P}D$. Sabemos que es un espacio de Hausdorff compacto extremadamente disconexo (por 10.49).

A cada $d \in D$ podemos asociarle el ultrafiltro $U_d = \{X \in \mathcal{P}D \mid d \in X\}$, de modo que la aplicación $D \longrightarrow \beta D$ dada por $d \mapsto U_d$ es inyectiva. Esto nos permite identificar cada elemento de D con el ultrafiltro principal que genera, y considerar $D \subset \beta D$.

Sabemos que los abiertos básicos de βD son los conjuntos de la forma

$$C_A = \{x \in \beta D \mid A \in x\},$$

para cada $A \subset D$, así como que la aplicación $A \mapsto C_A$ es un isomorfismo entre $\mathcal{P}D$ y el álgebra de abiertos cerrados de βD.

Observemos que, a través de la identificación $A \subset D \subset \beta D$, sucede que C_A no es sino la clausura de A en βD.

En efecto, si $d \in A$, entonces $A \in U_d$, luego $U_d \in C_A$. A través de la identificación esto no es sino la inclusión $A \subset C_A$ y, como C_A es cerrado, de hecho $\overline{A} \subset C_A$. Por otro lado, si $x \in C_A$, un entorno básico de x es de la forma C_B, para cierto $B \subset D$ tal que $B \in x$, y entonces, como también $A \in x$, tenemos que $A \cap B \in x$, y $\varnothing \neq A \cap B \subset C_{A\cap B} = C_A \cap C_B$, luego $A \cap C_B \neq \varnothing$. Por lo tanto, $x \in \overline{A}$.

Así pues, a partir de aquí escribiremos siempre $\overline{A}$ en lugar de C_A.

En particular $\overline{D} = \beta D$, luego D es denso en βD.

Notemos también que $\overline{A} \cap D = A$, pues si $d \in \overline{A} \cap D$, esto significa que $A \in U_d$, luego $d \in A$.

Como los puntos son cerrados, tenemos que $\overline{\{d\}} = \{d\}$, luego $\{d\}$ es un abierto básico de βD y, en particular, es abierto en D. Concluimos que la topología que βD induce en D es la discreta[6] y que D es abierto en βD.

El teorema siguiente resume parte de lo que hemos obtenido hasta aquí junto con una propiedad fundamental de βD:

Teorema 10.60 *Si D es un conjunto no vacío, entonces βD es un espacio de Hausdorff compacto que contiene a D como subespacio abierto discreto. Además, toda aplicación $f : D \longrightarrow K$ en un espacio de Hausdorff compacto tiene una única extensión continua $\bar{f} : \beta D \longrightarrow K$.*

[6] En topología se dice que βD es una *compactificación* del espacio discreto D, es decir, un espacio de Hausdorff compacto que contiene a D como subconjunto denso.

Demostración: Sólo falta demostrar la última propiedad. Dada una aplicación $f : D \longrightarrow K$, para cada $x \in \beta D$ consideramos el ultrafiltro

$$f^*(x) = \{A \in \mathcal{P}K \mid f^{-1}[A] \in x\}.$$

Como K es compacto y de Hausdorff, hemos visto que $f^*(x)$ converge a un único punto $\bar{f}(x) \in K$, lo que nos define una aplicación $\bar{f} : \beta D \longrightarrow K$.

Se trata de una aplicación continua, pues si $G \subset K$ es abierto y $x \in \bar{f}^{-1}[G]$, entonces $\bar{f}(x) \in G$. Podemos tomar un abierto G' tal que[7]

$$\bar{f}(x) \in G' \subset \overline{G}' \subset G.$$

Entonces $G' \in f^*(x)$ (por definición de convergencia de un filtro), luego $A = f^{-1}[G'] \in x$, luego $x \in \overline{A} \subset \bar{f}^{-1}[G]$. En efecto, la última inclusión se debe a que si $y \in \overline{A}$, entonces $f^{-1}[G'] \in y$, luego $G' \in f^*(y)$, luego $\bar{f}(y) \in \overline{G}' \subset G$. Por lo tanto, $\bar{f}^{-1}[G]$ es entorno de x y, por consiguiente, es abierto.

Por último, si $d \in D$, tenemos que $f^*(d) = \{A \in \mathcal{P}K \mid f(d) \in A\}$, que claramente converge a $f(d)$, luego $\bar{f}(d) = f(d)$, con lo que $\bar{f}$ extiende a f.

La unicidad de la extensión es inmediata, pues si dos aplicaciones continuas coinciden sobre un subconjunto denso son iguales. ■

Nota Las propiedades del teorema anterior determinan βD como espacio topológico salvo homeomorfismo, en el sentido de que si $\beta' D$ es otro espacio de Hausdorff compacto que contiene a D como subespacio denso discreto y satisface la misma propiedad de extensión, entonces la identidad en D se extiende a un homeomorfismo $\beta D \longrightarrow \beta' D$.

En general, la existencia de un (único) espacio de Hausdorff compacto βX que contiene a X como subespacio denso con la propiedad de que toda función continua $f : X \longrightarrow K$, para cualquier espacio de Hausdorff compacto K, admite una única extensión a βX puede demostrarse para una familia de espacios topoógicos X mucho más amplia que la de los espacios discretos, a saber, los llamados espacios *completamente regulares,* y la compactificación βX recibe el nombre de *compactificación de Stone-Čech* del espacio X.

Así pues, el espacio βD que estamos considerando es lo que en topología se conoce como *compactificación de Stone-Čech* del espacio discreto D. ■

Vamos a calcular el cardinal de βD. Obviamente, si D es finito, entonces D es cerrado en βD, luego $\beta D = D$. Si D es infinito, es inmediato que $|\beta D| \leq 2^{2^{|D|}}$. Vamos a probar que se da la igualdad. De hecho probaremos algo ligeramente más fuerte:

[7]Esto se sigue de que K es un compacto de Hausdorff: para cada $y \in K \setminus G$ existen abiertos disjuntos U_y, V_y tales que $f(x) \in U_y$, $y \in V_y$. Basta tomar un subcubrimiento finito $V_{y_1}, \ldots, V_{y_n}$ del compacto $K \setminus G$ y tomar $G' = \bigcap U_{y_i}$, $H = \bigcup V_{y_i}$. Así

$$f(x) \in G' \subset \overline{G}' \subset K \setminus H \subset G.$$

Definición 10.61 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 10.62 (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 $X_1, \ldots, X_m, Y_1, \ldots, Y_n \in C$ 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 $P = \mathcal{P}^f D \times \mathcal{P}^f \mathcal{P}^f D$.

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 $u_1, \ldots, u_m, v_1, \ldots, v_n$ 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 $B = \{A \cap u_i \mid i = 1, \ldots, m\}$, 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

$$G_f = \{X \in \mathcal{P}D \mid |D \setminus X| < |D|\} \cup \{X \in C \mid f(X) = 1\} \cup$$
$$\{D \setminus X \mid X \in C \land f(X) = 0\}.$$

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 10.35 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 $D \setminus X \in U_g$. ■

Como consecuencia inmediata:

Teorema 10.63 *Si D es un conjunto infinito, entonces $|\beta D| = 2^{2^{|D|}}$.*

Definición 10.64 Si D es un conjunto infinito, llamamos $D^* = \beta D \setminus D$, que es un espacio de Hausdorff compacto con la topología inducida de βD. Una base es la formada por los abiertos-cerrados $A^* = \overline{A} \cap D^* = \overline{A} \setminus A$, donde A recorre los subconjuntos de D.

Observemos que $A^* = \varnothing$ si y sólo si A es finito, pues, ciertamente, si A es finito entonces $\overline{A} = A$, y si A es infinito, el conjunto

$$\{A\} \cup \{X \in \mathcal{P}D \mid |D \setminus X| < \aleph_0\}$$

tiene la propiedad de la intersección finita, luego está contenido en un filtro que a su vez está contenido en un ultrafiltro no principal $x \in \overline{A} \setminus A$.

Por otro lado, todo abierto-cerrado de D^* es de la forma A^*, para cierto $A \subset D$. En efecto, en principio es unión de conjuntos de la forma A^*, pero por compacidad la unión se puede tomar finita, pero una unión finita de conjuntos de la forma A^* es también un conjunto A^*.

En definitiva, la aplicación $p : \mathcal{P}D \longrightarrow \mathbb{B}^*$ dada por $A \mapsto A^*$ es un epimorfismo en el álgebra $\mathbb{B}^*$ de abiertos-cerrados de D^* tal que $p(A) = \mathbb{O} \leftrightarrow A$ es finito. De aquí se sigue a su vez que si llamamos $\mathrm{Fin} = \mathcal{P}^f D$ al ideal de los subconjuntos finitos de $\mathcal{P}D$, entonces $\bar{p} : \mathcal{P}D/\mathrm{Fin} \longrightarrow \mathbb{B}^*$ dada por $\bar{p}([A]) = A^*$ es un isomorfismo de álgebras de Boole, lo que a su vez se traduce en que D^* es homeomorfo al espacio de Stone del álgebra $\mathcal{P}D/\mathrm{Fin}$.

Observemos que el álgebra $\mathcal{P}D/\mathrm{Fin}$ no es completa, por lo que D^* no es extremadamente disconexo.

En efecto, basta considerar una partición $\{D_n\}_{n\in\omega}$ de D en conjuntos infinitos. Si $d_n = [D_n] \in \mathcal{P}D/\mathrm{Fin}$, tenemos que el conjunto $\{d_n \mid n \in \omega\}$ no tiene supremo, ya que si $c = [C]$ es una cota superior, esto significa que $d_n \leq c$, es decir, que $D_n \setminus C$ es finito, luego si elegimos $x_n \in D_n \cap C$, llamamos $X = \{x_n \mid n \in \omega\}$ y tomamos $c^* = [C \setminus X] \neq \mathbb{O}$, sucede que $d_n \leq c^*$, pues $D_n \setminus (C \setminus X) = (D_n \setminus C) \cup \{x_n\}$ es finito, pero no se cumple $c \leq c^*$, pues $X \subset C \setminus (C \setminus X)$ es infinito.

Una última observación es que $\beta\omega$ es separable, luego cumple la c.c.n., mientras que el teorema 9.25 implica que ω^* contiene $2^{\aleph_0}$ abiertos disjuntos dos a dos.

Ejercicio: Probar que si $A \subset D$ entonces $\overline{A}$ es homeomorfo a βA. En particular si A es infinito A^* también lo es. Concluir que D^* no tiene puntos aislados.

Capítulo XI

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.

11.1 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 11.1 Un *lenguaje formal* (de primer orden) es una óctupla ordenada

$$\mathcal{L} = (V, F, R, r, \neg, \rightarrow, \bigwedge, =),$$

tal que

a) V es un conjunto infinito a cuyos elementos llamaremos *variables* de $\mathcal{L}$,

b) F es un conjunto arbitrario (tal vez vacío) a cuyos elementos llamaremos *funtores* de $\mathcal{L}$,

c) R es un conjunto arbitrario a cuyos elementos llamaremos *relatores* de $\mathcal{L}$,

d) Los conjuntos V, F y R son disjuntos dos a dos.

e) $r : F \cup R \longrightarrow \omega$, 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 $\mathcal{L}$.

f) $\neg$, $\rightarrow$, $\bigwedge$, $=$ 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

$$\mathrm{Sig}(\mathcal{L}) = \mathrm{Var}(\mathcal{L}) \cup \mathrm{Const}(\mathcal{L}) \cup \bigcup_{n\in\omega\setminus\{0\}} \mathrm{Fn}_n(\mathcal{L}) \cup \bigcup_{n\in\omega\setminus\{0\}} \mathrm{Rel}_n(\mathcal{L}) \cup \{\neg, \rightarrow, \bigwedge\}.$$

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 $\mathfrak{L}$ 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 $\mathfrak{L}_a$ 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 $\mathfrak{L}_a$. Podríamos hacerlo, pero sería del todo irrelevante.[2] Si a $\mathfrak{L}_a$ le añadimos un relator diádico $\leq$ tenemos el *lenguaje $\mathfrak{L}_{ao}$ de la teoría de anillos ordenados.* ■

Un *modelo* de un lenguaje formal $\mathfrak{L}$ 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

$$\mathrm{Const}(\mathfrak{L}) \cup \bigcup_{n\in\omega\setminus\{0\}} \mathrm{Fn}_n(\mathfrak{L}) \cup \bigcup_{n\in\omega\setminus\{0\}} \mathrm{Rel}_n(\mathfrak{L})$$

tal que:

a) Si $c \in \mathrm{Const}(\mathfrak{L})$ entonces $I(c) \in M$.

b) Si $f \in \mathrm{Fn}_n(\mathfrak{L})$ entonces $I(f) : M^n \longrightarrow M$.

c) Si $R \in \mathrm{Rel}_n(\mathfrak{L})$ 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 $\mathfrak{L}$ 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 $\neg$, $\rightarrow$, $\bigwedge$ 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 $\mathfrak{L}_a$:

$$== +\neg\rightarrow, \qquad 1\cdot 1+1+0 \qquad 1+1=0\rightarrow 1+1+1=1.$$

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 $\mathfrak{L}$ emplearemos el teorema de recursión sobre la relación bien fundada en $\mathrm{Cad}(\mathfrak{L})$ 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 $f : \mathrm{Cad}(\mathfrak{L}) \longrightarrow 2$ 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]

a) Las variables y las constantes de $\mathfrak{L}$ son *términos.*

b) Si $t_1, \ldots, t_n$ son términos de $\mathfrak{L}$ y f es un funtor n-ádico de $\mathfrak{L}$, entonces $ft_1 \cdots t_n$ es un *término* de $\mathfrak{L}$.

[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*:

a) 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 $\mathcal{L}$.

b) Si α, β son fórmulas de $\mathcal{L}$, también lo son $\neg\alpha$ y $\rightarrow \alpha\beta$.

c) 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 $\rightarrow \alpha\beta$ escribiremos $\alpha \rightarrow \beta$. Definimos también:

$$\alpha \vee \beta = \neg\alpha \rightarrow \beta, \quad \alpha \wedge \beta = \neg(\neg\alpha \vee \neg\beta),$$

$$\alpha \leftrightarrow \beta = (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha), \qquad \bigvee x\alpha = \neg\bigwedge x\neg\alpha.$$

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

$$\{(0, \bigwedge), (1, x), (2, \bigwedge), (3, y), (4, =), (5, +), (6, x), (7, y), (8, +), (9, y), (10, x)\}.$$

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 $v : \mathrm{Var}(\mathcal{L}) \longrightarrow M$.

De este modo, cada valoración asigna un significado a cada variable de $\mathcal{L}$.

[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.

Si v es una valoración de $\mathfrak{L}$ en M, x es una variable de $\mathfrak{L}$ 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 $M(t)[v]$:

a) Si x es una variable, $M(x)[v] = v(x)$.

b) Si c es una constante, $M(c)[v] = \bar{c}$.

c) 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 $\mathrm{Form}(\mathfrak{L}) \times \mathrm{Val}(M)$, 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 $F : \mathrm{Form}(\mathfrak{L}) \times \mathrm{Val}(M) \longrightarrow 2$ 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:

a) $M \vDash Rt_1 \cdots t_n[v]$ si y sólo si $\bar{R}(M(t_1)[v], \ldots, M(t_n)[v])$.

b) $M \vDash \neg\alpha[v]$ si y sólo si no $M \vDash \alpha[v]$.

c) $M \vDash (\alpha \rightarrow \beta)[v]$ si y sólo si no $M \vDash \alpha[v]$ o bien $M \vDash \beta[v]$.

d) $M \vDash \bigwedge x\alpha[v]$ 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:

a) $M \vDash (\alpha \vee \beta)[v]$ si y sólo si $M \vDash \alpha[v]$ o $M \vDash \beta[v]$.

b) $M \vDash (\alpha \wedge \beta)[v]$ si y sólo si $M \vDash \alpha[v]$ y $M \vDash \beta[v]$.

c) $M \vDash (\alpha \leftrightarrow \beta)[v]$ si y sólo si $M \vDash \alpha[v]$ y $M \vDash \beta[v]$ o bien no $M \vDash \alpha[v]$ y no $M \vDash \beta[v]$.

d) $M \vDash \bigvee x\alpha[v]$ 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 $\mathfrak{L}$ (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 $\neg$, $\rightarrow$, $\bigwedge$, $\bigvee$, 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:

a) $\mathrm{Vlib}(Rt_1, \ldots, t_n) = \mathrm{Vlib}(t_1) \cup \cdots \cup \mathrm{Vlib}(t_n)$,

b) $\mathrm{Vlib}(\neg\alpha) = \mathrm{Vlib}(\alpha)$,

c) $\mathrm{Vlib}(\alpha \rightarrow \beta) = \mathrm{Vlib}(\alpha) \cup \mathrm{Vlib}(\beta)$,

d) $\mathrm{Vlib}(\bigwedge x\, \alpha) = \mathrm{Vlib}(\alpha) \setminus \{x\}$.

A partir de aquí se demuestra inmediatamente que

a) $\mathrm{Vlib}(\alpha \vee \beta) = \mathrm{Vlib}(\alpha) \cup \mathrm{Vlib}(\beta)$,

b) $\mathrm{Vlib}(\alpha \wedge \beta) = \mathrm{Vlib}(\alpha) \cup \mathrm{Vlib}(\beta)$,

c) $\mathrm{Vlib}(\alpha \leftrightarrow \beta) = \mathrm{Vlib}(\alpha) \cup \mathrm{Vlib}(\beta)$,

d) $\mathrm{Vlib}(\bigvee x\, \alpha) = \mathrm{Vlib}(\alpha) \setminus \{x\}$.

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 11.2 *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.*

a) Si v y w coinciden en $\mathrm{Vlib}(t)$*, entonces $M(t)[v] = M(t)[w]$.*

b) 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 $\alpha \rightarrow \beta$. 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.

$$M \vDash \textstyle\bigwedge x\, \alpha[v] \text{ syss para todo } a \in M \ M \vDash \alpha[v_x^a]$$
$$\text{syss para todo } a \in M \ M \vDash \alpha[w_x^a] \text{ syss } M \vDash \textstyle\bigwedge x\, \alpha[w],$$

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.

11.2 Teorías formales

Definición 11.3 Sea $\mathfrak{L}$ un lenguaje formal y sea $\Gamma \subset \mathrm{Form}(\mathfrak{L})$ 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 $\mathfrak{L}$ 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.

Una *teoría* sobre un lenguaje formal $\mathfrak{L}$ es un conjunto T de sentencias de $\mathfrak{L}$ tal que si $\alpha \in \mathrm{Sent}(\mathfrak{L})$ y $T \vDash \alpha$, entonces $\alpha \in T$.

Si $\Gamma \subset \mathrm{Sent}(\mathfrak{L})$ es claro que

$$T(\Gamma) = \{\alpha \in \mathrm{Sent}(\mathfrak{L}) \mid \Gamma \vDash \alpha\}$$

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 $\mathfrak{L}$, también es claro que

$$T(M) = \{\alpha \in \mathrm{Sent}(\mathfrak{L}) \mid M \vDash \alpha\}$$

es una teoría sobre $\mathfrak{L}$.

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 $\bigwedge x(x \neq 0 \rightarrow \bigvee y\ xy = 1)$ 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 $\mathcal{L}$:

a) Existe $\alpha \in \mathrm{Sent}(\mathcal{L})$ tal que $\Gamma \vDash \alpha$ y $\Gamma \vDash \neg\alpha$.

b) Γ no tiene modelos.

c) $T(\Gamma) = \mathrm{Sent}(\mathcal{L})$.

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 11.4 *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] $\bigvee x\, \phi(x) \rightarrow \phi(c)$ *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 $\bigvee x\, \phi(x) \rightarrow \phi(c_\phi)$.

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 $\Gamma' = \bigcup\limits_{n\in\omega} \Gamma_n$. 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 11.5 *Sea $\mathcal{L}$ un lenguaje formal y sea T una teoría $\mathcal{L}$ tal que:*

a) T es finitamente consistente.

b) T es completa.

c) 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

$$(\bigvee x\ fc_1 \cdots c_n = x \rightarrow fc_1 \cdots c_n = c) \in T$$

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

$$\bigvee x\, t_j(c_1, \ldots, c_n) = x \rightarrow t_j(c_1, \ldots, c_n) = c'_j.$$

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

$$\bigvee x\ x = t_j(c_1, \ldots, c_n) \rightarrow c'_j = t_j(c_1, \ldots, c_n).$$

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

$$M \vDash \neg\alpha[[c_1,\ldots,c_n]] \quad \text{syss} \quad \neg M \vDash \alpha[[c_1],\ldots,[c_n]] \quad \text{syss} \quad \alpha(c_1,\ldots,c_n) \notin T$$

syss $\neg\alpha(c_1,\ldots,c_n) \in T$. En el último paso usamos que T es finitamente consistente y completa, pues por la completitud sabemos que $\alpha(c_1,\ldots,c_n) \in T$ o $\neg\alpha(c_1,\ldots,c_n) \in T$ 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),

$$M \vDash \phi[[c_1],\ldots,[c_n]] \quad \text{syss} \quad \neg M \vDash \alpha[[c_1],\ldots,[c_n]] \lor M \vDash \beta[[c_1],\ldots,[c_n]]$$

$$\text{syss} \quad \alpha(c_1,\ldots,c_n) \notin T \lor \beta(c_1,\ldots,c_n) \in T \quad \text{syss} \quad T \vDash \phi(c_1,\ldots,c_n)$$

syss $\phi(c_1,\ldots,c_n) \in T$.

Finalmente, si $\phi = \bigwedge x\, \alpha(x, x_1,\ldots,x_n)$ y el resultado vale para α,

$$M \vDash \phi[[c_1],\ldots,[c_n]] \quad \text{syss} \quad \bigwedge c \in \mathrm{Const}(\mathcal{L})\ M \vDash \alpha[[c],[c_1],\ldots,[c_n]]$$

$$\text{syss} \quad \bigwedge c \in \mathrm{Const}(\mathcal{L})\ \alpha(c, c_1,\ldots,c_n) \in T.$$

Veamos que esto implica que $\bigwedge x\, \alpha(x, c_1,\ldots,c_n) \in T$. En caso contrario, como existe una constante c tal que

$$\bigvee x\, \neg\alpha(x, c_1,\ldots,c_n) \to \neg\alpha(c, c_1,\ldots,c_n) \in T,$$

resulta que si $\bigwedge x\, \alpha(x, c_1,\ldots,c_n) \notin T$, entonces $\neg\bigwedge x\, \alpha(x, c_1,\ldots,c_n) \in T$, luego $T \vDash \bigvee x\, \neg\alpha(x, c_1,\ldots,c_n)$, luego $T \vDash \neg\alpha(c, c_1,\ldots,c_n)$, luego $\alpha(c, c_1,\ldots,c_n) \notin T$, contradicción.

Recíprocamente, si $\bigwedge x\, \alpha(x, c_1,\ldots,c_n) \in T$ y $c \in \mathrm{Const}(\mathcal{L})$, entonces es claro que $T \vDash \alpha(c, c_1,\ldots,c_n)$, luego $\alpha(c, c_1,\ldots,c_n) \in T$.

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 11.6 (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 11.4, 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 $M \vDash T$. En particular tenemos que $M \vDash \Gamma$. 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 $M_0 \vDash \Gamma$, 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 11.4 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 4.35 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 $T = \bigcup\limits_{n\in\omega} \Gamma'_n$. 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 $M \vDash \Delta \setminus \{\phi\}$, pero no puede ser $M \vDash \phi$, porque Δ es contradictorio, luego $M \vDash \neg\phi$, luego $M \vDash \Delta'$, 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 11.7 (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 11.5 (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 10.37:

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 11.8 *Las afirmaciones siguientes son equivalentes a* (TU):

a) *Toda álgebra de Boole tiene un ultrafiltro (resp. un ideal primo).*

b) *Todo filtro (resp. ideal) en un álgebra de Boole puede extenderse a un ultrafiltro (resp. ideal primo).*

c) *El principio de coherencia.*

d) *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

a) $\mathcal{D}z \subset I$.

b) $\bigwedge x \in \mathcal{D}z\ z(x) \in \mathcal{F}_x$.

c) $\bigwedge xy \in \mathcal{D}z\ (z(x) \cup z(y) : x \cup y \longrightarrow 2)$.

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 $\varnothing = Z_x \cap \bigcap\limits_i (Z \setminus Z_{t_i}) \in U$).

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 11.6, 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 $A = \operatorname{Sent}(\mathcal{L})$ 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 $\mathcal{L}$:

a) $\neg f\mathbb{O}$, $f\mathbb{1}$,

b) $fb \vee fb'$, para cada $b \in \mathbb{B}$,

c) $fb_1 \wedge \cdots \wedge fb_n \rightarrow f(b_1 \wedge \cdots \wedge b_n)$, 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 10.5 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 11.9 (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 (teorema 10.53) hemos observado que TU implica que el producto de espacios de Hausdorff compactos es compacto. Ahora podemos demostrar el recíproco:

Teorema 11.10 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 $h : 2^{\mathbb{B}} \longrightarrow X = \prod\limits_{b\in\mathbb{B}} \{b, b'\}$ 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 10.5) 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 $f \in \bigcap\limits_{\mathbb{C}} B_{\mathbb{C}}$. 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 $\mathbb{O} = f(\mathbb{O}) \in I$, luego $\mathbb{O} \in I_0$ 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 11.11 (TU) *Todo producto de espacios compactos de Hausdorff no vacíos es no vacío.*

DEMOSTRACIÓN: Sea $X = \prod\limits_{i \in I} X_i$ un producto de espacios de Hausdorff compactos no vacíos.

Sea Z el conjunto de todas las funciones f tales que

$$\mathcal{D}f \subset I \land \bigwedge i \in \mathcal{D}f \ f(i) \in X_i.$$

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

$$U_i = \{A \in \mathcal{P}X_i \mid \{f \in Z \mid i \in \mathcal{D}f \land f(i) \in A\} \in U\}$$

es un ultrafiltro en X_i. (Aquí usamos que, como $Z_i \in U$, se cumple $X_i \in U_i$.) Por las propiedades tras la definición 10.50 tenemos que U_i 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 11.12 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 $\land$, $\lor$ y $'$ en $\mathbb{B}_T$ dadas por

$$[\alpha] \land [\beta] = [\alpha \land \beta], \qquad [\alpha] \lor [\beta] = [\alpha \lor \beta], \qquad [\alpha]' = [\neg\alpha]$$

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

$$\mathbb{1} = T, \qquad \mathbb{O} = \mathbb{1}'.$$

(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 $\rightarrow$ y $\leftrightarrow$ dadas para álgebras de Boole arbitrarias, es claro que

$$[\alpha] \rightarrow [\beta] = [\alpha \rightarrow \beta], \quad [\alpha] \leftrightarrow [\beta] = [\alpha \leftrightarrow \beta].$$

A su vez, $[\alpha] \leq [\beta]$ equivale a que siempre que α es verdadera en un modelo de T sucede que β también lo es.

Teorema 11.13 (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 $\Delta = \{\delta_1, \ldots, \delta_n\}$, tenemos que $[\delta_1 \wedge \cdots \wedge \delta_n] \in F$ y $[\delta_1 \wedge \cdots \wedge \delta_n] \leq [\phi]$, luego $[\phi] \in F$, luego $\phi \in T_F$.

Además T_F es finitamente consistente, pues si $\alpha_1, \ldots, \alpha_n \in T_F$, entonces $[\alpha_1 \wedge \cdots \wedge \alpha_n] \in F$, luego $[\alpha_1 \wedge \cdots \wedge \alpha_n] \neq \mathbb{0}$, luego la conjunción tiene un modelo, que también será un modelo de $\{\alpha_1, \ldots, \alpha_n\}$. 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 11.14 (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 $\mathfrak{L}$ 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):

a) $p \preceq p$,

b) $p \preceq q \wedge q \leq p \rightarrow p = q$,

c) $p \preceq q \wedge q \preceq r \rightarrow p \preceq r$,

d) $p \preceq q \vee q \preceq p$,

e) $p \preceq q$ 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 $x \leq^* y \leftrightarrow \operatorname{rang}(x) \leq \operatorname{rang}(y)$). 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 11.15 (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 11.11.

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 11.16 (TU)[10] *Si una teoría T tiene modelos finitos de cardinal arbitrariamente grande, entonces tiene modelos infinitos.*

DEMOSTRACIÓN: Sea $\mathfrak{L}$ el lenguaje de T y sea $\mathfrak{L}'$ el lenguaje que resulta de añadir a $\mathfrak{L}$ un conjunto numerable de constantes $\{c_n\}_{n\in\omega}$. Sea Γ el conjunto de sentencias de $\mathfrak{L}'$ 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.

11.3 Submodelos, inmersiones

Estudiamos ahora las aplicaciones que relacionan dos modelos de un mismo lenguaje formal.

Definición 11.17 Una *inmersión* $i : N \longrightarrow M$ entre dos modelos de un mismo lenguaje formal $\mathfrak{L}$ es una aplicación que verifica las propiedades siguientes:

a) Para toda constante c de $\mathfrak{L}$ se cumple que $i(N(c)) = M(c)$.

b) Para todo relator n-ádico R de $\mathfrak{L}$ se cumple que

$$\bigwedge a_1 \ldots a_n \in N(N(R)(a_1, \ldots, a_n) \leftrightarrow M(R)(i(a_1), \ldots, i(a_n))).$$

c) Para todo funtor n-ádico f de $\mathfrak{L}$ se cumple que

$$\bigwedge a_1 \ldots a_n \in N(i(N(f)(a_1, \ldots, a_n)) = M(f)(i(a_1), \ldots, i(a_n))).$$

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 $\mathfrak{L}$ 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 11.6 del teorema de compacidad.

a) $M(c) \in N$ para toda constante c de $\mathcal{L}$.

b) $M(f)|_{N^n} : N^n \longrightarrow N$, 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 11.18 *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

$$i(N(t)[a_1, \ldots, a_n]) = i(N(f)(N(t_1)[a_1, \ldots, a_n], \ldots, N(t_m)[a_1, \ldots, a_n]))$$

$$= M(f)(i(N(t_1)[a_1, \ldots, a_n]), \ldots, i(N(t_m)[a_1, \ldots, a_n])$$

$$= M(f)(M(t_1)[i(a_1), \ldots, i(a_n)], \ldots, M(t_m)[i(a_1), \ldots, i(a_n)])$$

$$= M(t)[i(a_1), \ldots, i(a_n)].$$

■

Con esto podemos probar que dos modelos isomorfos satisfacen las mismas sentencias:

Teorema 11.19 *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 $\phi = \alpha \rightarrow \beta$ 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 $i(a)$ recorre M. ■

Definición 11.20 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 11.21 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 11.22 *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*

$$\bigwedge a_1 \cdots a_n \in N(\bigvee a \in M M \vDash \phi[a, a_1, \ldots, a_n] \rightarrow \bigvee a \in N M \vDash \phi[a, a_1, \ldots, a_n]).$$

Demostración: Veamos en primer lugar que N es un submodelo. Si c es una constante de $\mathcal{L}$ entonces $\bigvee a \in M M \vDash (x = c)[a]$, luego por hipótesis $\bigvee a \in N M \vDash (x = c)[a]$, 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 $\bigvee a \in M M \vDash x = fx_1 \cdots x_n[a, a_1, \ldots, a_n]$, luego por hipótesis también se cumple $\bigvee a \in N M \vDash x = fx_1 \cdots x_n[a, a_1, \ldots, a_n]$, 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 11.19 (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,

$$\bigvee a \in M\ M \vDash \phi[a,a_1,\ldots,a_n] \rightarrow M \vDash \bigvee x\,\phi(x)[a_1,\ldots,a_n]$$

$$\rightarrow N \vDash \bigvee x\,\phi(x)[a_1,\ldots,a_n] \rightarrow \bigvee a \in N\ N \vDash \phi[a,a_1,\ldots,a_n]$$

$$\rightarrow \bigvee a \in N\ M \vDash \phi[a,a_1,\ldots,a_n].$$

■

De aquí podemos obtener una técnica para construir submodelos elementales. Para ello necesitamos algunas definiciones:

Definición 11.23 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 $N_{k+1}(X) = N_k(X) \cup \bigcup\limits_{\phi} h_\phi[N_k(X)]$, 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 11.24 (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 11.25 (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 11.26 (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

$$\begin{aligned} M \vDash \phi[a_1, \ldots, a_n] \rightarrow M' \vDash \phi(c_{a_1}, \ldots, c_{a_n}) \rightarrow M'' \vDash \phi(c_{a_1}, \ldots, c_{a_n}) \\ \rightarrow M'' \vDash \phi[i(a_1), \ldots, i(a_n)]. \end{aligned}$$

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

$$M \vDash \phi[a_1, \ldots, a_n] \rightarrow M'' \vDash \phi[i(a_1), \ldots, i(a_n)] \rightarrow N \vDash \phi[i(a_1), \ldots, i(a_n)].$$

■

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 11.27 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 11.28 *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 11.29 *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 11.18 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. ■

11.4 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 11.30 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 $\prod\limits_{i \in I} M_i$ 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 $\prod\limits_{i \in I}^U M_i$.

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 $\bar{c} \in \prod\limits_{i \in I} M_i$ 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 $\phi : \prod\limits_{i\in I}^U M_i \longrightarrow M_{i_0}$ 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 11.31 (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 $\phi(x_1,\ldots,x_n) \in \mathrm{Form}(\mathcal{L})$ y $f_1,\ldots,f_n \in \prod\limits_{i\in I} M_i$, entonces*

$$\prod_{i\in I}^U M_i \vDash \phi[[f_1],\ldots,[f_n]] \leftrightarrow \{i \in I \mid M_i \vDash \phi[f_1(i),\ldots,f_n(i)]\} \in U.$$

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 $t(x_1,\ldots,x_n)$ un término de $\mathcal{L}$ y $f_1,\ldots,f_n \in \prod\limits_{i\in I} M_i$. Veamos que

$$\Big(\prod_{i\in I}^U M_i\Big)(t)[[f_1],\ldots,[f_n]] = [g],$$

donde $g(i) = M_i(t)[f_1(i),\ldots,f_n(i)]$.

Lo probamos por inducción sobre la longitud de t. Si $t(x_1,\ldots,x_n) = x_i$, entonces el miembro izquierdo es $[f_i]$, y $g = f_i$, luego se cumple la igualdad.

Si $t(x_1,\ldots,x_n) = c$, 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 $t(x_1,\ldots,x_n) = Ft_1(x_1,\ldots,x_n)\cdots t_r(x_1,\ldots,x_n)$, donde F es un funtor r-ádico de $\mathcal{L}$, entonces

$$\Big(\prod_{i\in I}^U M_i\Big)(t)[[f_1],\ldots,[f_n]]$$

$$= \Big(\prod_{i\in I}^U M_i\Big)(F)\Big(\Big(\prod_{i\in I}^U M_i\Big)(t_1)[[f_1],\ldots,[f_n]],\ldots,\Big(\prod_{i\in I}^U M_i\Big)(t_r)[[f_1],\ldots,[f_n]]\Big)$$

$$= \Big(\prod_{i\in I}^U M_i\Big)(F)([g_1],\ldots,[g_r]) = [g],$$

donde $g_j(i) = M_i(t_j)[f_1(i),\ldots,f_n(i)]$ (por hipótesis de inducción) y

$$g(i) = M_i(F)(g_1(i),\ldots,g_r(i)) = M_i(t)[f_1(i),\ldots,f_n(i)].$$

Veamos ahora el teorema por inducción sobre la longitud de ϕ.

Si $\phi(x_1,\ldots,x_n) = Rt_1(x_1,\ldots,x_n)\cdots t_r(x_1,\ldots,x_n)$, donde R es un relator r-ádico de $\mathcal{L}$, entonces

$$\prod_{i\in I}^U M_i \vDash \phi[[f_1],\ldots,[f_n]]$$

$$\leftrightarrow \Big(\prod_{i\in I}^U M_i\Big)(R)\Big(\Big(\prod_{i\in I}^U M_i\Big)(t_1)[[f_1],\ldots,[f_n]],\ldots,\Big(\prod_{i\in I}^U M_i\Big)(t_r)[[f_1],\ldots,[f_n]]\Big)$$

$$\leftrightarrow \Big(\prod_{i\in I}^U M_i\Big)(R)([g_1],\ldots,[g_r]),$$

donde, según hemos probado, $g_j(i) = M_i(t_j)[f_1(i),\ldots,f_n(i)]$. Esto equivale a

$$\{i\in I \mid M_i(R)[g_1(i),\ldots,g_r(i)]\}\in U \leftrightarrow \{i\in I \mid M_i \vDash \phi[f_1(i),\ldots,f_n(i)]\}\in U.$$

Si $\phi(x_1,\ldots,x_n) = \neg\psi(x_1,\ldots,x_n)$ y el teorema vale para ψ, entonces

$$\prod_{i\in I}^U M_i \vDash \phi[[f_1],\ldots,[f_n]] \leftrightarrow \neg\prod_{i\in I}^U M_i \vDash \psi[[f_1],\ldots,[f_n]]$$

$$\leftrightarrow \{i\in I \mid M_i \vDash \psi[f_1(i),\ldots,f_n(i)]\}\notin U$$

$$\leftrightarrow \{i\in I \mid M_i \vDash \phi[f_1(i),\ldots,f_n(i)]\}\in U.$$

Si $\phi(x_1,\ldots,x_n) = \psi(x_1,\ldots,x_n)\rightarrow\chi(x_1,\ldots,x_n)$ y el teorema vale para ψ y χ, probaremos la coimplicación de las negaciones, es decir, que

$$\neg\prod_{i\in I}^U M_i \vDash (\psi\rightarrow\chi)[[f_1],\ldots,[f_n]]$$

$$\leftrightarrow \{i\in I \mid M_i \vDash (\psi\rightarrow\chi)[f_1(i),\ldots,f_n(i)]\}\notin U$$

En efecto,

$$\neg\prod_{i\in I}^U M_i \vDash (\psi\rightarrow\chi)[[f_1],\ldots,[f_n]]$$

$$\leftrightarrow \prod_{i\in I}^U M_i \vDash \psi[[f_1],\ldots,[f_n]] \wedge \neg\prod_{i\in I}^U M_i \vDash \chi[[f_1],\ldots,[f_n]]$$

$$\leftrightarrow \{i\in I \mid M_i \vDash \psi[f_1(i),\ldots,f_n(i)]\}\in U$$

$$\wedge\ \{i\in I \mid M_i \vDash \neg\chi[f_1(i),\ldots,f_n(i)]\}\in U$$

$$\leftrightarrow \{i\in I \mid M_i \vDash \psi[f_1(i),\ldots,f_n(i)]\}\cap\{i\in I \mid M_i \vDash \neg\chi[f_1(i),\ldots,f_n(i)]\}\in U$$

$$\leftrightarrow \{i\in I \mid \neg M_i \vDash (\psi\rightarrow\chi)[f_1(i),\ldots,f_n(i)]\}\in U$$

$$\leftrightarrow \{i\in I \mid M_i \vDash (\psi\rightarrow\chi)[f_1(i),\ldots,f_n(i)]\}\notin U.$$

Si $\phi(x_1,\ldots,x_n) = \bigwedge x\psi(x,x_1,\ldots,x_n)$ y el teorema vale para ψ, probaremos también la coimplicación de las negaciones:

$$\neg\prod_{i\in I}^U M_i \vDash \bigwedge x\,\psi[[f_1],\ldots,[f_n]]$$

$$\leftrightarrow \{i\in I \mid M_i \vDash \bigwedge x\,\psi[f_1(i),\ldots,f_n(i)]\}\notin U.$$

En efecto:

$$\neg \prod_{i\in I}^U M_i \vDash \bigwedge x\, \psi[[f_1],\ldots,[f_n]] \leftrightarrow \bigvee f\in \prod_{i\in I} M_i \neg \prod_{i\in I}^U M_i \vDash \psi[[f],[f_1],\ldots,[f_n]]$$

$$\leftrightarrow \bigvee f\in \prod_{i\in I} M_i\ \{i\in I \mid M_i \vDash \psi[f(i), f_1(i),\ldots,f_n(i)]\} \notin U$$

$$\leftrightarrow \bigvee f\in \prod_{i\in I} M_i\ \{i\in I \mid M_i \vDash \neg\psi[f(i), f_1(i),\ldots,f_n(i)]\} \in U. \tag{11.1}$$

Basta probar que esto equivale a

$$\{i\in I \mid M_i \vDash \bigvee x \neg\psi[f_1(i),\ldots,f_n(i)]\} \in U, \tag{11.2}$$

pues claramente esto equivale a $\{i\in I \mid M_i \vDash \bigwedge x\psi[f_1(i),\ldots,f_n(i)]\} \notin U$.

Si f cumple (11.1), es claro que el conjunto de (11.1) está contenido en el conjunto de (11.2). Como el primero está en U el segundo también. Recíprocamente, si se cumple (11.2), para cada i en el conjunto de (11.2) sea[11] $f(i)\in M_i$ tal que $M_i \vDash \neg\psi[f(i), f_1(i),\ldots,f_n(i)]$ y para los demás $i\in I$ tomamos $f(i)\in M_i$ arbitrario. Es claro que f cumple (11.1). ■

Hay un caso particular del teorema anterior que tiene especial interés:

Definición 11.32 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 $\prod\limits_{i\in I}^U M$, 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 11.33 *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 $\phi(x_1,\ldots,x_n)\in \mathrm{Form}(\mathcal{L})$ y $a_1,\ldots,a_n\in M$, entonces

$$M\vDash \phi[a_1,\ldots,a_n] \leftrightarrow \{i\in I \mid M\vDash \phi[c_{a_1}(i),\ldots,c_{a_n}(i)]\}\in U$$

$$\leftrightarrow \mathrm{Ult}_U(M) \vDash \phi[j_U(a_1),\ldots,j_U(a_n)].$$

■

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 si suponemos en su lugar que M admite un buen orden, pues esto es todo lo que requiere en este caso la construcción de la función f en la parte final de la prueba.

Teorema 11.34 (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 $\prod\limits_{\Delta \in I}^{U} M_\Delta \vDash \phi$, es decir, $\prod\limits_{\Delta \in I}^{U} M_\Delta \vDash \Gamma$. ■

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 11.35 (TU) *El axioma de elección es equivalente a que, para todo modelo M de un lenguaje formal,* $\mathrm{Ult}_U(M)$ *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 $a \in x \land x \in X$ 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:

$$\begin{array}{ll}
\text{(AP1)} & \bigwedge x\; x' \neq 0 \\
\text{(AP2)} & \bigwedge xy(x' = y' \rightarrow x = y) \\
\text{(AP3)} & \bigwedge x\; x + 0 = x \\
\text{(AP4)} & \bigwedge xy(x + y' = (x + y)') \\
\text{(AP5)} & \bigwedge x\; x \cdot 0 = 0 \\
\text{(AP6)} & \bigwedge xy(xy' = xy + x) \\
\text{(AP7)} & \bigwedge x_1 \cdots x_n(\phi(0) \wedge \bigwedge x(\phi(x) \rightarrow \phi(x')) \rightarrow \bigwedge x\phi(x)),
\end{array}$$

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 L_{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, si identificamos a $\mathbb{R}$ con su imagen por la inmersión elemental $j_U : \mathbb{R} \longrightarrow \mathbb{R}^*$, entonces $\mathbb{R}$ es un subcuerpo de $\mathbb{R}^*$, y podemos definir un *infinitésimo* como un $\epsilon \in \mathbb{R}^*$ tal que $|\epsilon| < 1/n$, para todo $n \in \mathbb{N}$. Entonces, tenemos que en $\mathbb{R}^*$ hay infinitésimos no nulos. ■

Bibliografía

[1] Barwise, J. (editor), *Handbook of Mathematical Logic,* North Holland, Amsterdam, 1977.

[2] Devlin, K.J. *Constructibility,* Springer, Berlín (1984)

[3] Engelking, R, *General Topology,* Helderman, Berlín (1989)

[4] Galvin, F. *Chain conditions and products, Fund. Math,* **108,** 1 (1980), 33–48.

[5] Givant, S., Halmos, P., *Introduction to Boolean algebras,* Springer, (2009)

[6] Howard, P.E., *Łos' theorem and the Boolean prime ideal theorem imply the axiom of choice,* Proc. Amer. Math. Soc. **49,** 2 (1975).

[7] Jech, T.J. *The Axiom of Choice,* North Holand, Amsterdam, 1973.

[8] — *Set Theory,* Academic Press, New York, 1978.

[9] Kunen, K. *Combinatorics,* (en Barwise).

[10] — *Set Theory. An Introduction to Independence Proofs,* North Holland, Amsterdam, 1985.

[11] Pohlers, W. *Proof Theory, The first step to impredicativity,* Springer, Berlin (2009).

[12] Sikorski, R. *Boolean Algebras.* Springer Verlag, Berlin, 1969.

Índice de Materias

abierta (aplicación), 262
abierto, 238
abierto regular, 313
acumulación (punto de), 253
adherente (punto), 251
AEN, 90
aislado (punto), 253
álef (función), 106
álgebra
    cociente, 330
    de Boole, 305
        completa, 311
    de conjuntos, 308
    de Lindenbaum, 366
    de Suslin, 326
    degenerada, 307
altura, 283
anillo, 27
    cociente, 37
    ordenado, 30
        arquimediano, 198
anticadena, 267, 283, 322
antisimétrica (relación), 20
aplicación, 11
árbol, 283
    bien podado, 284
    completo, 288
    de Aronszajn, 287, 289
    de Kurepa, 302
    de Suslin, 291
    ramificado, 291
Aronszajn (árbol de), 287
asimétrica (relación), 20
asociativa (propiedad), 27
átomo, 321
automorfismo, 309

Axioma
    de comprensión, 4
    de elección, 88
        de Gödel, 150
        numerable, 90
    de extensionalidad, 2
    de infinitud, 48
    de la unión, 16
    de partes, 18
    de reemplazo, 15
    de regularidad, 85
    del conjunto vacío, 6
    del par, 9

base, 240
    de entornos, 241
    de numeración, 68
bet (función), 147
bien fundada
    clase, 40
    relación, 75
bien ordenable (conjunto), 103
bien podado (árbol), 284
bola abierta, 241
buen orden, 25
Burali-Forti (antinomia de), 55

cadena, 283
camino, 283
Cantor (forma normal de), 70
cardinal, 101, 103
    de Mahlo, 168
    débilmente inaccesible, 128
    fuertemente inaccesible, 146
    límite, 128
        fuerte, 146
    regular, singular, 128

sucesor, 128
cero-dimensional, 333
cerrado, 251
en un ordinal, 153
clase, 2
propia, 7
clausura, 77, 251
transitiva, 77
cociente (clase), 21
cofinal (aplicación), 124
cofinalidad, 124
compacto, 270
numerablemente, 274
compatibilidad
en un árbol, 283
en un c.p.o., 315
compleción, 215, 319
complemento, 5
completitud, 331
de un álgebra, 322
completo (conjunto), 356
composición, 13
condición de cadena, 322, 332
numerable, 267
conexa
clase, 40
relación, 20
conjuntista (relación), 76
conjunto, 2
dual, 310
conmutativa (propiedad), 27
consecuencia lógica, 355
consistente, 356
constante, 348
continua (función), 257
continuo, 225
función del, 136
contradictorio, 356
convergencia, 203, 250
de filtros, 337
cota, 22
creciente (función), 24
cuadrado $\square_\kappa$, 178
cuasidisjunta (familia), 268
cubrimiento, 270, 271
cuerpo, 29
métrico, 202

decreciente (función), 24
degenerada (álgebra), 307
denso, 225
conjunto, 203, 253
en sí mismo, 199
derivada (de una función normal), 184
derivado (conjunto), 253
designador, 353
diamante $\diamondsuit$, 171
diferencia, 5
simétrica, 328
disjuntas (clases), 5
distancia, 201
a un conjunto, 252
dominio, 11
dual (conjunto), 310

ED (elecciones dependientes), 86
elementalmente equivalentes, 370
entero (número), 194
entorno, 239
epimorfismo
de álgebras, 309
de anillos, 33
épsilon (número), 71
equipotencia, 97
espacio
compacto, 270
de Hausdorff, 239
métrico, 202
topológico, 238
estacionario (conjunto), 159
exponenciación
de cardinales, 112
de ordinales, 64

fórmula, 351
Feferman-Schütte (ordinal de), 190
filtro, 329
en un conjunto, 157
finitamente consistente, 356
finito (conjunto), 90
de Dedekind, 116
frontera, 253

fuertemente crítico (ordinal), 189
función, 11
  de Skolem, 372
  normal, 56
funtor, 348

Hartogs (álef de), 111
Hausdorff (fórmula de), 136
hipótesis
  de Kurepa, 302
  de los cardinales singulares, 142
  de Suslin, 279
  del continuo, 113
homeomorfismo, 262
homomorfismo
  de álgebras de Boole, 308
  de anillos, 33
    ordenados, 35

ideal, 36, 328
  en un conjunto, 157
  maximal, 37
  primo, 37, 328
imagen, 11
inclusión, 13
incompatibilidad
  en un árbol, 283
  en un c.p.o., 315
ínfimo, 23
infinita (clase), 107
  de Dedekind, 116
inmersión, 315, 368
  completa, 315
  densa, 225, 316
  elemental, 370
  isométrica, 202, 203
interior, 251
  punto, 251
intersección, 5
  diagonal, 156
intervalo, 223
inversa, 12
inverso (elemento), 27
irreflexiva (relación), 20
isometría, 202, 203
isomorfismo, 368
  de álgebras, 309
  de anillos, 33
    ordenados, 35

Kurepa
  árbol de, 302
  hipótesis de, 302

límite
  de una sucesión, 203, 250
  ordinal, 46
lenguaje formal, 348
lexicográfico (orden), 60
ley de composición interna, 27

métrica discreta, 242
Mahlo (cardinal de), 168
maximal, 22
máximo, 23
minimal, 22
mínimo, 23
minuspotencia, 97
modelo, 349, 355
monótona (función), 24
monomorfismo
  de álgebras, 309
  de anillos, 33

número
  entero, 194
  natural, 46
  racional, 198
  real, 220, 229
neutro (elemento), 27
nivel (en un árbol), 283
normal (función), 56

operación, 27
orden canónico en $\Omega \times \Omega$, 56
ordinal
  de un conjunto, 54
  número, 45
  sucesor, límite, 46

par, 9
  ordenado, 10
parte entera, fraccionaria, 198

partes, 18
partición, 324
pertenencia, 2
precontinuo, 225
preorden, 315
primer axioma de numerabilidad, 255
principio
    de elecciones dependientes, 86
    de buena ordenación, 93
    de numerabilidad, 93
producto
    cardinales
        infinito, 121
    cartesiano, 11
    de cardinales, 107
    de ordinales, 61
punto de acumulación (de un filtro), 337

raíz cuadrada, 220
racional (número), 198
rama, 283
ramificado, 291
rango, 11
    de un conjunto regular, 83
real (número), 220, 229
reflexiva (relación), 20
regresiva (aplicación), 160
regular
    cardinal, 128
    conjunto, 82
relación, 20
    de equivalencia, 21
    de orden, 22
relator, 348
restricción, 12

saturación, 332
sección inicial abierta, 226
segundo axioma de numerabilidad, 263
semejanza, 24
sentencia, 353
separable, 265
separativo (preorden), 315
simétrica (relación), 20
singular (cardinal), 128
sistema Δ, 268
Sorgenfrey (recta de), 265
Stone (espacio de), 333
subálgebra, 307
subárbol, 284
subbase, 242
subcubrimiento, 270
submodelo, 368
    elemental, 371
subsucesión, 206
sucesión (convergente, de Cauchy), 203
suma
    de cardinales, 107
        infinita, 120
    de ordinales, 58
supremo, 23
Suslin
    álgebra de, 326
    árbol de, 291
    hipótesis de, 279, 280, 294
    recta de, 280

término, 350
teoría, 355
Teorema
    de Cantor, 99, 113
    de Cantor-Bernstein, 99
    de compacidad, 359, 379
    de Fodor, 160
    de inducción transfinita, 48, 49
    de König, 137
    de Löwenheim-Skolem, 373
    de los intervalos encajados, 221
    de los ultrafiltros, 361
    de recursión transfinita, 49
    de Silver, 163
    de Solovay, 162
    de Stone, 333
    de Tychonoff, 275, 339
    general de inducción transfinita, 76, 80
    general de recursión transfinita, 78, 81
topología, 238

de orden, 243
discreta, 239
producto, 246
relativa, 244
trivial, 239
usual de $\mathbb{R}$, 243
transitiva
clase, 40, 76
relación, 20

ultrafiltro, 329
fijo, libre, 331
uniforme, 344
ultrapotencia, 378
ultraproducto, 375
unívoca (clase), 11
unión, 5

valor absoluto, 31, 202
valoración, 351
variable, 348
libre, 353
Veblen (funciones de), 187

Zorn (lema de), 93