PATRICK SUPPES

Teoría Axiomática de Conjuntos

CENTRO REGIONAL DE AYUDA TECNICA · REGIONAL TECHNICAL AIDS CENTER

EDITORIAL
Norma
CALI - COLOMBIA

TEORIA AXIOMATICA DE CONJUNTOS

TEORIA AXIOMATICA DE CONJUNTOS

PATRICK SUPPES

Versión castellana de
Hernando Alfonso Castillo,
Profesor de la Universidad Pedagógica
Nacional, Bogotá

CENTRO REGIONAL DE AYUDA TECNICA
AGENCIA PARA EL DESARROLLO INTERNACIONAL **A I D**
MEXICO

EDITORIAL NORMA

CALI - COLOMBIA

NOTA A ESTA EDICION

Esta publicación es traducida de **Axiomatic Set Theory** editada originalmente en inglés por *D. Van Nostrand Company, Inc. 1960.* La presente edición se preparó conjuntamente por el Centro Regional de Ayuda Técnica de México y la Agencia para el Desarrollo Internacional (AID), Departamento de Estado del Gobierno de los Estados Unidos de América. El Centro es un organismo dedicado a la producción de versiones en español del material fílmico e impreso de los programas de cooperación técnica de la Alianza para el Progreso.

IMPRESO EN COLOMBIA
PRINTED IN COLOMBIA

CARVAJAL & CIA

Prólogo

Este libro está destinado, ante todo, para servir como texto en cursos de teoría axiomática de conjuntos. Se ha desarrollado en detalle el sistema de Zermelo-Fraenkel. La preparación matemática que se necesita es mínima; en particular, no se requiere conocimiento previo de teoría de conjuntos o de lógica matemática. Por otra parte, los estudiantes necesitarán cierto grado de cultura matemática general, especialmente para dominar los dos últimos capítulos. Aun cuando en todo el libro se usa un poco de notación lógica, las demostraciones están escritas en estilo informal y se ha tratado de evitar el exceso de simbolismo. Se ha hecho un glosario de los símbolos de uso más frecuente.

Los ocho capítulos están organizados así: En el capítulo 1 se hace una breve introducción. El capítulo 2 trata de desarrollos generales y el capítulo 3, de relaciones y funciones. No hay teoremas difíciles en estos tres capítulos y pueden estudiarse muy rápidamente en un curso avanzado. El principal énfasis pedagógico se ha hecho sobre el papel exacto que desempeñan los axiomas introducidos en el capítulo 2, los cuales aparecen resumidos al final del capítulo.

En el capítulo 4 se consideran los temas clásicos de equipotencia de conjuntos, conjuntos finitos y números cardinales. El teorema de Schröder-Bernstein se demuestra desde el principio del capítulo. El desarrollo de la teoría de conjuntos finitos sigue al pie de la letra el conocido artículo de Alfred Tarski, publicado en 1924. La teoría de los números cardinales se ha simplificado mediante la introducción de un axioma especial según el cual los números cardinales de dos conjuntos equipotentes son idénticos. Este axioma no es parte del sistema usual de Zermelo-Fraenkel y por ello toda definición o teorema que de-

penda de él se ha marcado con el símbolo '†'; pero permite un desarrollo tan simple y natural, que su introducción me ha parecido plenamente justificada. El capítulo 5 abarca parte del mismo contenido desde otro punto de vista. Los números naturales se definen como los ordinales de von Neumann y se desarrolla la teoría de definiciones por recurrencia. Se introduce el axioma de infinitud y la sección final trata de los hechos básicos acerca de conjuntos enumerables.

En el capítulo 6 se da en detalle la construcción usual de los racionales y de los reales. Se usan las sucesiones de Cauchy de números racionales, en lugar de las cortaduras de Dedekind, para definir los números reales. La mayor parte de los hechos elementales acerca de conjuntos con la potencia del continuo se ha demostrado en la sección final. Puesto que para muchos cursos de teoría de conjuntos puede no ser factible incluir la construcción de los números reales en el tiempo asignado, o porque dicho tema puede estar incluido en otros cursos, el libro se ha escrito de tal manera que este capítulo puede omitirse sin pérdida de continuidad.

El capítulo 7 trata de inducción transfinita y aritmética ordinal. El tratamiento de la inducción transfinita y la definición por recurrencia transfinita es uno de los más detallados que se hayan publicado hasta ahora. Se han dado muchas formulaciones sinónimas, en la esperanza de que la consideración sucesiva de ellas clarificará al estudiante el carácter esencial del proceso transfinito. Se introduce el sistema axiomático de sustitución para establecer un esquema de recurrencia apropiado para definir la adición ordinal. Los hechos más familiares acerca de los alefs y conjuntos bien ordenados se han demostrado en la parte final del capítulo.

El capítulo 8 trata sobre todo del axioma de escogencia y sus equivalentes como el principio maximal de Hausdorff y el lema de Zorn. Varios hechos importantes cuyas demostraciones requieren el axioma de escogencia, también se han aplazado para empezar a estudiarlos en este capítulo. Un ejemplo típico es la identidad entre el infinito ordinario y el de Dedekind.

Aun cuando la bibliografía consignada al final del libro es pequeña, si se compara con la que da Fraenkel en su Abstract Set Theory *("Teoría abstracta de conjuntos"), he tratado de* *incluir muchas de las más importantes monografías sobre cada tema. Puesto que la teoría de conjuntos, aun quizás la axiomática, está convirtiéndose finalmente en parte del patrimonio intelectual de todo joven matemático, es de algún interés histórico anotar que la mayor parte de los documentos a que se hace referencia en el texto se publicaron antes de 1930.*

Espero que este libro sea útil para varios tipos de cursos. En un curso semestral de teoría de conjuntos para estudiantes de cuarto año de universidad o primero de post-grado se puede ver todo el libro, con excepción quizás del capítulo 6. Los cursos de filosofía sobre los fundamentos de la matemática podrían abarcar con provecho los cuatro primeros capítulos, que terminan con la construcción de los números naturales como cardinales finitos. El material de los primeros seis capítulos, que terminan con la construcción de los números reales, es adecuado para un curso universitario de fundamentos de análisis, o como lectura adicional para el curso de teoría de funciones de variable real.

PATRICK SUPPES

Stanford, California
Enero, 1960

CONTENIDO

Capítulo 1

Introducción

§ 1.1 **La teoría de conjuntos y los fundamentos de la matemática.** Entre las muchas ramas de la matemática moderna, la teoría de conjuntos ocupa un puesto único: con muy raras excepciones, las entidades que se estudian y analizan en matemática pueden considerarse como ciertos conjuntos o clases particulares de objetos.* Esto significa que las varias ramas de la matemática pueden definirse formalmente dentro de la teoría de conjuntos. Como consecuencia, muchas preguntas fundamentales acerca de la naturaleza de la matemática pueden reducirse a preguntas acerca de la teoría de conjuntos.

El matemático práctico, lo mismo que el hombre de la calle, raras veces se encuentra con la pregunta insólita: ¿Qué es un número? Pero el intento de responder precisamente a esta pregunta ha motivado gran parte del trabajo de matemáticos y filósofos de la fundamentación matemática durante los últimos cien años. La caracterización de los números enteros, de los racionales y de los reales, ha sido un problema central para las investigaciones clásicas de Weierstrass, Dedekind, Kronecker, Frege, Peano, Russell, Whitehead, Brouwer y otros. Las perplejidades acerca de la naturaleza del número no se originaron en el siglo diecinueve. Una de las más espléndidas contribuciones de los antiguos matemáticos griegos fue la teoría de la proporción de Eudoxio, expuesta en el libro V de los *Elementos* de Euclides; el principal objetivo de Eudoxio fue dar un tratamiento riguroso a las cantidades irracionales como la media geométrica entre 1 y 2. Puede decirse realmente que el desarrollo detallado a partir de los axiomas generales de la teoría de conjuntos,de la teoría de números y del análisis, tiene gran parte del espíritu de Eudoxio. Sin embargo, el desarrollo real de la teoría de conjuntos no proviene directamente de un intento de resolver este problema central de la naturaleza del número, sino de las investigaciones de Georg Cantor, alrededor de 1870, en la teoría de series infinitas y otros temas de análisis relacionados con ella.* Cantor, a quien se considera usualmente el fundador de la teoría de conjuntos como disciplina matemática, fue llevado por su trabajo a la consideración de conjuntos infinitos o clases de carácter arbitrario. En 1874 publicó su famosa demostración de que el conjunto de los números reales no puede ponerse en correspondencia biunívoca con el conjunto de los números naturales (los enteros no negativos). En 1878 introdujo la noción fundamental de que dos conjuntos son

* Intuitivamente queremos significar con *conjunto* o *clase* una colección de entidades de cualquier tipo. Así, podemos hablar del conjunto de todos los irlandeses, o del conjunto de todos los números primos. En la matemática ordinaria las palabras 'conjunto', 'clase', 'colección', 'agregado', son sinónimos y así las usamos aquí, excepto en algunos pocos pasajes explícitamente denotados.

* Para una visión histórica detallada del trabajo de Cantor, véase *Introduction to Cantor*, de Jourdain [1915].

equipotentes o de la misma potencia *(Mächtigkeit)* si cada uno puede ponerse en correspondencia biunívoca con el otro. Es claro que dos conjuntos finitos tienen la misma potencia, precisamente cuando tienen el mismo número de elementos. Así, la noción de potencia lleva, en el caso de los conjuntos infinitos,a una generalización del concepto de número natural, al de número cardinal infinito. El desarrollo de la teoría general de números transfinitos fue uno de los grandes triunfos de las investigaciones matemáticas de Cantor.

La consideración técnica de los muchos conceptos básicos de teoría de conjuntos introducidos por Cantor, se hará oportunamente. Desde el punto de vista de los fundamentos de la matemática, el aspecto filosóficamente revolucionario de la obra de Cantor fue su audaz insistencia en el infinito real, esto es, en la existencia de conjuntos infinitos como objetos matemáticos a la par de los números y de los conjuntos finitos. Históricamente el concepto de infinito ha desempeñado un papel tan importante como el concepto de número en la literatura de los fundamentos de la matemática. Casi no hay filósofo serio de la matemática, desde Aristóteles , que no haya luchado mucho con este difícil concepto.

Naturalmente se espera encontrar en un libro de teoría de conjuntos un análisis riguroso de los conceptos de número y de infinito; pero otros temas, algunos controvertidos e importantes en investigación de fundamentos, son también parte tradicional de esta materia y, por consiguiente, se tratan en los capítulos que siguen. Son típicos el álgebra de conjuntos, la teoría general de relaciones, las relaciones de orden en particular, las funciones, conjuntos finitos, números cardinales, conjuntos infinitos, aritmética ordinal, inducción transfinita, definición por recurrencia transfinita, axioma de escogencia, lema de Zorn. En este momento no se espera que el lector sepa lo que significan estas frases, pero la lista puede darle idea del contenido detallado de este libro.

La teoría de conjuntos se desarrolla axiomáticamente en vez de intuitivamente. Muchas consideraciones nos han movido a escoger el enfoque axiomático. Una es la opinión del autor de que el desarrollo axiomático de la teoría de conjuntos es una de las realizaciones más grandiosas de la matemática moderna. A los conceptos que fueron vagos y desagradablemente inexactos durante muchos años y aun siglos, puede dárseles un significado preciso. Los axiomas adecuados para la teoría de conjuntos proporcionan una respuesta clara y constructiva a la pregunta: ¿Exactamente cuáles suposiciones, fuera de las de lógica elemental, se requieren como base de la matemática moderna? La consideración más importante, sin embargo, es el descubrimiento hecho alrededor de 1900, de varias paradojas en la teoría de conjuntos simplemente intuitiva, que admite la existencia de conjuntos de objetos que tienen una propiedad definida cualquiera. Se requiere un enfoque axiomático particular y restringido para evitar estas paradojas, que se discuten en las secciones 1.3 y 1.4.

§ 1.2 Lógica y notación. Usaremos muchos símbolos de lógica para efectos de precisión y brevedad, especialmente en los capítulos iniciales, pero las demostraciones están escritas más que todo en un estilo informal. La teoría se presenta como una teoría axiomática del tipo familiar en geometría y otras partes de la matemática, y no como un sistema lógico formal para el cual se den reglas exactas de sintaxis y de semántica. La claridad de las demostraciones es suficiente para que cualquier lector, familiarizado con la lógica matemática, pueda dar demostraciones formalizadas en cualquier sistema convencional de lógica. Sin embargo, no se requiere familiaridad con la lógica matemática para entender ninguna parte de este libro.

En este punto introducimos los pocos símbolos lógicos que vamos a usar. Primero consideramos cinco símbolos para las cinco conectivas proposicionales más comunes. La negación de una fórmula **P** se escribe como **-P**. La conjunción de dos fórmulas **P** y **Q** se escribe como **P** & **Q**. La disyunción de **P** y **Q** como **P** $\vee$ **Q**. La implicación, con **P** como antecedente y **Q** como consecuente, como **P** $\rightarrow$ **Q**. La equivalencia, **P** *si y sólo si* **Q**, como **P** $\leftrightarrow$ **Q**. El cuantificador universal *Para todo* **v** como ($\forall$**v**) y el cuantificador existencial *Para algún* **v** como ($\exists$**v**). También usaremos el símbolo (E!**v**) para *Existe exactamente un* **v** *tal que*. Esta notación puede resumirse en la siguiente tabla.

NOTACION LOGICA

-P	No es el caso de que **P**
P & **Q**	**P** y **Q**
P $\vee$ **Q**	**P** o **Q**
P $\rightarrow$ **Q**	Si **P**, entonces **Q**
P $\leftrightarrow$ **Q**	**P** si y sólo si **Q**
($\forall$**v**)**P**	Para todo **v**, **P**
($\exists$**v**)**P**	Para algún **v**, **P**
(E!**v**)**P**	Existe exactamente un **v** tal que **P**

Así, la proposición:

Para todo x existe un y tal que $x < y$

se simboliza:

(1) $(\forall x)(\exists y)(x < y)$.

La proposición:

Para todo ε existe un δ tal que para todo y si $|x-y|<\delta$, entonces $|f(x) - f(y)| < \varepsilon$

se simboliza:

(2) $(\forall \epsilon)(\exists \delta)(\forall y)(|x - y| < \delta \rightarrow |f(x) - f(y)| < \epsilon)$.

La proposición:

Para todo x existe exactamente un y tal que $x + y = 0$

se simboliza:

$$(\forall x)(\mathrm{E}!y)(x + y = 0).$$

Un símbolo lógico puede corresponder a varias expresiones del lenguaje ordinario. Así, ($\forall$**v**)**P** se puede leer *Para todo* **v**, **P** o también *Para cada* **v**, **P**. Las proposiciones (1) y (2) ilustran el uso de paréntesis para efectos de puntuación. No parece necesaria una explicación formal. Sin embargo, una convención concerniente al predominio relativo de las conectivas proposicionales &, $\vee$, $\rightarrow$ y $\leftrightarrow$ reducirá considerablemente el número de paréntesis. La convención es que $\leftrightarrow$ y $\rightarrow$ predominan sobre & y $\vee$. Así, la fórmula:

$$(x < y \;\&\; y < z) \rightarrow x < z$$

se puede escribir sin paréntesis:

(3) $x < y \;\&\; y < z \rightarrow x < z.$

En forma análoga,

$$x + y \neq 0 \leftrightarrow (x \neq 0 \vee y \neq 0)$$

se puede escribir:

$$x + y \neq 0 \leftrightarrow x \neq 0 \vee y \neq 0.$$

Los principios de lógica que se necesitan en lo que sigue y con los cuales puedan no estar familiarizados algunos lectores, se explicarán intuitivamente cuando sean usados. Un principio acerca del cual hay algún desacuerdo entre los matemáticos, es que la doble barra '=' se toma como signo de identidad. La fórmula '$x = y$' se puede leer 'x es el mismo y', 'x es idéntico con y' o 'x es igual a y'. Esta última lectura se permite aquí solamente si se entiende que la igualdad significa identidad (que es lo que significa en casi todos los contextos matemáticos ordinarios). La situación exacta de la relación de identidad en la teoría de conjuntos se discute en § 2.2.

Unas pocas notas sobre los cuantificadores pueden ser útiles también. El *alcance* de un cuantificador es el cuantificador mismo junto con la fórmula más pequeña que lo sigue inmediatamente. Lo que es la fórmula más pequeña se indica siempre por medio de paréntesis. Así en la fórmula

(4) $(\exists x)(x < y) \vee y = 0$

el alcance del cuantificador '$(\exists x)$' es la fórmula '$(\exists x)(x < y)$'. Siguiendo una práctica casi universal en matemática, omitiremos en la formulación de *axiomas y teoremas* cualquier cuantificador universal cuyo alcance sea la fórmula total. Por ejemplo, en lugar de (1) escribiríamos: $(\exists y)(x<y)$.

En unos pocos lugares necesitaremos las nociones de variables *ligadas* y *libres.* Una aparición de una variable en una fórmula es ligada si y sólo si esta aparición está dentro del alcance de un cuantificador que use esta variable. Una aparición de una variable en una fórmula es libre si no es ligada. Finalmente, una variable es una *variable ligada* en una fórmula si y sólo si por lo menos una aparición es ligada; es una variable libre en una fórmula si y solamente si por lo menos una aparición es libre. En la fórmula (1) de esta sección, todas las variables son ligadas; en (3) todas las variables son libres; en (4) 'x' es ligada y 'y' es libre. En virtud de la convención establecida en el párrafo precedente, en relación con la omisión de los cuantificadores universales en axiomas y teoremas, todas las variables que aparezcan en axiomas y teoremas son ligadas.

§ 1.3 Esquema axiomático de abstracción y paradoja de Russell. En su desarrollo inicial de la teoría de conjuntos, Cantor no trabajó explícitamente a partir de axiomas. Sin embargo, el análisis de sus demostraciones indica que casi todos los teoremas por él demostrados, pueden derivarse de tres axiomas: (i) El axioma de extensionalidad para conjuntos, el cual afirma que dos conjuntos son idénticos si tienen los mismos elementos; (ii) el axioma de abstracción, el cual afirma que, dada una propiedad, existe un conjunto cuyos elementos son precisamente aquellas entidades que tienen tal propiedad; (iii) el axioma de escogencia, el cual no se formula en este momento y no es pertinente para nuestra discusión de las paradojas.

El origen de la confusión es el axioma de abstracción. La primera formulación explícita de él parece ser el axioma V de Frege [1893]. En 1901 Bertrand Russell descubrió que de este axioma podía desprenderse una contradicción, considerando el conjunto de todas las cosas que tienen la propiedad de no ser elementos de sí mismas.* Puesto que esta paradoja fue históricamente importante para motivar el desarrollo de nuevos axiomas restringidos para la teoría de conjuntos, se hará su deducción aquí. Para la formulación simbólica necesitamos introducir el predicado binario '$\in$' de pertenencia a un conjunto. La fórmula '$x \in y$' se lee 'x es un elemento de y', 'x pertenece a y' o, a veces, 'x está en y'. Así, si A es el conjunto de los primeros cinco enteros positivos impares, la proposición '$7 \in A$' es verdadera y '$6 \in A$' es falsa.

Usando '$\in$' y la notación lógica introducida en la sección que precede, podemos dar una formulación precisa del axioma de abstracción:

(1) $$(\exists y)(\forall x)(x \in y \leftrightarrow \varphi(x)),$$

donde se entiende que $\varphi(x)$ es una fórmula en la cual la variable 'y' no es libre. Para obtener la paradoja de Russell, queremos que $\varphi(x)$ afirme que x no es elemento de sí mismo. La fórmula apropiada es, claramente,

$$-(x \in x).$$

* Frege expresó su propia reacción a la paradoja de Russell en un famoso apéndice al segundo volumen de su *Grundgesetze der Arithmetik,* publicado en 1903. La traducción de los renglones dados aquí es de Geach y Black [1952, p. 234]. "Difícilmente puede sobrevenirle a un escritor científico algo más infortunado que ver vacilar uno de los fundamentos de su edificio, después de que su trabajo está terminado".

"Esta es la posición en que me ha colocado una carta de Mr. Bertrand Russell, precisamente cuando estaba para terminarse la impresión de este volumen. Me refiero a mi axioma V. Nunca me ha pasado inadvertido que le falta la auto-evidencia de los otros axiomas y la cual debe justamente exigirse de una ley lógica... De buena gana yo habría prescindido de este fundamento si hubiese sabido de un sustituto. Aun ahora no veo cómo puede establecerse científicamente la aritmética; cómo pueden los números considerarse como objetos lógicos y someterse a revisión, a menos que se nos permita —así sea condicionalmente— pasar de un concepto a su extensión. ¿Puedo yo siempre hablar de la extensión de un concepto, hablar de una clase? Y si no ¿cómo se reconocen los casos excepcionales?. . . Estas son las preguntas sugeridas por la comunicación de Mr. Russell". Para una discusión reciente del apéndice de Frege, véase Quine [1955].

Entonces tenemos como un ejemplo del axioma de abstracción:

(2) $(\exists y)(\forall x)(x \in y \leftrightarrow -(x \in x))$.

Tomando $x = y$ en (2), inferimos:

(3) $y \in y \leftrightarrow -(y \in y)$,

que es lógicamente equivalente a la contradicción:

(4) $y \in y \,\&\, -(y \in y)$.

Esta simple deducción tiene consecuencias de largo alcance para la fundamentación axiomática de la teoría de conjuntos. Ella muestra sencillamente que al admitir (1) como un axioma hemos permitido demasiado. Si adherimos a la lógica ordinaria, no podemos sostener, de una manera consecuente, que para cada propiedad exista un *conjunto* correspondiente de cosas que tengan esa propiedad.

Considerando cómo construir de nuevo los fundamentos de la teoría de conjuntos, quizás la primera cosa para destacar es que el axioma de abstracción es realmente un paquete de infinitos axiomas, más bien que un solo axioma: cuando reemplazamos la expresión '$\varphi(x)$' en (1) por *cualquier* fórmula en la cual 'y' no sea una variable libre, tenemos un nuevo axioma. Un axioma que permite esta clase de sustitución de fórmulas se llama usualmente un *esquema axiomático*. La razón para usar la palabra 'esquema' es obvia. Como aparece (1) no es una aserción definida sino un esquema para hacer muchas aserciones. A partir del esquema obtenemos una aserción definida sustituyendo '$\varphi(x)$' por una fórmula definida.

El esquema axiomático que usaremos se debe a Ernst Zermelo [1908] y se llama usualmente el *esquema axiomático de separación* (Aussonderung Axiom) porque nos permite separar los elementos de un conjunto dado que satisfacen alguna propiedad y forman el conjunto que consta precisamente de esos elementos. Así, si sabemos que el conjunto de los animales existe, podemos usar el *esquema* axiomático de separación para afirmar la existencia del conjunto de los animales que tienen la propiedad de ser hombres. Esto es, la propiedad de ser humanos nos permite separar a los hombres de los otros animales. La forma precisa del axioma correspondiente a (1) es:

(5) $(\exists y)(\forall x)[x \in y \leftrightarrow x \in z \,\&\, \varphi(x)]$.

El cambio de (1) a (5) es sutil pero fuerte. (1) afirmaba la existencia de conjuntos incondicionalmente. (5), por su parte, es completamente condicional; primero tenemos que haber dado el conjunto z y luego podemos afirmar la existencia del subconjunto y.

Debe ser claro que no podemos pasar de (5) a una contradicción como (4). Usando de nuevo la fórmula '$-(x \in x)$' como un ejemplo de (5) tenemos:

(6) $(\exists y)(\forall x)[x \in y \leftrightarrow x \in z \,\&\, -(x \in x)]$,

y de nuevo tomando $x = y$, inferimos:

(7) $y \in y \leftrightarrow y \in z \,\&\, -(y \in y)$,

lo cual no es contradictorio. Para hacer un poco más claro el significado de (7), sea z el conjunto A cuyos únicos dos elementos son el conjunto que consiste en el número 1 y el conjunto consistente del número 2, esto es,

(8) $A = \{\{1\}, \{2\}\}$.

(En (8) hemos introducido informalmente una notación familiar para describir conjuntos: describimos un conjunto escribiendo nombres o descripciones de sus elementos, separados por comas y encerrando el total entre llaves. En el capítulo siguiente se define formalmente esta notación). Considerando ahora el conjunto A y la fórmula de Russell '$-(x \in x)$', tenemos, por el esquema axiomático de separación:

(9) $(\exists y)[y \in y \leftrightarrow y \in A \,\&\, -(y \in y)]$.

La verdad de (9) se ve, escogiendo al mismo A como un y apropiado, puesto que A no es un elemento de sí mismo. Así, el miembro de la izquierda es falso y el de la derecha también lo es, ya que '$A \in A \,\&\, -(A \in A)$' es contradictorio.

Tanto el esquema axiomático de abstracción como el esquema axiomático de separación se han formulado como si fuera perfectamente claro por cuáles fórmulas exactamente se puede sustituir '$\varphi(x)$'. En el capítulo siguiente se considera una definición sintáctica rigurosa o *fórmula.* Lo que ha sido importante históricamente es que por medio de una definición rigurosa de las fórmulas de una teoría (aquí, la teoría de conjuntos) es como se puede hacer precisa la aplicación de un esquema axiomático como el de separación. Zermelo [1908] formuló originalmente el esquema axiomático de separación en términos de preguntas o afirmaciones que tienen la propiedad de ser *definidas.* En términos generales, sostuvo que un enunciado es definido si puede decidirse de manera no arbitraria, cuándo un objeto satisface o no a tal enunciado.* Su formulación del esquema axiomático es entonces (parafraseando ligeramente): Si un enunciado $\varphi(x)$ está definido para todos los elementos de un conjunto M, entonces existe siempre un subconjunto $M\varphi$ de M, el cual contiene exactamente aquellos elementos x de M para los cuales $\varphi(x)$ es verdadero.

La primera clarificación real de esta noción de definitud la dio Skolem [1922] quien caracteriza los enunciados definidos como aquellos que satisfacen precisamente su definición rigurosa de fórmula. Para una discusión un poco más extensa véase Zermelo [1929], y Skolem [1930].*

No es factible entrar en los detalles de estos documentos de Zermelo y Skolem, pero algunos lectores no interesados en la claridad por sí misma, pueden extrañarse de por qué Zermelo estaba tan interesado ante todo en restringir el esquema axiomático de separación a enunciados *definidos.* La respuesta a este interrogante se da más fácilmente en el contexto de la discusión de paradojas ulteriores que aparecen en los fundamentos de la matemática.

Antes de pasar a esas paradojas en la sección siguiente, puede hacerse una observación histórica acerca de los axiomas que se van a considerar en lo que sigue. Esencialmente, corresponden muy de cerca a los de Zermelo [1908]. Sin embargo, cuando lleguemos a la teoría de inducción transfinita y aritmética ordinal, necesitaremos agregar un esquema axiomático más sólido que el de separación, a saber, el que usualmente se llama *esquema axiomático de sustitución*, debido a Fraenkel [1922a].† Por estas razones, el sistema de teoría axiomática descrito en este libro se suele llamar *teoría de conjuntos de Zermelo-Fraenkel* en la literatura sobre la materia, aunque parecería más apropiado históricamente, llamarla de Zermelo-Fraenkel-Skolem.

§ 1.4 **Más paradojas.** Por su simplicidad la paradoja de Russell se ha introducido para mostrar por qué es inconsistente la axiomatización directa y obvia de la teoría de conjuntos intuitiva. Otras paradojas se descubrieron antes de la de Russell; la primera que se publicó fue, aparentemente, la paradoja del mayor ordinal, debida a Burali-Forti [1897]. Un análisis completo de las diez o doce paradojas ‡ que se han discutido en la literatura matemática estaría fuera de lugar en este libro; pero el lector encontrará un buen estudio en Beth [1950]. Muchas de las paradojas son variaciones relativamente ligeras unas de otras, de modo que sólo describiremos breve e informalmente las más importantes.

F. P. Ramsey [1926] parece ser la primera persona que divide clara y explícitamente las paradojas en dos clases: las lógicas o matemáticas, y las lingüísticas o semánticas. Infor-

* La decisión no tiene que ser por algún procedimiento efectivo o finito. Para un estudio más a fondo de este punto véase Zermelo [1929].

* El estudio de Zermelo [1929] trata también de precisar la noción de definitud; fue escrito sin conocer el documento de Skolem [1922] y no proporciona una formulación tan satisfactoria como el de Skolem. En un trabajo de 1930, Skolem hizo algunas críticas notables al estudio de Zermelo. Una clarificación menos detallada, pero esencialmente correcta de *definitud* fue la que dio independientemente Fraenkel [1922b].

† Esencialmente el mismo axioma fue propuesto, al mismo tiempo e independientemente, por Skolem [1922].

‡ Una paradoja se llama también *antinomia* en la literatura.

malmente hablando, la primera clase surge de construcciones puramente matemáticas; la segunda, de la consideración directa del lenguaje que usamos para hablar de matemática y de lógica.

La paradoja de Russell pertenece a la primera clase, lo mismo que la paradoja de Burali-Forti, que se discutirá más adelante en § 5.3. La idea general de esta paradoja es como sigue: En teoría intuitiva de conjuntos, todo conjunto bien ordenado tiene un número ordinal. Aún más, el conjunto de todos los ordinales es bien ordenado; por consiguiente el conjunto de todos los números ordinales tiene un número ordinal, digamos Θ . Pero el conjunto de todos los ordinales hasta, e incluyendo, un ordinal dado, es bien ordenado; así que tiene un número ordinal que excede en uno al ordinal dado. En consecuencia, el conjunto de todos los ordinales, incluyendo Θ tiene el número ordinal $\Theta + 1$, que es mayor que Θ . Por consiguiente, Θ no es el número ordinal de todos los ordinales.

Podría pensarse que algún artificio como el que bloqueó la deducción directa de la paradoja de Russell haría lo mismo con la de Burali-Forti, pero no es este el caso. Por ejemplo, J. B. Rosser [1942] dedujo esta última paradoja en el sistema de Quine [1940] mostrando de ese modo su inconsistencia, aunque es claro que no es posible la deducción directa de la paradoja de Russell en el sistema de Quine.

Otra bien conocida paradoja de la primera clase es la del mayor número cardinal, debida a Cantor, que la descubrió en 1899 y que se publicó por primera vez, con su correspondencia, en 1932. Operando de nuevo en teoría intuitiva de conjuntos, consideramos el número cardinal n del conjunto S de todos los conjuntos. Por una parte es claro que n es el mayor cardinal posible. Pero podemos también considerar el conjunto de todos los subconjuntos de S y su cardinal, p. Por un teorema clásico de la teoría de conjuntos intuitiva, p debe ser mayor que n.

Para los lectores no familiarizados con las nociones de número cardinal y de número ordinal, usadas libremente para describir las dos últimas paradojas, puede decirse que en los capítulos siguientes se desarrollarán estas nociones en detalle y completamente *ab ovo.* Aunque por el momento no hagamos un análisis exacto, es claro, de un modo general, que esas paradojas no surgen cuando el axioma primario para construir conjuntos es el esquema axiomático de separación de Zermelo, pues entonces no puede establecerse la existencia del conjunto de todos los conjuntos o del conjunto de todos los números ordinales.

La más vieja paradoja semántica es la del mentiroso, debida a Epiménides de Creta, que decía: "Yo estoy mintiendo". Si la afirmación es verdadera, entonces está mintiendo y la afirmación es falsa. Si la afirmación es falsa, entonces no está mintiendo y la afirmación es verdadera. Hay muchas versiones modernas. Considérese la oración: "La única oración escrita en esta pizarra es falsa". Si la oración es verdadera, debe ser falsa y recíprocamente.

Un acertijo divertido y de la misma clase, que data de la antigüedad, es el dilema del cocodrilo. Este ha robado un niño y dice al padre: "Te devolveré a tu hijo si adivinas si te lo devolveré o no". El padre replica: "Tú no me devolverás al niño". ¿Qué debe hacer el cocodrilo?

La primera paradoja semántica moderna que ha sido publicada parece ser la paradoja de Richard [1905], que está relacionada con la demostración de la no ennumerabilidad del conjunto de los números reales, debida a Cantor (demostración que se da en § 6.6.* Entenderemos por una *expresión* del idioma cualquier sucesión finita de las veintiséis letras básicas del alfabeto, una coma, un punto y un espacio en blanco; o sea que una expresión es una sucesión finita de algunos

* Para un análisis y exposición de la paradoja de Richard véase Church [1934].

de esos veintinueve símbolos. Ahora ordenemos las expresiones, de acuerdo con el número total de símbolos y lexicográficamente dentro del número total cada una. Así tenemos,

a
b
⋮
aa
ab
⋮
aaa
⋮

Ahora borremos aquellas expresiones que no definen números reales; sea E la sub-sucesión restante. Traduciendo y parafraseando un poco, podemos usar la formulación original de Richard para definir un cierto número real N con respecto a E: "El número real cuya parte entera es cero y cuyo n-simo decimal es p más uno,si el n-simo decimal del número real definido por el n-simo elemento de E es p y p no es ni ocho ni nueve; y es simplemente uno si su n-simo decimal es ocho o nueve". Por construcción, N no es un elemento de E. ya que difiere de todo número real de E por lo menos en un puesto decimal; pero N está definido por una expresión finita y por tanto está en E. De este modo se llega a la contradicción.

La tercera y final paradoja semántica que mencionaremos aquí es la de *heterologicidad,* debida a Grelling-Nelson [1908]. Un predicado se llama heterológico si la proposición que atribuye al predicado la propiedad expresada por el predicado es falsa. Así, el predicado 'rojo' es heterológico puesto que la proposición: "El predicado 'rojo' es rojo" es falsa. La contradicción surge de preguntar si el predicado 'heterológico' es él mismo heterológico. Claramente, si lo es, inferimos que no lo es; y si no lo es, que sí lo es.

Una discusión detallada de esas paradojas semánticas nos apartaría mucho de la teoría de conjuntos propiamente dicha y nos llevaría al dominio general de la lógica formal; pero es pertinente ver cómo las inferencias que llevan a ellas están bloqueadas en la teoría de conjuntos de Zermelo-Fraenkel. Zermelo introdujo específicamente su noción de definitud en el esquema axiomático de separación para prevenir la construcción de paradojas semánticas (cf. Zermelo [1908, p. 264]). Como se observó en la sección precedente, esta noción de definitud se precisa reduciéndola a la noción sintáctica de fórmula. Con referencia a las paradojas semánticas puede hacerse más claro el objeto de esta reducción. Cada una de estas paradojas surge de tener disponibles en el lenguaje expresiones para referirse a otras expresiones del idioma. Cualquier lengua con medios de expresión tan ilimitados es forzosamente inconsistente.*

En consecuencia es importante distinguir entre el objeto lenguaje —aquí, el lenguaje en el cual hablamos acerca de conjuntos— y el meta-lenguaje, esto es, el lenguaje en el cual hablamos acerca del objeto lenguaje. Aun cuando la teoría de conjuntos no se desarrolla en este libro de manera completamente formalizada, al comienzo del capítulo siguiente consideramos una definición rigurosa de *fórmula* para el objeto lenguaje que usamos. Nuestro meta-lenguaje es cierto fragmento,

* En Tarski [1956, p. 402] se expresa esto más sucintamente: "El origen principal de las dificultades que encontramos parece descansar en lo siguiente: No se ha tenido siempre en cuenta que los conceptos semánticos tienen un carácter relativo; que es preciso relacionarlos siempre con un idioma particular. No se ha tenido en cuenta que el lenguaje *acerca del cual* hablamos no tiene necesariamente que coincidir con el lenguaje *en el cual* hablamos. Se ha realizado la semántica de una lengua en la lengua misma y —hablando en forma general— se ha procedido como si hubiera una sola lengua en el mundo. El análisis de las antinomias mencionadas muestra, por el contrario, que los conceptos semánticos simplemente no tienen lugar en el idioma al cual se refieren; que el idioma que contiene su propia semántica y dentro del cual las leyes lógicas usuales subsisten, debe ser inevitablemente inconsistente".

vagamente definido, del idioma ordinario, incrementado con ciertos símbolos familiares de la matemática intuitiva. Será obvio que nuestro objeto lenguaje no es lo bastante rico para proporcionar medios directos de expresar las paradojas semánticas. En otras palabras, evitamos esas paradojas restringiendo severamente la riqueza de nuestro lenguaje. Obsérvese que cuando se usa un lenguaje formalizado, es intuitivamente claro que hay pocas perspectivas de deducir una de las paradojas semánticas en este lenguaje; la situación intuitiva de las paradojas matemáticas o lógicas no es usualmente tan clara.

Los asuntos semánticos no se discutirán en lo que sigue. Se han discutido superficialmente aquí para aclarar la necesidad de lo que equivale a una restricción semántica al esquema axiomático de separación. Debería mencionarse, además, que se necesita una formalización rigurosa y completa del objeto lenguaje para demostrar hechos meta-matemáticos relacionados con la teoría de conjuntos de Zermelo-Fraenkel. Por 'hechos meta-matemáticos' entendemos hechos acerca del objeto lenguaje. Un ejemplo de un hecho meta-matemático importante es que el *esquema* axiomático de separación no puede ser reemplazado por un número finito de axiomas del objeto lenguaje.

Finalmente, debe recalcarse que la teoría de conjuntos de Zermelo-Fraenkel no proporciona sino uno de los varios enfoques posibles de la fundamentación matemática. Hay una alternativa tan íntimamente ligada a ella, que debe mencionarse aquí, a saber, la teoría de conjuntos de von Neumann-Bernays-Gödel.* Hay dos diferencias esenciales. Esta última puede ser axiomatizada de manera finita. No se requiere esquema axiomático como el de separación, sino que es suficiente, en su lugar, un número finito de construcciones y clases. En lo que llamaremos por brevedad teoría de conjuntos de von Neumann, hay una distinción técnica entre clases y conjuntos. Todo conjunto es una clase pero no recíprocamente. Aquellas clases que no son conjuntos se llaman *clases propias* y la característica que las distingue es que no son elementos de otras clases. La clase de todos los números ordinales y la clase de todos los conjuntos existen ambas, pero ambas son clases propias. Así las paradojas de Burali-Forti y la de Cantor no pueden construirse, porque requieren que esas clases sean elementos de otras clases. Observaciones análogas se aplican a la paradoja de Russell. En los capítulos siguientes se dan frecuentemente indicaciones informales para llamar la atención a las ligeras variaciones requeridas en los teoremas, definiciones o demostraciones de la teoría de von Neumann. Las teorías de Zermelo y de von Neumann están tan cercanamente relacionadas, que cualquiera que esté familiarizado con una de ellas dominará pronto la otra.

§ 1.5 Presentación de axiomas. Puesto que los axiomas que usaremos para la teoría de conjuntos de Zermelo-Fraenkel se introducen individualmente en diversas secciones de los capítulos siguientes, quizá sea útil una presentación rápida que proporcione una visión general del desarrollo. Las observaciones en este momento son superficiales, pues presentaremos los axiomas sólo por su nombre. En el capítulo siguiente consideraremos

* Formulada originalmente por von Neumann en una serie de monografías [1925], [1928a], [1929]. Su formulación difiere considerablemente de la teoría de conjuntos de Zermelo, porque la noción de función se toma como fundamental en lugar de la de clase o conjunto. En una serie de estudios publicados en el *Journal of Simbolic Logic* Bernays modificó el enfoque de von Neumann para permanecer más cerca del sistema original de Zermelo (véase en la Bibliografía la lista de monografías). Introdujo dos relaciones de pertenencia: una entre conjuntos y otra entre conjuntos y clases. En Gödel [1940] la teoría está más simplificada aún; las nociones primitivas son las de conjunto, clase y pertenencia (aun cuando la pertenencia sola es suficiente). Un estudio de R. M. Robinson [1937] proporciona un sistema simplificado, cercano al sistema original de von Neumann.

estos siete axiomas, que son los principales que vamos a necesitar:

Axioma de extensionalidad
Esquema axiomático de separación
Axioma de unión
Axioma de apareamiento
Axioma de regularidad
Axioma de suma
Axioma del conjunto potencia.

Hacia el final del Capítulo 2 mostraremos que el axioma de unión es redundante, o sea que puede deducirse de los otros seis. Se usa al principio del capítulo a fin de simplificar los desarrollos iniciales.

En el Capítulo 3, que trata de relaciones y funciones, no se introducen nuevos axiomas. En el Capítulo 4 se presenta un axioma especial para números cardinales y se usa principalmente en el contexto de ese capítulo. Este axioma especial no es parte de la teoría de conjuntos clásica de Zermelo-Fraenkel, pero facilita enormemente la construcción de la teoría intuitiva del número cardinal dentro de nuestra estructura axiomática.

El axioma de infinitud se introduce en el Capítulo 5 para hacer posible la demostración de que el conjunto de todos los números naturales existe. Los números naturales pueden sin embargo construirse prescindiendo de este axioma. El Capítulo 6 trata de las construcciones de los números reales y no se necesitan más axiomas para este trabajo.

En el Capítulo 7 se usa el esquema axiomático de sustitución cuando es necesario para el desarrollo de la aritmética ordinal y la inducción transfinita. Se muestra también que el axioma de apareamiento se puede deducir de este esquema y el axioma del conjunto potencia. El Capítulo 8, el final, está dedicado principalmente al axioma de escogencia.

Capítulo 2

Desarrollos generales

§ 2.1 **Preliminares: Fórmulas y definiciones.** (a) Definamos explícitamente la noción de fórmula, requerida en el esquema axiomático de separación (y más tarde en el esquema axiomático de sustitución); y (b) fijemos el concepto de las definiciones que vamos a adoptar para introducir los muchos símbolos definidos que se requieren.

En el Capitulo 1 se hizo una importante distinción entre el objeto lenguaje, esto es, el lenguaje en el cual hablamos acerca de conjuntos, y el meta-lenguaje, o sea, el lenguaje en el cual tratamos acerca del objeto lenguaje. Usamos el meta-lenguaje, que para nosotros es el idioma ordinario, incrementado con una cierta cantidad de lenguaje matemático intuitivo, para describir rigurosamente el objeto lenguaje. Puede ser útil considerar esta descripción como análoga a una caracterización rigurosa de un juego como el ajedrez o el bridge; pero esta analogía no debe llevarse muy lejos, pues la mayor parte de las expresiones de nuestro objeto lenguaje tienen un significado definido en términos de ideas matemáticas intuitivas que no tienen las posiciones o movimientos de un juego como el ajedrez.

Comenzamos con una quíntuple clasificación de los símbolos del objeto lenguaje en constantes, variables, conectivas proposicionales, cuantificadores u operadores, y símbolos de puntuación o agrupación.* Las dos constantes primitivas del lenguaje son el símbolo de la relación de pertenencia, $\in$, introducido informalmente en el Capítulo 1, y la constante '0' que denota el conjunto vacío. Además, tomamos de la lógica el predicado constante '$=$', que es el símbolo de la identidad. Las variables generales, que recorren todos los objetos, son: 'x', 'y', 'z',. . . con sub-índices o super-índices, o sin ellos. Las conectivas proposicionales son las cinco mencionadas en § 1.2: $-$, $\&$, $\vee$, $\rightarrow$, $\leftrightarrow$; los tres cuantificadores u operadores lógicos que usamos, $\forall$,$\exists$,$E!$, se mencionaron también en § 1.2. Finalmente, los paréntesis a izquierda y a derecha son nuestros únicos símbolos de puntuación.

Las *expresiones* del objeto lenguaje son sucesiones finitas de las cinco clases de símbolos del lenguaje. Algunas de esas expresiones se llaman *fórmulas primitivas* del objeto lenguaje, simplemente por razón de su estructura. Ahora definimos tales fórmulas, de modo que con sólo mirar la forma de una expresión, podemos decidir automáticamente, en un número finito de pasos, si se trata o no de una fórmula primitiva. Si bien esta definición es puramente sintáctica o estructural, son precisamente las expresiones que la satisfacen las que tienen un significado intuitivo claro. Una expresión como '$(\rightarrow \in x$' no es una fórmula primitiva ni tiene significado intuitivo.

Definimos primero las fórmulas primitivas *atómicas*.

Una fórmula atómica primitiva es una expresión de la forma ($\mathbf{v} \in \mathbf{w}$), *o de la*

* Esta clasificación la originó von Neumann [1927]. Para discusión detallada de estos temas, véase el primer capítulo de Church [1956].

forma $(\mathbf{v} = \mathbf{w})$, *donde* $\mathbf{v}$, $\mathbf{w}$ *son variables generales o la constante* '0'. *

Así, '$x \in y$' y '$z = 0$' son fórmulas primitivas atómicas.

Podemos ahora dar lo que usualmente se llama una definición recurrente de las *fórmulas primitivas:*

a) *Toda fórmula atómica primitiva es una fórmula primitiva;*
b) *Si* $\mathbf{P}$ *es una fórmula primitiva, entonces* $-\mathbf{P}$ *es una fórmula primitiva;*
c) *Si* $\mathbf{P}$ *y* $\mathbf{Q}$ *son fórmulas primitivas, entonces,* $(\mathbf{P} \,\&\, \mathbf{Q})$, $(\mathbf{P} \vee \mathbf{Q})$, $(\mathbf{P} \rightarrow \mathbf{Q})$, *y* $(\mathbf{P} \leftrightarrow \mathbf{Q})$ *son fórmulas primitivas;*
d) *Si* $\mathbf{P}$ *es una fórmula primitiva y* $\mathbf{v}$ *es una variable general, entonces,* $(\forall \mathbf{v})\mathbf{P}$, $(\exists \mathbf{v})\mathbf{P}$ *y* $(\mathrm{E}!\mathbf{v})\mathbf{P}$ *son fórmulas primitivas;*
e) *Ninguna expresión del objeto lenguaje es una fórmula primitiva. a menos que se siga de las reglas* a) - d).

Los siguientes son ejemplos de fórmulas primitivas del objeto lenguaje que no son atómicas '$(\exists x)(\forall y) - (y \in x)$', '$x \in y \rightarrow y \in z$', '$(\mathrm{E}!\, z) \quad (0 = z)$'. En términos de esta definición, una formulación rigurosa del esquema axiomático de separación es la siguiente:

Cualquier fórmula primitiva del objeto lenguaje de la forma $(\exists \mathbf{v})((\exists \mathbf{w}_1)(\mathbf{w}_1 \in \mathbf{v} \vee \mathbf{v} = 0) \,\&\, (\forall \mathbf{w})\,(\mathbf{w} \in \mathbf{v} \leftrightarrow \mathbf{w} \in \mathbf{u} \,\&\, \varphi))$ *es un axioma, siempre que la variable* $\mathbf{v}$ *sea distinta de* $\mathbf{u}$ *y* $\mathbf{w}_1$ *y no sea libre en la fórmula primitiva* φ.

La primera cláusula del axioma garantiza que un individuo arbitrario no puede hacer el papel del conjunto vacío, 0. En la sección siguiente se dan razones que justifican las restricciones sobre la variable v.

En principio, todos los axiomas y teoremas que formularemos en las páginas siguientes se pueden escribir como fórmulas primitivas del objeto lenguaje; en efecto, nuestro objeto lenguaje oficial consistirá en esas fórmulas primitivas. Para facilitar el trabajo será útil y conveniente introducir por definición mucha notación adicional. En la práctica aplicaremos el esquema axiomático de separación de fórmulas que no están escritas únicamente en la notación primitiva; pero ya que en cualquier punto de nuestro desarrollo habrá precedido sólo un número finito de definiciones, tal fórmula puede reemplazarse por una fórmula primitiva, mediante un número finito de sustituciones.

Con respecto a las definiciones, nuestro punto de vista es, entonces, que se pueden admitir informalmente, si se dan indicaciones claras para eliminar los símbolos nuevos de cualquier contexto. Así pues, exigimos que una fórmula del objeto lenguaje que introduzca un nuevo símbolo satisfaga el siguiente:

Criterio de eliminabilidad. *Una fórmula* $\mathbf{P}$ *que introduce un nuevo símbolo satisface el criterio de eliminabilidad si y sólo si, cuando quiera que* $\mathbf{Q}_1$ *sea una fórmula en la cual el nuevo símbolo aparece, hay una fórmula primitiva* $\mathbf{Q}_2$ *tal que* $\mathbf{P} \rightarrow (\mathbf{Q}_1 \leftrightarrow \mathbf{Q}_2)$ *es deducible de los axiomas.*

Nótese que hemos formulado este criterio sin dar una definición rigurosa de *fórmula* (en oposición a *fórmula primitiva*). Tal definición es viable, si hacemos la lista de todos los símbolos definidos que se han introducido en este libro y luego procedemos, en términos de esta lista, como hicimos antes con la notación primitiva. No llevaremos a cabo

* En esta definición, como en cualquier otra parte, usamos las letras en negrilla '**u**', '**v**', '**w**', '$\mathbf{u}_1$', '$\mathbf{v}_1$', '$\mathbf{w}_1$', ... como variables meta-matemáticas, las cuales toman como valores variables 'x', 'y', 'z',... o la constante '0' del objeto lenguaje. Usamos letras en negrilla '**P**', '**Q**'. . . o letras griegas φ y Ψ como variables meta-matemáticas que toman como valores fórmulas del objeto lenguaje. Las convenciones acerca del uso y mención seguidos aquí, las cuales son probablemente obvias, son: (i) las constantes '$\in$' e '$=$', las conectivas proposicionales, los símbolos de cuantificación, y los paréntesis a izquierda y a derecha, se usan como nombres de sí mismos, (ii) la yuxtaposición de nombres de expresiones denota una operación binaria sobre expresiones que producen nuevas expresiones (por ejemplo '$x \in y$' & '$y \in z$' = '$x \in y \,\&\, y \in z$'). Para una discusión más detallada de estas convenciones, véase el capítulo 6 de Suppes (1957).

esta tediosa tarea, pero sí queremos mencionar un segundo criterio que deben satisfacer nuestras definiciones, a saber: que no deben ser creativas.

> **Criterio de no creatividad.** *Una fórmula* **P** *que introduce un nuevo símbolo satisface el criterio de no creatividad si y sólo si no hay fórmula primitiva* **Q** *tal que* **P** $\rightarrow$ **Q** *sea deducible de los axiomas sin que* **Q** *lo sea.*

En otras palabras, una definición no debería funcionar como un axioma que permita la deducción de alguna fórmula previamente indemostrable, en la cual sólo aparezca la notación primitiva.

El problema clásico de la teoría de la definición, para una teoría matemática formulada rigurosamente, es proporcionar reglas de definición cuya satisfacción asegure la satisfacción de los dos criterios que acabamos de expresar. Podemos restringirnos aquí a las reglas para definir símbolos de operación. Con ligeras modificaciones se producen reglas apropiadas para definir símbolos de relación y constantes individuales.* En estas reglas nos referimos a *definiciones precedentes,* lo cual implica que éstas se dan en una sucesión fija y no simultáneamente; este enfoque permite usar símbolos ya definidos, en las definiciones de los símbolos nuevos.*

Las definiciones propias de los símbolos de operación pueden ser equivalencias o identidades. Comenzamos con las primeras.

> ***Una equivalencia* P *que introduce un nuevo símbolo n-ario de operación* O *es una definición propia si y sólo si* P *es de la forma***
>
> $$\mathbf{O}(\mathbf{v}_1, \ldots, \mathbf{v}_n) = \mathbf{w} \leftrightarrow \mathbf{Q}$$
>
> *y se satisfacen las siguientes restricciones:* (i) $\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{w}$ *son variables distintas;* (ii) **Q** *no tiene variables libres diferentes de* $\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{w}$; (iii) **Q** *es una fórmula en la cual las únicas constantes no lógicas son los símbolos primitivos o previamente definidos de la teoría de conjuntos; y* (iv) *la fórmula* (E!w) **Q** *es deducible de los axiomas y definiciones que preceden.*

Con respecto a la frase "constantes no lógicas" en (iii), las únicas constantes lógicas son las introducidas en §1.2; todas las otras constantes son no lógicas. Fácilmente se justifican las varias restricciones. Aquí sólo destacaremos la importancia de (iv). Considérese la siguiente definición de la aritmética elemental para la pseudo-operación $\bigstar$.

(1) $x \bigstar y = z \leftrightarrow x < z \;\&\; y < z.$

Claramente es falso que

$$(\mathrm{E}!z)\ (x < z \;\&\; y < z).$$

Así que (1) viola (iv) y queremos demostrar que esta violación lleva a una contradicción. Puesto que $1 < 3,\ 2 < 3,\ 1 < 4,\ 2 < 4$, inferimos inmediatamente de (1):

$$1 \star 2 = 3$$

y además

$$1 \star 2 = 4.$$

Por consiguiente,

$$4 = 3,$$

lo que es absurdo. En lenguaje matemático ordinario el punto (iv) requiere que la ejecución de una operación produzca siempre un objeto único.

Para una definición que sea una identidad tenemos la siguiente regla.

> *Una identidad* **P** *que introduce un nuevo símbolo n-ario de operación* **O** *es una definición propia si y sólo si* **P** *es de la forma*
>
> $$\mathbf{O}(\mathbf{v}_1, \ldots, \mathbf{v}_n) = \mathbf{t}$$
>
> *y se satisfacen las siguientes restricciones:* (i) $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *son variables distintas;* (ii) *el término* **t** *no tiene variables libres diferentes de* $\mathbf{v}_1, \ldots, \mathbf{v}_n$; (iii) *las únicas constantes no lógicas en el término* **t** *son*

* Las constantes individuales pueden tratarse, en efecto, como símbolos de operación de grado cero.

* Las reglas que se dan a continuación, y otros temas conexos, se tratan más detalladamente en el capítulo 8 de Suppes [1957].

símbolos primitivos y símbolos previamente definidos de la teoría de conjuntos.

Un ejemplo de una definición por medio de una identidad, en aritmética, es la definición de sustracción en términos de adición y de la operación negativa.

$$x - y = x + (-y).$$

Es viable probar que las definiciones que satisfacen algunas de las reglas que acabamos de dar o las análogas para símbolos de relación y constantes individuales, satisfacen los criterios de eliminabilidad y de no creatividad. Desafortunadamente, muchas de las definiciones comunes en matemática y muchas de las definiciones que se van a introducir en lo que sigue, no satisfacen el criterio de eliminabilidad; así también, muchas de las definiciones de símbolos de operación dejan de satisfacer una de las dos reglas anteriores. La razón de esta falla puede expresarse simplemente así: las definiciones son frecuentemente condicionales en la forma. Ejemplo típico de definición condicional en aritmética es una definición de división, en la cual surge el problema de la división por cero:

(1) $y \neq 0 \rightarrow (x/y = z \leftrightarrow x = y \cdot z).$

Usando (1) como definición del símbolo de operación para la división, no podemos eliminar el símbolo de contextos como:

$$1/0 \neq 2.$$

Por otra parte, podemos usar (1) para eliminar la división en todos los casos "interesantes", o sea, en todos aquellos que satisfacen la hipótesis de (1). Aún más, no es difícil modificar las dos reglas dadas, de tal manera que las definiciones condicionales que las satisfacen satisfagan el criterio de no creatividad. En efecto, las modificaciones apropiadas de la regla para las equivalencias que definen símbolos de operación están incorporadas en lo siguiente:

Una implicación $\mathbf{P}$ *que introduce un nuevo símbolo de operación* $\mathbf{O}$ *es una definición condicional si y sólo si* $\mathbf{P}$ *es de la forma*

$$\mathbf{Q} \rightarrow [\mathbf{O}(\mathbf{v}_1, \ldots, \mathbf{v}_n) = \mathbf{w} \leftrightarrow \mathbf{R}]$$

y se satisfacen las siguientes restricciones: (i) *la variable* $\mathbf{w}$ *no es libre en* $\mathbf{Q}$; (ii) *las variables* $\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{w}$ *son distintas;* (iii) $\mathbf{R}$ *no tiene variables libres diferentes de* $\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{w}$; (iv) $\mathbf{Q}$ *y* $\mathbf{R}$ *son fórmulas en las cuales las únicas constantes no lógicas son los símbolos primitivos y los símbolos previamente definidos de la teoría de conjuntos;* (v) *la fórmula* $\mathbf{Q} \rightarrow (\mathrm{E!}\mathbf{w})\,\mathbf{R}$ *es deducible de los axiomas y definiciones que preceden.*

Convertir una definición condicional de un símbolo de operación en una definición propia que satisfaga el criterio de eliminabilidad es asunto de rutina una vez que se escoge un objeto que puede ser el resultado de efectuar la operación cuando no se satisface la hipótesis de la definición condicional. En aritmética, la escogencia natural es el número cero. Estando de acuerdo sobre esto, podemos reemplazar la definición condicional (1) de división por

$$x/y = z \leftrightarrow (y \neq 0 \rightarrow x = y \cdot z) \ \& \ (y = 0 \rightarrow z = 0).$$

La escogencia natural correspondiente en la teoría de conjuntos es el conjunto vacío. De modo que cualquier definición condicional que satisfaga la regla antes formulada puede convertirse en una definición propia, escribiéndola como:

(2) $\mathbf{O}(\mathbf{v}_1, \ldots, \mathbf{v}_n) = \mathbf{w} \leftrightarrow (\mathbf{Q} \rightarrow \mathbf{R}) \ \& \ (-\mathbf{Q} \rightarrow \mathbf{w} = 0).$

En lo que sigue usaremos continuamente definiciones condicionales, pero subentendemos que la notación que ellas introducen puede ser eliminada siempre, en favor de la notación primitiva, formulándolas de nuevo como definiciones propias de la forma indicada por (2).

Desde un punto de vista lógico, las definiciones que hemos venido describiendo son axiomas no creativos expresados en el objeto lenguaje. Se clasifican propiamente como axiomas porque funcionan como premisas adicionales en la deducción de teoremas, pero su carácter no creativo asegura que no refuerzan realmente la teoría de conjuntos tal como fue formulada en los axiomas creativos básicos. Ocasionalmente introduciremos esquemas de definición que, como el esquema axiomático de separación, deberían formularse propiamente en el meta-lenguaje. Tales esquemas de definición aparecerán principalmente en relación con la introducción de nuevos métodos de ligar variables. Aumentamos también nuestra notación primitiva con la introducción de varios tipos de variables: variables de conjuntos, que recorren conjuntos pero no individuos ('A', 'B', 'C',...), variables cardinales, que recorren los números cardinales ('$\mathfrak{m}$', '$\mathfrak{n}$', '$\mathfrak{p}$',...), variables ordinales, que recorren los números ordinales ('α', 'β', 'γ',...), variables que recorren los enteros no negativos ('m', 'n', 'p',...), variables racionales, que recorren los números racionales no negativos ('M', 'N', 'P',...). No consideraremos aquí explícitamente reglas para los esquemas de definición que introducen nuevas variables o nuevos métodos de ligar variables, pero será claro, para el pequeño número de tales esquemas que se usan efectivamente, cómo puede demostrarse que ellos satisfacen los dos criterios de eliminabilidad y de no creatividad, o cómo pueden ser ligeramente modificados para obtener tal satisfacción.

§ 2.2 **Axiomas de extensionalidad y separación.** Comenzamos con la definición de la noción de conjunto. El contenido de la definición concuerda con ideas intuitivas: un conjunto es algo que tiene elementos, o es el conjunto vacío.

Definición 1. *y es un conjunto*

$$\leftrightarrow (\exists x)\ (x \in y \vee y = 0).$$

Como es de esperarse, la noción de conjunto se necesita a casa paso. Por ejemplo, la mayoría de las definiciones que vamos a introducir son condicionales, y se entiende intuitivamente que se aplican sólo a conjuntos. Para no tener que estar escribiendo continuamente el predicado 'es un conjunto', adoptaremos la siguiente convención en relación con las variables: las letras bastardillas mayúsculas 'A', 'B', 'C', etc., se usarán solamente para conjuntos. Las bastardillas minúsculas, 'x', 'y', 'z', etc., se pueden tomar como valores tanto de conjuntos como de individuos. (Llamaremos *variables generales* a estos últimos símbolos). Con esta convención bien presente, podemos omitir, sin confusión alguna, el predicado 'es un conjunto'.

La traducción de proposiciones que incluyen variables de conjuntos, a la notación básica de variables generales, es inmediata. Las tres reglas que se necesitan son muy simples; en lugar de dar un enunciado formal de ellas, ilustraremos su uso por medio de tres ejemplos: uno que se refiere a un cuantificador universal, otro a un cuantificador existencial y otro a un cuantificador de existencia y unicidad. La proposición:

$$(\forall A)(\exists x)-(x \in A)$$

se traduce:

$$(\forall y)(y \text{ es un conjunto} \rightarrow (\exists x)-(x \in y)),$$

y la proposición:

$$(\forall x)(\exists A)-(x \in A)$$

se traduce:

$$(\forall x)(\exists y)(y \text{ es un conjunto} \ \& -(x \in y)).$$

La proposición:

$$(\mathrm{E}!A)(\forall x)(x \in A)$$

se traduce:

$$(\mathrm{E}!y)(y \text{ es un conjunto} \ \& \ (\forall x)(x \in y)).$$

Debe notarse que la constante individual que denota el conjunto vacío se usa en el definiens de la definición 1. Se acostumbra en muchos desarrollos axiomáticos de la teoría de conjuntos definir el símbolo para el conjunto vacío, en lugar de introducirlo como un símbolo primitivo. Pero esto no es posible aquí, pues los axiomas están limitados a permitir individuos situados dentro del dominio del discurso. A este respecto seguimos la formulación original de la teoría de conjuntos de Zermelo, hecha en 1908. Sin embargo, nuestros axiomas no postulan realmente la existencia de individuo alguno y están por tanto acordes con el concepto de que sólo hay conjuntos en el dominio del discurso. Una definición usual de conjunto vacío es:

$$0 = x \leftrightarrow (\forall y)(y \notin x),$$

pero es fácil demostrar, con base en esta definición, que cualquier individuo es idéntico con el conjunto vacío, y esto efectivamente excluye los individuos.

Los dos axiomas que se consideran en esta sección son el *axioma de extensionalidad*

$$(\forall x)(x \in A \leftrightarrow x \in B) \rightarrow A = B$$

y el *esquema axiomático de separación*

$$(\exists B)(\forall x)(x \in B \leftrightarrow x \in A \;\&\; \varphi(x)).$$

Se entiende en el esquema axiomático de separación que la variable 'B' no es libre en $\varphi(x)$. Una formulación meta-matemática rigurosa de este esquema se dio en la sección anterior.* Para efectos de trabajo intuitivo sostendremos la forma que hemos acabado de usar, la cual es una mezcla del objeto lenguaje y del meta-lenguaje; pero el lector debe tener bien claro que éste es un esquema axiomático, no un axioma único. La restricción de que 'B' no sea libre en $\varphi(x)$ es esencial, pues sin ella podríamos deducir una contradicción, cuando quiera que A sea un conjunto no vacío. Para ver esto, sea $\varphi(x)$ la expresión '$-(x \in B)$' y sea A el conjunto que consiste en el conjunto vacío (la existencia de A se sigue de otros axiomas de este capítulo). Entonces tenemos:

$$(\exists B)(0 \in B \leftrightarrow 0 \in A \;\&\; -(0 \in B)),$$

lo cual, puesto que $0 \in A$, implica:

$$(\exists B)(0 \in B \leftrightarrow -(0 \in B)),$$

un absurdo. Por otra parte, es legítimo, y a veces necesario, que $\varphi(x)$ contenga otras variables libres y no simplemente 'x'; solamente 'B' está excluida.

Pasamos ahora a los desarrollos sistemáticos. Primero definimos la notación usual '$\notin$' para algo que no es elemento de algo.

Definición 2. $x \notin y \leftrightarrow -(x \in y)$.

Análogamente, usamos la notación de la lógica '$x \neq x$' para significar '$-(x = x)$'. Como primer teorema, tenemos:

Teorema 1. $x \notin 0$.

Demostración. Tomando $\varphi(x)$ como '$x \neq x$', se tiene, por el esquema axiomático de separación:

(1) $(\exists A)(\forall x)(x \in A \leftrightarrow x \in 0 \;\&\; x \neq x)$.

Supongamos ahora que algún x está en A; entonces, por (1), $x \neq x$, lo que es absurdo. Por tanto, concluimos:

(2) $(\forall x)(x \notin A)$,

y por consiguiente, por la definición 1,

(3) $A = 0$.

El teorema se sigue de (2) y (3). Q.E.D.

En seguida demostramos un teorema sencillo, relativo a la unicidad del conjunto vacío.

Teorema 2. $(\forall x)(x \notin A) \leftrightarrow A = 0$.

Demostración. Si $A = 0$, entonces, por el teorema 1, $x \notin A$. Por otra parte, si para todo x, $x \notin A$, entonces no hay elementos en el conjunto A y por la definición 1, $A = 0$. Q.E.D.

El resto de esta sección se relaciona con las nociones de inclusión e inclusión propia entre conjuntos. Si A y B son conjuntos tales que todo elemento de A es elemento de B, entonces decimos que *A está incluido en B*, o que *A es un subconjunto de B*, lo cual se simboliza: $A \subseteq B$. Así, podemos escribir:

El conjunto de los Irlandeses está contenido en el conjunto de los hombres

o:

* Es importante notar que, estrictamente hablando, la formulación con variables de conjuntos es más débil que la formulación meta-matemática con un solo tipo de variable, pues la primera expresa:

$$x \text{ es un conjunto} \longrightarrow (\exists y)(y \text{ es un conjunto } \& \;(\forall z)(z \in y \leftrightarrow z \in x \;\&\; \varphi(z))),$$

mientras que la versión meta-matemática inicial no tiene esta forma condicional. Por otra parte, no hay verdadero interés en que el axioma se aplique cuando x es un individuo.

El conjunto de los Irlandeses es un subconjunto del conjunto de los hombres

o sencillamente:

El conjunto de los Irlandeses $\subseteq$ el conjunto de los hombres.
Formalmente, tenemos:

Definición 3. $A \subseteq B \leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$.

Desde un punto de vista formal, la definición 3 es una definición condicional de un símbolo binario de relación. El hecho de que es una definición condicional está encubierto por el uso de letras mayúsculas, de la manera ya acordada. Esta misma observación se aplica a todas las definiciones en las cuales se usan variables de conjuntos.

Teorema 3. $A \subseteq A$.

Demostración. Puesto que es una verdad lógica que

$$(\forall x)(x \in A \rightarrow x \in A),$$

se sigue inmediatamente de la definición 3, que

$$A \subseteq A. \qquad \text{Q.E.D.}$$

El teorema 3 afirma sencillamente que la inclusión es reflexiva; el teorema siguiente afirma que tiene la propiedad de antisimetría, como suele llamarse.

Teorema 4 $A \subseteq B \;\&\; B \subseteq A \rightarrow A = B$.

Demostración. Si $A \subseteq B$ y $B \subseteq A$, entonces se sigue de la definición 3 que

$$(\forall x)(x \in A \leftrightarrow x \in B).$$

En consecuencia, por el axioma de extensionalidad, $A = B$. Q.E.D.

Teorema 5. $A \subseteq 0 \rightarrow A = 0$.

Demostración. En virtud de la definición 3 y de la hipótesis del teorema, si $x \in A$, entonces $x \in 0$. Pero por el teorema 1, $x \notin 0$. En consecuencia, para todo x, $x \notin A$ y por el teorema 2, $A = 0$. Q.E.D.

La transitividad de la inclusión se enuncia en el siguiente teorema.

Teorema 6. $A \subseteq B \;\&\; B \subseteq C \rightarrow A \subseteq C$.

Demostración. Considérese un elemento arbitrario x. Ya que $A \subseteq B$, si $x \in A$, entonces $x \in B$; pero $B \subseteq C$; en consecuencia, si $x \in B$, entonces, $x \in C$. Así, por la transitividad de implicación, si $x \in A$, entonces $x \in C$. Q.E.D.*

Aquí se ejemplifica un procedimiento típico usado en demostraciones informales. Necesitamos demostrar algo acerca de todos los elementos x. Para hacerlo es suficiente dar el argumento para un x arbitrario. El uso de la frase 'elemento arbitrario' corresponde, en el lenguaje de la lógica, a introducir una variable libre en una premisa (en este caso la premisa es $x \in A$).

Ahora definimos la *inclusión propia.*

Definición 4. $A \subset B \leftrightarrow A \subseteq B \;\&\; A \neq B$

Usando informalmente la notación de llaves, que no ha sido aún formalmente definida, tenemos:

$$\{1,2\} \subset \{1,2,3\}$$

pero no es el caso de que

$$\{1,2\} \subset \{1,2\}.$$

(Aquí describimos un conjunto escribiendo los nombres de sus elementos separados por comas, y encerramos el total con llaves). Los cuatro teoremas siguientes expresan propiedades que se espera sean cumplidas por la inclusión propia; las demostraciones se dejan como ejercicios.

Teorema 7. $-(A \subset A)$

Teorema 8. $A \subset B \rightarrow -(B \subset A)$

Teorema 9. $A \subset B \;\&\; B \subset C \rightarrow A \subset C$.

Teorema 10. $A \subset B \rightarrow A \subseteq B$.

EJERCICIOS

1. Demostrar los teoremas 7 a 10.
2. Formular la definición 4 como una definición condicional, sin usar variables de conjuntos 'A', 'B', etc.

* La "transitividad de implicación" significa precisamente que de $\mathbf{P} \rightarrow \mathbf{Q}$ y $\mathbf{Q} \rightarrow \mathbf{R}$ podemos inferir que $\mathbf{P} \rightarrow \mathbf{R}$.

3. Formular los teoremas 2 y 3 sin usar variables de conjuntos.

4. Dar una definición formal de la noción de individuo, siguiendo los lineamientos de la definición 1.

§ 2.3 Intersección, unión y diferencia entre conjuntos. Las propiedades elementales de las tres operaciones binarias básicas entre conjuntos constituyen el tema de esta sección. Usando de nuevo informalmente la notación de llaves para conjuntos, se pueden dar algunos ejemplos simples que ilustran esas operaciones. Si A y B son conjuntos, entonces se entiende por *intersección* entre A y B (en símbolos: $A \cap B$) el conjunto de todas las cosas que pertenecen tanto a A como a B. Así,

$$\{1,2\} \cap \{2,3\} = \{2\}$$

y

$$\{1\} \cap \{2\} = 0.$$

La *unión* entre A y B (en símbolos: $A \cup B$) significa el conjunto de todas las cosas que pertenecen por lo menos a uno de los conjuntos A y B. Por ejemplo,

$$\{1,2\} \cup \{2,3\} = \{1,2,3\}$$

y

$$\{1\} \cup \{2\} = \{1,2\}.$$

La *diferencia* entre A y B (en símbolos: $A \sim B$) significa el conjunto de todas las cosas que pertenecen a A pero no a B. Así,

$$\{1,2\} \sim \{2,3\} = \{1\}$$

y

$$\{1\} \sim \{2\} = \{1\}.$$

Los teoremas básicos que establecen la existencia de los conjuntos intersección y diferencia entre dos conjuntos se pueden demostrar usando el esquema axiomático de separación. No se puede decir lo mismo para la unión de dos conjuntos y por eso en este punto introducimos el *axioma de unión,* el cual más tarde demostraremos que es redundante, en términos del conjunto completo de axiomas introducidos en este capítulo:*

$$(\exists C)(\forall x)(x \in C \leftrightarrow x \in A \vee x \in B).$$

No usamos este axioma inmediatamente, sino que primero desarrollamos las propiedades de la operación intersección.

Teorema 11. $(E!C)(\forall x)(x \in C \leftrightarrow x \in A \;\&\; x \in B)$.

Demostración. El siguiente es un ejemplo del esquema axiomático de separación:

$$(\exists C)(\forall x)(x \in C \leftrightarrow x \in A \;\&\; x \in B).$$

Necesitamos ahora demostrar que C es único. Supongamos que hubiera un segundo conjunto, C', tal que, para todo x,

$$x \in C' \leftrightarrow x \in A \;\&\; x \in B;$$

entonces, para todo x,

$$x \in C' \leftrightarrow x \in C$$

y en virtud del axioma de extensionalidad,

$$C' = C. \qquad \text{Q.E.D.}$$

El teorema que se acaba de demostrar justifica formalmente la definición de intersección.

Definición 5. $A \cap B = y \leftrightarrow (\forall x)(x \in y \leftrightarrow x \in A \;\&\; x \in B) \;\&\; y$ es un conjunto.

Corrientemente, la tendencia natural es escribir, en lugar de la definición 5, la fórmula

(1) $A \cap B = C \leftrightarrow (\forall x)(x \in C \leftrightarrow x \in A \;\&\; x \in B)$,

pero (1) no se traduce en variables generales de manera satisfactoria, pues se transforma en:

(2) x,y,z son conjuntos $\rightarrow (x \cap y = z \leftrightarrow (\forall w)\,(w \in z \leftrightarrow w \in x \;\&\; w \in y))$,

y las razones para prevenir la aparición libre de 'z' en la hipótesis de (2) son obvias; pues si aparece, no podemos demostrar, por ejemplo, que $0 \cap 0 \neq z$ para cualquier individuo z. Nótese que la regla para las definiciones condicionales, dada en la sección precedente, prohibió tal aparición libre de 'z'.

Si las reglas dadas al comienzo de este capítulo hubieran sido más liberales, habríamos podido adoptar como definición de intersección el teorema siguiente, que tiene la virtud de facilitar mucho las demostracio-

*El axioma de suma introducido luego en § 2.6 se llama a veces axioma de unión. El presente axioma, que es redundante, no debe confundirse con él.

nes; pero la liberalización de dichas reglas no es aconsejable porque la no creatividad de las definiciones llega a ser mucho menos obvia y en muchos casos dificulta la demostración.

Teorema 12. $x \in A \cap B \leftrightarrow x \in A \;\&\; x \in B$.

Demostración. Usando la identidad:

$$A \cap B = A \cap B$$

y cambiando '$A \cap B$' por 'z' en la definición 5, obtenemos el teorema de una vez. Q.E.D.

Los dos teoremas siguientes establecen la conmutatividad y la asociatividad de la intersección. Las demostraciones se dejan como ejercicios.

Teorema 13. $A \cap B = B \cap A$.

Teorema 14. $(A \cap B) \cap C = A \cap (B \cap C)$.

Una operación binaria es idempotente si, cuando se efectúa entre un elemento y él mismo, el resultado es precisamente tal elemento. El teorema siguiente establece la idempotencia de la intersección.

Teorema 15. $A \cap A = A$.

Demostración. Por el teorema 12,

$$x \in A \cap A \leftrightarrow x \in A \;\&\; x \in A,$$

pero

$$x \in A \;\&\; x \in A \leftrightarrow x \in A,$$

así, por la definición 5,

$$A \cap A = A. \qquad \text{Q.E.D.}$$

En seguida se formulan tres teoremas intuitivamente obvios; sólo se demuestra el primero.

Teorema 16. $A \cap 0 = 0$.

Demostración. En virtud del teorema 12,

$$x \in A \cap 0 \leftrightarrow x \in A \;\&\; x \in 0,$$

pero, por el teorema 1,

$$x \notin 0.$$

En consecuencia,

$$x \notin A \cap 0,$$

y puesto que el argumento vale para todo x, por el teorema 2,

$$A \cap 0 = 0. \qquad \text{Q.E.D.}$$

Teorema 17. $A \cap B \subseteq A$.

Teorema 18. $A \subseteq B \leftrightarrow A \cap B = A$.

Ahora nos referimos al teorema que justifica la operación de unión entre conjuntos. La demostración de este teorema requiere el uso del axioma de unión, por primera vez.

Teorema 19. $(\mathrm{E}!C)(\forall x)(x \in C \leftrightarrow x \in A \vee x \in B)$.

Demostración. Semejante a la demostración del teorema 11, pero usando el axioma de unión en lugar del esquema axiomático de separación.

Definición 6. $A \cup B = y \leftrightarrow (\forall x)(x \in y \leftrightarrow x \in A \vee x \in B) \;\&\; y$ es un conjunto.

Para trabajar necesitamos inmediatamente un teorema para la operación de unión, análogo al teorema 12.

Teorema 20. $x \in A \cup B \leftrightarrow x \in A \vee x \in B$.

Demostración. Semejante a la demostración del teorema 12.

Ya que muchas de las demostraciones de los teoremas concernientes a la unión entre conjuntos son paralelas a las que se refieren a la intersección, podemos descartarlas frecuentemente, haciendo referencia al teorema correspondiente para la intersección, como hemos hecho con las demostraciones de los teoremas 19 y 20.

Los tres teoremas siguientes establecen la conmutatividad, la asociatividad y la idempotencia de la unión.

Teorema 21. $A \cup B = B \cup A$.

Teorema 22. $(A \cup B) \cup C = A \cup (B \cup C)$.

Teorema 23. $A \cup A = A$.

En los cuatro teoremas siguientes se establecen otros hechos.

Teorema 24. $A \cup 0 = A$.

Teorema 25. $A \subseteq A \cup B$.

Teorema 26. $A \subseteq B \leftrightarrow A \cup B = B$.

Teorema 27. $A \subseteq C \;\&\; B \subseteq C \rightarrow A \cup B \subseteq C$.

Ahora establecemos dos leyes distributivas fundamentales para la intersección y la unión; demostraremos la primera.

Teorema 28. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

Demostración. Sea x un elemento arbitrario. En virtud del teorema 12,

$$x \in (A \cup B) \cap C \leftrightarrow x \in A \cup B \;\&\; x \in C,$$

y por el teorema 20,

$$x \in A \cup B \;\&\; x \in C \leftrightarrow (x \in A \vee x \in B) \;\&\; x \in C,$$

y por las leyes distributivas de la lógica proposicional,*

$$(x \in A \vee x \in B) \;\&\; x \in C \leftrightarrow (x \in A \;\&\; x \in C) \vee x \in B \;\&\; x \in C).$$

Usando de nuevo el teorema 12,

$$(x \in A \;\&\; x \in C) \vee (x \in B \;\&\; x \in C) \leftrightarrow x \in A \cap C \vee x \in B \cap C.$$

Usando de nuevo el teorema 20,

$$x \in A \cap C \vee x \in B \cap C \leftrightarrow x \in (A \cap C) \cup (B \cap C).$$

De la transitividad y de la equivalencia inferimos:

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

finalmente, por el axioma de extensionalidad,

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C). \quad \text{Q.E.D.}$$

En la demostración del teorema 28 se ha empleado un artificio que se usa repetidas veces. Para demostrar que dos conjuntos son idénticos, comenzamos por considerar un elemento arbitrario de uno de los conjuntos y demostramos que pertenece a este conjunto si y sólo si pertenece al otro. Usando el axioma de extensionalidad, obtenemos inmediatamente la identidad de los dos conjuntos.

Teorema 29. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

En seguida enunciamos el teorema justificante y la definición de la operación de diferencia entre conjuntos.

* La ley en cuestión consiste en que de (**P** v **Q**) & **R** podemos inferir (**P** & **R**) v (**Q** & **R**) y recíprocamente, donde **P**, **Q**, y **R** son fórmulas cualesquiera.

Teorema 30. $(E!C)(\forall x)(x \in C \leftrightarrow x \in A \;\&\; x \notin B)$.

Demostración. Semejante a la del teorema 11, pero tomando aquí $\varphi(x)$ como '$x \notin B$'.

Definición 7. $A \sim B = y \leftrightarrow (\forall x)(x \in y \leftrightarrow x \in A \;\&\; x \notin B) \;\&\; y$ es un conjunto.

Teorema 31. $x \in A \sim B \leftrightarrow x \in A \;\&\; x \notin B$.

Demostración. Semejante a la del teorema 12.

El teorema siguiente asegura obviamente el hecho de que la diferencia entre conjuntos no es idempotente, supuesta la existencia de conjuntos no vacíos.

Teorema 32. $A \sim A = 0$.

Demostración. Por el teorema 1,

$$x \notin 0.$$

Por la lógica proposicional,

$$x \in 0 \leftrightarrow x \in A \;\&\; x \notin A,$$

finalmente, por la definición 7,

$$A \sim A = 0. \qquad \text{Q.E.D.}$$

Los teoremas restantes de esta sección establecen hechos relativos a las operaciones de intersección, unión y diferencia entre conjuntos. Las demostraciones de los teoremas se obtienen fácilmente siguiendo un método parecido al que se usó para el teorema 28. Como con ese teorema, las demostraciones dependen del aprovechamiento de propiedades formales de las conectivas proposicionales, análogas a las propiedades formales enunciadas en los teoremas. Aquí se da solamente la demostración del primero de esos teoremas.

Teorema 33. $A \sim (A \cap B) = A \sim B$.

Demostración. Sea x un elemento arbitrario. Entonces,

$$x \in A \sim (A \cap B) \leftrightarrow x \in A \;\&\; -(x \in A \cap B)$$

por el teorema 31

$$\leftrightarrow x \in A \;\&\; -(x \in A \;\&\; x \in B)$$

por el teorema 12

$$\leftrightarrow x \in A \;\&\; (x \notin A \vee x \notin B)$$

Por lógica proposicional

$\leftrightarrow (x \in A \ \& \ x \notin A) \vee (x \in A \ \& \ x \notin B)$

Por lógica proposicional

$\leftrightarrow x \in A \ \& \ x \notin B$ Por lógica proposicional

Q.E.D.

Se ha adoptado aquí un estilo staccato, que consiste en exhibir una serie de equivalencias y que es semejante al usado frecuentemente para una cadena de identidades. Algunos lectores pueden hallar más claro este método de presentación que el más prolijo que se usó en la demostración del teorema 28.

Teorema 34. $A \cap (A \sim B) = A \sim B$.

Teorema 35. $(A \sim B) \cup B = A \cup B$.

Teorema 36. $(A \cup B) \sim B = A \sim B$.

Teorema 37. $(A \cap B) \sim B = 0$.

Teorema 38. $(A \sim B) \cap B = 0$.

Teorema 39. $A \sim (B \cup C) = (A \sim B) \cap (A \sim C)$.

Teorema 40. $A \sim (B \cap C) = (A \sim B) \cup (A \sim C)$.

En la teoría de conjuntos de von Neumann, el universo V, que es la clase de todos los conjuntos, existe. El complemento $\sim A$ de un conjunto A puede definirse como

$$\sim A = V \sim A.$$

Pero esto no es posible en la teoría de conjuntos de Zermelo-Fraenkel y puede ser de interés ver con algún detalle por qué no. Análogamente a los teoremas justificantes de las definiciones de las tres operaciones ya consideradas, necesitaríamos demostrar:

(1) $(E!B)(\forall x)(x \in B \leftrightarrow x \notin A)$

y entonces definiríamos la complementación así:

(2) $\sim A = y \leftrightarrow (\forall x)(x \in y \leftrightarrow x \notin A)$ $\& \ y$ es un conjunto.

Supongamos ahora que fuera posible demostrar (1). Sea $A = 0$; entonces,

(3) $(E!B)(\forall x)(x \in B)$,

esto es, B es el conjunto universal al cual todo objeto pertenece; pero con B a la mano, el esquema axiomático de separación se reduce al esquema axiomático de abstracción tomando A como el conjunto universal B, y se puede deducir la paradoja de Russell como en § 1.3. Concluimos que (1) no puede demostrarse y la definición (2) es imposible en la teoría de conjuntos de Zermelo-Fraenkel. Se puede formalizar un aspecto de esta discusión, en el útil resultado de que no existe un conjunto universal. Como se acaba de indicar, la demostración de este teorema sigue el método de argumentación de la paradoja de Russell, por una *reductio ad absurdum.*

Teorema 41. $-(\exists A)(\forall x)(x \in A)$.

EJERCICIOS

1. Demostrar los teoremas 13 y 14.
2. Demostrar los teoremas 17 y 18.
3. Demostrar los teoremas 21, 22 y 23.
4. Demostrar los teoremas 24, 25, 26 y 27.
5. ¿Puede darse un ejemplo de una operación de la aritmética ordinaria que sea idempotente?
6. Demostrar el teorema 29.
7. Demostrar los teoremas 34, 35 y 36.
8. Demostrar los teoremas 37 y 38.
9. Demostrar los teoremas 39 y 40.
10. Dar una demostración detallada del teorema 41.
11. Hallar una identidad que sirva luego como definición de intersección en términos de diferencia.
12. Definamos la operación de *diferencia simétrica* por medio de la identidad:

$$A \div B = (A \sim B) \cup (B \sim A).$$

Demostrar:

(a) $A \div 0 = A$
(b) $A \div B = B \div A$
(c) $(A \div B) \div C = A \div (B \div C)$
(d) $A \cap (B \div C) = (A \cap B) \div (A \cap C)$
(e) $A \sim B \subseteq A \div B$
(f) $A = B \leftrightarrow A \div B = 0$
(g) $A \div C = B \div C \rightarrow A = B$
(h) Hallar una identidad que sirva luego como definición de diferencia, en términos de diferencia simétrica e intersección.

§ **2.4 Axioma de apareamiento y parejas ordenadas.** Los tres axiomas considerados hasta ahora nos permiten demostrar la existencia de solamente un conjunto: el conjunto vacío. Ahora introducimos un axioma que establece que, dados dos elementos cualesquiera, esto es, dos conjuntos o individuos cualesquiera, podemos formar el conjunto que consta de esos dos elementos. Este axioma se llama usualmente el *axioma de apareamiento:*

$$(\exists A)(\forall z)(z \in A \leftrightarrow z = x \vee z = y).$$

Si quisiéramos hacer del axioma de unión una parte más integrante de nuestro sistema, podríamos reemplazar el axioma de apareamiento por un axioma más débil, según el cual el conjunto unitario consistente en cualquier elemento, existe. El axioma de apareamiento se sigue de considerar la unión de dos conjuntos unitarios. Sin embargo, como ya se ha observado al final del capítulo 1, queremos demostrar hacia el final de este capítulo que el axioma de unión se puede deducir del axioma de apareamiento y del axioma de suma, el cual no ha sido introducido aún.

Para preparar la definición de conjuntos de dos elementos tenemos el refuerzo usual del axioma, como se expresa en el siguiente teorema.

Teorema 42. $(E!A)(\forall z)(z \in A \leftrightarrow z = x \vee z = y)$.

Demostración. Semejante a la del teorema 11.

Definición 8. $\{x,y\} = w \leftrightarrow (\forall z)(z \in w \leftrightarrow z = x \vee z = y)$ & w es un conjunto.

Ahora se tiene el teorema de costumbre.

Teorema 43. $z \in \{x,y\} \leftrightarrow z = x \vee z = y$.

Demostración. Semejante a la del teorema 12.

Un teorema menos trivial pero también útil sobre parejas no ordenadas es el siguiente.

Teorema 44. $\{x,y\} = \{u,v\} \rightarrow (x = u \,\&\, y = v) \vee (x = v \,\&\, y = u)$.

Demostración. En virtud del teorema 43,

$$u \in \{u,v\}.$$

Por la hipótesis del teorema,

$$u \in \{x,y\}.$$

En virtud del teorema 43, de nuevo,

(1) $u = x \vee u = y$.

Con argumentos semejantes,

(2) $v = x \vee v = y$,

(3) $x = u \vee x = v$,

(4) $y = u \vee y = v$.

Ahora podemos considerar dos casos.

Caso 1. $x = y$. Entonces, en virtud de (1), $x = u$ y en virtud de (2), $y = v$.

Caso 2. $x \neq y$. En vista de (1), o $x = u$, o bien, $y = u$. Supongamos $x \neq u$. Entonces, $y = u$; por (3), $x = v$. Por otra parte, supongamos $y \neq u$. Entonces, $x = u$ y por (4), $y = v$. Q.E.D.

Conviene, para uso subsiguiente, definir conjuntos unitarios, ternas y cuaternas. Es evidente la naturalidad de las definiciones.

Definición 9. $\{x\} = \{x,x\}$

$$\{x,y,z\} = \{x,y\} \cup \{z\}$$

$$\{x,y,z,w\} = \{x,y\} \cup \{z,w\}.$$

Como corolario inmediato del teorema 44, tenemos un teorema intuitivamente obvio, con respecto a los conjuntos unitarios. La demostración se deja como ejercicio.

Teorema 45. $\{x\} = \{y\} \rightarrow x = y$.

Ahora estamos en situación de definir parejas ordenadas en términos de conjuntos unitarios y duplas no ordenadas. Esta definición fue históricamente importante para reducir la teoría de relaciones a la teoría de conjuntos y se debe a Kuratowski (1921); pero la primera definición que permitió esta reducción se encuentra en Wiener (1914).

Definición 10. $\langle x,y \rangle = \{\{x\}, \{x,y\}\}$.

Dentro de la teoría de conjuntos, como veremos en el capítulo siguiente, las relaciones se definen como conjuntos de parejas ordenadas. Sin algo a mano, como la presente definición, es imposible desarrollar la teoría de relaciones, a menos que la noción de pareja ordenada se tome como primitiva. Esencialmente, nuestra única intuición acerca de una pareja ordenada es que es una entidad que representa dos objetos en un orden dado. El siguiente teorema establece que la definición 10 es adecuada con respecto a esta idea; a saber, dos parejas ordenadas son idénticas solamente cuando el primer elemento de una es idéntico con el primer elemento de la otra y en forma semejante para los segundos elementos.

Teorema 46. $\langle x,y \rangle = \langle u,v \rangle \rightarrow x = u \,\&\, y = v.$

Demostración. En virtud de la definición 10 y de la hipótesis del teorema,

$$\{\{x\}, \{x,y\}\} = \{\{u\}, \{u,v\}\}.$$

Por el teorema 44,

$$(1)\ (\{x\} = \{u\} \,\&\, \{x,y\} = \{u,v\}) \vee (\{x\} = \{u,v\} \,\&\, \{x,y\} = \{u\}).$$

Supongamos que subsiste la primera alternativa de (1). Entonces, ya que

$$\{x\} = \{u\},$$

por el teorema 45

$$x = u,$$

y por el teorema 44 y la suposición de que $\{x,y\} = \{u,v\}$

$$y = v,$$

que establece el resultado pedido.

Supongamos ahora que subsiste la segunda alternativa de (1). Entonces, puesto que $\{x\} = \{x,x\}$, por el teorema 44,

$$x = u \,\&\, x = v,$$

y en forma similar,

$$x = u \,\&\, y = u.$$

Por consiguiente,

$$x = u \,\&\, y = v. \qquad \text{Q.E.D.}$$

Las parejas ordenadas desempeñan un papel muy importante en la sección de este capítulo que trata de productos cartesianos y en el capítulo siguiente que trata de relaciones y funciones.

EJERCICIOS

1. Demostrar el teorema 45.
2. Demostrar que
$$x = y \rightarrow \langle x,y \rangle = \{\{x\}\}.$$
3. ¿Es siempre verdadero que si $\{x,y,z\} = \{x,y,w\}$, entonces $z = w$?
4. Demostrar, usando la demostración de un teorema como el 46, que es adecuada la siguiente definición de parejas ordenadas:
$$\langle x,y \rangle = \{\{x,0\}, \{y, \{0\}\}\}.$$

§ **2.5 Definición por abstracción.** En muchas ramas de la matemática moderna se acostumbra usar la notación:

$$\{x\colon \varphi(x)\}$$

para designar el conjunto de todos los objetos que tienen la propiedad φ. Por ejemplo,

$$\{x\colon x > \sqrt{2}\}$$

es el conjunto de todos los números reales mayores que $\sqrt{2}$; como otro ejemplo,

$$\{x\colon 1 < x < 4 \,\&\, x \text{ es un entero}\} = \{2,3\}.$$

Debemos aclarar por qué el uso de esta notación se llama *definición por abstracción*. Comenzamos por considerar alguna propiedad, tal como ser mayor de $\sqrt{2}$ y abstraemos de esta propiedad el *conjunto* de todas las entidades que tienen la propiedad.

Nuestro objetivo es dar una definición formal de esta operación de abstracción, pero debe observarse que para definirla no estamos introduciendo un nuevo símbolo de relación, ni de operación, ni de constante individual. Lo que estamos introduciendo es un operador que proporciona un nuevo método de ligar variables. Así en la expresión

$$\{x\colon x > \sqrt{2}\}$$

la notación

$$\{-\colon -\}$$

liga la variable 'x'.

Esquema de definición 11.

$\{x: \varphi(x)\} = y \leftrightarrow [(\forall x)(x \in y \leftrightarrow \varphi(x))$ & y es un conjunto$] \vee [y = 0$ & $-(\exists B)(\forall x)(x \in B \leftrightarrow \varphi(x))]$.

De la definición se desprende claramente que $\{x: \varphi(x)\}$ es un conjunto. El quid del segundo miembro de la disyunción del definiens es hacer $\{x: \varphi(x)\}$ igual al conjunto vacío, si no hay conjunto no vacío que tenga como elementos precisamente aquellas entidades con la propiedad φ. La manera de traducir las fórmulas en las cuales las variables de conjuntos están ligadas por abstracción es inmediata. Así, la fórmula esquemática

$$\{A: \varphi(A)\}$$

se traduce,

$$\{x: x \text{ es un conjunto } \& \ \varphi(x)\}.$$

Hay muchos esquemas teoremáticos intuitivamente obvios, acerca de la operación abstracción, algunos de los cuales formulamos y demostramos en seguida.

Esquema teoremático 47. $y \in \{x: \varphi(x)\} \rightarrow \varphi(y)$.

Demostración. Si $y \in \{x: \varphi(x)\}$, entonces

$$\{x: \varphi(x)\} \neq 0,$$

y, por el esquema de definición 11,

$$y \in \{x: \varphi(x)\} \leftrightarrow \varphi(y);$$

podemos concluir, a partir de la hipótesis del teorema, $\varphi(y)$. Q.E.D.

Teorema 48. $A = \{x: x \in A\}$.

Demostración. Es una verdad lógica que

$$(\forall x)(x \in A \leftrightarrow x \in A).$$

Así que, tomando $\varphi(x)$ en la definición 11 como '$x \in A$', obtenemos el teorema directamente. Q.E.D.

Teorema 49. $0 = \{x: x \neq x\}$.

Demostración. Supongamos que hubiera un y tal que

$$y \in \{x: x \neq x\}.$$

Entonces, por el teorema 47,

(1) $\qquad y \neq y,$

lo que es absurdo. Q.E.D.

Semejante al teorema 41, tenemos también:

Teorema 50. $0 = \{x: x = x\}$.

Podemos demostrar como teoremas, fórmulas sencillas que podrían usarse para definir intersección, unión y diferencia entre conjuntos.

Teorema 51. $A \cap B = \{x: x \in A \ \& \ x \in B\}$.

Demostración. Usese el teorema 11 y la definición 11.

Teorema 52. $A \cup B = \{x: x \in A \vee x \in B\}$.

Teorema 53. $A \sim B = \{x: x \in A \ \& \ x \notin B\}$.

Un punto de interés metodológico es que, si estos tres últimos teoremas se usan como definiciones de las tres operaciones, no se requiere teorema justificante previo a la definición. (Nótese que no se exige tal teorema en la regla para definir símbolos de operación por identidades en § 2.1.) Por la definición 11 sabemos que si el conjunto de elementos intuitivamente apropiados no existe, entonces el resultado de efectuar la operación es el conjunto vacío. Sin embargo, para hacer un trabajo serio con las operaciones, necesitamos la existencia del conjunto intuitivamente apropiado, lo cual, en otras palabras, significa que los teoremas justificantes vienen *después* en lugar de antes de la definición. Esto se ilustra más adelante en § 2.7. Las definiciones que no necesitan un teorema justificante se llaman frecuentemente *libres de axioma.*

En lo que sigue, es conveniente tener una forma de definición por abstracción, más flexible que la proporcionada por la definición 11. En particular, queremos estar en posibilidad de poner términos complicados antes de los dos puntos en lugar de variables singulares, simplemente. Por ejemplo, en § 2.8

definimos el producto cartesiano entre dos conjuntos por medio de:

(1) $A \times B = \{\langle x,y\rangle : x \in A \;\&\; y \in B\}$,

pero sobre la base de la definición 11 necesitamos reemplazar (1) por la expresión más complicada:

$$A \times B = \{x: (\exists y)(\exists z)(y \in A \;\&\; z \in B \;\&\; x = \langle y,z\rangle)\}.$$

En el estilo de la definición 11, tenemos:

Esquema de definición 12.

$$\{\tau(x_1, \ldots ,x_n) : \varphi(x_1, \ldots ,x_n)\} = \{y:(\exists x_1) \ldots (\exists x_n)(y = \tau(x_1, \ldots ,x_n) \;\&\; \varphi(x_1, \ldots ,x_n))\}.$$

Es evidente que los esquemas de definición 11 y 12 difieren de las otras definiciones introducidas antes, en que estos dos son esquemas que deberían tener una formulación meta-matemática. Por ejemplo, la definición 12 podría darse en la forma siguiente:

Si (i) $\mathbf{v}_1, \ldots ,\mathbf{v}_n, \mathbf{w}$ *son variables diferentes cualesquiera,* (ii) $\tau(\mathbf{v}_1, \ldots ,\mathbf{v}_n)$ *es cualquier término en el cual no aparecen variables ligadas y aparecen libres exactamente* $\mathbf{v}_1, \ldots ,\mathbf{v}_n$, *y* (iii) ω *no aparece en la fórmula* φ, *entonces es válida la identidad*

$$\{\tau(\mathbf{v}_1, \ldots ,\mathbf{v}_n) : \varphi\} = \{\mathbf{w}: (\exists \mathbf{v}_1) \ldots (\exists \mathbf{v}_n)\,(\mathbf{w} = \tau(\mathbf{v}_1, \ldots ,\mathbf{v}_n) \;\&\; \varphi)\}.$$

Las cláusulas (i) a (iii) aclaran las restricciones impuestas a la definición 12. Realmente no es necesario exigir que τ no tenga variables ligadas y en algunos contextos ello podría ser inconveniente, aunque no se presentan tales casos en este libro. Cuando se use la definición 11 o la 12, nos referiremos a ellas usualmente, diciendo *definición por abstracción,* en lugar de usar los números que les están asignados. Cerramos esta sección con un esquema teoremático que expresa la importante idea de que las propiedades equivalentes son extensionalmente idénticas. La demostración se deja como ejercicio.

Esquema teoremático 54. $(\forall x)(\varphi(x) \leftrightarrow \Psi(x)) \rightarrow \{x: \varphi(x)\} = \{x: \Psi(x)\}$.

EJERCICIOS

1. Para efectos de completa claridad, el esquema de definición 11 debería estar precedido por el siguiente teorema:

$$(\mathrm{E}!y)[((\forall x)\,(x \in y \leftrightarrow \varphi(x)) \;\&\; y \text{ is a set}) \vee (y = 0 \;\&\; -(\exists B)(\forall x)(x \in B \leftrightarrow \varphi(x)))].$$

2. ¿Por qué en el teorema 47 no se puede reemplazar el signo de implicación por uno de equivalencia, $\leftrightarrow$?
3. Demostrar el teorema 50.
4. Dar una demostración detallada del teorema 51.
5. Demostrar los teoremas 52 y 53.
6. Definir por abstracción el conjunto no ordenado de dos elementos.
7. Demostrar el teorema 54.
8. Dar un contra-ejemplo del siguiente:

$$(\forall x)(\varphi(x) \rightarrow \Psi(x)) \rightarrow \{x: \varphi(x)\} \subseteq \{x: \Psi(x)\}.$$

9. Los teoremas 49 y 50 sugieren el siguiente principio:

$$(\forall x)(\varphi(x) \leftrightarrow -\Psi(x)) \rightarrow \{x: \varphi(x)\} = \{x: \Psi(x)\}.$$

Si es verdadero, demostrarlo; si no, dar un contra-ejemplo.

§ 2.6 Axioma de suma y familias de conjuntos. El axioma de suma, que es la base de esta sección, postula la existencia de la unión de una familia de conjuntos.* Para ilustrar la notación, sea

$$A = \{\{1,2\}, \{2,3\}, \{4\}, \text{Jane Austen}\}.$$

Entonces,

$$\bigcup A = \{1,2,3,4\}.$$

Aquí, A es una familia de conjuntos, junto con un individuo. La *unión* o *suma* de A (en símbolos $\bigcup A$) es el conjunto de todas las cosas que pertenecen a algún elemento de A. Nótese que cualquier individuo contenido en A está fuera de $\bigcup A$. Para determinar $\bigcup A$ necesitamos considerar solamente aquellos elementos de A que son conjuntos no vacíos.

La definición formal usa la notación de abstracción introducida en la sección precedente.

Definición 13. $\bigcup A = \{x: (\exists B)(x \in B \;\&\; B \in A)\}$.

Sabemos, por las características de la defini-

* La palabra 'familia' es un sinónimo común para 'conjunto'; las expresiones *familia de conjuntos* y *conjunto de conjuntos* se usan indistintamente.

ción por abstracción, que si el conjunto apropiado de elementos no existe, entonces $\bigcup A$ es simplemente el conjunto vacío. Sin embargo, para cualquier trabajo serio con la unión de una familia de conjuntos, necesitamos la existencia de un conjunto intuitivamente apropiado. Para este fin introducimos el *axioma de suma:*

$$(\exists C)(\forall x)(x \in C \leftrightarrow (\exists B)(x \in B \ \& \ B \in A)).$$

Tenemos, de una vez, como una consecuencia del axioma y de la definición de $\bigcup A$, el teorema deseado:

Teorema 55. $x \in \bigcup A \leftrightarrow (\exists B)(x \in B \ \& \ B \in A)$.

Las propiedades elementales más obvias de la operación $\bigcup$ se establecen en los siguientes teoremas. Algunas de las demostraciones se dejan como ejercicios.

Teorema 56. $\bigcup 0 = 0$.

Demostración. Por el teorema 1,

$$-(\exists B)(B \in 0).$$

Por consiguiente, por el teorema 55, para todo x,

$$x \notin \bigcup 0. \qquad \text{Q.E.D.}$$

Teorema 57. $\bigcup \{0\} = 0$.

Demostración. Si $B \in \{0\}$, entonces

$$B = 0$$

y entonces

$$x \notin B.$$

En consecuencia, por el teorema 55, para todo x,

$$x \notin \bigcup \{0\}. \qquad \text{Q.E.D.}$$

Si se hubiera postulado que no hubiese individuos, esto es, que todo objeto es un conjunto, podríamos demostrar que, si $\bigcup A = 0$, entonces, o bien $A = 0$, o bien $A = \{0\}$. Así, las sumas de muchos conjuntos diferentes pueden ser vacías; en verdad, la suma de cualquier conjunto cuyos elementos son únicamente individuos y el conjunto vacío.

Teorema 58. $\bigcup \{A\} = A$.

Teorema 59. $\bigcup \{A, B\} = A \cup B$.

Demostración. En virtud de la propiedad fundamental de duplas no ordenadas, si $C \in \{A, B\}$, entonces

$$C = A \vee C = B.$$

Por el teorema 55,

$$(1) \quad x \in \bigcup \{A, B\} \leftrightarrow x \in A \vee x \in B,$$

y la inferencia deseada es obvia, a partir de (1). Q.E.D.

Teorema 60. $\bigcup (A \cup B) = (\bigcup A) \cup (\bigcup B)$.

Demostración.

$$x \in \bigcup (A \cup B) \leftrightarrow (\exists C)(x \in C \ \& \ C \in A \cup B).$$

Por el teorema 55

$$\leftrightarrow (\exists C)((x \in C \ \& \ C \in A) \vee (x \in C \ \& \ C \in B)).$$

Por el teorema 20 y la lógica proposicional.

$$\leftrightarrow (\exists C)(x \in C \ \& \ C \in A) \vee (\exists C)(x \in C \ \& \ C \in B).$$

Por la lógica cuantificacional *

$$\leftrightarrow x \in \bigcup A \vee x \in \bigcup B$$

por el teorema 55

$$\leftrightarrow x \in \bigcup A \cup \bigcup B$$

por el teorema 20

Q.E.D.

Teorema 61. $A \subseteq B \rightarrow \bigcup A \subseteq \bigcup B$.

Demostración.

$$x \in \bigcup A \leftrightarrow (\exists C)(x \in C \ \& \ C \in A)$$

por el teorema 55,

$$\rightarrow (\exists C)(x \in C \ \& \ C \in B)$$

por la hipótesis del teorema,

$$\rightarrow x \in \bigcup B \qquad \text{por el teorema 55,}$$

Q.E.D.

Teorema 62. $A \in B \rightarrow A \subseteq \bigcup B$.

*Claramente, de $(\exists v)(P \vee Q)$ podemos inferir $(\exists v)P \vee (\exists v)Q$, y recíprocamente.

Teorema 63. $(\forall A)(A \in B \rightarrow A \subseteq C) \rightarrow \bigcup B \subseteq C$.

Teorema 64. $(\forall A)(A \in B \rightarrow A \cap C = 0) \rightarrow (\bigcup B) \cap C = 0$.

Teorema 65. $\bigcup \langle x,y \rangle = \{x,y\}$.

Demostración.

$\bigcup \langle x,y \rangle = \bigcup \{\{x\},\{x,y\}\}$
por definición de parejas ordenadas

$= \{x\} \cup \{x,y\}$
por el teorema 59,

$= \{x,y\}$ Q.E.D.

Teorema 66. $\bigcup \bigcup \langle A,B \rangle = A \cup B$.

Nos referimos ahora a la definición y propiedades de la *intersección* de una familia de conjuntos. El contenido intuitivo de esta noción debe ser claro, a partir de las discusiones de la unión. Si, como antes,

$$A = \{\{1,2\}, \{2,3\}, \{4\}, \text{Jane Austen}\},$$

entonces

$$\bigcap A = 0,$$

puesto que no hay ningún número común a todos los conjuntos que son elementos de A. Como un segundo ejemplo, si

$$B = \{\{1,2\}, \{2,3\}\},$$

entonces

$$\bigcap B = \{1,2\} \cap \{2,3\} = \{2\}.$$

Los desarrollos formales que siguen requieren un pequeño comentario.

Definición 14. $\bigcap A = \{x: (\forall B)(B \in A \rightarrow x \in B)\}$.

No hay ningún teorema relacionado con la definición 14 de la misma manera que el teorema 55 lo está con la definición 13, o sea que no podemos demostrar:

(1) $x \in \bigcap A \leftrightarrow (\forall B)(B \in A \rightarrow x \in B)$,

y la razón es obvia. Si A no tiene conjuntos como elementos, entonces el miembro de la derecha de (1) es siempre verdadero y todo x debe ser un elemento de $\bigcap A$. Pero no hay conjunto alguno que tenga toda entidad x como elemento, hecho que se establece por el teorema 41. Lo que estamos en capacidad de demostrar es el resultado más restringido:

Teorema 67. $x \in \bigcap A \leftrightarrow (\forall B)(B \in A \rightarrow x \in B)$ & $(\exists B)(B \in A)$.

Demostración. [Necesidad]. Por hipótesis, $x \in \bigcap A$. Por consiguiente, $\bigcap A \neq 0$. Así que, en virtud de la definición 14 y de las propiedades generales de la definición por abstracción, inferimos que

(1) $x \in \bigcap A \leftrightarrow (\forall B)(B \in A \rightarrow x \in B)$.

Hagamos ahora la suposición de que

(2) $-(\exists B)(B \in A)$.

Entonces es verdadero vacíamente que

$$(\forall B)(B \in A \rightarrow x \in B),$$

de lo cual podemos inferir

(3) $(\forall B)(B \in A \rightarrow x \in B) \leftrightarrow x = x$.

Las equivalencias (1) y (3) permiten decir que, para todo x,

$$x \in \bigcap A \leftrightarrow x = x,$$

en consecuencia, por el teorema 54,

$$\{x: x \in \bigcap A\} = \{x: x = x\},$$

pero en virtud del teorema 48, el miembro de la izquierda es $\bigcap A$ y por el teorema 50, el miembro de la derecha es el conjunto vacío; de modo que inferimos,

$$\bigcap A = 0$$

lo que contradice la hipótesis según la cual $x \in \bigcap A$ y demuestra que nuestra suposición (2) es falsa.

[Suficiencia]. Por hipótesis, existe un conjunto, digamos B^*, que es un elemento de A. Entonces, podemos aplicar el esquema axiomático de separación para obtener:

$$(4) \qquad (\exists C)(\forall x)(x \in C \leftrightarrow x \in B^* \ \& \ (\forall B)(B \in A \rightarrow x \in B)).$$

Y por el hecho de que $x \in B^*$ se sigue de $B^* \in A$, y la otra parte de nuestra hipótesis, a saber, que

$$(\forall B)(B \in A \rightarrow x \in B),$$

inferimos de (4) que

$$(5) \qquad (\exists C)(\forall x)(x \in C \leftrightarrow (\forall B)(B \in A \rightarrow x \in B)).$$

Que $x \in \bigcap A$ se sigue de (5), la definición de $\bigcap A$ y las condiciones de definición de las definiciones por abstracción. Q.E.D.

En esta demostración se ha usado una notación entre paréntesis rectangulares, que conviene frecuentemente, para demostrar una equivalencia. Consideramos la fórmula que es el miembro de la *derecha* de la equivalencia que establece una condición necesaria y suficiente para que valga la fórmula que está a la izquierda. Así, si queremos demostrar un teorema de la forma $\mathbf{P} \leftrightarrow \mathbf{Q}$, establecemos que $\mathbf{Q}$ es una condición *necesaria* para $\mathbf{P}$ suponiendo $\mathbf{P}$ y deduciendo $\mathbf{Q}$. Establecemos que $\mathbf{Q}$ es una condición *suficiente* para $\mathbf{P}$ deduciendo $\mathbf{P}$ a partir de $\mathbf{Q}$.

El orden de desarrollo de esta sección es algo falaz. La demostración del teorema 67 no depende del axioma de suma y la teoría elemental de la operación $\bigcap$ podría haber precedido a la consideración de este axioma.

Teorema 68. $\bigcap 0 = 0$.

Demostración. Supongamos que $\bigcap 0 \neq 0$. Entonces, existe un x en $\bigcap 0$; por el teorema 67 existe un conjunto $B \in 0$, lo que es absurdo. Q.E.D.

Es importante observar que en la teoría de conjuntos de von Neumann, la cual admite conjuntos que no son elementos de ningún otro conjunto, o sea, clases propias, el símbolo de operación '$\bigcap$' se define de tal manera que el teorema 68 es falso. En efecto, el teorema es,

$$(1) \qquad \bigcap 0 = V,$$

donde V es el universo, esto es, la clase propia que tiene como elementos todas las cosas que son elementos de algo. La diferencia radical entre (1) y el teorema 68 hace resaltar el carácter ligeramente artificial de cualquier forma de teoría axiomática de conjuntos. Intuitivamente, (1) puede parecer preferible al teorema 68, pero (1) conlleva la admisión de clases propias, lo cual aparece más bien grotesco desde el punto de vista de la teoría de conjuntos intuitiva e informal.

Teorema 69. $\bigcap \{0\} = 0$.

Demostración. Supongamos que hay un elemento x en $\bigcap \{0\}$. Entonces, en virtud de la definición 14, $x \in 0$, lo que es absurdo. Q.E.D.

Los cuatro teoremas siguientes, lo mismo que los dos anteriores, se refieren a la intersección de familias de conjuntos, extremadamente simples. Dos de las demostraciones se omiten.

Teorema 70. $\bigcap \{A\} = A$.

Demostración. Si

$$x \in \bigcap \{A\},$$

entonces, ya que $A \in \{A\}$, por la definición 14,

$$x \in A.$$

Por otra parte, si $x \in A$, entonces, ya que para todo B en $\{A\}$, $B = A$, por el teorema 67,

$$x \in \bigcap \{A\}. \qquad \text{Q.E.D.}$$

Teorema 71. $\bigcap \{A,B\} = A \cap B$.

Teorema 72. $\bigcap \langle x,y \rangle = \{x\}$.

Teorema 73. $\bigcap \bigcap \langle A,B \rangle = A$.

Demostración. En virtud del teorema 72,

$$\bigcap \langle A,B \rangle = \{A\},$$

y en virtud del teorema 70,

$$\bigcap \{A\} = A. \qquad \text{Q.E.D.}$$

En seguida están cinco implicaciones generales relativas a intersecciones de familias de conjuntos.

Teorema 74. $A \subseteq B \;\&\; (\exists C)(C \in A) \rightarrow \bigcap B \subseteq \bigcap A$.

Demostración. Sea x un elemento arbitrario de $\bigcap B$. Entonces, para todo $C \in B$, debemos tener:

$$x \in C,$$

pero la hipótesis del teorema nos asegura que si $C \in A$, entonces $C \in B$. Por consiguiente, para todo $C \in A$, debemos tener: $x \in C$; así, $x \in \bigcap A$, el resultado pedido. Q.E.D.

La explicación rigurosa de por qué se requiere la condición $(\exists C)(C \in A)$ en la hipótesis del teorema 74, se deja como ejercicio.

Teorema 75. $A \in B \rightarrow \bigcap B \subseteq A$.

Teorema 76. $A \in B \;\&\; A \subseteq C \rightarrow \bigcap B \subseteq C$.

Teorema 77. $A \in B \;\&\; A \cap C = 0 \rightarrow (\bigcap B) \cap C = 0$.

Teorema 78. $(\exists C)(C \in A) \;\&\; (\exists D)(D \in B) \rightarrow \bigcap (A \cup B) = (\bigcap A) \cap (\bigcap B)$.

Demostración.

$x \in \bigcap (A \cup B) \leftrightarrow (\forall C)(C \in A \cup B \rightarrow x \in C)$
Por el teorema 67 y la hipótesis del teorema

$\leftrightarrow (\forall C)(C \in A \vee C \in B \rightarrow x \in C)$.
Por el teorema 20

$\leftrightarrow (\forall C)[(C \in A \rightarrow x \in C) \;\&\; (C \in B \rightarrow x \in C)]$.
Por la lógica proposicional

$\leftrightarrow (\forall C)(C \in A \rightarrow x \in C) \;\&\; (\forall C)(C \in B \rightarrow x \in C)$.
Por la lógica cuantificacional *

$\leftrightarrow x \in \bigcap A \;\&\; x \in \bigcap B$ Por el teorema 67 y la hipótesis del teorema

$\leftrightarrow x \in (\bigcap A) \cap (\bigcap B)$ Por el teorema 12.

La formulación rigurosa del teorema 78 es sensible a la forma en que la teoría axiomática de conjuntos sea usada. Si se admiten clases propias y $\bigcap 0 = V$, entonces el teorema se formula incondicionalmente:

$$\bigcap (A \cup B) = (\bigcap A) \cap (\bigcap B).$$

Si el esquema usado es la teoría de conjuntos de Zermelo, *sin* individuos, entonces la formulación es simplemente,

(1) $A \neq 0 \;\&\; B \neq 0 \rightarrow \bigcap (A \cup B) = (\bigcap A) \cap (\bigcap B)$.

La teoría de conjuntos de Zermelo *con* individuos requiere la formulación dada en el teorema. La inexactitud de (1), para nuestro esquema de desarrollo, se ve tomando

$$A = \{\text{Euler}\} \neq 0$$
$$B = \{\{\text{Euler}\}\} \neq 0.$$

Entonces,

$$\bigcap A = 0$$

y por consiguiente,

$$(\bigcap A) \cap (\bigcap B) = 0,$$

pero

$$\bigcap (A \cup B) = \{\text{Euler}\} \neq 0.$$

El siguiente grupo de teoremas incluye tanto unión como intersección de una familia de conjuntos.

Teorema 79. $\bigcap A \subseteq \bigcup A$.

Demostración. Si $x \in \bigcap A$, entonces, por el teorema 67,

(1) $(\forall B)(B \in A \rightarrow x \in B) \;\&\; (\exists B)(B \in A)$.

Se sigue de (1) que

$$(\exists B)(B \in A \;\&\; x \in B),$$

por consiguiente, por el teorema 55, $x \in \bigcup A$. Q.E.D.

* Claramente, a partir de $(\forall v)(P \;\&\; Q)$ podemos inferir $(\forall v)P \;\&\; (\forall v)Q$, y recíprocamente.

Teorema 80. $\bigcup \bigcap \langle A,B\rangle = A$.

Teorema 81. $\bigcap \bigcup \langle A,B\rangle = A \cap B$.

En muchos contextos matemáticos, en lugar de $\bigcup A$ y $\bigcap A$ se usa a menudo la notación,

(1) $$\bigcup_{B\in A} B$$

y

(2) $$\bigcap_{B\in A} B$$

En realidad es conveniente una notación más flexible que (1) y (2), en los capítulos finales para el desarrollo de la teoría de números ordinales. Al introducir en este momento el esquema de definición apropiado, usamos la expresión '$\tau(x)$' para un esquema de términos del mismo modo que hemos usado '$\varphi(x)$' para un esquema de fórmulas.

Esquema de definición 15.

(a) $\bigcup_{x\in A} \tau(x) = \bigcup \{y: (\exists x)(y = \tau(x) \;\&\; x \in A)\}$

(b) $\bigcap_{x\in A} \tau(x) = \bigcap \{y: (\exists x)(y = \tau(x) \;\&\; x \in A)\}$.

Así, si $A = \{1,2,3\}$ y $\tau(x) = \{x\} \cup \{4\}$, entonces

$$\bigcup_{x\in A} \tau(x) = \bigcup \{\{1,4\}, \{2,4\}, \{3,4\}\}$$
$$= \{1,2,3,4\}$$

y

$$\bigcap_{x\in A} \tau(x) = \{4\}.$$

Se usan frecuentemente otras notaciones diferentes de las anteriores para unión e intersección de familias de conjuntos, pero no se presentarán formalmente. Por ejemplo,

$$\bigcup_{\varphi(x)} x = \bigcup \{x: \varphi(x)\}.$$

Desde el punto de vista lógico hay una gran diferencia entre las definiciones 13 y 14, por una parte y la definición 15, por la otra. Las dos primeras introducen símbolos de operación, mientras que la definición 15 introduce un operador que proporciona una nueva manera de ligar variables y bajo este respecto puede agruparse con las definiciones 11 y 12.

Formulamos, sin demostración, algunos teoremas relativos a las nociones introducidas por la definición 15. Nótese que estos teoremas, como el teorema 78, establecen leyes distributivas generales e importantes. En los ejercicios se dan algunos resultados adicionales.

Teorema 82. $\bigcup_{x\in A} x = \bigcup A$.

Teorema 83. $\bigcap_{x\in A} x = \bigcap A$.

Teorema 84. $A \cap \bigcup B = \bigcup_{C\in B} (A \cap C)$.

Teorema 85. $(\exists D)(D \in B) \rightarrow A \cup \bigcap B = \bigcap_{C\in B} (A \cup C)$.

Finalmente, concluimos esta sección demostrando que el axioma de unión es redundante. Ya que este teorema no es relativo a conjuntos sino a nuestros axiomas particulares de la teoría de conjuntos, lo señalamos como un meta-teorema, o sea, un teorema meta-matemático.

Meta-teorema 1. *El axioma de unión es deducible del axioma de extensionalidad, el axioma de apareamiento y el axioma de suma.*

Demostración. Dados dos conjuntos cualesquiera, A y B, por el axioma de apareamiento tenemos el conjunto

$$\{A,B\}.$$

Ahora $x \in \bigcup \{A,B\}$

$\leftrightarrow (\exists D)(D \in \{A,B\} \;\&\; x \in D)$

por el teorema 55

$\leftrightarrow (\exists D)((D = A \vee D = B) \;\&\; x \in D)$

por el teorema 43

$\leftrightarrow x \in A \vee x \in B$ por la lógica cuantificacional.

A partir de las equivalencias anteriores, es sólo cuestión de lógica cuantificacional deducir que

$$(\exists C)(\forall x)(x \in C \leftrightarrow x \in A \vee x \in B),$$

que es precisamente el axioma de unión.

Q.E.D.

En relación con la demostración anterior, es fácil constatar que los teoremas 43 y 55 dependen de no más de los tres axiomas mencionados. La identificación precisa de los puntos en los cuales se requiere el axioma de extensionalidad se deja como ejercicio.

EJERCICIOS

1. Dado que $A = \{\{1,2\}, \{2,0\}, \{1,3\}\}$, hallar $\bigcup A$, $\bigcap A$, $\bigcap\bigcup A$.

2. Dado que $A = \{\{\{1,2\}, \{1\}\}, \{\{1,0\}\}\}$, hallar $\bigcup A$, $\bigcap A$, $\bigcup\bigcup A$, $\bigcap\bigcap A$, $\bigcup\bigcap A$, $\bigcap\bigcup A$.

3. Determinar un conjunto específico A que sirva como contra-ejemplo a la aserción general

$$\bigcap A = 0 \rightarrow A = 0 \vee A = \{0\}.$$

4. Determinar conjuntos específicos A y B que sirvan como contra-ejemplo a la aserción general

$$\bigcap A \cap \bigcap B = \bigcap (A \cap B).$$

5. Dar una definición de $\bigcup A$ por medio de una equivalencia, sin usar la notación de abstracción.

6. En el documento original de Zermelo [1908] él definió '$\bigcap$' de tal manera que si A tiene un individuo como uno de sus elementos, $\bigcap A = 0$. Formular de nuevo la definición 14, para estar de acuerdo con la de Zermelo y demostrar, por medio de contra-ejemplos, cuáles de los teoremas de esta sección no son válidos cuando se usa esta definición revisada.

7. Demostrar el teorema 58.

8. Demostrar los teoremas 62, 63 y 64.

9. Demostrar el teorema 66.

10. Demostrar los teoremas 71 y 72.

11. Con respecto a la parte existencial de la hipótesis del teorema 74, demostrar, por medio de un ejemplo, que si esa parte se omite, el enunciado resultante no es un teorema.

12. Demostrar los teoremas 75, 76 y 77.

13. Demostrar los teoremas 80 y 81.

14. Demostrar que

$$0 \in A \rightarrow \bigcap A = 0.$$

15. Demostrar que

$$(\forall C)(C \in A \rightarrow (\exists D)(D \in B \;\&\; C \subseteq D)) \rightarrow \bigcup A \subseteq \bigcup B.$$

16. Demostrar los teoremas 82 y 83.

17. Demostrar los teoremas 84 y 85.

18. Demostrar que $\bigcap\limits_{x \in A} (\{x\} \sim B) = \bigcap\limits_{x \in A} \{x\} \sim B$.

19. Explicar en cuáles puntos de la demostración del meta-teorema 1 se requiere el axioma de extensionalidad.

§ 2.7 Axioma del conjunto potencia. En esta sección tratamos de la noción del conjunto de todos los subconjuntos de un conjunto dado. Este conjunto se llama *conjunto potencia* del conjunto dado. El nombre "conjunto potencia" tiene su origen en el hecho de que si un conjunto A tiene n elementos, entonces su conjunto potencia (en símbolos: $\mathcal{P}A$) tiene 2^n elementos.
Para ilustrar esta noción, si

$$A = \{1,2\},$$

entonces

$$\mathcal{P}A = \{0, \{1\}, \{2\}, A\}.$$

Debe ser intuitivamente claro que, como en este ejemplo, el conjunto vacío es un elemento del conjunto potencia de cualquier conjunto; aún más, cualquier conjunto es un elemento de su propio conjunto potencia.

La definición formal apropiada, es obvia.

Definición 16. $\mathcal{P}A = \{B : B \subseteq A\}$.

Esta definición es libre de axioma en el mismo sentido que lo son las definiciones 13 y 14, pero para demostrar el teorema requerido que concierne a $\mathcal{P}A$, se necesita el *axioma del conjunto potencia* que garantice la existencia del conjunto intuitivamente apropiado:

$$(\exists B)(\forall C)(C \in B \leftrightarrow C \subseteq A).$$

Es importante notar que podríamos haber tomado la formulación más débil '$(\exists B)(\forall C)(C \subseteq A \rightarrow C \in B)$' y luego haber usado el esquema axiomático de separación para obtener el presente axioma. Podemos demostrar inmediatamente,

Teorema 86. $B \in \mathcal{P}A \leftrightarrow B \subseteq A$.

Demostración. Usar la definición 16, el axioma del conjunto potencia y las propiedades de la definición por abstracción.

Teorema 87. $A \in \mathcal{P}A$.

Demostración. Por el teorema 5,
$$A \subseteq A,$$
por consiguiente, por el teorema 86, obtenemos el resultado pedido. Q.E.D.

Teorema 88. $0 \in \mathcal{P}A$.

Teorema 89. $\mathcal{P}0 = \{0\}$.

Demostración. Puesto que $0 \subseteq 0$,
$$0 \in \mathcal{P}0.$$
Además, si $A \in \mathcal{P}0$, entonces, por el teorema 86,
$$A \subseteq 0,$$
pero, por el teorema 4,
$$A = 0. \qquad \text{Q.E.D.}$$

Teorema 90. $\mathcal{P}\mathcal{P}0 = \{0, \{0\}\}$.

Hay sólo cuatro teoremas adicionales relacionados con conjuntos potencia, que queremos formular en esta sección.

Teorema 91. $A \subseteq B \leftrightarrow \mathcal{P}A \subseteq \mathcal{P}B$.

Demostración. [Necesidad] Si $C \in \mathcal{P}A$ entonces, por el teorema 86,
$$C \subseteq A,$$
por nuestra hipótesis,
$$C \subseteq B,$$
en virtud, de nuevo, del teorema 86,
$$C \in \mathcal{P}B.$$
[Suficiencia]. Por el teorema 87, $A \in \mathcal{P}A$, y por nuestra hipótesis de que $\mathcal{P}A \subseteq \mathcal{P}B$,
$$A \in \mathcal{P}B,$$
pero, por el teorema 86, $A \subseteq B$. Q.E.D.

Teorema 92. $(\mathcal{P}A) \cup (\mathcal{P}B) \subseteq \mathcal{P}(A \cup B)$.

Demostración.

$$\begin{aligned} C \in (\mathcal{P}A) \cup (\mathcal{P}B) &\leftrightarrow C \in \mathcal{P}A \vee C \in \mathcal{P}B \\ &\leftrightarrow C \subseteq A \vee C \subseteq B \\ &\rightarrow C \subseteq A \cup B \\ &\rightarrow C \in \mathcal{P}(A \cup B). \text{Q.E.D.} \end{aligned}$$

Debe ser obvia la justificación de los pasos de esta demostración.

Teorema 93. $\mathcal{P}(A \cap B) = (\mathcal{P}A) \cap (\mathcal{P}B)$.

Teorema 94. $\mathcal{P}(A \sim B) \subseteq ((\mathcal{P}A) \sim (\mathcal{P}B)) \cup \{0\}$.

EJERCICIOS

1. Hallar: $\mathcal{P}$ { Arquímedes },
 $\mathcal{P}\mathcal{P}$ { Arquímedes },
 $\mathcal{P}$ {{ Arquímedes, Newton },0}.
2. Hallar
 $$\mathcal{P}\mathcal{P}\mathcal{P}0.$$
3. Demostrar los teoremas 88 y 90.
4. Demostrar el teorema 93.
5. Demostrar el teorema 94.
6. Dar contra-ejemplos para mostrar que no siempre es el caso de que

 (a) $(\mathcal{P}A) \cup (\mathcal{P}B) = \mathcal{P}(A \cup B)$

 (b) $\mathcal{P}(A \sim B) = (\mathcal{P}A) \sim (\mathcal{P}B)$.

§ **2.8 Producto cartesiano entre conjuntos.** El producto cartesiano entre dos conjuntos A y B (en símbolos, $A \times B$) es el conjunto de todas las parejas ordenadas $\langle x, y\rangle$ tales que $x \in A$ y $y \in B$. Por ejemplo, si
$$A = \{1,2\}$$
$$B = \{\text{Arquímedes, Eudoxio}\},$$
entonces
$$A \times B = \{\langle 1, \text{Arquímedes}\rangle, \langle 1, \text{Eudoxio}\rangle, \langle 2, \text{Arquímedes}\rangle, \langle 2, \text{Eudoxio}\rangle\}.$$
Formalmente, tenemos:

Definición 17. $A \times B = \{\langle x,y\rangle : x \in A \ \& \ y \in B\}$.

Para demostrar los teoremas acostumbrados acerca de productos cartesianos, debemos demostrar que existe el conjunto intuitivamente apropiado. La demostración de este hecho depende, de un modo esencial, del axioma del conjunto potencia. La idea decisiva de la demostración es la de que si
$$x = \langle y,z\rangle,$$
$$y \in A \quad \text{y} \quad z \in B,$$
entonces
$$x \in \mathcal{P}\mathcal{P}(A \cup B).$$

Teorema 95. $(\exists C)(\forall x)(x \in C \leftrightarrow (\exists y)(\exists z)(y \in A \,\&\, z \in B \,\&\, x = \langle y,z \rangle)$.

Demostración. En virtud del esquema axiomático de separación,

(1) $(\exists C)(\forall x)(x \in C \leftrightarrow x \in \mathcal{P}\mathcal{P}(A \cup B) \,\&\, (\exists y)(\exists z)(y \in A \,\&\, z \in B \,\&\, x = \langle y,z \rangle))$.

Puesto que el teorema es precisamente (1) sin '$x \in \mathcal{P}\mathcal{P}(A \cup B)$', nuestra tarea es demostrar que la equivalencia dada en (1) vale aun cuando esta cláusula se elimine. Dado (1) se sigue de una vez que

(2) $x \in C$

implica

(3) $(\exists y)(\exists z)(y \in A \,\&\, z \in B \,\&\, x = \langle y,z \rangle)$.

Para establecer la implicación recíproca es suficiente demostrar que (3) implica

(4) $x \in \mathcal{P}\mathcal{P}(A \cup B)$,

ya que,en virtud de (1), es obvio que (3) implica (2).

De este modo, necesitamos sólo demostrar que (3) implica (4). Ahora, por (3) y la definición de parejas ordenadas,

$$x = \{\{y\}, \{y,z\}\},$$

y ya que por hipótesis $y \in A$ y $z \in B$, tenemos:

$$\{y\} \subseteq A \cup B,$$

y

$$\{y,z\} \subseteq A \cup B,$$

en consecuencia, por el teorema 86,

$$\{y\} \in \mathcal{P}(A \cup B)$$

y

$$\{y, z\} \in \mathcal{P}(A \cup B).$$

Así que

$$\{\{y\}, \{y, z\}\} \subseteq \mathcal{P}(A \cup B),$$

o sea,

$$x \subseteq \mathcal{P}(A \cup B),$$

pero, en virtud, de nuevo, del teorema 86, tenemos:

$$x \in \mathcal{P}\mathcal{P}(A \cup B),$$

que es lo que queríamos demostrar. Q.E.D.

Tenemos entonces, de manera casi inmediata, los dos útiles teoremas siguientes.

Teorema 96. $x \in A \times B \leftrightarrow (\exists y)(\exists z)(y \in A \,\&\, z \in B \,\&\, x = \langle y,z \rangle)$.

Teorema 97. $\langle x,y \rangle \in A \times B \leftrightarrow x \in A \,\&\, y \in B$.

Ahora nos referimos a ciertos teoremas cuyo contenido intuitivo es obvio. Varias de las demostraciones se han omitido y dejado como ejercicios.

Teorema 98.

$$A \times B = 0 \leftrightarrow A = 0 \vee B = 0.$$

Demostración. [Necesidad]. Usamos un argumento indirecto. Por hipótesis, $A \times B = 0$. Supongamos ahora que

$$A \neq 0 \,\&\, B \neq 0.$$

Entonces, por el teorema 2,

$$(\exists y)(y \in A) \,\&\, (\exists z)(z \in B),$$

y por el teorema 96,

$$\langle y,z \rangle \in A \times B,$$

lo que contradice la hipótesis y demuestra que nuestra suposición es falsa.

[Suficiencia]. A partir de la condición de que $A = 0$ o $B = 0$ y del teorema 2, inferimos

(1) $-(\exists y)(y \in A) \vee -(\exists z)(z \in B)$,

y se sigue de (1) que

$$-(\exists y)(\exists z)(y \in A \,\&\, z \in B \,\&\, x = \langle y,z \rangle),$$

y por el teorema 96, para todo x,

$$x \notin A \times B.$$

Por consiguiente, por el teorema 2,

$$A \times B = 0. \qquad \text{Q.E.D.}$$

Teorema 99.

$$A \times B = B \times A \leftrightarrow (A = 0 \vee B = 0 \vee A = B).$$

Demostración. [Necesidad]. Supongamos que $A \neq 0$, $B \neq 0$ y $A \neq B$, esto es, supongamos que la condición no vale. Puesto que $A \neq B$, existe un x tal que, o bien $x \in A \,\&\, x \notin B$ o bien $x \notin A \,\&\, x \in B$. Para precisar, supongamos que vale la primera alternativa; sea y un elemento de B (existen tales elementos, ya que $B \neq 0$). Entonces, por el teorema 97,

$$\langle x,y \rangle \in A \times B,$$

partiendo de la hipótesis de que $A \times B = B \times A$, tenemos

$$\langle x,y \rangle \in B \times A,$$

pero en virtud del teorema 97, de nuevo,

$$x \in B,$$

lo que contradice nuestra suposición de que $x \notin B$.

[Suficiencia]. Podemos usar el teorema 98 para combinar dos de las tres posibilidades; a saber, de $A = 0 \vee B = 0$ inferimos que

$$A \times B = 0 = B \times A.$$

Supongamos ahora la tercera posibilidad: $A = B$. Entonces, puesto que es una verdad lógica que

$$A \times A = A \times A$$

tenemos, de una vez, que

$$A \times B = B \times A. \qquad \text{Q.E.D.}$$

Teorema 100. $A \neq 0 \;\&\; A \times B \subseteq A \times C \rightarrow B \subseteq C$.

Demostración. Si $B = 0$, la demostración es trivial, de modo que suponemos $B \neq 0$. Ya que por hipótesis $A \neq 0$, sea

$$x \in A \;\&\; y \in B.$$

Entonces, por el teorema 97,

$$\langle x,y \rangle \in A \times B,$$

además, por hipótesis,

$$\langle x,y \rangle \in A \times C.$$

Por consiguiente, usando de nuevo el teorema 97,

(1) $\qquad y \in C.$

Puesto que y es un elemento arbitrario de B, (1) establece que $B \subseteq C$. Q.E.D.

La demostración del siguiente teorema se deja como ejercicio.

Teorema 101. $B \subseteq C \rightarrow A \times B \subseteq A \times C$.

Los tres teoremas siguientes establecen tres leyes distributivas para la operación de formar el producto cartesiano entre dos conjuntos. Sólo el primero se demuestra aquí.

Teorema 102. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Demostración. $\langle x,y \rangle \in A \times (B \cap C)$

$\leftrightarrow x \in A \;\&\; y \in B \cap C$ — por el teorema 97

$\leftrightarrow x \in A \;\&\; y \in B \;\&\; y \in C$ — por el teorema 12

$\leftrightarrow x \in A \;\&\; y \in B \;\&\; x \in A \;\&\; y \in C$ — por lógica proposicional

$\leftrightarrow \langle x,y \rangle \in A \times B \;\&\; \langle x,y \rangle \in A \times C$ — por el teorema 97

$\leftrightarrow \langle x,y \rangle \in (A \times B) \cap (A \times C)$ — por el teorema 12

Q.E.D.

Teorema 103. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Teorema 104. $A \times (B \sim C) = (A \times B) \sim (A \times C)$.

EJERCICIOS

1. Demostrar los teoremas 96 y 97.
2. Demostrar el teorema 101.
3. Demostrar los teoremas 103 y 104.
4. Dar un contra-ejemplo simple para mostrar que, en general, no es el caso de que

$$A \cup (B \times C) = (A \times B) \cup (A \times C).$$

5. ¿Es asociativa la operación producto cartesiano? Si lo es, demostrarlo. Si no, dar un contra-ejemplo.
6. Demostrar que

$$A \times \bigcap B = \bigcap_{C \in B} (A \times C).$$

§2.9 Axioma de regularidad. Es difícil pensar en un conjunto que pueda considerarse razonablemente como elemento de sí mismo. Ciertamente, el conjunto de todos los hombres, por ejemplo, no es un hombre y por consiguiente no es un elemento de sí mismo. Quizás podría argüirse que, en teoría de conjuntos intuitiva, el conjunto de todos los objetos abstractos o el conjunto de todos los conjuntos deberían dar un ejemplo de un conjunto que sea elemento de sí mismo, pero, como vimos en el capítulo primero, el conjunto de todos los conjuntos es en sí mismo un objeto paradójico.

Estas observaciones sugieren que tomemos como axioma

(1) $$A \notin A.$$

Sin embargo, la adopción de (1) no prohibiría la situación no intuitiva de que hubiese conjuntos distintos A y B tales que

(2) $$A \in B \;\&\; B \in A.$$

(Si usted no cree que (2) no es intuitivo, trate de dar un ejemplo simple de conjuntos A y B que satisfagan (2)). Más aún, si tomamos (2) como axioma, se admitirían ciclos más largos de pertenencia no intuitivos, como la existencia de conjuntos distintos A, B y C tales que

(3) $$A \in B \;\&\; B \in C \;\&\; C \in A.$$

Evitamos tales ciclos de cualquier longitud n, adoptando un axioma que es (bajo la hipótesis de nuestros otros axiomas, incluido el de escogencia) equivalente al de la no existencia de sucesiones descendentes infinitas de conjuntos (i.e., $A_{i+1} \in A_i$). La forma del axioma que adoptamos, el *axioma de regularidad,* se debe a Zermelo [1930], si bien von Neumann ya había dado [1929, p. 231] un axioma esencialmente equivalente pero más complicado.*

$$A \neq 0 \rightarrow (\exists x)[x \in A \;\&(\forall y)(y \in x \rightarrow y \notin A)].$$

Este axioma fue llamado por Zermelo el *Axiom der fundierung.* Intuitivamente expresa que, dado un conjunto no vacío A, existe un elemento x de A tal que la intersección entre A y x es vacía. La parte '$(\forall y)(y \in x \rightarrow y \notin A)$' que expresa que la intersección entre A y x es vacía no se ha reemplazado por la fórmula de aspecto más simple '$A \cap x = 0$' debido a la definición condicional de intersección; porque si x es un individuo, la definición no asigna significado intuitivo a la intersección de x con cualquier otro objeto. Cuando es claro que x debe ser un conjunto, usamos la fórmula más simple en las demostraciones.

Ahora usamos el axioma de regularidad para demostrar (1) y la negación de (2) como teoremas.

Teorema 105. $A \notin A$.

Demostración. Supongamos que A es un conjunto tal que $A \in A$. Puesto que $A \in \{A\}$, entonces tenemos,

(1) $$A \in \{A\} \cap A.$$

En virtud del axioma de regularidad, hay algún x en $\{A\}$ tal que

$$\{A\} \cap x = 0,$$

pero ya que $\{A\}$ es un conjunto unitario,

$$x = A,$$

por tanto,

$$\{A\} \cap A = 0,$$

lo que contradice (1). Q.E.D.

Teorema 106. $-(A \in B \;\&\; B \in A)$.

Demostración. Supongamos que $A \in B$ & $B \in A$. Entonces,

(1) $A \in \{A,B\} \cap B$ y $B \in \{A,B\} \cap A$.

Por el axioma de regularidad hay un x en $\{A, B\}$ tal que $\{A,B\} \cap x = 0$ y por el teorema 43,

$$x = A \text{ o } x = B.$$

Por consiguiente,

$$\{A,B\} \cap A = 0 \quad \text{o} \quad \{A,B\} \cap B = 0,$$

lo que contradice (1). Q.E.D.

La demostración del teorema 106 se desarrolló exactamente como la del teorema precedente. En forma análoga se desarrolla la demostración de la imposibilidad de un ciclo de tres o más conjuntos.

Como ejemplo del tipo de teorema para el cual el axioma de regularidad es esencial,

* La idea esencial fue formulada antes aun por von Neumann [1925, p. 239] y antes de éste, por Mirimanoff [1917].

podemos demostrar uno acerca de productos cartesianos, que puede parecer obvio intuitivamente, pero que no se puede demostrar solamente con base en los axiomas introducidos al comienzo.

Teorema 107. $A \subseteq A \times A \rightarrow A = 0.$

Demostración. Ya que por hipótesis A es un subconjunto de $A \times A$, a partir de la definición de producto cartesiano sabemos que si $z \in A$, entonces hay elementos x y y tales que

(1) $$z = \langle x,y \rangle = \{\{x\}, \{x,y\}\}$$

y

(2) $$x \in A \ \& \ y \in A.$$

Supongamos, en contra de la tesis del teorema, que $A \neq 0$. Apliquemos el axioma de regularidad a $A \cup \bigcup A$; por tanto, hay un conjunto no vacío C tal que

$$C \in A \cup \bigcup A$$

y

(3) $$C \cap (A \cup \bigcup A) = 0.$$

De (1) se sigue que C debe ser un conjunto no vacío y no el conjunto vacío o un individuo; tanto los elementos de A como de $\bigcup A$ deben ser conjuntos no vacíos. Supongamos ahora que $C \in A$. Entonces, por el teorema 62, $C \subseteq \bigcup A$ y ya que C no es vacío debemos tener,

$$C \cap \bigcup A \neq 0,$$

lo que contradice (3). Así que C debe estar en $\bigcup A$; pero con base en (1), existen elementos en x y y tales que

$$C = \{x\} \vee C = \{x, y\}$$

y con base en (2), $x, y \in A$; por tanto, en cualquier caso,

$$C \cap A \neq 0,$$

lo que también contradice (3) y demuestra que es falsa nuestra suposición de que $A \neq 0$.

Q.E.D.

Aun cuando el axioma de regularidad tiene muchas consecuencias naturales e impone, como Zermelo puntualizó en su documento de 1930, una condición que se cumplirá en todas las aplicaciones prácticas, es posible construir sistemas de teoría de conjuntos que contradigan este axioma. Dos ejemplos son, el sistema de ontología de Lesniewski (para una buena información, véase Slupecki [1955]) y el sistema de Quine [1940].

EJERCICIOS

1. Demostrar que para conjuntos cualesquiera, A, B, C, es falso que

$$A \in B \ \& \ B \in C \ \& \ C \in A.$$

2. Demostrar que si $A = A \times B$ entonces $A = 0$.
3. Demostrar que si $A \times B \neq 0$ entonces existe un C en $A \times B$ tal que $(\bigcup C) \cap (A \times B) = 0$.
4. Demostrar un análogo del teorema 46, usando la siguiente definición de parejas ordenadas:

$$\langle x,y \rangle = \{x, \{x,y\}\}.$$

§ 2.10 Resumen de Axiomas. Para referencia posterior, resumimos aquí los seis axiomas no redundantes presentados en este capítulo. Se ha omitido el axioma de unión porque se demostró en § 2.6 que tal axioma se sigue del axioma de extensionalidad, el axioma de apareamiento y el axioma de suma. Estos seis axiomas son suficientes para todos los desarrollos del capítulo 3, que trata de relaciones y funciones.

Axioma de extensionalidad

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

Esquema axiomático de separación

$$(\exists B)(\forall x)(x \in B \leftrightarrow x \in A \ \& \ \varphi(x)).$$

Axioma de apareamiento

$$(\exists A)(\forall z)(z \in A \leftrightarrow z = x \vee z = y).$$

Axioma de suma

$$(\exists C)(\forall x)(x \in C \leftrightarrow (\exists B)(x \in B \ \& \ B \in A)).$$

Axioma de conjunto potencia

$$(\exists B)(\forall C)(C \in B \leftrightarrow C \subseteq A).$$

Axioma de regularidad

$$A \neq 0 \rightarrow (\exists x)[x \in A \ \& \ (\forall y)(y \in x \rightarrow y \notin A)].$$

Capítulo 3

Relaciones y Funciones

§ 3.1 **Operaciones entre relaciones binarias.** En los contextos cuotidianos hablamos frecuentemente de *relaciones* que se cumplen entre dos o entre varias cosas. Así, podemos decir que Augusto estaba en la relación de padrastro con respecto a Tiberio, o que la relación de "estar entre" se cumple para tres puntos. Cuando nos referimos a relaciones en los contextos ordinarios, insistimos en que debe haber alguna descripción intuitiva del tipo de conexión existente entre los ítems que están en una relación dada. Afortunadamente, esta idea vaga de conexión se puede pasar por alto en los contextos formales y se puede definir una relación simplemente como un conjunto de parejas ordenadas. En este capítulo trataremos casi exclusivamente de la teoría de relaciones binarias, esto es, relaciones que se cumplen entre dos cosas. Aún más, como veremos, la teoría de relaciones n-arias puede construirse dentro de la teoría de relaciones binarias. En consecuencia, omitimos el adjetivo modificativo "binaria" en la definición formal.*

Definición 1. A es una relación $\leftrightarrow (\forall x)(x \in A \rightarrow (\exists y)(\exists z)(x = \langle y, z\rangle))$.

Es interesante notar que ésta es nuestra primera definición de un símbolo unario de relación, pues la definición 1 del capítulo 2 caracterizaba la propiedad de ser un conjunto. Una idea natural sería que las definiciones subsiguientes, que conciernen a relaciones, deben ser bastante condicionales en la forma, como las definiciones que siguen a la definición de conjuntos. Sin embargo, no es este el caso y casi todas las que siguen se aplican a conjuntos arbitrarios, no exclusivamente a aquellos conjuntos que tienen el carácter de relaciones.

La inclusión de relaciones n-arias en esta definición se puede ejemplificar considerando relaciones ternarias, o sea, relaciones 3-arias. Un conjunto A es una relación ternaria, si y sólo si A es una relación y

$$(\forall x)(x \in A \rightarrow (\exists y)(\exists z)(\exists w)(x = \langle\langle y, z\rangle, w\rangle)).$$

Por otra parte, nótese que no para toda relación intuitiva que aparece en teoría de conjuntos hay un conjunto correspondiente de parejas ordenadas. Por ejemplo, no hay conjunto alguno que corresponda a la relación de inclusión entre conjuntos. En la teoría de conjuntos de von Neumann hay una clase propia que es la relación de inclusión entre conjuntos, pero no hay clase propia alguna que corresponda a la relación de inclusión entre clases propias.

Comenzamos los desarrollos sistemáticos con tres teoremas simples, después de introducir la útil notación $x\,A\,y$.

Definición 2. $x\,A\,y \leftrightarrow \langle x, y\rangle \in A$.

Teorema 1. *0 es una relación.*

Demostración. Es inmediata de acuerdo

* Las definiciones y los teoremas se han numerado de nuevo en cada capítulo. Una referencia a una definición o teorema, sin mención explícita del capítulo, corresponde a una definición o teorema del mismo capítulo en el cual está la referencia.

con la definición de relaciones, puesto que el conjunto vacío no tiene elementos.

Teorema 2. *R es una relación* & $S \subseteq R \to$ *S es una relación.*

Demostración. Sea x un elemento arbitrario de S. Entonces, por hipótesis,

$$x \in R,$$

por lo tanto, también por nuestra hipótesis, existen un y y un z tales que

$$x = \langle y, z\rangle.$$

Entonces, de acuerdo con la definición 1, S es una relación. Q.E.D.

Teorema 3. *R y S son relaciones* $\to R \cap S$, $R \cup S$ *y* $R \smile S$ *son relaciones.*

El uso de las variables 'R' y 'S' en los dos últimos teoremas no es una innovación formal, pues todas las letras mayúsculas en bastardilla son variables de conjuntos; se entiende que son puramente sugestivas del hecho que estamos considerando intuitivamente los conjuntos que son relaciones, si bien los teoremas valen para conjuntos arbitrarios.

Si R es una relación, entonces el *dominio* de R (en símbolos: $\mathfrak{D}R$) es el conjunto de todos los objetos x tales que, para algún y, $\langle x, y\rangle \in R$. Así, si

$$R_1 = \{\langle 0, 1\rangle, \langle 2, 3\rangle\},$$

entonces

$$\mathfrak{D}R_1 = \{0, 2\}.$$

El *recorrido* de R (en símbolos $\mathfrak{R}R$) es el conjunto de todos los objetos y, tales que, para algún x, $\langle x, y\rangle \in R$. Así,

$$\mathfrak{R}R_1 = \{1, 3\}.$$

El recorrido de una relación se llama también *contra-dominio* o *dominio converso.* El *campo* de una relación R (en símbolos, $\mathfrak{F}R$) es la unión de su dominio y su recorrido. Por ejemplo,

$$\mathfrak{F}R_1 = \{0, 1, 2, 3\}.$$

En los desarrollos formales obvios, relacionados con los conceptos de dominio, recorrido y campo, el único problema difícil es demostrar que existe el conjunto intuitivamente apropiado. Como es usual, las definiciones mismas son libres de axioma.

Definición 3. $\mathfrak{D}A = \{x: (\exists y)(x\ A\ y)\}$.

El siguiente teorema confirma que $\mathfrak{D}A$ es el conjunto apropiado.

Teorema 4. $x \in \mathfrak{D}A \leftrightarrow (\exists y)(x\ A\ y)$.

Demostración. En virtud del esquema axiomático de separación,

(1) $(\exists B)(\forall x)(x \in B \leftrightarrow x \in \bigcup\bigcup A\ \&\ (\exists y)(x\ A\ y))$.

Queremos establecer la equivalencia obtenida de (1) omitiendo

(2) $$x \in \bigcup\bigcup A.$$

En consecuencia, necesitamos demostrar que (2) está implicado por la aserción de que existe un y tal que

(3) $$x\ A\ y.$$

La siguiente cadena de implicaciones sirve para ese propósito. Por la definición 2 tenemos, a partir de (3):

$$\langle x, y\rangle \in A,$$

por lo tanto, en virtud de la definición de parejas ordenadas,

$$\{\{x\}, \{x, y\}\} \in A.$$

Así que, por el teorema 55 del capítulo 2,

$$\{x\} \in \bigcup A,$$

y en virtud del teorema 55, de nuevo,

$$x \in \bigcup\bigcup A.$$

Se sigue fácilmente de (1) que

(4) $(\exists B)(\forall x)(x \in B \leftrightarrow (\exists y)(x\ A\ y))$.

El resto de la demostración requiere simplemente una manipulación rutinaria de la definición por abstracción. Puede ser útil presentar además los detalles. Por sustitución apropiada en el esquema de definición 11, del capítulo 2, obtenemos:

(5) $\mathfrak{D}A = \{x: (\exists y)(x\ A\ y)\} \leftrightarrow [(\forall x)(x \in \mathfrak{D}A \leftrightarrow (\exists y)(x\ A\ y)) \vee [-(\exists B)(\forall x)(x \in B \leftrightarrow (\exists y)(x\ A\ y))\ \&\ \mathfrak{D}A = 0]]$.

En virtud de la definición 3 obtenemos, a partir de (5),

(6) $(\forall x)(x \in \mathfrak{D}A \leftrightarrow (\exists y)(x\ A\ y)) \lor$
$[-(\exists B)(\forall x)(x \in B \leftrightarrow (\exists y)(x\ A\ y))$
$\&\ \mathfrak{D}A = 0]$,

además, a partir de (4) y (6), concluimos inmediatamente que nuestro teorema es válido. Q.E.D.

Nótese que, a pesar de la apariencia formidable de (5) y (6), la inferencia del teorema, a partir de (4), (5), (6) y la definición 3, involucra únicamente lógica proposicional.

Teorema 5. $\mathfrak{D}(A \cup B) = \mathfrak{D}A \cup \mathfrak{D}B$.

Demostración. $x \in \mathfrak{D}(A \cup B)$

$\leftrightarrow (\exists y)(x\ A \cup B\ y)$ por el teorema 4

$\leftrightarrow (\exists y)(x\ A\ y \lor x\ B\ y)$ por el teorema 20 del capítulo 2

$\leftrightarrow (\exists y)(x\ A\ y) \lor (\exists y)(x\ B\ y)$ por la lógica cuantificacional

$\leftrightarrow x \in \mathfrak{D}A \lor x \in \mathfrak{D}B$ por el teorema 4

$\leftrightarrow x \in \mathfrak{D}A \cup \mathfrak{D}B$ por el teorema 20 del capítulo 2

Q.E.D.

Se enuncian, sin demostración, dos teoremas semejantes, relacionados con dominios, intersecciones y diferencias.

Teorema 6. $\mathfrak{D}(A \cap B) \subseteq \mathfrak{D}A \cap \mathfrak{D}B$.

Teorema 7. $\mathfrak{D}A \sim \mathfrak{D}B \subseteq \mathfrak{D}(A \sim B)$.

La noción de *recorrido* se puede definir en forma simétrica a la de dominio.

Definición 4. $\mathfrak{R}A = \{y: (\exists x)(x\ A\ y)\}$.

Puesto que los teoremas sobre la operación recorrido son paralelos a los correspondientes a la operación dominio, se han omitido las demostraciones. Aún más, el teorema obvio, análogo al teorema 4, no se ha formulado.

Teorema 8. $\mathfrak{R}(A \cup B) = \mathfrak{R}A \cup \mathfrak{R}B$.

Teorema 9. $\mathfrak{R}(A \cap B) \subseteq \mathfrak{R}A \cap \mathfrak{R}B$.

Teorema 10. $\mathfrak{R}A \sim \mathfrak{R}B \subseteq \mathfrak{R}(A \sim B)$.

La noción de *campo* de un conjunto se define como era de esperarse.

Definición 5. $\mathfrak{F}A = \mathfrak{D}A \cup \mathfrak{R}A$.

Por el momento no demostraremos teoremas acerca de la operación campo $\mathfrak{F}$, pero más adelante haremos uso de ella.

Ahora nos referimos a la importante noción de *operación conversa.* Como en el caso de las tres operaciones que acaban de introducirse, la definición se aplica a conjuntos arbitrarios, no únicamente a relaciones. La conversa de una relacion R (en símbolos: $\breve{R}$) es la relación tal que para todos los x y y, $x\ \breve{R}\ y$ si y sólo si, $y\ R\ x$. La conversa de una relación se obtiene simplemente invirtiendo el orden de los elementos de todas las parejas que constituyen la relación. Así, la conversa de la relación de esposo es la de esposa. Con respecto a la relación simple R_1 introducida antes,

$$\breve{R}_1 = \{\langle 1, 0\rangle, \langle 3, 2\rangle\}.$$

La definición está construida de tal modo que los elementos de los conjuntos que no son parejas ordenadas no pertenecen al converso del conjunto; así, el converso de todo conjunto es una relación.

Definición 6. $\breve{A} = \{\langle x, y\rangle: y\ A\ x\}$.

Como es usual, el problema inmediato es mostrar que los axiomas enunciados en el capítulo 2 son suficientemente fuertes para garantizar la existencia del conjunto converso apropiado.

Teorema 11. $x\ \breve{A}\ y \leftrightarrow y\ A\ x$.

Demostración. En virtud del esquema axiomático de separación,

(1) $(\exists B)(\forall x)(x \in B \leftrightarrow x \in \mathfrak{R}A \times \mathfrak{D}A\ \&$
$(\exists y)(\exists z)(x = \langle y, z\rangle\ \&\ z\ A\ y))$.

Como en las demostraciones previas, el paso decisivo es demostrar que la fórmula

(2) $(\exists y)(\exists z)(x = \langle y, z\rangle\ \&\ z\ A\ y)$

implica

(3) $x \in \mathcal{R}A \times \mathcal{D}A$.

Las siguientes implicaciones son suficientes, dado que $x = \langle y, z\rangle$:

$$\begin{aligned} z\,A\,y &\rightarrow y \in \mathcal{R}A \;\&\; z \in \mathcal{D}A \\ &\rightarrow \langle y, z\rangle \in \mathcal{R}A \times \mathcal{D}A \\ &\rightarrow x \in \mathcal{R}A \times \mathcal{D}A. \end{aligned}$$

Así tenemos justificación para concluir, a partir de (1), que

(4) $(\exists B)(\forall x)(x \in B \leftrightarrow (\exists y)(\exists z)$
$(x = \langle y, z\rangle \;\&\; z\,A\,y))$.

Por los pasos de rutina realizados previamente (ver, por ejemplo, la demostración del teorema 4), inferimos de (4) y de la definición 6,

(5) $x \in \breve{A} \leftrightarrow (\exists y)(\exists z)(x = \langle y, z\rangle \;\&\; z\,A\,y)$.

Nuestro teorema se sigue por aplicación directa de la lógica cuantificacional a (5).

Q.E.D.

La estrategia de esta demostración, como otras que apelan al esquema axiomático de separación para establecer la existencia de algún conjunto, se divide, de manera natural, en dos partes. Primera, debe decidirse cuál conjunto, cuya existencia se conoce, tiene al conjunto pedido como subconjunto. Aquí la respuesta es que el conjunto A es intuitivamente un subconjunto del producto cartesiano entre el recorrido y el dominio de A. Segunda, debe demostrarse que la satisfacción de la condición φ en el axioma de separación implica la pertenencia al conjunto más grande. Aquí esto consiste en demostrar que (2) implica (3). Cuando esas dos partes de la demostración se han llevado a cabo, es casi siempre cosa de rutina realizar lo que queda.

Nos referimos ahora a algunos teoremas acerca de la operación conversa; su contenido intuitivo debe ser obvio.

Teorema 12. *$\breve{A}$ es una relación.*

Demostración. Si $x \in \breve{A}$, entonces, en virtud de la definición de la operación conversa y del teorema 47 del capítulo 2,

$$(\exists y)(\exists z)\,(x = \langle y, z\rangle);$$

entonces, el teorema se sigue de la definición de relaciones. Q.E.D.

Teorema 13. $\breve{\breve{A}} \subseteq A$.

Teorema 14. *R es una relación* $\rightarrow \breve{\breve{R}} = R$.

En seguida se enuncian tres leyes distributivas.

Teorema 15. $\overset{\smile}{A \cap B} = \breve{A} \cap \breve{B}$.

Demostración. En virtud del teorema 12 y del teorema 3, es claro que necesitamos considerar sólo parejas ordenadas:

$$\begin{aligned} x\,\overset{\smile}{A \cap B}\,y &\leftrightarrow y\,A \cap B\,x \\ &\leftrightarrow y\,A\,x \;\&\; y\,B\,x \\ &\leftrightarrow x\,\breve{A}\,y \;\&\; x\,\breve{B}\,y \\ &\leftrightarrow x(\breve{A} \cap \breve{B})y. \end{aligned}$$

Q.E.D.

(Nótese que al escribir una sucesión de equivalencias no justificamos ahora cada paso, cuando la inferencia es obvia, a partir de teoremas anteriores.)

Teorema 16. $\overset{\smile}{A \cup B} = \breve{A} \cup \breve{B}$.

Teorema 17. $\overset{\smile}{A \sim B} = \breve{A} \sim \breve{B}$.

La noción que es natural introducir en seguida es la de *producto relativo* entre dos conjuntos. Si R y S son relaciones, entonces el producto relativo entre R y S (en símbolos R/S) es la relación que se cumple entre x y y, si y sólo si existe un z tal que R se cumple entre x y z y S se cumple entre z y y. Simbólicamente, tenemos:

Definición 7. $A/B = \{\langle x, y\rangle\colon (\exists z)$
$(x\,A\,z \;\&\; z\,B\,y)\}$.

Si, por ejemplo,

$$R = \{\langle 1, 3\rangle, \langle 2, 3\rangle\}$$
$$S = \{\langle 3, 1\rangle\},$$

entonces

$$R/S = \{\langle 1, 1\rangle, \langle 2, 1\rangle\}$$
$$S/R = \{\langle 3, 3\rangle\}.$$

La demostración del siguiente teorema, que usa el esquema axiomático de separación para determinar el problema usual de existencia, se deja como ejercicio.

Teorema 18. $xA/By \leftrightarrow (\exists z)(x\ A\ z\ \&\ z\ B\ y)$.

Las demostraciones de los siguientes cuatro teoremas son fáciles y se dejarán como ejercicios.

Teorema 19. *A/B es una relación.*

Teorema 20. $0/A = 0$.

Teorema 21. $\mathfrak{D}(A/B) \subseteq \mathfrak{D}A$.

Teorema 22. $A \subseteq B\ \&\ C \subseteq D \rightarrow A/C \subseteq B/D$.

Siguen tres teoremas que establecen leyes distributivas; solamente se da aquí la demostración de uno de ellos.

Teorema 23. $A/(B \cup C) = (A/B) \cup (A/C)$.

Demostración. En virtud del teorema 19 y del hecho ya demostrado que la unión de dos relaciones es una relación, sabemos de una vez que tanto $A/(B \cup C)$ como $(A/B) \cup (A/C)$ son relaciones. Por tanto,las siguientes equivalencias demuestran nuestro teorema:

$x\ A/(B \cup C)\ y$

$\leftrightarrow (\exists z)(x\ A\ z\ \&\ z\ B \cup C\ y)$

$\leftrightarrow (\exists z)(x\ A\ z\ \&\ (z\ B\ y \vee z\ C\ y))$

$\leftrightarrow (\exists z)((x\ A\ z\ \&\ z\ B\ y) \vee (x\ A\ z\ \&\ z\ C\ y))$

$\leftrightarrow (\exists z)(x\ A\ z\ \&\ z\ B\ y) \vee (\exists z)(x\ A\ z\ \&\ z\ C\ y)$

$\leftrightarrow x\ A/By \vee x\ A/Cy$

$\leftrightarrow x(A/B) \cup (A/C)y$. Q.E.D.

Debe notarse que el hallazgo de una demostración de este tipo depende de alguna familiaridad con la manipulación de cuantificadores.

Teorema 24. $A/(B \cap C) \subseteq (A/B) \cap (A/C)$.

Teorema 25. $(A/B) \sim (A/C) \subseteq A/(B \sim C)$.

El ejemplo que sigue a la definición de la operación producto relativo indica que esta operación no es conmutativa. Cuando se combina con la operación conversa, tenemos el siguiente intercambio de orden:

Teorema 26. $\overset{\smile}{A/B} = \breve{B}/\breve{A}$.

Demostración.

$x\ \overset{\smile}{A/B}\ y \leftrightarrow yA/Bx$

$\leftrightarrow (\exists z)(y\ A\ z\ \&\ z\ B\ x)$

$\leftrightarrow (\exists z)(x\ \breve{B}\ z\ \&\ z\ \breve{A}\ y)$

$\leftrightarrow x\ \breve{B}/\breve{A}\ y$. Q.E.D.

El teorema siguiente muestra que la operación producto relativo es asociativa y por tanto pueden omitirse los paréntesis sin ambigüedad en las apariciones reiteradas del símbolo de producto relativo.

Teorema 27. $(A/B)/C = A/(B/C)$.

La demostración se omite debido a que es un ejercicio inmediato de lógica cuantificacional.

Ahora definimos la noción de dominio de una relación *restringido* a un conjunto dado. Como es usual, la definición se aplica a conjuntos arbitrarios.

Definición 8. $R|A = R \cap (A \times \mathcal{R}(R))$.*

La definición se puede ilustrar con un ejemplo sencillo. Sea

$R = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 0, \text{Edgar Guest}\rangle\}$,

$A = \{1, 2\}$.

Entonces,

$$R|A = \{\langle 1, 2\rangle, \langle 2, 3\rangle\}.$$

Se dejan como ejercicios las demostraciones de los siguientes seis teoremas:

Teorema 28. $x\ R|A\ y \leftrightarrow x\ R\ y\ \&\ x \in A$.

Teorema 29. $A \subseteq B \rightarrow R|A \subseteq R|B$.

Teorema 30. $R|(A \cap B) = (R|A) \cap (R|B)$.

Teorema 31. $R|(A \cup B) = (R|A) \cup (R|B)$.

* La línea vertical es una notación usual para esta noción. Véase, por ejemplo, Kuratowski (1933, p. 12).

Teorema 32. $R|(A \sim B) = (R|A) \sim (R|B)$.

Teorema 33. $(R/S)|A = (R|A)/S$.

La siguiente definición introduce la notación * $R``A$, que se lee *la imagen del conjunto A bajo R*. Así, si R y A están definidas como en el ejemplo anterior,

$$R``A = \{2, 3\},$$

y

$$R``\{0\} = \{\text{Edgar Guest}\}.$$

Definición 9. $R``A = \mathfrak{R}(R|A)$.

La mayoría de las demostraciones concernientes a imágenes de conjuntos se han omitido. Para reducir el número de paréntesis en la formulación de estos teoremas, usamos la convención de que '$\cup$', '$\cap$', '$\sim$' dominan a '``'. Así, $R``A \cup B$ es $(R``A) \cup B$ no $R``(A \cup B)$.

Teorema 34. $y \in R``A \leftrightarrow (\exists x)(x\, R\, y \;\&\; x \in A)$.

Teorema 35. $R``(A \cup B) = R``A \cup R``B$.

Demostración.

$$\begin{aligned} y \in R``(A \cup B) &\leftrightarrow (\exists x)(x\, R\, y \;\&\; x \in A \cup B) \\ &\leftrightarrow (\exists x)(x\, R\, y \;\&\; x \in A) \vee (\exists x)(x\, R\, y \;\&\; x \in B) \\ &\leftrightarrow y \in R``A \vee y \in R``B \\ &\leftrightarrow y \in R``A \cup R``B. \qquad \text{Q.E.D.} \end{aligned}$$

Teorema 36. $R``(A \cap B) \subseteq R``A \cap R``B$.

Un ejemplo sencillo muestra que la inclusión no puede convertirse en identidad, para este teorema. Sea

$$R_1 = \{\langle 1, 3\rangle, \langle 2, 3\rangle\},$$
$$A_1 = \{1\},$$
$$B_1 = \{2\}.$$

Entonces,

$$R_1``(A_1 \cap B_1) = 0,$$

pero

$$R_1``A_1 \cap R_1``B_1 = \{3\}.$$

* La notación $R``A$ sigue la de Whitehead y Russell.

Teorema 37. $R``A \sim R``B \subseteq R``(A \sim B)$.

Demostración.

$$\begin{aligned} & y \in R``A \sim R``B \\ & \leftrightarrow y \in R``A \;\&\; y \notin R``B \\ & \leftrightarrow (\exists x)(x\, R\, y \;\&\; x \in A) \;\&\; -(\exists z)(z\, R\, y \;\&\; z \in B) \\ & \leftrightarrow (\exists x)(x\, R\, y \;\&\; x \in A) \;\&\; (\forall z)(z\, R\, y \rightarrow z \notin B) \\ & \rightarrow (\exists x)(x\, R\, y \;\&\; x \in A \;\&\; x \notin B) \\ & \rightarrow (\exists x)(x\, R\, y \;\&\; x \in A \sim B) \\ & \rightarrow y \in R``(A \sim B). \qquad \text{Q.E.D.} \end{aligned}$$

Los conjuntos particulares usados en el ejemplo que precede a este teorema pueden usarse para mostrar de nuevo que la inclusión no puede convertirse en identidad:

$$R_1``A_1 \sim R_1``B_1 = 0$$
$$R_1``(A_1 \sim B_1) = R_1``A_1 = \{3\}.$$

Teorema 38. $A \subseteq B \rightarrow R``A \subseteq R``B$.

Teorema 39. $R``A = 0 \leftrightarrow \mathfrak{D}R \cap A = 0$.

El siguiente teorema es algo sorprendente.

Teorema 40. $\mathfrak{D}R \cap A \subseteq \breve{R}``(R``A)$.

Demostración.

$$\begin{aligned} x \in \mathfrak{D}R \cap A &\leftrightarrow (\exists y)(x\, R\, y \;\&\; x \in A) \\ &\rightarrow (\exists y)(x\, R\, y \;\&\; y \in R``A) \\ &\rightarrow (\exists y)(y\, \breve{R}\, x \;\&\; y \in R``A) \\ &\rightarrow x \in \breve{R}``(R``A). \qquad \text{Q.E.D.} \end{aligned}$$

Los conjuntos particulares R_1, A_1, y B_1 muestran por qué la inclusión no puede reemplazarse por la identidad y por qué la equivalencia de la línea (1) de la demostración debe debilitarse, convirtiéndose en una implicación en la línea (2).

$$\mathfrak{D}R_1 \cap A_1 = \{1\},$$

pero

$$\breve{R}_1``(R_1``A_1) = \{1, 2\}.$$

Teorema 41. $(R``A) \cap B \subseteq R``(A \cap \breve{R}``B)$.

Demostración.

$$
\begin{aligned}
& y \in (R``A) \cap B \\
& \leftrightarrow (\exists x)(x\, R\, y \;\&\; x \in A \;\&\; y \in B) \\
& \rightarrow (\exists x)(x\, R\, y \;\&\; x \in \breve{R}``B \;\&\; x \in A) \\
& \leftrightarrow (\exists x)(x\, R\, y \;\&\; x \in A \cap \breve{R}``B) \\
& \leftrightarrow y \in R``(A \cap \breve{R}``B). \qquad \text{Q.E.D.}
\end{aligned}
$$

En la última sección de este capítulo se dan algunos otros teoremas sobre las operaciones restricción e imagen, bajo la hipótesis adicional de que R es una función.

EJERCICIOS

1. Dar un contra-ejemplo para el enunciado:

$$\mathfrak{D}A = 0 \rightarrow A = 0.$$

2. ¿Cuáles (si los hay) de los teoremas análogos a 5, 6, 7 se cumplen para la operación campo $\mathfrak{F}$?

3. Demostrar que el producto cartesiano entre dos conjuntos es una relación.

4. Demostrar el teorema 3.

5. ¿Bajo qué condiciones

$$\mathfrak{D}(A \times B) = A?$$

6. ¿Bajo qué condiciones

$$\mathfrak{F}(A \times B) = A \cup B?$$

7. Demostrar los teoremas 6 y 7.

8. Dar un contra-ejemplo al enunciado

$$\mathfrak{D}A \cap \mathfrak{D}B \subseteq \mathfrak{D}(A \cap B).$$

9. Demostrar los teoremas 8, 9 y 10.

10. Dar un contra-ejemplo al enunciado

$$\breve{\breve{A}} = A.$$

11. Demostrar que

$$\overbrace{A \times B} = B \times A.$$

12. Demostrar los teoremas 13 y 14.

13. Demostrar los teoremas 16 y 17.

14. Demostrar que

$$(A \times B)/(A \times B) \subseteq A \times B.$$

15. Demostrar los teoremas 19 a 22.

16. Demostrar los teoremas 24 y 25.

17. Dar un contra-ejemplo al enunciado

$$(A/B) \cap (A/C) \subseteq A/(B \cap C).$$

18. Demostrar el teorema 27.

19. Demostrar que

$$x \in \mathfrak{D}A \rightarrow x\, A/\breve{A}x.$$

20. Determinar si es verdadero que:

(a) $R/\bigcup A = \bigcup(R/A)$,

(b) $(\forall R)(R \in A \rightarrow R/R \subseteq R) \rightarrow \bigcup A/\bigcup A \subseteq \bigcup A$,

(c) $(\forall R)(R \in A \rightarrow R/R \subseteq R) \rightarrow \bigcap A/\bigcap A \subseteq \bigcap A$,

(d) $(\forall R)(R \in A \rightarrow R/\breve{R} = R) \rightarrow \bigcup A/\overbrace{\bigcup A} = \bigcup A$,

(e) $(\forall R)(R \in A \rightarrow R/\breve{R} = R) \rightarrow \bigcap A/\overbrace{\bigcap A} = \bigcap A$.

21. Sea R la relación numérica tal que

$$x\, R\, y \leftrightarrow x + y = 1.$$

Sea A el conjunto de los números primos entre 10 y 20. Describir explícitamente $R|A$.

22. Demostrar el teorema 28.

23. Demostrar los teoremas 29 a 31.

24. Demostrar los teoremas 32 y 33.

25. Sea R la relación numérica tal que

$$x\, R\, y \leftrightarrow 2x + 1 = y.$$

Sea A el conjunto de los enteros.

(a) ¿Qué conjunto es $\breve{R}``A$?
(b) ¿Qué conjunto es $R``A$?
(c) ¿Qué conjunto es $(R/R)``A$?

26. Demostrar el teorema 34.

27. Demostrar el teorema 36.

28. Demostrar los teoremas 38 y 39.

29. Demostrar que $R``0 = 0$.

§ **3.2 Relaciones de orden.** En todos los dominios de la matemática y en muchas ramas de las ciencias empíricas se presentan relaciones que ordenan conjuntos de objetos. Hay un sin fin de teoremas interesantes acerca de varias relaciones de orden y sus propiedades. Aquí consideramos solamente algunas de las más útiles; entre los ejercicios se incluye un gran número de teoremas adicionales.

Comenzamos con las propiedades fundamentales de reflexividad, simetría, transitividad y otras similares, en términos de las cuales definimos diferentes tipos de orden. Debido a que estas nociones son tan familiares, los ejemplos ilustrativos se dan sólo muy rara vez.*

* Se pueden encontrar ejemplos y aplicaciones elementales, entre otros, en Suppes (1957, capítulo 10).

Con respecto a la generalidad de la definición, la situación es la misma que en la sección anterior: las definiciones valen para conjuntos arbitrarios, no sólo para relaciones. Sin embargo, para aumentar el contenido intuitivo inmediato de los teoremas, en esta sección usaremos sistemáticamente las letras 'R', 'S', 'T', como variables de conjuntos en aquellos contextos en los cuales las ideas consideradas se refieren, de manera natural, a relaciones. Pero debe entenderse muy bien que el uso de las variables 'R', 'S', 'T' no implica restricción formal alguna a las definiciones y teoremas. Por ejemplo, definimos la propiedad de transitividad para conjuntos arbitrarios R, no solamente para relaciones. También, sin introducir una definición numerada, usamos en adelante la notación familiar: '$x, y \in A$' para '$x \in A$ & $y \in A$' y '$x,y,z \in A$' para '$x \in A$ & $y \in A$ & $z \in A$', etc.

Comenzamos con ocho definiciones básicas.

Definición 10. R *es reflexiva en* A $\leftrightarrow (\forall x)(x \in A \rightarrow x \, R \, x)$.

Definición 11. R *es antirreflexiva en* A $\leftrightarrow (\forall x)(x \in A \rightarrow -(x \, R \, x))$.

Definición 12. R *es simétrica en* A $\leftrightarrow (\forall x)(\forall y)(x,y \in A \; \& \; x \, R \, y \rightarrow y \, R \, x)$.

Definición 13. R *es asimétrica en* A $\leftrightarrow (\forall x)(\forall y)(x,y \in A \; \& \; x \, R \, y \rightarrow -(y \, R \, x))$.

Definición 14. R *es antisimétrica en* A $\leftrightarrow (\forall x)(\forall y)(x,y \in A \; \& \; x \, R \, y \; \& \; y \, R \, x \rightarrow x = y)$.

Definición 15. R *es transitiva en* A $\leftrightarrow (\forall x)(\forall y)(\forall z)(x,y,z \in A \; \& \; x \, R \, y \; \& \; y \, R \, z \rightarrow x \, R \, z)$.

Definición 16. R *es conexa en* A $\leftrightarrow (\forall x)(\forall y)(x,y \in A \; \& \; x \neq y \rightarrow x \, R \, y \lor y \, R \, x)$.

Definición 17. R *es fuertemente conexa en* A $\leftrightarrow (\forall x)(\forall y)(x,y \in A \rightarrow x \, R \, y \lor y \, R \, x)$.

Con el objeto de relacionar a las ocho propiedades anteriores las operaciones introducidas en la sección precedente, es más elegante considerar las propiedades unarias correspondientes, esto es, referirse a relaciones que son reflexivas, en vez que reflexivas en algún conjunto A, etc. Las definiciones generales que se acaban de dar serán útiles más tarde. Por brevedad, definimos las ocho propiedades unarias, con un recorte; las definiciones son obvias: simplemente tomamos A como el campo de la relación.

Definición 18. R *es*

$$\left\{\begin{matrix}\textit{reflexiva}\\ \vdots\\ \textit{fuertemente}\\ \textit{conexa.}\end{matrix}\right\} \leftrightarrow R \textit{ es} \left\{\begin{matrix}\textit{reflexiva}\\ \vdots\\ \textit{fuertemente}\\ \textit{conexa.}\end{matrix}\right\} \textit{en } \mathfrak{F}R.$$

Para formular los teoremas pedidos, necesitamos la noción de relación de identidad en un conjunto. Es claro, por el teorema 50 del capítulo 2:

$$\{x: x = x\} = 0$$

que no podemos definir una relación de identidad general apropiada, pero lo que podemos hacer es definir, para cada conjunto A, la relación idéntica $\mathcal{I}A$, sobre A. (Así, el símbolo '$\mathcal{I}$' no es una constante individual que designa la relación de identidad, sino un símbolo de operación unaria.)

Definición 19. $\mathcal{I}A = \{\langle x, x\rangle: x \in A\}$.

Además de la definición, para propósitos de trabajo necesitamos el teorema usual que garantice que $\mathcal{I}A$ es el conjunto vacío solamente cuando esperamos que lo sea.

Teorema 42. $x \, \mathcal{I}A \, x \leftrightarrow x \in A$.

Demostración. Puesto que

$$\langle x, x\rangle = \{\{x\}, \{x, x\}\} = \{\{x\}\},$$

es claro que

$$\mathcal{I}A \subseteq \mathcal{P}\mathcal{P}A.$$

Más aún, es fácil demostrar que

(1) $x \in A \rightarrow \{\{x\}\} \in \mathcal{P}\mathcal{P}A.$

En virtud del esquema axiomático de separación y de la definición de abstracción, podemos usar (1) para obtener el teorema. Q.E.D.

En ésta y en las demostraciones subsiguientes, en las cuales usamos el esquema axiomático de separación para demostrar la existencia de algún conjunto, nos restringimos a la consideración de dos pasos definitivos: Decidir cuál conjunto, cuya existencia se conoce, tiene como subconjunto al conjunto pedido y luego demostrar que la satisfacción de la condición apropiada φ en el axioma (aquí φ es '$x \in A$') implica pertenencia al conjunto más grande. Quizás es conveniente observar que la demostración formal no requiere la inferencia de que

$$\mathcal{I}A \subseteq \mathcal{P}\mathcal{P}A,$$

aunque esto se sigue fácilmente. Pero la búsqueda de un conjunto que tenga a $\mathcal{I}A$ como subconjunto es una consideración estratégica esencial para hallar una demostración válida.

Formulamos, sin demostración, tres teoremas sencillos concernientes a las relaciones de identidad.

Teorema 43. $\mathfrak{D}\mathcal{I}A = A.$

Teorema 44. $\mathcal{I}A/\mathcal{I}A = \mathcal{I}A.$

Teorema 45. *R es una relación*

$$\leftrightarrow (\mathcal{I}\mathfrak{D}R)/R = R.$$

Los ocho teoremas que siguen podrían usarse como definiciones y así se toman frecuentemente. En las demostraciones se usan propiedades familiares de las operaciones, sin referencia explícita a los teoremas apropiados.

Teorema 46. *R es reflexiva* $\leftrightarrow \mathcal{I}\mathfrak{F}R \subseteq R.$

Demostración. [Necesidad]. Por la definición 17, todo elemento de $\mathcal{I}\mathfrak{F}R$ es de la forma $\langle x, x\rangle$, por tanto, por el teorema 28, $x \in \mathfrak{F}R$, y entonces se sigue, de la hipótesis de que R es reflexiva, que $\langle x, x\rangle \in R$.

[Suficiencia]. Sea x un elemento arbitrario de $\mathfrak{F}R$. Ya que nuestra hipótesis es la de que

$$\mathcal{I}\mathfrak{F}R \subseteq R,$$

se sigue, de una vez, que

$$\langle x, x\rangle \in \mathrm{R},$$

pero entonces R es reflexiva. Q.E.D.

Esta demostración es completamente trivial, pero ilustra el acceso a las de los siete teoremas restantes, la mayor parte de los cuales no se demuestra aquí.

Teorema 47. *R es antirreflexiva*
$\leftrightarrow R \cap \mathcal{I}\mathfrak{F}R = 0.$

Teorema 48. *R es simétrica*
$\leftrightarrow \breve{\breve{R}} = \breve{R}.$

Teorema 49. *R es asimétrica*
$\leftrightarrow R \cap \breve{R} = 0.$

Teorema 50. *R es antisimétrica*
$\leftrightarrow R \cap \breve{R} \subseteq \mathcal{I}\mathfrak{D}R.$

Teorema 51. *R es transitiva*
$\leftrightarrow R/R \subseteq R.$

Demostración. [Necesidad]. Si

$$x\,R/R\,y,$$

entonces existe un z tal que

$$x\,R\,z\;\&\;z\,R\,y,$$

por tanto, por la hipótesis de transitividad,

$$x\,R\,y.$$

[Suficiencia]. A partir de nuestra hipótesis de que

$$R/R \subseteq R$$

tenemos, de una vez,

(1) $(\exists z)\,(x\,R\,z\;\&\;z\,R\,y) \rightarrow x\,R\,y,$

pero es un hecho familiar de lógica cuantificacional que (1) es equivalente lógicamente a

(2) $x\,R\,z\;\&\;z\,R\,y \rightarrow x\,R\,y.$ Q.E.D.

Teorema 52. *R es conexa* $\leftrightarrow (\mathfrak{F}R \times \mathfrak{F}R)$
$\sim \mathcal{I}\mathfrak{F}R \subseteq R \cup \breve{R}.$

Demostración. [Necesidad]. Si

(1) $x\,[(\mathfrak{F}R \times \mathfrak{F}R) \sim \mathfrak{I}\mathfrak{F}R]\,y,$

entonces

(2) $x \in \mathfrak{F}R \;\&\; y \in \mathfrak{F}R \;\&\; x \neq y,$

pero (2), junto con la hipótesis de que R es conexa, da:

(3) $x\,R\,y \vee y\,R\,x,$

por consiguiente,

(4) $x(R \cup \breve{R})y.$

[Suficiencia]. Queremos deducir (3) de (2), bajo la hipótesis de que

(5) $(\mathfrak{F}R \times \mathfrak{F}R) \sim \mathfrak{I}\mathfrak{F}R \subseteq R \cup \breve{R}.$

Ahora, (5) asegura que (1) implica (4); pero (1) es equivalente a (2) y (3) es equivalente a (4). Q.E.D.

Teorema 53. *R es fuertemente conexa* $\leftrightarrow \mathfrak{F}R \times \mathfrak{F}R = R \cup \breve{R}.$

En los ejercicios se formulan numerosos hechos adicionales: la asimetría implica la antirreflexividad; la simetría y la transitividad implican la reflexividad; todas las ocho propiedades enunciadas en la definición 18 son invariantes con respecto a la operación conversa, etc.

Ahora usamos esas ocho propiedades para definir cinco tipos de relaciones de orden; los tipos no son mutuamente exclusivos. Por ejemplo, toda ordenación parcial es también una cuasi-ordenación.

Definición 20. *R es una cuasi-ordenación de A* $\leftrightarrow$ *R es reflexiva y transitiva en A.*

Definición 21. *R es una ordenación parcial de A* $\leftrightarrow$ *R es reflexiva, antisimétrica y transitiva en A.*

Definición 22. *R es una ordenación simple de A* $\leftrightarrow$ *R es antisimétrica, transitiva y fuertemente conexa en A.*

Definición 23. *R es una ordenación parcial estricta de A* $\leftrightarrow$ *R es asimétrica y transitiva en A.*

Definición 24. *R es una ordenación simple estricta de A* $\leftrightarrow$ *R es asimétrica, transitiva y conexa en A.*

Análogamente a la definición 16, definimos también, en masa, los predicados unarios apropiados.

Definición 25. *R es una*

$$\left\{\begin{array}{c}\textit{cuasi-}\\\textit{ordenación}\\ \vdots \\ \textit{Ordenación}\\\textit{simple estricta}\end{array}\right\} \leftrightarrow R \text{ } \textit{es una} \left\{\begin{array}{c}\textit{cuasi-}\\\textit{ordenación}\\ \vdots \\ \textit{ordenación}\\\textit{simple estricta}\end{array}\right\} \textit{de } \mathfrak{F}R.$$

Las definiciones 20 a 24 serán útiles en el capítulo 6, el cual trata de la construcción de los números reales. Por el momento formulamos algunos teoremas obvios acerca de las ordenaciones de la definición 25.

Teorema 54. *R es una ordenación parcial* $\rightarrow$ *R es una cuasi-ordenación.*

Teorema 55. *R es una ordenación simple* $\rightarrow$ *R es una ordenación parcial.*

Teorema 56. *R es una ordenación simple* $\rightarrow$ $\breve{R}$ *es una ordenación simple.*

Teorema 57. *R y S son cuasi-ordenaciones* $\rightarrow$ $R \cap S$ *es una cuasi-ordenación.*

Demostración. Necesitamos demostrar que $R \cap S$ es reflexiva y transitiva. Sea x un elemento arbitrario de $\mathfrak{F}(R \cap S)$. Entonces, $x \in \mathfrak{F}R$ y $x \in \mathfrak{F}S$, por tanto, por la hipótesis,

$$x\,R\,x \;\&\; x\,S\,x,$$

luego

$$x\; R \cap S\; x.$$

La transitividad se establece por las siguientes implicaciones; la segunda línea se sigue de la primera, sobre la base de la hipótesis del teorema:

$$x\,R \cap S\,y \;\&\; y\,R \cap S\,z$$
$$\rightarrow x\,R\,y \;\&\; y\,R\,z \;\&\; x\,S\,y \;\&\; y\,S\,z$$
$$\rightarrow x\,R\,z \;\&\; x\,S\,z$$
$$\rightarrow x\,R \cap S\,z.$$

Q.E.D.

La unión de dos cuasi-ordenaciones cualesquiera no es una cuasi-ordenación. Por ejemplo, sea

$$R = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 1, 2\rangle\}$$

y

$$S = \{\langle 2, 2\rangle, \langle 3, 3\rangle, \langle 2, 3\rangle\},$$

entonces R y S son cuasi-ordenaciones, pero $R \cup S$ no lo es, pues no cumple la propiedad transitiva. Sin embargo, si los campos de R y S son mutuamente disjuntos, entonces, su unión es una cuasi-ordenación, como se establece en el teorema siguiente;

Teorema 58. *R y S son cuasi-ordenaciones* $\& \mathcal{F}R \cap \mathcal{F}S = 0 \rightarrow R \cup S$ *es una cuasi-ordenación.*

Un enunciado preciso sobre la relación entre ordenaciones parciales y ordenaciones parciales estrictas lo dan los dos teoremas siguientes.

Teorema 59. *R es una ordenación parcial* $\rightarrow R \sim \mathcal{I}\mathcal{F}R$ *es una ordenación parcial estricta.*

Teorema 60. *R es una ordenación parcial estricta* $\rightarrow R \cup \mathcal{I}\mathcal{F}R$ *es una ordenación parcial.*

En el teorema siguiente se expresa el sentido en el cual una ordenación simple, o una ordenación simple estricta, es completa.

Teorema 61. $R \subseteq S \subseteq A \times A$ $\&$ *R y S son ordenaciones estrictas simples de* $A \rightarrow R = S$.

Ahora queremos introducir la importante noción de relación bien-ordenante de un conjunto. Si R es una ordenación simple estricta en A, entonces R bien-ordena A, si todo subconjunto no vacío de A tiene un primer elemento o elemento mínimo (bajo la relación R). En realidad, como veremos, necesitamos suponer solamente que R es conexa en A, más bien que suponer que es una ordenación simple estricta en A. La asimetría y la transitividad de R en A son entonces demostrables, según el hecho de que cualquier elemento de A, excepto el último (bajo la relación R), tiene un sucesor inmediato.

Puesto que esta noción de buena ordenación es algo más sutil que las nociones de orden introducidas previamente, será útil considerar varios ejemplos antes de la definición formal y los teoremas. En estos ejemplos, como en los anteriores, usaremos enteros; en verdad, números reales, aun cuando estas entidades no se han definido aún formalmente dentro de nuestro sistema de teoría de conjuntos.

Sea N el conjunto de los enteros positivos. Entonces N es bien ordenado por la relación *menor que*, ya que todo subconjunto no vacío de N tiene un primer elemento, a saber, el mínimo entero del conjunto. Por otra parte, N no es bien ordenado por la relación *mayor que*, pues muchos subconjuntos carecen de primeros elementos, en particular el mismo N. N no tiene un primer elemento, con respecto a $>$, precisamente porque no hay un entero mayor que todos.

La noción de buena ordenación se concibe de modo que, a diferencia de las otras propiedades de orden consideradas hasta aquí, no es invariante bajo la operación conversa, esto es, si R es una buena ordenación, no se sigue que $\breve{R}$ sea una buena ordenación. Ya tenemos un ejemplo de esto: $<$ bien-ordena N, pero $\breve{<}$ no. Para un ejemplo algo diferente, consideremos

$$A = \left\{0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \cdots, \frac{n-1}{n}, \cdots, 1\right\},$$

o sea,

$$A = \left\{\frac{n-1}{n} : n \text{ es un entero positivo}\right\} \cup \{1\}.$$

El conjunto A es bien ordenado por $<$, pero no por $\breve{<}$, esto es, no por $>$. En este caso, el mismo conjunto A tiene un primer elemento bajo la relación $>$, pero el subconjunto $A \sim \{1\}$ no lo tiene.

Por medio de una modificación apropiada de la definición de R-primer elemento de A podemos construir la definición de buena ordenación de tal manera que $<$ o $\leq$ bien-ordena N, esto es, podemos hacer que nuestras buenas ordenaciones sean ordenaciones simples o también que sean ordenaciones simples estrictas. La escogencia es, en alto grado, arbitraria; podemos, si queremos, considerar una buena ordenación que no sea ninguna de las dos. Por ejemplo, si $A = \{1, 2, 3\}$ y

$$R = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 1, 2\rangle, \langle 2, 3\rangle, \langle 1, 3\rangle\},$$

entonces intuitivamente, R bien-ordena A aun cuando R no es ni ordenación simple ni ordenación simple estricta de A. Pero esta generalización es trivial y existe una razón convincente para escoger ordenaciones simples estrictas más bien que ordenaciones simples; la relación de pertenencia es una ordenación simple estricta de los números ordinales tal como los definiremos y —como veremos en el capítulo 7— hay una conexión natural entre cualquier buena ordenación de un conjunto y la buena ordenación de los ordinales por la relación de pertenencia.

Ahora nos referimos a los desarrollos formales. Es conveniente, técnicamente, distinguir entre la noción de elemento *mínimo* y la de *primer* elemento. Un elemento mínimo no tiene predecesores, mientras que un primer elemento precede a todo otro elemento. Claramente, todo primer elemento es mínimo pero no recíprocamente. Para demostrar la asimetría de las buenas ordenaciones es más simple usar el concepto de elemento mínimo en su definición.

Definición 26. *x es un elemento R-mínimo de $A \leftrightarrow x \in A$ & $(\forall y)$ $(y \in A \rightarrow -(yRx))$.*

Un rasgo obvio de esta definición es el de que si $R \cap (A \times A)$ es vacío, entonces todo elemento de A es un elemento R-mínimo. Sin embargo, tales situaciones degeneradas no son de mucho interés; en el caso de buenas ordenaciones procuramos la unicidad del elemento mínimo.

Definición 27. *x es un R-primer elemento de $A \leftrightarrow x \in A$ & $(\forall y)(y \in A$ & $x \neq y \rightarrow xRy)$.*

En seguida definimos buenas ordenaciones. Luego formulamos una sencilla condición necesaria y suficiente, en términos de asimetría y primer elemento en lugar del concepto de elemento mínimo.

Definición 28. *R bien-ordena $A \leftrightarrow R$ es conexa en A & $(\forall B)$ $(B \subseteq A$ & $B \neq 0 \rightarrow B$ tiene un elemento R-mínimo).*

Ahora demostraremos que, bajo esta definición, R es asimétrica y transitiva.

Teorema 62. *R bien-ordena $A \rightarrow R$ es asimétrica y transitiva en A.*

Demostración. Para establecer la asimetría, supongamos, por el camino de la contradicción, que hay elementos x y y en A tales que $x\,R\,y$ y $y\,R\,x$. Entonces, contrario a la hipótesis de que R bien-ordena A, el subconjunto no vacío $\{x, y\}$ de A no tiene elemento R-mínimo. Para la transitividad, supongamos que para algunos elementos $x, y, z \in A$, tenemos $x\,R\,y$ y $y\,R\,z$, pero no $x\,R\,z$. Puesto que R es conexa en A, debemos tener entonces: $z\,R\,x$. Sin embargo, el subconjunto $\{x,y,z\}$ no tiene entonces un elemento R-mínimo, pues $z\,R\,x$ desecha x como elemento R-mínimo, $x\,R\,y$ desecha y y $y\,R\,z$ desecha z. Por tanto, nuestra suposición es absurda. Q.E.D.

Dejamos como ejercicio la demostración de los tres teoremas siguientes.

Teorema 63. *R bien-ordena $A \leftrightarrow R$ es asimétrica y conexa en A & $(\forall B)(B \subseteq A$ & $B \neq 0 \rightarrow B$ tiene un R-primer elemento).*

Teorema 64. *R bien-ordena A & $A \neq 0 \rightarrow A$ tiene un único R-primer elemento.*

Teorema 65. *R bien-ordena A & $B \subseteq A \rightarrow R$ bien-ordena B.*

Por otra parte, no es, desde luego, verdadero en general que, si R bien-ordena A y $S \subseteq R$, entonces S bien-ordena A.

Nuestra tarea siguiente es demostrar el teorema acerca de sucesores inmediatos únicos. Se necesitan dos definiciones.

Definición 29. *y es un sucesor R-inmediato de $x \leftrightarrow x\,R\,y$ & $(\forall z)$ $(x\,R\,z \rightarrow z = y \vee y\,R\,z)$.*

Definición 30. *x es un elemento R-último de $A \leftrightarrow x \in A$ & $(\forall y)(y \in A$ & $x \neq y \rightarrow y\, R\, x)$.*

La definición de último elemento es obviamente similar a la de primer elemento. En efecto, tenemos:

Teorema 66. *x es un elemento R-último de $A \leftrightarrow x$ es un elemento $\breve{R}$-primero de A.*

Ahora puede establecerse el resultado concerniente a los sucesores inmediatos.

Teorema 67. *R bien-ordena A & $x \in A$ & x no es un elemento R-último de $A \rightarrow x$ tiene un único sucesor R-inmediato.*

Demostración. Considérese $B = \{y: x\, R\, y\}$. Por hipótesis el conjunto B no es vacío, ya que x no es el último elemento de la ordenación y se ve fácilmente que B tiene un primer elemento único, que es el sucesor inmediato de x. Q.E.D.

En la teoría de números ordinales será conveniente tener disponibles la noción de una R-sección y ciertos hechos acerca de tales secciones. Se introduce también la noción, íntimamente ligada a la anterior, de R-segmento de un conjunto, generado por un elemento.

Definición 31. *B es una R-sección de*

$$A \leftrightarrow B \subseteq A \;\&\; A \cap \breve{R}``B \subseteq B.$$

Así que un conjunto B es una R-sección de un conjunto A si todos los R-predecesores en A de elementos de B pertenecen a B; obviamente, $\breve{R}``B$ es precisamente el conjunto de los R-predecesores de elementos de B. Si, por ejemplo,

$$A = \{1, 2, 3, 4\}$$
$$B_1 = \{1, 2\}$$
$$B_2 = 0$$
$$B_3 = \{2, 3\},$$

entonces B_1 y B_2 son $<$-secciones de A, pero B_3 no lo es, puesto que $1 < 2$ y $1 \in A \sim B_3$. Por otra parte, B_1 no es una $>$-sección de A, puesto que $3 > 2$ y $3 \in A \sim B_1$.

Definición 32. $\mathcal{S}(A, R, x) = \{y: y \in A$ & $y\, R\, x\}$.

La notación: $\mathcal{S}(A, R, x)$ se lee: *el R-segmento de A generado por x.* El conjunto $\mathcal{S}(A, R, x)$ es precisamente el conjunto de los R-predecesores de x que son también elementos de A.

Teorema 68. *$x \in A$ & R es transitiva en $A \rightarrow \mathcal{S}(A, R, x)$ es una R-sección de A.*

Demostración. Supongamos que $y \in \mathcal{S}(A, R, x)$. Necesitamos demostrar que los R-predecesores de y que son elementos de A, son también elementos de $\mathcal{S}(A, R, x)$. Sea z uno de tales R-predecesores de y, esto es,

$$z \in A \cap \breve{R}``\{y\},$$

por tanto,

(1) $\qquad z\, R\, y.$

Puesto que $y \in \mathcal{S}(A, R, x)$, tenemos

(2) $\qquad y\, R\, x$

luego, por la hipótesis de transitividad, se sigue de (1) y (2)

$$z\, R\, x,$$

de lo cual concluimos: $z \in \mathcal{S}(A, R, x)$. Q.E.D.

Sobre la base de este teorema se demuestra fácilmente que

Teorema 69. *R bien-ordena $A \rightarrow (B$ es una R-sección de A & $B \neq A \leftrightarrow (\exists x)(x \in A$ & $B = \mathcal{S}(A, R, x)))$.*

Algunos conceptos ulteriores de orden tales como los de una *R-cota superior* de x, un *R-supremo* de x y un *retículo* se presentan en los ejercicios.

EJERCICIOS

1. Demostrar lo siguiente:
   (a) R es asimétrica $\rightarrow R$ es antirreflexiva.
   (b) R es asimétrica $\rightarrow R$ es antisimétrica.
   (c) $\mathcal{I}\, A$ es simétrica y antisimétrica.
   (d) R es relación simétrica y antisimétrica $\rightarrow (\exists A)(R = \mathcal{I} A)$.
   (e) R es simétrica y transitiva $\rightarrow R$ es reflexiva.
   (f) R es fuertemente conexa $\rightarrow R$ es conexa.
2. Demostrar que
   R es reflexiva $\rightarrow \mathfrak{D}R = \mathfrak{D}\breve{R}$.
3. Demostrar que
   R es una relación $\rightarrow$ (R es simétrica $\leftrightarrow R = \breve{R}$).
4. Demostrar los teoremas 43 a 45.

5. Demostrar los teoremas 47 a 49.
6. Demostrar los teoremas 50 y 51.
7. Demostrar el teorema 53.
8. Demostrar lo siguiente:
   (a) R es reflexiva $\rightarrow \breve{R}$ es reflexiva.
   (b) R y S son reflexivas $\rightarrow R \cup S$ es reflexiva.
   (c) R es antirreflexiva $\rightarrow \breve{R}$ es antirreflexiva.
   (d) R y S son antirreflexivas $\rightarrow R \cap S$, $R \cup S$ y $R \sim S$ son antirreflexivas.
   (e) R es simétrica $\rightarrow \breve{R}$ es simétrica.
   (f) R y S son simétricas $\rightarrow R \cap S$, $R \cup S$ y $R \sim S$ son simétricas.
   (g) R es asimétrica $\rightarrow \breve{R}$, $R \cap S$ y $R \sim S$ son asimétricas.
   (h) R es antisimétrica $\rightarrow \breve{R}, R \cap S$ y $R \sim S$ son antisimétricas.
   (i) R es transitiva $\rightarrow \breve{R}$ es transitiva.
   (j) R es conexa $\rightarrow \breve{R}$ es conexa.
   (k) R es fuertemente conexa $\rightarrow \breve{R}$ es fuertemente conexa.
   (l) $R \cup \mathscr{I}\mathfrak{F}R$ es reflexiva.
   (m) $R \sim \mathscr{I}\mathfrak{F}R$ es antirreflexiva.
   (n) R es asimétrica $\rightarrow R \cup \mathscr{I}\mathfrak{F}R$ es antisimétrica.
   (o) R es antisimétrica $\rightarrow R \sim \mathscr{I}\mathfrak{F}R$ es asimétrica.
   (p) R es transitiva $\rightarrow R \cup \mathscr{I}\mathfrak{F}R$ es transitiva.
   (q) R es transitiva y antisimétrica $\rightarrow R \sim \mathscr{I}\mathfrak{F}R$ es transitiva.
9. Dar un contra-ejemplo para cada una de las siguientes aserciones:
   (a) R y S son reflexivas $\rightarrow R \sim S$ es reflexiva.
   (b) R y S son reflexivas $\rightarrow R/S$ es reflexiva.
   (c) R y S son antirreflexivas $\rightarrow R/S$ es antirreflexiva.
   (d) R y S son simétricas $\rightarrow R/S$ es simétrica.
   (e) R y S son asimétricas $\rightarrow R \cup S$ es asimétrica.
   (f) R y S son asimétricas $\rightarrow R/S$ es asimétrica.
   (g) R y S son antisimétricas $\rightarrow R \cup S$ es antisimétrica.
   (h) R y S son transitivas $\rightarrow R \cup S$ es transitiva.
   (i) R y S son transitivas $\rightarrow R \sim S$ es transitiva.
   (j) R y S son transitivas $\rightarrow R/S$ es transitiva.
   (k) R y S son conexas $\rightarrow R \cap S$ es conexa.
   (l) R y S son conexas $\rightarrow R \cup S$ es conexa.
   (m) R y S son conexas $\rightarrow R \sim S$ es conexa.
   (n) R y S son conexas $\rightarrow R/S$ es conexa.
10. Demostrar los teoremas 54 a 56.
11. Demostrar los teoremas 58 a 60.
12. Dar un contra-ejemplo al enunciado de que, si $R \sim \mathscr{I}\mathfrak{F}R$ es una ordenación parcial estricta, entonces R es una ordenación parcial.
13. Demostrar el teorema 61.
14. Considérense los siguientes conjuntos y relaciones:

N = conjunto de los enteros positivos.
I = conjunto de los enteros (negativos y no negativos).
Neg = conjunto de los enteros negativos.
Rac = conjunto de los números racionales no negativos.

$$xR_1y \leftrightarrow x < y + 2,$$
$$xR_2y \leftrightarrow x < y - 2,$$
$$xR_3y \leftrightarrow |x| < |y| \vee (|x| = |y| \;\&\; x < y),$$
$$xR_4y \leftrightarrow |x| > |y| \vee (|x| = |y| \;\&\; x > y).$$

¿Cuáles de las siguientes afirmaciones son verdaderas? Para aquellas que son falsas dar un contra-ejemplo explícito.
   (a) $<$ bien-ordena Neg
   (b) $>$ bien-ordena Neg
   (c) $<$ bien-ordena I
   (d) $<$ bien-ordena Rac
   (e) R_1 bien-ordena N
   (f) R_2 bien-ordena N
   (g) R_3 bien-ordena I
   (h) R_3 bien-ordena Neg
   (i) $\breve{R}_3$ bien-ordena N
   (j) $\breve{R}_4$ bien-ordena Neg
   (k) R_4 bien-ordena I
   (l) $\breve{R}_4$ bien-ordena I
   (m) $\breve{R}_4$ bien-ordena Rac
15. Demostrar el teorema 63.
16. Demostrar los teoremas 64 y 65.
17. Considérese el conjunto
$A = \{< x, y > : x$ y y son enteros positivos$\}$.
Defínase una relación que bien-ordene A.
18. Considérese el conjunto
$B = \{< x, y > : x$ y y son enteros negativos o no negativos$\}$.
Defínase una relación que bien-ordene B.
19. Definir una relación que bien-ordene los números racionales no negativos. (Puesto que los racionales no negativos no son bien-ordenados en magnitud, esto es, bien-ordenados por *menor que*, debe usarse algún otro artificio; es esencial usar el hecho de que todo número racional es la razón de dos enteros.)
20. Sean

N = conjunto de los enteros positivos

$$S_1 = \{x : x \in N \;\&\; x < 10^6\}$$

$x R_1 y$ si y sólo si $x < y + 1$.

Entonces, ¿cuáles de las siguientes afirmaciones son verdaderas?
   (a) S_1 es una $<$-sección de N.
   (b) S_1 es una $>$-sección de N.
   (c) S_1 es una R_1-sección de N.
   (d) $\{1\}$ es una R_1-sección de N.
21. Demostrar el teorema 69.
22. ¿Qué hipótesis adicionales de ordenación (si las hay) se necesitan para garantizar que si A y B son R-secciones de C, entonces o $A \subseteq B$ o $B \subseteq A$?
23. Considérense las siguientes definiciones:
   (i) x es una cota R-inferior de $A \leftrightarrow (\forall y)(y \in A \rightarrow x \, R \, y)$.

(ii) x es un R-ínfimo de $A \leftrightarrow x$ es una cota R-inferior de A & $(\forall y)(y$ es una cota R-inferior de $A \rightarrow y\, R\, x)$.*

(iii) y es una cota R-superior de $A \leftrightarrow (\forall x)(x \in A \rightarrow x\, R\, y)$.

(iv) y es un R-supremo de $A \leftrightarrow y$ es una cota R-superior de A & $(\forall x)(x$ es una cota R-superior de $A \rightarrow y\, R\, x)$.+

(v) A es un retículo relativo a $R \leftrightarrow R$ es una ordenación parcial de A & $(\forall x)(\forall y)(x \in A$ & $y \in A \rightarrow \{x,y\}$ tiene un R-supremo y un R-ínfimo en A).

(a) Construir dos ordenaciones parciales de un conjunto de cinco elementos, una de las cuales dé un retículo y la otra no.

(b) ¿Cuántos retículos diferentes se pueden construir con un conjunto de tres elementos?

(c) Demostrar que, si A es un retículo relativo a R, entonces A es un retículo relativo a $\breve{R}$.

(d) Demostrar que, si R es una ordenación simple de A, entonces A es un retículo relativo a R.

(e) Dar un contra-ejemplo a la aserción de que, si A es un retículo relativo a R y $B \subseteq A$, entonces B es un retículo relativo a R.

(f) Demostrar que, si A es un retículo relativo a R_1 y B es un retículo relativo a R_2, entonces $A \times B$ es un retículo relativo a la relación R tal que si $x, u \in A$ y $y, v \in B$, entonces

$$\langle x,y\rangle\, R\, \langle u,v\rangle \leftrightarrow x\, R_1\, u \;\&\; y\, R_2\, v.$$

§ 3.3 **Relaciones de equivalencia y particiones.** Una relación que es reflexiva, simétrica y transitiva en un conjunto, es una *relación de equivalencia* sobre ese conjunto. El ejemplo más ubicuo es la relación de identidad. La relación de paralelismo entre rectas es un ejemplo geométrico familiar de una relación de equivalencia; la relación de congruencia entre figuras, es otro ejemplo. La significación fundamental de las relaciones de equivalencia es la de que ellas justifican la aplicación de un principio general de abstracción: Los objetos que son equivalentes en algún respecto generan clases idénticas. A menudo es mucho más simple el análisis de clases de equivalencia de objetos, en vez del de los objetos mismos. La familia de tales clases de equivalencia de un conjunto dado A forman una *partición* del conjunto, esto es, una familia de subconjuntos no vacíos de A, mutuamente disjuntos, cuya unión iguala a A. Recíprocamente, como veremos, toda partición de un conjunto define una única relación de equivalencia sobre ese conjunto.

Por brevedad definimos bajo el mismo número los predicados unario y binario.

Definición 33.

(i) R es una relación de equivalencia $\leftrightarrow R$ es una relación & R es reflexiva, simétrica y transitiva;

(ii) R es una relación de equivalencia sobre $A \leftrightarrow A = \mathfrak{F}\, R$ & R es una relación de equivalencia.

A diferencia de las definiciones de orden de la sección anterior, la presente definición requiere que R sea una relación. La motivación para agregar el requisito adicional aquí es principalmente terminológica. La frase 'R es una equivalencia' no es deseable, pues 'equivalencia' se usa en varios sentidos diferentes en lógica y en teoría de conjuntos. Por otra parte, cuando se usa la frase 'R es una relación de equivalencia', no parece sobrante el requerir que R sea una relación. La simplicidad del siguiente teorema proporciona una motivación secundaria.

La exigencia en el definiens de (ii) de que $A = \mathfrak{F}\, R$ se hace por conveniencia técnica para el ligamen entre las relaciones de equivalencia y las particiones; se verá en lo que sigue que esta conveniencia es obvia.

Teorema 70. *R es una relación de equivalencia $\leftrightarrow R/\breve{R} = R$.*

El siguiente teorema liga las cuasi-ordenaciones y las relaciones de equivalencia, de una manera natural.

Teorema 71. *R es una cuasi-ordenación $\rightarrow \breve{R} \cap \breve{\breve{R}}$ es una relación de equivalencia.*

La siguiente definición introduce la notación $R[x]$; llamamos a $R[x]$ la *R-coclase* de x. In-

* Un R-ínfimo de A se llama frecuentemente una R-máxima cota inferior de A.

\+ Un R-supremo de A se llama también una cota superior R-mínima de A.

tuitivamente, $R[x]$ es, simplemente, el conjunto de todos los objetos con respecto a los cuales x está en la relación R. Cuando R es una relación de equivalencia, nos referimos a $R[x]$ como la *R-clase de equivalencia* de x.

Definición 34. $R[x] = \{y\colon x\ R\ y\}$.

Si P es la relación de paternidad, esto es, $x\ P\ y$ si y sólo si x es el padre de y, entonces

$$P\,[\text{Jorge VI}] = \{\text{Isabel, Margarita}\}$$

y

$$P\,[\text{Tomás de Aquino}] = 0$$

(Desde luego, P no es una relación de equivalencia.)

Tomemos, como ejemplo artificial sencillo,

$$R = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle\}.$$

Entonces R es una relación de equivalencia y

$$R[1] = R[2] = \{1, 2\},$$

$$R[3] = \{3\}.$$

Nótese que en lugar de la definición 34 habríamos podido usar

$$R[x] = R\text{“}\{x\}.$$

No se acostumbra en matemática ser tan explícito acerca de la relación R por medio de la cual se abstrae la clase de equivalencia [x]. Sin embargo, sería incompatible con nuestras reglas de definición omitir la variable libre 'R' en el definiendum. Se necesita hacer énfasis en que la notación $R[x]$ no es usual y quizás se usa sólo en este libro, mientras que la notación $[x]$ se usa frecuentemente.

Tenemos el teorema acostumbrado cuya demostración depende del esquema axiomático de separación.

Teorema 72. $y \in R[x] \leftrightarrow x\ R\ y$.

Los dos teoremas siguientes colocan sobre una base sistemática el principio de abstracción mencionado al comienzo de la sección. Como veremos, estos dos teoremas proporcionan el vínculo esencial entre las relaciones de equivalencia y las particiones.

Teorema 73. $x, y \in \mathfrak{F}\, R$ *& R es una relación de equivalencia* $\rightarrow (R[x] = R[y] \leftrightarrow x\ R\ y)$.

Demostración. Supongamos: $R[x] = R[y]$. Puesto que R es reflexiva, tenemos: $y\ R\ y$; por el teorema anterior,

$$y \in R[y],$$

por tanto, de acuerdo a lo supuesto,

$$y \in R[x];$$

y en virtud, de nuevo, del teorema precedente, $x\ R\ y$.

Supongamos ahora: $x\ R\ y$. Sea z un elemento arbitrario de $R[y]$. En vista del teorema anterior tenemos:

$$y\ R\ z,$$

por consiguiente, ya que R es transitiva,

$$x\ R\ z,$$

siendo así,

$$z \in R[x].$$

Concluimos que

(1) $\qquad R[y] \subseteq R[x].$

Ahora, sea u un elemento arbitrario de $R[x]$; tenemos, de una vez,

$$x\ R\ u.$$

Puesto que R es simétrica tenemos, por lo supuesto,

$$y\ R\ x,$$

en consecuencia, en virtud de la transitividad de R,

$$y\ R\ u$$

y

$$u \in R[y].$$

Así que

(2) $\qquad R[x] \subseteq R[y],$

inferimos inmediatamente, a partir de (1) y (2) que

$$R[x] = R[y]. \qquad \text{Q.E.D.}$$

La demostración anterior ilustra una estrategia que es muy común. Queremos demostrar que los conjuntos $R[x]$ y $R[y]$ son idénticos. No es conveniente operar con una sucesión de equivalencias como las usadas en varias demostraciones anteriores. En lugar de eso, nuestra estrategia consiste en mostrar que un elemento arbitrario de $R[y]$ pertenece a $R[x]$, o sea que $R[y]$ es un subconjunto de $R[x]$. Luego, mostramos que $R[x]$ es un subconjunto de $R[y]$. Estos dos resultados juntos establecen la identidad de los dos conjuntos.

El segundo de los dos teoremas mencionados muestra que las clases de equivalencia no se traslapan.

Teorema 74. *R es una relación de equivalencia* $\rightarrow R[x] = R[y] \vee R[x] \cap R[y] = 0$.

Nótese que en este teorema, a diferencia del que precede, no hay necesidad de exigir que x y y estén en $\mathfrak{F}R$, pues si $x \notin \mathfrak{F}R$, entonces $R[x] = 0$ y la conclusión del teorema se satisface.

Ahora nos referimos a las *particiones*. Toscamente hablando, una partición de un conjunto A es una familia de subconjuntos no vacíos de A, mutuamente exclusivos, cuya unión iguala a A. Por ejemplo, si

$$A = \{ 1, 2, 3, 4, 5 \}$$

y

$$\Pi = \{ \{ 1, 2 \}, \{ 3, 5 \}, \{ 4 \} \},$$

entonces, Π es una partición de A.

Formalmente, tenemos:

Definición 35. *Π es una partición de* $A \leftrightarrow \cup\Pi = A \;\&\; (\forall B)(\forall C)(B \in \Pi \;\&\; C \in \Pi \;\&\; B \neq C \rightarrow B \cap C = 0) \;\&\; (\forall x)(x \in \Pi \rightarrow (\exists y)(y \in x))$.

El uso de la letra 'Π' no tiene significado formal, pero refleja una práctica tan acostumbrada como sugestiva. Nótese que la última cláusula del definiens excluye tanto los individuos como el conjunto vacío de la pertenencia a una partición. Sin embargo, el conjunto vacío es una partición, a saber, una partición de sí mismo. En contraste, para conjuntos no vacíos tenemos:

Teorema 75. $A \neq 0 \rightarrow \{A\}$ *es una partición de A.*

La noción de una partición que es *más fina* que otra, se usa frecuentemente. La idea intuitiva es la de que Π_1 es más fina que Π_2 si todo elemento de Π_1 es un subconjunto de algún elemento de Π_2 y por lo menos uno de tales elementos es un subconjunto propio. Por ejemplo, si

$$A = \{1, 2, 3\},$$

$$\Pi_1 = \{\{1\}, \{2, 3\}\},$$

$$\Pi_2 = \{A\},$$

entonces Π_1 es más fina que Π_2. Por otra parte, si

$$\Pi_3 = \{ \{ 1, 2 \}, \{ 3 \} \},$$

entonces, ninguna de las particiones Π_1, Π_3 es más fina que la otra; simplemente no son comparables con respecto a la finura. En lugar de decir que un elemento de Π_1 es un subconjunto *propio* de Π_2, podemos exigir que $\Pi_1 \neq \Pi_2$, como se ha hecho en nuestra definición formal, la cual es condicional en la forma.

Definición 36. *Π_1 y Π_2 son particiones de A* $\rightarrow$ (Π_1 *es más fina que* $\Pi_2 \leftrightarrow \Pi_1 \neq \Pi_2 \;\&\; (\forall A)(A \in \Pi_1 \rightarrow (\exists B)(B \in \Pi_2 \;\&\; A \subseteq B)))$.

Dejamos como ejercicio, algo intrigante, la demostración del teorema siguiente.

Teorema 76. *Todo conjunto tiene una partición que es la más fina de todas.*

Debe ser claro lo que se quiere decir con 'la más fina de todas las particiones', a saber, una partición que es más fina que cualquier otra partición del conjunto. Una sugerencia concerniente a la demostración es considerar el conjunto potencia del conjunto dado, además del esquema axiomático de separación. Debe ser intuitivamente obvio cuál es la partición más fina de cualquier conjunto. El problema es demostrarlo.

Para establecer, de manera precisa, el ligamen estrecho entre las relaciones de equivalencia y las particiones, definimos un conjunto tal que, cuando R es una relación de equivalencia sobre A, quiere decirse que es la partición de A generada por R.

Definición 37. $\Pi(R) = \{B : (\exists x)(B = R[x] \;\&\; B \neq 0\}$.

Por ejemplo, si

$$A_1 = \{1, 2, 3\}$$

$$R_1 = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\},$$

entonces

$$\mathbf{II}(R_1) = \{\{1, 2\}, \{3\}\};$$

fácilmente se ve que R_1 es una relación de equivalencia sobre A_1 y $\mathbf{II}(R_1)$ es una partición de A_1. Más generalmente, tenemos:

Teorema 77. *R es una relación de equivalencia sobre $A \rightarrow \mathbf{II}(R)$ es una partición de A.*

Tenemos también un teorema que liga la inclusión de las relaciones de equivalencia con la finura de las particiones asociadas:

Teorema 78. *R_1 y R_2 son relaciones de equivalencia sobre $A \rightarrow (R_1 \subset R_2 \leftrightarrow \mathbf{II}(R_1)$ es más fina que $\mathbf{II}(R_2))$.*

Nótese que, si no hubiéramos exigido en la definición de relaciones de equivalencia que $A = \mathfrak{F}R$, entonces este teorema tendría que ser formulado de otra manera, pues R_1 podría contener parejas ordenadas cuyos elementos no pertenecieran a A.

Ahora queremos definir las relaciones generadas por una partición. La definición es general en la forma, así que no está restringida a las particiones.

Definición 38. $\mathsf{R}(\Pi) = \{\langle x, y\rangle : (\exists B)(B \in \Pi \;\&\; x \in B \;\&\; y \in B)\}$.

Tenemos el teorema usual (que fue omitido en el caso de la definición 37).

Teorema 79. $x\mathsf{R}(\Pi)y \leftrightarrow (\exists B)(B \in \Pi \;\&\; x \in B \;\&\; y \in B)$.

En correspondencia al teorema 77 tenemos el siguiente:

Teorema 80. *Π es una partición de $A \rightarrow \mathsf{R}(\Pi)$ es una relación de equivalencia sobre A.*

Demostración. Primero, puesto que Π es una partición de A, dado cualquier elemento x de A, existe un B en Π con $x \in B$, por tanto $x \mathsf{R} (\Pi)x$, así que $\mathsf{R}(\Pi)$ es reflexiva en A. Segundo, supongamos $x \mathsf{R} (\Pi)y$. Entonces existe un $B \in \Pi$ tal que $x \in B$ y $y \in B$. Entonces, por la definición 38,

$$y\mathsf{R}(\Pi)x,$$

por tanto, $\mathsf{R}(\Pi)$ es simétrica en A. Tercero, supongamos que $x \mathsf{R} (\Pi)y$ y $y \mathsf{R} (\Pi)z$. Entonces existe un B tal que $x \in B$ y $y \in B$; además, existe un C tal que $y \in C$ y $z \in C$. Puesto que y está tanto en B como en C, concluimos de la definición de particiones que

$$B = C$$

así que $z \in B$. Entonces, por la definición 38, $x \mathsf{R} (\Pi)z$ y vemos que $\mathsf{R}(\Pi)$ es transitiva en A. Q.E.D.

El teorema siguiente muestra que si generamos una partición por medio de una relación de equivalencia R, entonces la relación de equivalencia generada por la partición es simplemente R otra vez; en forma similar, si comenzamos con la relación de equivalencia generada por una partición, esta relación genera la partición dada.

Teorema 81. *Π es una partición de A & R, es una relación de equivalencia sobre*

$$A \rightarrow (\Pi = \mathbf{II}(R) \leftrightarrow \mathsf{R}(\Pi) = R).$$

EJERCICIOS

1. Demostrar:
   (a) $(R \cap S)[x] = R[x] \cap S[x]$
   (b) $(R \cup S)[x] = R[x] \cup S[x]$.
2. En correspondencia a (a) y (b) del ejercicio 1, ¿qué es válido para la diferencia entre conjuntos?
3. Demostrar el teorema 70.
4. Demostrar el teorema 71.
5. Demostrar el teorema 72.
6. Demostrar el teorema 74.
7. Considérese que todo elemento de A es una relación de equivalencia.
   (a) ¿Es $\bigcap A$ una relación de equivalencia?
   (b) ¿Es $\bigcup A$ una relación de equivalencia?
   Si lo es, demostrarlo. Si no, dar un contra-ejemplo.
8. Dar dos particiones de los números naturales, una de las cuales sea más fina que la otra.
9. Demostrar el teorema 76.
10. Demostrar el teorema 77.
11. Demostrar que si R es una cuasi-ordenación entonces $\mathbf{II}(R \cap \breve{R})$ es una partición de $\mathfrak{F}R$.

12. Demostrar el teorema 78.
13. Demostrar los teoremas 79 y 80.
14. Demostrar el teorema 81.

§ 3.4 Funciones. Desde el siglo dieciocho ha atraído mucha atención el trabajo de generalizar y clarificar el concepto de función. La representación de funciones 'arbitrarias' debida a Fourier (en realidad, las casi continuas) por medio de series trigonométricas, encontró mucha oposición; más tarde, cuando Weierstrass y Riemann dieron ejemplos de funciones continuas sin derivadas, los matemáticos rehusaron considerarlas seriamente. Aún hoy muchos textos de cálculo diferencial e integral no dan una definición de función matemáticamente satisfactoria. Una definición precisa y completamente general es inmediata dentro de nuestro enfoque teórico de conjuntos. Una función es simplemente una relación de muchos a uno, esto es, una relación tal que cualquier elemento de su dominio se relaciona exactamente con un elemento en su recorrido. (Desde luego, elementos diferentes del dominio pueden estar relacionados con el mismo elemento del recorrido.) La definición formal es obvia.

Definición 39. *f es una función* $\leftrightarrow$ *f es una relación* & $(\forall x)(\forall y)(\forall z)\,(x f y\ \&\ x f z \rightarrow y = z)$.

El uso de la variable 'f' no quiere decir que tenga alguna significación formal. La usamos aquí en lugar de 'A' o 'R' para estar de acuerdo con el uso matemático ordinario. Para resumir nuestro uso de variables hasta este punto:

'A', 'B', 'C', . . . , 'R', 'S', 'T', . . . , Π, 'f', 'g',... son variables (con o sin sub-índices) las cuales toman conjuntos como valores;

'x', 'y', 'z', . . .

son variables (con o sin sub-índices) que toman conjuntos o individuos como valores.

En el caso de funciones no estamos satisfechos con el uso de la notación $x f y$, sino que queremos también tener a mano la notación funcional usual: $f(x) = y$, donde '$f(x)$' se lee 'f de x'.*

Definición 40. $f(x) = y \leftrightarrow [(\mathrm{E}!z)\,(x f z)\ \&\ x f y] \vee [-(\mathrm{E}!z)\,(x f z)\ \&\ y = 0]$.

La definición está construida de tal modo que la notación '$f(x)$' tenga un significado definido para todo conjunto f y para todo objeto x. Por ejemplo, si

$$f = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 3, 4\rangle\}$$

entonces,

$$f(1) = 0$$

$$f(2) = 0$$

$$f(3) = 4.$$

La operación de formar la composición de dos funciones es tan extensamente usada en ciertas ramas de la matemática que se han usado varios símbolos especiales para ella; nosotros usamos un pequeño círculo '$\circ$'. Así, informalmente,

$$(f \circ g)(x) = f(g(x)).$$

La composición se define directamente en términos de producto relativo; introducimos el nuevo símbolo '$\circ$' en lugar de usar el símbolo de producto relativo porque el orden de 'f' y 'g' en '$f \circ g$' es el natural para las funciones y es el inverso del que corresponde al término producto relativo.

Definición 41. $f \circ g = g/f$.

Tenemos los dos teoremas sencillos:

Teorema 82. *f y g son funciones* $\rightarrow f \cap g$ *y $f \circ g$ son funciones.*

Teorema 83. *f y g son funciones* $\rightarrow (f \circ g)(x) = f(g(x))$.

Recordando la noción de restricción del dominio de una relación tenemos:

Teorema 84. $(f \circ g)\,|A = f \circ (g|A)$.

* En lógica matemática, siguiendo el uso de Whitehead y Russell en *Principia Mathematica*, se usa frecuentemente $f\text{'}\,x$ en lugar de: $f(x)$.

Previsto que f es una función, podemos fortalecer dos teoremas iniciales sobre la operación imagen (teoremas 36 y 37).

Teorema 85. *f es una función* $\to \breve{f}``(A \cap B) = \breve{f}``A \cap \breve{f}``B \;\&\; \breve{f}``A \sim \breve{f}``B = \breve{f}``(A \sim B)$.

Y podemos fortalecer el análogo del teorema 40 para el recorrido de f.

Teorema 86. *f es una función* $\to (\mathfrak{R}f) \cap B = f``(\breve{f}``B)$.

Tenemos también:

Teorema 87. *f es una función* $\& \; A \cap B = 0 \to \breve{f}``A \cap \breve{f}``B = 0$.

Ahora definimos la noción de función 1—1.

Definición 42. *f es* $1-1 \leftrightarrow f$ y $\breve{f}$ *son funciones.*

Tenemos el resultado obvio:

Teorema 88. *f es* $1-1 \;\&\; x_1 \in \mathfrak{D}f \;\&\; x_2 \in \mathfrak{D}f \to (f(x_1) = f(x_2) \leftrightarrow x_1 = x_2)$.

Cuando f es $1-1$ es posible una definición sencilla de su *inversa.*

Definición 43. *f es* $1-1 \to f^{-1} = \breve{f}$.

En los siguientes teoremas están expresados hechos útiles.

Teorema 89. *f es* **1-1** $\to (f^{-1}(y) = x \leftrightarrow f(x) = y)$.

Teorema 90. *f es* 1-1 $\& \; x \in \mathfrak{D}f \to f^{-1}(f(x)) = x$.

Teorema 91. *f es* 1-1 $\& \; y \in \mathfrak{R}f \to f(f^{-1}(y)) = y$.

Teorema 92. *f y g son* 1-1 $\to f \cap g$ *es* $1-1$.

Teorema 93. *f y g son* 1-1 $\& \; \mathfrak{D}f \cap \mathfrak{D}g = 0 \;\&\; \mathfrak{R}f \cap \mathfrak{R}g = 0 \to f \cup g$ *es* 1-1.

Es deseable también definir de manera formal en este punto algún lenguaje matemático usual, el cual usaremos mucho en los últimos capítulos. Lo resumimos en una definición.

Definición 44.

(i) *f es una función sobre (o de) A hacia (o en) $B \leftrightarrow f$ es una función* $\& \; \mathfrak{D}f = A \;\&\; \mathfrak{R}f \subseteq B$;

(ii) *f es una función de A sobre $B \leftrightarrow f$ es una función* $\& \; \mathfrak{D}f = A \;\&\; \mathfrak{R}f = B$;

(iii) *f aplica A en $B \leftrightarrow f$ es una función* $1-1 \;\&\; \mathfrak{D}f = A \;\&\; \mathfrak{R}f \subseteq B$;

(iv) *f aplica A sobre $B \leftrightarrow f$ es una función* $1-1 \;\&\; \mathfrak{D}f = A \;\&\; \mathfrak{R}f = B$.

La distinción entre 'en' y 'sobre' en esta definición es usual en la literatura matemática y tiene su contra-parte en el uso ordinario. Una función $1-1$ aplica *A sobre B* cuando el recorrido de f es todo B; aplica *A en B* cuando el recorrido de f es sólo algún subconjunto de B.

Concluimos esta sección definiendo el conjunto de todas las funciones de B hacia A, el cual se designa ordinariamente con A^B. Este concepto es útil en una gran variedad de contextos matemáticos.

Definición 45. $A^B = \{f: f$ *es una función* $\& \; \mathfrak{D}f = B \;\&\; \mathfrak{R}f \subseteq A\}$.

En virtud del esquema axiomático de separación podemos establecer el teorema usual.

Teorema 94. $f \in A^B \leftrightarrow f$ *es una función* $\& \; \mathfrak{D}f = B \;\&\; \mathfrak{R}f \subseteq A$.

Formulamos sin demostración cinco teoremas elementales.

Teorema 95. $A^0 = \{0\}$.

Teorema 96. $A \neq 0 \to 0^A = 0$.

Teorema 97. $A^B = 0 \leftrightarrow A = 0 \;\&\; B \neq 0$.

Teorema 98. $A^{\{x\}} = \{\{\langle x, y\rangle\}: y \in A\}$.

Teorema 99. $A \subseteq B \to A^C \subseteq B^C$.

EJERCICIOS

1. Formular y demostrar una condición necesaria y suficiente para que la unión de dos funciones sea una función.
2. Demostrar los teoremas 82 y 83.
3. Demostrar el teorema 84.
4. Demostrar los teoremas 85 y 86.

5. Demostrar el teorema 87.
6. Demostrar los teoremas 89 a 93.
7. Demostrar que si f es $1-1$ entonces:

(a) $f``(A \cap B) = f``A \cap f``B$,
(b) $f``(A \sim B) = f``A \sim f``B$.

8. Dado que f y g son $1-1$ considérense las siguientes aserciones. Si una aserción es verdadera, demostrarla. Si es falsa, dar un contra-ejemplo.

(a) $f \cup g$ es 1-1,
(b) $f \sim g$ es 1-1,
(c) $f \circ g$ es 1-1,
(d) $f \cup f^{-1}$ es 1-1,
(e) $A \cap B = 0 \rightarrow f|A \cup g|B$ es 1-1,
(f) $A \cap B = 0 \rightarrow f``A \cap g``B = 0$.

9. Demostrar el teorema 94.
10. Demostrar los teoremas 95 a 99.
11. Considérese el ejercicio 23 de § 3.2, en el cual se han definido los retículos. Queremos desarrollar una formulación equivalente en términos de operaciones. Sea A un retículo relativo a R, y x, $y \in A$. Entonces definimos:

$$x \cap_{A,R} y = R\text{-ínfimo de } \{x,y\}$$
$$x \cup_{A,R} y = R\text{-supremo de } \{x,y\}.$$

Demostrar (los sub-índices 'A' y 'R' se han suprimido, por brevedad):

(a) $x \cap x = x$
(b) $x \cup x = x$
(c) $x \cap y = y \cap x$
(d) $x \cup y = y \cup x$
(e) $x \cap (y \cap z) = (x \cap y) \cap z$
(f) $x \cup (y \cup z) = (x \cup y) \cup z$
(g) $x \cap (x \cup y) = x$
(h) $x \cup (x \cap y) = x$.

Ahora, para ir por el otro camino, suponiendo para cualesquiera x, y, $z \in A$, las propiedades (a)–(g), definimos:

$$x R' y \leftrightarrow x \cap y = y.$$

Demostrar que A es un retículo relativo a R'.

12. Podemos definir formalmente la notación lambda para la abstracción:

Si $\mathbf{v}$ *y* $\mathbf{w}$ *son variables diferentes y* $\mathbf{w}$ *no aparece en el término* $\mathbf{t}$, *entonces la identidad*

$$(\lambda \mathbf{v})(\mathbf{t}) = \{\langle \mathbf{v},\mathbf{w}\rangle : \mathbf{t} = \mathbf{w}\}$$

es válida.

Hallar los siguientes conjuntos:

(a) $(\lambda A)(\{x\colon x \in A \ \&\ A \subseteq B\})$
(b) $(\lambda A)(\{x\colon x \in B \sim A \ \&\ A \subseteq B\})$
(c) $(\lambda A)(\{x\colon x \in A \ \&\ A = 0\})$

13. Demostrar:

(a) $(\lambda A)(A \cap A) = 0$
(b) $(\lambda A)(A \cup A) = 0$
(c) $(\lambda A)(A \sim A) = 0$
(d) $(\lambda A)(A/A) = 0$

(El significado de (a)—(d) es el de que no hay conjuntos que correspondan a las operaciones entre conjuntos. Por ejemplo, en vista de (a) no podemos considerar la operación de un conjunto que se intersecta consigo mismo como un cierto conjunto de parejas ordenadas. Este resultado para el caso especial de conjuntos que se intersectan consigo mismos se generaliza fácilmente para mostrar que no hay conjunto que corresponda a la operación binaria de intersección para dos conjuntos distintos cualesquiera.)

Capítulo 4

Equipotencia, conjuntos finitos y números cardinales

§ 4.1 **Equipotencia.** Los axiomas consignados al final del capítulo 2 § (2.10) bastan para esta sección y la siguiente; pero en § 4.3, que trata de números cardinales, introducimos un axioma especial cuyo uso se indicará siempre con '†'.

En § 1.1 se mencionó como fundamental la noción de Cantor referente a dos conjuntos que tienen la misma potencia, o, como diremos, que son *equipotentes.* Es fundamental porque es la base para generalizar la noción de entero positivo a la de número cardinal. Dos conjuntos son equipotentes si existe una correspondencia $1-1$ entre ellos; los conjuntos equipotentes tienen el mismo número cardinal. Esta noción intuitiva de correspondencia $1-1$ se precisa fácilmente; tal correspondencia es precisamente una función $1-1$. Formalmente tenemos:*

Definición 1.

(i) *$A \approx B$ bajo f, si y sólo si f es una función $1-1$ cuyo dominio es A y cuyo recorrido es B;*

(ii) *$A \approx B$, si y sólo si existe una f tal que $A \approx B$ bajo f.*

Por ejemplo, si

$$A_1 = \{1, 3, 5\}$$
$$A_2 = \{1, 7, 9\},$$

entonces A_1 y A_2 son equipotentes. Cualquiera de las varias funciones establecerá esto:

$$f_1 = \{\langle 1, 1\rangle, \langle 3, 7\rangle, \langle 5, 9\rangle\},$$

o también,

$$f_2 = \{\langle 1, 7\rangle, \langle 3, 9\rangle, \langle 5, 1\rangle\}.$$

Es claro que dos conjuntos finitos son equipotentes cuando tienen el mismo número de elementos. (Desde luego, no hemos definido todavía las nociones de finitud o de número dentro de nuestro enfoque axiomático.) También es claro que si un conjunto finito es un subconjunto propio de otro, entonces los dos conjuntos no pueden tener la misma potencia, esto es, no pueden ser equipotentes. Sin embargo, la situación es completamente diferente para los conjuntos infinitos. Considérese, por ejemplo, el conjunto N de enteros positivos $\{1, 2, 3, \ldots\}$ y el conjunto E de los números pares $\{2, 4, 6, \ldots\}$. Obviamente, E es un subconjunto propio de N, pero E y N son equipotentes, lo cual se muestra fácilmente considerando la función el doble, f, tal que para todo entero positivo n

$$f(n) = 2n.$$

Vemos, de una vez, que f es $1-1$, $\mathfrak{D}f = N$, y $\mathfrak{R}f = E$.

Los tres primeros teoremas muestran que la equipotencia tiene las tres propiedades características de una relación de equivalencia.

Teorema 1. $A \approx A$.

Demostración. La función idéntica $\mathfrak{I}A$ es una función $1-1$ apropiada. Q.E.D.

Teorema 2. *Si $A \approx B$, entonces $B \approx A$.*

* En este capítulo y en lo que sigue, usamos simbolismo lógico sólo rara vez para formular definiciones y teoremas; pero en cualquier caso, será obvia la formulación simbólica apropiada.

Teorema 3. *Si* $A \approx B$ & $B \approx C$, *entonces* $A \approx C$.

Demostración. Sea f una función $1-1$ que establece $A \approx B$, con $\mathfrak{D}f = A$; sea g una función $1-1$ correspondiente, que verifica $B \approx C$ con $\mathfrak{D}g = B$. Entonces la función $g \circ f$ es $1-1$, $\mathfrak{D}(g \circ f) = A$ y $\mathfrak{R}(g \circ f) = C$, de donde $A \approx C$. Q.E.D.

Ahora formulamos varios teoremas que relacionan la equipotencia a las operaciones y relaciones introducidas previamente. Estos teoremas simplifican mucho el desarrollo de la aritmética cardinal en § 4.3. El primer teorema se usa para justificar la definición de adición cardinal. El segundo se usa para justificar la definición de multiplicación cardinal; el tercero se usa para demostrar la conmutatividad de las multiplicación cardinal, etc. El orden de estos teoremas es casi el mismo que el de los teoremas correspondientes para números cardinales en § 4.3.

Teorema 4. *Si* $A \approx B$ & $C \approx D$ & $A \cap C = 0$ & $B \cap D = 0$, *entonces* $A \cup C \approx B \cup D$.

Demostración. Por la hipótesis, existen funciones f y g que son $1-1$ y tales que $A \approx B$, bajo f y $C \approx D$, bajo g. Se sigue también de la hipótesis que

$$\mathfrak{D}f \cap \mathfrak{D}g = 0$$

y

$$\mathfrak{R}f \cap \mathfrak{R}g = 0,$$

por tanto, en virtud del teorema 93 de § 3.4, $f \cup g$ es $1-1$ y se ve fácilmente que

$$A \cup C \approx B \cup D \text{ bajo } f \cup g. \quad \text{Q.E.D.}$$

Teorema 5. *Si* $A \approx B$ & $C \approx D$, entonces $A \times C \approx B \times D$.

Demostración. Sea $A \approx B$ bajo la función f y $C \approx D$ bajo la función g. Entonces la función h tal que para $x \in A$ y $y \in C$

$$h(\langle x, y\rangle) = \langle f(x), g(y)\rangle$$

establece la equipotencia entre $A \times C$ y $B \times D$. Q.E.D.

Teorema 6. $A \times B \approx B \times A$.

Demostración. La función f tal que para $x \in A$ y $y \in B$

$$f(\langle x, y\rangle) = \langle y, x\rangle$$

es apropiada para establecer la equipotencia pedida. Q.E.D.

Teorema 7. $A \times (B \times C) \approx (A \times B) \times C$.

Teorema 8. $A \times \{x\} \approx A$ & $\{x\} \times A \approx A$.

Demostración. Para la primera mitad del teorema es apropiada la función f definida sobre $A \times \{x\}$ tal que para $y \in A$

$$f(\langle y, x\rangle) = y.$$

Para la segunda mitad del teorema puede usarse una función similar. Q.E.D.

Teorema 9. *Existen conjuntos* C *y* D *tales que* $A \approx C$ & $B \approx D$ & $C \cap D = 0$.

Demostración. Definamos

$$C = A \times \{0\}$$
$$D = B \times \{\{0\}\}.$$

Entonces, por el teorema precedente, $A \approx C$ y $B \approx D$ y, naturalmente, $C \cap D = 0$. Q.E.D.

El siguiente teorema se usa para justificar la definición de exponenciación cardinal.

Teorema 10. *Si* $A \approx B$ & $C \approx D$, *entonces* $A^C \approx B^D$.

Demostración. Por hipótesis existen funciones f y g que son 1-1 tales que $A \approx B$ bajo f y $C \approx D$ bajo g. Si $h \in A^C$ entonces,

(1) $$f \circ h \in B^C$$

y, a partir de (1), inferimos:

$$f \circ h \circ g^{-1} \in B^D.$$

Más aún, si $h' \in B^D$, entonces existe un único $h \in A^C$ tal que $h' = f \circ h \circ g^{-1}$ (en efecto, $h = f^{-1} \circ h' \circ g$). Por tanto, si definimos la función f' sobre A^C tal que para todo $h \in A^C$

$$f'(h) = f \circ h \circ g^{-1},$$

entonces f' es 1-1 y su recorrido es B^D. Q.E.D.

Omitimos la demostración de los tres siguientes teoremas, que corresponden a tres leyes fundamentales de la exponenciación cardinal.

Teorema 11. *Si* $B \cap C = 0$, *entonces* $A^{B \cup C} \approx A^B \times A^C$.

Teorema 12. $(A \times B)^C \approx A^C \times B^C$.

Teorema 13. $(A^B)^C \approx A^{B \times C}$.

Anticipamos ahora la definición del entero 2, dada en el capítulo 5, para formular un teorema clásico en la notación usual: el conjunto potencia $\mathcal{P}A$ es equipotente con 2^A.

Teorema 14. *Si* $2 = \{0, \{0\}\}$, *entonces* $\mathcal{P}A \approx 2^A$.

Demostración. Sea $B \in \mathcal{P}A$. Entonces existe una función $g_B \in 2^A$ tal que

$$g_B(x) = \begin{cases} 0 \text{ si } x \in B \\ \{0\} \text{ si } x \in A \sim B. \end{cases}$$

Se ve fácilmente que a cada B corresponde una única g_B, y para cada $h \in 2^A$ existe un único $B \in \mathcal{P}A$ tal que $h = g_B$, lo que establece la correspondencia pedida. Q.E.D.

Pasamos a definir, de la manera obvia, la relación $\preceq$ de *ser igual o menor que, en potencia,* lo que podemos llamar también, *ser igual o menos potente que,* aun cuando la frase 'menos potente' no es muy usual.

Definición 2. $A \preceq B$ *si y sólo si existe un conjunto* C *tal que* $A \approx C$ & $C \subseteq B$.

Tres teoremas sencillos:

Teorema 15. *Si* $A \approx B$, *entonces* $A \preceq B$.

Teorema 16. *Si* $A \subseteq B$, *entonces* $A \preceq B$.

Teorema 17. *Si* $A \preceq B$ & $B \preceq C$, *entonces* $A \preceq C$.

Un teorema menos obvio, pero fundamental para la teoría de la potencia de Cantor, es el siguiente, cuya demostración es la más difícil de todas las que se han dado en los primeros cuatro capítulos.

Teorema 18. [Teorema de Schröder-Bernstein] * *Si* $A \preceq B$ & $B \preceq A$, *entonces* $A \approx B$

Demostración. Siguiendo la hipótesis del teorema, suponemos que

$$f \text{ aplica } A \text{ sobre } B_1 \subseteq B$$

y que

$$g \text{ aplica } B \text{ sobre } A_1 \subseteq A.$$

Podemos mostrar que A y B tienen la misma potencia si podemos hallar un subconjunto K de A tal que g aplica $B \sim f``K$ sobre $A \sim K$. La h definida como sigue proporcionará la correspondencia apropiada:

$$h = (f|K) \cup (\breve{g}|(A \sim K)),$$

ya que

$$\text{el dominio de } h = K \cup (A \sim K) = A,$$

y

$$\begin{aligned} \text{el recorrido de } h &= (f``K) \cup (\breve{g}``(A \sim K)) \\ &= (f``K) \cup (B \sim f``K) = B. \end{aligned}$$

En otras palabras, necesitamos hallar un subconjunto K de A tal que

$$g``(B \sim f``K) = A \sim K.$$

Para este efecto demostramos ahora que, si definimos

$$D = \{C\colon\ C \subseteq A \ \&\ g``(B \sim f``C) \subseteq A \sim C\},$$

entonces $\bigcup D$ es un K apropiado.

Observamos primero que, si $C_1 \subseteq A$ & $C_2 \subseteq A$ y $C_1 \subseteq C_2$, entonces

$$g``(B \sim f``C_2) \subseteq g``(B \sim f``C_1),$$

por tanto,

$$(1) \quad A \sim g``(B \sim f``C_1) \subseteq A \sim g``(B \sim f``C_2).$$

* El teorema fue demostrado independientemente por E. Schröder y F. Bernstein, hacia 1890. Debido a que el teorema fue conjeturado por Cantor, se llama a veces el teorema de Cantor-Bernstein. La demostración que se da aquí está de acuerdo con la que dio Fraenkel (1953, pp. 102-3) y la cual el mismo Fraenkel acredita a J. M. Whitaker.

Más aún, para el caso especial en que $C \in D$, tenemos,

(2) $C \subseteq A \sim g``(B \sim f``C)$.

(Esto se sigue de la definición de D y del hecho que para subconjuntos cualesquiera X y Y de A, $X \subseteq A \sim Y$, si y sólo si $Y \subseteq A \sim X$.) Puesto que todo $C \in D$ es un subconjunto de $\bigcup D$, concluimos, a partir de (1) y (2), que, si $C \in D$, entonces

(3) $C \subseteq A \sim g``(B \sim f``\bigcup D)$.

Por el teorema 63 del capítulo 2 podemos inferir, a partir de (3), que

(4) $\bigcup D \subseteq A \sim g``(B \sim f``\bigcup D)$.

Ahora, sea

(5) $F = A \sim g``(B \sim f``\bigcup D)$.

Entonces, en virtud de (1), (4), (5)

$$A \sim g``(B \sim f``\bigcup D) \subseteq A \sim g``(B \sim f``F),$$

o sea,

$$F \subseteq A \sim g``(B \sim f``F),$$

por tanto, concluimos

$$F \in D,$$

o sea,

(6) $A \sim g``(B \sim f``\bigcup D) \subseteq \bigcup D$.

A partir de (4) y (6), tenemos

$$\bigcup D = A \sim g``(B \sim f``\bigcup D),$$

lo cual, para $K = \bigcup D$, es equivalente a:

$$g``(B \sim f``K) = A \sim K,$$

que es la conclusión pedida. Q.E.D.

Tendremos ocasión de usar el teorema de Schröder-Bernstein en las demostraciones de varios teoremas subsiguientes. Por el momento completamos nuestra lista de teoremas sobre la relación $\preceq$. Principalmente tenemos el siguiente resultado de monotonía:

Teorema 19. *Si $A \preceq B$ & $C \preceq D$, entonces*

(i) *si $B \cap D = 0$, entonces $A \cup C \preceq B \cup D$,*

(ii) $A \times C \preceq B \times D$,

(iii) $A^C \preceq B^D$, *previsto que no se cumpla que $A = B = C$ & $D \neq 0$.*

Como consecuencia inmediata de (i) de este teorema, obtenemos:

Teorema 20. $A \preceq A \cup B$.

Ahora definimos, de la manera esperada, la relación $\prec$ de *tener menor potencia.* Decimos 'no $B \preceq A$' como una abreviatura de 'no es el caso de que $B \preceq A$'.

Definición 3. $A \prec B$, *si y sólo si* $A \preceq B$ *& no* $B \preceq A$.

En el siguiente teorema se resumen tres resultados sencillos:

Teorema 21.

(i) *No* $A \prec A$;

(ii) *Si* $A \prec B$, *entonces no* $B \prec A$;

(iii) *Si* $A \prec B$ & $B \prec C$, *entonces* $A \prec C$.

En el siguiente teorema se resumen algunas relaciones entre la equipotencia y la potencia relativa.

Teorema 22.

(i) *Si* $A \preceq B$, *entonces no* $B \prec A$;

(ii) *Si* $A \preceq B$ & $B \prec C$, *entonces,* $A \prec C$;

(iii) *Si* $A \prec B$ & $B \preceq C$, *entonces* $A \prec C$;

(iv) $A \preceq B$ *si y sólo si o* $A \approx B$ *o* $A \prec B$.

Demostración. Demostramos solamente (iv). [Necesidad]. Supongamos que no $A \prec B$. Entonces, en vista de la definición 3, o no $A \preceq B$ o $B \preceq A$; pero, por hipótesis, $A \preceq B$, así que también, $B \preceq A$. Por el teorema de Schröder-Bernstein concluimos que $A \approx B$.

[Suficiencia]. Si $A \approx B$, entonces, obviamente, $A \preceq B$. Si $A \prec B$, entonces, por la definición 3, $A \preceq B$. Q.E.D.

Es de fundamental importancia el teorema de Cantor según el cual, todo conjunto tiene menos potencia que su conjunto potencia.

Teorema 23. $A \prec \mathcal{P}A$.

Demostración. La demostración hace uso del argumento básico empleado para construir la paradoja de Russell en teoría de conjuntos intuitiva, si bien la demostración de Cantor fue históricamente anterior a la paradoja de Russell.

La función f sobre A tal que para x en A

$$f(x) = \{x\}$$

establece que

$$(1) \qquad A \leq \mathcal{P}A,$$

ya que el conjunto de conjuntos unitarios de elementos de A es un subconjunto del conjunto potencia de A.

Ahora supongamos $A \approx \mathcal{P}A$ bajo la función g, digamos ($\mathfrak{D}g = A$ & $\mathfrak{R}g = \mathcal{P}A$). Definamos:

$$B = \{y: y \in A \;\&\; y \notin g(y)\}.$$

Por tanto, sobre la base de nuestra suposición, debe existir algún x en A tal que

$$g(x) = B.$$

Pero podemos inferir fácilmente que

$$x \in g(x), \textit{ si y sólo si } x \notin g(x),$$

lo que es absurdo. Concluimos que nuestra suposición es falsa y que no es el caso de que $A \approx \mathcal{P}A$; a partir de este resultado inferimos (1) y la contrapositiva del teorema de Schröder-Bernstein, o sea que no es el caso de que $\mathcal{P}A \leq A$; esto establece el teorema.
Q.E.D.

El hecho más importante acerca de la potencia relativa de conjuntos, la cual no hemos establecido aún, es la de que la potencia relativa de dos conjuntos es siempre comparable, o sea que tenemos siempre $A \prec B$, $A \approx B$ o $B \prec A$. Este resultado, conocido como la ley de tricotomía, no sólo requiere el axioma de escogencia en su demostración, sino que es equivalente a él. Diferimos esta demostración hasta el capítulo 8, donde discutimos el axioma de escogencia con más detalle. La importancia de la tricotomía para la teoría clásica de números cardinales debe ser obvia: sin ella, dos cardinales cualesquiera dejan de ser comparables necesariamente; tal estado de cosas es inconveniente en cualquier teoría de cantidad, finita o infinita.

EJERCICIOS

1. Demostrar el teorema 2.
2. Demostrar el teorema 7.
3. Demostrar los teoremas 11 a 13.
4. Demostrar que si f es una función, entonces $\mathfrak{D}f = f$.
5. Demostrar los teoremas 15 a 17.
6. Demostrar que si $B \neq 0$, entonces $A \leq A \times B$.
7. Usar el teorema de Schröder-Bernstein para demostrar que, si $A \subseteq B \subseteq C$ & $A \approx C$, entonces $B \approx C$. Recíprocamente, demostrar que este resultado implica el teorema de Schröder-Bernstein.
8. Demostrar el teorema 19.
9. Demostrar el teorema 21.
10. Demostrar las partes (i) a (iii) del teorema 22.
11. Demostrar que, si $B \approx C$ & $A \prec B$, entonces $A \prec C$.
12. Demostrar que, si $x \notin A$ & $y \notin B$ & $A \cup \{x\} = B \cup \{y\}$, entonces $A \approx B$.

§ **4.2 Conjuntos finitos.** La noción del sentido común es la de que un conjunto es finito cuando tiene exactamente n elementos para algún entero n no negativo. Si no es finito, entonces es infinito. Esta idea del sentido común es técnicamente buena y la usaremos en lo que sigue, pero también es instructivo tratar de encontrar una definición de finitud que no requiera referencia explícita a los números. Tal enfoque es también intuitivamente bueno, ya que continuamente juzgamos que un conjunto es finito, sin una idea clara de su cardinalidad. Por ejemplo, cualquiera cree que el conjunto de los cabellos de las cabezas de todos los clérigos zurdos y ojiazules que vivieron en 1900 es finito, pero probablemente ninguno podría estimar con alguna aproximación la cardinalidad de este conjunto.

Dedekind [1888] propuso una definición no numérica.* Un conjunto finito se caracteriza por no ser equipotente con ninguno de sus subconjuntos propios. La consideración de ejemplos simples de conjuntos finitos sugiere que esta definición es intuitivamente aceptable. Nótese, desde luego, que no estamos buscando alguna definición arbitraria de finitud, sino una definición según la cual sean finitos aquellos conjuntos que son fini-

* Este enfoque fue sugerido independientemente por Peirce, aproximadamente al mismo tiempo. (Véase Peirce [1932, Vol. III, pp. 210-249].)

tos en el sentido de tener n elementos, para algún entero n.

Por aceptable que pueda parecer la definición de Dedekind, ella requiere el axioma de escogencia para demostrar que todo conjunto finito de Dedekind es finito en el sentido ordinario. Esta demostración se dará en el capítulo 8.

Muchas otras definiciones alternas de finitud han sido propuestas por Zermelo, Russell, Sierpinski, Kuratowski y Tarski, para mencionar los más conocidos. En Tarski [1924b], se da una visión sistemática y completa y se propone la definición de Tarski. Ya que la definición de Tarski es simple y no requiere el axioma de escogencia para demostrar su equivalencia con la definición numérica ordinaria, la adoptaremos aquí. Los desarrollos de esta sección siguen muy de cerca el artículo de Tarski.

La idea es la de que un conjunto es finito cuando una familia de subconjuntos, no vacía, del conjunto dado tiene un elemento del cual ningún otro miembro de la familia es un subconjunto propio. Esto es, en la terminología de la definición 26 del capítulo 3, toda familia no vacía de subconjuntos tiene un elemento mínimo con respecto a la relación $\subset$ de ser un subconjunto propio. Formalmente, definimos tanto los elementos mínimos como los máximos.

Definición 4.

(i) *x es un elemento mínimo de A, si y sólo si $x \in A$ & x es un conjunto & para todo B, si $B \in A$, entonces no $B \subset x$;*

(ii) *x es un elemento mínimo de A, si y sólo si $x \in A$ & x es un conjunto & para todo B, si $B \in A$, entonces no $x \subset B$.*

Por ejemplo, si

$$A = \{1, 2, 3\},$$

$$K_1 = \{\{1, 2\}, \{1\}, \{3\}\},$$

y

$$K_2 = \{0, \{1, 3\}, A\},$$

entonces los conjuntos $\{1\}$ y $\{3\}$ son elementos mínimos de K_1; el conjunto vacío es el elemento mínimo de K_2. Obviamente, cualquier otra familia, no vacía, de subconjuntos de A tiene un elemento mínimo. Por otra parte, consideremos el conjunto N de enteros positivos y consideremos la familia F de subconjuntos $\{N_1, N_2, \ldots, N_n, \ldots\}$ donde N_n es

$$N \sim \{1, 2, \ldots, n\text{-}1\}.$$

Entonces, claramente, F no tiene elemento mínimo y esta situación es típica de los conjuntos infinitos. Los elementos máximos de K_1 son los conjuntos $\{1, 2\}$ y $\{3\}$ y el único elemento máximo de K_2 es el mismo conjunto A.

La definición de Tarski, a diferencia de la de Dedekind, no requiere la noción de equipotencia. Sin embargo, más adelante, en esta sección, demostraremos algunos teoremas acerca de la equipotencia y potencia relativa de conjuntos finitos, que nos referirán a las ideas de la sección precedente.

Definición 5. *A es finito, si y sólo si toda familia de subconjuntos de A tiene un elemento mínimo.*

Nos referimos ahora a algunos teoremas elementales. Las demostraciones de los dos primeros son muy simples.

Teorema 24. *El conjunto vacío es finito.*

Teorema 25. *$\{x\}$ es finito.*

Teorema 26. *Si A es finito y $B \subseteq A$, entonces B es finito.*

Demostración. Sea K una familia no vacía de subconjuntos de B. Ya que $B \subseteq A$, K es una familia no vacía de subconjuntos de A y por la hipótesis del teorema debe tener un elemento mínimo. Q.E.D.

Teorema 27. *Si A es finito, entonces $A \cap B$ y $A \sim B$ son finitos.*

Demostración. Notamos que

$$A \cap B \subseteq A,$$

$$A \sim B \subseteq A,$$

y entonces se aplica el teorema precedente. Q.E.D.

La demostración de que la unión de dos conjuntos es finita es más difícil.

Teorema 28. *Si A y B son finitos, entonces $A \cup B$ es finito.*

Demostración. Sea K una familia no vacía de subconjuntos de $A \cup B$. Para establecer el teorema es necesario demostrar que K tiene un elemento mínimo.

Definimos:

(1) $L = \{C\colon C \subseteq A \;\&\; \exists D \subseteq B$ tal que $C \cup D \in K\}$.

La siguiente consideración muestra que L no es vacío. Sea E algún elemento de K. Entonces $C = E \cap A$ es un elemento de L, pues podemos tomar a D como $E \sim A$.

Puesto que A es finito, L tiene un elemento mínimo, digamos C^*. Observamos:

(2) $C^* \in L$

(3) $C^* \subseteq A$.

Definimos ahora

$$M = \{E\colon E \subseteq B \;\&\; E \cup C^* \in K\}.$$

En virtud de (2) y (3), M no es vacío; puesto que B es finito, M, como L, tiene un elemento mínimo, digamos E^*.

Ahora tenemos:

(4) $E^* \in M$

(5) $E^* \subseteq B$

(6) $E^* \cup C^* \in K$.

Para completar la demostración, demostramos que $E^* \cup C^*$ es un elemento mínimo de K. Supongamos, por vía de contradicción, que existe un conjunto G tal que

(7) $G \in K$

(8) $G \subset E^* \cup C^*$.

Ahora, a partir de (3) y (5), vemos que

(9) $G \cap C^* \subseteq C^* \subseteq A$

(10) $G \cap E^* \subseteq E^* \subseteq B$

y, a partir de (8),

(11) $G = (G \cap C^*) \cup (G \cap E^*)$.

A partir de (7), (9), (11) y la definición de L, inferimos

$$G \cap C^* \in L,$$

y puesto que C^* es un elemento mínimo de L,

(12) $G \cap C^* = C^*$.

Ahora, a partir de (7), (11) y (12),

$$(G \cap E^*) \cup C^* \in K,$$

así que, recordando (10),

$$G \cap E^* \in M.$$

Puesto que E^* es un elemento mínimo de M,

(13) $G \cap E^* = E^*$.

A partir de (11), (12) y (13) concluimos que

$$G = C^* \cup E^*,$$

lo que contradice (8) y demuestra que nuestra suposición es falsa. Q.E.D.

Como consecuencia inmediata de los teoremas 25 y 28, tenemos:

Teorema 29. *Si A es finito, entonces $A \cup \{x\}$ es finito.*

Realizamos ahora la formulación y demostración de un principio de inducción para conjuntos finitos. Como veremos, tal principio puede usarse como definición de conjuntos finitos, hecho que fue reconocido por Whitehead y Russell en *Principia Mathematica* (Vol. II, *120.23). Una formulación esquemática del principio de inducción para los enteros no negativos es como sigue:

Si

(i) $\varphi(0)$

(ii) $(\forall n)(\varphi(n) \to \varphi(n+1))$,

entonces $(\forall n)\varphi(n)$.

En el capítulo siguiente demostramos este principio para los enteros. El principio de inducción correspondiente para un conjunto finito agrega la hipótesis de que el conjunto es finito y sustituye a (ii) por

$$(\forall x)(\forall B)(x \in A \;\&\; \varphi(B) \to \varphi(B \cup \{x\}),$$

la idea es la de que, si el conjunto A es finito, partimos del conjunto vacío y agregamos elementos de A, uno cada vez, hasta que agotemos a A.

La demostración del teorema relativo a inducción para conjuntos finitos se facilita si se dispone de la noción ya definida de *elemento máximo* de una familia de subconjuntos. Las demostraciones de los dos teoremas acerca de los elementos máximos se dejan como ejercicios.

Teorema 30. *Toda familia no vacia de subconjuntos de un conjunto finito tiene un elemento máximo.*

El segundo teorema es el recíproco del teorema 30 y los dos a la vez muestran que un conjunto finito puede ser definido en términos de toda familia no vacía de sus subconjuntos que tienen un elemento máximo.

Teorema 31. *Si toda familia, no vacia, de subconjuntos de un conjunto A tiene un elemento máximo, entonces A es finito.*

Estamos listos ahora para el primer teorema de inducción.

Esquema teoremático 32. *Si*

(i) *A es finito*,

(ii) $\varphi(0)$,

(iii) $(\forall x)(\forall B)(x \in A \;\&\; B \subseteq A \;\&\; \varphi(B) \rightarrow \varphi(B \cup \{x\}))$, *entonces* $\varphi(A)$.

Demostracion. Supongamos que valen (i) y (ii). Definimos

(1) $K = \{B\colon\ B \subseteq A \;\&\; \varphi(B)\}$.

El conjunto K no es vacío, ya que $0 \subseteq A$ y $\varphi(0)$; además, $0 \in K$. Por tanto, en virtud del teorema 30 y (i), K tiene un elemento máximo, digamos B. Queremos demostrar que $B = A$, y por tanto $\varphi(A)$. Supongamos que ocurriera que $B \neq A$. Sobre la base de (1), $B \subseteq A$, así que,

$$A \sim B \neq 0.$$

Sea $x \in A \sim B$. Entonces, $B \cup \{x\} \subseteq A$ y, en virtud de (iii), $\varphi(B \cup \{x\})$; por tanto,

$$B \cup \{x\} \in K,$$

lo que contradice que B sea un elemento máximo de K y demuestra que nuestra suposición es falsa. Q.E.D.

Tomando $\varphi(B)$ como '$B \in K$' inferimos inmediatamente, por el teorema 32, la siguiente formulación 'conjuntista' de inducción para conjuntos finitos. Es importante notar que el recíproco se cumple; a saber, el teorema 32 se sigue del teorema 33 si hacemos $K = \{B\colon\ B \in \mathcal{P}A \;\&\; \varphi(B)\}$.

Teorema 33.

(i) *A es finito*,

(ii) $0 \in K$,

(iii) $(\forall x)(\forall B)(x \in A \;\&\; B \subseteq A \;\&\; B \in K \rightarrow B \cup \{x\} \in K)$, *entonces* $A \in K$.

En el siguiente teorema se establece que esta propiedad inductiva de los conjuntos finitos puede usarse para caracterizarlos.

Teorema 34. *A es finito, si y sólo si A pertenece a todo conjunto K que satisface* (ii) *y* (iii) *del teorema 33.*

Demostración. La necesidad se sigue del teorema 33. Para demostrar la suficiencia, supongamos que A pertenece a todo conjunto K que satisface (ii) y (iii). Sea K_1 la familia de todos los subconjuntos finitos de A. En virtud del teorema 24, $0 \in K_1$. Más aún, si $B \in K_1$ y $x \in A$, entonces, por el teorema 29, $B \cup \{x\} \in K_1$, de donde, por hipótesis, $A \in K_1$, así que es finito. Q.E.D.

La definición de Sierpinski (1918), modificada ligeramente por Tarski, se da en el teorema siguiente, cuya demostración es semejante a la del que precede.

Teorema 35. *A es finito, si y sólo si A pertenece a todo conjunto K tal que*

(i) $0 \in K$,

(ii) *si* $x \in A$, *entonces* $\{x\} \in K$,

(iii) *si* $B \in K \;\&\; C \in K$, *entonces* $B \cup C \in K$.

La definición de Sierpinski fue modificada por Kuratowski [1920] y proporciona el siguiente teorema, cuya demostración se deja como ejercicio.

Teorema 36. *A es finito, si y solamente si el conjunto potencia $\mathcal{P}A$ es el único conjunto K que satisface las condiciones:*

(i) $K \subseteq \mathcal{P}A$,

(ii) $0 \in K$,

(iii) *si* $x \in A$, *entonces* $\{x\} \in K$,

(iv) *si* $B \in K$ & $C \in K$, *entonces* $B \cup C \in K$.

Nuestro objetivo siguiente es demostrar algunos hechos concernientes a la finitud del conjunto potencia y del conjunto suma de un conjunto dado. Demostramos antes un teorema preliminar, el cual establece que, si podemos aplicar A sobre B y A es finito, entonces B es finito.

Teorema 37. *Si A es finito y f es una función cuyo dominio es A y cuyo recorrido es B, entonces B es finito.*

Demostración. Definimos

$$K = \{C\colon C \subseteq A \,\&\, f``C \text{ es finito}\}.$$

Queremos demostrar, por inducción, (usando el teorema 33) que $A \in K$, por tanto B es finito, ya que $f``A = B$. Primero observamos, de manera inmediata, que $0 \in K$ porque $0 \subseteq A$ y $f``0 = 0$. Supongamos, para la segunda parte de la inducción, que $x \in A$ y $C \in K$. Necesitamos demostrar que $C \cup \{x\} \in K$. Obviamente, $C \cup \{x\} \subseteq A$. Puesto que f es una función, $f``\{x\}$ es un conjunto unitario y, por tanto, finito (teorema 25); ya que $C \in K$, $f``C$ es finito. Por consiguiente, en vista del teorema 28, $(f``C) \cup f``\{x\}$ es finito. Pero, en virtud del teorema 35 del capítulo 3,

$$f``(C \cup \{x\}) = (f``C) \cup f``\{x\},$$

y $f``(C \cup \{x\})$ es finito. Concluimos que

$$C \cup \{x\} \in K,$$

lo que completa la demostración. Q.E.D.

Teorema 38. *Si un conjunto es finito, entonces su conjunto potencia es finito.*

Demostración. Como en la demostración precedente, definimos un cierto conjunto y luego demostramos por inducción que A es un elemento de él. Definimos:

$$K = \{B\colon B \subseteq A \,\&\, \mathcal{P}B \text{ es finito}\}.$$

De nuevo es obvio que $0 \in K$. Supongamos, como es usual, para la segunda parte de la inducción, que $B \in K$ y $x \in A$. Si $x \in B$, la inducción es inmediata, así que podemos suponer que $x \notin B$. Claramente, $B \cup \{x\} \subseteq A$. Queda por demostrar que el conjunto potencia, $\mathcal{P}(B \cup \{x\})$, es finito, dado que $\mathcal{P}B$ es finito, para demostrar que $B \cup \{x\} \in K$. Definamos:

(1) $f = \{\langle C, C \cup \{x\}\rangle\colon C \in \mathcal{P}B\}$.

Demostramos ahora que f es una función cuyo recorrido es $\mathcal{P}(B \cup \{x\}) \sim \mathcal{P}B$. (Obviamente el dominio de f es $\mathcal{P}B$.) Es evidente, por (1), que f es una función. El problema es demostrar que su recorrido es el conjunto pedido. Si $C \in \mathcal{P}B$, entonces

$$C \cup \{x\} \in \mathcal{P}(B \cup \{x\}) \sim \mathcal{P}B$$

ya que $x \notin B$. Por otra parte, si

$$D \in \mathcal{P}(B \cup \{x\}) \sim \mathcal{P}B,$$

entonces $$D \sim \{x\} \in \mathcal{P}B,$$

por consiguiente, $\langle D \sim \{x\}, D\rangle \in f$.

Concluimos que $\mathcal{P}(B \cup \{x\}) \sim \mathcal{P}B$ es el recorrido de f. Aplicando ahora el teorema precedente y usando la hipótesis inductiva de que $\mathcal{P}B$ es finito, inferimos que $\mathcal{P}(B \cup \{x\}) \sim \mathcal{P}B$ es finito.

Notamos que

$$\mathcal{P}(B \cup \{x\}) = (\mathcal{P}(B \cup \{x\}) \sim \mathcal{P}B) \cup \mathcal{P}B$$

y ya que, en virtud del teorema 28, la unión de dos conjuntos finitos es finita, obtenemos que $\mathcal{P}(B \cup \{x\})$ es finito; por tanto,

$$B \cup \{x\} \in K,$$

lo que completa la inducción. Q.E.D.

Dejamos como ejercicio la demostración inductiva del siguiente teorema.

Teorema 39. *Si A es finito y todo conjunto que es elemento de A es finito, entonces $\bigcup A$ es finito.*

Los dos últimos teoremas se pueden usar para demostrar cada uno el recíproco del otro, esto es, el teorema 39 es útil para demostrar el recíproco del teorema 38 y viceversa. Dejamos estos dos recíprocos como ejercicios.

Teorema 40. *Si $\mathcal{P}A$ es finito, entonces A es finito.*

Teorema 41. *Si A es una familia de conjuntos y $\bigcup A$ es finito, entonces A es fi-*

nito y todo conjunto que sea un elemento de A es finito.

Nótese que el teorema 41 no es exactamente el recíproco del teorema 39, pues la hipótesis adicional requiere que A sea una familia de conjuntos. Obviamente, $\bigcup A$ podría ser finito y A infinito, siempre que A tenga solamente un número finito de conjuntos como elementos, ya que los elementos de A no contribuyen a $\bigcup A$.

Consideramos ahora algunos teoremas sobre equipotencia de conjuntos finitos. La demostración del primero se sigue, de una vez, a partir del teorema 37.

Teorema 42. *Si A es finito y $A \approx B$, entonces B es finito.*

Teorema 43. *Si A es finito y $B \preceq A$, entonces B es finito.*

Demostración. Dado que $B \preceq A$, entonces existe un subconjunto C de A tal que $B \approx C$; pero ya que A es finito, teniendo en cuenta el teorema 24, C es finito, así que por el teorema anterior y la simetría de la equipotencia, B es finito. Q.E.D.

Se mencionó, al final de la sección anterior, la ley de tricotomía, o sea, el teorema que afirma que para dos conjuntos A y B tenemos siempre: $A \prec B$, $A \approx B$, $B \prec A$ y esta ley es equivalente al axioma de escogencia. Sin embargo, sin el axioma de escogencia podemos demostrar, por inducción, la ley de tricotomía, si uno de los conjuntos es finito.

Teorema 44. *Si A es finito, entonces $A \prec B$, $A \approx B$ o $B \prec A$.*

Demostración. La inducción se realiza sobre subconjuntos de A. Definamos:

$$K = \{C\colon C \subseteq A \ \&\ (C \prec B, C \approx B \text{ o } B \prec C)\}.$$

Claramente, $0 \in K$, pues si $B = 0$, entonces $0 \approx B$; si $B \neq 0$, entonces $0 \prec B$. Para la segunda parte de la inducción suponemos, como es usual, que $C \in K$ y que $x \in A$; queremos demostrar que $C \cup \{x\} \in K$. El caso no trivial ocurre cuando $x \notin C$. Por hipótesis,

$$C \prec B, \quad C \approx B, \text{ o } B \prec C.$$

Estas tres posibilidades llevan a los tres casos:

Caso 1. $C \prec B$. Entonces existe un subconjunto propio D de B tal que $C \approx D$, bajo la función f, digamos. Puesto que D es un subconjunto propio de B, existe un y en $B \sim D$; por tanto,

$$f \cup \{\langle x, y\rangle\}$$

establece que

$$C \cup \{x\} \approx D \cup \{y\},$$

así que

$$C \cup \{x\} \preceq B,$$

lo cual implica

$$C \cup \{x\} \approx B \text{ o } C \cup \{x\} \prec B,$$

y, por consiguiente,

$$C \cup \{x\} \in K.$$

Caso 2. $C \approx B$. Puesto que $C \subseteq C \cup \{x\}$, se cumple que $C \approx C \cup \{x\}$ o que $C \prec C \cup \{x\}$. Si subsiste la primera alternativa, entonces $C \cup \{x\} \approx B$. Si subsiste la segunda, entonces $B \prec C \cup \{x\}$. En cualquier caso se sigue que $C \cup \{x\} \in K$.

Caso 3. $B \prec C$. Ya que $C \preceq C \cup \{x\}$, tenemos, de una vez, que $B \prec C \cup \{x\}$, así que $C \cup \{x\} \in K$. Q.E.D.

Es una consecuencia fácil del teorema que se acaba de demostrar (y de algunos resultados precedentes) que un conjunto finito tiene siempre menos potencia que uno que no es finito.

Teorema 45. *Si A es finito y B no lo es, entonces $A \prec B$.*

Podemos demostrar ahora el importante teorema de que un conjunto finito (en el sentido de Tarski) es un conjunto finito de Dedekind. Como se observó ya, toda demostración conocida de este teorema requiere el axioma de escogencia. Para referencia futura, es conveniente definir formalmente la finitud de Dedekind.

Definición 6. *Un conjunto es finito según Dedekind, si y solamente si no es* *equipotente a ninguno de sus subconjuntos propios.*

Demostramos ahora:

Teorema 46. *Si un conjunto es finito, entonces es finito según Dedekind.*

Demostración. Supongamos, contrario al teorema, que A es un conjunto finito con un subconjunto propio B tal que

$$A \approx B$$

bajo la función f, digamos. Definimos

$$K = \{C: C \subseteq A \,\&\, f``C \subset C\}.$$

Puesto que $f``A = B$ y $B \subset A$, vemos de una vez, que $A \in K$. Así que la familia K de subconjuntos de A no es vacía; además, puesto que A es finito, K tiene un elemento mínimo, digamos D. En consecuencia,

(1) $$f``D \notin K$$

pues $f``D \subset D$ y $D$ es un elemento mínimo. Por otra parte, en vista del hecho que $D \approx f``D$ y $f``D \subset D$, tenemos que

$$f``(f``D) \subset f``D,$$

así que

(2) $$f``D \in K,$$

pero (1) y (2) son, conjuntamente, absurdos y nuestra suposición es falsa. Q.E.D.

Dejamos como ejercicio demostrar tres consecuencias interesantes del teorema anterior. La tercera de éstas, que es equivalente al axioma de escogencia, ha sido demostrada por Tarski [1924a], cuando se ha eliminado la restricción a conjuntos finitos.

Teorema 47. *Si A es finito y $B \subset A$, entonces $B \prec A$.*

Teorema 48. *Si A, B y C son finitos y si $A \prec B$ y $B \cap C = 0$, entonces*

$$A \cup C \prec B \cup C.$$

Teorema 49. *Si A, B, C y D son finitos y si $A \prec B$, $C \prec D$ y $B \cap D = 0$, entonces*

$$A \cup C \prec B \cup D.$$

En el siguiente teorema se da una propiedad de conjuntos finitos, muy ligada a la finitud de Dedekind.

Teorema 50. *Si A es finito y $x \notin A$ entonces $A \prec A \cup \{x\}$.*

Cerramos el desarrollo sistemático de esta sección con dos útiles teoremas, el primero de los cuales demostramos.

Teorema 51. *El producto cartesiano de dos conjuntos finitos es finito.*

Demostración. Sean A y B conjuntos finitos. Si uno de los dos es vacío, $A \times B = 0$, de modo que podemos suponer que ninguno es vacío. Definimos

$$C = \{A \times \{y\} : y \in B\}.$$

Observamos que

$$\bigcup C = A \times B.$$

Además, sobre la base del teorema 8,

$$A \approx A \times \{y\},$$

por tanto, en virtud del teorema 42, $A \times \{y\}$ es finito. Pero $C \approx B$, y por consiguiente C es finito; además se sigue del teorema 39 que $\bigcup C$ es finito. Q.E.D.

Teorema 52. *Si A y B son finitos, entonces A^B es finito.*

Se pueden obtener propiedades adicionales de conjuntos finitos y definiciones equivalentes ulteriores, introduciendo nociones de orden; pero no trataremos estos tópicos aquí, excepto en algunas notas informales. Para más detalles, se refiere al lector a Tarski [1924b]. Stäckel [1907] propuso que los conjuntos finitos se definiesen como aquellos que pueden ser doblemente bien ordenados. Más exactamente, A es finito si y sólo si existe una relación R tal que R y $\breve{R}$ bien-ordenan A. Esta definición es equivalente, como se puede demostrar, a la definición de Tarski usada aquí (véase el teorema 37 del capítulo 5).

Algunos lectores pueden estar descontentos porque no se ha dicho nada esencial acerca de los conjuntos infinitos. Esta omisión ha sido deliberada, pues hasta que no se introduzca el axioma de infinitud y se demuestre la existencia del conjunto de los cardinales finitos o de los ordinales finitos, no se puede demostrar nada de mucho interés respecto de los conjuntos infinitos. Tales conjuntos se considerarán en la parte final del capítulo siguiente.

EJERCICIOS

1 Dar un ejemplo, diferente del que se ha dado en el texto, de una familia no vacía de conjuntos que no tenga un elemento mínimo o un elemento máximo.

2. Demostrar los teoremas 24 y 25.

3 Demostrar los teoremas 30 y 31.

4 Dar un ejemplo intuitivo para demostrar que el teorema 33 falla si se omite la hipótesis de que A sea finito.

5 Demostrar el teorema 35.

6. Demostrar el teorema 36.

7. Demostrar el teorema 39.

8. Demostrar los teoremas 40 y 41.

9. Demostrar el teorema 42.

10. Demostrar el teorema 45.

11. Demostrar los teoremas 47 a 49.

12. Demostrar el teorema 50.

13. Demostrar que cualquier subconjunto de un conjunto que es finito, según Dedekind, es también finito, según Dedekind.

14. Demostrar que, si $A \approx B$ y A es finito según Dedekind, entonces B es finito según Dedekind.

15. Demostrar que si $B \prec A$ y A es finito según Dedekind, entonces B es finito según Dedekind.

16 Demostrar el teorema 52.

§ 4.3 **Números cardinales.** La definición de Frege-Russell de números cardinales es bella en su simplicidad. El número cardinal $\overline{\overline{A}}$ del conjunto A es la clase de todos los conjuntos equipotentes con A, esto es

$$(1) \qquad \overline{\overline{A}} = \{B\colon B \approx A\}.$$

Cantor usó la doble barra para indicar dos niveles de abstracción. La primera barra significa que se abstrae de la naturaleza particular de los elementos del conjunto; la segunda barra, que se abstrae de su orden. (Estas ideas algo vagas de abstracción están representadas por la definición formal clara de $\overline{\overline{A}}$.)

Podemos, como ejemplo, definir los cardinales finitos cero, uno y dos. (Agregamos un sub-índice 'f' para indicar que estamos siguiendo la discusión original de Frege y de Russell.)

$$0_f = \{0\},$$

o sea que 0_f es el conjunto de todos los conjuntos que no tienen elementos;

$$1_f = \{A\colon (\exists x)(x \in A \ \&\ (\forall y)(y \in A \rightarrow x = y))\},$$

esto es, 1_f es el conjunto de todos los conjuntos unitarios; una definición equivalente, usando la relación de equipotencia, es:

$$1_f = \{A\colon A \approx \{0\}\}.$$

Procedemos en forma similar para definir:

$$2_f = \{A\colon A \approx \{0, \{0\}\}\},$$

o, de manera equivalente,

$$2_f = \{A\colon (\exists x)(\exists y)(x \in A \ \&\ y \in A \ \&\ x \neq y \ \&\ (\forall z)(z \in A \rightarrow z = x \vee z = y))\}.$$

Tenemos entonces resultados como

$$\{\text{Edgar Guest, T. S. Eliot}\} \in 2_f$$

y vemos que 2_f es simplemente el conjunto de todas las parejas.

También será útil, para propósitos de comparación, formular la definición clásica de adición entre números cardinales. Para mayor claridad establecemos:

$$\mathfrak{m} \text{ es un número cardinal} \leftrightarrow (\exists A)(\mathfrak{m} = \overline{\overline{A}}).$$

Definimos entonces:

Si $\mathfrak{m}$ y $\mathfrak{n}$ son números cardinales, entonces

$$(2) \quad \mathfrak{m} + \mathfrak{n} = \{C\colon (\exists A)(\exists B)(A \in \mathfrak{m} \ \&\ B \in \mathfrak{n} \ \&\ A \cap B = 0 \ \&\ C \approx A \cup B)\}.$$

La idea intuitiva de esta definición debe ser clara: el número cardinal que es la *suma* de dos números cardinales $\mathfrak{m}$ y $\mathfrak{n}$ es el conjunto de todos los conjuntos que son equipotentes a un conjunto que consiste de la unión de un elemento de $\mathfrak{m}$ y un elemento de $\mathfrak{n}$, previsto que los dos conjuntos elementos sean disjuntos. Por ejemplo, tenemos:

$$\{\text{C. P. Snow}\} \in 1_f,$$

$$\{\text{Jane Austen, Elizabeth Bowen}\} \in 2_f,$$

así que,

$$2_f + 1_f = 1_f + 2_f = \{A\colon A \approx \{\text{C. P. Snow}\} \cup \{\text{Jane Austen, Elizabeth Bowen}\}\}.$$

De una vez es obvio también que

$$2_f + 1_f = 3_f,$$

ya que

$$\{\text{C. P. Snow, Jane Austen, Elizabeth Bowen}\} \in 3_f.$$

Los desarrollos correspondientes de (1) y (2) en teoría de conjuntos intuitiva son realmente bonitos, pero dentro de nuestro enfoque axiomático no podemos demostrar que el conjunto A es diferente del conjunto vacío. Hay por lo menos tres caminos que podemos tomar para obtener los números cardinales en la teoría de conjuntos de Zermelo-Fraenkel. Uno es introducir una nueva idea primitiva y un axioma especial para números cardinales, que es lo que haremos en este capítulo. Un segundo camino es definir los números cardinales como cierto tipo de números ordinales. Esta definición requiere el axioma de escogencia para demostrar que todo conjunto tiene un número cardinal; esto se verá en el capítulo 8. Un tercer camino es operar con los axiomas actuales (y más adelante con el axioma de infinitud) por medio de la noción de *rango* de un conjunto, pero esta construcción es más bien complicada y no se discutirá aquí.

El axioma especial que introducimos requiere una nueva idea primitiva, a saber, la de número cardinal de un conjunto A (en símbolos, $\mathcal{K}(A)$). La idea intuitiva del axioma debe ser clara. Nos gustaría seguir a Frege y a Russell y definir los números cardinales como clases de equivalencia de conjuntos equipotentes, pero no podemos demostrar que existen las clases de equivalencia apropiadas. Así que postulamos que con cada conjunto A está asociado un objeto $\mathcal{K}(A)$, el número cardinal de A, tal que con dos conjuntos equipotentes asociamos el mismo número cardinal. Nótese que, sobre la base de este axioma y de los otros axiomas introducidos, no podemos demostrar que el número cardinal de un conjunto es él mismo un conjunto. Formalmente, el *axioma para números cardinales* es:

$$\mathcal{K}(A) = \mathcal{K}(B) \leftrightarrow A \approx B.$$

Más aún, junto con la introducción del nuevo término primitivo '$\mathcal{K}$' necesitamos extender la definición de la fórmula primitiva que aparece en §2.1 para incluir este término. Esta extensión amplía también el campo de acción del esquema axiomático de separación. Cualquier definición o teorema que dependa del nuevo axioma o que use el nuevo término primitivo '$\mathcal{K}$' estará marcado con '†'.*

Hasta donde yo sé, el primer uso explícito de este nuevo axioma se encuentra en Tarski [1924a]; en este artículo Tarski se propone demostrar que cierto conjunto de aserciones acerca de los números cardinales es equivalente al axioma de escogencia. Naturalmente para este efecto necesitó construir los números cardinales sin usar el axioma de escogencia. Los desarrollos sistemáticos de este capítulo no siguen el artículo de Tarski, el cual está relacionado con cuestiones más avanzadas y especiales que las que estamos interesados en considerar en este momento. Una de las mejores presentaciones no axiomáticas de las ideas tratadas en esta sección se encuentra en los capítulos 2 y 5 de Sierpinski [1928] (véase también Sierpinski [1958]).

Nuestro principal objetivo en esta sección es desarrollar la aritmética elemental de los números cardinales. No distinguiremos entre cardinales finitos e infinitos en esta etapa. Si bien se pueden demostrar unos pocos teoremas especiales acerca de cardinales infinitos, nada de mucho interés es posible sin el axioma de infinitud y el conjunto de cardinales finitos. En efecto, la presente sección puede aprovecharse para apreciar cuánta aritmética elemental de cardinales es independiente de la distinción entre conjuntos finitos e infinitos.

* Nótese que, independientemente del axioma, podemos demostrar que

(1) $(\exists x)(\mathcal{K}(A) = x)$,

una vez que admitimos el término primitivo '$\mathcal{K}$', pues es una verdad de lógica que $\mathcal{K}(A) = \mathcal{K}(A)$, y (1) es una consecuencia lógica de esta verdad.

Usamos letras alemanas minúsculas '$\mathfrak{m}$', '$\mathfrak{n}$', '$\mathfrak{p}$', '$\mathfrak{q}$', '$\mathfrak{r}$', con o sin sub-índices para simbolizar números cardinales. Definimos para cualquier objeto x:

> †**Definición 7.** *x es un número cardinal si y sólo si existe un conjunto A tal que $\mathcal{K}(A) = x$.*

Pero, como antes, en situaciones similares, omitiremos la hipótesis 'es un número cardinal' en los teoremas y definiciones subsiguientes y usaremos el tipo especial de letra indicado ya. Las demostraciones de la mayor parte de los teoremas se siguen directamente de los teoremas apropiados de § 4.1.

Una herramienta importante en lo que sigue es el teorema que afirma que, dados dos números cardinales cualesquiera, podemos determinar dos conjuntos mutuamente disjuntos que corresponden a los dos números cardinales.

> †**Teorema 53.** *Existen conjuntos A y B tales que*
>
> (i) $A \cap B = 0$,
> (ii) $\mathcal{K}(A) = \mathfrak{m}$,
> (iii) $\mathcal{K}(B) = \mathfrak{n}$.

Demostración. En vista de la definición 7, existen conjuntos A' y B' tales que $\mathcal{K}(A') = \mathfrak{m}$ y $\mathcal{K}(B') = \mathfrak{n}$; además, en virtud del teorema 9, existen conjuntos A y B tales que $A \cap B = 0$, $A \approx A'$ y $B \approx B'$. Por el axioma para cardinales, entonces, $\mathcal{K}(A) = \mathfrak{m}$ y $\mathcal{K}(B) = \mathfrak{n}$. Q.E.D.

Podemos definir la adición de una manera muy similar a la de Cantor, pero primero necesitamos demostrar el teorema justificante apropiado.

> †**Teorema 54.** *Existe exactamente un número cardinal $\mathfrak{p}$ y existen conjuntos A y B tales que*
>
> (i) $A \cap B = 0$,
> (ii) $\mathcal{K}(A) = \mathfrak{m}$,
> (iii) $\mathcal{K}(B) = \mathfrak{n}$,
> (iv) $\mathcal{K}(A \cup B) = \mathfrak{p}$.

Demostración. (i) - (iii) se siguen inmediatamente, a partir del teorema precedente y la existencia de $\mathfrak{p}$ es una verdad de lógica. Queremos demostrar que $\mathfrak{p}$ es independiente de los conjuntos particulares A y B.

Supongamos que existieran los conjuntos A' y B' y un número cardinal $\mathfrak{p}'$ tal que

(1) $A' \cap B' = 0$

(2) $\mathcal{K}(A') = \mathfrak{m}$

(3) $\mathcal{K}(B') = \mathfrak{n}$

(4) $\mathcal{K}(A' \cup B') = \mathfrak{p}'$.

Se sigue del axioma para cardinales y de (2) y (3) que

(5) $A' \approx A$

(6) $B' \approx B$.

En virtud del teorema (4) inferimos de (5) y (6) que

$$A' \cup B' \approx A \cup B,$$

por consiguiente, por el axioma para cardinales,

$$\mathcal{K}(A' \cup B') \doteq \mathcal{K}(A \cup B)$$

o sea

$$\mathfrak{p}' = \mathfrak{p},$$

que era lo que se quería demostrar. Q.E.D.

Con el teorema 54 a la mano, podemos definir la adición entre números cardinales.

> † **Definición 8.** $\mathfrak{m} + \mathfrak{n} = \mathfrak{p}$ *si y sólo si existen conjuntos A y B tales que*
>
> (i) $A \cap B = 0$,
> (ii) $\mathcal{K}(A) = \mathfrak{m}$,
> (iii) $\mathcal{K}(B) = \mathfrak{n}$,
> (iv) $\mathcal{K}(A \cup B) = \mathfrak{p}$.

Podemos demostrar fácilmente que la adición entre cardinales es conmutativa y asociativa.

> †**Teorema 55.** $\mathfrak{m} + \mathfrak{n} = \mathfrak{n} + \mathfrak{m}$.

Demostración. En virtud del teorema 53, existen conjuntos A y B tales que $A \cap B = 0$,

$\mathcal{K}(A) = \mathfrak{m}$, y $\mathcal{K}(B) = \mathfrak{n}$, por tanto, por la definición 8,

$$\mathcal{K}(A \cup B) = \mathfrak{m} + \mathfrak{n},$$

y

$$\mathcal{K}(B \cup A) = \mathfrak{n} + \mathfrak{m},$$

pero

$$A \cup B = B \cup A,$$

por consiguiente

$$\mathfrak{m} + \mathfrak{n} = \mathfrak{n} + \mathfrak{m}. \qquad \text{Q.E.D.}$$

†**Teorema 56.** $(\mathfrak{m} + \mathfrak{n}) + \mathfrak{p} = \mathfrak{m} + (\mathfrak{n} + \mathfrak{p})$.

Demostración. La demostración se sigue de la asociatividad de la operación unión entre conjuntos. Q.E.D.

Definimos el número cardinal $\mathbf{0}$ de la manera obvia, lo mismo que los números cardinales 1 y 2.

† **Definición 9.**

$$\mathbf{0} = \mathcal{K}(0)$$

$$\mathbf{1} = \mathcal{K}(\{0\})$$

$$\mathbf{2} = \mathcal{K}(\{0, \{0\}\}).$$

Y tenemos el teorema cuya sencilla demostración omitimos:

† **Teorema 57.** $\mathfrak{m} + \mathbf{0} = \mathfrak{m}$.

Nos referimos ahora a la multiplicación entre cardinales. La idea simple consiste en que la multiplicación entre cardinales corresponde al producto cartesiano entre conjuntos, que es, obviamente, el caso para los cardinales finitos. Así, si A tiene 3 elementos y B tiene 4 elementos, entonces $A \times B$ tiene $3 \cdot 4 = 12$ elementos.

De nuevo necesitamos un teorema justificante.

†**Teorema 58.** *Existe exactamente un número cardinal* $\mathfrak{p}$ *y existen conjuntos* A *y* B *tales que*

(i) $\mathcal{K}(A) = \mathfrak{m}$
(ii) $\mathcal{K}(B) = \mathfrak{n}$
(iii) $\mathcal{K}(A \times B) = \mathfrak{p}$.

Demostración. (i)-(ii) y la existencia de $\mathfrak{p}$ son inmediatas. Supongamos ahora que existiesen conjuntos A', B' y un número cardinal $\mathfrak{p}'$ tales que

(1) $\mathcal{K}(A') = \mathfrak{m}$
(2) $\mathcal{K}(B') = \mathfrak{n}$
(3) $\mathcal{K}(A' \times B') = \mathfrak{p}'$.

Entonces (1), (2) y el axioma para cardinales dan:

$$A' \approx A$$

$$B' \approx B,$$

por tanto, por el teorema 5,

$$A' \times B' \approx A \times B,$$

así que,

$$\mathcal{K}(A' \times B') = \mathcal{K}(A \times B);$$

y entonces

$$\mathfrak{p}' = \mathfrak{p}. \qquad \text{Q.E.D.}$$

Denotamos la multiplicación, como es acostumbrado, mediante yuxtaposición; ocasionalmente se usará un punto para efecto de claridad.

† **Definición 10.** $\mathfrak{m}\mathfrak{n} = \mathfrak{p}$ *si y sólo si existen conjuntos* A *y* B *tales que*

(i) $\mathcal{K}(A) = \mathfrak{m}$
(ii) $\mathcal{K}(B) = \mathfrak{n}$
(iii) $\mathcal{K}(A \times B) = \mathfrak{p}$.

La conmutatividad y la asociatividad de la multiplicación cardinal se siguen, de una vez, del hecho que la operación producto cartesiano entre conjuntos tiene esas propiedades en lo que respecta a equipotencia.

† **Teorema 59.** $\mathfrak{m}\mathfrak{n} = \mathfrak{n}\mathfrak{m}$.

Demostración. Usar el teorema 6.

† **Teorema 60.** $(\mathfrak{m}\mathfrak{n})\mathfrak{p} = \mathfrak{m}(\mathfrak{n}\mathfrak{p})$.

Demostración. Usar el teorema 7.

† **Teorema 61.** $\mathfrak{m} \cdot \mathbf{1} = \mathfrak{m}$.

Demostración. Sea

$$\mathcal{K}(A) = \mathfrak{m}.$$

Sabemos que

$$\mathcal{K}(\{0\}) = \mathbf{1},$$

y a partir de la definición de multiplicación

$$\mathcal{K}(A \times \{0\}) = \mathfrak{m} \cdot \mathbf{1},$$

pero, sobre la base del teorema 8, sabemos que

$$A \times \{0\} \approx A,$$

por consiguiente,

$$\mathcal{K}(A \times \{0\}) = \mathfrak{m}$$

así que,

$$\mathfrak{m} \cdot \mathbf{1} = \mathfrak{m}. \qquad \text{Q.E.D.}$$

Dejamos como ejercicio la demostración del teorema según el cual la multiplicación cardinal es distributiva con respecto a la adición cardinal.

†**Teorema 62.** $\mathfrak{m}(\mathfrak{n} + \mathfrak{p}) = \mathfrak{m}\mathfrak{n} + \mathfrak{m}\mathfrak{p}$.

El conjunto A^B de todas las funciones de B hacia A es la base para definir exponenciación de cardinales. Comenzamos, como es usual, con el teorema justificante, cuya demostración omitimos en este caso. El teorema preciso que debe usarse en la demostración es el teorema 10 de § 4.1.

† **Teorema 63.** *Existe exactamente un número cardinal* $\mathfrak{p}$ *y existen los conjuntos* A *y* B *tales que*

(i) $\mathcal{K}(A) = \mathfrak{m}$,
(ii) $\mathcal{K}(B) = \mathfrak{n}$,
(iii) $\mathcal{K}(A^B) = \mathfrak{p}$.

† **Definición 11.** $\mathfrak{m}^\mathfrak{n} = \mathfrak{p}$ *si y solamente si existen conjuntos* A *y* B *tales que*

(i) $\mathcal{K}(A) = \mathfrak{m}$,
(ii) $\mathcal{K}(B) = \mathfrak{n}$,
(iii) $\mathcal{K}(A^B) = \mathfrak{p}$.

Escogiendo el teorema apropiado de §4.1 se demuestran fácilmente los tres siguientes teoremas acerca de exponentes.

† **Teorema 64.** $\mathfrak{m}^{\mathfrak{n}+\mathfrak{p}} = \mathfrak{m}^\mathfrak{n}\mathfrak{m}^\mathfrak{p}$.

† **Teorema 65.** $(\mathfrak{m}\mathfrak{n})^\mathfrak{p} = \mathfrak{m}^\mathfrak{p}\mathfrak{n}^\mathfrak{p}$.

† **Teorema 66.** $(\mathfrak{m}^\mathfrak{n})^\mathfrak{p} = \mathfrak{m}^{\mathfrak{n}\mathfrak{p}}$.

También podemos demostrar fácilmente:

† **Teorema 67.** $\mathfrak{m}^1 = \mathfrak{m}$.

† **Teorema 68.** $\mathfrak{m}^0 = \mathbf{1}$.

† **Teorema 69.** *Si* $\mathfrak{m} \neq \mathbf{0}$ *entonces,* $\mathbf{0}^\mathfrak{m} = \mathbf{0}$.

Concluimos esta sección con algunos pocos teoremas sobre desigualdades entre números cardinales.

† **Definición 12.** $\mathfrak{m} \leq \mathfrak{n}$ *si y solamente si existen conjuntos* A *y* B *tales que*

(i) $\mathcal{K}(A) = \mathfrak{m}$
(ii) $\mathcal{K}(B) = \mathfrak{n}$
(iii) $A \preceq B$.

Se demuestra fácilmente que

† **Teorema 70.** $\mathfrak{m} \leq \mathfrak{n}$ *si y solamente si, para todos los* A *y los* B, *si* $\mathcal{K}(A) = \mathfrak{m}$ *y* $\mathcal{K}(B) = \mathfrak{n}$, *entonces* $A \preceq B$.

A partir de los teoremas 1 y 15 se sigue, de una vez, que

† **Teorema 71.** $\mathfrak{m} \leq \mathfrak{m}$.

Usando el teorema 17, podemos demostrar:

† **Teorema 72.** *Si* $\mathfrak{m} \leq \mathfrak{n}$ *y* $\mathfrak{n} \leq \mathfrak{p}$, *entonces* $\mathfrak{m} \leq \mathfrak{p}$.

A partir del teorema de Schröder-Bernstein (teorema 18), inferimos que $\leq$ es antisimétrica.

†**Teorema 73.** *Si* $\mathfrak{m} \leq \mathfrak{n}$ *y* $\mathfrak{n} \leq \mathfrak{m}$, *entonces* $\mathfrak{m} = \mathfrak{n}$.

También ocurre que las tres operaciones introducidas son monotónicas con respecto a la relación $\leq$. La demostración se sigue directamente del teorema 19 de §4.1.

† **Teorema 74.** *Si* $\mathfrak{m} \leq \mathfrak{n}$ *y* $\mathfrak{m}' \leq \mathfrak{n}'$, *entonces*

(i) $\mathfrak{m} + \mathfrak{m}' \leq \mathfrak{n} + \mathfrak{n}'$,
(ii) $\mathfrak{m}\mathfrak{m}' \leq \mathfrak{n}\mathfrak{n}'$,
(iii) $\mathfrak{m}^{\mathfrak{m}'} \leq \mathfrak{n}^{\mathfrak{n}'}$.

Sobre la base del teorema 20, tenemos:

† **Teorema 75.** $\mathfrak{m} \leq \mathfrak{m} + \mathfrak{n}$.

Podemos definir la desigualdad estricta, de la manera aritmética.

†**Definición 13.** $\mathfrak{m} < \mathfrak{n}$ *si y solamente si* $\mathfrak{m} \leq \mathfrak{n}$ *y* $\mathfrak{m} \neq \mathfrak{n}$.

Podemos demostrar entonces:

† **Teorema 76.** $\mathfrak{m} < \mathfrak{n}$ *si y solamente si existen conjuntos* A *y* B *tales que*

(i) $\mathcal{K}(A) = \mathfrak{m}$,
(ii) $\mathcal{K}(B) = \mathfrak{n}$,
(iii) $A \prec B$.

Tenemos tres propiedades obvias enunciadas en el siguiente teorema, que corresponde al teorema 21.

† **Teorema 77.**

(i) *No* $\mathfrak{m} < \mathfrak{m}$,
(ii) *si* $\mathfrak{m} < \mathfrak{n}$ *, entonces no* $\mathfrak{n} < \mathfrak{m}$,
(iii) *si* $\mathfrak{m} < \mathfrak{n}$ *y* $\mathfrak{n} < \mathfrak{p}$*, entonces* $\mathfrak{m} < \mathfrak{p}$.

Nótese que la aserción $\mathfrak{m} < \mathfrak{n}$, $\mathfrak{m} = \mathfrak{n}$, o $\mathfrak{n} < \mathfrak{m}$ es simplemente la ley de tricotomía para números cardinales. Como se puntualizó ya, la equivalencia de esta ley con el axioma de escogencia se demostrará en el capítulo 8. Lo que es también importante y sorprendente, es que, si preguntamos bajo qué circunstancias subsisten las propiedades de monotonía expresadas en el teorema 74, con respecto a la desigualdad estricta $<$, la respuesta es, como demuestra Tarski [1924a], que (iii) no se cumple y tanto (i) como (ii) son *equivalentes* con el axioma de escogencia.

Una propiedad importante que podemos demostrar sin el axioma de escogencia es:

† **Teorema 78.** $\mathfrak{m} < 2^{\mathfrak{m}}$.

Demostración. Seleccionemos A de modo que

$$\mathcal{K}(A) = \mathfrak{m}.$$

Entonces

$$\mathcal{K}(\{0, \{0\}\}^A) = 2^{\mathfrak{m}}.$$

Además, en virtud del teorema 14,

$$\mathcal{P}A \approx \{0, \{0\}\}^A,$$

y en vista del teorema 23

$$A \prec \mathcal{P}A,$$

por tanto, por el teorema 22,

$$A \prec \{0, \{0\}\}^A.$$

Así que por el teorema 76,

$$\mathfrak{m} < 2^{\mathfrak{m}}. \qquad \text{Q.E.D.}$$

El teorema siguiente establece que no hay un número cardinal que sea el mayor de todos. La demostración sigue las líneas de la deducción de la paradoja de Cantor, que se discutió en §1.4.

†**Teorema 79.** *Para todo* $\mathfrak{m}$ *existe un* $\mathfrak{n}$ *tal que* $\mathfrak{m} < \mathfrak{n}$.

Demostración. Supongamos que no; esto es, supongamos que hay un número cardinal $\mathfrak{m}$ mayor que todos. En virtud de la definición 7, existe entonces un conjunto A tal que

$$\mathcal{K}(A) = \mathfrak{m}.$$

Por otra parte, a partir del axioma para números cardinales, sabemos que existe un $\mathfrak{n}$ que es el número cardinal del conjunto potencia de A, o sea,

$$\mathcal{K}(\mathcal{P}A) = \mathfrak{n}.$$

En vista del teorema 23,

$$A \prec \mathcal{P}A,$$

así que, por el teorema 76,

$$\mathfrak{m} < \mathfrak{n},$$

lo que es contrario a nuestra suposición.

Q.E.D.

Definimos la noción de *sucesor* $\mathfrak{m}'$ de un número cardinal $\mathfrak{m}$, para usarla en relación con la teoría de cardinales finitos en la sección siguiente. En la teoría de los números ordinales, el sucesor de cualquier conjunto A es $A \cup \{A\}$ o $A \cup \{x\}$ para $x \notin A$. Es adecuado un enfoque similar aquí.

† **Definición 14.** $\mathfrak{m}' = \mathfrak{n}$ *si y solamente si existe un conjunto* A *tal que* $\mathcal{K}(A) = \mathfrak{m}$ & $\mathcal{K}(A \cup \{A\}) = \mathfrak{n}$.

Concluimos esta sección con tres teoremas acerca de la función sucesor y una definición más.

† **Teorema 80.** *Si* $\mathfrak{m}' = \mathfrak{n}'$ *entonces* $\mathfrak{m} = \mathfrak{n}$.

Demostración. Sea

$$\mathcal{K}(A) = \mathfrak{m}$$
$$\mathcal{K}(B) = \mathfrak{n}.$$

Entonces, por hipótesis,

$$A \cup \{A\} \approx B \cup \{B\}$$

bajo la función f, digamos. Entonces, $A \approx B$ bajo la función g definida por

$$g = \begin{cases} f|A \text{ si } f(A) = B \\ (f \cup \{\langle f^{-1}(B), f(A)\rangle\}) \sim \{\langle A, f(A)\rangle, \langle f^{-1} \\ (B), B\rangle\} \end{cases}$$

Pero ya que $A \approx B$ se sigue, del axioma para números cardinales, que $\mathfrak{m} = \mathfrak{n}$. Q.E.D.

† **Teorema 81.** $\mathfrak{m}' = \mathfrak{m} + 1$.

† **Teorema 82.** *No es el caso de que exista un* $\mathfrak{n}$ *tal que* $\mathfrak{m} < \mathfrak{n} < \mathfrak{m}'$.

Demostración. Supongamos que hubiese un $\mathfrak{n}$ tal; sea

$$\mathcal{K}(A) = \mathfrak{m}$$
$$\mathcal{K}(B) = \mathfrak{n}.$$

Entonces, por hipótesis

(1) $$A \prec B$$

(2) $$B \prec A \cup \{A\}.$$

Supongamos que (2) se ha establecido por una función f, digamos. Debe haber un subconjunto propio C de $A \cup \{A\}$ tal que

$$B \approx C$$

bajo f. Supongamos que A mismo no está en el recorrido de f; entonces $B \preceq A$, lo que contradice (1) y el teorema 22 de § 4.1. Así que A está en el recorrido de f y debe existir un elemento x en $A \sim C$. Definamos la función h por:

$$h = (f \cup \{\langle f^{-1}(A), x\rangle\}) \sim \{\langle f^{-1}(A), A\rangle\}.$$

Entonces, claramente,

$$B \preceq A$$

bajo h, lo que contradice de nuevo (1), así que nuestra suposición es absurda.

Q.E.D.

Definamos, también para su uso en la sección siguiente, el conjunto de todos los precedentes de un número cardinal. Sin usar el esquema axiomático de sustitución, el cual se introduce más adelante, no podemos demostrar que para un cardinal arbitrario este conjunto no es vacío, pero podemos demostrar esto por inducción, para cardinales finitos mayores que $\mathbf{0}$.

† **Definición 15.** $\mathfrak{Q}(\mathfrak{m}) = \{\mathfrak{n} : \mathfrak{n} < \mathfrak{m}\}$.

Así que, $\mathfrak{Q}(\mathbf{0}) = \mathbf{0}$ y $\mathfrak{Q}(1) = \{\mathbf{0}\}$.

Todo teorema de aritmética que se formule en esta sección debe ser familiar al lector, desde el punto de vista de expresar una propiedad de los números naturales dados intuitivamente. Es importante recordar que estos teoremas subsisten también para cardinales infinitos o transfinitos y que no toda propiedad familiar de los números naturales es compartida por los cardinales infinitos. Por ejemplo, si $\mathfrak{m}$ es un cardinal finito, entonces

$$\mathfrak{m} < \mathfrak{m} + 1,$$

como era de esperarse, pero si $\mathfrak{m}$ es un cardinal transfinito,

$$\mathfrak{m} = \mathfrak{m} + 1.$$

También la suma de dos cardinales transfinitos es siempre igual o menor que su producto, lo que no es cierto para cardinales finitos (ya que $1 + 2 > 1 \cdot 2$).

En caso de que el lector esté confundido por el uso de las frases 'cardinal finito', 'cardinal infinito', 'cardinal transfinito', puede decirse que los tópicos denotados por esas frases se explicarán más adelante. En la sección siguiente discutiremos los cardinales finitos y en la parte final del capítulo siguiente, distinguiremos entre cardinales infinitos y cardinales transfinitos; $\mathfrak{m}$ es un cardinal infinito si existe un conjunto infinito A tal que $\mathcal{K}(A) = \mathfrak{m}$; $\mathfrak{m}$ es un cardinal transfinito si existe un conjunto A, infinito según Dedekind, tal que $\mathcal{K}(A) = \mathfrak{m}$. Como es obvio, a partir de las notas de la sección que trata de conjuntos finitos, cualquier demostración conocida requiere el axioma de escogencia para demostrar que un cardinal es infinito si y sólo si es transfinito.

EJERCICIOS

1. Demostrar en detalle el teorema 56.
2. Demostrar el teorema 57.
3. Demostrar el teorema 62.
4. Demostrar el teorema 63.
5. Demostrar los teoremas 64 a 66.
6. Demostrar los teoremas 67 a 69.
7. Demostrar el teorema 70.
8. Demostrar el teorema 73.
9. Demostrar el teorema 76.
10. Para cada uno de los casos siguientes, demostrar que se cumple o dar un contra-ejemplo.
    (a) $\mathcal{K}(A \sim B) \leq \mathcal{K}(A)$,
    (b) $\mathcal{K}(A \sim B) \leq \mathcal{K}(B)$,
    (c) Si $B \subseteq A$, entonces $\mathcal{K}(A) = \mathcal{K}(A \sim B) + \mathcal{K}(B)$,
    (d) $\mathcal{K}(A \cap B) = \mathcal{K}(A)$ si y solamente si $A \subseteq B$,
    (e) $\mathcal{K}(A \times (B \sim C)) = 0$ si y solamente si $A = 0$ o $B = 0$ o $B = C$.
11. Demostrar el teorema 81.
12. Considérese la definición 15. Con los axiomas dados atrás, ¿qué dificultad se encuentra al tratar de demostrar que $\mathfrak{n} \in \mathfrak{Q}(\mathfrak{m})$ si y sólo si $\mathfrak{n} < \mathfrak{m}$?

§ 4.4 Cardinales finitos. Ahora combinamos los resultados de las secciones que tratan de conjuntos finitos y de números cardinales, para definir los números cardinales (a los cuales llamaremos *cardinales finitos* por brevedad) y demostramos que ellos tienen las propiedades que se esperan de los números naturales dados intuitivamente (es decir, enteros no negativos). Al usar la frase 'números naturales dados intuitivamente' no queremos implicar que los números naturales son entidades abstractas bien definidas, distintas, pero con muchas propiedades en común con los cardinales finitos. Los matemáticos han estado de acuerdo por algún tiempo sobre lo que deben ser las propiedades esenciales de los números naturales. En esta sección demostramos que los cardinales finitos —y más adelante los ordinales finitos— tienen estas propiedades, aun cuando los cardinales finitos y los ordinales no son necesariamente las mismas entidades.

Hay, desde luego, una distinción esencial entre nuestra construcción de los cardinales y la de los ordinales. Los ordinales son conjuntos particulares, específicos, en tanto que los cardinales son objetos que no podemos clasificar aún como conjuntos o individuos. A este respecto nuestra posición con respecto al carácter de los cardinales es semejante a la del matemático laborioso respecto a los números naturales: no está interesado en una definición explícita de los números naturales en términos de otras entidades conocidas, sino solamente en conocer sus propiedades matemáticas esenciales. En particular requiere que los números naturales satisfagan a los cinco axiomas de Peano, los cuales pueden formularse en lógica elemental, independientes de la teoría de conjuntos. Estos axiomas están basados en tres símbolos primitivos: el predicado "es un número natural", el símbolo de operación unaria '$'$' para la función sucesor (intuitivamente, $x' = x + 1$), y la constante individual '0' para el número cero. Los axiomas de Peano son:

P1. 0 *es un número natural.*
P2. *Si* x *es un número natural, entonces* x' *es un número natural.*
P3. *No existe ningún número natural* x *tal que* $x' = 0$.
P4. *Si* x *y* y *son números naturales y* $x' = y'$, *entonces* $x = y$.
P5. *Si* $\varphi(0)$ *y, para cualquier número natural* x, *si* $\varphi(x)$ *entonces* $\varphi(x')$, *entonces, para todo número natural* x, $\varphi(x)$.

El axioma P2 dice que el sucesor de cualquier número natural es un número natural. El axioma P3 dice que cero no es el sucesor de ningún número natural, o sea que expresa el hecho intuitivamente obvio de que no hay número natural x tal que

$$x + 1 = 0.$$

El axioma P4 afirma que la función sucesor es 1-1. El axioma P5 es realmente un esquema axiomático que expresa el principio de inducción para los números naturales.

Es una pregunta apropiada y no una vana especulación filosófica, la de por qué los matemáticos están casi uniformemente de acuerdo sobre los axiomas de Peano. Antes de que se formularan axiomas adecuados, se demostraron teoremas difíciles y profundos sobre los números naturales. Los axiomas putativos que no dieron lugar a esos teoremas debieron ser excluidos, porque parece que, independientemente de cualquier axioma, existe una noción bastante precisa de lo que es verdadero o falso respecto de los números naturales. El autor no está preparado para hacer una descripción exacta de esas nociones intuitivas y sería demasiada divagación el examinar lo que otras personas han dicho sobre estos tópicos. Pero debería puntualizarse que, decir que los números naturales *son* los cardinales finitos o los ordinales finitos, no significa hacer una descripción exacta, pues esas ideas intuitivas pero precisas acerca de los números naturales se usan, ellas mismas, para decidir si la identificación propuesta es aceptable.

Prosiguiendo ahora con los desarrollos formales, definimos cardinales finitos como cardinales de conjuntos finitos, donde por conjunto finito se entiende un conjunto finito en el sentido de Tarski.*

† **Definición 16.** *x es un número cardinal si y solamente si existe un conjunto finito A tal que* $\mathcal{K}(A) = x$.†

Comenzamos por demostrar los axiomas de Peano para los cardinales finitos.

†**Teorema 83. 0** *es un cardinal finito.*

Demostración. Es inmediata, a partir de la definición 9 y del teorema 24.

†**Teorema 84.** *Si* $\mathfrak{m}$ *es un cardinal finito, entonces* $\mathfrak{m}'$ *es un cardinal finito.*

Demostración. Sobre la base de la hipótesis de que $\mathfrak{m}$ es un cardinal finito, existe un conjunto finito A tal que $\mathcal{K}(A) = \mathfrak{m}$, y en virtud de la definición de la función sucesor,

$$\mathcal{K}(A \cup \{A\}) = \mathfrak{m}'$$

y se sigue del hecho que A es finito y del teorema 29 que $A \cup \{A\}$ es finito; por consiguiente, $\mathfrak{m}'$ es un cardinal finito. Q.E.D.

†**Teorema 85.** *No hay ningún cardinal finito* $\mathfrak{m}$ *tal que* $\mathfrak{m}' = \mathbf{0}$.

Demostración. Supongamos, por vía de contradicción, que hubiera un tal $\mathfrak{m}$. Supongamos que $\mathcal{K}(A) = \mathfrak{m}$. Entonces, a partir de la definición de 0 y sucesor y del axioma para cardinales,

$$A \cup \{A\} = 0,$$

lo que es absurdo. Q.E.D.

La demostración del axioma P4 de Peano para cardinales finitos es inmediata a partir del teorema 80 y no necesita ser formulado.

Finalmente, para demostrar el principio de inducción para cardinales finitos usamos el principio de inducción para conjuntos finitos (teorema 33).

†**Esquema teoremático 86.** *Si*

(i) $\varphi(\mathbf{0})$,

(ii) *para todo cardinal finito* $\mathfrak{m}$ *si* $\varphi(\mathfrak{m})$ *entonces* $\varphi(\mathfrak{m}')$,

entonces, para todo cardinal finito $\mathfrak{m}$, $\varphi(\mathfrak{m})$.

Demostración. Supongamos que hubiera un cardinal finito $\mathfrak{m}$ para el cual $\varphi(\mathfrak{m})$ es

* No he visto desarrollada la teoría de cardinales finitos, sobre esta base, en la literatura; pero parece ser un enfoque bastante natural.

† No introducimos un tipo de letra especial para cardinales finitos, pues reservamos las letras minúsculas en bastardilla '*m*', '*n*', '*p*', '*q*', '*r*' para ordinales finitos. La razón para esto es la de que en el capítulo 6 construimos los números racionales y los reales a partir de los ordinales finitos, en lugar de los cardinales finitos, para no hacer que esta construcción dependa del axioma para números cardinales.

falso. Sea A un conjunto finito tal que $\mathcal{K}(A) = \mathfrak{m}$. Deducimos una contradicción, por inducción sobre subconjuntos de A. Definamos: $L = \{B: B \subseteq A \ \& \ \varphi(\mathcal{K}(B))\}$.

A partir de (i) de la hipótesis, sabemos que $0 \in$ L. Supongamos ahora para la inducción que $B \in L$ y $x \in A \sim B$. A partir de la definición de L el conjunto B es finito porque es un subconjunto del conjunto finito A. Queremos demostrar que $\varphi(\mathcal{K}(B \cup \{x\}))$. Observemos primero que, evidentemente,

(1) $$B \cup \{B\} \approx B \cup \{x\}.$$

Sea $\mathcal{K}(B) = \mathfrak{n}$. Entonces, por (ii) de la hipótesis y del hecho que $B \in L$ y por tanto $\varphi(\mathcal{K}(B))$, inferimos $\varphi(\mathfrak{n}')$, pero

(2) $$\mathcal{K}(B \cup \{B\}) = \mathfrak{n}',$$

por consiguiente, a partir de (1), (2) y del axioma para cardinales,

$$\mathcal{K}(B \cup \{x\}) = \mathfrak{n}',$$

así que $\varphi(\mathcal{K}(B \cup \{x\}))$ y $B \cup \{x\} \in L$. Se sigue entonces, del teorema 33, que $A \in L$ y, por tanto, $\varphi(\mathcal{K}(A))$, esto es, $\varphi(\mathfrak{m})$, lo que contradice nuestra suposición. Q.E.D.

Cimentando en estos cinco teoremas y en el desarrollo general de la aritmética cardinal de § 4.3, se construye fácilmente la aritmética elemental completa de adición, multiplicación y exponenciación.

Formulamos, sin demostración, cuatro teoremas acerca de la relación *menor que*. Las demostraciones son inmediatas, a partir de hechos relativos a conjuntos finitos, demostrados en § 4.2.

†**Teorema 87.** *Si* $\mathfrak{m}$ *es un cardinal finito, entonces* $\mathfrak{m} < \mathfrak{m} + 1$.

†**Teorema 88.** *Si* $\mathfrak{m}$ *es un cardinal finito y* $\mathfrak{n}$ *no lo es, entonces* $\mathfrak{m} < \mathfrak{n}$.

†**Teorema 89.** *Si* $\mathfrak{m}$ *es un cardinal finito y* $\mathfrak{n} < \mathfrak{m}$, *entonces* $\mathfrak{n}$ *es un cardinal finito.*

†**Teorema 90.** *Si* $\mathfrak{m}$ *es un cardinal finito, entonces* $\mathfrak{n} < \mathfrak{m}$, $\mathfrak{n} = \mathfrak{m}$, *o* $\mathfrak{m} < \mathfrak{n}$.

Concluimos esta sección con una sucesión de teoremas que conducen al resultado de que $<$ bien-ordena cualquier conjunto de cardinales finitos. Primero demostramos, por inducción, que el conjunto $\mathcal{Q}(\mathfrak{m})$ de los precedentes de un cardinal finito $\mathfrak{m}$ no es vacío si $\mathfrak{m}$ es mayor que $\mathbf{0}$.

†**Teorema 91.** *Si* $\mathfrak{m}$ *es un cardinal finito, entonces* $\mathfrak{n} \in \mathcal{Q}(\mathfrak{m})$ *si y solamente si* $\mathfrak{n} < \mathfrak{m}$.

Demostración. Teniendo en cuenta el carácter de la definición por abstracción, usada para definir $\mathcal{Q}(\mathfrak{m})$, es claro que para establecer el teorema necesitamos demostrar que, para todo $\mathfrak{m}$, existe un conjunto A tal que, para todo $\mathfrak{n}$, $\mathfrak{n} \in A$ si y solamente si $\mathfrak{n} < \mathfrak{m}$. Para $\mathfrak{m} = 0$, podemos tomar $A = 0$. Para la segunda parte de la inducción, suponemos que existe tal conjunto A para $\mathfrak{m}$. Pero es fácil ver que

$$B = A \cup \{\mathfrak{m}\}$$

es el conjunto apropiado para $\mathfrak{m} + 1$, esto es, bajo la hipótesis inductiva para A, $\mathfrak{n} \in B$ si y solamente si $\mathfrak{n} < \mathfrak{m} + 1$. Q.E.D.

Tampoco es difícil demostrar que si $\mathfrak{m}$ es un cardinal finito, entonces $\mathcal{Q}(\mathfrak{m})$ tiene $\mathfrak{m}$ elementos.

†**Teorema 92.** *Si* $\mathfrak{m}$ *es un cardinal finito entonces* $\mathcal{K}(\mathcal{Q}(\mathfrak{m})) = \mathfrak{m}$.

A continuación queremos demostrar que $<$ bien-ordena $\mathcal{Q}(\mathfrak{m})$, cuando $\mathfrak{m}$ es un cardinal finito. Tal como se presentan las cosas, el símbolo '$<$' no designa un conjunto, como no lo designan '$=$' y '$\subseteq$', pero, con una restricción apropiada, siguiendo los lineamientos usados para la identidad en el capítulo 2, se puede obtener la entidad teórica conjuntista requerida.

†**Definición 17.** $<|A = \{\langle \mathfrak{n}, \mathfrak{m}\rangle : \mathfrak{n} \in A \ \& \ \mathfrak{m} \in A \ \& \ \mathfrak{n} < \mathfrak{m}\}$.

(Nótese que hemos usado la barra vertical de restricción definida en el capítulo 3 debido a su sugestividad, aun cuando realmente aquí el símbolo completo '$<|$' es un símbolo de operación unaria.) Es muy simple aplicar el esquema axiomático de separación para obtener:

†**Teorema 93.** $\mathfrak{n} <|A\ \mathfrak{m}$ *si y sólo si* $\mathfrak{n} \in A$ & $\mathfrak{m} \in A$ & $\mathfrak{n} < \mathfrak{m}$.

Para evitar la notación engorrosa, es conveniente definir:

†**Definición 18.** $<_{\mathfrak{m}} = <|\mathfrak{Q}(\mathfrak{m})$.

Podemos entonces demostrar por inducción (usando el teorema 86) que

†**Teorema 94.** *Si* $\mathfrak{m}$ *es un cardinal finito, entonces* $<_{\mathfrak{m}}$ *bien-ordena* $\mathfrak{Q}(\mathfrak{m})$.

Demostración. Obviamente $<_0$ bien-ordena $\mathfrak{Q}(0)$, ya que $\mathfrak{Q}(0)$ es vacío.
Para la segunda parte de la inducción, suponemos que

(1) $<_{\mathfrak{m}}$ bien-ordena $\mathfrak{Q}(\mathfrak{m})$.

Ahora es obvio, a partir de las definiciones pertinentes, que

$$\mathfrak{Q}(\mathfrak{m}') = \mathfrak{Q}(\mathfrak{m}) \cup \{\mathfrak{m}\}.$$

Necesitamos demostrar que cualquier subconjunto no vacío A de $\mathfrak{Q}(\mathfrak{m}')$ tiene un $<_{\mathfrak{m}'}$-primer elemento, pues la conectividad de $\mathfrak{Q}(\mathfrak{m}')$ bajo la relación dada se sigue del teorema 90. (Estas son las dos condiciones requeridas para que $<_{\mathfrak{m}'}$ bien-ordene $\mathfrak{Q}(\mathfrak{m}')$; confróntese la definición 27 del capítulo 3.) Si $A \subseteq \mathfrak{Q}(\mathfrak{m})$, entonces que A tiene un $<_{\mathfrak{m}'}$-primer elemento se sigue de la hipótesis inductiva (1). Al otro extremo, si $A = \{\mathfrak{m}\}$, se sigue de una vez la conclusión pedida. La tercera posibilidad, a saber, que no $A \subseteq \mathfrak{Q}(\mathfrak{m})$ y $A \cap \mathfrak{Q}(\mathfrak{m}) \neq 0$, es igualmente simple. $A \sim \{\mathfrak{m}\} \subseteq \mathfrak{Q}(\mathfrak{m})$, así que $A \sim \{\mathfrak{m}\}$ tiene un $\mathfrak{m}'$ primer elemento, digamos $\mathfrak{n}$, y claramente $\mathfrak{n} < \mathfrak{m}$, por consiguiente, $\mathfrak{n}$ es también el $<_{\mathfrak{m}'}$-primer elemento de A, lo que completa nuestra demostración inductiva. Q.E.D.

Finalmente, demostramos:

†**Teorema 95.** *Cualquier conjunto A de cardinales finitos es bien ordenado por* $<|A$.

Demostración. Si A es vacío no hay nada que demostrar, así que podemos suponer que $A \neq 0$. La conectividad de $<|A$ se sigue del teorema 90. Sea B un subconjunto no vacío de A. Para completar la demostración necesitamos demostrar que B tiene un $<|A$-primer elemento. Escojamos un elemento $\mathfrak{m}$ de B. Si $B \cap \mathfrak{Q}(\mathfrak{m}) = 0$ entonces, claramente, $\mathfrak{m}$ es el $<|A$-primer elemento de B.

Si $B \cap \mathfrak{Q}(\mathfrak{m}) \neq 0$, sea

$$C = B \cap \mathfrak{Q}(\mathfrak{m}).$$

Obviamente, si $\mathfrak{n} \in C$ y $\mathfrak{p} \in B \sim C$,

(1) $\mathfrak{n} < \mathfrak{p}$,

pero, ya que C es un subconjunto no vacío de $\mathfrak{Q}(\mathfrak{m})$, en virtud del teorema precedente, C tiene un $<_{\mathfrak{m}}$-primer elemento, digamos $\mathfrak{n}^*$, y en vista de (1) no hay dificultad en demostrar que $\mathfrak{n}^*$ es el $<|A$-primer elemento de B. Q.E.D.

Debe notarse que no hay esperanza de demostrar, sin el axioma de escogencia, el análogo del teorema 95 para un conjunto de cardinales arbitrarios, pues la conectividad del conjunto es simplemente la ley de tricotomía.

EJERCICIOS

1. Demostrar los teoremas 87 y 88.
2. Demostrar los teoremas 89 y 90.
3. Demostrar los teoremas 92 y 93.

En los siguientes ocho ejercicios, supóngase que $\mathfrak{m}$, $\mathfrak{n}$, $\mathfrak{p}$ *y* $\mathfrak{q}$ *son cardinales finitos.*

4. Demostrar que, si $\mathfrak{m}+\mathfrak{n}=\mathfrak{p}$, entonces $\mathfrak{m} \leq \mathfrak{p}$.
5. Demostrar que $\mathfrak{n} \leq \mathfrak{m}+\mathfrak{n}$.
6. Demostrar que, si $\mathfrak{m} < \mathfrak{n}$, entonces $\mathfrak{m}+\mathfrak{p} < \mathfrak{n}+\mathfrak{p}$.
7. Demostrar que, si $\mathfrak{m}+\mathfrak{p} < \mathfrak{n}+\mathfrak{p}$, entonces $\mathfrak{m} < \mathfrak{n}$.
8. Demostrar que, si $\mathfrak{m} < \mathfrak{n}$ & $\mathfrak{p} < \mathfrak{q}$, entonces $\mathfrak{m}+\mathfrak{p} < \mathfrak{n}+\mathfrak{q}$.
9. Demostrar que, si $\mathfrak{m} < \mathfrak{n}$ & $\mathfrak{p} \neq 0$, entonces $\mathfrak{m}\mathfrak{p} < \mathfrak{n}\mathfrak{p}$.
10. Demostrar que, si $\mathfrak{m}\mathfrak{p} < \mathfrak{n}\mathfrak{p}$, entonces $< \mathfrak{n}$.
11. Demostrar que, si $\mathfrak{m} < \mathfrak{n}$ & $\mathfrak{p} < \mathfrak{q}$, entonces $\mathfrak{m}\mathfrak{p} \vee \mathfrak{n}\mathfrak{q}$.
12. Sea R la relación cuyo campo es el conjunto de los cardinales finitos. Demostrar que existe una función f con $\mathfrak{D}R = \mathfrak{D}f$ y $f \subseteq R$. (Esta aserción, quitada la restricción a cardinales finitos, es una forma del axioma de escogencia.)

Capítulo 5

Ordinales finitos y conjuntos enumerables

§ 5.1 **Definición y propiedades generales de los ordinales.** En este capítulo desarrollaremos primero, con alguna extensión, la teoría general de los números ordinales, siguiendo las ideas de von Neumann [1923]. Luego dirigimos nuestra atención hacia los ordinales finitos cuya teoría desarrollamos independientemente de la de los cardinales finitos de la sección final del capítulo anterior e independientemente del axioma especial para números cardinales. La teoría de los números ordinales no depende de este axioma en ninguna parte de éste o de los capítulos subsiguientes. En la última sección de este capítulo consideramos la teoría de los conjuntos enumerables y retornamos brevemente a la teoría de los números cardinales.

La teoría de ordinales finitos dada en este capítulo es ciertamente más complicada que la de los cardinales finitos del capítulo 4, pero tiene la gran virtud de no depender de axioma especial alguno. Cuando la teoría de números cardinales se hace independientemente de este axioma especial y del axioma de escogencia por el uso de la noción de rango de un conjunto (véase Scott [1955]), es, en sus fases iniciales, más complicada que la teoría de los ordinales. Este enfoque, vía el concepto de rango, no se seguirá aquí.

Comenzamos con alguna descripción de la teoría clásica de Cantor para números ordinales. Esta teoría depende de definir primero la noción de *tipo de orden* y luego de designar los números ordinales como ciertos tipos de orden especiales, a saber, los tipos de orden de los conjuntos bien ordenados. Informalmente hablando, un tipo de orden es el conjunto de todos los conjuntos simplemente ordenados que se pueden poner en correspondencia 1-1 con un conjunto dado, simplemente ordenado, de modo que se "preserva" el orden. Para precisar más, es deseable, para efectos de claridad, tratar con parejas ordenadas: $\mathfrak{A} = \langle A, R\rangle$ es una *estructura de orden simple,* si y solamente si R es una ordenación estricta simple de A. Clásicamente, se suprime la referencia a la ordenación R y se usa una sola barra sobre A para indicar el tipo de orden. Seremos más explícitos. Primero definimos la noción de dos estructuras de orden simple que son *semejantes*, para captar la noción de un orden que preserva la correspondencia 1-1. La definición no necesita la suposición de que las parejas son estructuras de orden simple; se sigue un formato común en álgebra abstracta, lo que explica el uso de las letras alemanas '$\mathfrak{A}$' y '$\mathfrak{B}$'. (Esta definición es un caso especial de la definición general de isomorfismo de sistemas algebraicos.)

Definición 1.

(i) $\mathfrak{A} = \langle A, R\rangle$ *es semejante, bajo* f, *a* $\mathfrak{B} = \langle B, S\rangle$ *si y solamente si*

(a) f *es una función 1-1,*

(b) $\mathfrak{D}f = A$ *y* $\mathfrak{R}f = B$,

(c) *para todo* $x, y \in A$ xRy *si y solamente si* $f(x)Sf(y)$.

(ii) $\mathfrak{A} = \langle A, R\rangle$ *es semejante a* $\mathfrak{B} = \langle B, S\rangle$ *si y solamente si existe una* f *tal que* $\mathfrak{A}$ *es semejante, bajo* f, *a* $\mathfrak{B}$.

Obviamente la notación $\mathfrak{A} = \langle A, R\rangle$ en el definiendum no satisface nuestras reglas formales de definición. Deberíamos tener:

> $\mathfrak{A}$ *es semejante, bajo f, a* $\mathfrak{B}$ *si y solamente si existen conjuntos A, B, R y S tales que* $\mathfrak{A} = \langle A, R\rangle$, $\mathfrak{B} = \langle B, S\rangle$ y . . .

Pero el uso que hemos seguido está más difundido y es intuitivamente más claro. Si, por ejemplo,

$$A = \{1, 2, 3\}$$
$$B = \{3, 5, 7\}$$
R = menos que restringido a A
S = más que restringido a B,

entonces $\langle A, R\rangle$ es semejante a $\langle B, S\rangle$, pues podemos tomar como función apropiada:

$$f = \{\langle 1, 7\rangle, \langle 2, 5\rangle, \langle 3, 3\rangle\}.$$

En teoría de conjuntos intuitiva definiríamos, si no fuera por las paradojas: *si* $\mathfrak{A}$ *es una estructura de orden simple, entonces*

(1) $\quad \overline{\overline{\mathfrak{A}}} = \{\mathfrak{B}\colon \mathfrak{B}$ *es semejante a* $\mathfrak{A}\}$.

La dificultad con (1) es exactamente la dificultad encontrada con la definición correspondiente de números cardinales: no podemos demostrar que la clase de equivalencia $\overline{\overline{\mathfrak{A}}}$, que es el tipo de orden de $\mathfrak{A}$, no es vacía. El desarrollo fácil y natural de la teoría del tipo de orden requeriría la introducción de un nuevo axioma como el axioma para cardinales.*

Debe mencionarse que los tipos de orden se pueden definir simplemente en términos de relaciones; si R es una ordenación simple, entonces

$$\overline{\overline{R}} = \{S\colon \langle \mathfrak{F}S, S\rangle \text{ es semejante a } \langle \mathfrak{F}R, R\rangle\}$$

pero ninguna de las dificultades de (1) se evitan con este enfoque.

En vista de las dificultades para la definición por abstracción de los números cardinales o de los tipos de orden, es en realidad una suerte que, para el caso especial de los números ordinales, los cuales son clásicamente tipos de orden de conjuntos bien ordenados, se pueda adoptar un recurso que no requiere axiomas especiales para respaldarlo. La idea consiste en escoger precisamente un representante de cada tipo de orden que sea un ordinal y llamar a este representante *el* ordinal. O sea que, en el caso de las buenas ordenaciones, estamos de hecho capacitados para construir un ejemplo definido de cada buena ordenación posible, lo que no podemos hacer en el caso de ordenaciones arbitrarias. Los representantes definidos que escogemos se construyen a partir del conjunto vacío:

$$1 = \{0\}$$
$$2 = \{0, \{0\}\} = \{0, 1\}$$
$$3 = \{0, \{0\}, \{0, \{0\}\}\} = \{0, 1, 2\}$$
$$\cdots\cdots\cdots\cdots$$

Cada ordinal tiene como elementos a todos los ordinales más pequeños y la relación de pertenencia proporciona la buena ordenación adecuada. Esta construcción se debe a von Neumann [1923]. Su adecuación intuitiva para proporcionar un representante de cada tipo de buena ordenación se puede explicar por medio del siguiente argumento informal, por el cual estoy reconocido a Dana Scott.

Sea R una buena ordenación de A. Queremos dar un método de asociar una nueva buena ordenación con R, que no dependa de la naturaleza particular de los elementos de A. Dicho de otra manera, queremos definir una función, digamos f, sobre A que proporcionará un representante apropiado definido correspondiente a la ordenación debida a R. La definición es como sigue: Sea a_0 el R-primer elemento de A. Hacemos

$$f(a_0) = 0.$$

* Podemos mencionar los cuatro tipos de orden más importantes y sus nombres comúnmente aprobados. Así,
ω es el tipo de orden de $\langle N, <\rangle$, donde N es el conjunto de los números naturales;
ω^* es el tipo de orden de $\langle N, >\rangle$, o también el tipo de orden de los enteros negativos *menor que*;
η es el tipo de orden de $\langle$Rac, $<\rangle$, donde Rac es el conjunto de los números racionales;
λ es el tipo de orden de $\langle$Re, $<\rangle$, donde Re es el conjunto de los números reales. Cada uno de esos tipos de orden puede caracterizarse en forma abstracta (ver, por ejemplo, Sierpinski [1928]).

Sea a_1 el siguiente elemento de A bajo R. Hacemos

$$f(a_1) = \{f(a_0)\}$$
$$= \{0\}.$$

En forma similar, para a_2

$$f(a_2) = \{f(a_o), f(a_1)\}$$
$$= \{0, \{0\}\},$$

y para cualquier entero n

$$f(a_n) = \{f(a_o), f(a_1), \ldots, f(a_{n-1})\}.$$

Por otra parte, esta construcción se puede extender más allá de los enteros. En general, el valor de f para cada elemento a es simplemente el conjunto de los valores de la función, de los elementos que preceden a a en la ordenación R. Formalmente, para todo a en A,

$$f(a) = f``\breve{R}``\{a\}.$$

Además, no es difícil demostrar que para $a, b \in A$

aRb si y solamente si $f(a) \in f(b)$.

Por otra parte, si S bien-ordena B y $\langle A, R\rangle$ es semejante a $\langle B, S\rangle$ bajo la función g, digamos, entonces, para a en A,

$$f(a) = f'(g(a)),$$

donde f' se construye para $\langle B, S\rangle$ como se construyó f para $\langle A, R\rangle$. Las funciones f y f' han aplicado las dos buenas ordenaciones sobre un representante adecuado que sustituye las relaciones R y S por un fragmento de la relación de pertenencia. Así, en lugar de la definición por abstracción tenemos un procedimiento sencillo y natural para representar cualquier buena ordenación por medio de la relación de pertenencia. En el capítulo 7 (teorema 81) demostramos que esta representación es posible siempre.

Ahora procedemos a la construcción formal de los ordinales. Se necesitan algunas nociones preliminares. Comenzamos con la definición de "fragmentos" de la relación de pertenencia. Definimos una relación $\mathcal{E} A$ que corresponde a la pertenencia del mismo modo que $\mathcal{I} A$ corresponde a la identidad.

Definición 2. $\mathcal{E}A = \{\langle x, y\rangle : x \in A \;\&\; y \in A \;\&\; x \in y\}$.

Principalmente en virtud del esquema axiomático de separación, tenemos:

Teorema 1. $\langle x, y\rangle \in \mathcal{E}A$ *si y solamente si* $x \in A \;\&\; y \in A \;\&\; x \in y$.

Definición 3. *A es completo si y solamente si todo elemento de A es un subconjunto de A.*

Ilustraremos esta noción con algunos ejemplos. Sean

$$A_1 = \{\text{James Joyce}, \{0\}\}.$$
$$A_2 = \{0, \{0\}\}.$$

Entonces A_2 es completo pero A_1 no lo es. Nótese que no podríamos definir la completez por la condición:

(1) Para todo x, si $x \in A$, entonces $x \subseteq A$,

porque la definición de '$\subseteq$' era condicional y no puede hacerse decisión alguna respecto a la relación de inclusión para individuos. Por ejemplo, con (1) como definiens no estaríamos en posibilidad de decidir si {James Joyce} es completo. La formulación, en palabras, de la definición 3 implica que todo elemento de un conjunto completo es un conjunto.

Tenemos el resultado simple:

Teorema 2. *Si A y B son completos, entonces $A \cap B$ y $A \cup B$ son completos.*

Podemos ahora formular la definición de los ordinales, que se presenta en la forma sencilla debida a Robinson [1937].

Definición 4. *A es un ordinal si y solamente si A es completo y $\mathcal{E} A$ hace conexo a A.*

La adecuación de esta definición depende del axioma de regularidad. Sin la consideración de ese axioma necesitamos algo como lo siguiente: A es un ordinal, si y solamente si

(i) $\mathcal{E}A$ bien-ordena A,

(ii) A es completo.

La condición (i) prohibe una sucesión descendente infinita de elementos de A, lo cual se prohibe también en el axioma de regularidad. Sin este axioma tenemos,

$$0 \neq \{0\}, \{0\} \neq \{0, \{0\}\}, \text{ etc.}$$

En el resto de esta sección demostramos algunos teoremas generales acerca de los ordinales, la mayor parte de los cuales se necesitan para la construcción de los ordinales finitos en la sección siguiente. Comenzamos por demostrar que todo ordinal está bien ordenado por la relación de pertenencia. Como es de esperarse, por las anotaciones anteriores, la demostración depende del axioma de regularidad.

Teorema 3. *Si A es un ordinal, entonces εA bien-ordena A.*

Demostración. Ya que A es un ordinal, εA hace conexo a A; necesitamos demostrar solamente que todo subconjunto no vacío B de A tiene εA-primer elemento. Por el axioma de regularidad y el hecho que todo elemento de B es un conjunto, existe un conjunto C en B tal que

$$B \cap C = 0.$$

Por tanto, ningún elemento de B es también un elemento de C, así que C es un εA-primer elemento de B. Q.E.D.

La demostración del siguiente teorema usa hechos relativos a las εA-secciones establecidas en §3.2.

Teorema 4. *Si A es un ordinal, $B \subset A$ y B es completo, entonces $B \in A$.*

Demostración. En vista del teorema 3, sabemos que εA bien-ordena A. Además, puesto que B es completo, si $x \,\varepsilon A y$ y $y \in B$, entonces $x \in B$. Por tanto, B es una εA-sección de A, así que, en virtud del teorema 69 de § 3.2, existe un z en A tal que

(1) $\quad B = \{x\colon x \in A \;\&\; x \,\varepsilon A\, z\}.$

Pero ya que A es completo, todo elemento de z es un elemento de A y (1) se reduce simplemente a

$$B = \{x\colon x \in z\},$$

o sea,

$$B = z,$$

y z es un elemento de A. Q.E.D.

Teorema 5. *Si A y B son ordinales, entonces $A \subset B$ si y sólo si $A \in B$.*

Demostración. Si $A \subset B$, entonces, puesto que A es completo, por el teorema precedente, $A \in B$. Si $A \in B$, entonces, ya que B es completo, $A \subset B$. Q.E.D.

Teorema 6. *Todo elemento de un ordinal es un ordinal.*

Demostración. Sea A un ordinal y $B \in A$. Puesto que A es completo, $B \subseteq A$, así que εB, que es un subconjunto de εA, hace conexo a B. Además, puesto que εA bien-ordena A, bien-ordena B, de modo que es transitivo sobre B. Así, si tenemos

$$x \,\varepsilon A\, y \;\&\; y \,\varepsilon A\, B,$$

inferimos $x \,\varepsilon A\, B$, esto es, $x \in B$, de donde, $y \subseteq B$ y B es completo.
Entonces B es un ordinal. Q.E.D.

Las demostraciones de los dos teoremas siguientes se dejan como ejercicios. La primera es ligeramente difícil.

Teorema 7. *Si A y B son ordinales, entonces $A \subseteq B$ o $B \subseteq A$.*

Teorema 8. *Si A y B son ordinales, entonces subsiste exactamente una de las situaciones siguientes:*

$$A \in B, B \in A, A = B.$$

Teorema 9. *Si B es un conjunto de ordinales, entonces $\bigcup B$ es un ordinal.*

Demostración. Puesto que B es un conjunto de ordinales y los elementos de los ordinales son ordinales (teorema anterior), en vista del teorema 8, $\varepsilon \bigcup B$ hace conexo a $\bigcup B$. Para mostrar que $\bigcup B$ es completo, sea $C \in \bigcup B$. Entonces existe un ordinal D tal que $C \in D$ y $D \in B$. Ya que D es completo, $C \subseteq$

D y en virtud del teorema 62 de §2.6, a partir de $D \in B$ inferimos $D \subseteq \bigcup B$, así que por transitividad de la inclusión, concluimos: $C \subseteq \bigcup B$. Q.E.D.

Esta demostración ilustra la técnica típica directa para demostrar que un conjunto es un ordinal: demostrar que el conjunto es conexo por la relación de pertenencia y que es completo.

Definimos *menor que* estricto y débil para conjuntos, en términos de pertenencia y también *mayor que* estricto y débil.

Definición 5.
(i) $A < B$ *si y solamente si* $A \in B$.
(ii) $A \leq B$ *si y solamente si* $A < B$ *o* $A = B$,
(iii) $A > B$ *si y solamente si* $B < A$,
(iv) $A \geq B$ *si y solamente si* $B \leq A$.

Nos restringimos a un teorema acerca del menor que estricto, pero las propiedades elementales de orden de las otras tres relaciones se demuestran fácilmente y así las suponemos en lo que sigue.

Teorema 10. *Si* A, B, C *son ordinales, entonces*
(i) *no* $A < A$,
(ii) *si* $A < B$, *entonces no* $B < A$,
(iii) *si* $A < B$ *y* $B < C$, *entonces* $A < C$,
(iv) *se cumple sólo una de las siguientes situaciones:*

$$A < B, A = B, B < A.$$

El teorema siguiente muestra que cada ordinal es precisamente el conjunto de ordinales más pequeños. Omitimos la demostración.

Teorema 11. *Si* A *es un ordinal, entonces* $A = \{B\colon B$ *es un ordinal &* $B < A\}$.

Ahora demostramos que el conjunto de todos los ordinales no existe.

Teorema 12. *No existe el conjunto* A *tal que para todo* x, $x \in A$ *si y solamente si* x *es un ordinal.*

Demostración. La demostración consiste en mostrar que si existiera tal conjunto, digamos A, entonces sería un ordinal y por consiguiente, un elemento de sí mismo, en contra del hecho que ε_A bien-ordena A. O sea que es absurdo tener $A \in A$.

Supongamos que A es el conjunto de todos los ordinales. En virtud del teorema 8, ε_A hace conexo a A. Sea B un elemento arbitrario de A. En vista del teorema 6, todo elemento de B es un ordinal, por tanto un elemento de A, así que $B \subseteq A$, lo que establece la completez de A. A es entonces un ordinal, pero esto significa que $A \in A$.
Q.E.D.

Este teorema muestra que en la teoría de conjuntos de Zermelo, la paradoja del mayor ordinal, de Burali-Forti (véase la discusión en §1.4) está bloqueada por el hecho de que el conjunto de todos los ordinales no existe. Debe enfatizarse que la demostración de este teorema no depende realmente del axioma de regularidad, pues si no se supone este axioma, entonces, como ya se indicó, es parte de la definición de los ordinales el requerir que si A es un ordinal, ε_A bien-ordena A, lo que implica $A \notin A$.*

Concluimos esta sección introduciendo la noción de *sucesor* para los ordinales. La idea intuitiva es la misma que para cardinales y las definiciones están íntimamente relacionadas. Ninguna confusión resulta del uso del mismo símbolo acostumbrado para las dos funciones sucesor, pues en el contexto en donde aparezcan será claro si se trata de cardinales (construidos por medio del axioma especial para cardinales) o de ordinales.

Definición 6. $A' = A \cup \{A\}$.

Por ejemplo,

$$\mathbf{0}' = \mathbf{0} \cup \{\mathbf{0}\} = \{\mathbf{0}\} = \mathbf{1}$$

$$\mathbf{1}' = \{\mathbf{0}\}' = \{\mathbf{0}\} \cup \{\{\mathbf{0}\}\} = \{\mathbf{0}, \{\mathbf{0}\}\} = \mathbf{2}.$$

Formulamos, sin demostración, algunos teoremas muy parecidos a los que ya han sido formulados para cardinales.

* En la teoría de conjuntos de von Neumann existe la clase de todos los ordinales, pero es una clase propia, así que no puede ser elemento de sí misma ni de cualquier otra clase.

Teorema 13. *Si* $A' = B'$, *entonces* $A = B$.

Teorema 14. *Si* A *es un ordinal, entonces* $\bigcup A' = A$.

Teorema 15. *Si A es un ordinal, entonces no existe ningún ordinal B tal que*

$$A < B < A'.$$

Teorema 16. A' *es un ordinal si y solamente si* A *es un ordinal.*

EJERCICIOS

1. Demostrar que la definición 4 de ordinales es equivalente a la otra definición dada inmediatamente después de ella en el texto.
2. Dar una demostración detallada del teorema 1.
3. Demostrar el teorema 2.
4. Demostrar que un conjunto A cuyos elementos son únicamente conjuntos es completo si y solamente si $\bigcup A \subseteq A$.
5. Demostrar los teoremas 7 y 8. (Sugerencia: supóngase $A \cap B \subset A \mathbin{\&} A \cap B \subset B$ y luego dedúzcase un absurdo.)
6. Demostrar el teorema 10.
7. Demostrar el teorema 11.
8. Demostrar los teoremas 13 y 14.
9. Demostrar los teoremas 15 y 16.
10. Demostrar que, si A y B son ordinales y $A \in B$, entonces $B \notin A'$.
11. Sea B un conjunto de ordinales. Demostrar
    (a) Si $C \in B$, entonces $C \leq \bigcup B$,
    (b) Si D es un ordinal y, para todo C en B, $C \leq D$, entonces $\bigcup B \leq D$.
12. Dar un contra-ejemplo para mostrar que (b), ejercicio 11, es falso si se omite el requerimiento de que D sea un ordinal.
13. Demostrar que, si B es un conjunto no vacío de ordinales, entonces $\bigcap B$ es el $\mathcal{E}B$-primer elemento de B.

§ 5.2 Ordinales finitos y definiciones recurrentes. Los ordinales finitos son simplemente ordinales que están bien ordenados por la conversa de la relación de pertenencia. Para facilidad intuitiva de referencia, al construir los números reales en el capítulo siguiente, llamaremos *números naturales* a los ordinales finitos.

Definición 7. *A es un número natural si y sólo si A es un ordinal y* $\breve{\mathcal{E}}A$ *bien-ordena A.*

Esta definición podría reemplazarse por la siguiente: A es un número natural si y solamente si A es un ordinal y A es un conjunto finito en el sentido de Tarski. En realidad, para indicar cuán rápida y directamente se pueden desarrollar tanto la teoría de los números naturales como la de los ordinales finitos a partir de los axiomas de la teoría de conjuntos de Zermelo, hemos hecho la mayor parte de esta sección independientemente de la teoría de conjuntos finitos dada en §4.2.

Para los números naturales usaremos las letras minúsculas en bastardilla, '*m*', '*n*', '*p*', '*q*', '*r*', '*s*', y '*t*' con o sin sub-índices.

Nuestra primera tarea es demostrar los cinco axiomas de Peano (véase §4.4).

La demostración del siguiente teorema es obvia.

Teorema 17. 0 *es un número natural.*

Teorema 18. *Si n es un número natural, entonces* n' *es un número natural.*

Demostración. Ya que n es un número natural, n es un ordinal, así que, por último teorema de la sección precedente, n' es un ordinal. Por tanto sabemos que $\mathcal{E}n'$ y entonces $\breve{\mathcal{E}}n'$ hacen conexo a n'. Para demostrar que n' es bien-ordenado por $\breve{\mathcal{E}}n'$ y es, por consiguiente, un número natural, necesitamos demostrar solamente que todo subconjunto no vacío de n' tiene un $\breve{\mathcal{E}}n'$-primer elemento. Si un subconjunto no vacío de n' tiene a n como un elemento, n es su $\breve{\mathcal{E}}n'$-primer elemento; si no lo es, es un subconjunto de n y por la hipótesis del teorema tiene un $\breve{\mathcal{E}}n$-primer elemento y entonces un $\breve{\mathcal{E}}n'$-primer elemento. Q.E.D.

Teorema 19. *No hay ningún número natural n tal que* $n' = 0$.

Demostración. Supongamos que hubiera un tal número n. Entonces $n \in n'$, de donde $n \in 0$, lo que es absurdo. Q.E.D.

Teorema 20. *Si n, m son números naturales y* $n' = m$, *entonces* $n = m$.

Demostración. Es consecuencia inmediata del teorema 13. Q.E.D.

La demostración del esquema de inducción se facilita con el siguiente teorema, cuya demostración se deja como ejercicio.

Teorema 21. *Si $A \leq n$, entonces A es un número natural.*

Ahora demostramos:

Esquema teoremático 22. *Si*

(i) $\varphi(0)$,

(ii) *para todo n, si $\varphi(n)$, entonces $\varphi(n')$,* *entonces, para todo n, $\varphi(n)$.*

Demostración. Consideremos la hipótesis del teorema y supongamos que existe un n tal que no es el caso de que $\varphi(n)$. Sea

$$L(n) = \{B: B \leq n \;\&\; \varphi(B) \text{ es falso}\}.$$

Entonces $\mathcal{E}n'$ bien-ordena $L(n)$. Sea B^* el primer elemento de $L(n)$. Ya que B^* no es cero, $\mathcal{E}B^*$ bien-ordena B^* y existe un $\mathcal{E}B^*$-primer elemento de B^*, digamos D. O sea, D es el $\mathcal{E}B^*$-último elemento de B^*.

Además, puesto que $D < B^*$,

(1) $\qquad \varphi(D).$

Pero

(2) $\qquad D' = B^*,$

ya que, si $D' \neq B^*$, entonces

$$D' \in B^* \qquad \text{(¿Por qué?)}$$

y D no sería $\mathcal{E}B^*$-último elemento de B^*. Por tanto, a partir de (1), (2) y la hipótesis del teorema inferimos que

$$\varphi(B^*),$$

lo que es absurdo. Q.E.D.

Los teoremas 17 a 20 y el teorema 22 corresponden a los cinco axiomas de Peano.

El desarrollo ulterior de la aritmética de los números naturales no puede seguir los lineamientos que se siguieron para la aritmética de los cardinales finitos. El axioma para cardinales justificó directamente las definiciones explícitas de adición, multiplicación y exponenciación entre cardinales, de manera sencilla y natural.

Para ilustrar los problemas que nos ocupan podemos referirnos por el momento a la definición de adición. Dados simplemente los axiomas de Peano, P1 a P5, formulados en lógica de predicado con identidad y sin teoría de conjuntos, se puede demostrar (J. Robinson [1949]) que una definición propia, explícita de adición, no puede formularse dentro de este enfoque. El procedimiento acostumbrado es adoptar dos nuevos axiomas:

P6. *Si x es un número natural, entonces* $x + 0 = x$.

P7. *Si x y y son números naturales, entonces*

$$x + y' = (x + y)'.$$

Para ilustrar el uso de estos axiomas podemos demostrar que $1 + 3 = 4$, donde, como era de esperarse,

(1) $\qquad 1 = 0'$

(2) $\qquad 2 = 1'$

(3) $\qquad 3 = 2'$

(4) $\qquad 4 = 3'$

Tenemos entonces:

$$\begin{aligned}
1 + 3 &= 1 + 2' && \text{por (3)}\\
&= (1 + 2)' && \text{por P7}\\
&= (1 + 1')' && \text{por (2)}\\
&= (1 + 1)'' && \text{por P7}\\
&= (1 + 0')'' && \text{por (1)}\\
&= (1 + 0)''' && \text{por P7}\\
&= 1''' && \text{por P6}\\
&= 2'' && \text{por (2)}\\
&= 3' && \text{por (3)}\\
&= 4 && \text{por (4)}
\end{aligned}$$

Una pareja de postulados como P6 y P7 se dice que proporciona una "definición" *inductiva* o *recurrente* de adición. Desde el punto de vista de la teoría de la definición como se formuló en § 2.1, tales "definiciones" no son propias. En particular violan el criterio de eliminabilidad de una manera mucho más profunda que las definiciones condicionales. Por ejemplo, dados P1 a P7, no podemos eliminar el símbolo de adición del teorema aritmético:

$$x + y = y + x.$$

Las definiciones recurrentes, sin embargo, están cerca de ser propias; lo que queremos demostrar es que, dado el aparato adicional de la teoría de conjuntos, podemos sustituir una definición recurrente por una definición propia explícita. Naturalmente, si estuviéramos interesados en considerar sólo la adición y quizás la multiplicación y la exponenciación, sería posible obviar la teoría general de definiciones recurrentes y justificar cada una por un argumento especial.* La ventaja de la teoría general es la de que proporciona una imagen clara de los recursos ulteriores de definición que se agregan a la teoría elemental de números por el uso de la teoría general de conjuntos.

Sobre la base de los axiomas introducidos atrás, podemos presentar la teoría de las definiciones recurrentes por medio de un esquema teoremático. Puesto que no podemos demostrar la existencia del conjunto de los números naturales o de cualquier otro conjunto infinito, no podemos definir las operaciones binarias usuales de la aritmética como funciones propias de la teoría de conjuntos. Para el desarrollo de la teoría elemental de números no es ésta una cuestión que concierna mucho, pero tanto para la teoría de conjuntos enumerables como para la teoría de números reales en el capítulo siguiente, es esencial la existencia del conjunto de los números naturales. Asegurada la existencia de este conjunto, queda fácilmente establecida la existencia de las operaciones binarias sobre los números naturales, como funciones.

Así que, para poder disponer desde el principio de la construcción de las operaciones aritméticas como ciertos conjuntos, introducimos en este punto el *axioma de infinitud.*

$$(\exists A)[0 \in A \ \& \ (\forall B)(B \in A \rightarrow B \cup \{B\} \in A)].$$

El tratar de demostrar la existencia de un conjunto infinito de objetos tiene una historia más bien rara y a veces tergiversada. La proposición No. 66 del famoso *¿Was sind und was sollen die Zahlen?* de Dedekind, publicada por primera vez en 1888, afirma que existe un sistema infinito. (Los sistemas de Dedekind corresponden a nuestros conjuntos.) Su demostración es una combinación tan bella de razonamiento matemático y de epistemología incierta, que daré una libre traducción de ella aquí.

> **Demostración.** *Mi mundo de ideas, esto es, la totalidad S de todas las cosas que pueden ser objeto de mi pensamiento es infinito. Porque, si s es un elemento de S, entonces la idea s′, de que s puede ser un objeto de mi pensamiento, es ella misma un elemento de S. Si se considera como última la imagen* $\varphi(s)$ del elemento *s, entonces la aplicación* φ *de S, definida por este medio, tiene la propiedad de que la imagen S′ es una parte de S y desde luego S′ es una parte propia de S, porque existen en S elementos (por ejemplo mi ego individual) que son diferentes de cualquier idea tal como s′ y por consiguiente no están contenidos en S′. Finalmente, es evidente que si a y b son elementos diferentes de S, entonces sus imágenes a′ y b′ son también diferentes; en consecuencia, la aplicación* φ *es 1-1. Por consiguiente, S es infinito.**

La demostración de Dedekind depende, desde luego, de usar su definición de sistemas (o conjuntos) infinitos, pero lo que interesa es su excursión en la epistemología de las ideas.† En ningún sentido esta demostración satisface a los cánones modernos. En Russell, [1903, §339], se encuentran argumentos más sutiles, pero Russell reconoció más tarde que sus argumentos eran también falaces.††

*** Esto se hace, por ejemplo, en el pequeño trabajo clásico de Landau [1930].**

* Un argumento similar se encuentra en Bolzano [1851, § 13].

† Las críticas epistemológicas a la visión de Dedekind se encuentran en Russell [1920, pp. 139-140].

†† Russell empieza valientemente § 339: "Que hay clases infinitas es tan evidente que escasamente puede ser negado. Puesto que, sin embargo, ello es susceptible de demostración formal, puede ser también demostrado.

Hasta donde yo sé, el primer reconocimiento, inequívocamente claro, de que tal axioma se necesita, se encuentra en el importante documento de Zermelo, de 1908.* La formulación de Zermelo es esencialmente la siguiente:

$$(\exists A)\{0 \in A \ \&\ (\forall B)(B \in A \rightarrow \{B\} \in A)\}.$$

El construyó los números naturales como $0, \{0\}, \{\{0\}\}, \{\{\{0\}\}\}, \ldots$, cuyo enfoque no se generaliza tan fácilmente a la construcción de los ordinales infinitos como lo hace el que se ha adoptado en este libro. Unos pocos años después de Zermelo, Whitehead y Russell postularon un axioma de infinitud en *Principia Mathematica*, y existe una discusión interesante en Ramsey [1926] acerca de si su axioma de infinitud puede o no considerarse como una verdad lógica.

Volviendo a las consideraciones sistemáticas, definimos primero el conjunto ω de todos los números naturales y luego dejamos como ejercicio la demostración de que ω no es vacío. El axioma de infinitud es esencial para la demostración.

Definición 8. $\omega = \{A\colon A$ *es un número natural*$\}$.

Tenemos entonces:

Teorema 23. $A \in \omega$ *si y solamente si* A *es un número natural.*

Será conveniente, para lo que sigue, usar ω para dar una formulación "conjuntista" del principio de inducción.

Teorema 24. *Si*

(i) $0 \in A$,

(ii) *para todo* n, *si* $n \in A$, *entonces*, $n' \in A$, *entonces* $\omega \subseteq A$.

entonces $\omega \subseteq A$.

Volvemos ahora a nuestra tarea principal de la definición justificante, por recurrencia. Para las funciones de un argumento queremos un teorema como:

Para todo objeto x *y todo conjunto* G, *existe una única* F *tal que*

(i) F *es una función sobre* ω,

(ii) $F(0) = x$,

(iii) *para todo* n, $F(n') = G(F(n))$.

Es importante notar que x no necesita ser un número natural; puede ser cualquier individuo o conjunto (usamos "objeto" como término neutro) y G no necesita ser una función; si no es una función, tampoco necesita incluir $F(n)$ en su dominio. Desde luego, cuando G es defectuosa en uno de estos respectos, entonces

$$G(F(n)) = 0,$$

en virtud de la definición 39 de § 3.4.

Para funciones F de dos argumentos requerimos:

Para conjuntos cualesquiera G *y* H, *existe una única* F *tal que para cualesquiera* m, n,

(i) F es una función sobre $\omega \times \omega$

(ii) $F(\langle m, 0\rangle) = H(m)$,

(iii) $F(\langle m, n'\rangle) = G(\langle m, F(\langle m, n\rangle)\rangle)$.

Nótese de nuevo que G y H no necesitan ser funciones, aunque es natural, al definir las operaciones usuales por recurrencia, tener a G y a H como funciones simples que apliquen los números naturales o, parejas de números naturales en los números naturales. Por ejemplo, si con F se quiere significar la operación adición, hacemos

$$H(m) = m,$$

ya que

$$m + 0 = m,$$

y

$$(1) \quad G(\langle m, F(\langle m, n\rangle)\rangle) = F(\langle m, n\rangle)'.$$

Sin embargo, (1) no es completamente correcto; puesto que el símbolo de sucesor no designa una función en nuestro universo teórico conjuntista, no sabemos directamente que G es una función propia de la teoría de conjuntos. Pero esta dificultad se remedia fácilmente por la técnica de definir un fragmento de la función sucesor intuitiva, corres-

* Por otra parte, Zermelo [1909] fue el primero en reconocer que la teoría elemental de números podría desarrollarse sin el axioma de infinitud.

pondiente a lo que hicimos antes en el caso de la identidad y la pertenencia.

Definición 9. $\mathfrak{S}_A = \{\langle B, B'\rangle : B \in A\}$.

Es válido el teorema esperado:

Teorema 25. $\langle B, B'\rangle \in \mathfrak{S}_A \leftrightarrow B \in A$.

Por simplicidad de notación en esta sección, definimos además:

Definición 10. $\mathfrak{S} = \mathfrak{S}_\omega$.

Así, $\mathfrak{S}(0) = 1$ y $\mathfrak{S}(1) = 2$,

donde definimos, como ya se indicó:

Definición 11.

$$1 = \{0\},$$

$$2 = \{0, \{0\}\}.$$

Y reemplazamos a (1) por

$$G(\langle m, F(\langle m, n\rangle)\rangle) = \mathfrak{S}(F(\langle m, n\rangle)).$$

Definimos también, en este momento, $n-1$ y $n-2$ para cualquier ordinal.

Definición 12.

(i) *Si $A \neq 0$ & A es un ordinal, entonces $A - 1 = B$ si y solamente si $B' = A$*

(ii) *Si $A \neq 0$ & $A \neq 1$ & A es un ordinal, entonces $A - 2 = B$ si y solamente si $(B')' = A$.*

En vez de formular teoremas separados para funciones de un argumento, funciones de dos argumentos, etc., podemos enunciar un teorema general sobre recurrencia para funciones de r argumentos. En el teorema usamos la notación

(2) $\langle m_0, m_1, \ldots, m_{r-2}, n\rangle$

para las r-plas que ahora consideramos. Primero definimos:

Definición 13. *x es una r-pla de A si y solamente si $x \in A^r$.*

En otras palabras, una r-pla de A es una función del conjunto de los números naturales menores que r, al conjunto A. Para justificar la notación '$\langle x, y\rangle$' para las parejas (esto es, 2-plas) cuando esta notación ha sido usada ya para parejas ordenadas, tenemos el siguiente teorema cuya demostración se deja como ejercicio:

Teorema 26. *$A^2 \approx A \times A$ bajo la función g tal que para cualquier $f \in A^2$, $g(f) = \langle f(0), f(1)\rangle$.*

Puesto que A^2 es equipotente con $A \times A$, usaremos la misma notación para duplas y para parejas ordenadas y esta ambigüedad no será fuente de dificultad. En efecto, en desarrollos intuitivos de teoría de conjuntos es común "identificar" los dos conceptos. Sin usar la notación (2), nuestro teorema fundamental de recurrencia puede ser formulado de la siguiente manera poco intuitiva:

Para conjuntos cualesquiera G y H y cualquier $r > 0$, existe una única F tal que

(i) *F es una función sobre ω^r,*

(ii) *para toda f, si $f \in \omega^r$ & $f(r-1) = 0$, entonces*

$$F(f) = H(f|r-1),$$

(iii) *para toda f y para todo n, si $f \in \omega^r$ y $f(r-1) = n$, entonces*

$$F((f|r-1) \cup \{\langle r-1, n'\rangle\}) = G((f|r-1) \cup \{\langle r-1, F(f)\rangle\}).$$

Para formular de nuevo el teorema de manera esquemática luego de adoptar (2), necesitamos:

Esquema de definición 14. *Si $x_0, \ldots, x_{r-1} \in A$, entonces $\langle x_0, \ldots, x_{r-1}\rangle = f$ si y solamente si f es una r-pla de A & $f(0) = x_0$ & . . . & $f(r-1) = x_{r-1}$.*

También modificamos de una manera usual la notación $f(x)$.

Definición 15.

$$f_x = f(x).$$

Principalmente, queremos escribir f_0, f_1, etc. Finalmente, para formular nuestro teorema en la notación familiar usamos 'm' en lugar de 'f' y cuando escribimos 'm_0', 'm_1' o algo similar, queremos expresar el valor de la función m para el argumento 0, etc., y no el valor numérico de la variable 'm_0', el valor numérico de la variable 'm_1', etc. como variables numéricas.

Teorema 27. *Para conjuntos cualesquiera G y H y para cualquier $r > 0$, existe una única F tal que, para cualquier m en ω^r,*

(i) *F es una función sobre ω^r,*

(ii) $F(\langle m_0, m_1, \ldots, m_{r-2}, 0\rangle) = H(\langle m_0, m_1, \ldots, m_{r-2}\rangle)$,

(iii) *para todo número natural n,*

$F(\langle m_0, m_1, \ldots, m_{r-2}, n'\rangle) = G(\langle m_0, m_1, \ldots, m_{r-2}, F(\langle m_0, \ldots, m_{r-2}, n\rangle)\rangle)$.

Demostración. Por brevedad de notación damos la demostración para el caso especial en que $r = 2$, pero el argumento para un $r > 0$ arbitrario es casi idéntico y podemos dejarlo como ejercicio. Consideramos funciones que para $r = 2$ podrían definirse sobre $\omega \times n'$ para algún n. Para hacer paralelo el argumento para r arbitrario, definimos:

$\mathfrak{D}(n) = \{g\colon g$ es una función & $\mathfrak{D}g = \{0, 1\}$ & $g(0) \in \omega$ & $g(1) \in n'\}$.

Primero, en virtud del esquema axiomático de separación, existe un conjunto A tal que $f \in A$ si y solamente si

(1) $f \in \mathcal{P}(\omega^2 \times (\mathcal{R}(G \cup H) \cup \{0\}))$,

y existe un n tal que, para todo m,

(2) f es una función sobre $\mathfrak{D}(n)$,

(3) $f(m, 0) = H(m)$,

(4) para todo $p < n$,

$$f(\langle m, p'\rangle) = G(\langle m, f(\langle m, p\rangle)\rangle).$$

La inclusión de $\{0\}$ en el conjunto potencia de (1) toma en cuenta el caso en que G y H no están definidas. Es claro que (1) está implicado por (2) a (4). Además, vemos fácilmente que $A \neq 0$, para la función f sobre $\mathfrak{D}(0)$ tal que, para todo $m \in \omega$,

(5) $f(m, 0) = H(m)$

esté en A. (Como se indicó en (3) y (5), para el resto de la demostración eliminamos los paréntesis angulares que designan parejas, ya que no puede resultar confusión alguna de esto.)

(6) Si $f, g \in A$ entonces $f \subseteq g$ o $g \subseteq f$.

Sea $\mathfrak{D}(n)$ el dominio de f y sea $\mathfrak{D}(n_1)$ el dominio de g. Entonces $n \cap n_1$ es n o n_1. Supongamos, para precisar, que es n. Ahora supongamos que existe un número natural $p < n$ tal que para algún m

(7) $$f(m, p) \neq g(m, p).$$

Sea p^* el menor de tales números; esto es, p^* es el $\mathcal{E}_\omega$-primer elemento de

$$\{p\colon p < n \ \& \ (\exists m)(f(m, p) \neq g(m, p))\}.$$

Ahora, $p^* \neq 0$ ya que para todo m

$$f(m, 0) = g(m, 0) = H(m).$$

Tenemos entonces,

(8) $f(m, p^*) = G(m, f(m, p^* - 1)) \neq G(m, g(m, p^* - 1)) = g(m, p^*)$.

Pero, por otra parte; ya que p^* es el menor número natural para el cual se cumple (7), tenemos:

$$f(m, p^* - 1) = g(m, p^* - 1)$$

y *a fortiori*

$$G(m, f(m, p^* - 1)) = G(m, g(m, p^* - 1)),$$

lo que contradice (8) y hace que nuestra suposición (7) sea falsa. Por consiguiente, se establece (6).

Definimos ahora:

(9) $$F = \cup A.$$

Se sigue, de una vez, a partir de (6) que F es una función, pues si $\langle x, y\rangle \in F \in A$ y $\langle x, z\rangle \in g \in A$, entonces ambas parejas pertenecen, o a f o a g y por tanto $y = z$. Además, se sigue de (5) y (9) que para todo m

$$F(m, 0) = H(m),$$

lo que satisface (ii) del teorema.

Dirigimos ahora nuestra atención hacia (iii). Si $\langle m, n'\rangle$ está en el dominio de F, entonces, para algún f en A, $\langle m, n'\rangle$ es un elemento del dominio de f y entonces,

$$f(m, n') = G(m, f(m, n)),$$

de donde,

$$F(m, n') = G(m, F(m, n)).$$

Para demostrar que ω^2 es el dominio de F suponemos que p es el menor número natural tal que, para algún $m, \langle m, p\rangle$ no está en el dominio de F. Entonces, en vista de (5), $p \neq 0$, así que $\langle m, p-1\rangle$ está en $\mathfrak{D}F$ y $F \in A$; pero entonces también,

$$(10)\ F \cup \bigcup_{m\in\omega} \{\langle\langle m, p\rangle, G(m, F(m, p-1))\rangle\} \in A.$$

Podemos concluir de (10) que $\langle m, p\rangle \in \mathfrak{D}F$, contrario a nuestra suposición. Concluimos que ω^2 es el dominio de F. Finalmente, dejamos como ejercicio la demostración sencilla de que F es única. Q.E.D.

Demostrado este teorema general y fundamental, acerca de la existencia de una única función F que satisface al definiens de una definición recurrente, podemos definir las operaciones artiméticas usuales sin teoremas justificantes individuales. Simplemente elegimos las funciones apropiadas G y H.

Definimos primero la adición entre números naturales por medio de la recurrencia ya indicada. Usamos el mismo símbolo '$+$' para adición cardinal y para adición ordinal finita (y más adelante para adición ordinal arbitraria), pero en cualquier contexto dado siempre será claro lo que se quiere decir. Puede notarse que el símbolo para la adición ordinal finita designa una entidad de la teoría de conjuntos; en particular, un cierto conjunto de parejas ordenadas, en cada una de las cuales el primer elemento es una dupla. En contraste, el símbolo para adición cardinal o para adición ordinal general no designa conjunto alguno.

Definición 16. $+ = f$ *si y solamente si*

(i) *f es una función sobre ω^2,*

(ii) *para todo m,*

$$f(\langle m, 0\rangle) = m,$$

(iii) *para todo m, n,*

$$f(\langle m, n'\rangle) = \mathfrak{S}(f(\langle m, n\rangle)).$$

Para obtener la notación usual, definimos:

Definición 17. $m + n = p$ *si y solamente si* $\langle\langle m, n\rangle, p\rangle \in +$.

Como consecuencias inmediatas de la definición 16, tenemos:

Teorema 28.

(i) $m + 0 = m$,

(ii) $m + n' = (m + n)'$.

Las leyes familiares, conmutativa y asociativa de la adición se enuncian en los dos siguientes teoremas. Sus demostraciones ilustran usos típicos de inducción matemática (vía el teorema 24). Nótese que los teoremas correspondientes para la aritmética cardinal no necesitaban ser demostrados inductivamente.

Teorema 29. $m + n = n + m$.

Demostración. Necesitamos dos resultados preliminares:

(I) $0 + n = n$

(II) $m' + n = (m + n)'$,

cada uno de los cuales demostramos inductivamente, usando el teorema 24. Para demostrar (I) definimos:

(1) $Z = \{n\colon 0 + n = n\}$,

y queremos demostrar que $Z = \omega$, esto es, todo número natural pertenece a Z. Primero, en virtud del teorema 28,

$$0 \in Z.$$

Ahora suponemos que $n \in Z$, esto es,

(2) $0 + n = n$.

Entonces tenemos:

$$\begin{aligned} 0 + n' &= (0 + n)' && \text{por el teorema 28} \\ &= n' && \text{por (2).} \end{aligned}$$

Por tanto, si $n \in Z$, entonces $n' \in Z$, así que, en virtud del teorema 24,

$$Z = \omega$$

(ya que se sigue de (1) que $Z \subseteq \omega$, y del teorema 24, que $\omega \subseteq Z$).

Ahora, para demostrar (II) definimos:

$$A(m) = \{n\colon m' + n = (m + n)'\}.$$

Por dos aplicaciones del teorema 28,

$$m' + 0 = m' = (m + 0)',$$

así que,

$$0 \in A(m).$$

Ahora, supongamos que $n \in A(m)$, esto es,

(3) $$m' + n = (m + n)'.$$

Entonces,

$$\begin{aligned} m' + n' &= (m' + n)' && \text{por el teorema 28} \\ &= ((m + n)')' && \text{por (3)} \\ &= (m + n')' && \text{por el teorema 28,} \end{aligned}$$

así que, $n' \in A(m)$ cuando quiera que $n \in A(m)$. De donde, por el teorema 24,

$$A(m) = \omega,$$

lo que establece (II) y completa nuestra preparación para la principal tarea que tenemos entre manos.

Definimos:

$$B(n) = \{m\colon m + n = n + m\}.$$

Primero tenemos:

$$\begin{aligned} 0 + n &= n && \text{por (I)} \\ &= n + 0 && \text{por el teorema 28,} \end{aligned}$$

y, por consiguiente,

$$0 \in B(n).$$

Ahora suponemos $m \in B(n)$, esto es,

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

Entonces,

$$\begin{aligned} m' + n &= (m + n)' && \text{por (II)} \\ &= (n + m)' && \text{por (4)} \\ &= n + m' && \text{por el teorema 28,} \end{aligned}$$

de donde, $m' \in B(n)$ cuando quiera que $m \in B(n)$, y concluimos que

$$B(n) = \omega,$$

que es el resultado pedido. Q.E.D.

La demostración de la ley asociativa de la adición es semejante en estructura.

Teorema 30. $(m + n) + p = m + (n + p)$.

Demostración. Definimos:

$$A(m, n) = \{p\colon (m + n) + p = m + (n + p)\}.$$

Ahora,

$$\begin{aligned} (m + n) + 0 &= m + n && \text{por el teorema 28} \\ &= m + (n + 0) && \text{de nuevo por el teorema 28} \end{aligned}$$

por consiguiente, $0 \in A(m, n)$.

Sea p un elemento de $A(m, n)$. Entonces,

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

y tenemos

$$\begin{aligned} (m + n) + p' &= ((m + n) + p)' && \text{por el teorema 28} \\ &= (m + (n + p))' && \text{por (1)} \\ &= m + (n + p)' && \text{por el teorema 28} \\ &= m + (n + p') && \text{por el teorema 28,} \end{aligned}$$

de donde $p' \in A(m,n)$, y podemos concluir:

$$A(m, n) = \omega. \qquad \text{Q.E.D.}$$

Formulamos, sin demostración, un teorema familiar.

Teorema 31. *Si $m \leq n$, entonces existe un único número natural p tal que $m + p = n$.*

Ahora nos referimos a la definición de multiplicación. Si hubiéramos procedido sin la teoría de conjuntos habríamos agregado a P6 y P7 dos axiomas más:

P8. *Si x es un número natural, entonces* $x \cdot 0 = 0$.

P9. *Si x, y son números naturales, entonces*

$$x \cdot y' = (x \cdot y) + x.$$

Esos dos axiomas predicen exactamente la definición que usamos.

Definición 18. $\cdot = f$ *si y solamente si:*

(i) *f es una función sobre ω^2,*

(ii) *para todo m,*
$$f(\langle m, 0\rangle) = 0,$$

(iii) *para todo m, n,*
$$f(\langle m, n'\rangle) = f(\langle m, n\rangle) + m.$$

Análoga a la definición 17, tenemos:

Definición 19. $m \cdot n = p$, *si y solamente si* $\langle\langle m, n\rangle, p\rangle \in$.

Cuando no se presta a confusión designamos la multiplicación por yuxtaposición en lugar del punto.

Dejamos como ejercicios las demostraciones de los tres teoremas siguientes.

Teorema 32. $mn = nm$.

Teorema 33 $m(n + p) = mn + mp$.

Teorema 34. $(mn)p = m(np)$.

Otros teoremas adicionales se han dejado como ejercicios.

Concluimos esta sección con la definición de la operación exponencial. El esquema recurrente es:

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

La definición formal apropiada es:

Definición 20. $\exp = f$, *si y solamente si:*
(i) f *es una función sobre* ω^2
(ii) *para todo* m,

$$f(\langle m, 0\rangle) = 1,$$

(iii) *para todo* m, n,

$$f(\langle m, n'\rangle) = f(\langle m, n\rangle) \cdot m.$$

Como deferencia hacia la notación ortodoxa:

Definición 21. $m^n = \exp(m, n)$.

En el capítulo siguiente, que trata de la construcción de los números racionales y reales, supondremos que se ha desarrollado completamente la aritmética elemental de los enteros, pues, con el teorema 27 a la mano, es perfectamente obvio cómo continuar los desarrollos. En realidad, en los ejercicios se han dado varios detalles.

En el capítulo 7 se indicará cómo puede generalizarse el teorema 27 a lo que se denomina una recurrencia de orden de valores. Así, cuando F es una función de un argumento, tenemos:

(1) $$F(n) = G(F \mid n),$$

esto es, el valor de F para el argumento n puede depender de todos los argumentos precedentes y de los valores de F, que se indican a la derecha de (1), por la restricción del dominio de F a n. Un ejemplo sencillo de tal recurrencia de orden de valores es la definición de la función apropiada que produce la sucesión de Fibonacci

$$0, 1, 1, 2, 3, 5, 8, 13, \ldots$$

Intuitivamente, excepto para los dos primeros términos, cada término es simplemente la suma de los dos que le preceden.

El esquema recurrente es:

$$F(0) = 0$$
$$F(1) = 1$$
$$F(n + 1) = F(n - 1) + F(n),$$

esto es, el término general $F(n + 1)$ depende no sólo de $F(n)$ sino también de $F(n - 1)$.

Concluimos esta sección con la definición de finitud ordinaria ya anticipada en § 4.2 y dejamos como ejercicio la demostración de la equivalencia de esta definición con la de Tarski que se usó en § 4.2.

Definición 22. *Un conjunto es finito ordinario si y solamente si es equipotente con algún número natural.*

Teorema 35. *Un conjunto es finito ordinario si y solamente si es finito en el sentido de Tarski.*

Tenemos también:

Teorema 36. *Un conjunto finito es equipotente exactamente con un número natural.*

Sobre la base de este teorema y la definición de números naturales, no es difícil demostrar que la definición de finitud de Stäckel [1907] en términos de doble ordenación es equivalente a la de Tarski.

Teorema 37. *Un conjunto es finito en el sentido de Tarski si y solamente si puede bien-ordenarse doblemente, es decir, si y solamente si existe una relación* R *tal que tanto* R *como* $\breve{R}$ *bien-ordenan el conjunto.*

EJERCICIOS

1. Demostrar: *A es un número natural, si y solamente si A es un ordinal y para todo B, si $B \in A'$, entonces existe*

un ordinal C tal que $B = C'$ o $B = 0$. (Esta equivalencia se usa a veces como definición de los números naturales.)

2. Dar un contra-ejemplo a: *A es un número natural, si y solamente si A es un ordinal y $A = 0$ o existe un ordinal B tal que $A = B'$.*
3. Demostrar el teorema 21.
4. Dar una demostración detallada del teorema 23.
5. Dar un contra-ejemplo para mostrar que no todo subconjunto de un número natural es un número natural.
6. Demostrar que, si A es un número natural y B es el $\mathcal{E}A$-último elemento de A, entonces $A = B'$.
7. ¿Es válida la aserción del ejercicio 6 para ordinales arbitrarios?
8. Demostrar que, si A es un número natural, entonces $\bigcup(A')$ lo es también.
9. Si $A \subset \omega$, ¿es verdadero que $\bigcup A$ es un número natural? Si la respuesta es afirmativa, demostrarlo; si no, dar un contra-ejemplo.
10. Si A es un ordinal, ¿qué conjunto es $\bigcap A$?
11. Si $A \subseteq \omega$, ¿es $\bigcap A$ un número natural?
12. Demostrar que $\bigcup \omega = \omega$.
13. Completar la demostración del teorema 27 demostrando que F es única.
14. Indicar qué cambios se requieren en la demostración del teorema 27 para hacerlo adecuado para r arbitrario.
15. Demostrar el teorema 31.
16. Demostrar el teorema 32.
17. Demostrar los teoremas 33 y 34.
18. Dar un esquema recurrente y luego definir explícitamente:
    (a) la operación factorial $n!$;
    (b) la sucesión de Fibonacci mencionada al final de la sección (con una ligera reformulación de la recurrencia dada para la sucesión se puede incluir en el alcance del teorema 27).
19. Demostrar los hechos familiares elementales acerca de la operación de exponenciación para números naturales.
20. Demostrar los ejercicios 4 a 12 de § 4.4 para números naturales.
21. Demostrar el teorema 35.
22. Demostrar el teorema 36.
23. Demostrar el teorema 37.

§ 5.3 Conjuntos enumerables. Un conjunto enumerable es uno que es equipotente con el conjunto de los números naturales. Un tal conjunto proporciona el ejemplo más simple de un conjunto infinito. Comenzamos con algunos teoremas generales acerca de conjuntos infinitos.

Definición 23. *Un conjunto es infinito si y solamente si no es finito.*

Los dos primeros teoremas pueden demostrarse fácilmente usando resultados de § 4.2.

Teorema 38. *Si A es infinito y $A \approx B$, entonces B es infinito.*

Teorema 39. *Si $A \subseteq B$ y A es infinito, entonces B es infinito.*

De algún interés mayor es el teorema siguiente que proporciona una condición necesaria y suficiente para que un conjunto sea infinito.

Teorema 40. *Un conjunto A es infinito si y solamente si, para todo número natural n, existe un subconjunto de A equipotente con n.*

Demostración. [Necesidad]. En virtud del esquema axiomático de separación, existe un C tal que, para todo n,

$$n \in C \leftrightarrow n \in \omega \;\&\; (\exists B)(B \subseteq A \;\&\; B \approx n).$$

Demostramos por inducción que $C = \omega$.

Ya que el conjunto vacío es subconjunto de cualquier conjunto,

$$0 \in C.$$

Ahora supongamos que $n \in C$. Entonces, por la hipótesis, existe un subconjunto B de A tal que

$$B \approx n.$$

Puesto que A es infinito, $B \neq A$, pues si $A = B$, entonces $A \approx n$ y A sería finito (teorema 35). Sea, x por consiguiente, un elemento de $A \sim B$. Entonces,

$$B \cup \{x\} \subseteq A$$

y claramente, en vista del teorema 4 de § 4.1,

$$B \cup \{x\} \approx n'$$

de donde $n' \in C$.

[Suficiencia]. Supongamos, si es posible, que A es finito. Entonces, (teorema 35), para algún n,

$$A \approx n.$$

Pero por la hipótesis debe existir un subconjunto propio no vacío B de A tal que $B \approx n'$. Sea $x \in B$; entonces, $B \sim \{x\} = n$, de donde A es equipotente con uno de sus subconjuntos propios, a saber, $B \sim \{x\}$ y esto contradice al teorema 46 de § 4.2. Q.E.D.

Usando este teorema y algunos resultados anteriores es fácil demostrar:

Teorema 41. *El conjunto ω de los números naturales es infinito.*

Un teorema más difícil es el siguiente, que expresa una condición necesaria y suficiente para que un conjunto sea finito. La demostración de la suficiencia es la parte difícil porque envuelve definición por recurrencia de una función (teorema 27).

Teorema 42. *A es finito si y solamente si $A \prec \omega$.*

Demostración. [Necesidad]. Este teorema se sigue inmediatamente del teorema precedente y del teorema 45 de § 4.2.

[Suficiencia]. Por hipótesis, $A \prec \omega$. Sea B un subconjunto propio de ω tal que $A \approx B$. Si B tiene un número natural mayor que todos, digamos m, entonces $B \subseteq m'$; ya que m' es finito, también lo es B y por tanto también lo es A. La cosa difícil de demostrar es que en realidad B debe tener un número natural mayor que todos. (Suponemos que B no es vacío; de otro modo la demostración es trivial.) Usamos una demostración indirecta. Supongamos que B no tiene un número natural mayor que todos, esto es, dado cualquier natural existe siempre uno mayor en B. Usando el teorema 27 definimos la función F sobre ω como sigue:

(1) $F(0) = \varepsilon\omega$-primer elemento de B.

(2) $F(n') = \varepsilon\omega$-primer elemento de $B \sim F(n)$.

(Nótese que es sencillo definir funciones G y H que correspondan a los miembros de la derecha de (1) y (2).)

Puesto que B no tiene un elemento mayor que todos, es claro que, para todo n y m, si $n \neq m$, entonces

$$F(n) \neq F(m),$$

de donde, $B \approx \omega$ bajo F, contrario a la hipótesis y nuestra suposición es falsa. Q.E.D.

Ahora nos referimos a conjuntos enumerables y comenzamos por formular de nuevo la definición dada al comienzo de la sección.

Definición 24. *Un conjunto es enumerable si y solamente si es equipotente con el conjunto ω de todos los números naturales.*

Como una consecuencia inmediata de los teoremas 38 y 41 tenemos:

Teorema 43. *Todo conjunto enumerable es infinito.*

Algo sorprendente: toda demostración conocida del recíproco parcial, a saber que todo conjunto infinito tiene un subconjunto enumerable, requiere el axioma de escogencia. En efecto, este recíproco es el paso esencial para demostrar que el infinito ordinario implica el infinito de Dedekind, concepto este que ahora definimos formalmente. Los dos teoremas que siguen a la definición son consecuencias inmediatas de resultados anteriores.

Definición 25. *Un conjunto es infinito si y solamente si no es finito según Dedekind.*

Teorema 44. *Un conjunto es infinito según Dedekind si y solamente si tiene un subconjunto propio equipotente con él.*

Teorema 45. *A es infinito según Dedekind si y solamente si $A \approx A \cup \{A\}$.*

La contrapositiva del teorema 46 del capítulo 4 es:

Teorema 46. *Si un conjunto es infinito según Dedekind, entonces es infinito.*

Nos referimos ahora a dos teoremas más difíciles que, entre ambos, establecen otra condición necesaria y suficiente para que un conjunto sea infinito según Dedekind.

Teorema 47. *Todo conjunto que tiene un subconjunto enumerable es infinito según Dedekind.*

Demostración. Sea B un subconjunto enumerable de A. Entonces,

$$B \approx \omega$$

bajo alguna función 1-1, digamos f. Ahora consideremos la función g definida sobre A por

$$g(x) = \begin{cases} \check{f}(f(x)') & \text{si } x \in \mathfrak{D}f \\ x & \text{si } x \in A \sim \mathfrak{D}f. \end{cases}$$

(Intuitivamente, si $x \in \mathfrak{D}f$ y $f(x) = n$, escribimos: x_n. Entonces, si $x \in \mathfrak{D}f$ simplemente tenemos: $g(x_n) = x_{n+1}$.) Obviamente

$$g \text{ es } 1\text{-}1$$

$$\mathfrak{D}g = A$$

$$\mathfrak{R}g = A \sim \{\check{f}(0)\},$$

de donde

$$A \approx A \sim \{\check{f}(0)\},$$

lo que establece nuestro teorema. Q.E.D.

Ahora demostramos el recíproco, que requiere definición recurrente de una función apropiada.

Teorema 48. *Todo conjunto infinito según Dedekind tiene ùn subconjunto enumerable.*

Demostración. Sea A un conjunto infinito, según Dedekind y sea B un subconjunto propio de A tal que $A \approx B$ bajo la función f, digamos. Sea x^* un elemento de $A \sim B$. Definimos recurrentemente (teorema 27) una función g sobre ω:

$$g(0) = x^*$$

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

Claramente, para cada n, $g(n) \in A$. Lo que necesitamos demostrar es que la función g es 1-1. Supongamos, por vía de contradicción, que g no es 1-1. Entonces sea p el menor número natural tal que para algún $q < p$

(1) $$g(p) = g(q).$$

Obviamente, $p \neq 0$. Además, puesto que

(2) $$g(p) = f(g(p - 1)),$$

sabemos que $g(p) \in B$, y ya que $g(0) = x^* \notin B$, tenemos

$$g(p) \neq g(0)$$

así que, a partir de (1),

$$g(q) \neq g(0),$$

de donde

$$q \neq 0.$$

Así,

(3) $$g(q) = f(g(q - 1)),$$

y de (1) a (3) se sigue que

$$f(g(p - 1)) = f(g(q - 1)),$$

además, puesto que f es 1-1,

$$g(p - 1) = g(q - 1),$$

lo que contradice nuestra suposición de que p es el menor número natural que satisface a (1) con $q < p$. Q.E.D.

Teorema 49. *Todo subconjunto de un conjunto enumerable es enumerable o es finito.*

Demostración. Sea A un conjunto enumerable y sea $B \subseteq A$. Entonces $B \preceq A$. Si $B \approx A$ entonces B es enumerable. Si $B \prec A$, entonces $B \prec \omega$, ya que $A \approx \omega$, así que, por el teorema 42, B es finito. Q.E.D.

Este teorema representa una aplicación significativa del teorema 42. La simplicidad de la demostración depende enteramente de la realizada anteriormente para el teorema 42.

Teorema 50. *Si A es finito y B es enumerable, entonces, $A \cup B$ es enumerable.*

Demostración. Sea

$$C = A \sim B;$$

a partir de la hipótesis del teorema, C es finito, así que existe un número natural n tal que (teorema 35)

$$C \approx n$$

bajo f, digamos. Ahora, B es enumerable, de donde,

$$B \approx \omega$$

bajo una función g, digamos. Ahora definamos una nueva función h sobre $A \cup B$:

$$h(x) = \begin{cases} f(x) & \text{si } x \in C \\ g(x) + n & \text{si } x \in B. \end{cases}$$

Claramente h es 1-1 y aplica $A \cup B$ sobre ω. Q.E.D.

La demostración del teorema siguiente es más difícil y la omitimos.

Teorema 51. *Si A y B son enumerables, entonces $A \cup B$ es enumerable.*

Tenemos algunos teoremas correspondientes acerca de la enumerabilidad de los productos cartesianos. En este caso demostramos el segundo.

Teorema 52. *Si A es finito, pero no vacío, y B es enumerable, entonces $A \times B$ es enumerable.*

Teorema 53. $\omega \times \omega = \omega$.

Demostración. La demostración se basa en el arreglo de la doble sucesión

$$\langle 0, 0\rangle, \langle 0, 1\rangle, \langle 0, 2\rangle, \ldots$$

$$\langle 1, 0\rangle, \langle 1, 1\rangle, \langle 1, 2\rangle, \ldots$$

$$\langle 2, 0\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle, \ldots$$

en una sucesión única, por el método de las diagonales (procedemos a lo largo de diagonales):

(1) $\langle 0, 0\rangle, \langle 0, 1\rangle, \langle 1, 0\rangle, \langle 0, 2\rangle, \langle 1, 1\rangle, \langle 2, 0\rangle, \ldots$

Otra manera de caracterizar (1) es decir que ordenamos primero de acuerdo a la suma de los dos números y luego por el primer elemento, dentro de una suma fijada. Definimos sobre $\omega \times \omega$ una función f tal que

$$f(\langle 0, 0\rangle) = 0$$

$$f(\langle 0, 1\rangle) = 1$$

$$f(\langle 1, 0\rangle) = 2$$

$$f(\langle 0, 2\rangle) = 3$$

$$\cdots\cdots$$

Es claro que f aplica $\omega \times \omega$ sobre ω de la manera 1-1; se deja como ejercicio el hallar la forma aritmética precisa de f. Q.E.D.

Teorema 54. *Si $n \neq 0$, entonces $\omega^n = \omega$.*

Teorema 55. *Si A y B son enumerables, entonces $A \times B$ es enumerable.*

Teorema 56. *Si A es enumerable y $n \neq 0$, entonces A^n es enumerable.*

Nos referimos ahora a algunos teoremas acerca de cardinales infinitos y transfinitos. Las definiciones pertinentes y las demostraciones de los teoremas dependen todas del axioma especial para números cardinales. Debe ser claro, a partir de observaciones anteriores, que toda demostración conocida de que un cardinal es transfinito si y solamente si es infinito depende del axioma de escogencia.

†**Definición 26.** *x es un cardinal infinito si y solamente si existe un conjunto infinito A tal que $\mathcal{K}(A) = x$.*

†**Definición 27.** *x es un cardinal transfinito si y solamente si existe un conjunto A infinito según Dedekind tal que $\mathcal{K}(A) = x$.*

Sobre la base de los teoremas demostrados previamente, se deducen fácilmente los cuatro resultados siguientes.

†**Teorema 57.** *$\mathfrak{n}$ es un cardinal infinito si y solamente si para todo cardinal finito $\mathfrak{m}$, $\mathfrak{m} < \mathfrak{n}$.*

†**Teorema 58.** *$\mathfrak{n}$ es un cardinal transfinito si y solamente si $\mathfrak{n} = \mathfrak{n} + 1$.*

†**Teorema 59.** *Si un cardinal es un cardinal transfinito, entonces es un cardinal infinito.*

†**Teorema 60.** *Si $\mathfrak{m}$ es un cardinal infinito o transfinito y $\mathfrak{m} \leq \mathfrak{n}$, entonces, $\mathfrak{n}$ es un cardinal infinito o transfinito, respectivamente.*

Un teorema que requiere cierta cantidad de demostración (que se deja como ejercicio) es el de que la suma o el producto de un cardinal transfinito o infinito con otro cardinal (excepto 0 para el producto) es también un cardinal transfinito o infinito.

†**Teorema 61.** *Si $\mathfrak{m}$ es un cardinal transfinito o infinito, entonces*

(i) $\mathfrak{m} + \mathfrak{n}$ *es un cardinal transfinito o infinito, respectivamente,*

(ii) $\mathfrak{m}\mathfrak{n}$ *y* $\mathfrak{m}^{\mathfrak{n}}$ *son cardinales transfinitos o infinitos, respectivamente, previsto que* $\mathfrak{n} \neq 0$,

(iii) $\mathfrak{n}^{\mathfrak{m}}$ *es un cardinal transfinito o infinito, respectivamente, previsto que* $1 < \mathfrak{n}$.

Podemos usar algunos de estos resultados, particularmente el teorema 58, para demostrar una desigualdad para números transfinitos, que no vale para cardinales arbitrarios. Nótese que el método de demostración es específico para cardinales transfinitos y no funcionará para cardinales infinitos (sin el axioma de escogencia).

†**Teorema 62.** *Si* $\mathfrak{m}$ *y* $\mathfrak{n}$ *son cardinales transfinitos, entonces*

$$\mathfrak{m} + \mathfrak{n} \leq \mathfrak{m}\mathfrak{n}.$$

Demostración. Sobre la base del teorema 58,

$$\mathfrak{m} = \mathfrak{m} + 1$$
$$\mathfrak{n} = \mathfrak{n} + 1,$$

de donde, usando las leyes distributiva y conmutativa de § 4.3,

(1) $\mathfrak{m}\mathfrak{n} = (\mathfrak{m} + 1)(\mathfrak{n} + 1) = \mathfrak{m}\mathfrak{n} + \mathfrak{m} + \mathfrak{n} + 1 = (\mathfrak{m} + \mathfrak{n}) + (\mathfrak{m}\mathfrak{n} + 1).$

Primeramente, sobre la base del teorema 74 de § 4.3, sabemos que

$$\mathfrak{m} \leq \mathfrak{m} + \mathfrak{n}$$

y

$$\mathfrak{n} \leq \mathfrak{m}\mathfrak{n} + 1,$$

de donde, usando de nuevo el teorema 54,

(2) $\mathfrak{m} + \mathfrak{n} \leq (\mathfrak{m} + \mathfrak{n}) + (\mathfrak{m}\mathfrak{n} + 1).$

Nuestro teorema se sigue de (1) y (2). Q.E.D.

Por el uso del axioma de escogencia la desigualdad del teorema que se acaba de demostrar se puede reforzar con una igualdad, esto es, sobre la base de suponer el axioma de escogencia, podemos demostrar que la suma de dos cardinales transfinitos es igual a su producto. Nótese que el teorema es falso para cardinales finitos, ya que $\mathfrak{n} \cdot 1 < \mathfrak{n} + 1$.

Para convertir algunos de los teoremas acerca de conjuntos enumerables en teoremas acerca de números cardinales, necesitamos definir el cardinal $\aleph_0$ de los conjuntos enumerables. $\aleph_0$ se lee "alef sub-cero"; la letra '$\aleph$' es la primera letra del alfabeto hebreo. (Esta notación se originó con Cantor.)

†**Definición 28.** $\aleph_0 = \mathcal{K}(\omega)$.

Como consecuencias inmediatas de los teoremas 50 y 51 y la definición de adición cardinal en §4.3, tenemos:

†**Teorema 63.**

(i) *Si* $\mathfrak{n}$ *es un cardinal finito, entonces* $\aleph_0 + \mathfrak{n} = \aleph_0$,

(ii) $\aleph_0 + \aleph_0 = \aleph_0$.

La demostración del útil teorema siguiente se deja como ejercicio.

†**Teorema 64.** *Las tres condiciones siguientes son equivalentes:*

(i) $\mathfrak{m}$ *es un cardinal transfinito,*

(ii) $\aleph_0 \leq \mathfrak{m}$,

(iii) *existe un cardinal* $\mathfrak{n}$ *tal que* $\aleph_0 + \mathfrak{n} = \mathfrak{m}$.

Sobre la base de los teoremas 52 y 53, tenemos de una vez:

†**Teorema 65.**

(i) *Si* $\mathfrak{n}$ *es un cardinal finito y* $\mathfrak{n} \neq 0$, *entonces* $\mathfrak{n}\aleph_0 = \aleph_0$,

(ii) $\aleph_0\aleph_0 = \aleph_0$.

Y sobre la base del teorema 54:

†**Teorema 66.** *Si* $\mathfrak{n}$ *es un cardinal finito y* $\mathfrak{n} \neq 0$, *entonces* $\aleph_0^{\mathfrak{n}} = \aleph_0$.

Ahora demostramos dos hechos ulteriores acerca de los cardinales transfinitos.

†**Teorema 67.** *Si* $\mathfrak{u}$ *es un cardinal transfinito, entonces*

(i) $\mathfrak{u} + \aleph_0 = \mathfrak{u}$,

(ii) *si* $\mathfrak{n}$ *es un cardinal finito,* $\mathfrak{u} + \mathfrak{n} = \mathfrak{u}$.

Demostración. En virtud del teorema 64 existe un $\mathfrak{n}$ tal que

$$\aleph_0 + \mathfrak{n} = \mathfrak{u},$$

de donde,

$$\begin{aligned}
\mathfrak{u} + \aleph_0 &= (\aleph_0 + \mathfrak{n}) + \aleph_0 \\
&= \mathfrak{n} + (\aleph_0 + \aleph_0) \\
&= \mathfrak{n} + \aleph_0 && \text{por el teorema 63} \\
&= \aleph_0 + \mathfrak{n} \\
&= \mathfrak{u},
\end{aligned}$$

lo que demuestra (i). Con métodos similares se establece (ii):

$$\begin{aligned} \mathfrak{u} + \mathfrak{n} &= (\mathfrak{u} + \aleph_0) + \mathfrak{n} && \text{por (i)} \\ &= \mathfrak{u} + (\aleph_0 + \mathfrak{n}) && \\ &= \mathfrak{u} + \aleph_0 && \text{por el teorema 63} \\ &= \mathfrak{u} && \text{por (i), de nuevo} \end{aligned}$$

Q.E.D.

EJERCICIOS

1. Demostrar los teoremas 38 y 39.
2. Demostrar el teorema 41.
3. Demostrar el teorema 51.
4. Demostrar el teorema 52.
5. Hallar la forma aritmética exacta de la función f de la demostración del teorema 53.
6. Demostrar el teorema 54.
7. Demostrar los teoremas 55 y 56.
8. Demostrar que, si el dominio de una función es enumerable, la función es enumerable y su recorrido es finito o enumerable.
9. Demostrar que, si A es enumerable, entonces existe una familia B de conjuntos tales que
   (i) B es enumerable,
   (ii) si $C \in B$, entonces C es enumerable,
   (iii) si $C, D \in B$ y $C \neq D$, entonces $C \cap D = 0$,
   (iv) $\cup B = A$.

(Las demostraciones conocidas del recíproco de este teorema requieren el axioma de escogencia.)

10. Demostrar los teoremas 57 a 60.
11. Demostrar el teorema 61.
12. Demostrar el teorema 64.
13. Demostrar que, si $\mathfrak{n}$ es un cardinal finito, entonces $\mathfrak{n} < \aleph_0$.

Capítulo 6

*Números racionales y números reales**

§ 6.1 **Introducción.** Para mostrar que nuestros axiomas de la teoría de conjuntos son adecuados para permitir el desarrollo sistemático de la matemática clásica, no es suficiente construir meramente los números naturales como lo hicimos en el capítulo anterior. Como mínimo necesitamos mostrar que podemos construir entidades que tengan todas las propiedades esperadas de los números reales.

Los dos métodos básicos de la teoría de conjuntos para construir los números reales fuera de los números naturales se deben a Cantor y Dedekind, pero Bertrand Russell también merece crédito por clarificar el carácter riguroso de esas construcciones y por ser completamente explícito acerca de la identificación de los números reales con las entidades construidas.

Previa a la construcción de los números reales es la construcción de los números racionales (intuitivamente un elemento racional es un número que puede representarse como la razón de dos enteros). Se pueden seguir varios caminos de desarrollo:

I

Números Naturales
Enteros
Fraccionarios
Números racionales
Números reales

II

Números Naturales
Fraccionarios no negativos
Números racionales no negativos
Números reales no negativos
Todos los números reales

III

Números Naturales
Fraccionarios no negativos
Números racionales no negativos
Todos los números racionales
Números reales

Se pueden seguir muchas variantes de estos tres caminos, dependientes de la elección del nivel al cual se introducen los números negativos. Aquí se adoptará el camino III. Los fraccionarios no negativos se definen como parejas ordenadas de enteros no negativos. Así el fraccionario $\frac{1}{2} = \langle 1, 2\rangle$. Los números racionales no negativos se definen como ciertas clases de equivalencia de fraccionarios. Por ejemplo, el número racional no negativo $[\frac{1}{2}]$ correspondiente al fraccionario $\frac{1}{2}$ es el conjunto de todos los fraccionarios m/n tales que $n = 2m$. Para obtener todos los números racionales, subimos a otro nivel de abstracción. Decimos que dos parejas ordenadas $\langle x, y\rangle$ y $\langle u, v\rangle$ de números racionales no negativos son equivalentes cuando

$$x + v = y + u,$$

y un número racional es precisamente una clase de equivalencia de tales parejas ordenadas. Quizás puede parecer raro distinguir entre el fraccionario $\frac{1}{2}$, el número racional no negativo $[\frac{1}{2}]$, la pareja ordenada $\langle[\frac{1}{2}], [\frac{0}{1}]\rangle$, y el número racional $[\langle[\frac{1}{2}], [\frac{0}{1}]\rangle]$. Pero, como veremos, cada nivel de abstracción se construye sobre el precedente de una manera natural.

*Este capítulo puede omitirse sin pérdida de continuidad.

Con todos los números racionales disponibles, el procedimiento de Dedekind para construir los números reales es definir una *sección* o *corte* de los racionales como una pareja ordenada $\langle A,B\rangle$ de conjuntos tales que

(i) A y B son ambos no vacíos,
(ii) $A \cup B =$ el conjunto de los racionales,
(iii) si $x \in A$ y $y \in B$ entonces $x<y$.

A se llama la *clase inferior* y B la *clase superior*, ya que todo elemento de A precede a todo elemento de B. Un *número real* es entonces, simplemente, una sección de los racionales.

Una definición algo más simple fue dada por Peano y Russell. Como lo sugiere una rápida inspección de la definición anterior, ¿por qué no pasar por alto al conjunto A o al conjunto B? Esto nos lleva a: un *corte inferior* o *segmento inferior* de los racionales es un conjunto A tal que

(i) $A \neq 0$,
(ii) $A \subset \mathrm{Ra}$,
(iii) si $x \in A$ y $y \in \mathrm{Ra} \sim A$ entonces $x < y$,
(iv) para todo x en A, existe un y en A tal que $x < y$, donde Ra es el conjunto de los números racionales.

La demostración de que los segmentos inferiores de los racionales tienen todas las propiedades esperadas de los números reales se da con gran detalle en Landau [1930].

El enfoque de Cantor para los números reales es menos algebraico y de carácter más analítico. El usa la noción básica de *sucesión* de racionales, esto es, la noción de una función cuyo dominio es ω y cuyo recorrido es un subconjunto de Ra. Una sucesión x es una *sucesión de Cauchy* si, para todo número racional positivo ϵ, existe un número natural N tal que para todos $m, n > N$

$$|x_n - x_m| < \epsilon.$$

(Usando la notación tradicional, escribimos x_n, en lugar de $x(n)$.)*

Siguiendo a Cantor, dos sucesiones de Cauchy x y y se dicen equivalentes si para todo número racional positivo ϵ existe un número natural N tal que para todo $n > N$

$$|x_n - y_n| < \epsilon.$$

Los números reales se definen entonces como clases de equivalencia de sucesiones de Cauchy.

En este capítulo seguimos a Cantor más bien que a Dedekind por la razón de que cuando se usan las sucesiones de Cauchy los métodos de demostración son mucho más característicos de los métodos generales del análisis, en particular, de los que se emplean en la teoría de series infinitas.

§ 6.2 **Fraccionarios.** Volviendo ahora a los desarrollos sistemáticos, comenzamos por construir los fraccionarios no negativos, los cuales, por brevedad, llamaremos simplemente fraccionarios. Como en el capítulo anterior, usaremos las variàbles 'm', 'n', 'p', 'q' y 'r', con o sin sub-índices, para los números naturales.

Definición 1. *x es un fraccionario* $\leftrightarrow (\exists m)(\exists n)(n \neq 0 \;\&\; x = \langle m, n\rangle)$.

Intuitivamente, $x = \dfrac{m}{n}$, y para tener disponible esta notación usual, definimos:

Definición 2. *Si $n \neq 0$, entonces* $\dfrac{m}{n} = \langle m, n\rangle$.

Hallaremos también conveniente tener a mano el conjunto Fr de los fraccionarios.

Definición 3. $\mathrm{Fr} = \{x$: *x es un fraccionario* $\}$.

En todos los usos de definición de la notación de abstracción en este capítulo será obvio que el conjunto definido es el intuitivamente apropiado y no el conujnto vacío. Así

* El nombre *sucesión de Cauchy* honra al gran matemático francés A. L. Cauchy [1789-1857].

que no enunciaremos ni demostraremos teoremas como:

$x \in \mathrm{Fr} \leftrightarrow x$ es un fraccionario.

Ahora definimos la relación $\simeq_f$ (el sub-índice es por "fraccionario") tal que, si $n_1 \neq 0$ y $n_2 \neq 0$, entonces

$$\frac{m_1}{n_1} \simeq_f \frac{m_2}{n_2} \leftrightarrow m_1 n_2 = m_2 n_1.$$

Definición 4.

$$\simeq_f = \left\{ \langle \frac{m_1}{n_1}, \frac{m_2}{n_2} \rangle : n_1 \neq 0 \;\&\; n_2 \neq 0 \;\& \; m_1 n_2 = m_2 n_1 \right\}.$$

Como nuestro primer teorema tenemos entonces,

Teorema 1. $\simeq_f$ *es una relación de equivalencia sobre* Fr.

Demostración. Para indicar cómo va la demostración, demostramos que $\simeq_f$ es reflexiva en Fr. Sea m/n un fraccionario; entonces, $mn = mn$, de donde, $m/n \simeq_f m/n$. Q.E.D. En todas estas demostraciones se usan, sin referencia explícita, hechos elementales acerca de operaciones y relaciones sobre los números naturales.

Teorema 2. *Si* $\frac{m}{n} \in \mathrm{Fr}$ *y* $p \neq 0$, *entonces* $\frac{m}{n} \simeq_f \frac{mp}{np}$.

Ahora definimos *menor que* para fraccionarios.

Definición 5. $<_f = \left\{ \langle \frac{m_1}{n_1}, \frac{m_2}{n_2} \rangle : n_1 \neq 0 \;\&\; n_2 \neq 0 \;\&\; m_1 n_2 < m_2 n_1 \right\}.$

Dos teoremas esperados son:

Teorema 3. $<_f$ *es una ordenación parcial estricta de* Fr.

Teorema 4. *Si* $x, y \in \mathrm{Fr}$ *entonces ocurre exactamente una de las siguientes situaciones:* $x \simeq_f y$, $x <_f y$, $y <_f x$.

Ya que $<_f$ es un conjunto, es posible una definición muy simple de *mayor que* para fraccionarios: es la conversa de menor que.

Definición 6. $>_f = \breve{<}_f$.

Los dos teoremas siguientes afirman, respectivamente, que no hay un fraccionario mayor que todos y que entre dos fraccionarios existe un tercero.

Teorema 5. *Si* $x \in \mathrm{Fr}$, *entonces existe un* $y \in \mathrm{Fr}$ *tal que* $x <_f y$.

Teorema 6. *Si* $x, y \in \mathrm{Fr}$, *y* $x <_f y$, *entonces existe un* $z \in \mathrm{Fr}$ *tal que* $x <_f z <_f y$.

El último teorema expresa una propiedad importante que las relaciones pueden o no tener en un conjunto. Si el campo de R contiene a A y para cualquier x, y en A, si $x R y$, existe un z en A tal que

$$x R z \;\&\; z R y,$$

entonces se dice que R es *densa* en A. Así, el teorema dice que $<_f$ es densa en Fr.

El siguiente teorema dice que la relación $\simeq_f$ tiene la propiedad de sustitución esperada, con respecto a menor que, para fraccionarios.

Teorema 7. *Si* $x,y,u,v \in \mathrm{Fr} \;\&\; x <_f y \;\&\; x \simeq_f u \;\&\; y \simeq_f v$, *entonces* $u <_f v$.

Ahora definimos *adición* entre fraccionarios.

Definición 7.

$$F+ = \left\{ \langle \frac{m_1}{n_1}, \frac{m_2}{n_2}, \frac{m_3}{n_3} \rangle : n_1 \neq 0 \;\&\; n_2 \neq 0 \;\&\; n_3 \neq 0 \;\&\; \frac{m_1 n_2 + n_1 m_2}{n_1 n_2} = \frac{m_3}{n_3} \right\}.$$

Para justificar la notación apropiada tenemos:

Teorema 8. *Si* $x,y \in \mathrm{Fr}$, *entonces existe un único* z *en* Fr *tal que* $\langle x, y, z \rangle \in F+$.

Definición 8. *Si* $x,y,z \in \mathrm{Fr}$, *entonces* $x + y = z \leftrightarrow \langle x, y, z \rangle \in F+$.

Nótese que, ya que la definición dada atrás del símbolo '+' para ordinales era condicional, no puede surgir confusión alguna de la omisión del sub-índice aquí. Obviamente, este no es el caso para menor que. Por un procedimiento similar habría podido omitirse el sub-índice de '$\simeq_f$'.

Tenemos la batería esperada de teoremas. El primero establece que la equivalencia de fraccionarios tiene la propiedad de sustitución con respecto a la adición entre fraccionarios. Este teorema, como el teorema 7, es decisivo para desarrollar la teoría de los números racionales en la sección siguiente.

Teorema 9. *Si $x,y,u,v \in$ Fr & $x \simeq_f u$ & $y \simeq_f v$, entonces $x + y \simeq_f u + v$.*

Teorema 10. *Si $n \neq 0$, entonces* $\frac{m_1}{n} + \frac{m_2}{n} \simeq_f \frac{m_1 + m_2}{n}$.

Teorema 11. *La adición entre fraccionarios es conmutativa y asociativa.*

Demostración. Solamente demostramos la asociatividad

$$\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) + \frac{m_3}{n_3} = \left(\frac{m_1 n_2 + n_1 m_2}{n_1 n_2}\right) + \frac{m_3}{n_3}$$

$$= \frac{(m_1 n_2 + n_1 m_2) n_3 + (n_1 n_2) m_3}{(n_1 n_2) n_3}$$

$$= \frac{m_1 n_2 n_3 + n_1 m_2 n_3 + n_1 n_2 m_3}{n_1 n_2 n_3}$$

$$= \frac{m_1 (n_2 n_3) + n_1 (m_2 n_3 + n_2 m_3)}{n_1 (n_2 n_3)}$$

$$= \frac{m_1}{n_1} + \left(\frac{m_2 n_3 + n_2 m_3}{n_2 n_3}\right)$$

$$= \frac{m_1}{n_1} + \left(\frac{m_2}{n_2} + \frac{m_3}{n_3}\right) \qquad \text{Q.E.D.}$$

Teorema 12. *La adición entre fraccionarios es monotónica respecto a la relación menor que para fraccionarios, esto es, si $x, y, z \in$ Fr y $x <_f y$, entonces*

$$x + z <_f y + z$$

y

$$z + x <_f z + y.$$

Teorema 13. *La adición entre fraccionarios tiene la propiedad de cancelación con respecto a menor que para fraccionarios, esto es, si $x, y, z \in$ Fr y*

$$x + z <_f y + z$$

o

$$z + x <_f z + y,$$

entonces

$$x <_f y.$$

Cuando decimos que una operación simplemente tiene la propiedad de cancelación, queremos decir que ello sucede con respecto a la relación de identidad. Así, una operación binaria $*$ tiene la *propiedad de cancelación* si y solamente si siempre que $x * z = y * z$ o $z * x = z * y$, entonces $x = y$. Dejamos como ejercicio el problema de determinar si la adición y la multiplicación entre fraccionarios tienen la propiedad de cancelación. (Con respecto a la identidad.)

Definimos ahora la multiplicación entre fraccionarios.

Definición 9.

$$F\cdot = \left\{\left\langle \frac{m_1}{n_1}, \frac{m_2}{n_2}, \frac{m_3}{n_3} \right\rangle : n_1 \neq 0 \ \& \ n_2 \neq 0 \ \& \ n_3 \; 0 \neq \ \& \ \frac{m_1 m_2}{n_1 n_2} = \frac{m_3}{n_3}\right\}.$$

Teorema 14. *Si $x, y \in$ Fr, entonces existe un único z en Fr tal que $\langle x,y,z\rangle \in F\cdot$.*

Definición 10. *Si $x,y,z \in$ Fr, entonces $xy = z \leftrightarrow \langle x, y, z\rangle \in F\cdot$.*

Teorema 15. *Si $x,y,u,v \in$ Fr & $x \simeq_f u$ & $y \simeq_f v$, entonces $xy \simeq_f uv$.*

Teorema 16. *La multiplicación entre fraccionarios es conmutativa y asociativa; además, es distributiva (tanto a izquierda como a derecha) con respecto a la adición entre fraccionarios.*

Teorema 17. *La multiplicación entre fraccionarios tiene la propiedad de cancelación, con respecto a menor que para fraccionarios.*

El siguiente teorema expresa esencialmente que la división entre fraccionarios, excepto por cero, es siempre posible.

Teorema 18. *Si* $x, y \in$ Fr *y* $y >_f \frac{0}{1}$, *entonces existe un* z *en* Fr *tal que* $x \simeq_f yz$.

Demostración. Sea

$$x = \frac{m_1}{n_1}$$

$$y = \frac{m_2}{n_2}.$$

Entonces tomemos

$$z = \frac{m_1 n_2}{m_2 n_1},$$

de donde

$$\begin{aligned} yz &= \left(\frac{m_2}{n_2}\right)\left(\frac{m_1 n_2}{m_2 n_1}\right) \\ &= \frac{m_2 m_1 n_2}{n_2 m_2 n_1} \\ &= \left(\frac{m_1}{n_1}\right)\left(\frac{m_2 n_2}{m_2 n_2}\right) \\ &\simeq \left(\frac{m_1}{n_1}\right)\left(\frac{1}{1}\right) \\ &\simeq \frac{m_1 \cdot 1}{n_1 \cdot 1} \\ &\simeq \frac{m_1}{n_1} \\ &\simeq x. \end{aligned}$$

Q.E.D.

Algunas propiedades obvias ulteriores de los fraccionarios se han formulado como ejercicios.

EJERCICIOS

1. Completar la demostración del teorema 1.
2. Demostrar los teoremas 2, 3 y 4.
3. Demostrar los teoremas 5, 6 y 7.
4. Demostrar el teorema 8.
5. Definir $\leq_f$ de la manera obvia.
   (a) ¿Es esta relación antisimétrica?
   (b) Demostrar que, si $x,y,u,v \in$ Fr & $x \leq_f y$ & $x \simeq_f u$ & $y \simeq_f v$, entonces $u \leq_f v$.
   (c) Demostrar que, si $x,y,z \in$ Fr & $x \leq_f y$ & $y <_f z$ entonces $x <_f y$.
6. Dar una definición condicional directa de adición entre fraccionarios sin usar como patrón la definición 7.
7. Demostrar los teoremas 9 y 10.
8. Demostrar los teoremas 11 y 12.
9. Demostrar los teoremas 13 y 14.
10. Demostrar los teoremas 15 y 16.
11. Demostrar el teorema 17.
12. ¿Tienen la adición y la multiplicación entre fraccionarios la propiedad de cancelación (con respecto a la identidad)?
13. Definir $0_f = \frac{0}{1}$, y $1_f = \frac{1}{1}$. Demostrar que, si $x,y,z,u,v \in$ Fr, entonces:
   (a) $x + 0_f = x$,
   (b) $x \cdot 0_f = 0_f$,
   (c) $x \cdot 1_f = x$,
   (d) si $xz <_f yz$ y $z >_f 0_f$ entonces $x <_f y$.
   (e) si $y <_f z$ y $x >_f 0_f$ entonces $xy <_f xz$.
14. Dar un contra-ejemplo para mostrar que el teorema 18 es falso si $\simeq$ se reemplaza por la identidad.

§ 6.3 **Números racionales no negativos.** Desarrollamos ahora la teoría de los números racionales no negativos como clases de equivalencia de fraccionarios.

Definición 11. *Si* $x \in$ Fr, *entonces*

$$[x]_r = \{y\colon y \in \mathrm{Fr}\ \&\ y \simeq_f x\}.$$

Así, $[x]_r$ es el conjunto de todos los fraccionarios equivalentes al fraccionario x. Usamos el sub-índice 'r' para indicar "racional no negativo". (Es importante darse cuenta que los varios sub-índices introducidos en este capítulo, como 'f' y 'r', no son variables.)

Definición 12. $\mathrm{Nr} = \{A\colon (\exists x)(x \in \mathrm{Fr}\ \&\ A = [x]_r\}$.

Tenemos, como resultado obvio,

Teorema 19. *El conjunto* Nr *de los racionales no negativos es una partición del conjunto* Fr *de los fraccionarios.*

Usamos las letras mayúsculas 'M', 'N', 'P', 'Q', con o sin sub-índices, para números racionales no negativos.

Definición 13. $<_r = \{\langle M, N\rangle\colon M,N \in \mathrm{Nr}\ \&\ (\exists x)(\exists y)(x \in M\ \&\ y \in N\ \&\ x <_f y)\}$.

Ahora usamos el teorema 7 para demostrar:

Teorema 20. $<_r$ *es una ordenación simple estricta de* Nr.

Demostración. Necesitamos demostrar que $<_r$ es asimétrica, transitiva y conexa en Nr.

[Asimetría]. Supongamos que $M, N \in$ Nr y $M <_r N$. Entonces existe un fraccionario x en M y un y en N tales que

(1) $$x <_f y.$$

Supongamos ahora que existe un fraccionario u en M y un v en N tales que

(2) $$v <_f u.$$

A partir del teorema 19 y de hechos familiares del capítulo 3, que tienen que ver con las particiones, sabemos que

$$M = [x]_r = [u]_r,$$

$$N = [y]_r \quad [v]_r,$$

de donde $x \simeq_f u$ y $y \simeq_f u$, así que, en virtud del teorema 7 y (1),

$$u <_f v,$$

lo que es absurdo, ya que $<_f$ es asimétrica (teorema 3). Entonces no existen fracciones en M y N que satisfacen (2) y concluimos que no es el caso de que $N <_r M$.

[Transitividad]. Supongamos: $M,N,P \in$ Nr & $M <_r N$ & $N <_r P$. Entonces existe un fraccionario x en M, y_1 en N, y_2 en N, z en P, tales que

$$x <_f y_1 \;\&\; y_2 <_f z,$$

pero

$$y_1 \simeq_f y_2,$$

de donde, por el teorema 7,

$$x <_f y_2,$$

así que, en virtud de la transitividad de $<_f$ (teorema 3),

$$x <_f z,$$

a partir de lo cual concluimos:

$$M <_r P.$$

[Conectividad]. Supongamos que $M, N \in$ Nr y que $M \neq N$. Puesto que tanto M como N son diferentes del conjunto vacío, sea x un elemento arbitrario de M y y de N. En virtud del teorema 4 tenemos:

$$x \simeq_f y,\ x <_f y,\ \text{o}\ y <_f x,$$

pero si $x \simeq_f y$, entonces $M = [x]_r = [y]_r = N$, contrario a nuestra suposición, por tanto, $x <_f y$ o $y <_f x$, lo que establece que $M <_r N$ o $N <_r M$. Q.E.D.

Esta demostración ilustra la clase típica de argumento que se usa para ir de un nivel de abstracción a otro más alto. Todo depende de dos consideraciones: $<_f$ tiene la mayor parte de las propiedades que se esperan de $<_r$ y $\simeq_f$ tiene propiedades de sustitución como la identidad.

Ahora definimos la adición de números racionales no negativos. Para demostrar que todo es como debe ser, hacemos uso decisivo del teorema 9.

Definición 14. $N{+} = \{\langle [x]_r, [y]_r, [z]_r \rangle : x,y,z \in \mathrm{Fr} \;\&\; x + y = z\}$.

Teorema 21. *Si* $M, N \in$ Nr *entonces existe un único* P *en* Nr *tal que* $\langle M,N,P \rangle \in N{+}$.

Demostración. En virtud de la definición de Nr existe un x en Fr y un y en Fr tales que

$$M = [x]_r$$

$$N = [y]_r.$$

Ya que $x + y \in \mathrm{Fr}$, sea

$$P = [x + y]_r.$$

Entonces, $\langle M,N,P \rangle \in N{+}$.

Para establecer la unicidad de P, supongamos $\langle M,N,P_1 \rangle \in N{+}$. Entonces, por la definición 14, deben existir elementos u, v, w tales que

$$M = [u]_r$$

$$N = [v]_r$$

$$P_1 = [w]_r$$

$$u + v = w.$$

Pero entonces,

$$u \simeq_f x$$

$$v \simeq_f y,$$

de donde, por el teorema 9,

$$u + v \simeq_f x + y,$$

esto es,

$$w \simeq_f x + y,$$

de lo cual concluimos:

$$P_1 = [w]_\nu = [x + y]_\nu = P,$$

como se requería. Q.E.D.

El teorema que se acaba de demostrar justifica la definición de adición entre números racionales no negativos.

Definición 15. *Si $M, N, P \in$ Nr, entonces*

$$M + N = P \leftrightarrow \langle M, N, P\rangle \in N+.$$

Teorema 22. *La adición entre números racionales no negativos es conmutativa y asociativa, tiene la propiedad de cancelación y es monotónica con respecto a la relación menor que para números racionales no negativos.*

Demostración. Solamente demostramos la conmutatividad; las partes restantes de la demostración siguen una estrategia semejante.

Existen fraccionarios x y y tales que

$$M = [x]_\nu$$

$$N = [y]_\nu,$$

de donde

$$\begin{aligned} M + N &= [x]_\nu + [y]_\nu \\ &= [x + y]_\nu \\ &= [y + x]_\nu \\ &= [y]_\nu + [x]_\nu \\ &= N + M. \end{aligned}$$

Q.E.D.

Ahora formulamos, sin demostración ni comentario, la definición análoga y los teoremas para multiplicación entre números racionales no negativos.

Definición 16. $N\cdot = \{\langle [x]_\nu, [y]_\nu, [z]_\nu\rangle : x, y, z \in \mathrm{Fr}\ \&\ xy = z\}$.

Teorema 23. *Si $M, N \in$ Nr, entonces existe un único P en Nr tal que $\langle M,N,P\rangle \in N\cdot$.*

Definición 17. *Si $M, N, P, \in$ Nr, entonces $MN = P \leftrightarrow \langle M, N, P\rangle \in N\cdot$.*

Teorema 24. *La multiplicación entre los números racionales no negativos es conmutativa y asociativa y es distributiva con respecto a la adición entre números racionales no negativos.*

Según los lineamientos del ejercicio 13 de la sección precedente, podemos definir el cero y el uno para los números racionales no negativos.

Definición 18. $0_\nu = [\frac{0}{1}]_\nu$

Definición 19. $1_\nu = [\frac{1}{1}]_\nu$.

Teorema 25. *Tenemos*:

(i) $0_\nu \neq 1_\nu$,

(ii) *Si $M \in$ Nr, entonces $M + 0_\nu = M$ y $M \cdot 1_\nu = M$,*

(iii) *Si $M, N, P \in$ Nr y $0_\nu <_\nu M$ & $N <_\nu P$, entonces $M\,N <_\nu M\,P$,*

(iv) *Si $M, N \in$ Nr y $0_\nu <_\nu N$, entonces existe un P en Nr tal que $M = N\,P$.*

Para introducir la sustracción ordinaria, debemos construir el conjunto completo de los números racionales, positivos, negativos y cero. Este es el objetivo de la sección siguiente.

EJERCICIOS

1. Demostrar el teorema 19.
2. Completar la demostración del teorema 22.
3. Demostrar que, si $M, N \in$ Nr y $M, <_\nu N$, entonces existe un único P en Nr tal que

$$M + P = N.$$

4. Demostrar el teorema 23.
5. Demostrar el teorema 24.
6. Demostrar el teorema 25.
7. Demostrar que, si $M, N \in$ Nr y $0_\nu <_\nu M$, entonces existe un entero n tal que

$$N <_\nu \left[\frac{n}{1}\right]_\nu \cdot M.$$

(Este resultado establece que los números racionales no negativos tienen la que se conoce como propiedad arquimediana.)

§ 6.4 **Números racionales.** Antes de que podamos definir el conjunto completo de los números racionales, necesitamos entidades que estén, con respecto a los números racionales, en la situación en que los fraccionarios están respecto de los números racionales no negativos. Una pareja ordenada $\langle M, N\rangle$ de números racionales no negativos se interpreta intuitivamente como $M - N$. Los desarrollos formales son muy similares a los que han precedido, así que el tratamiento será más bien resumido. Con la sustracción en mente, designamos el conjunto de parejas de números racionales no negativos, con 'Sb'.

Definición 20. $\mathrm{Sb}=\{\langle M, N\rangle : M,N \in \mathrm{Nr}\}$.

Definición 21. $\simeq_\sigma = \{\langle\langle M_1,N_1\rangle, \langle M_2,N_2\rangle\rangle : M_1,N_1,M_2,N_2 \in \mathrm{Nr} \,\&\, M_1+N_2=M_2+N_1\}$.

Teorema 26. $\simeq_\sigma$ *es una relación de equivalencia sobre* Sb.

Definición 22. $<_\sigma = \{\langle\langle M_1,N_1\rangle,\langle M_2,N_2\rangle\rangle : M_1, N_1,M_2,N_2 \in \mathrm{Nr} \,\&\, M_1+N_2 <_\nu M_2+N_1\}$.

Omitimos los teoremas obvios sobre $<_\sigma$.

Definición 23.
$S+ = \{\langle\langle M_1,N_1\rangle, \langle M_2,N_2\rangle, \langle M_3,N_3\rangle\rangle : M_1,N_1,M_2,N_2,M_3,N_3 \in \mathrm{Nr} \,\&\, \langle M_1 + M_2, N_1 + N_2\rangle = \langle M_3,N_3\rangle\}$.

Teorema 27. *Si* $M, N \in \mathrm{Sb}$, *entonces existe un único* P *en* Sb *tal que* $\langle M, N, P\rangle \in S+$.

Definición 24. *Si* $M, N, P \in \mathrm{Sb}$, *entonces* $M + N = P \leftrightarrow \langle M, N, P\rangle \in S+$.

Definición 25.
$S\cdot = \{\langle\langle M_1,N_1\rangle, \langle M_2,N_2\rangle, \langle M_3,N_3\rangle\rangle : M_1, N_1,M_2,N_2, M_3,N_3 \in \mathrm{Nr} \,\&\, \langle M_1M_2+ N_1N_2, M_1N_2 + N_1M_2\rangle = \langle M_3,N_3\rangle\}$.

La idea simple e intuitiva de esta definición más bien compleja es la de que

$$(M_1 - N_1)(M_2 - N_2) = M_3 - N_3 \leftrightarrow M_1M_2 - M_1N_2 - N_1M_2 + N_1N_2 = M_3 - N_3.$$

Teorema 28. *Si* $M,N \in \mathrm{Sb}$, *entonces existe un único* P *en* Sb *tal que* $\langle M,N,P\rangle \in S\cdot$.

Definición 26. *Si* $M,N,P \in \mathrm{Sb}$, *entonces* $MN = P \leftrightarrow \langle M, N, P\rangle \in S\cdot$.

Teorema 29. *Si* $M_1,M_2,N_1,N_2 \in \mathrm{Sb} \,\&\, M_1 \simeq_\sigma M_2 \,\&\, N_1 \simeq_\sigma N_2$, *entonces:*

(i) *Si* $M_1 <_\sigma N_1$, *entonces* $M_2 <_\sigma N_2$,

(ii) $M_1 + N_1 \simeq_\sigma M_2 + N_2$,

(iii) $M_1N_1 \simeq_\sigma M_2N_2$.

En resumen, este teorema establece que la relación de equivalencia definida para Sb tiene las propiedades de sustitución apropiadas. En lugar de formular propiedades de las operaciones sobre parejas ordenadas de números racionales no negativos, continuamos definiendo clases de equivalencia de estas parejas y así obtenemos los números racionales. Siguiendo a Whitehead y Russell, usamos el sub-índice '$_s$' para operaciones y relaciones entre números racionales, reservando '$_r$' para los números reales. También para los propósitos del trabajo ulterior usamos informalmente las variables generales 'x', 'y', 'z', 'u', 'v', con o sin sub-índices, para números racionales. La referencia explícita al conjunto Ra de los racionales evitará cualquier ambigüedad.

Definición 27. *Si* $M \in \mathrm{Sb}$, *entonces* $[M]_s = \{N : N \in \mathrm{Sb} \,\&\, N \simeq_\sigma M\}$.

Definición 28. $\mathrm{Ra} = \{x : (\exists M)(M \in \mathrm{Sb} \,\&\, x = [M]_s)\}$.

Antes de formular un teorema amplio sobre los números racionales necesitamos definir *menor que, adición* y *multiplicación.*

Definición 29. $<_s = \{\langle [M]_s, [N]_s\rangle : M,N \in \mathrm{Sb} \,\&\, M <_\sigma N\}$.

Definición 30. $R+ = \{\langle [M]_s, [N]_s, [P]_s\rangle : M,N,P \in \mathrm{Sb} \,\&\, M + N = P\}$.

Teorema 30. *Si* x y y *son números racionales* (p. ej., $x,y \in \mathrm{Ra}$), *entonces existe un único racional* z *tal que* $\langle x, y, z\rangle \in R+$.

Definición 31. *Si* x, y y z *son números racionales, entonces*

$$x + y = z \leftrightarrow \langle x, y, z\rangle \in R+.$$

Definición 32. $R\cdot = \{\langle [M]_s, [N]_s, [P]_s\rangle : M, N, P \in \mathrm{Sb} \,\&\, MN = P\}$.

Teorema 31. *Si x y y son números racionales, entonces existe un único número racional z tal que $\langle x, y, z\rangle \in R$.*

Definición 33. *Si x, y y z son números racionales entonces*

$$xy = z \leftrightarrow \langle x, y, z\rangle \in R\cdot.$$

Definimos también el cero y el uno.

Definición 34.

$$0_s = [\langle 0_\nu, 0_\nu\rangle]_s$$

$$1_s = [\langle 1_\nu, 0_\nu\rangle]_s$$

Teorema 32. *La relación menor que y las operaciones de adición y multiplicación para números racionales junto con 0_s y 1_s tienen las quince propiedades siguientes para todos los números racionales x, y, y z:*

(1) $x + y = y + x$,
(2) $xy = yx$,
(3) $(x + y) + z = x + (y + z)$,
(4) $(xy)z = x(yz)$,
(5) $x(y + z) = xy + xz$,
(6) $x + 0 = x$,
(7) $x \cdot 1 = x$,
(8) *Existe un número racional y tal que $x + y = 0$,*
(9) *Si $y \neq 0$, entonces existe un número racional z tal que $x = yz$,*
(10) *Si $x <_s y$, entonces no $y <_s x$,*
(11) *Si $x <_s y$ y $y <_s z$, entonces $x <_s z$,*
(12) *Si $x \neq y$, entonces $x <_s y$ o $y <_s x$,*
(13) *Si $y <_s z$, entonces $x + y <_s x + z$,*
(14) *Si $0 <_s x$ y $y <_s z$, entonces $xy <_s xz$,*
(15) $0_s \neq 1_s$.

La demostración de las quince partes del teorema se dejan como ejercicio. A partir de este punto supoñemos todos los resultados aritméticos familiares, acerca de los números racionales, sin desarrollo explícito adicional.*

Suponiendo definido el negativo de un número racional y $\leq_s$, es deseable también, por su importancia para la siguiente sección, definir el valor absoluto de un número racional y resumir las propiedades de esta operación.

Definición 35. *Si x es un número racional, entonces*

$$|x| = y \leftrightarrow (x \geq_s 0 \rightarrow y = x) \,\&\, (x <_s 0 \rightarrow y = -x).$$

En la notación matemática usual escribiríamos:

$$|x| = \begin{cases} x \text{ si } x \geq 0, \\ -x \text{ si } x < 0. \end{cases} \qquad \text{Q.E.D.}$$

Teorema 33. *Si x y y son números racionales, entonces:*

(i) $|x| \geq 0$
(ii) $|xy| = |x| \cdot |y|$
(iii) $|x + y| \leq |x| + |y|$
(iv) $|x| - |y| \leq |x - y|$
(v) $x \cdot |y| \leq |xy|$.

Para indicar cuántos niveles de abstracción hemos recorrido, definimos los números racionales correspondientes a los números naturales.

Definición 36. $n_s = \left[\left\langle \left[\frac{n}{1}\right]_\nu, \left[\frac{0}{1}\right]_\nu \right\rangle\right]_s$

Los hechos expresados en el teorema final de esta sección son tanto intrínsecamente interesantes como útiles más adelante. La demostración usa el método diagonal de Cauchy para reordenar una sucesión doblemente infinita en una simplemente infinita. (Compárese la demostración de § 5.3 en la que $\omega \times \omega \approx \omega$.)

Teorema 34. *El conjunto de los números racionales es enumerable y puede ser bien ordenado sin usar el axioma de escogencia.*

* Los desarrollos deductivos de las quince propiedades del teorema 33 se encuentran en mi *Introduction to Logic.*

Demostración. Será obvio que la ordenación construida establece ambas partes de la demostración. Se omiten los detalles. Representamos todo número racional por un fraccionario m/n tal que m y n no tienen factor común mayor de 1. Así el número racional un medio se representa con $\frac{1}{2}$, no con $\frac{2}{4}$ ó $\frac{3}{6}$. El negativo un medio, con $-\frac{1}{2}$, cero, con $\frac{0}{1}$, etc. (La traducción de estas nociones intuitivas en las construcciones con clases de equivalencia usadas para obtener los números racionales es cuestión de rutina.) Ordenamos los fraccionarios, primero de acuerdo con la suma de m y n. Si $m + n = m' + n'$, m/n precede a m'/n', cuando $m<m'$. Finalmente, los fraccionarios negativos preceden inmediatamente a sus contrapartes positivos. La ordenación es entonces:

$$\frac{0}{1}, -\frac{1}{1}, \frac{1}{1}, -\frac{1}{2}, \frac{1}{2}, -\frac{2}{1}, \frac{2}{1}, -\frac{1}{3}, \frac{1}{3}, -\frac{3}{1}, \frac{3}{1}, -\frac{1}{4}, \frac{1}{4}, -\frac{2}{3}, \frac{2}{3}, \cdots$$

Q.E.D.

Para evitar el uso continuo de sub-índices en las secciones subsiguientes no distinguiremos entre n_s y n y el contexto será claro cuando la entidad es apropiada. Puede considerarse una definición útil, que se refiere tanto a n como a n_s. Esta es la definición del menor entero igual o mayor que un número racional positivo.

Definición 37. *Si x es un número racional positivo, entonces*

$$[x] = n \leftrightarrow x \leq n_s \;\&\; (\forall m)(x \leq m_s \rightarrow n_s \leq m_s).$$

Que en la notación intuitiva usual es:*

$$\left[\frac{1}{2}\right] = 1$$

$$[2] = 2$$

$$\left[1\frac{1}{7}\right] = 2.$$

* Este uso adicional de los paréntesis rectangulares no debe dar lugar a confusión, puesto que no se usa aquí sub-índice alguno. Es realmente más común definir $[x]$ como el mayor entero $\leq x$. La presente notación es muy conveniente para nuestros propósitos.

EJERCICIOS

1. Demostrar el teorema 26.
2. Demostrar los teoremas 27 y 28.
3. Demostrar el teorema 29.
4. Demostrar los teoremas 30 y 31.
5. Demostrar el teorema 32. (Este ejercicio tiene quince partes.)
6. Demostrar el teorema 33.
7. Dar una demostración detallada del teorema 34.
8. Demostrar que, si x y y son números racionales positivos, entonces:
   (i) $[x + y] \leq [x] + [y]$,
   (ii) $[xy] \leq [x]\,[y]$.

§ 6.5 Sucesiones de Cauchy de números racionales. Ahora desarrollamos los hechos fundamentales acerca de sucesiones de Cauchy de números racionales sobre la base de las cuales construimos los números reales en la sección siguiente. La notación de sub-índice '$_s$' se ha eliminado en esta sección y en lo que resta del capítulo.

Definición 38. *x es una sucesión si y solamente si x es una función sobre el conjunto ω de los números naturales.*

Introducimos la notación usual de sub-índices para los *elementos* de una sucesión.

Definición 39. †*Si x es una sucesión,* $x_n = x(n)$.

En la terminología usual, x_n es el *n-simo elemento* o *término* de la sucesión x.

Violando ligeramente nuestras reglas usuales de definición, introducimos también una notación que se acostumbra para sucesiones.

Definición 40. *Si x es una sucesión,* $\langle x_1, x_2, \ldots, x_n, \ldots \rangle = x$.

Las sucesiones en las cuales estamos particularmente interesados son:

Definición 41. *x es una sucesión de números racionales si y solamente si x es una sucesión y el recorrido de x es un subconjunto del conjunto de los números racionales.*

† Esta definición esencialmente duplica la definición 15 de §5.2.

Las operaciones sobre sucesiones de números racionales se definen de la manera esperada. La línea de razonamiento que justifica las definiciones es también obvia para requerir teoremas separados.

Definición 42. *Si* x y y *son sucesiones de números racionales entonces,*

$$x + y = z \leftrightarrow (\forall n)(x_n + y_n = z_n).$$

Definición 43. *Si* x y y *son sucesiones de números racionales, entonces*

$$xy = z \leftrightarrow (\forall n)(x_n y_n = z_n).$$

Claramente, si x y y son sucesiones de números racionales, entonces también lo son $x + y$ y xy.

Las demostraciones de las propiedades esperadas de estas operaciones de adición y multiplicación se siguen fácilmente a partir de las propiedades de las operaciones correspondientes para los números racionales.

Teorema 35. *La adición entre sucesiones de números racionales es conmutativa y asociativa y tiene la propiedad de cancelación.*

Demostración. Solamente demostramos la cancelación a derecha. Sean x,y y z sucesiones de números racionales.

$$\begin{aligned} x + z = y + z &\leftrightarrow (\forall n)(x_n + z_n = y_n + z_n) \\ &\leftrightarrow (\forall n)(x_n = y_n) \\ &\leftrightarrow x = y. \end{aligned}$$

Q.E.D.

Teorema 36. *La multiplicación entre sucesiones de números racionales es conmutativa, asociativa y distributiva con respecto a la adición.*

Las sucesiones de números racionales esenciales para la construcción de los números reales son las sucesiones de Cauchy que se van a definir ahora.

Definición 44. *x es una sucesión de Cauchy de números racionales si y solamente si x es una sucesión de números racionales y para todo número racional $\varepsilon > 0$ existe un entero positivo N tal que para todos los $m,n > N$*

$$|x_n - x_m| < \epsilon.*$$

Como se puntualizó en la introducción de este capítulo, las sucesiones de Cauchy se llaman también *sucesiones convergentes, sucesiones regulares* y *sucesiones fundamentales.*

No están de más algunos ejemplos de sucesiones de Cauchy en vista de la importancia fundamental de la noción. Sea x la sucesión de números racionales tal que $x_0 = 0$ y para $n \geq 1$

$$x_n = \frac{1}{n}$$

Para demostrar que x es una sucesión de Cauchy necesitamos hallar, para cada número racional positivo ϵ, un entero N tal que para $m, n > N$

$$|x_n - x_m| < \epsilon.$$

Aquí es fácil hallar el N apropiado. Sea

$$N = \left[\frac{1}{\epsilon}\right].$$

Entonces las desigualdades siguientes para $m,n > [\frac{1}{\epsilon}]$ establecen que x es una sucesión de Cauchy:

$$\begin{aligned} \left|\frac{1}{n} - \frac{1}{m}\right| &\leq \frac{1}{n} \\ &< \frac{1}{\left[\frac{1}{\epsilon}\right]} \\ &< \frac{1}{\frac{1}{\epsilon}} \\ &< \epsilon. \end{aligned}$$

Como un segundo ejemplo, sea x la sucesión tal que para $n > 0$

$$x_n = \frac{n^2 - 1}{n^2}.$$

* Usamos 'ε' en deferencia a la notación tradicional, aún cuando viola nuestra convención anterior, según la cual, las letras griegas minúsculas son variables que toman como valores a números ordinales. Por una razón semejante usamos frecuentemente "entero positivo" o simplemente "entero" en lugar de "número natural".

Aquí la escogencia natural de N es $\left[\frac{1}{\sqrt{\epsilon}}\right]$, pero $\sqrt{\varepsilon}$ no es en general un número racional. Dejamos como ejercicio una escogencia apropiada de número racional.

Ahora queremos demostrar el hecho importante de que la suma y el producto de dos sucesiones de Cauchy es también una sucesión de Cauchy. La demostración concerniente al producto de dos de tales sucesiones hace uso del siguiente hecho.

Teorema 37. *Si x es una sucesión de Cauchy de números racionales, entonces existe un número racional positivo δ tal que, para todo n,*

$$|x_n| < \delta.$$

Demostración. En virtud del hecho de que x es una sucesión de Cauchy existe un entero N tal que para todos los $m, n > N$

$$(1) \qquad |x_n - x_m| < 1.$$

Sea

$$(2)\ \delta = \max(|x_0|, |x_1|, \dots, |x_N|, |x_{N+1}|) + 1.$$

Obviamente, para $n \leq N + 1$,

$$|x_n| < \delta.$$

Supongamos entonces que $n > N + 1$. En virtud de (1),

$$|x_n| < |x_{N+1}| + 1,$$

pero en vista de (2)

$$|x_{N+1}| + 1 \leq \delta.$$

Q.E.D.

Teorema 38. *Si x y y son sucesiones de Cauchy de números racionales, entonces $x + y$, xy son también sucesiones de Cauchy de números racionales.*

Demostración. [Suma]. Sea $\varepsilon > 0$. Por hipótesis existen números M y N tales, que si $m,n > M$, entonces

$$\left|x_n - x_m\right| < \frac{\epsilon}{2},$$

y si $m,n > N$,

$$\left|y_n - y_m\right| < \frac{\epsilon}{2}.$$

Sea

$$P = \max(M,N).$$

Si $m,n > P$, entonces

$$\begin{aligned} |(x_n + y_n) - (x_m + y_m)| &= |(x_n - x_m) + (y_n - y_m)| \\ &\leq |x_n - x_m| + |y_n - y_m| \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} \\ &< \epsilon. \end{aligned}$$

[Producto]. Sea $\varepsilon > 0$. En virtud del teorema precedente existen números racionales positivos δ_1 y δ_2 tales que, para todo n,

$$|x_n| < \delta_1$$

$$|y_n| < \delta_2.$$

Sea $\delta = \max(\delta_1, \delta_2)$. Además, puesto que x y y son sucesiones de Cauchy, existe un entero M_1 tal que para $m,n > M_1$

$$|x_n - x_m| < \epsilon/(2\delta),$$

y existe un entero M_2 tal que para $m,n > M_2$

$$|y_n - y_m| < \epsilon/(2\delta).$$

Sea $M = \max(M_1, M_2)$. Entonces, para $m,n > M$,

$$\begin{aligned} |x_n y_n - x_m y_m| &= |x_n y_n - x_n y_m + x_n y_m - x_m y_m| \\ &\leq |x_n|\,|y_n - y_m| + |y_m|\,|x_n - x_m| \\ &< \delta\left(\frac{\epsilon}{2\delta}\right) + \delta\left(\frac{\epsilon}{2\delta}\right) \\ &< \epsilon. \end{aligned}$$

Q.E.D.

En nuestro desarrollo los números reales son ciertas clases de equivalencia de sucesiones de Cauchy de números reales; ahora definimos la relación de equivalencia apropiada.

Definición 45. *Si x y y son sucesiones de Cauchy de números racionales, entonces $x \simeq_c y$, si y solamente si, para todo número racional positivo ε, existe un entero N tal que, para todo $n > N$*

$$|x_n - y_n| < \epsilon.$$

Nótese que dos sucesiones de Cauchy pueden ser equivalentes aun si difieren en todos los términos. Por ejemplo, si para $n > 0$

$$x_n = \frac{n^2 - 1}{n^2},$$

$$y_n = \frac{n^2 + 1}{n^2}.$$

Entonces, para todo $n>0, x_n \neq y_n$, pero $x \simeq_c y$.

Ya que no hemos definido la relación $\simeq_c$ como una entidad de la teoría de conjuntos, debe estudiarse el teorema apropiado que se refiere a sus propiedades como relación de equivalencia. La demostración se deja como ejercicio.

Teorema 39. *Si x, y y z son sucesiones de Cauchy de números racionales, entonces:*

(i) $x \simeq_c x$,

(ii) *si* $x \simeq_c y$, *entonces* $y \simeq_c x$,

(iii) *si* $x \simeq_c y$ y $y \simeq_c z$, *entonces* $x \simeq_c z$.

La relación *menor que* para sucesiones de Cauchy es análoga a la equivalencia.

Definición 46. *Si x y y son sucesiones de Cauchy de números racionales, entonces: $x <_c y$ si y solamente si existe un número racional $\delta > 0$ y un entero N tal que para $n > N$*

$$y_n > x_n + \delta.$$

Son válidas las propiedades esperadas.

Teorema 40. *Si x y y son sucesiones de Cauchy de números racionales, entonces es válida exactamente una de las siguientes situaciones:*

$$x \simeq_c y,\ x <_c y,\ y <_c x.$$

Demostración. Es obvio, a partir de las definiciones dadas, que a lo más una de las relaciones puede ser válida. Así que necesitamos demostrar que por lo menos una es válida.

Supongamos que x no es equivalente a y. Se sigue inmediatamente de la definición 45 que existe un número racional positivo 2ε tal que, para todo entero N, existe un $n > N$ tal que

(1) $$|x_n - y_n| > 2\epsilon.$$

Pero ya que x y y son sucesiones de Cauchy, existe un entero M_1 tal que, si $m, n > M_1$, entonces

$$\left|x_n - x_m\right| < \frac{\epsilon}{2},$$

y existe un entero M_2 tal que, si $m,n > M_2$, entonces

$$\left|y_n - y_m\right| < \frac{\epsilon}{2}$$

Usando el resultado que lleva a (1), existe un entero p tal que

$$p > \max(M_1, M_2)$$

y

(2) $$|x_p - y_p| > 2\epsilon.$$

Tenemos ahora dos posibilidades: $x_p > y_p$ o $y_p > x_p$.

Supongamos que $x_p > y_p$. Entonces, en virtud de (2),

(3) $$x_p > y_p + 2\epsilon.$$

Además, para todo $n > p$

(4) $$\left|x_p - x_n\right| < \frac{\epsilon}{2}$$

(5) $$\left|y_p - y_n\right| < \frac{\epsilon}{2},$$

de donde, a partir de (3) y (4),

(6) $$x_n > x_p - \frac{\epsilon}{2} > y_p + 2\epsilon - \frac{\epsilon}{2} = y_p + \frac{3\epsilon}{2}.$$

Pero se sigue a partir de (5) que

(7) $$y_p > y_n - \frac{\epsilon}{2},$$

e inferimos a partir de (6) y (7) que, para todo $n > p$,

$$x_n > y_n - \frac{\epsilon}{2} + \frac{3\epsilon}{2} = y_n + \epsilon.$$

Así que sobre nuestra suposición, $y <_c x$.

Si $y_p > x_p$, inferimos con el mismo tipo de razonamiento que $x <_c y$. Q.E.D.

La demostración de que *menor que* es asimétrica y transitiva para sucesiones de Cauchy se deja como ejercicio.

Teorema 41. *Si x, y y z son sucesiones de Cauchy de números racionales, entonces:*

(i) *Si $x <_c y$, entonces no $y <_c x$,*

(ii) *Si $x <_c y$ y $y <_c z$, entonces $x <_c z$.*

El teorema final de esta sección establece que la relación de equivalencia definida para sucesiones de Cauchy tiene las propiedades de sustitución adecuadas.

Teorema 42. *Si x, y, u, v son sucesiones de Cauchy de números racionales y $x \simeq_c u$ y $y \simeq_c v$, entonces:*

(i) *Si $x <_c y$, entonces $u <_c v$,*

(ii) $x + y \simeq_c u + v$,

(iii) $xy \simeq_c uv$.

Demostración. Demostramos solamente (iii). Sea $\varepsilon > 0$. Por el teorema 37 existen números racionales positivos δ_1, δ_2, δ_3, δ_4 tales que para todo n

$$|x_n| < \delta_1$$
$$|y_n| < \delta_2$$
$$|u_n| < \delta_3$$
$$|v_n| < \delta_4.$$

Sea $\delta = \max(\delta_1, \delta_2, \delta_3, \delta_4)$. Por la hipótesis de equivalencia existe un entero N tal que para $n > N_1$

$$|x_n - u_n| < \epsilon/2\delta,$$

y existe un entero N_2 tal que para $n > N_2$

$$|y_n - v_n| < \epsilon/2\delta.$$

Sea $N = \max(N_1, N_2)$. Entonces para todo $n > N$, tenemos:

$$\begin{aligned} |x_n y_n - u_n v_n| &= |x_n y_n - u_n y_n + u_n y_n - u_n v_n| \\ &\leq |y_n|\,|x_n - u_n| + |u_n|\,|y_n - v_n| \\ &< \delta(\epsilon/2\delta) + \delta(\epsilon/2\delta) \\ &< \epsilon. \end{aligned}$$

Q.E.D.

Nótese cuán similar es esta demostración a la demostración de que el producto de dos sucesiones de Cauchy es una sucesión de Cauchy.

EJERCICIOS

1. Demostrar que el conjunto de todas las sucesiones de números racionales existe.
2. Sea x la sucesión tal que

$$x_0 = 0$$
$$x_n = \frac{n^2 - 1}{n^2} \quad \text{para } n > 0.$$

Demostrar que x es una sucesión de Cauchy.

3. Sea x la sucesión tal que

$$x_n = \frac{2^n}{n!}$$

Demostrar que x es una sucesión de Cauchy.

4. Completar la demostración del teorema 35.
5. Demostrar el teorema 36.
6. Demostrar el teorema 39.
7. Demostrar el teorema 41.
8. Completar la demostración del teorema 42.
9. Primero definimos: x es una *sucesión monótona creciente de enteros* si y solamente si (i) x es una sucesión, (ii) el recorrido de x es un subconjunto de ω, (iii) si $m < n$, entonces $x_m < x_n$. Enseguida definimos: x es una *sub-sucesión* de y si y solamente si y es una sucesión y existe una sucesión monótona creciente de enteros z tal que $x = y \circ z$. (Esto proporciona una definición precisa de la idea intuitivamente familiar de sub-sucesión. El símbolo $\circ$ designa composición entre funciones.)

(a) Dar un ejemplo de una sucesión de números racionales que no sea una sucesión de Cauchy, pero que tenga una sub-sucesión que lo sea.

(b) Dar un ejemplo de una sucesión de números racionales que no tenga sub-sucesión alguna que sea una sucesión de Cauchy.

(c) Demostrar que toda sub-sucesión de una sucesión de Cauchy de números racionales es también una sucesión de Cauchy de números racionales.

(d) Demostrar que, si y es una sucesión de Cauchy de números racionales y x es una sub-sucesión de y, entonces $x \simeq_c y$.

§ 6.6 **Números Reales.** Comenzamos por definir clases de equivalencia de sucesiones de Cauchy de números racionales.

Definición 47. *Si x es una sucesión de Cauchy de números racionales, entonces $[x]_r = \{y: y$ es una sucesión de Cauchy de números racionales & $y \simeq_c x\}$.*

Y definimos entonces el conjunto Re de los números reales.

Definición 48. Re $= \{y\colon (\exists x)(x$ *es una sucesión de Cauchy de números racionales* & $y = [x]_r)\}$.

Tenemos el teorema obvio:

Teorema 43. *El conjunto de los números reales es una partición del conjunto de sucesiones de Cauchy de números racionales.*

Definimos enseguida menor que, adición y multiplicación.

Definición 49. $<_r = \{\langle [x]_r, [y]_r\rangle : x, y$ *son sucesiones de Cauchy de números racionales* & $x <_c y\}$.

Definición 50. $R+ = \{\langle [x]_r, [y]_r, [z]_r\rangle\colon x, y, z$ *son sucesiones de Cauchy de números racionales* & $x + y = z\}$.

Teorema 44. *Si* x y y *son números reales, entonces existe un único número real* z *tal que* $\langle x, y, z\rangle \in R+$.

Definición 51. *Si* $x, y, z \in$ Re, *entonces* $x + y = z \leftrightarrow \langle x, y, z\rangle \in R+$.

Definición 52. $R\cdot = \{\langle [x]_r, [y]_r, [z]_r\rangle\colon x,y,z$ *son sucesiones de Cauchy de números racionales* & $xy = z\}$.

Teorema 45. *Si* x y y *son números reales, entonces existe un único número real* z *tal que* $\langle x, y, z\rangle \in R$.

Definición 53. *Si* $x,y,z, \in$ Re, *entonces* $xy = z \leftrightarrow \langle x, y, z\rangle \in R$.

También definimos los números reales cero y uno.

Definición 54. $0_r = [\langle 0_s, 0_s, \ldots, 0_s, \ldots\rangle]_r$.

Definición 55. $1_r = [\langle 1_s, 1_s, \ldots, 1_s, \ldots\rangle]_r$.

Nuestro teorema amplio sobre propiedades elementales de los números reales es como el teorema 32 para los números racionales. Ya que todas las partes de la demostración se parecen mucho a las demostraciones de los teoremas precedentes, no se demuestra nada aquí.

Teorema 46. *La relación menor que y las operaciones de adición y multiplicación para números reales junto con* 0_r *y* 1_r *tienen todas las quince propiedades enunciadas en el teorema* 32.

Para completar la construcción de los números reales necesitamos solamente demostrar que ellos satisfacen una propiedad ulterior: todo conjunto no vacío de números reales que tiene una cota superior tiene una mínima cota superior.* Sin embargo, la demostración de que esta propiedad se satisface requiere algunos otros resultados que son importantes y de interés intrínseco. Comenzamos con la noción de número real *correspondiente a* un número racional.

Definición 56. *Si* x *es un número real y* s *es un número racional, entonces* x *corresponde a* s, *si y solamente si la sucesión* $\langle s, s, \ldots, s, \ldots\rangle$ *es un elemento de* x.

Tenemos, como consecuencia inmediata del hecho que el conjunto de los números reales es una partición del conjunto de sucesiones de Cauchy de números racionales, el resultado:

Teorema 47. *Dado cualquier número racional existe un único número real correspondiente a él.*

Combinando este teorema con el teorema 34 obtenemos:

Teorema 48. *El conjunto de números reales correspondientes a números racionales es enumerable y puede ser bien ordenado sin usar el axioma de escogencia.*

En el teorema siguiente se formula una propiedad útil de los números reales correspondientes a números racionales: brevemente, los números reales racionales, como pue-

* Es bien conocido que esta propiedad y las quince del teorema 32 caracterizan adecuadamente a los números reales; en casi cualquier libro de teoría de funciones de variable real se encuentra una discusión de estos asuntos.

den llamarse apropiadamente, son densos en el conjunto de todos los números reales.*

Teorema 49. *Si x y y son dos números reales distintos cualesquiera, entonces existe un número real z correspondiente a algún número racional, tal que z está entre x y y, esto es, si $x < y$, entonces $x < z$ & $z < y$; si $y < x$, entonces $y < z$ & $z < x$.*

Demostración. Para precisar, sea $x < y$. Sea $a \in x$ y $b \in y$, de donde a y b son sucesiones de Cauchy de números racionales con

(1) $$a < b.$$

A partir de (1), la definición 46 y la definición 42, inferimos que existe un número racional positivo δ y un entero N tal que para todos los $m,n > N$

(2) $$b_n - a_n > \delta$$

(3) $$|a_n - a_m| < \delta/4$$

(4) $$|b_n - b_m| < \delta/4.$$

Sea s un número racional tal que

(5) $$\delta/4 < s < \delta/2,$$

y considérese el número racional $a_{N+1} + s$. Afirmo que el número real z correspondiente a $a_{N+1} + s$ está entre x y y. (Aquí $z = [\langle a_{N+1} + s, a_{N+1} + s, \ldots, a_{N+1} + s, \ldots\rangle]_r$.)

Primero, inferimos, a partir de (3), que

$$a_n - a_{N+1} < \delta/4,$$

de donde, multiplicando por -1 y sumando s a ambos lados, obtenemos:

$$(a_{N+1} + s) - a_n > s - \delta/4,$$

de lo cual concluimos, por la definición 46, que

$$\langle a_{N+1} + s, a_{N+1} + s, \ldots, a_{N+1} + s, \ldots\rangle > a,$$

y por esto, a partir de la definición 49,

$$z > x.$$

* En lo que resta de este capítulo omitimos el sub-índice 'r' en '$<_r$' y en cualquier otra parte.

En forma similar, a partir de (2) y (4) inferimos

$$b_m - (a_{N+1} + s) = (b_{N+1} - a_{N+1}) + (b_m - b_{N+1}) - s > \delta - \delta/4 - s.$$

En virtud de (5) sabemos que $\delta - \delta/4 - s$ es positivo y concluimos que $y >_r z$. Q.E.D.

Definimos las sucesiones de Cauchy de números reales del mismo modo qué definimos tales sucesiones de números racionales.

Definición 57. *x es una sucesión de números reales si y solamente si x es una sucesión y el recorrido de x es un subconjunto del conjunto de los números reales.*

Definición 58. *x es una sucesión de Cauchy de números reales si y solamente si x es una sucesión de números reales y, para todo número real $\varepsilon > 0$, existe un entero positivo N tal que, para todos los $m,n > N$,*

$$|x_n - x_m| < \epsilon.$$

La demostración del primer teorema acerca de sucesiones de Cauchy de números reales no es difícil y la dejamos como ejercicio.

Teorema 50. *Si a es una sucesión de Cauchy de números racionales y si x es la sucesión de números reales tal que, para todo n, x_n es el número real correspondiente a a_n, entonces x es una sucesión de Cauchy de números reales. Recíprocamente, si x es una sucesión de Cauchy, entonces lo es a.*

Ahora definimos la importante noción de límite. Sin duda esta noción constituye *el* concepto fundamental del cálculo diferencial e integral y del análisis en general. Lo que queremos mostrar es que una sucesión de números reales tiene un límite si y solamente si es una sucesión de Cauchy. Este resultado se llama a veces el Principio General de Convergencia. En terminología más reciente debería llamarse el teorema sobre la completez del sistema de los números reales. Independientè de la terminología, el hecho importante es el de que este resultado, como la propiedad de la mínima cota superior, expresa la diferencia esencial entre los números reales y los números racionales. Es fácil construir ejemplos de sucesiones de Cauchy de números racionales que no tienen límite. Por ejemplo, sea $x_0 = 0$ y para $n \geq 1$

$$x_n = \left(1 + \frac{1}{n}\right)^n.$$

Es fácil ver que x es una sucesión de Cauchy de números racionales, aunque no tenga límite entre los números racionales. (Su límite es, en efecto, la base e para los logaritmos naturales: $e = 2{,}71828\ldots$)

Definición 59. *Si x es una sucesión de números reales, entonces y es un límite de x si y solamente si y es un número real y, para todo número real $\varepsilon > 0$, existe un entero positivo N tal que, para todo $n > N$,*

$$|x_n - y| < \epsilon.$$

La demostración del teorema siguiente es inmediata.

Teorema 51. *Una sucesión de números reales tiene a lo más un límite.*

Este teorema justifica la definición de la notación usual para el límite de una sucesión.

Definición 60. *Si x es una sucesión de números reales y si y es el límite de x, entonces*

$$\lim_{n \to \infty} x_n = y.$$

Teorema 52. *Una sucesión de números reales tiene un límite si y solamente si es una sucesión de Cauchy.*

Demostración. [Necesidad]. Sea x una sucesión de números reales cuyo límite es y. Sea ε cualquier número real positivo. Entonces, por la definición 59, existe un entero N tal que para $m,n > N$

$$|y - x_n| < \epsilon/2$$

$$|y - x_m| < \epsilon/2,$$

de donde

$$|x_n - x_m| \leq |y - x_n| + |y - x_m| < \epsilon/2 + \epsilon/2 = \epsilon,$$

y concluimos, a partir de la definición 58, que x es una sucesión de Cauchy de números reales.

[Suficiencia]. Sea x una sucesión de Cauchy de números reales. Sea W la buena ordenación de los números reales racionales, correspondiente a la descrita para los números racionales en la demostración del teorema 34. Sea y_n el W-primer número real racional entre x_n y $x_n + \frac{1}{n}$, esto es,

$$x_n < y_n < x_n + \frac{1}{n},$$

de donde, para todo número real positivo ϵ, existe un entero N tal que, para todo $n > N$,

$$(1) \qquad \left|x_n - y_n\right| < \frac{1}{N} < \epsilon/3.$$

Además, y es una sucesión de Cauchy de números reales, para

$$|y_n - y_m| < |y_n - x_n| + |x_n - x_m| + |x_m - y_m|,$$

y N puede escogerse de tal manera que, para $m,n > N$,

$$|y_n - x_n| < \epsilon/3$$

$$|x_m - y_m| < \epsilon/3$$

$$|x_n - x_m| < \epsilon/3,$$

por consiguiente,

$$|y_n - y_m| < \epsilon.$$

Ahora, sea a_n el número racional al cual corresponde y_n. Por el teorema 50, a es una sucesión de Cauchy de números racionales, así que $[a]_r$ es un número real. A partir de la definición 45 se sigue fácilmente que, para todo número real positivo ϵ, existe un entero N tal que, para $n > N$,

$$(2) \qquad |y_n - [a]_r| < \epsilon/2,$$

de donde, combinando (1) y (2), N puede escogerse de modo que, para $n > N$,

$$|x_n - [a]_r| \leq |x_n - y_n| + |y_n - [a]_r| < \epsilon/2 + \epsilon/3 < \epsilon,$$

lo que establece que $[a]_r$ es el límite de x.

Q.E.D.

Debe notarse que la introducción de la buena ordenación W de los números racionales en la segunda mitad de la demostración anterior no es ortodoxa. Las demostraciones usuales que se encuentran en la mayor parte de los textos sobre funciones de variables reales dicen: *Selecciónese* un y_n tal que

$$x_n < y_n < x_n + \frac{1}{n},$$

pero se requiere un número infinito de tales selecciones, así que las demostraciones usuales dependen del axioma de escogencia. Muchas demostraciones del análisis que dependen del axioma de escogencia pueden modificarse de la manera que se modificó esta demostración, para evitar tal dependencia.

El hecho de que toda sucesión de Cauchy de números reales tiene un límite muestra que no podemos extender el sistema numérico más allá, definiendo lo que pudiéramos llamar números super-reales como clases de equivalencia de sucesiones de Cauchy de números reales. Los números super-reales tienen exactamente las mismas propiedades de los números reales. A cada número real corresponde un único número super-real y recíprocamente. Además, esta relación de unicidad se preserva bajo las operaciones de adición y multiplicación y también bajo las operaciones de límite.

Ahora procedemos tan directamente como es posible a formular el teorema de la mínima cota superior.

Definición 61. *Si A es un conjunto de números reales, entonces y es una cota superior de A si y solamente si y es un número real y, para todo x en A, $x \leq y$.*

Definición 62. *Si A es un conjunto de números reales, entonces y es una mínima cota superior de A si y solamente si y es una cota superior de A y, para todo z que sea una cota superior de A, $y \leq z$.*

Dejamos como ejercicio las demostraciones de los dos teoremas siguientes, así como la demostración de que un conjunto vacío de números reales no tiene mínima cota superior.

Teorema 53. *Si A es un conjunto de números reales, entonces y es una mínima cota superior de A si y solamente si y es una cota superior de A y, para todo número real positivo ε, existe un x en A tal que $x > y - \varepsilon$.*

Teorema 54. *Un conjunto de números reales puede tener a lo más una mínima cota superior.*

Ahora estamos preparados para demostrar:

Teorema 55. *Si un conjunto no vacío de números reales tiene una cota superior, entonces tiene una mínima cota superior.*

Demostración. Sea A un conjunto que satisface las hipótesis del teorema. Claramente existen dos números reales x_0 y u_0 tales que $u_0 - x_0 = 1$, u_0 es una cota superior de A y x_0 no lo es. Ahora definimos inductivamente x_n y u_n

$$x_1 = \begin{cases} \dfrac{x_0 + u_0}{2} & \text{si } \dfrac{x_0 + u_0}{2} \text{ no es una cota superior de } A, \\[2ex] x_0 & \text{si } \dfrac{x_0 + u_0}{2} \text{ es una cota superior de } A. \end{cases}$$

$$u_1 = \begin{cases} \dfrac{x_0 + u_0}{2} & \text{si } \dfrac{x_0 + u_0}{2} \text{ es una cota superior de } A, \\[2ex] u_0 & \text{si } \dfrac{x_0 + u_0}{2} \text{ no es una cota superior de } A. \end{cases}$$

Y en general,

$$x_n = \begin{cases} \dfrac{x_{n-1} + u_{n-1}}{2} & \text{si } \dfrac{x_{n-1} + u_{n-1}}{2} \text{ no es una cota superior de } A, \\[2ex] x_{n-1} & \text{si } \dfrac{x_{n-1} + u_{n-1}}{2} \text{ es una cota superior de } A. \end{cases}$$

$$u_n = \begin{cases} \dfrac{x_{n-1} + u_{n-1}}{2} & \text{si } \dfrac{x_{n-1} + u_{n-1}}{2} \text{ es una cota superior de } A, \\[2ex] u_{n-1} & \text{si } \dfrac{x_{n-1} + u_{n-1}}{2} \text{ no es una cota superior de } A. \end{cases}$$

Tenemos entonces:

$$(1) \qquad u_n - x_n = \frac{1}{2^n}$$

y

$$u_{n-1} - u_n \leq \frac{1}{2^n},$$

a partir de lo cual inferimos fácilmente que la sucesión u es una sucesión de Cauchy de números reales, pues, dado $\varepsilon > 0$, existe un N tal que, para todos los $m,n > N$ con $n > m$,

$$\frac{1}{2^{m+1}} + \cdots + \frac{1}{2^n} < \epsilon,$$

de donde,

$$\begin{aligned} |u_m - u_n| &= |u_m - u_{m+1}| + |u_{m+1} - u_{m+2}| \\ &+ \cdots + |u_{n-1} - u_n| \\ &\leq \frac{1}{2^{m+1}} + \cdots + \frac{1}{2^n} < \epsilon. \end{aligned}$$

Y por el teorema 52, la sucesión u tiene un límite, digamos $y\star$. Queremos demostrar que $y\star$ es la mínima cota superior de A. Primero, establecemos que $y\star$ es una cota superior de A. Sea $x \in A$. Para todo n, $u_n \geq x$. Ya que para todo ε existe un n tal que

$$u_n - y\star < \epsilon,$$

tenemos

$$y\star + \epsilon > u_n,$$

de donde,

$$(2) \qquad y\star + \epsilon > x,$$

pero ya que (2) debe ser válido para todo $\varepsilon > 0$,

$$y\star \geq x.$$

Así que $y\star$ es una cota superior de A.
Ahora supongamos que z es una cota superior de A tal que $z < y\star$. Entonces sobre la base de (1) existe un n tal que

$$u_n - x_n < y\star - z,$$

pero

$$y\star - x_n \leq u_n - x_n,$$

de donde,

$$y\star - x_n < y\star - z,$$

así que

$$z < x_n,$$

pero entonces z no es una cota superior de A ya que x_n no lo es, contrario a nuestra suposición, lo que completa la demostración de que $y\star$ es la mínima cota superior de A.

Q.E.D.

EJERCICIOS

1. Demostrar los teoremas 44 y 45.
2. Demostrar el teorema 46. (Este ejercicio tiene quince partes.)
3. Demostrar los teoremas 47 y 48.
4. Demostrar el teorema 50.
5. Demostrar el teorema 51.
6. Demostrar los teoremas 53 y 54.
7. Demostrar que un conjunto vacío de números reales no tiene una mínima cota superior.
8. Sean x y y sucesiones de números reales que tienen un límite. Demostrar que

   (a) $\lim\limits_{n \to \infty} (x_n + y_n) = \lim\limits_{n \to \infty} x_n + \lim\limits_{n \to \infty} y_n,$

   (b) $\lim\limits_{n \to \infty} (x_n y_n) = \lim\limits_{n \to \infty} x_n \cdot \lim\limits_{n \to \infty} y_n,$

   (c) si, para todo n, $y_n \neq 0$ y $\lim\limits_{n \to \infty} y_n \neq 0$,

   entonces

   $$\lim_{n \to \infty} \left(\frac{x_n}{y_n}\right) = \frac{\lim\limits_{n \to \infty} x_n}{\lim\limits_{n \to \infty} y_n}.$$

9. Sea x una sucesión de Cauchy de números reales y sea y una sub-sucesión de x. Demostrar que

   $$\lim_{n \to \infty} y_n = \lim_{n \to \infty} x_n.$$

10. Definir de la manera obvia las nociones de cota inferior y de máxima cota inferior de un conjunto de números reales y demostrar que todo conjunto no vacío de números reales que tiene una cota inferior tiene una máxima cota inferior.
11. Una sucesión x de números reales se dice *acotada* si existe un número real $x\star$ tal que, para todo n,

   $$|x_n| \leq x\star.$$

¿Es acotada toda sucesión de Cauchy de números reales? Si lo es demostrarlo; si no, dar un contra-ejemplo.

§ 6.7 Conjuntos con la potencia del continuo.

La primera cuestión de esta sección final del capítulo es demostrar el famoso teorema de Cantor, de 1874, según el cual el conjunto de los números reales no es enumerable. Un teorema preliminar útil es el de que todo número real puede representarse de manera única con un decimal que no termina. La formulación rigurosa de esto último es la siguiente, generalizada a cualquier raíz entera ≥ 2.

Teorema 56. *Sea r un entero ≥ 2. Todo número real x es representable de manera única con respecto a la raíz r, como una sucesión $\langle a, d_1, d_2, \ldots, d_n, \ldots \rangle$ tal que*

(i) *a es el mayor entero igual o menor que x,*

(ii) *para todo n, $0 \leq d_n < r$ y d_n es un entero,*

(iii) *no es el caso de que exista un N tal que para todo $n > N$, $d_n = r - 1$,*

(iv) *la sucesión cuyos términos c_n están definidos en forma recurrente por*

$$C_0 = a$$

$$c_{n+1} = c_n + d_{n+1}/r^{n+1}$$

es una sucesión de Cauchy que converge a x.

Demostración. Sea x cualquier número real. Sea ar el mayor entero que es igual o menor que rx. Entonces existe un número no negativo $\varepsilon_1 < r$ tal que

$$x = a + \frac{\epsilon_1}{r}.$$

De manera similar,

$$\epsilon_1 = d_1 + \frac{\epsilon_2}{r}, \quad \epsilon_2 = d_2 + \frac{\epsilon_3}{r}, \cdots, \quad \epsilon_n = d_n + \frac{\epsilon_{n+1}}{r},$$

donde para todo n, $0 \leq d_n, \epsilon_n < r$ y d_n es un entero. Así,

$$x = a + \frac{d_1}{r} + \frac{d_2}{r^2} + \cdots + \frac{d_n}{r^n} + \frac{\epsilon_{n+1}}{r^{n+1}},$$

y en consecuencia,

$$0 \leq x - \left(a + \frac{d_1}{r} + \frac{d_2}{r^2} + \cdots + \frac{d_n}{r^n}\right) < \frac{1}{r^n},$$

esto es, para todo n, usando la definición de (iv)

$$0 \leq x - c_n < \frac{1}{r^n},$$

pero $\lim\limits_{n\to\infty} \dfrac{1}{r_n} = 0$, de donde, $\lim\limits_{n\to\infty} c_n = x$.

Q.E.D.

Nótese que la condición (iii) del teorema elimina para la raíz 10, por ejemplo, una sucesión infinita de nueves. Así, 5,000. . . no puede, según el teorema, representarse también por medio de 4,999. . ., representación que debe ser excluida para garantizar la unicidad.

La demostración del recíproco del teorema 56 se deja como ejercicio.

Teorema 57. *Sea $\langle a, d_1, d_2, \ldots, d_n, \ldots \rangle$ una sucesión tal que*

(i) *a es un entero,*

(ii) *existe un entero $r \geq 2$ tal que, para todos los n, $0 \leq d_n < r$ y cada d_n es un entero.*

Entonces existe un único número real x tal que la sucesión cuyos términos c_n están definidos recurrentemente por: $c_0 = a$ y $c_{n+1} = c_n + d_{n+1}/r^{n+1}$, es una sucesión de Cauchy que converge a x.

Escogiendo la raíz 2 no es difícil, sobre la base de los teoremas 56 y 57, demostrar:

Teorema 58. *El conjunto de todos los números reales es equipotente con el conjunto 2^ω.*

En virtud de los teoremas 14 y 23 del capítulo 4, se sigue del teorema 58 que

Teorema 59. *El conjunto de los números reales no es enumerable.*

También es útil dar la demostración más constructiva, debida a Cantor, de este teorema, usando su importante "método diagonal". Usamos el teorema 56 y representamos los números reales por sus desarrollos decimales. Obviamente, el conjunto de los números reales es infinito. Supongamos ahora que es también enumerable. Entonces hay una función f 1-1 de ω al conjunto de los números reales. Sea

$$r_n = f(n).$$

Todo número real r_n lo representamos en notación decimal como

$$r_n = a^{(n)}\, d_1^{(n)}\, d_2^{(n)}\, d_3^{(n)} \ldots,$$

donde $a^{(n)}$ es el mayor entero igual o menor que r_n.
Ahora considérese el número real

$$c = a\,.\,d_1 d_2 d_3 \ldots$$

definido como sigue:

$$a = \begin{cases} 2 & \text{si} \quad a^{(0)} = 1 \\ 1 & \text{si} \quad a^{(0)} \neq 1. \end{cases}$$

(Aquí $a^{(0)}$ es, desde luego, el mayor entero igual o menor que r_0.)
Y

$$d_n = \begin{cases} 2 & \text{si} \quad d^{(n)} = 1 \\ 1 & \text{si,} \quad d^{(n)} \neq 1. \end{cases}$$

Así, si

$$r_0 = 4{,}333\ldots$$

$$r_1 = 7{,}12171217\ldots$$

$$r_2 = 0{,}689689\ldots$$

$$r_3 = 0{,}414141\ldots,$$

entonces,

$$c = 1{,}211\ldots.$$

Pero puede no haber r_n tal que

$$c = r_n$$

pues el n-simo decimal de r_n debe diferir del n-simo decimal de c. (Contamos el entero a como el 0-ésimo decimal.) Por tanto no hay un n tal que

$$c = f(n),$$

y nuestra suposición es falsa. De esto se deduce que el conjunto de los números reales no es enumerable.

Los conjuntos equipotentes con el conjunto de los números reales se llaman frecuentemente *conjuntos con la potencia del continuo.* En los teoremas siguientes se han resumido algunos hechos básicos acerca de tales conjuntos; las demostraciones no se han dado en detalle.

Teorema 60. *La unión entre un conjunto finito o enumerable con un conjunto que tenga la potencia del continuo es, de nuevo, un conjunto con la potencia del continuo.*

Demostración. Compárese con la demostración del teorema 67 del capítulo 5.

Teorema 61. *Si A es un conjunto con la potencia del continuo y B es un conjunto finito o enumerable, entonces $A \sim B$ es un conjunto con la potencia del continuo.*

Teorema 62. *El conjunto de todos los números reales que constituyen el intervalo comprendido entre dos números reales diferentes a y b tiene la potencia del continuo.*

Demostración. Considérese primero la aplicación f de los números reales positivos sobre el intervalo $(0,1)$:

$$f(x) = \frac{x}{1+x}.$$

De una manera similar se aplican los números reales negativos sobre el intervalo $(-1,0)$. Se sigue de una vez a partir de esas dos aplicaciones 1-1 que el conjunto de los números reales del intervalo $(-1,1)$ tiene la potencia del continuo. Dejamos como ejercicio construir una función 1-1 que aplique cualquier intervalo finito (a,b) sobre $(-1,1)$.

Teorema 63. *Todo conjunto con la potencia del continuo puede representarse como la unión de n subconjuntos mutuamente disjuntos, cada uno de los cuales tiene la potencia del continuo.*

La demostración se hace por inducción sobre n.
Además,

Teorema 64. *Todo conjunto con la potencia del continuo puede representarse como* *la unión de una sucesión infinita de conjuntos sin elementos comunes y cada uno de los cuales tiene la potencia del continuo.*

Demostración. Usese la sucesión $\langle A_1, A_2, \ldots, A_n, \ldots\rangle$ definida por: A_n es el conjunto de todos los números reales x tales que

$$n - 1 \leq x < n.$$

Con el mismo enfoque es fácil mostrar que

Teorema 65. *El producto cartesiano de dos conjuntos, de los cuales uno es enumerable y el otro tiene la potencia del continuo, tiene la potencia del continuo.*

Podemos demostrar también

Teorema 66. *El producto cartesiano de dos conjuntos que tienen la potencia del continuo tiene también la potencia del continuo.*

Demostración. Demostramos que $(0,1) \times (0,1) \approx (0,1)$. Para este propósito, semejante a la representación decimal del teorema 56, podemos representar cualquier número real x del intervalo $(0,1)$ como

$$x = \frac{d_1}{2} + \frac{d_2}{4} + \frac{d_3}{8} + \ldots, \quad d_n = 0 \text{ ó } 1.$$

Considerando solamente $d_n = 1$, tenemos

$$x = (\tfrac{1}{2})^{p_1} + (\tfrac{1}{2})^{p_2} + (\tfrac{1}{2})^{p_3} + \ldots,$$

con $p_1 < p_2 < p_3 < \ldots$ Definimos ahora

$$a_1 = p_1,\ a_2 = p_2 - p_1,\ a_3 = p_3 - p_2, \ldots$$

y representamos

$$x = (\tfrac{1}{2})^{a_1} + (\tfrac{1}{2})^{a_1+a_2} + (\tfrac{1}{2})^{a_1+a_2+a_3} + \ldots,$$

o, en notación más simple, podemos representar x por la sucesión $< a_1, a_2, a_3 \ldots, a_n, \ldots >$. Tenemos una representación similar de $y \varepsilon (0,1)$ como $< b_1, b_2, b_3, \ldots, b_n, \ldots >$. Definimos entonces $f(< x,y >)$ como el número de $(0,1)$ representado por la sucesión $< a_1, b_1, a_2, b_2, a_3, b_3, \ldots, a_n, b_n, \ldots >$. Es inmediato demostrar que f es una aplicación 1-1 de $(0,1) \times (0,1)$ sobre $(0,1)$.*

Usando el axioma especial para cardinales, podemos definir,

†**Definición 63.** $\mathfrak{c} = \mathcal{K}(\mathrm{Re})$.

El símbolo '$\mathfrak{c}$' es el usual para la cardinalidad del continuo. Usando esta definición, formulamos un teorema general sobre la aritmética cardinal de $\mathfrak{c}$. La demostración de cada parte del teorema se sigue directamente de uno o más de los teoremas inmediatamente precedentes de esta sección.

†**Teorema 67.**

(i) *Si* $\mathfrak{n}$ *es un cardinal finito, entonces*

$$\mathfrak{n} + \mathfrak{c} = \mathfrak{n} \cdot \mathfrak{c} = \mathfrak{c},$$

(ii) $\aleph_0 + \mathfrak{c} = \mathfrak{c}$,

(iii) $\aleph_0 \cdot \mathfrak{c} = \mathfrak{c}$,

(iv) $2^{\aleph_0} = \mathfrak{c}$.

(v) $\mathfrak{c} + \mathfrak{c} = \mathfrak{c}$.

(vi) $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$.

No se sabe si existe un conjunto que sea de mayor potencia que un conjunto enumerable y de menor potencia que el continuo. La conjetura de que no hay tales conjuntos se llama *hipótesis del continuo.* Sierpinski [1956] resume de manera perfecta las consecuencias importantes conocidas de esta hipótesis. Una de las más interesantes, que es realmente equivalente a la hipótesis del continuo, es la siguiente proposición (la equivalencia fue demostrada por Sierpinski en 1919): El conjunto de todos los puntos del plano es la unión de dos conjuntos, de los cuales uno es a lo más enumerable sobre cualquier recta paralela al eje de las ordenadas y el otro es a lo más enumerable sobre cualquier recta paralela al eje de las abscisas.

Se demostró antes que el conjunto de todos los números reales es equipotente a 2^{ω}.

* La demostración de que no existe función 1-1 continua que establezca esta correspondencia no es demasiado difícil (ver Sierpinski [1958, p. 66]).

Esta relación es la base de la *hipótesis generalizada del continuo:* Dado un conjunto infinito A, no existe conjunto alguno de potencia mayor que la de A y menor que el conjunto de todos los subconjuntos de A. Gödel ([1938], [1940]) ha demostrado el importante resultado de que la hipótesis generalizada del continuo puede agregarse consistentemente a los otros axiomas de la teoría de conjuntos,* esto es, si los otros axiomas son conjuntamente consistentes, entonces la adición de la hipótesis generalizada del continuo como un nuevo axioma no dará lugar a contradicción.

EJERCICIOS

1. Demostrar el teorema 57
2. Demostrar el teorema 58.
3. Demostrar el teorema 60.
4. Demostrar el teorema 61.
5. Completar la demostración del teorema 62.
6. Demostrar el teorema 63.
7. Demostrar el teorema 64.
8. Demostrar el teorema 65.
9. Demostrar el teorema 66.
10. Demostrar que no existe aplicación continua del plano sobre la recta.
11. Demostrar el teorema 67.

* Su demostración se refiere en realidad a los axiomas de la teoría de conjuntos de von Neumann, como se presenta en sus documentos, pero con pequeñas modificaciones la demostración vale para los axiomas de la teoría de conjuntos de Zermelo-Fraenkel también.

Capítulo 7

Inducción transfinita y aritmética ordinal

§ 7.1 **Inducción transfinita y definición por recurrencia transfinita.** El foco del presente capítulo es la teoría de los números ordinales. La primera sección considera la inducción transfinita y la definición por recurrencia transfinita para números ordinales. El esquema axiomático de sustitución se necesita para justificar el esquema general de recurrencia. La segunda sección presenta los elementos de la aritmética ordinal. La tercera sección considera los números cardinales, de nuevo, pero sin usar el axioma especial para cardinales. En particular se introduce el concepto de un alef. La cuarta sección generaliza los resultados de § 7.1 a conjuntos bien ordenados. Además se demuestra el teorema fundamental para conjuntos bien ordenados. La sección final (§ 7.5) presenta un resumen revisado de los axiomas; se usa el esquema axiomático de sustitución para deducir el axioma de apareamiento y el esquema axiomático de separación.

Nuestro primer problema es extender el principio de inducción para los números naturales (ordinales finitos) al principio de inducción transfinita para todos los ordinales. Como lo establece el teorema 12 de § 5.1, el conjunto de todos los ordinales no existe, así que no puede darse una formulación general de la inducción transfinita. Sin embargo, como veremos, es posible una formulación conjuntista a partir de cualquier ordinal dado. También puede demostrarse un esquema general para todos los ordinales, análogo al teorema 22 de § 5.2; en efecto, comenzamos con esto.

Las letras iniciales del alfabeto griego, en minúscula, o sea 'α', 'β', 'γ', 'δ', . . . , con o sin sub-índices, indicará variables que toman ordinales como valores.

> **Esquema teoremático 1.** [Principio de inducción transfinita: primera formulación]. *Si para todo* α
>
> (i) $(\forall\beta)(\beta < \alpha \to \varphi(\beta)) \to \varphi(\alpha)$,
>
> *entonces para todo* α, $\varphi(\alpha)$.

Demostración. Asegurada la hipótesis del teorema, supongamos que existe un α tal que $\varphi(\alpha)$ es falso. Sea

$$L(\alpha) = \{\beta\colon \beta \leq \alpha \ \&\ \varphi(\beta) \text{ es falso}\}.$$

Entonces, $\varepsilon_{\alpha'}$ bien-ordena $L(\alpha)$. Sea β^* el primer elemento de $L(\alpha)$. Por la hipótesis sobre β^*, para todo $\gamma < \beta^*$ tenemos: $\varphi(\gamma)$. Pero entonces por la hipótesis (inductiva), esto es, (i) del teorema, $\varphi(\beta^*)$, lo que es una contradicción. Q.E.D.

La formulación del teorema 1, cuando se especializa para los números naturales, proporciona lo que se llama frecuentemente una inducción de "curso de valores" porque se consideran *todos* los números naturales menores que un número dado, no solamente el precedente inmediato.

La demostración de la formulación conjuntista de la inducción transfinita es una variante trivial de la anterior, así que solamente formulamos el teorema, pero debe notarse el hecho de que este teorema, en contraste con el teorema 1, se refiere a un ordinal α.

Teorema 2. [Principio de inducción transfinita: Segunda formulación]. *Si para todo ordinal $\beta < \alpha$ tenemos que $\beta \subseteq A$ implica que $\beta \in A$, entonces $\alpha \subseteq A$. Simbólicamente:*

$$(\forall \beta)(\beta < \alpha \,\&\, \beta \subseteq A \rightarrow \beta \in A) \rightarrow \alpha \subseteq A.$$

Si tomamos $\alpha = \omega$, tenemos, como un caso especial del teorema, una formulación de inducción para los números naturales, ligeramente diferente del teorema 24 de § 5.2:

Si $m \in A$ siempre que $m \subseteq A$, entonces $\omega \subseteq A$.

La formulación de la inducción transfinita proporcionada por el teorema 2 tiene cierto interés desde el punto de vista de las aplicaciones. Al usar la inducción transfinita para demostrar un teorema, se desea saber frecuentemente cuán "lejos" va la inducción, esto es, cuál es el ordinal α más pequeño que será suficiente para aplicar el teorema 2. Desde luego, en la inducción ordinaria siempre tomamos $\alpha = \omega$.

Ahora queremos enunciar, sin demostración, una tercera formulación de la inducción transfinita que usa una condición como la usual para inducción sobre los números naturales: si $\varphi(n)$, entonces $\varphi(n')$, y restringe las inducciones de curso total de valores a *ordinales límite,* esto es, ordinales que no tienen precedente inmediato y no son cero.

Definición 1. *α es un ordinal límite si y solamente si $\alpha \neq 0$ y no existe β tal que $\beta' = \alpha$.*

El ordinal ω es el único ordinal límite que hemos introducido atrás. Se enuncia aquí, sin demostración, un hecho útil acerca de ordinales límite.

Teorema 3. *Si α es un ordinal límite, entonces $\bigcup \alpha = \alpha$.*

Esquema teoremático 4. [Principio de inducción transfinita: Tercera formulación].

Supongamos que

(i) $\varphi(0)$,
(ii) *para todo α, si $\varphi(\alpha)$, entonces $\varphi(\alpha')$ y,*
(iii) *para todo ordinal límite γ, si para todo $\beta < \gamma$, $\varphi(\beta)$, entonces $\varphi(\gamma)$.*

Entonces para todo ordinal α, $\varphi(\alpha)$.

Antes de volver a las recurrencias transfinitas, puede enunciarse un esquema teoremático útil sobre la existencia de un ordinal mínimo que satisfaga a una propiedad dada. Su demostración se deja como ejercicio.

Esquema teoremático 5. *Si existe un α tal que $\varphi(\alpha)$, entonces existe un ordinal mínimo β tal que $\varphi(\beta)$.*

Para introducir subsiguientemente las operaciones ordinales de adición, multiplicación y exponenciación, no es suficiente tener a mano el principio de inducción transfinita. Es necesario justificar la definición por recurrencia transfinita de la misma manera general que justificamos la definición por recurrencia de las operaciones sobre números naturales en § 5.2. Hasta donde yo sé, la primera demostración de un teorema general que justifique la definición por recurrencia transfinita se encuentra en von Neumann [1928b].

La demostración de la primera formulación es muy semejante a la demostración del teorema 27 de § 5.2 sobre la definición por recurrencia. La mayor diferencia en la formulación es la de que la función H (el teorema dice "conjunto H" pero en las aplicaciones estamos siempre interesados en funciones) toma el total de F restringido a β como su argumento, en lugar del precedente simplemente como en el teorema 27. Una forma no adulterada del teorema 27 no podría ser usada, desde luego, para los ordinales en general ya que los ordinales límite no tienen precedentes inmediatos.

Teorema 6. [Recurrencia transfinita: Primera formulación]. *Sea H cualquier con-*

junto y α cualquier ordinal. Entonces existe una única F tal que

(i) *F es una función sobre α,*
(ii) *para todo $\beta < \alpha$,*
$$F(\beta) = H(F \mid \beta).$$

Demostración. Primero, en virtud del esquema axiomático de separación, existe un conjunto A tal que $f \in A$ si y solamente si:

(1) $f \in \mathcal{P}(\alpha \times (\mathcal{R}H \cup \{0\}))$,

y existe un β tal que

(2) f es una función sobre β,
(3) para todo γ, si $\gamma < \beta$, entonces $f(\gamma) = H(f|\gamma)$.

Como en el caso del teorema 27 de §5.2, la idea de la demostración es mostrar que $\cup A$ es la función F pedida. Comenzamos por demostrar:

(4) Si $f, g \in A$, entonces $f \subseteq g$ ó $g \subseteq f$.

Sea β_1 el dominio de f y β_2 el dominio de g. Entonces $\beta_1 \cap \beta_2$ es β_1 o β_2. Ahora supongamos que existe un γ en $\beta_1 \cap \beta_2$ tal que
$$f(\gamma) \neq g(\gamma).$$
Sea $\gamma_\star$ el más pequeño de tales ordinales (ver teorema 5). Tenemos entonces:
$$f \mid \gamma_\star = g \mid \gamma_\star,$$
y *a fortiori*

(5) $$H(f \mid \gamma_\star) = H(g \mid \gamma_\star),$$

pero entonces
$$f(\gamma_\star) = g(\gamma_\star),$$

contrario a nuestra suposición, por tanto, se establece (4).

Ahora definimos:
$$F = \cup A.$$

Se sigue, de una vez, a partir de (4) que F es una función. Además, si β está en el dominio de F, entonces, para algún f en A, β está en el dominio de f y, en consecuencia,
$$f(\beta) = H(f \mid \beta),$$
de donde
$$F(\beta) = H(F \mid \beta).$$

Resta solamente demostrar que α es el dominio de F. Supongamos que no. Sea β^* el ordinal más pequeño menor que α y que no está en el dominio de F. Entonces existe un f en A cuyo dominio es β^*. Por tanto,
$$f \cup [\langle \beta^*, H(f \mid \beta^*)\rangle] \in A,$$
y, por consiguiente, $\beta^\star$ está en el dominio de F, contrario a nuestra suposición. La demostración de que F es única se deja como ejercicio. Q.E.D.

Como podría esperarse, se puede dar una versión de recurrencia transfinita, muy ligada al teorema 27 de § 5.2, haciendo uso de ordinales límite. El contenido intuitivo de la condición (iv) del teorema se discutirá en relación con las definiciones de adición ordinal y de multiplicación en § 7.3.

Teorema 7. [Recurrencia transfinita: Segunda formulación]. *Sea x cualquier objeto, G cualquier conjunto y α cualquier ordinal no nulo. Entonces existe una única* F tal que

(i) *F es una función sobre α,*
(ii) $F(0) = x$,
(iii) *para todo β con $\beta' < \alpha$,*
$$F(\beta') = G(F(\beta)),$$
(iv) *para todo $\beta < \alpha$, si β es un ordinal límite, entonces*
$$F(\beta) = \bigcup_{\gamma \in \beta} F(\gamma).$$

Demostración. La demostración de esta formulación del teorema, justificante de la recurrencia transfinita, es posible con la especificación de la función H apropiada en el teorema precedente.

Sea
$$L = \mathcal{R}G \cup \{x\}.$$

Primero definimos la noción de una α-sucesión de L. Una α-sucesión de L es una función cuyo dominio es α y cuyo recorrido es un subconjunto de L. (Una sucesión de elementos de L, en el sentido matemático usual, es precisamente una ω-sucesión.) Ahora consideremos la función H definida como sigue:

(1) El dominio de H es el conjunto de β-sucesiones de L con $\beta < \alpha$,

(2) Para la 0-sucesión 0,

$$H(0) = x,$$

(3) Para cualquier β'-sucesión s

$$H(s) = G(s(\beta)),$$

(4) Para β un ordinal límite y s una β-sucesión,

$$H(s) = \bigcup_{\gamma\in\beta} s(\gamma).$$

Nótese que en virtud de la definición 15 de § 2.6

$$\bigcup_{\gamma\in\beta} s(\gamma) = \bigcup\{y: (\exists\gamma)(\gamma \in \beta \;\&\; y = s(\gamma))\},$$

y puesto que $s(\gamma) \in L$, se sigue, a partir del esquema axiomático de separación, que el conjunto $\{y: (\exists\gamma)(\gamma \in \beta \;\&\; y = s(\gamma))\}$ siempre existe en el sentido apropiado, esto es, no es vacío. (En relación con el recorrido de H, véase el ejercicio 6, al final de la sección.) En vista del teorema precedente (teorema 6) existe una función única F definida sobre α tal que, para todo $\beta < \alpha$,

$$(5) \qquad F(\beta) = H(F \mid \beta).$$

Observamos que, en virtud de (1), $F \mid \beta$ es una β-sucesión. Por tanto, por (2) y (5)

$$F(0) = H(F \mid 0) = x,$$

lo que establece (ii) del teorema.

Sobre la base de (3) y (5)

$$F(\beta') = H(F \mid \beta') = G([F \mid \beta'](\beta)) = G(F(\beta)),$$

lo que demuestra (iii).

Finalmente, en vista de (4) y (5), si β es un ordinal límite,

$$F(\beta) = H(F \mid \beta) = \bigcup_{\gamma\in\beta} ([F \mid \beta](\gamma)) = \bigcup_{\gamma\in\beta} (F(\gamma)).$$

La unicidad de F es obvia. Q.E.D.

Debe notarse que el teorema 7 es menos general que el teorema 6, porque no todas las funciones F del teorema 6 satisfacen (iv) del teorema 7, esto es, satisfacen:

$$F(\beta) = \bigcup_{\gamma\in\beta} F(\gamma)$$

para β un ordinal límite. Por ejemplo, en el teorema 6, sea α, ω' y para cualquier β-sucesión s con $\beta \leq \omega'$ definamos

$$H(s) = \begin{cases} 0 \text{ si } \beta \text{ es un ordinal límite} \\ 1 \text{ en cualquier otro caso.} \end{cases}$$

Entonces

$$F(\omega) = 0,$$

pero

$$\bigcup_{n\in\omega} F(n) = \bigcup\{1\} = 1.$$

Debe ser claro por qué los teoremas 6 y 7 no proporcionan la justificación óptima para la introducción de las operaciones de la adición ordinal. El conjunto de todos los ordinales no existe, así que no puede esperarse que se defina la adición o la multiplicación ordinal como una función de la teoría de conjuntos. El objetivo restante de esta sección es establecer un esquema teoremático que justifique la definición de los símbolos apropiados de operación. Para comenzar, demostramos un esquema de recurrencia transfinita análogo al teorema 6. Este esquema se ha puesto después de los teoremas 6 y 7 porque su demostración requiere el esquema axiomático de sustitución, el cual introduciremos luego.

La necesidad de una formulación esquemática de la recurrencia transfinita puede hacerse quizás más evidente por la discusión de las dificultades que surgen cuando tratamos de usar el teorema 7 para definir la adición ordinal. El esquema recurrente que tenemos pensado es simplemente:

(i) $\alpha + 0 = \alpha$,

(ii) $\alpha + \beta' = (\alpha + \beta)'$

(iii) Si β es un ordinal límite,

$$\alpha + \beta = \bigcup_{\gamma\in\beta} (\alpha + \gamma).$$

Las condiciones (i) y (ii) proporcionan un esquema recurrente como el de la adición entre enteros. La tercera condición es nueva. Podemos ilustrar su significado intuitivo considerando $\omega + \omega$. No hemos demostrado aún que $\omega + \omega$ existe, pero dejando este asunto de lado por el momento, la idea básica es la de que

$$\omega + \omega = \{0, 1, 2, 3, \ldots, \omega, \omega + 1, \omega + 2, \omega + 3, \ldots\}.$$

Y vemos fácilmente que esto es precisamente lo que hacemos a partir de:

$$\omega + \omega = \bigcup_{\gamma \in \omega} (\omega + \gamma) = \bigcup_{n \in \omega} (\omega + n).$$

La forma de (iii) debe aclarar por qué (iv) del teorema 7 tiene la forma que tiene.

Desafortunadamente, surgen complicaciones inmediatamente si tratamos de aplicar el teorema 7 a la conversión de esas tres condiciones en una definición precisa de una función unaria $\alpha+$. (Puesto que el teorema 7 proporciona solamente funciones unarias, para cada ordinal α, definimos $\alpha+$, en lugar del símbolo de operación binaria $+$.) Primero, no podemos definir simplemente una función $\alpha+$ para todos los ordinales, ya que el conjunto de todos los ordinales no existe. Supongamos entonces que definimos $\alpha+$ con respecto a algún ordinal η, el cual requiere un sub-índice: $\alpha +_\eta$. Entonces tendríamos:

$$(1)\qquad \begin{cases} \alpha +_\eta 0 = \alpha \\ \alpha +_\eta \beta' = (\alpha +_\eta \beta)' \end{cases}$$

y así sucesivamente; podríamos naturalmente imponer la restricción de que el dominio de $\alpha +$ es η. Sin embargo, la relativización de la adición ordinal a algún ordinal η no es suficiente para permitir la aplicación del teorema 7. Como se anotó, previamente a la definición de la adición entre enteros, no podemos usar simplemente el símbolo de sucesor al elegir una función particular G, pues no hay conjunto alguno designado por el símbolo de sucesor. Para tratar la adición entre enteros introdujimos la notación '$\mathfrak{S}_A$' para designar la función sucesor restringida a A. Probablemente la sugerencia natural es entonces ensayar $\mathfrak{S}_\eta$ en (1):

$$(2)\qquad \begin{cases} \alpha +_\eta 0 = \alpha \\ \alpha +_\eta \mathfrak{S}_\eta(\beta) = \mathfrak{S}_\eta(\alpha +_\eta \beta). \end{cases}$$

No hay dificultad acerca de $\mathfrak{S}_\eta(\beta)$ ya que $\beta \in \eta$, pero la situación es diferente para $\mathfrak{S}_\eta(\alpha +_\eta \beta)$. Si α es suficientemente grande, puede suceder que $\alpha +_\eta \beta > \eta$, y, por consiguiente, $\mathfrak{S}_\eta(\alpha +_\eta \beta) = 0$. Por ejemplo,

$$(3)\qquad \mathfrak{S}_\omega(\omega +_\omega 3) = 0,$$

mientras que

$$(4)\qquad (\omega +_\omega 3)' = \omega +_\omega 4 \neq 0.$$

La dificultad que surge por (2) y el caso particular (3) es fundamental y sobre la base del teorema 7 es imposible hacer arreglos que permitan la construcción de una aritmética ordinal razonable.

Como ya se anotó, para demostrar el teorema de recurrencia apropiado necesitamos el esquema axiomático de sustitución. La idea intuitiva del axioma es la de que si tenemos una fórmula $\varphi(x,y)$ con la propiedad funcional de que para todo x en un conjunto A existe por lo menos un y tal que $\varphi(x, y)$, entonces podemos afirmar que el *conjunto* de los y existe y "sustituir" A por este nuevo conjunto. Formalmente, tenemos:*

Esquema axiomático de sustitución. *Si*

$$(\forall x)(\forall y)(\forall z)(x \in A \ \&\ \varphi(x,y) \ \&\ \varphi(x,z) \rightarrow y = z),$$

entonces

$$(\exists B)(\forall y)(y \in B \leftrightarrow (\exists x)(x \in A \ \&\ \varphi(x,y))).$$

La hipótesis del axioma requiere simplemente que $\varphi(x,y)$ sea funcional en x. Si se eliminara este requerimiento estaríamos inmediatamente en dificultad. Por ejemplo, podríamos tomar $\varphi(x, y)$ de modo que

$$x \subseteq y,$$

y tomar $A = \{0\}$; entonces, puesto que el conjunto vacío es un subconjunto de todo

* Este axioma se llama también el *esquema axiomático de sustitución*; se originó con Fraenkel [1922]. En la literatura de teoría de conjuntos el axioma se acredita usualmente sólo a Fraenkel, pero Skolem [1922, p. 226] lo formuló independientemente y al mismo tiempo. En Fraenkel [1928], puede decirse que se conoce la formulación hecha independientemente por Skolem.

conjunto, B sería el paradójico conjunto de todos los conjuntos.

En la última sección de este capítulo mostramos que el esquema axiomático de separación se sigue del esquema axiomático de sustitución (la demostración es trivial) y también que el axioma de apareamiento se sigue del axioma del conjunto potencia y del esquema axiomático de sustitución.

Esquema teoremático 8. [Recurrencia transfinita: Tercera formulación].† *Sea τ cualquier término. Entonces el siguiente es un teorema: Para cualquier ordinal α existe una F única tal que:*

(i) *F es una función sobre α,*
(ii) *para todo $\beta < \alpha$,*

$$F(\beta) = \tau(F|\beta).$$

Demostración. Comparando ahora con el primer paso de la demostración del teorema 6, tomamos $\varphi(\beta, f)$ de modo que:

$\varphi(\beta,f) \leftrightarrow f$ sea una función sobre β & $(\forall\gamma)(\gamma < \beta \rightarrow f(\gamma) = \tau(f|\gamma))$.

Si tenemos: $\varphi(\beta,f)$ & $\varphi(\beta,f')$, se sigue fácilmente por inducción transfinita (teorema 1) que $f = f'$, pues supongamos que hubiera un γ tal que $f(\gamma) \neq f'(\gamma)$. Sea $\gamma*$ el primero de tales ordinales. Entonces

$$f|\gamma* = f'|\gamma*,$$

y *a fortiori*

$$\tau(f|\gamma*) = \tau(f'|\gamma*),$$

de donde

$$f(\gamma*) = f'(\gamma*),$$

lo que es absurdo.

Ya que φ tiene la propiedad adecuada muchos-uno podemos aplicar el esquema axiomático de sustitución para obtener: existe un conjunto A tal que

$$f \in A \leftrightarrow (\exists\beta)(\beta \in \alpha' \,\&\, \varphi(\beta,f)).$$

† Esta formulación está más bien ligada a la original de von Neumann [1928].

El resto de la demostración consiste simplemente en demostrar que $\bigcup A$ es la función F pedida y es esencialmente la misma que la parte correspondiente del teorema 6.

Q.E.D.

Análogo al teorema 7 tenemos otra formulación en la forma de un esquema. Dejamos la demostración como ejercicio.

Esquema teoremático 9. [Recurrencia transfinita: Cuarta formulación]. *Sea τ cualquier término. Entonces el siguiente es un teorema:*
Si x es cualquier objeto y α cualquier ordinal no nulo, entonces existe una F única tal que

(i) *F es una función sobre α,*
(ii) $F(0) = x$,
(iii) *para todo ordinal β con $\beta' < \alpha$,*

$$F(\beta') = \tau(F(\beta)),$$

(iv) *para todo ordinal límite $\beta < \alpha$,*

$$F(\beta) = \bigcup_{\gamma\in\beta} F(\gamma).$$

Para los propósitos de las aplicaciones es necesario saber que una función definida por recurrencia transfinita (vía los teoremas 6 a 9) es independiente del ordinal particular escogido en el sentido expresado por el teorema siguiente. La demostración se ha dejado como ejercicio. Se entiende en la formulación del teorema que no importa cuál de los cuatro teoremas se use, las funciones F_1 y F_2 están definidas con respecto al mismo objeto x, conjunto F o término τ, según el caso.

Teorema 10. *Sean F_1 y F_2 definidas por recurrencia transfinita a partir de α_1 y α_2 respectivamente por el uso del teorema* 6, 7, 8 ó 9. *Entonces,*

$$F_1|\alpha_2 = F_2|\alpha_1.$$

Sobre la base del teorema 9 podemos definir la adición ordinal como sigue:

$\alpha + \beta = \gamma$ si y solamente si existe una función f tal que

(i) *f es una función sobre β',*
(ii) $f(0) = \alpha$,

(iii) *para todo* η *con* $\eta < \beta$

$$f(\eta') = f(\eta)',$$

(iv) *para todo ordinal límite* $\eta < \beta'$

$$f(\eta) = \bigcup_{\theta \in \eta} f(\theta),$$

(v) $f(\beta) = \gamma$.

En esta definición hemos establecido esencialmente una jerarquía de funciones unarias $\alpha +$, para cada α con dominio β'. Un procedimiento más satisfactorio estéticamente es el de usar los teoremas 9 y 10 para demostrar un esquema general sobre la base de lo que puede dar una definición más intuitiva de las operaciones ordinales binarias como la adición. Para este esquema general necesitamos el siguiente resultado general, cuya demostración depende del esquema axiomático de sustitución.

Esquema teoremático 11.

$$y \in \bigcup_{x \in A} \tau(x) \leftrightarrow (\exists x)(\exists B)(x \in A \ \& \ B = \tau(x) \ \& \ y \in B)$$

Podemos entonces establecer, sobre la base de los teoremas precedentes:

Esquema teoremático 12. [Recurrencia transfinita: Quinta formulación]. *Sea* $\sigma(\alpha_1, \ldots, \alpha_{n-1})$ *cualquier término con a lo más* $n - 1$ *variables libres y sea* $\mu(\alpha_1, \ldots, \alpha_n)$ *cualquier término con a lo más* n *variables libres. Entonces un término* $\tau(\alpha_1, \ldots, \alpha_n)$ *puede definirse por el esquema recurrente:*

(i) $\tau(\alpha_1, \ldots, \alpha_{n-1}, 0) = \sigma(\alpha_1, \ldots, \alpha_{n-1})$,

(ii) *para todo* β,
$\tau(\alpha_1, \ldots, \alpha_{n-1}, \beta') = \mu(\alpha_1, \ldots, \alpha_{n-1}, \tau(\alpha_1, \ldots, \alpha_{n-1}, \beta))$,

(iii) *para todo ordinal límite* β,
$\tau(\alpha_1, \ldots, \alpha_{n-1}, \beta) = \bigcup_{\gamma \in \beta} \tau(\alpha_1, \ldots, \alpha_{n-1}, \gamma)$.

Las variables libres $\alpha_1, \ldots, \alpha_{n-1}$ son los parámetros de recurrencia de este teorema. Dado este teorema, podemos usar en § 7.2 los esquemas apropiados de recurrencia mismos para definir la adición, la multiplicación y la exponenciación ordinales.

EJERCICIOS

1. Demostrar el teorema 3.
2. Demostrar el teorema 4.
3. Demostrar el teorema 5.
4. Completar la demostración del teorema 6, demostrando que F es única.
5. Dar otro ejemplo diferente del dado en el texto para una función F del teorema 6 que no satisfaga

$$F(\beta) = \bigcup_{\gamma \in \beta} F(\gamma)$$

para un ordinal límite β.

6. En la demostración del teorema 7, necesitamos saber que el recorrido de H es un conjunto para saber que H, como una función, es un conjunto bien definido. ¿De qué conjunto es el recorrido de H un subconjunto?
7. Demostrar el teorema 9.
8. Demostrar el teorema 10.
9. Demostrar el teorema 11.
10. Demostrar el teorema 12.

§ 7.2 Elementos de aritmética ordinal. Nuestra intención es dar las principales orientaciones acerca de la aritmética ordinal, pero no desarrollarla en un sentido completo (en relación con esto véase Sierpinski [1928] y Bachmann [1955]).

Los teoremas iniciales sobre adición ordinal y multiplicación se asimilan a los de la adición y la multiplicación entre enteros dados en § 5.2. Las demostraciones por inducción transfinita juegan aquí el papel que las demostraciones por inducción jugaban en § 5.2. Consideradas como generalizaciones de las operaciones entre enteros, el hecho más destacado acerca de la adición y de la multiplicación ordinales es el de que ellas no son conmutativas. En contraste, la adición y la multiplicación cardinales son conmutativas, como vimos en § 4.3. Podemos usar el teorema 12 para introducir la adición ordinal por el esquema de recurrencia dado ya en § 7.1.

Definición 2. *La operación de adición ordinal se define por medio del siguiente esquema recurrente:*

(i) $\alpha + 0 = \alpha$,

(ii) $\alpha + \beta' = (\alpha + \beta)'$,

(iii) *si β es un ordinal límite,*

$$\alpha + \beta = \bigcup_{\gamma \in \beta} (\alpha + \gamma).$$

La existencia de $\bigcup_{\gamma \in \beta} (\alpha + \beta)$ en el sentido intuitivo apropiado se sigue de los resultados anteriores consignados en § 7.1. El papel de (iii) se aclarará en las demostraciones subsiguientes de los teoremas de esta sección.

Dejamos como un ejercicio la demostración del siguiente resultado, el cual usamos periódicamente sin mención explícita.

Teorema 13. *$\alpha + \beta$ es un ordinal.*

Nos referimos ahora a la aritmética elemental de la adición ordinal. Muchas de las demostraciones exhiben métodos típicos de argumentar por medio de inducción transfinita.

Teorema 14. $\alpha + 0 = 0 + \alpha = \alpha$.

Demostración. Por (i) de la definición tenemos inmediatamente que

$$\alpha + 0 = \alpha.$$

La demostración de que $0 + \alpha = \alpha$ es más complicada; ella exhibe las tres partes típicas de un argumento directo por medio de inducción transfinita (como se formuló en el teorema 4).

Parte 1. $\alpha = 0$. Necesitamos demostrar:

$$0 + 0 = 0.$$

Parte 2. Suponiendo $0 + \alpha = \alpha$, necesitamos demostrar:

$$0 + \alpha' = \alpha'.$$

Parte 3. Suponiendo que α es un ordinal límite y que para $\beta < \alpha$,

$$0 + \beta = \beta,$$

necesitamos demostrar:

$$0 + \alpha = \alpha.$$

La parte 1 se sigue de una vez de (i) de la definición de adición.

Para establecer la parte 2, usamos (ii) de la definición y nuestra hipótesis inductiva:

$$\begin{aligned} 0 + \alpha' &= (0 + \alpha)' \\ &= \alpha'. \end{aligned}$$

Para demostrar la parte 3 usamos (iii) de la definición:

$$\begin{aligned} 0 + \alpha &= \bigcup_{\beta \in \alpha} (0 + \beta) \\ &= \bigcup_{\beta \in \alpha} \beta \quad \text{por la hipótesis inductiva} \\ &= \alpha \quad \text{por el teorema 3} \end{aligned}$$

ya que α es un ordinal límite, $\bigcup \alpha = \alpha$.

Habiendo demostrado las partes 1 a 3, concluimos inmediatamente, por inducción transfinita (teorema 4), que nuestro teorema es válido para todos los ordinales. Q.E.D.

El siguiente teorema es una consecuencia inmediata de la definición de adición ordinal.

Teorema 15. $\alpha + \beta' = (\alpha + \beta)'$.

Haciendo $\beta = 0$, tenemos:

Teorema 16. $\alpha + 1 = \alpha'$.

El teorema siguiente establece que la adición ordinal es *monótona a derecha* con respecto a la relación *menor que.*

Teorema 17. *Si $\beta < \gamma$, entonces $\alpha + \beta < \alpha + \gamma$.*

Demostración. La demostración se hace por inducción transfinita sobre γ.

Parte 1. Si $\gamma = 0$, la hipótesis del teorema es falsa, así que el teorema se cumple vacíamente.

Parte 2. Supongamos que tenemos que, si $\beta < \gamma$, entonces

$$\alpha + \beta < \alpha + \gamma.$$

Para demostrar que el teorema se cumple para el sucesor de γ tenemos que considerar dos casos.

Caso 1. $\beta < \gamma$. Entonces tenemos:

$$\alpha + \beta < \alpha + \gamma,$$

pero

$$\alpha + \gamma < (\alpha + \gamma)'$$

y, por el teorema 15,

$$(\alpha + \gamma)' = \alpha + \gamma',$$

de donde, por transitividad,

$$\alpha + \beta < \alpha + \gamma'.$$

Caso 2. $\beta = \gamma$. Entonces tenemos las dos consecuencias siguientes:

$$\beta < \gamma'$$

y

$$\alpha + \beta = \alpha + \gamma,$$

pero, como antes,

$$\alpha + \gamma < \alpha + \gamma',$$

por consiguiente,

$$\alpha + \beta < \alpha + \gamma'.$$

(Nótese que no necesitamos considerar el caso de $\gamma < \beta$, pues por el teorema 15 de § 5.1 tenemos entonces $\gamma' \leq \beta$ y el teorema se cumple vacíamente.)

Parte 3. Supongamos ahora que γ es un ordinal límite (esta es la única parte de la hipótesis inductiva que necesitamos para esta parte). Ya que $\beta < \gamma$, desde luego, $\beta \in \gamma$. Pero por (iii) de la definición de adición,

$$\alpha + \gamma = \bigcup_{\delta \in \gamma} (\alpha + \delta),$$

y así, en vista de la definición 15 de § 2.6 y el teorema 13,

$$\alpha + \gamma = \bigcup A$$

donde

$$A = \{\eta\colon \exists \delta \in \gamma \;\&\; \eta = \alpha + \delta\}.$$

Ahora, $\beta \in \gamma$, de donde $\beta' \in \gamma$ (pues γ es un ordinal límite), así que

$$\alpha + \beta' \in A.$$

pero

$$(\alpha + \beta)' = \alpha + \beta'$$

y

$$\alpha + \beta \in (\alpha + \beta)',$$

de donde

$$\alpha + \beta \in \bigcup A,$$

o sea,

$$\alpha + \beta \in \alpha + \gamma. \qquad \text{Q.E.D.}$$

Por otra parte, la adición ordinal no es monótona a izquierda con respecto a *menor que,* esto es, no tenemos en general,

si $\alpha < \beta$, entonces $\alpha + \gamma < \beta + \gamma$.

Por ejemplo,

$$1 < 2,$$

pero

$$1 + \omega = 2 + \omega.$$

(La verificación de este hecho se deja como ejercicio.)

Como una consecuencia inmediata del teorema precedente y del teorema 14, tenemos:

Teorema 18. *Si* $\beta > 0$, *entonces* $\alpha + \beta > \alpha$.

Podemos también deducir fácilmente una ley de cancelación a izquierda a partir de la monotonía a derecha de la adición ordinal. El ejemplo dado antes del teorema 18 muestra que la cancelación a derecha no es válida.

Teorema 19. *Si* $\alpha + \beta = \alpha + \gamma$, *entonces* $\beta = \gamma$.

Demostración. Supongamos $\beta \neq \gamma$. Para precisar, sea $\beta < \gamma$. Entonces por el teorema 17,

$$\alpha + \beta < \alpha + \gamma,$$

lo que contradice la hipótesis del teorema. Q.E.D.

Damos una ley monotónica a izquierda para la adición ordinal con respecto a $\leq$. La demostración es similar a la del teorema 17 y se deja como ejercicio.

Teorema 20. *Si* $\alpha \leq \beta$, *entonces* $\alpha + \gamma \leq \beta + \gamma$.

Como consecuencia inmediata tenemos:

Teorema 21. $\alpha + \beta \geq \beta$.

Ahora demostramos un hecho útil acerca de ordinales límite.

Teorema 22. *Si β es un ordinal límite, entonces $\alpha + \beta$ es un ordinal límite.*

Demostración. Supongamos que $\alpha + \beta$ no es un ordinal límite. En virtud del teorema 21, $\alpha + \beta \neq 0$. Por consiguiente, existe un γ tal que

$$\text{(1)} \qquad \gamma' = \alpha + \beta, \\ = \bigcup_{\delta \in \beta} (\alpha + \delta),$$

en virtud de (iii) de la definición de adición. Entonces,

$$\gamma \in \bigcup_{\delta \in \beta} (\alpha + \delta),$$

por tanto, existe un $\delta_1 \in \beta$ tal que

$$\gamma \in \alpha + \delta_1,$$

por consiguiente,

$$\text{(2)} \qquad \gamma' < (\alpha + \delta_1)' = \alpha + \delta_1'.$$

(1) y (2) dan:

$$\alpha + \beta < \alpha + \delta_1',$$

se sigue, a partir de la contrapositiva del teorema 20, que

$$\beta < \delta_1',$$

lo que es absurdo, porque $\delta_1 \in \beta$, así que $\delta_1' \in \beta$. Q.E.D.

El teorema siguiente afirma que una propiedad básica de la adición entre enteros es válida también para la adición ordinal general.

Teorema 23. *Si $\alpha \leq \beta$, entonces existe un γ único tal que $\alpha + \gamma = \beta$.*

Demostración. Si $\alpha = \beta$, tomamos $\gamma = 0$. Supongamos entonces que $\alpha < \beta$. Ahora, por el teorema 21,

$$\alpha + \beta \geq \beta.$$

Sea γ el menor ordinal tal que

$$\text{(1)} \qquad \alpha + \gamma \geq \beta.$$

Afirmo que, en efecto,

$$\alpha + \gamma = \beta,$$

pues supongamos que

$$\alpha + \gamma > \beta.$$

Claramente $\gamma \neq 0$, así que hay dos casos para considerar. Primero, supongamos que γ tiene un precedente inmediato $\gamma - 1$. Entonces,

$$\alpha + \gamma = \alpha + (\gamma - 1)' = (\alpha + (\gamma - 1))',$$

de donde, por el teorema 15 de § 5.3,

$$\alpha + \gamma > \alpha + (\gamma - 1) \geq \beta,$$

contrario a la suposición de que γ es el menor ordinal que satisface (1).

Segundo, supongamos que γ es un ordinal límite. Entonces por las hipótesis básicas sobre γ, para cada $\delta < \gamma$,

$$\alpha + \delta < \beta,$$

y, por consiguiente, por el teorema 63 de § 2.6,

$$\bigcup_{\delta \in \gamma} (\alpha + \delta) \subseteq \beta,$$

así que,

$$\bigcup_{\delta \in \gamma} (\alpha + \delta) \leq \beta.$$

Pero

$$\alpha + \gamma = \bigcup_{\delta \in \gamma} (\alpha + \delta),$$

y así tenemos

$$\alpha + \gamma \leq \beta,$$

lo que se combina con (1) para dar

$$\alpha + \gamma = \beta.$$

Que γ es único se sigue de una vez a partir de la ley de cancelación a izquierda; esto es, dado

$$\alpha + \gamma_1 = \alpha + \gamma_2 = \beta,$$

en virtud del teorema 19

$$\gamma_1 = \gamma_2. \qquad \text{Q.E.D.}$$

Por el mismo método de argumentación usada en la demostración que precede, es fácil establecer:

Teorema 24. *No existe ordinal γ alguno tal que, para todo $\delta < \beta$,*

$$\alpha + \delta < \gamma < \alpha + \beta.$$

Este teorema dice, en otras palabras, que $\alpha + \beta$ es el primer ordinal mayor que $\alpha + \delta$ para todo $\delta < \beta$.

Se muestra que la adición ordinal no es conmutativa por medio del simple contraejemplo:

$$1 + \omega \neq \omega + 1.$$

Por otra parte, es asociativa.

Teorema 25. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma.$

Demostración. La demostración se hace por inducción transfinita sobre γ.

Parte 1. En virtud del teorema 14

$$\begin{aligned}\alpha + (\beta + 0) &= \alpha + \beta \\ &= (\alpha + \beta) + 0.\end{aligned}$$

Parte 2. Nuestra hipótesis inductiva dice

$$(1) \qquad \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma,$$

y entonces tenemos las siguientes identidades:

$$\begin{aligned}\alpha + (\beta + \gamma') &= \alpha + (\beta + \gamma)' \\ &\qquad \text{por el teorema 15} \\ &= (\alpha + (\beta + \gamma))' \\ &\qquad \text{por el teorema 15} \\ &= ((\alpha + \beta) + \gamma)' \\ &\qquad \text{por (1)} \\ &= (\alpha + \beta) + \gamma' \\ &\qquad \text{por el teorema 15.}\end{aligned}$$

Parte 3. La hipótesis inductiva es la de que γ es un ordinal límite y, para todo $\delta \in \gamma$,

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

A partir de la definición de adición y del hecho que $\beta + \gamma$ es un ordinal límite (teorema 22), tenemos:

$$\begin{aligned}\alpha + (\beta + \gamma) &= \bigcup_{\theta \in \beta + \gamma} (\alpha + \theta) \\ &= \bigcup \{\eta : (\exists\, \theta)(\theta \in \beta + \gamma \,\&\, \eta = \alpha + \theta\} \\ &\qquad \text{por definición.}\end{aligned}$$

Pero ya que cada ordinal η tiene como elementos todos los ordinales más pequeños, podemos sustituir en la última expresión '$\theta \in \beta + \gamma$' por '$\beta + \delta \in \beta + \gamma$', y obtenemos

$$\begin{aligned}\alpha + (\beta + \gamma) &= \bigcup \{\, \eta : (\exists\, \delta)\,(\beta + \delta \in \beta \\ &\qquad + \gamma \,\&\, \eta = \alpha + (\beta + \delta))\,\} \\ &= \bigcup \{\, \eta : (\exists\, \delta)(\delta \in \gamma \,\&\, \eta = \\ &\qquad \alpha + (\beta + \delta))\,\} \\ &\qquad \text{por los teoremas} \\ &\qquad \text{17 y 20} \\ &= \bigcup_{\delta \in \gamma} \alpha + (\beta + \delta) \\ &\qquad \text{por definición} \\ &= \bigcup_{\delta \in \gamma} (\alpha + \beta) + \delta \\ &\qquad \text{por la hipótesis} \\ &\qquad \text{inductiva} \\ &= (\alpha + \beta) + \gamma. \qquad \text{Q.E.D.}\end{aligned}$$

Ahora nos referimos a la definición de multiplicación ordinal y a un cierto número de teoremas elementales acerca de esta operación. La definición, como la de adición, simplemente generaliza la definición correspondiente para los enteros. Nótese que se sigue la convención acostumbrada de yuxtaponer para denotar multiplicación. Ocasionalmente se usa un punto para efectos de claridad.

Definición 3. *La operación de multiplicación ordinal se define por medio del siguiente esquema recurrente:*

(i) $\alpha \cdot 0 = 0$,

(ii) $\alpha \cdot \beta' = \alpha \cdot \beta + \alpha$,

(iii) *si β es un ordinal límite,*

$$\alpha \cdot \beta = \bigcup_{\gamma \in \beta} \alpha \cdot \gamma.$$

Las demostraciones de varios de los teoremas se han dejado como ejercicios.

Teorema 26. *$\alpha \cdot \beta$ es un ordinal.*

Teorema 27. $0 \cdot \alpha = 0$.

Teorema 28. $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$.

Ahora demostramos que la multiplicación ordinal, como la adición ordinal, es monónica a derecha con respecto a *menor que.* En el caso de la multiplicación tenemos que agregar la condición de que $\alpha > 0$.

Teorema 29. *Si $\alpha > 0$ y $\beta < \gamma$, entonces $\alpha\beta < \alpha\gamma$.*

Demostración. La demostración, como la del teorema correspondiente para la adición (teorema 17), se hace por inducción transfinita sobre γ.

Parte 1. Si $\gamma = 0$, la hipótesis del teorema es siempre falsa y el teorema se cumple vacíamente.

Parte 2. La hipótesis inductiva para esta parte es idéntica en apariencia a la formulación del teorema. Para demostrar que el teorema es válido para el sucesor de γ hay que considerar dos casos.

Caso 1. $\beta < \gamma$. Entonces tenemos:

$$\alpha\beta < \alpha\gamma,$$

pero

$$\alpha\gamma' = \alpha\gamma + \alpha,$$

y puesto que $\alpha > 0$, en virtud del teorema 18,

$$\alpha\gamma < \alpha\gamma',$$

de donde, por transitividad,

$$\alpha\beta < \alpha\gamma'.$$

Caso 2. $\beta = \gamma$. Por tanto, $\alpha\beta = \alpha\gamma$. Entonces,

$$\alpha\gamma' = \alpha\gamma + \alpha > \alpha\gamma.$$

Luego,

$$\alpha\gamma' > \alpha\beta.$$

Parte 3. Como en el caso del teorema correspondiente para la adición, la única parte de la hipótesis inductiva que necesitamos es la de que γ es un ordinal límite. Puesto que $\beta < \gamma$, tenemos que $\beta \in \gamma$. Pero es una propiedad fundamental de la multiplicación ordinal la de que

$$\alpha\gamma = \bigcup_{\delta \in \gamma} \alpha\delta,$$

de donde, por un argumento exactamente igual al usado en la demostración del teorema 17,

$$\alpha\beta \in \alpha\gamma,$$

o sea,

$$\alpha\beta < \alpha\gamma. \qquad \text{Q.E.D.}$$

Como una consecuencia fácil del teorema 29, tenemos:

Teorema 30. *Si $\alpha \neq 0$ y $\beta \neq 0$, entonces $\alpha\beta \neq 0$.*

Como otro resultado inmediato tenemos una ley de cancelación a izquierda, previsto que $\alpha > 0$.

Teorema 31. *Si $\alpha\beta = \alpha\gamma$ y $\alpha > 0$, entonces $\beta = \gamma$.*

Un contra-ejemplo para la cancelación a derecha está dado por la igualdad

$$2\omega = 3\omega.$$

Como una propiedad esperada de los ordinales límite tenemos:

Teorema 32. *Si β es un ordinal límite y $\alpha > 0$, entonces $\alpha\beta$ es un ordinal límite.*

La demostración se deja como ejercicio, como la del correspondiente "dual a izquierda".

Teorema 33. *Si α es un ordinal límite y $\beta > 0$, entonces $\alpha\beta$ es un ordinal límite.*

Ahora demostramos el importante hecho de que la multiplicación es distributiva a izquierda con respecto a la adición.

Teorema 34. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Demostración. La demostración se hace por inducción transfinita sobre γ. Suponemos $\alpha \neq 0$ (para la parte 3), pues de otro modo la demostración es trivial, en vista del teorema 27.

Parte 1. $\alpha(\beta + 0) = \alpha\beta = \alpha\beta + 0 = \alpha\beta + \alpha \cdot 0$.

Parte 2. Tenemos las siguientes identidades:

$$\begin{aligned}
\alpha(\beta + \gamma') &= \alpha(\beta + \gamma)' \\
&\quad \text{por el teorema 15} \\
&= \alpha(\beta + \gamma) + \alpha \\
&\quad \text{por (ii) de la definición 3} \\
&= (\alpha\beta + \alpha\gamma) + \alpha \\
&\quad \text{por la hipótesis inductiva} \\
&= \alpha\beta + (\alpha\gamma + \alpha) \\
&\quad \text{por asociatividad} \\
&= \alpha\beta + \alpha\gamma' \\
&\quad \text{por (ii) de la definición 3.}
\end{aligned}$$

Parte 3. Supongamos que γ es un ordinal límite. Entonces, por el teorema 22, $\beta + \gamma$ es también un ordinal límite, de donde, a partir de la definición de multiplicación,

$$\begin{aligned}
\alpha(\beta + \gamma) &= \bigcup_{\theta \in \beta + \gamma} \alpha\theta \\
&= \bigcup_{\theta \in \bigcup_{\delta \in \gamma} (\beta + \delta)} \alpha\theta \\
&\qquad \text{por definición de adición} \\
&= \bigcup \{\eta : (\exists\theta)(\theta \in \bigcup_{\delta \in \gamma} (\beta + \delta) \,\&\, \eta = \alpha\theta)\}
\end{aligned}$$

por definición

$$= \bigcup \{\eta\colon (\exists\theta)(\exists\delta)(\delta \in \gamma \,\&\, \theta \in \beta + \delta \,\&\, \eta = \alpha\theta)\}.$$

En virtud del teorema 29, puesto que, si $\theta < \beta$, entonces $\alpha\theta < \alpha(\beta + \delta)$ para cualquier $\delta \in \gamma$, así que podemos considerar solamente valores θ para los cuales existe un $\delta \in \gamma$ tal que $\theta = \beta + \delta$, porque si $\theta_1 < \beta$ y $\theta_2 = \beta + \delta$ para algún δ, entonces cualquier elemento de $\alpha\theta_1$ es también un elemento de $\alpha\theta_2$ y la unión de la familia indicada de conjuntos permanece inalterada si se omite θ_1. Por tanto, podemos reemplazar la última identidad por

$$\alpha(\beta + \gamma) = \bigcup \{\eta\colon (\exists\delta)(\delta \in \gamma \,\&\, \eta = \alpha(\beta + \delta)\}$$

$$= \bigcup_{\delta\in\gamma} \alpha(\beta + \delta)$$

por definición

$$= \bigcup_{\delta\in\gamma} (\alpha\beta + \alpha\delta)$$

por la hipótesis inductiva

$$= \bigcup \{\eta\colon (\exists\delta)(\delta \in \gamma \,\&\, \eta = \alpha\beta + \alpha\delta)\}$$

por definición

$$= \bigcup \{\eta\colon (\exists\theta)(\theta \in \alpha\gamma \,\&\, \eta = \alpha\beta + \theta)\}$$

por lógica cuantificacional, la hipótesis de que $\alpha \neq 0$ y el teorema 29

$$= \bigcup_{\theta\in\alpha\gamma} (\alpha\beta + \theta)$$

por definición

$$= \alpha\beta + \alpha\gamma$$

por definición de adición y el teorema 32.

Q.E.D.

Un ejemplo simple que muestra que la multiplicación no es distributiva a derecha es el siguiente, cuya verificación se deja como ejercicio:

$$(1 + 1)\omega \neq 1 \cdot \omega + 1 \cdot \omega.$$

La demostración de la asociatividad de la multiplicación ordinal se hace por inducción transfinita sobre γ. Esta demostración se deja como ejercicio.

Teorema 35. $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

Del carácter de las definiciones de la adición y la multiplicación ordinales, es obvia la definición de exponenciación ordinal.

Definición 4. *La operación de exponenciación ordinal se define por medio del siguiente esquema recurrente:*

(i) $\alpha^0 = 1$,

(ii) $\alpha^{\beta'} = \alpha^\beta \cdot \alpha$,

(iii) *si β es un ordinal límite y $\alpha > 0$, entonces*

$$\alpha^\beta = \bigcup_{\gamma\in\beta} \alpha^\gamma,$$

(iv) *si β es un ordinal límite y $\alpha = 0$, entonces*

$$\alpha^\beta = 0.$$

Las demostraciones de los teoremas sobre exponenciación se han dejado como ejercicios.

Teorema 36. $\alpha^1 = \alpha$.

Teorema 37. *Si* $\beta > 0$, *entonces* $0^\beta = 0$.

Teorema 38. $1^\alpha = 1$.

Teorema 39. $\alpha^{\beta+\gamma} = \alpha^\beta\ \alpha^\gamma$.

Teorema 40. $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$.

Por otra parte, no siempre tenemos:

$$(\alpha\beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma,$$

pues

$$(\omega \cdot 2)^2 \neq \omega^2 \cdot 2^2.$$

Teorema 41. *Si* $\alpha > 1$ *y* $\beta < \gamma$, *entonces* $\alpha^\beta < \alpha^\gamma$.

Por inducción transfinita sobre β podemos también demostrar:

Teorema 42. *Si* $\alpha > 1$ *y* $\beta > 1$, *entonces*

$$\alpha + \beta \leq \alpha\beta \leq \alpha^\beta.$$

A partir de los teoremas y contra-ejemplos dados atrás en esta sección, puede verse que la aritmética de la adición, multiplicación y exponenciación ordinales difiere en tres aspectos principales de la aritmética de las operaciones correspondientes entre enteros. (i) La adición y la multiplicación ordinales no son conmutativas. (ii) La multiplicación ordinal no es distributiva a la derecha, con respecto a la adición ordinal, o sea que no siempre se tiene:

(1) $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma.$

(iii) La regla de exponentes

(2) $(\alpha \cdot \beta)^\gamma = \alpha^\gamma \beta^\gamma$

a veces falla. De las tres, (i) es más importante, pues si suponemos que la adición y la multiplicación son conmutativas, podemos deducir (1) y (2). Vale la pena mencionar también que ciertas operaciones sobre 0 y 1 que son ordinariamente indefinidas en el análisis están definidas en la aritmética ordinal. Por ejemplo, 0^0, ∞^0, 1^∞ no están definidos en análisis, pero aquí:

$$0^0 = \omega^0 = \alpha^0 = 1,$$
$$1^\omega = 1^\beta = 1.$$

Varias investigaciones se han dedicado a proseguir el desarrollo de la aritmética ordinal, según los lineamientos de los resultados clásicos de la teoría de números. En este sentido se da algún material en los ejercicios del final de esta sección. Aquí nos restringimos a enunciar que los análogos del "último teorema" de Fermat y la Hipótesis de Goldbach se sabe que son falsos en la teoría de números ordinales (Sierpinski [1950]). En teoría elemental de números el "último teorema" de Fermat es la aserción de que, para $n \geq 3$, no existen números naturales a, b, c tales que

$$a^n + b^n = c^n.$$

La verdad o falsedad de esta aserción es uno de los famosos problemas abiertos de la teoría de números. El análogo para la teoría de números ordinales es falso. Para cualquier ordinal $\mu \geq 1$ existen números ordinales α, β, γ tales que

$$\alpha^\mu + \beta^\mu = \gamma^\mu.$$

En particular, si μ tiene un precedente inmediato (esto es, μ no es un ordinal límite), entonces, para $\xi \geq 1$

$$(\omega^\xi)^\mu + (\omega^\xi \cdot 2)^\mu = (\omega^\xi \cdot 3)^\mu.$$

Si μ es un ordinal límite, entonces, para $\xi \geq 1$,

$$(\omega^\xi)^\mu + (\omega^{\xi \cdot \mu})^\mu = (\omega^{\xi \cdot \mu} + 1)^\mu.$$

La Hipótesis de Goldbach es la de que todo número natural par >2 es la suma de dos números primos. Sobre la base de la definición obvia de números ordinales primos, la hipótesis es falsa para números ordinales. Puede demostrarse que $\omega + 10$ no es una suma tal.

Ahora nos referimos a las operaciones suma y producto infinitos. Desde un punto de vista formal, estas dos son operaciones unarias sobre sucesiones de ordinales. Hemos usado la noción de μ-sucesión en la demostración del teorema 7; la definimos de nuevo aquí.

Definición 5. *Una μ-sucesión de ordinales es una función cuyo dominio es el ordinal μ y cuyo recorrido es un conjunto de ordinales.*

Las sucesiones en el sentido ordinario del análisis son ω-sucesiones. Usamos una notación muy acostumbrada para μ-sucesiones, a saber $\{\alpha_\xi\}_{\xi<\mu}$, donde α_ξ es el ξ-ésimo término de la sucesión.

Definición 6. *La operación suma infinita para ordinales se define para cualquier μ- sucesión de ordinales $\{\alpha_\xi\}_{\xi<\mu}$ por medio del siguiente esquema recurrente:*

(i) $\sum_{\xi<0} \alpha_\xi = 0,$

(ii) *si $\nu < \mu$, entonces*

$$\sum_{\xi<\nu'} \alpha_\xi = \sum_{\xi<\nu} \alpha_\xi + \alpha_\nu,$$

(iii) *si ν es un ordinal límite y $\nu \leq \mu$, entonces*

$$\sum_{\xi<\nu} \alpha_\xi = \bigcup_{\eta\in\nu} \sum_{\xi<\eta} \alpha_\xi.$$

Es quizás importante notar la forma que el esquema recurrente tomaría si usáramos una notación funcional común para μ-sucesiones. Así, sea f cualquier sucesión de ordinales para μ-sucesiones. O sea que f es cualquier sucesión de ordinales. Entonces,

$$\Sigma f|0 = 0,$$
$$\Sigma f|\nu' = \Sigma f|\nu + f(\nu),$$

para ν un ordinal límite

$$\Sigma f|\nu = \bigcup_{\eta \in \nu} \Sigma f|\eta.$$

A pesar de la mayor simplicidad de la última notación, usaremos en lo que sigue la notación más acostumbrada introducida en la definición 6.

Por inducción transfinita podemos demostrar que cualquier ordinal puede obtenerse por agregación iterada de 1.

Teorema 43. *Sea* $\{\alpha_\xi\}_{\xi<\mu}$ *la* μ*-sucesión tal que, para todo* $\xi < \mu$, $\alpha_\xi = 1$. *Entonces,*

$$\mu = \sum_{\xi<\mu} \alpha_\xi.$$

Demostración. Usando el teorema 4, procedemos por inducción sobre μ.

Parte 1. Si $\mu=0$, entonces, por (i) de la definición precedente,

$$\sum_{\xi<0} \alpha_\xi = 0.$$

Parte 2. Supongamos que el teorema vale para μ. Ahora, por (ii) de la definición,

$$\begin{aligned} \sum_{\xi<\mu'} \alpha_\xi &= \sum_{\xi<\mu} \alpha_\xi + 1 \\ &= \mu + 1 \qquad \text{por la hipótesis inductiva} \\ &= \mu'. \end{aligned}$$

Parte 3. Si μ es un ordinal límite, entonces, por (iii) de la definición,

$$\begin{aligned} \sum_{\xi<\mu} \alpha_\xi &= \bigcup_{\eta\in\mu} \sum_{\xi<\eta} \alpha_\xi \\ &= \bigcup_{\eta\in\mu} \eta \qquad \text{por la hipótesis inductiva} \\ &= \mu \qquad \text{por el teorema 3.} \end{aligned}$$

Q.E.D.

Podemos demostrar también que la multiplicación es adición iterada.

Teorema 44. *Sea* $\{\alpha_\xi\}_{\xi<\beta}$ *la* β*-sucesión tal que, para todo* $\xi < \beta$, $\alpha_\xi = \alpha$. *Entonces,*

$$\alpha \cdot \beta = \sum_{\xi<\beta} \alpha_\xi.$$

Demostración. Como en la última demostración, procedemos por inducción transfinita.

Parte 1. $\beta = 0$. Por (i) de la definición 6,

(1) $$\sum_{\xi<0} \alpha_\xi = 0,$$

y por el teorema 27,

(2) $$\alpha \cdot 0 = 0,$$

y así, (1) y (2) establecen la parte 1.

Parte 2. Supongamos que el teorema es válido para β. Entonces, por (ii) de la definición 6,

$$\begin{aligned} \sum_{\xi<\beta'} \alpha_\xi &= \sum_{\xi<\beta} \alpha_\xi + \alpha_\beta \\ &= \sum_{\xi<\beta} \alpha_\xi + \alpha \qquad \text{por la hipótesis del teorema} \\ &= \alpha \cdot \beta + \alpha \qquad \text{por la hipótesis inductiva} \\ &= \alpha \cdot \beta' \qquad \text{por la definición 3.} \end{aligned}$$

Parte 3. Si β es un ordinal límite, entonces

$$\begin{aligned} \alpha \cdot \beta &= \bigcup_{\gamma\in\beta} \alpha \cdot \gamma \qquad \text{por definición de multiplicación} \\ &= \bigcup_{\gamma\in\beta} \sum_{\xi<\gamma} \alpha_\xi \qquad \text{por la hipótesis inductiva} \\ &= \sum_{\xi<\beta} \alpha_\xi \qquad \text{por (iii) de la definición 6.} \end{aligned}$$

Q.E.D.

El teorema siguiente es semejante al teorema 22 en su formulación y demostración; así que la demostración se deja como ejercicio.

Teorema 45. *Si* μ *es un ordinal límite y, para todo* $\xi < \mu$, $\alpha_\xi \neq 0$, *entonces* $\sum_{\xi<\mu} \alpha_\xi$ *es un ordinal límite.*

Para formular una ley asociativa de la suma de una sucesión de ordinales, existe cierta dificultad para hallar una notación apropiada. Para ilustrar estas ideas, consideremos la suma finita:

$$\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5.$$

Si

$$\begin{aligned} \gamma_0 &= \alpha_0 + \alpha_1 + \alpha_2 \\ \gamma_1 &= \alpha_3 + \alpha_4 \\ \gamma_2 &= \alpha_5, \end{aligned}$$

la ley asociativa general afirma que

$$\gamma_0 + \gamma_1 + \gamma_2 = \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5.$$

Es más simple introducir una notación para las sumas parciales de los sub-índices que para los γ_ξ directamente. Sea β_0 el número de términos α de γ, esto es, tres; en general, sea β el número de términos α de γ. Aquí,

$$\beta_0 = 3$$
$$\beta_1 = 2$$
$$\beta_2 = 1.$$

Sean σ_ν las sumas parciales de los β. Así,

$$\sigma_\nu = \sum_{\eta<\nu} \beta.$$

En nuestro ejemplo,

$$\sigma_0 = 0$$
$$\sigma_1 = 3$$
$$\sigma_2 = \beta_0 + \beta_1 = 5$$
$$\sigma_3 = \beta_0 + \beta_1 + \beta_2 = 6.$$

Nuestro ejemplo puede entonces representarse por:

$$\sum_{\xi<6} \alpha_\xi = \sum_{\nu<3} \Big(\sum_{\xi<\beta_\nu} \alpha_{\sigma_\nu+\xi}\Big).$$

En esta notación tenemos la ley asociativa general siguiente.

Teorema 46. *Si* $\lambda = \sum_{\eta<\mu} \beta_\eta$ *y, para* $v < \mu$, $\sigma_\nu = \sum_{\eta<\nu} \beta_\eta$, *entonces*

$$\sum_{\xi<\lambda} \alpha_\xi = \sum_{\nu<\mu} \Big(\sum_{\xi<\beta_\xi} \alpha_{\sigma_\nu+\xi}\Big).$$

Demostración. Sin pérdida de generalidad podemos suponer que,para todo $\eta < \mu$, $\beta_\eta \neq 0$. Procedemos por inducción transfinita sobre μ.

Parte 1. $\mu = 0$. La demostración es inmediata.

Parte 2. Supongamos que el teorema es válido para μ.

Entonces,

$$\lambda = \sum_{\eta<\mu'} \beta_\eta = \sum_{\eta<\mu} \beta_\eta + \beta_\mu.$$

Además,

$$\sum_{\xi<\lambda} \alpha_\xi = \sum_{\xi<\sigma_\mu+\beta_\mu} \alpha_\xi$$
$$= \sum_{\xi<\sigma_\mu} \alpha_\xi + \sum_{\xi<\beta_\mu} \alpha_{\sigma_\mu+\xi}$$
$$= \sum_{\nu<\mu} \Big(\sum_{\xi<\beta_\nu} \alpha_{\sigma_\nu+\xi}\Big) + \sum_{\xi<\beta_\mu} \alpha_{\sigma_\mu+\xi} \quad \text{por la hipótesis inductiva}$$
$$= \sum_{\nu<\mu'} \Big(\sum_{\xi<\beta_\nu} \alpha_{\sigma_\nu+\xi}\Big).$$

Parte 3. Sea μ un ordinal límite. Entonces,

(1) $$\lambda = \sum_{\eta<\mu} \beta_\eta = \bigcup_{\delta<\mu} \sum_{\eta<\delta} \beta_\eta.$$

En virtud del teorema 45, λ es un ordinal límite.

Tenemos entonces:

$$\sum_{\xi<\lambda} \alpha_\xi = \bigcup_{\delta<\mu} \sum_{\xi<\sigma_\delta} \alpha_\xi$$
por (i) y (iii) de la definición 6
$$= \bigcup_{\delta<\mu} \sum_{\nu<\delta} \Big(\sum_{\xi<\beta_\nu} \alpha_{\sigma_\nu+\xi}\Big)$$
por la hipótesis inductiva
$$= \sum_{\nu<\mu} \Big(\sum_{\xi<\beta_\nu} \alpha_{\sigma_\nu+\xi}\Big)$$
por (iii) de la definición 6.

Q.E.D.

Puede usarse la ley asociativa general para la adición para demostrar una ley distributiva general, de la cual el teorema 34 es un caso especial. En relación con esto debe notarse que la adición binaria se obtiene de la operación Σ considerando solamente sucesiones de longitud dos. La demostración de esta ley distributiva se deja como ejercicio.

Teorema 47.

$$\alpha \cdot \sum_{\eta<\mu} \beta_\eta = \sum_{\eta<\mu} \alpha \cdot \beta_\eta.$$

Análogo a la definición de suma de una sucesión de ordinales, definimos el *producto* de una sucesión tal.

Definición 7. *La operación producto infinito para ordinales se define para cualquier* μ*-sucesión de ordinales* $\{\alpha_\xi\}_{\xi<\mu}$ *por medio del siguiente esquema recurrente:*

(i) $\prod_{\xi<0} \alpha_\xi = 1,$

(ii) *si* $\nu < \mu$, *entonces*

$$\prod_{\xi<\nu'} \alpha_\xi = \prod_{\xi<\nu} \alpha_\xi \cdot \alpha_\nu,$$

(iii) *si* ν *es un ordinal límite y* $\nu \leq \mu$, *entonces*

$$\prod_{\xi<\nu} \alpha_\xi = \bigcup_{\eta\in\nu} \prod_{\xi<\eta} \alpha_\xi,$$

a menos que $\alpha_\xi = 0$ *para algún* $\xi < \nu$, *en cuyo caso* $\prod_{\xi<\nu} \alpha_\xi = 0$.

Formulamos sin demostración algunos teoremas sobre esta operación de producto infinito. Las demostraciones son análogas en estructura a las que se dan sobre sumas infinitas.

Teorema 48. *Sea* $\{\alpha_\xi\}_{\xi<\beta}$ *la* β*-sucesión tal que, para todo* $\xi < \beta$, $\alpha_\xi = \alpha$. *Entonces,*

$$\alpha^\beta = \prod_{\xi<\beta} \alpha_\xi.$$

El siguiente teorema establece la ley asociativa general para productos.

Teorema 49. *Si* $\lambda = \sum_{\eta<\mu} \beta_\eta$ *y, para* $\nu < \mu$ $\sigma_\nu = \sum_{\eta<\nu} \beta_\eta$, *entonces*

$$\prod_{\xi<\lambda} \alpha_\xi = \prod_{\nu<\mu} \left(\prod_{\xi<\beta_\nu} \alpha_{\sigma_\nu+\xi}\right).$$

Hay también una ley de potencias, de la cual

$$\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$$

es un caso especial.

Teorema 50. *Si* $\lambda = \sum_{\eta<\mu} \beta_\eta$, *entonces* α^λ

$$= \prod_{\eta<\mu} \alpha^{\beta_\eta}.$$

Como teorema final resumimos algunos resultados particulares interesantes y las demostraciones de ellos que no son difíciles.

Teorema 51.

(i) *Si para* $\xi < \omega$, $\alpha_\xi = \xi + 1$, *entonces*

$$\sum_{\xi<\omega} \alpha_\xi = 1 + 2 + 3 + \cdots = \omega$$

$$\prod_{\xi<\omega} \alpha_\xi = 1 \cdot 2 \cdot 3 \cdot \cdots = \omega.$$

(ii) *Si para* $\xi < \omega$, $\alpha_\xi = n$, *entonces*

$$\sum_{\xi<\omega} \alpha_\xi = n + n + n + \cdots = \omega \text{ para } n > 0,$$

$$\prod_{\xi<\omega} \alpha_\xi = n \cdot n \cdot n \cdot \cdots = \omega \text{ para } n > 1.$$

(iii) *Si para* $\xi < \omega$, $\alpha_\xi = \omega$, *entonces*

$$\sum_{\xi<\omega} \alpha_\xi = \omega + \omega + \omega + \cdots = \omega^2$$

$$\prod_{\xi<\omega} \alpha_\xi = \omega \cdot \omega \cdot \omega \cdot \cdots = \omega^\omega.$$

Es conveniente notar que las cinco operaciones sobre números ordinales definidas en esta sección tienen cláusulas esencialmente idénticas en sus definiens con respecto a los ordinales límite. Podemos definir la noción de una sucesión transfinita de ordinales que tiene un límite y entonces definir la continuidad de una función de ordinales. Usando estas ideas, la cláusula que acabamos de mencionar puede sustituirse por el requerimiento de que la función sea continua (en la variable apropiada si es una función de varias variables).

Brevemente indicamos las definiciones pertinentes. Sea $\{\alpha_\xi\}_{\xi<\mu}$ una μ-sucesión de ordinales donde μ es un ordinal límite. Entonces, α es el *límite* de esta sucesión; en símbolos,

$$\alpha = \lim_{\xi<\mu} \alpha_\xi$$

si y solamente si, para todo $\xi < \mu$, $\alpha_\xi \leq \alpha$ y para todo $\beta < \alpha$ existe un $\nu < \mu$ tal que, si $\nu < \xi$, entonces $\beta < \alpha_\xi$.

Sea f una función sobre algún ordinal α y tal que su recorrido sea un conjunto de ordinales. Entonces, f es *continua* si y solamente si, para todo número límite $\lambda < \alpha$,

$$f(\lambda) = \lim_{\xi<\lambda} f(\xi).$$

Así, sin usar una notación rigurosa, podemos afirmar que $\alpha + \beta$ es continua en β, y de modo similar para $\alpha \cdot \beta$ y α^β. Por otra parte, estas tres operaciones no son continuas en α, pues

$$\lim_{\xi<\omega} (\xi + 1) = \omega \neq \omega + 1$$

$$\lim_{\xi<\omega} (\xi \cdot 2) = \omega \neq \omega \cdot 2$$

$$\lim_{\xi<\omega} \xi^2 = \omega \neq \omega^2.$$

EJERCICIOS

1. Se han dado varios contra-ejemplos sin demostración a través de esta sección. Haciendo uso de teoremas cualesquiera, demostrar los siguientes:
   (a) $1 + \omega = 2 + \omega$
   (b) $n + \omega = \omega$
   (c) $1 + \omega < \omega + 1$
   (d) si $n \neq 0$, entonces $n + \omega < \omega + n$
   (e) $2\omega = 3\omega$
   (f) si $n \neq 0$, entonces $n\omega = \omega$
   (g) $2\omega < \omega \cdot 2$
   (h) $\omega \cdot 2 = \omega + \omega$
   (i) $(1 + 1)\omega < 1 \cdot \omega + 1 \cdot \omega$
2. Demostrar los teoremas 20 y 21.
3. ¿Es verdadero el recíproco del teorema 22? Si lo es, demostrarlo; si no, dar un contra-ejemplo.
4. Demostrar el teorema 27.
5. Demostrar el teorema 28.
6. Demostrar los teoremas 30 y 31.
7. Demostrar los teoremas 32 y 33.
8. Demostrar el teorema 35.
9. Demostrar las dos leyes de cancelación siguientes para la multiplicación ordinal:
   (a) Si $\alpha\beta > \alpha\gamma$, entonces $\beta > \gamma$.
   (b) Si $\alpha\gamma > \beta\gamma$, entonces $\alpha > \beta$.
10. Demostrar que, si $\gamma < \alpha\beta$, entonces existe un único $\alpha \; < \alpha$ y un único $\beta \; <' \beta$ tales que $\gamma = \alpha\beta \; + \alpha$.
11. Si $\alpha > 0$, entonces para cualquier ordinal β existe un único γ y un único $\delta < \alpha$ tales que,
$$\beta = \alpha\gamma + \delta.$$
12. Si α es un ordinal límite, entonces existe un único β tal que $\alpha = \omega\beta$.
13. Demostrar el teorema 36.
14. Demostrar el teorema 37.
15. Demostrar el teorema 38.
16. Demostrar el teorema 39.
17. Demostrar el teorema 40.
18. Demostrar que $(\omega \cdot 2)^2 \neq \omega^2 \cdot 2^2$.
19. Demostrar el teorema 41.
20. Demostrar el teorema 42.
21. Demostrar el teorema 45.
22. Demostrar el teorema 47.
23. Demostrar el teorema 48.
24. Demostrar el teorema 49.
25. Demostrar el teorema 50.
26. Demostrar el teorema 51.
27. Demostrar que, si para $\xi < \omega$, $\alpha_\xi = \omega^2$, entonces
$$\sum_{\xi < \omega} \alpha_\xi = \omega^2 + \omega^2 + \omega^2 + \cdots = \omega^3.$$
28. Demostrar que, si para $\xi < \omega + \omega$, $\alpha_\xi = \omega$, entonces
$$\prod_{\xi < \omega + \omega} \alpha_\xi = \omega \cdot \omega \cdot \omega \cdots \omega \cdot \omega \cdot \omega \cdots = \omega^{\omega + \omega}.$$
29. Demostrar que, si para $\xi < \omega$, $\alpha_\xi = \omega^\xi$, entonces
$$\sum_{\xi < \omega} \alpha_\xi = 1 + \omega + \omega^2 + \omega^3 + \cdots = \omega^\omega.$$
30. Definimos: β es un residuo de γ si y solamente si $\beta > 0$ y existe un α tal que $\alpha + \beta = \gamma$.
Demostrar que si $\alpha > \beta$, α y β son residuos de γ, entonces β es un residuo de α.
31. Definimos: α es aditivamente indescomponible si y solamente si $\alpha > 0$ y α no es la suma de dos ordinales menores que él.
   (a) ¿Cuáles enteros, si los hay, son aditivamente indescomponibles?
   (b) Demostrar que ω es aditivamente indescomponible.
   (c) ¿Cuál es el más pequeño ordinal mayor que ω que es aditivamente indescomponible?
   (d) Usando la definición del ejercicio 30, caracterizar los residuos de un ordinal aditivamente indescomponible.
   (e) Demostrar que, si β es aditivamente indescomponible y $\alpha > \beta$, entonces $\alpha + \beta = \beta$.
   (f) Demostrar que, si $\beta > 1$ es aditivamente indescomponible y $\alpha > 0$, entonces $\alpha\beta$ es aditivamente indescomponible.
   (g) Demostrar que, para todo α, ω^α es aditivamente indescomponible.

§ 7.3 Números cardinales de nuevo y alefs.

Sin usar el axioma especial para cardinales o el axioma de escogencia, se puede hacer una cierta cantidad de teoría de los números cardinales, definiendo los números cardinales como ordinales iniciales. Un ordinal inicial es uno que no es equipotente con algún ordinal menor que él. Sin embargo, sin el axioma de escogencia no podemos mostrar que todo conjunto tiene un número cardinal y así no podemos desarrollar una aritmética cardinal razonable.

Por otra parte, podemos definir los *alefs*. En teoría de conjuntos intuitiva clásica, un alef es el número cardinal de un conjunto infinito bien ordenado. Esta no será nuestra definición, pero vendrá próximamente como un teorema. En otras palabras, definiremos los alefs puramente en términos de números ordinales y entonces demostraremos (en la sección siguiente) que el número cardinal de cualquier conjunto infinito bien ordenado es un alef. Es verdad que $\aleph_0$ fue definido en la definición 28 de § 5.3 como el número cardinal de ω (esta definición dependía del axioma especial para cardinales), pero el carácter real de los alefs, como la sucesión de números cardinales transfinitos no fue indicada en manera alguna por esta definición inicial.

Para evitar cualquier confusión se hace énfasis en que el material de esta sección es completamente independiente de § 4.3, § 4.4 y § 5.3, los cuales dependen del axioma especial para cardinales.

Definición 8. *x es un número cardinal si y solamente si x es un ordinal y, para todo ordinal α, si $x \approx \alpha$, entonces $x \leq \alpha$.*

Tenemos dos teoremas sencillos:

Teorema 52. *Todo número natural es un número cardinal.*

Teorema 53. *ω es un número cardinal.*

También tenemos, sin el axioma de escogencia, la ley de tricotomía para números cardinales.

Teorema 54. *Si α y β son números cardinales entonces se cumple exactamente una de las siguientes posibilidades: $\alpha \prec \beta$, $\beta \prec \alpha$, $\alpha = \beta$.*

Demostración. Ya que α y β son ordinales, entonces, $\alpha \subseteq \beta$ o $\beta \subseteq \alpha$. Así, por el teorema 16 de § 4.1, se cumple $\alpha \preceq \beta$ o $\beta \preceq \alpha$, a partir de lo cual el teorema se sigue fácilmente.

Q.E.D.

El hecho de que el teorema 54 pueda demostrarse sin el axioma de escogencia no significa que se pueda demostrar sin ese axioma la tricotomía, en términos de equipotencia, para conjuntos arbitrarios.

Definimos los cardinales transfinitos de una manera que está de acuerdo con la definición 27 de § 5.3. La última definición afirma que un cardinal transfinito es uno que es el cardinal de un conjunto infinito, según Dedekind. La presente definición requiere que el cardinal sea $\geq \omega$, lo que implica que ω sea un subconjunto de él. Pero de acuerdo con los teoremas 47 y 48 de § 5.3, todos, y no solamente aquellos conjuntos que tienen un subconjunto enumerable como ω, son infinitos según Dedekind.

Definición 9. *x es un cardinal transfinito si y solamente si x es un número cardinal y $x \geq \omega$.*

Uno de nuestros objetivos es demostrar que no hay un cardinal transfinito mayor que todos. Para este fin, asociamos con cada conjunto el conjunto de ordinales equipotente o menos potente que él. Esta noción será el artificio que nos permite evitar el axioma de escogencia; el enfoque se originó con Hartogs [1915], quien hace uso en su demostración del hecho que la ley de tricotomía implica que todo conjunto es bien ordenado. (La usamos también para la demostración correspondiente en el capítulo siguiente.)

Definición 10.

$$\mathcal{K}(A) = \{\alpha\colon \alpha \preceq A\}.$$

Se requiere una aplicación más bien sutil del esquema axiomático de sustitución para demostrar que $\mathcal{K}(A)$ no es vacío. El esquema axiomático de separación no puede usarse, pues no existe el conjunto apropiado de ordinales. Además, la aplicación del esquema axiomático de sustitución no es directa, porque, para un subconjunto dado B de A, puede haber muchos ordinales diferentes equipotentes con él; esto es, no podemos usar simplemente, para B en el conjunto potencia de A,

$$\varphi(B, \alpha) \text{ si y solamente si } B \approx \alpha.$$

Un camino indirecto pero exitoso es considerar subconjuntos *bien ordenados* de A como se muestra en la siguiente demostración.

Teorema 55. *$\alpha \in \mathcal{K}(A)$ si y solamente si $\alpha \preceq A$.*

Demostración. Para comenzar, es claro que

(1) $\alpha \preceq A$ si y solamente si existen conjuntos B y R tales que

(i) $B \subseteq A$,

(ii) R bien-ordena B

(iii) $\langle \alpha, \mathcal{E}\alpha\rangle$ es semejante a $\langle B, R\rangle$.

(La semejanza fue definida en § 5.1.) Ahora definimos:

(2) $\mathcal{W}(A) = \{\langle B, R\rangle\colon B \subseteq A \;\&\; R$ bien-ordena $B \;\&\; R \subseteq A \times A\}$.

En virtud del esquema axiomático de separación y del axioma del conjunto potencia se sigue que

(3) $x \in \mathcal{W}(A)$ si y solamente si existen conjuntos B y R tales que

(i) $x = \langle B, R\rangle$,
(ii) $B \subseteq A$,
(iii) R bien-ordena B.

La demostración de (3) se sigue de tomar como el conjunto básico para el esquema axiomático de separación

$$(\mathcal{P}A) \times \mathcal{P}(A \times A),$$

puesto que

(4) $$B \in \mathcal{P}A$$

y

(5) $$R \in \mathcal{P}(A \times A).$$

Para la aplicación del esquema axiomático de sustitución tomamos ahora para φ:

(6) $\varphi(x, \alpha)$ si y solamente si x es semejante a $\langle\alpha, \mathcal{E}\alpha\rangle$.

Claramente, a partir de las propiedades fundamentales de los ordinales, dos ordinales diferentes no puden ser semejantes bajo la relación de pertenencia, así que $\varphi(x, \alpha)$ y $\varphi(x, \beta)$, entonces $\alpha = \beta$. Por consiguiente, por el esquema axiomático de sustitución existe un conjunto C tal que

(7) $\alpha \in C \leftrightarrow (\exists x)(x \in \mathcal{W}(A)$ & x es semejante a $\langle\alpha, \mathcal{E}\alpha\rangle)$.

De (1), (3) y (7) se sigue que

(8) $\alpha \in C$ si y solamente si $\alpha \preceq A$,

y el teorema se sigue a partir de (8). Q.E.D.

Teorema 56. $\mathcal{H}(A)$ *es un ordinal.*

Demostración. Si $\alpha \in \mathcal{H}(A)$ y $\beta < \alpha$, entonces $\beta \in \mathcal{H}(A)$, pues si $\alpha \in \mathcal{H}(A)$, entonces existe un subconjunto B de A tal que $\alpha \approx B$ bajo alguna función, digamos f; pero entonces $f|\beta$ garantiza que $\beta \in \mathcal{H}(A)$. Por consiguiente, $\mathcal{H}(A)$ es completo y, puesto que es un conjunto de ordinales, es conexo por la relación de pertenencia. De donde, siendo completo y conexo, es un ordinal. Q.E.D.

El siguiente teorema afirma que no $\mathcal{H}(A) \preceq A$; debe notarse que el axioma de escogencia se necesita para demostrar el resultado más fuerte $A \prec \mathcal{H}(A)$, aun cuando esto puede establecerse para conjuntos bien ordenados, así que *a fortiori* para ordinales, sin el axioma de escogencia.

Teorema 57. *No* $\mathcal{H}(A) \preceq A$.

Demostración. Puesto que $\mathcal{H}(A)$ es un ordinal, en virtud del teorema 55,

(1) $\mathcal{H}(A) \preceq A$ si y solamente si $\mathcal{H}(A) \in \mathcal{H}(A)$,

pero ningún ordinal es un elemento de sí mismo; en consecuencia el teorema se sigue, de una vez, a partir de (1). Q.E.D.

Ahora demostramos que $\mathcal{H}(A)$ es el menor ordinal que tiene la propiedad de no ser $\preceq A$.

Teorema 58. *Si no* $\alpha \preceq A$, *entonces* $(A) \preceq \alpha$.

Demostración. Supongamos que $\alpha < \mathcal{H}(A)$. Entonces, puesto que $\mathcal{H}(A)$ es un ordinal, $\alpha \in \mathcal{H}(A)$; pero entonces, en virtud de la definición de $\mathcal{H}(A)$, $\alpha \preceq A$, lo que contradice la hipótesis del teorema. Q.E.D.

Se sigue fácilmente a partir del teorema que se acaba de demostrar, que

Teorema 59. $\mathcal{H}(A)$ *es un número cardinal.*

Además, los teoremas que hemos demostrado llevan directamente a la consecuencia, interesante filosóficamente, de que

Teorema 60. *No existe ningún número cardinal que sea mayor que todos.*

Demostración. Supongamos, si es posible, que hubiera un número cardinal mayor que todos, digamos α. Entonces, por el teorema 57,

(1) $$\text{no } \mathcal{H}(\alpha) \preceq \alpha,$$

y por el teorema 59, $\mathcal{H}(\alpha)$ es un número cardinal, de donde, por el teorema 54 y (1),

$$\alpha \prec \mathcal{H}(\alpha),$$

lo que es contrario a nuestra suposición acerca de α. Q.E.D.

Para definir los alefs es útil introducir primero la noción del menor ordinal que satisface una fórmula. Habría sido posible una consideración anterior de esta noción y en realidad habría sido conveniente, ocasionalmente.

Esquema de definición 11.
$\mu_\alpha(\varphi(\alpha)) = \beta \leftrightarrow [\varphi(\beta) \;\&\; (\forall\, \gamma)(\varphi(\gamma) \rightarrow \beta \leq \gamma)] \vee [-(\exists\, \alpha)\varphi(\alpha) \;\&\; \beta = 0]$.

Así,

$$\mu_\alpha(\alpha > 2) = 3,$$
$$\mu_\beta(\beta > \alpha) = \alpha + 1.$$

Se demuestra fácilmente que

Esquema teoremático 61. *Si $\varphi(\beta)$, entonces $\mu_\alpha(\varphi(\alpha)) \leq \beta$.*

Esquema teoremático 62. *Si $(\exists\ \alpha)\varphi(\alpha)$, entonces $\varphi(\mu_\alpha(\varphi(\alpha)))$.*

Ahora definimos:

Definición 12. *La operación alef se define por medio del siguiente esquema recurrente:**

(i) $\aleph_0 = \omega$,
(ii) $\aleph_{\alpha'} = \mu_\beta(\beta > \aleph_\alpha)$,
(iii) *si α es un ordinal límite,*

$$\aleph_\alpha = \bigcup_{\beta \in \alpha} \aleph_\beta.$$

Primero demostramos:

Teorema 63. *Existe un β tal que, para todo γ, si $\gamma \in \alpha$, entonces $\beta > \aleph_\gamma$.*

Demostración. Necesitamos considerar solamente $\alpha > 0$. En virtud del esquema axiomático de sustitución existe un conjunto no vacío A, tal que

$$A = \{\eta\colon (\exists\gamma)(\gamma \in \alpha \;\&\; \eta = \aleph_\gamma)\}.$$

Ahora, a partir de resultados anteriores sobre ordinales, $\bigcup A$ es un ordinal y además, si $\eta \in A$ entonces

$$\eta \leq \bigcup A.$$

Así que, si no hubiera $\beta > \bigcup A$, entonces $\mu_\xi(\xi \leq \bigcup A \;\&\; \xi \simeq \bigcup A)$ sería el mayor cardinal transfinito, contrario al teorema 60. Q.E.D.

* Para estar de acuerdo con la notación tradicional escribimos '$\aleph_\alpha$' en vez de '$\aleph(\alpha)$'.

Se sigue de este teorema, de la definición 12 y de algunos resultados anteriores sobre ordinales, que

Teorema 64. *Si $\alpha > 0$, entonces*

$$\aleph_\alpha = \mu_\beta((\forall\gamma)(\gamma \in \alpha \rightarrow \beta > \aleph_\gamma)).$$

Este teorema, junto con (i) de la definición, puede usarse como la definición de la operación alef.

Nos restringimos a unos pocos resultados ulteriores que se formulan sin demostración.

A partir de la definición 12 y de los teoremas 63 y 64 se sigue inmediatamente que

Teorema 65. *$\aleph_\alpha$ es un cardinal transfinito.*

Teorema 66. *Si $\alpha < \beta$, entonces $\aleph_\alpha < \aleph_\beta$.*

Teorema 67. *No existe cardinal transfinito β tal que $\aleph_\alpha < \beta < \aleph_{\alpha+1}$.*

La demostración del siguiente teorema presenta mayor dificultad.

Teorema 68. *Todo cardinal transfinito es un alef, o sea, para todo cardinal transfinito α existe un β tal que $\alpha = \aleph_\beta$.*

Retornamos brevemente a los alefs al final de la sección siguiente. Mencionamos aquí que cualquier número ordinal cuya cardinalidad sea $\aleph_0$ se dice que es un *número ordinal de la segunda clase.* (Los ordinales finitos son los números de la primera clase.) Se conocen muchos resultados matemáticos acerca de los números naturales de la segunda clase, pero están sin resolver muchos problemas difíciles que conciernen a ellos. (Algunas referencias son: Sierpinski [1928], Church y Kleene [1937], Church [1938], Denjoy [1946].)

EJERCICIOS

1. Demostrar los teoremas 52 y 53.
2. Dar una demostración detallada de (1) en la demostración del teorema 55.
3. Demostrar el teorema 59.
4. Demostrar que, si $A \subseteq B$, entonces $\mathcal{K}(A) \leq \mathcal{K}(B)$.
5. ¿Es verdadero que, si $A \subseteq B$, entonces $\mathcal{K}(A) < \mathcal{K}(B)$?
6. ¿Es verdadero que, si $A \subset B$, entonces $\mathcal{K}(A) \prec \mathcal{K}(B)$?
7. ¿Es verdadero que $\mathcal{K}(A \cup B) = \mathcal{K}(A) + \mathcal{K}(B)$?

8. Demostrar el teorema 61.
9. Demostrar el teorema 62.
10. Demostrar el teorema 64.
11. Demostrar el teorema 66.
12. Demostrar el teorema 67.
13. **Demostrar que, si α es un ordinal límite, entonces** no existe cardinal transfinito β tal que para todo $\gamma \in \alpha$, $\aleph_\gamma < \beta < \aleph_\alpha$.
14. Para todo cardinal α existe un ordinal β tal que $\alpha < \aleph_\beta$.
15. Demostrar el teorema 68.

§ 7.4 Conjuntos bien ordenados. Para comenzar, podemos formular el principio de inducción transfinita para conjuntos bien ordenados. La demostración es semejante a la del teorema 1. Debe notarse que el teorema 69 implica el teorema 1.

> **Teorema 69.** [Principio de inducción transfinita: cuarta formulación]. *Si*
> (i) *R bien-ordena A,*
> (ii) $(\forall y)[y \in A \;\&\; (\forall x)(x \in A \;\&\; x\,R\,y \rightarrow x \in B) \rightarrow y \in B]$, *entonces* $A \subseteq B$.

El enunciado (y la demostración) de un principio para conjuntos bien ordenados semejante al teorema 4 se deja como ejercicio.

Formulamos pero no demostramos que, si un conjunto ordenado satisface el principio de inducción transfinita, entonces es bien ordenado. Informalmente hablando, este teorema, combinado con el teorema 69, muestra que para aplicar la inducción transfinita a un conjunto ordenado es necesario y suficiente que el conjunto sea bien ordenado.

> **Teorema 70.** *Sea R una ordenación estricta simple de A y supongamos que A tiene un R-primer elemento. Además, sean A y R tales que, para cualquier conjunto B, si* $(\forall y)[y \in A \;\&\; (\forall x)(x \in A \;\&\; xRy \rightarrow x \in B) \rightarrow y \in B]$, *entonces* $A \subseteq B$. *Entonces R bien-ordena A.*

Usando la noción de un segmento, que fue introducida en la definición 32 del capítulo 3, podemos formular la recurrencia transfinita de una manera semejante al teorema 8.

> **Esquema teoremático 71.** [Recurrencia transfinita: sexta formulación]. *Sea* τ *cualquier término y supongamos que R bien-ordena A. Entonces existe una única función F sobre A tal que, para todo elemento x de A,*
> $$F(x) = \tau(F|\ \mathcal{S}\ (A,R,x)).$$

Usaremos este teorema en el capítulo 8, en la demostración de que, si todo conjunto puede ser bien ordenado, entonces es válido el lema de Zorn.

La noción de una *función creciente,* familiar en los contextos numéricos, se generaliza fácilmente a conjuntos ordenados.

> **Definición 13.** *f es una función creciente sobre* $\mathfrak{A} = \langle A, R\rangle$ *si y solamente si*
> (i) *f es una función sobre A.*
> (ii) $\mathcal{R}f \subseteq A$,
> (iii) *si* $x,y \in A$ *y* $x\,R\,y$, *entonces* $f(x)$ $Rf(y)$.

Ahora demostramos un teorema fundamental para tales funciones.

> **Teorema 72.** *Si R bien-ordena A y f es una función creciente sobre* $\langle A,R\rangle$, *entonces no existe elemento x alguno en A tal que* $f(x)Rx$.

Demostración. Supongamos, por vía de contradicción, que hubiera un elemento x en A tal que

(1) $$f(x)Rx.$$

Sea

$$B = \{x: f(x)\ Rx\}.$$

En virtud de (1), $B \neq 0$, o sea que tiene un R-primer elemento, digamos x_1. Así que tenemos,

(2) $$f(x_1)Rx_1.$$

Sea

(3) $$x_0 = f(x_1),$$

por tanto,

$$x_0 R x_1,$$

y puesto que f es creciente,

(4) $$f(x_0)Rf(x_1).$$

A partir de (3) y (4) tenemos entonces,

$$f(x_0)Rx_0,$$

pero entonces $x_0 \in B$ y x_1 no es el R-primer elemento de B, lo que es absurdo. Q.E.D.

Ahora formulamos algunos teoremas relativos a la semejanza (definición 1 de § 5.1) y a las funciones crecientes.

Teorema 73. *Si R bien-ordena A y f es una función creciente sobre $\langle A,R\rangle$, entonces $\langle A,R\rangle$ es semejante, bajo f, a $\langle \mathcal{R}f,R\rangle$.*

Demostración. Necesitamos verificar (a) — (c) de la definición 1 de § 5.1; (b) se sigue de una vez de la definición de funciones crecientes. Para establecer (a), esto es, que f es 1-1, considérense dos elementos diferentes x, $y \in A$. Puesto que $x \neq y$, debemos tener xRy o yRx. Para precisar, supongamos que xRy. Pero entonces, $f(x)Rf(y)$ y ya que R es antireflexiva, $f(x) \neq f(y)$. En relación con (c) ya tenemos que, si xRy, entonces $f(x)Rf(y)$. Necesitamos la recíproca. Supongamos $f(x)$ $Rf(y)$. Entonces, $x \neq y$ en virtud de la antireflexividad de R. Si $y\ R\ x$, entonces $f(y)R$ $f(x)$, pero esto es imposible, ya que R es asimétrica. Por tanto, ya que R es conexa, xRy. Q.E.D.

Dejamos como ejercicio la demostración de lo que es esencialmente el recíproco.

Teorema 74. *Si R bien-ordena A, B es un subconjunto de A y $\langle A,R\rangle$ es semejante bajo f a $\langle B,R\rangle$, entonces f es una función creciente sobre $\langle A,R\rangle$.*

Podemos usar los teoremas 72 y 74 para demostrar:

Teorema 75. *Si R bien-ordena A y $\langle A,R\rangle$ es semejante a sí mismo bajo f, entonces f es la función idéntica $\mathcal{I}A$.*

Demostración. Necesitamos demostrar que, para todo x en A,

$$f(x) = x.$$

Sobre la base de los teoremas 72 y 74 no existe elemento x en A tal que

$$(1) \qquad f(x)Rx.$$

Supongamos ahora que hay un elemento x en A tal que

$$(2) \qquad xRf(x).$$

En vista de la hipótesis del teorema, la función inversa f^{-1} es tal que $\langle A,R\rangle$ es semejante a sí mismo bajo f^{-1}. Así, en vista del teorema 74,

$$f^{-1}(x)Rf^{-1}(f(x)),$$

esto es,

$$(3) \qquad f^{-1}(x)Rx,$$

pero (3) es imposible de acuerdo con el teorema 72. Así que nuestra suposición es falsa y no valen ni (1) ni (2), para ningún x de A. Puesto que R es conexa en A, debe seguirse que $f(x) = x$. Q.E.D.

Se sigue, a partir del teorema que se acaba de demostrar, que

Teorema 76. *Si R bien-ordena A y S bien-ordena B, entonces existe a lo más una función f tal que $\langle A,R\rangle$ es semejante, bajo f, a $\langle B,S\rangle$.*

En otras palabras, dos conjuntos bien ordenados pueden ser semejantes a lo más en un respecto.

La aplicación relativa al teorema precedente da:

Teorema 77. *Ningún conjunto bien ordenado es semejante a uno de sus segmentos; esto es, si R bien-ordena A, entonces, para cualquier x en A, $\langle A,R\rangle$ no es semejante a $\langle \mathcal{S}(A,R,x),R\rangle$.*

Tenemos también:

Teorema 78. *Si R bien-ordena A, entonces el conjunto de todos los R-segmentos de A, ordenados por inclusión propia, es semejante a $\langle A,R\rangle$.*

(La inclusión propia restringida a subconjuntos de A se hace fácilmente una relación de la teoría de conjuntos, digamos $\subset|A$, correspondiente a $\mathcal{I}A$, $\mathcal{E}A$, $<|A$.)

Teorema 79. *Si*

(i) *R bien-ordena A,*
(ii) *S bien-ordena B,*
(iii) *para cada x en A existe un y en B tal que $\langle \mathcal{S}(A,R,x),R\rangle$ es semejante a $\langle \mathcal{S}(B,S,y),S\rangle$,*

(iv) *para cada y en B existe un x en A tal que* $\langle \mathcal{S}(B,S,y),S\rangle$ *es semejante a* $\langle \mathcal{S}(A,R,x),R\rangle$,

entonces, $\mathfrak{A} = \langle A, R\rangle$ *es semejante a* $\mathfrak{B} = \langle B, S\rangle$.

Demostración. Sobre la base del teorema 77, es claro que (iii) y (iv) implican que existe una función 1-1 f de A sobre B tal que $\langle \mathcal{S}(A,R,x),R\rangle$ es semejante a $\langle \mathcal{S}(B,S,f(x)),S\rangle$. Queremos mostrar que $\langle A,R\rangle$ es semejante, bajo f, a $\langle B,S\rangle$. Sea $x_1, x_2 \in A$, con x_1Rx_2. Entonces,

(1) $$\mathcal{S}(A,R,x_1) \subset \mathcal{S}(A,R,x_2),$$

por tanto, por la hipótesis y el teorema 77,

(2) $$\mathcal{S}(B,S,f(x_1)) \subset \mathcal{S}(B,S,f(x_2))$$

así que, a partir de la definición de segmentos,

(3) $$f(x_1)Sf(x_2).$$

Además, (3) implica (2), el cuál implica (1). Así, para $x_1,x_2 \in A$, x_1Rx_2 si y solamente si $f(x_1)Sf(x_2)$, lo que establece el teorema.

Q.E.D.

Ahora estamos en posición de demostrar el *teorema fundamental para conjuntos bien ordenados,* a saber, que dos conjuntos bien ordenados son semejantes, o uno es semejante a un segmento del otro. (Debe notarse que este teorema es el análogo, para conjuntos bien ordenados, de la ley de tricotomía para conjuntos no ordenados.) La demostración de este teorema fundamental no depende del esquema axiomático de sustitución.

Teorema 80. *Supongamos que R bien-ordena A y S bien-ordena B. Entonces vale una sola de las siguientes situaciones*

(i) $\langle A, R\rangle$ *es semejante a* $\langle B, S\rangle$,

(ii) *existe un x en A tal que* $\langle \mathcal{S}(A,R,x), R\rangle$ *es semejante a* $\langle B, S\rangle$, *o*

(iii) *existe un y en B tal que* $\langle A, R\rangle$ *es semejante a* $\langle \mathcal{S}(B,S,y), S\rangle$.

Demostración. Supongamos que $\langle A, R\rangle$ no es semejante a $\langle B, S\rangle$. Entonces, sobre la base del teorema 79, existe un segmento $\mathcal{S}(A,R,x)$ con x en A, que no es semejante a segmento alguno $\mathcal{S}(B,S,y)$ para y en B, o bien, existe un segmento $\mathcal{S}(B,S,y)$ no semejante a segmento alguno $\mathcal{S}(A,R,x)$. Queremos demostrar que la primera alternativa implica (ii); la demostración que la segunda implica (iii) es idéntica.

Sea $\mathcal{S}(A,R,x_0)$ el segmento más pequeño no semejante a segmento alguno $\mathcal{S}(B,S,y)$ para algún y en B. (La buena ordenación de los segmentos de $\langle A, R\rangle$ o $\langle B, S\rangle$ se sigue del teorema 78; en relación con esto véase también el ejercicio 6 al final de esta sección.) Queremos demostrar que todo segmento $\mathcal{S}(B,S,y)$ es semejante a algún segmento $\mathcal{S}(A,R,x)$. Supongamos, por vía de contradicción, que hubiera un segmento $\mathcal{S}(B,S,y)$ no semejante a algún segmento $\mathcal{S}(A,R,x)$. Sea $\mathcal{S}(B,S,y_0)$ el más pequeño de tales segmentos. Entonces, cada segmento $\mathcal{S}(B,S,y)$ del conjunto $\mathcal{S}(B,S,y_0)$ es semejante a un segmento $\mathcal{S}(A,R,x)$, y en cada caso,

(1) $$\mathcal{S}(A,R,x) \subset \mathcal{S}(A,R,x_0),$$

pues, de otra manera, $\mathcal{S}(A,R,x_0)$ sería semejante a algún segmento $\mathcal{S}(B,S,y)$, contrario a nuestra hipótesis acerca de él. Por un argumento correspondiente, todo segmento $\mathcal{S}(A,R,x)$ del conjunto $\mathcal{S}(A,R,x_0)$ es semejante a algún segmento del conjunto $\mathcal{S}(B,S,y_0)$: por tanto, podemos usar el teorema 79 para demostrar que $\mathcal{S}(A,R,x_0)$ es semejante a $\mathcal{S}(B,S,y_0)$. Pero esta semejanza contradice la definición de $\mathcal{S}(A,R,x_0)$, y concluimos que nuestra suposición de que existe un segmento tal como $\mathcal{S}(B,S,y_0)$ es falsa. En consecuencia concluimos que todo segmento $\mathcal{S}(B,S,y)$ es semejante a algún segmento $\mathcal{S}(A,R,x)$ y por el argumento que establece (1), $\mathcal{S}(A,R,x)$ debe ser un segmento de $\mathcal{S}(A,R,x_0)$. Ya que $\mathcal{S}(A,R,x_0)$ es el más pequeño segmento de A no semejante a algún segmento de B, concluimos, en virtud del teorema 79, de nuevo, que $\langle \mathcal{S}(A,R,x_0), R\rangle$ es semejante a $\langle B,S\rangle$, lo que establece (ii), previsto que se cumpla la primera de las dos alternativas formuladas al comienzo de la demostración. Q.E.D.

Ahora demostramos un teorema de representación para conjuntos bien ordenados en términos de números ordinales. La demostración usa el esquema axiomático de sustitución.

Teorema 81. *Si R bien-ordena A, entonces existe un único ordinal α tal que $\langle A, R\rangle$ es semejante a $\langle \alpha, \mathcal{E}\alpha\rangle$.*

Demostración. La idea de la demostración se opone a la discusión informal de § 5.1 dirigida a justificar intuitivamente la construcción de los ordinales debida a von Neumann. Usamos la sexta formulación de la recurrencia transfinita (teorema 71) para definir sobre A una función f tal que, para x en A,

(1) $f(x) = \mathcal{R}(f| \mathcal{S}(A,R,x))$.

Debemos demostrar que f es 1-1. Supongamos que no. Entonces, sea y el menor elemento bajo la ordenación R de A tal que, para algún x, xRy y $f(x) = f(y)$. Se sigue, de una vez, a partir de (1) que, entonces,

(2) $f(x) = f(x')$,

donde x' es el sucesor inmediato de x bajo la ordenación R; pero es claro también, a partir de (1), que

(3) $f(x') = f(x) \cup \{f(x)\}$.

Sin embargo, (2) y (3) son conjuntamente absurdas, de donde concluimos:

(4) f es 1-1.

En segundo lugar, no es difícil demostrar que $f(x)$ es un ordinal, a saber, que es completo y conexo por la relación de pertenencia. Sea B un elemento de $f(x)$, o sea,

$$B \in \mathcal{R}(f|\mathcal{S}(A,R,x)),$$

por tanto, debe haber un y en $\mathcal{S}(A, R, x)$, o sea, yRx, tal que $f(y) = B$; pero, claramente, si yRx, entonces $\mathcal{S}(A,R,y) \subset \mathcal{S}(A,R,x)$, así que

$$B = \mathcal{R}(f|\mathcal{S}(A,R,y)) \subseteq \mathcal{R}(f|\mathcal{S}(A,R,x)),$$

lo que muestra que B es un subconjunto de $f(x)$ y, por tanto, que $f(x)$ es completo. Para mostrar que $f(x)$ es conexo por la relación de pertenencia, sea $A,B \in f(x)$. Entonces existen elementos a y b en $\mathcal{S}(A,R,x)$ tales que $f(a) = A$ y $f(b) = B$. Supongamos $A \neq B$. Entonces, $a \neq b$ y por la conectividad de R en A, aRb o bRa. Si aRb, entonces, en virtud de (1) y del carácter 1-1 de f, $f(a) \in f(b)$. Si bRa, entonces $f(b) \in f(a)$, de donde $f(x)$ es conexo por la relación de pertenencia. Además, el argumento que se acaba de dar muestra que, si xRy, entonces, $f(x), \in f(y)$. Por otra parte, si $f(x) \in f(y)$, entonces xRy. Pues supongamos que no. Entonces, $x=y$ o yRx, a partir de la conectividad de R. Si lo primero, entonces $f(x) = f(y)$; si lo último, $f(y) \in f(x)$; cualquiera de las dos conclusiones es absurda bajo la hipótesis de que $f(x) \in f(y)$. Así hemos establecido para cualesquiera x,y en A

(5) xRy si y solamente si $f(x) \in f(y)$.

Finalmente, queremos demostrar que el recorrido de la función f, $\mathcal{R}(f)$, es un ordinal. Ya que cada elemento de $\mathcal{R}(f)$ es un ordinal, $\mathcal{R}(f)$ es conexo por la relación de pertenencia. Sea α un elemento de $\mathcal{R}(f)$. Demostramos por inducción transfinita que α es un subconjunto de $\mathcal{R}(f)$. Se sigue, de una vez, a partir de (1), que $0 \in \mathcal{R}(f)$. En segundo lugar, si $\beta < \alpha$ y $\beta \in \mathcal{R}(f)$, entonces existe un x en A tal que $f(x) = \beta$, y $f(x') = \beta'$ sobre la base de (3), de donde, $\beta' \in \mathcal{R}(f)$. Finalmente, si β es un ordinal límite, $B \leq \alpha$ y, para todo $\gamma < \beta$, $\gamma \in \mathcal{R}(f)$, entonces

$$\bigcup_{\gamma<\beta} \mathcal{S}(A,R,f^{-1}(\gamma))$$

es un R-segmento de A; en consecuencia, existe un y en A tal que $\beta = f(y)$, de donde, $\beta \in \mathcal{R}(f)$. Hemos establecido que

(6) $\mathcal{R}(f)$ es un ordinal.

Nuestro teorema se sigue, de una vez, a partir de (4), (5) y (6) pues la unicidad del ordinal $\mathcal{R}(f)$ es obvia. Q.E.D.

Nótese que el teorema fundamental para conjuntos bien ordenados (teorema 80) se sigue más bien directamente de este teorema de representación.

Concluimos esta sección con unos pocos teoremas sobre cardinales y alefs. A partir del teorema de representación que se acaba de demostrar se sigue fácilmente que

Teorema 82. *Si R bien-ordena A, entonces existe un único número cardinal α tal que $\alpha \approx A$.*

Este teorema justifica la definición del número cardinal de un conjunto bien ordenado.

Definición 14. *Si R bien-ordena A, entonces $\overline{\overline{A}} = x$ si y solamente si x es un número cardinal y $x \approx A$.*

Algunos teoremas obvios son:

Teorema 83. *Si R bien-ordena A y S bien-ordena B, entonces $\overline{\overline{A}} = \overline{\overline{B}}$ si y solamente si $A \approx B$.*

Teorema 84. $\overline{\overline{\alpha}} \leq \alpha$.

Finalmente, podemos combinar los resultados de los teoremas 68, 81 y 82 para dar el resultado clásico:

Teorema 85. *El número cardinal de un conjunto infinito bien ordenado es un alef.*

EJERCICIOS

1. Demostrar el teorema 69.
2. Formular y demostrar un análogo del teorema 4, para conjuntos bien ordenados.
3. Demostrar el teorema 70.
4. Demostrar el teorema 71.
5. Demostrar el teorema 74.
6. Supóngase que R bien-ordena A y sea $\langle A, R\rangle$ semejante a $\langle B, S\rangle$. Demostrar que S bien-ordena B.
7. Sea R una ordenación estricta simple de A y sea f una función creciente sobre $\langle A, R\rangle$.
   (i) ¿Es f una función 1-1?
   (ii) Si lo es, ¿es la inversa de f una función creciente?
8. Demostrar el teorema 76.
9. Sean R y S ordenaciones estrictas simples de A y sea f una función creciente tanto sobre $\langle A, R\rangle$ como sobre $\langle A, S\rangle$. ¿Cómo están relacionadas R y S?
10. Demostrar el teorema 77.
11. **Los teoremas 72 a 77 tienen la hipótesis de que R bien-ordena A. ¿En cuáles de estos teoremas puede debilitarse esta hipótesis en el siguiente sentido: es R una ordenación estricta simple de A?**
12. **Demostrar que, si R bien-ordena A y $x,y \in A$, entonces**
    (i) $\mathcal{S}(A,R,x) \subseteq \mathcal{S}(A,R,y)$ o $\mathcal{S}(A,R,y) \subseteq \mathcal{S}(A,R,x)$,
    (ii) $x\ R\ y$ si y solamente si $\mathcal{S}(A,R,x) \subset \mathcal{S}(A,R,y)$,
    (iii) si $x \neq y$, entonces $\mathcal{S}(A,R,x)$ no es semejante a $\mathcal{S}(A,R,y)$.
13. Demostrar el teorema 78.
14. **Demostrar que, si R bien-ordena A, S bien-ordena B y $\langle A, R\rangle$ es semejante a $\langle B, S\rangle$, entonces, para cada x en A, existe un y en B tal que es semejante a $\langle\ (B,S,y),S\rangle$.**
15. Dar un contra-ejemplo para mostrar que el teorema 79 no es válido si la hipótesis de buena ordenación se debilita a ordenación estricta simple.
16. Supóngase que R bien-ordena A y sea B un subconjunto de A. Demostrar que $\langle B, R\rangle$ es semejante a $\langle A, R\rangle$ o a $\langle \mathcal{S}(A,R,x),R\rangle$ para algún x en A.
17. Dada la definición

$$M(\alpha) = \{x\colon x \text{ es un cardinal transfinito } \&\ x \in \alpha\},$$

demostrar que para todo β existe un único cardinal transfinito α tal que $\langle\beta, \mathcal{E}\beta\rangle$ es semejante a $\langle M(\alpha), \mathcal{E}\alpha\rangle$. (Este resultado justifica una definición alterna de los alefs.)

§ *7.5 Resumen revisado de axiomas.* En vista del hecho que dos de nuestros axiomas iniciales pueden deducirse del esquema axiomático de sustitución y del axioma del conjunto potencia, éste parece un punto apropiado con respecto al cual debe revisarse el resumen de § 2.10. Demostramos primero:

Meta-teorema 1. *El esquema axiomático de separación es deducible del esquema axiomático de sustitución.*

Demostración. En el esquema axiomático de sustitución tomamos $\varphi(x,y)$ como $x = y\ \&\ \psi(y)$, lo cual es claramente funcional en x. Tenemos entonces:

$$(\exists B)(y)(y \in B \leftrightarrow (\exists x)(x \in A\ \&\ x = y\ \&\ \psi(y))),$$

a partir de lo cual se sigue el esquema axiomático de separación, por lógica cuantificacional elemental y por la lógica de la identidad. Q.E.D.

Dado el esquema axiomático de separación, podría parecer que la teoría de conjuntos de Zermelo podría extenderse a la teoría de conjuntos de Zermelo-Fraenkel, por la adición de un número finito de axiomas (*no* esquemas axiomáticos); pero Montague [1956] ha demostrado que tal extensión finita no es equivalente a la agregación del esquema axiomático de sustitución.

El siguiente resultado se ha mencionado antes; se refiere al que aparece en la obra de Zermelo [1930].

Meta-teorema 2. *El axioma de apareamiento es deducible del axioma del conjunto potencia y del esquema axiomático de sustitución.*

Demostración. En el esquema axiomático de sustitución seleccionamos como conjunto A, el conjunto potencia

(1) $\mathcal{P}\mathcal{P}(0) = \{0, \{0\}\}$.

Sean x, y dos objetos cuyo conjunto pareja queremos formar. Como $\varphi(u,v)$ en el esquema axiomático de sustitución (hemos cambiado las variables en φ para evitar confusión) tomamos:

(2) $(u = 0 \;\&\; v = x) \vee (u = \{0\} \;\&\; v = y)$.

Claramente, (2) es funcional en u, esto es, para cada u en $\mathcal{P}\mathcal{P}(0)$ existe exactamente un v tal que $\varphi(u,v)$. Aplicando, como se indicó, el esquema axiomático de sustitución a (1) y (2), obtenemos precisamente que existe un conjunto B que tiene como elementos a x y a y, esto es, a partir de $(\exists B)(\forall v)(v \in B \leftrightarrow (\exists u)(u \in \mathcal{P}\mathcal{P}(0) \;\&\; [(u = 0 \;\&\; v = x) \vee (u = \{0\} \;\&\; v = y)]))$ inferimos el axioma de apareamiento:

$(\exists A)(\forall z)(z \in A \leftrightarrow z = x \vee z = y)$. Q.E.D.

Con esas dos deducciones a mano, el sistema de teoría de conjuntos desarrollado en estos primeros siete capítulos depende solamente de siete axiomas. Además, puesto que el axioma para cardinales no es un axioma usual de la teoría de conjuntos de Zermelo, todo uso de ese axioma se indica con el símbolo †. Los siete axiomas, en orden cronológico de introducción, son

Axioma de extensionalidad:

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

Axioma de suma:

$$(\exists C)(\forall x)(x \in C \leftrightarrow (\exists B)(x \in B \;\&\; B \in A)).$$

Axioma de conjunto potencia:

$$(\exists B)(\forall C)(C \in B \leftrightarrow C \subseteq A).$$

Axioma de regularidad:

$$A \neq 0 \rightarrow (\exists x)[x \in A \;\&\; (\forall y)(y \in x \rightarrow y \notin A)].$$

Axioma para cardinales:

$$\mathcal{K}(A) = \mathcal{K}(B) \leftrightarrow A \approx B.$$

Axioma de infinitud:

$$(\exists A)(0 \in A \;\&\; (\forall B)(B \in A \rightarrow B \cup \{B\} \in A)).$$

Esquema axiomático de sustitución: Si $(\forall x)(\forall y)(\forall z)(x \in A \;\&\; \varphi(x,y) \;\&\; \varphi(x,z) \rightarrow y = z)$, *entonces* $(\exists B)(\forall y)(y \in B \leftrightarrow (\exists x)(x \in A \;\&\; \varphi(x,y)))$.

Capítulo 8

El axioma de escogencia

§ 8.1 **Algunas aplicaciones del axioma de escogencia.** En los capítulos 4, 5 y 7 se han mencionado varios resultados que requieren el axioma de escogencia para su demostración. La formulación del axioma que usaremos es:

> *Para cualquier conjunto A, existe una función f tal que, para todo subconjunto no vacío B de A, $f(B) \in B$.*

Para referencia futura designamos esta formulación con AC_1. La función f se llama frecuentemente una función de escogencia o una función de selección para el conjunto dado A. La función incluye en su dominio a todo subconjunto no vacío de A y selecciona exactamente un elemento de cada subconjunto. Para familiarizarnos con esta función de escogencia podemos considerar un ejemplo finito sencillo, para el cual el axioma no se necesita. Sea

$$A = \{1,2\}$$
$$B_1 = \{1\}$$
$$B_2 = \{2\}.$$

Entonces existen dos funciones de escogencia distintas f_1 y f_2 cuyos dominios son los subconjuntos no vacíos de A:

$$f_1(B_1) = f_2(B_1) = 1$$
$$f_1(B_2) = f_2(B_2) = 2$$
$$f_1(A) = 1$$
$$f_2(A) = 2.$$

Esta noción de una función de escogencia se formaliza fácilmente.

Definición 1. *f es una función de escogencia para A si y solamente si f es una función cuyo dominio es la familia de subconjuntos no vacíos de A y, para cada $B \subseteq A$ con $B \neq 0$, $f(B) \in B$.*

El axioma de escogencia puede ser formulado usando esta definición. *Todo conjunto tiene una función de escogencia,* si bien en la formulación dada atrás no se requería que el dominio de f se restringiera a subconjuntos no vacíos de A. Sin embargo, esta es una diferencia trivial.

Todo teorema o definición que depende del axioma de escogencia se indicará con '⋆'. Sin el axioma podemos demostrar los dos teoremas siguientes acerca de las funciones de escogencia. Dejamos las demostraciones, que no son difíciles, como ejercicios.

Teorema 1. *Si R bien-ordena A, entonces A tiene una función de escogencia.*

Teorema 2. *Todo conjunto finito tiene una función de escogencia.*

Históricamente el axioma de escogencia fue introducido primero por Zermelo [1904] para demostrar que todo conjunto puede ser bien ordenado. Hasta las dos o tres últimas décadas, probablemente la principal aplicación del axioma en matemática general se hizo a través del teorema de buena ordenación y la aplicación de la inducción transfinita a la buena ordenación garantizada por el teorema. Sin embargo, la tendencia reciente entre los matemáticos ha sido evitar la inducción transfinita y usar algún principio maximal. (Las formulaciones precisas se dan en la sección siguiente.)

En los capítulos precedentes se han mencionado aplicaciones específicas del axioma de escogencia. En §4.1 se mencionó que el axioma se necesitaba para demostrar la ley de tricotomía para la potencia de conjuntos, esto es, $A \prec B$, $B \prec A$ o $A \approx B$, para dos conjuntos cualesquiera A y B. En § 4.2 se afirmó que toda demostración conocida de que el infinito ordinario implica el infinito de Dedekind, requiere el axioma. En § 4.3 fue mencionada la necesidad de usar el axioma para demostrar la ley de tricotomía para números cardinales, construidos por el uso del axioma especial para ellos. Obviamente la tricotomía para potencia de conjuntos implica este resultado inmediatamente. En §5.3 notamos que el axioma se necesita para demostrar que todo conjunto infinito tiene un subconjunto enumerable. Este es el hecho crucial que se requiere para demostrar que el infinito ordinario implica el infinito de Dedekind. Finalmente, se afirmó en § 7.3 que la demostración de que todo conjunto tiene un número cardinal requiere el axioma, cuando los números cardinales se definen como ordinales iniciales.

Nos referimos ahora a las demostraciones de esos hechos, las cuales no se darán aquí, necesariamente, en el orden en que fueron formuladas en el texto.

Comenzamos con

⋆**Teorema 3.*** *Si un conjunto es infinito, entonces tiene un subconjunto enumerable.*

Demostración. Sea A un conjunto infinito y sea f una función de escogencia para A, como se postuló por el axioma de escogencia. Ahora usamos el teorema 27 de § 5.2 para definir una función única g sobre ω:

$$g(0) = f(A)$$
$$g(n') = f(A \sim \{ g(k)\colon k \leq n \}).$$

(Así, por ejemplo,

$$g(1) = f(A \sim \{g(0)\}) = f(A \sim \{f(A)\}).)$$

La idea intuitiva es la de que g asigna 0 al elemento x_0 seleccionado de A, luego 1 al elemento x_1 seleccionado de $A \sim \{x_0\}$, luego 2 al elemento x_2 seleccionado de $A \sim \{x_0, x_1\}$, etc. Puesto que siempre $f(B) \in B$, vemos que g es 1-1. Ahora supongamos que existe un n tal que

$$A \sim \{g(k)\colon k < n\} = 0;$$

entonces g establece que

$$A \approx n,$$

contrario a la hipótesis de que A es infinito. Entonces, para todo n,

$$A \sim \{g(k)\colon k < n\} \neq 0,$$

de donde concluimos que el recorrido de g es equipotente con ω, pero el recorrido de g es un subconjunto de A, lo que significa que el teorema ha sido demostrado. Q.E.D.

A partir del teorema que se acaba de demostrar y de los teoremas 46 y 47 de § 5.3, concluimos:

⋆**Teorema 4.** *Un conjunto es infinito según Dedekind si y solamente si es infinito.*

Para propósitos subsiguientes, demostramos ahora lo que Bernays ([1942], p. 141) llama apropiadamente un *teorema de numeración*: Todo conjunto puede ponerse en correspondencia 1-1 con algún ordinal.

⋆**Teorema 5.** [Teorema de numeración]. *Para cualquier conjunto A existe un ordinal α tal que $\alpha \approx A$.*

Demostración. En virtud del axioma de escogencia, existe una función F tal que, para todo subconjunto no vacío B de A,

$$F(B) \in B.$$

* Hacemos notar de nuevo que distinguimos con una estrella todos los teoremas y definiciones que dependen del axioma de escogencia.

Usamos F para definir el siguiente predicado φ: $\varphi(B,\beta)$ si y solamente si

(1) $B \subseteq A$,

existe una f tal que

(2) f es una función sobre β,

(3) $\mathcal{R}f = B$,

(4) $(\forall\gamma)(\gamma < \beta \to f(\gamma) = F(A \sim \mathcal{R}(f|\gamma))$.

Obviamente, f, si existe, es única y es 1-1, de donde, si $\varphi(B, \beta)$ y $\varphi(B, \beta_1)$, entonces $\beta = \beta_1$ y podemos aplicar el esquema axiomático de sustitución para formar el conjunto C tal que

$$\beta \in C \leftrightarrow (\exists B)(B \in \mathcal{P}A \;\&\; \varphi(B,\beta)).$$

El resto de la demostración sigue los lineamientos familiares de § 7.1 sobre inducción transfinita, considerando $\bigcup C$. Los detalles se dejan como ejercicio. Q.E.D.

Usando el teorema de numeración se pueden demostrar fácilmente los dos teoremas siguientes.

$\star$**Teorema 6.** *Todo conjunto puede ser bien ordenado; esto es, para todo conjunto A existe una relación R tal que R bien-ordena A.*

$\star$**Teorema 7.** [Tricotomía]. *Para dos conjuntos cualesquiera A y B, $A \prec B$, $B \prec A$ o $A \approx B$.*

Como otra consecuencia fácil del teorema de numeración, tenemos:

$\star$**Teorema 8.** *Para cualquier conjunto A existe un único número cardinal α tal que $\alpha \approx A$.*

Y este teorema justifica la introducción de la notación de doble barra debida a Cantor para el *número cardinal* de un conjunto.

$\star$**Definición 2.** $\overline{\overline{A}} = x$ *si y solamente si x es un número cardinal y $x \approx A$.*

Un teorema obvio es:

$\star$**Teorema 9.** $\overline{\overline{A}} = \overline{\overline{B}}$ *si y solamente si $A \approx B$.*

Sobre la base del teorema 9, podemos considerar el axioma especial para cardinales como redundante, una vez adoptado el axioma de escogencia. Es decir, este axioma especial es deducible de nuestros otros axiomas junto con el axioma de escogencia.

EJERCICIOS

1. ¿Cuántas funciones distintas de escogencia hay
   (a) para un conjunto de tres elementos?
   (b) para un conjunto de n elementos?
2. ¿Cuál es la función de escogencia obvia para el conjunto de los enteros negativos?
3. Demostrar el teorema 1.
4. Demostrar el teorema 2.
5. Completar la demostración del teorema 5.
6. Demostrar el teorema 6.
7. Demostrar el teorema 7.
8. Usar el axioma de escogencia para demostrar que, si A es una familia enumerable de conjuntos finitos, disjuntos dos a dos, entonces $\bigcup A$ es enumerable.
9. Demostrar el teorema 8.
10. Demostrar el teorema 9.
11. Demostrar que, si f es una función, entonces $\overline{\overline{\mathcal{R}f}} \leq \overline{\overline{\mathcal{D}f}}$.

§ 8.2 Equivalentes del axioma de escogencia.

En su documento clásico de 1904 Zermelo se propuso demostrar que el axioma de escogencia implica que todo conjunto puede ser bien ordenado. En ese documento él usó la siguiente formulación:

AC_2: *Si A es un conjunto de conjuntos no vacíos y disjuntos dos a dos, entonces existe un conjunto C cuya intersección con cualquier elemento B de A tiene exactamente un elemento, esto es, $C \cap B$ es un conjunto unitario.*

Nuestro objetivo en esta sección es formular cierto número de principios equivalentes a AC_1; muchas de las demostraciones se dejarán como ejercicios. Comenzamos con:

Teorema 10. AC_2 *es equivalente a* AC_1.

Otra formulación común es:

AC_3: *Dada cualquier relación R, existe una función $f \subseteq R$ tal que*

dominio de R = dominio de f.

Teorema 11. AC_3 *es equivalente a* AC_1.

Nuestro programa es ahora establecer las siguientes equivalencias:

Axioma de escogencia $\leftrightarrow$ teorema de numeración
$\leftrightarrow$ teorema de buena ordenación
$\leftrightarrow$ lema de Zorn
$\leftrightarrow$ ley de tricotomía.

Como era de esperarse, ninguno de los teoremas que establecen esas equivalencias depende del axioma de escogencia y en consecuencia, ninguno lleva estrella. En la sección anterior (teorema 5) hemos demostrado:

Axioma de escogencia $\rightarrow$ teorema de numeración.

Más adelante el enfoque obvio para demostrar los teoremas 6 y 7 da:

Teorema 12. *El teorema de numeración implica el teorema de buena ordenación y la ley de tricotomía.*

Nuestro paso siguiente es demostrar que el teorema de buena ordenación implica el lema de Zorn. Se necesitan algunas definiciones preliminares:

Definición 3.

(i) *A es una cadena si y solamente si A es un conjunto de conjuntos y, para dos conjuntos cualesquiera B y C en A, $B \subseteq C$ o $C \subseteq B$,*

(ii) *A es una cadena en B si y solamente si A es una cadena y $A \subseteq B$,*

(iii) *A es una cadena maximal en B si y solamente si A es una cadena en B y no existe cadena C en B tal que $A \subset C$.*

La idea intuitiva es la de que una cadena es un conjunto simplemente ordenado por la inclusión.* Como cadenas maximales considérese el conjunto $\mathcal{P}\omega$ de subconjuntos de enteros.

Entonces, la familia de conjuntos

$$0$$
$$\{1\}$$
$$\{1, 2\}$$
$$\dots$$
$$\{1, 2, \dots, n\}$$
$$\dots$$
$$\omega$$

es un ejemplo de una cadena maximal en $\mathcal{P}\omega$.

Necesitamos también recalcar (definición 4 del capítulo 4) la noción de un elemento máximo de un conjunto A. Por ejemplo, si

$$A = \{\{1\}, \{1,2\}, \{3\}\},$$

entonces $\{1,2\}$ y $\{3\}$ son elementos máximos de A. Si consideramos

$$A = \mathcal{P} B,$$

entonces B es el único elemento máximo de A. Si tomamos

$$A = (\mathcal{P}\,\omega) \sim \{\omega\},$$

entonces A tiene una infinidad de elementos máximos, a saber los conjuntos

$$\omega \sim \{1\}$$
$$\omega \sim \{2\}$$
$$\dots$$
$$\dots$$

La definición de elemento máximo es tal que requiere que el elemento sea un conjunto.

Ahora formulamos

Lema de Zorn Z_1: *Si $A \neq 0$ y si la suma de cada cadena no vacía que sea un subconjunto de A está en A, entonces A tiene un elemento máximo.*

Formulado simbólicamente, Z_1 es:

$A \neq 0$ & $(\forall B)(B \subseteq A$ & *B es una cadena no vacía* $\rightarrow \bigcup B \in A) \rightarrow$ *A tiene un elemento máximo.*

Este principio maximal se bautiza después de Zorn [1935], pero la historia de él y de algunos principios maximales que le están ligados, es muy confusa. Ciertamente Zorn

* Lo que aquí se llama una *cadena* se llama *nido* en Kelley [1955].

fue precedido esencialmente por F. Hausdorff, C. Kuratowski y R. L. Moore, por lo menos. Más adelante se dan algunas variantes en la formulación del lema de Zorn, particularmente el principio maximal de Hausdorff, el cual data de 1914.

Para continuar nuestras implicaciones queremos demostrar:

Teorema 13. *El teorema de buena ordenación implica el lema de Zorn* Z_1.

Demostración. La idea intuitiva de la demostración consiste en usar la buena ordenación R postulada para construir, para cualquier familia no vacía A de conjuntos, una cadena maximal: el R- primer elemento de A está en la cadena y del mismo modo cualquier elemento subsiguiente que incluya o esté incluido en todo elemento R-precedente de la cadena. La suma de esta cadena maximal es un elemento máximo, como se requería.

Sea A un conjunto que satisface las hipótesis de Z_1, y sea R una buena ordenación de A como se postuló. Podemos también hacer la hipótesis simplificante, no esencial, de que A tenga como elementos solamente conjuntos.

El primer paso para "construir" una cadena maximal es definir un término τ que puede usarse para definir una función, por recurrencia transfinita, que recoja los elementos de esta cadena maximal.

Definimos:

$$\tau(h) = \begin{cases} 1, & \text{si para todo } B \text{ en } \mathfrak{D}h \text{ tal que } h(B) = 1, \text{ tenemos} \\ & \qquad B \subseteq D \text{ o } D \subseteq B, \\ & \text{donde } D \text{ es el } R\text{-primer elemento de } A \sim \mathfrak{D}h; \\ 0, & \text{en cualquier otro caso.} \end{cases}$$

El segundo paso es aplicar recurrencia transfinita a τ y a R. Sobre la base de la sexta formulación de la recurrencia transfinita (teorema 71 de § 7.4) sabemos que existe una función única f tal que

(i) f es una función sobre A,

(ii) para todo conjunto $B \in A$,

$$f(B) = \tau(f|\ \mathcal{S}(A,R,B)).$$

El tercer paso es definir la cadena apropiada. Sea

$$C = \{B: B \in A \ \&\ f(B) = 1\}.$$

Para verificar que C es una cadena necesitamos demostrar que, para dos elementos cualesquiera B_1 y B_2 de C,

$$B_1 \subseteq B_2 \text{ o } B_2 \subseteq B_1.$$

Para precisar supongamos que B_1 R-precede a B_2 en la buena ordenación de A. Puesto que $B_1 \in C$,

$$(1) \qquad f(B_1) = 1,$$

también por la hipótesis

$$f(B_2) = 1,$$

pero, entonces,

$$\tau(f|\ \mathcal{S}(A,\ R,\ B_2)) = 1,$$

y B_2 es el R-primer elemento de

$$A \sim \mathfrak{D}\,(f|\ \mathcal{S}\,(A,R,B_2)),$$

por tanto, ya que $B_1 \in \mathcal{S}\,(A,R,B_2)$ por la definición de τ y (1),

$$B_1 \subseteq B_2 \text{ o } B_2 \subseteq B_1.$$

El cuarto paso es mostrar que $\bigcup C$ es un elemento máximo de A. Por la hipótesis del lema de Zorn, $\bigcup C \in A$ ya que C es una cadena que es un subconjunto de A. Supongamos que $\bigcup C$ no es un elemento máximo y sea

$$G = \{D: D \in A \ \&\ \bigcup C \subset D\}.$$

Sea $D_\star$ el R-primer elemento de G. Ahora, para cualquier $B \in C$,

$$B \subseteq \bigcup C,$$

de donde

$$B \subset D_\star,$$

pero entonces,

$$\tau(f \mid \mathcal{S}(A,R,D_\star)) = 1;$$

esto es,

$$f(D_\star) = 1$$

y

$$D_\star \in C,$$

lo que es absurdo. Así que nuestra suposición es falsa y $\bigcup C$ es un elemento máximo como se requería. Q. E. D.

Ahora completamos un ciclo de implicaciones demostrando:

Teorema 14. *El lema de Zorn* Z_1 *implica el axioma de escogencia* AC_1.

Demostración. Puesto que el tipo de razonamiento que se usa en esta demostración es bastante parecido al anterior se omiten algunos detalles.

Sea A cualquier conjunto no vacío y sea $G = \{ g: (\exists B)(g$ es una función sobre B & $B \subseteq \mathcal{P}A \sim \{0\}$ & para todo conjunto no vacío A_1 en B, $g(A_1) \in A_1)\}$.
G es, desde luego, la clase de funciones de escogencia definidas sobre algún conjunto de subconjuntos no vacíos de A. Usamos el lema de Zorn para mostrar que G debe tener, como elemento, por lo menos una función definida para todos los subconjuntos no vacíos de A.

Sea C una cadena que es un subconjunto de G. Entonces claramente $\bigcup C \in G$, de donde el lema de Zorn es aplicable a G. Sea f un elemento máximo de G. Afirmo que

$$\text{Dominio de } f = \mathcal{P}A \sim \{0\}.$$

Supongamos que no. Entonces existe un subconjunto no vacío B_1 de A tal que

$$B_1 \notin \mathfrak{D}f.$$

Sea z_1 algún elemento de B_1; definamos

$$f_1 = f \cup \{\langle B_1, z_1 \rangle\}.$$

Obviamente,

$$f \subset f_1$$

y

$$f_1 \in G,$$

de donde f *no* es un elemento máximo de G lo que es absurdo. Nuestra suposición es falsa y f es una función de escogencia para A.

Q.E.D.

Hemos establecido las equivalencias:

Axioma de escogencia

$AC_1 \leftrightarrow$ *teorema de numeración*
$\leftrightarrow$ *teorema de buena ordenación*
$\leftrightarrow$ *lema de Zorn* Z_1.

Enseguida queremos demostrar que la ley de tricotomía implica uno de los cuatro enunciados que acabamos de enumerar. (El teorema 12 junto con las equivalencias anteriores establece que una de las cuatro implica la ley de tricotomía.) Para este fin demostramos, usando algunos resultados de § 7.3,

Teorema 15. *La ley de tricotomia implica el teorema de numeración.*

Demostración. Sea A cualquier conjunto. Queremos demostrar que A tiene la misma potencia que algún ordinal, usando la ley de tricotomía. Usando la función de Hartog $\mathcal{H}$ introducida en § 7.3, tenemos, en virtud del teorema 57 de § 7.3,

$$\text{no } \mathcal{H}(A) \preceq A,$$

así que por la ley de tricotomía,

$$(1) \qquad A \prec \mathcal{H}(A).$$

A partir de (1) se sigue inmediatamente que existe un subconjunto L de $\mathcal{H}(A)$ tal que

$$(2) \qquad A \approx L.$$

Además, ya que $\mathcal{H}(A)$ es un ordinal (teorema 56 de § 7.3), L es bien ordenado y entonces, por el teorema de representación para conjuntos bien ordenados (teorema 81 de § 7.4), existe un ordinal α tal que

$$(3) \qquad L \simeq \alpha.$$

A partir de (2), (3) y la transitividad de la equipotencia se sigue la conclusión deseada.

Q.E.D.

Podemos usar ahora la noción de cadena maximal para formular el principio maximal de Hausdorff [1914, pp. 140-41].

Principio maximal de Hausdorff: H_1. *Si A es una familia de conjuntos, entonces toda cadena en A es un subconjunto de alguna cadena maximal en A.*

Una formulación algo simple pero equivalente es:

H_2: *Toda familia de conjuntos tiene por lo menos una cadena maximal.*

Enunciamos sin demostración:

Teorema 16. H_1 *es equivalente a* Z_1.

Teorema 17. H_2 *es equivalente a* H_1.

Fácilmente se dan formulaciones semejantes a Z_1, H_1, y H_2 para una relación arbitraria en lugar de la inclusión.

Definición 4.

(i) *y es una cota R-superior de A si y solamente si, para todo x en A, xRy;*

(ii) *y es un elemento R-máximo de A si y solamente si, para todo $x \neq y$ en A, no yRx.*

(iii) *A es una R-cadena de B si y solamente si $A \subseteq B$ y R ordena simplemente a A.*

Usando estas nociones, formulamos:

Lema de Zorn Z_2: *Si R ordena parcialmente a A y toda R-cadena de A tiene una cota R-superior en A, entonces A tiene un elemento R-máximo.*

Formulamos sin demostración:

Teorema 18. Z_2 *es equivalente a* Z_1.

Se deja como ejercicio la consideración de los análogos para relaciones arbitrarias H_1 y H_2.

Finalmente formulamos un principio maximal debido independientemente a Teichmüller [1939] y a Tukey [1940].

Definición 5. *A es un conjunto de carácter finito si y solamente si*

(i) *A es un conjunto no vacío de conjuntos,*

(ii) *todo subconjunto finito de un elemento de A es también un elemento de A,*

(iii) *si todo subconjunto finito de un conjunto es un elemento de A, entonces el conjunto es también un elemento de A.*

La idea intuitiva que está detrás de esta formulación es la de que una propiedad es de carácter finito si un conjunto tiene la propiedad cuando y solamente cuando todos sus subconjuntos finitos tienen la propiedad. Un ejemplo simple de tal propiedad es el siguiente. Supongamos que R ordena parcialmente a A. Entonces R ordena simplemente a A si y solamente si R ordena simplemente a todo subconjunto finito de A. (En efecto, es suficiente considerar sólo los dos subconjuntos elementos de A.)

Lema de Teichmüller-Tukey: T. *Cualquier conjunto de carácter finito tiene un elemento máximo.*

Demostramos:

Teorema 19. *El lema T de Teichmüller-Tukey es equivalente al lema de Zorn* Z_1.

Demostración. La demostración se da solamente como un complemento. Primero demostramos que Z_1 implica T. Sea A un conjunto de carácter finito y sea C cualquier cadena que es un subconjunto de A. Para aplicar Z_1 necesitamos demostrar que $\bigcup C \in A$. Sea F un subconjunto finito de $\bigcup C$. Entonces F es un subconjunto de la unión de una colección finita D de elementos de C, pues cada elemento de F debe pertenecer a algún elemento de C y hay sólo un número finito de elementos en F. Ahora, puesto que D es finito y es un subconjunto de la cadena C, tiene un elemento mayor que todos, digamos E; F debe ser un subconjunto de E, pues de otro modo C no sería una cadena. $E \in A$, por tanto, ya que A es un conjunto de carácter finito, $F \in A$; pero entonces también $\bigcup C \in A$. La hipótesis de Z_1 se satisface así por A y, en virtud de Z_1, A tiene un elemento máximo.

Ahora demostramos que T implica Z_1. Es más conveniente demostrar que T implica H_2, lo cual, en virtud de los teoremas 16 y 17, es equivalente a Z_1. Sea A una familia de conjuntos. Definimos:

$$B = \{C: C \subseteq A \ \& \ C \text{ es una cadena}\}.$$

Como se ha observado anteriormente, es obvio que B es un conjunto de carácter finito, o sea que B tiene un elemento máximo, digamos $C_\star$, pero $C_\star$ es una cadena maximal en A, pues si no lo fuera, no sería un elemento máximo de B y esto demuestra H_2. Q.E.D.

Los teoremas de esta sección y de la precedente han establecido las siguientes equivalencias:

Axioma de escogencia AC_1
$\leftrightarrow$ axioma de escogencia AC_2
$\leftrightarrow$ axioma de escogencia AC_3
$\leftrightarrow$ teorema de numeración
$\leftrightarrow$ teorema de buena ordenación
$\leftrightarrow$ lema de Zorn Z_1
$\leftrightarrow$ ley de tricotomía
$\leftrightarrow$ principio maximal de Hausdorff H_1
$\leftrightarrow$ principio maximal de Hausdorff H_2
$\leftrightarrow$ lema de Zorn Z_2
$\leftrightarrow$ lema T de Teichmüller-Tukey.

Un problema clásico abierto de la teoría de conjuntos es la independencia del axioma de escogencia (o sus equivalentes) con respecto a los demás axiomas de la teoría de conjuntos de Zermelo. La posibilidad de que sea independiente es bastante grande. El origen del interés filosófico en este problema es el carácter no constructivo del axioma de escogencia. La adopción o rechazo de este axioma ha provocado quizás más controversia entre los matemáticos de este siglo que cualquier otra cosa de los fundamentos de la matemática. Los matemáticos de inclinaciones constructivas objetan la postulación de la existencia de una función de escogencia, cuando no se da ninguna indicación sobre cómo se construye esta función. (Para una discusión interesante sobre este punto véanse *Supplementary Notes to Borel* [1950] y también Sierpinski [1928, capítulo 6].)

La afirmación de que el uso del axioma de escogencia pueda llevar a una contradicción es definitivamente falsa en el siguiente sentido. Ha sido demostrado por Gödel ([1938], [1940]) que el axioma de escogencia es relativamente consistente, esto es, si los otros axiomas de la teoría de conjuntos son consistentes, la adición de este axioma no lleva a contradicción.

Por otra parte, la aplicación del axioma de escogencia puede llevar a algunos resultados paradójicos. Quizás el ejemplo más celebrado es la paradoja de Banach-Tarski [1924] según la cual, usando este axioma, una esfera de radio dado puede descomponerse en un número finito de partes las cuales se colocan de nuevo de tal manera que se forman dos esferas con el mismo radio dado para la original. Más generalmente, Banach y Tarski demostraron que, en un espacio euclídeo de dimensión tres o más, dos conjuntos acotados arbitrarios con puntos interiores son equivalentes por descomposición finita, esto es, los dos conjuntos son susceptibles de descomposición en el mismo número finito de partes disjuntas con una correspondencia 1-1 de congruencia entre sus respectivas partes.

EJERCICIOS

1. Demostrar el teorema 10.
2. Demostrar el teorema 11.
3. Demostrar el teorema 12.
4. Considérese el conjunto potencia $\mathcal{P}\omega$ del conjunto de todos los enteros. Dar un ejemplo diferente, del que se da en el texto, de una cadena maximal en $\mathcal{P}\omega$.
5. Demostrar el teorema 16.
6. Demostrar el teorema 17.
7. Demostrar el teorema 18.
8. Formular un principio maximal de Hausdorff que esté con respecto a H_1 como Z_2 está con respecto a Z_1. Demostrar su equivalencia con H_1.
9. ¿Son las propiedades definidas en las definiciones 10 a 17 de § 3.2 propiedades de carácter finito? (El método para reformularlas en términos de conjuntos es obvio.)
10. Dar un ejemplo de una propiedad de una relación con respecto a un conjunto que no es de carácter finito.

§ 8.3 Axiomas que implican el axioma de escogencia. Sin dar detalles exactos concluimos este capítulo con una breve discusión de dos axiomas que, junto con los axiomas de Zermelo-Fraenkel enumerados en § 7.5, implican el axioma de escogencia, pero no necesariamente se cumple el recíproco.

Al final del capítulo 6 mencionamos la hipótesis generalizada del continuo, la cual afirma que para cualquier conjunto infinito A no existe conjunto alguno B tal que $A \prec B \prec 2^A$. Lindenbaum y Tarski [1926] enunciaron sin demostración que esta hipótesis implica el axioma de escogencia; una demostración de este hecho ha sido publicada por Sierpinski [1947].

Un axioma muy fuerte que implica el axioma de escogencia así como ciertos otros axiomas, como el del conjunto potencia, es el axioma de Tarski para conjuntos inaccesibles ([1938], [1939]). Antes de enunciar el axioma será útil considerar el problema que dio lugar al axioma, a saber, el problema de la existencia de números cardinales inaccesibles o números ordinales. Podemos caracterizar los números cardinales inaccesibles según los siguientes lineamientos. Para cada conjunto A de cardinales podemos demostrar, sobre la base de los resultados del capítulo 7, que existe un cardinal menor que todos que sigue a todós los elementos de A. Este cardinal lo denotamos por sup A. Así, $\aleph_0 = \sup\{1,2,3,\ldots,n,\ldots\}$, y $\aleph_1 = \sup\{\aleph_0\}$. Un cardinal $\mathfrak{m}$ que no es 0 se dice que es *inaccesible* si (i) para todo conjunto A de cardinales, tal que $\overline{\overline{A}} < \mathfrak{m}$ y $\mathfrak{n} < \mathfrak{m}$, para $\mathfrak{n}$ en A, tenemos:

$$\sup A < \mathfrak{m}$$

y (ii) si $\mathfrak{n} < \mathfrak{m}$ y $\mathfrak{p} < \mathfrak{m}$, entonces $\mathfrak{n}^{\mathfrak{p}} < \mathfrak{m}$. Obviamente $\aleph_0$ es inaccesible en el sentido de esta definición. La pregunta fundamental es: ¿Puede establecerse la existencia de algunos otros números cardinales inaccesibles, sobre la base de los axiomas de Zermelo-Fraenkel, incluyendo el axioma de escogencia? Shepherdson, en efecto, ha demostrado [1952] que el postulado de que no hay otros cardinales inaccesibles es consistente con los axiomas de la teoría de conjuntos de von Neumann-Bernays-Gödel y, con poca modificación, su demostración vale para la teoría de conjuntos de Zermelo-Fraenkel.

Fue para el propósito de establecer la existencia de números cardinales inaccesibles, para lo que Tarski introdujo su *axioma para conjuntos inaccesibles:* *

> *Para todo conjunto N existe un conjunto M con las siguientes propiedades:*
> (i) *N es equipotente con un subconjunto de M;*
> (ii) $\{A\colon A \subseteq M \;\&\; A \prec M\}$ *es equipotente con M;*
> (iii) *no existe subconjunto alguno P tal que el conjunto de todos los subconjuntos de P sea equipotente con M.*

Tarski ha demostrado que el número cardinal de un conjunto M es infinito e inaccesible si y solamente si M satisface las condiciones (ii) y (iii) del axioma.

* La versión dada aquí es la de Tarski [1939] la cual constituye una versión mejorada de la de Tarski [1938].

BIBLIOGRAFIA

Bachmann, H. *Transfinite Zahlen.* Berlín, 1955.

Banach, S., y A. Tarski. "Sur la décomposition des ensembles de points en parties respectivement congruentes," *Fundamenta Mathematicae,* Vol. 6 (1924), pp. 244-277.

Bernays, P. "A system of axiomatic set theory: I-VII," *Journal of Symbolic Logic,* Vol. 2 (1937), pp. 65-77; Vol. 6 (1941), pp. 1-17; Vol. 7 (1942), pp. 65-89, 133-145; Vol. 8 (1943), pp. 89-106; Vol. 13 (1948), pp. 65-79; Vol. 19 (1954), pp. 81-96.

Beth, E. W. *Les Fondements logiques des mathématiques.* Gauthier-Villars, París, 1950.

Bolzano, B. *Paradoxien des Unendlichen.* Leipzig, 1851.

Borel, E. *Lecons sur la théorie des fonctions,* 4a. ed. París, 1950.

Burali-Forti, C. "Una questione sui numeri transfiniti," *Rendic. Palermo,* Vol. 11 (1897), pp. 154-164 y 260.

Cantor, G. *Contributions to the Founding of the Theory of Transfinite Numbers.* Traducido por P.E.B. Jourdain. Chicago, 1915. Reimpreso recientemente por Dover Publications, Inc.

Church, A. "The Richard paradox," *Amer. Math. Monthly,* Vol. 41 (1934), pp. 356-361.

———"The constructive second number class," *Bull. Amer. Math. Soc.,* Vol. 44 (1938), pp. 224-232.

———*Introduction to Mathematical Logic.* Princeton University Press, Princeton, 1956.

Church, A., y S. C. Kleene. "Formal definition in the theory of ordinal numbers," *Fundamenta Mathematicae,* Vol. 28 (1937), pp. 11-21.

Dedekind, R. *Was sind und was sollen die Zahlen?* Braunschweig, 1888.

Denjoy, A. *L'Enumeration transfinie:* I. *La notion de rang.* París, 1946.

Fraenkel, A. "Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre," *Math. Annalen,* Vol. 86 (1922a), pp. 230-37.

———"Über den Begriff 'definit' und die Unabhängigkeit des Auswahlaxioms," *Sitzungsb. d. Preuss. Akad. d. Wiss., Physik.-math. Klasse* (1922b), pp. 253-257.

———*Einleitung in die Mengenlehre,* 3a. ed. Berlín, 1928.

———*Abstract Set Theory.* North-Holland Publishing Company, Amsterdam, 1953.

Frege, G. *Grundgesetze der Arithmetik,* Vols. I and II. Jena, 1893 and 1903

Geach, P., y M. Black. *Translations from the Philosophical Writings of Gottlob Frege.* Blackwell, Oxford, 1952.

Gödel, K. "The consistency of the axiom of choice and of the generalized continuum hypothesis," *Proc. Nat'l Academy of Sciences,* U.S.A., Vol. 24 (1938), pp. 556-557.

———*The Consistency of the Axiom of Choice and of the Generalized Continuum Hypothesis with the Axioms of Set Theory.* Annals of Mathematics Studies, No. 3, Princeton, 1940.

Grelling, K., y L. Nelson. "Bemerkungen zu den Paradoxien von Russell und Burali-Forti," *Abh. der Friesschen Schule,* N. S. Vol. 2 (1908), pp. 301-324.

Hartogs, F. "Uber das Problem der Wohlordnung," *Math. Annalen,* Vol. 76 (1915), pp. 438-443.

Hausdorff, F. *Grundzüge der Mengenlehre,* 1a. ed. Leipzig, 1914. Reimpreso por Chelsea Publishing Company, New York, 1949.

Kelley, J. L. *General Topology.* Van Nostrand, Princeton, 1955.

Kuratowski, C. "Sur la notion de l'ensemble fini," *Fundamenta Mathematicae,* Vol. 1 (1920), pp. 129-131.

——"Sur la notion de l'ordre dans la théorie des ensembles," *Fundamenta Mathematicae,* Vol. 2 (1921), pp. 161-171.

——*Topologie,* Vol. I. Monogr. Mat., T. III, Varszawa y Lwow, 1933.

Landau, E. *Grundlagen der Analysis.* Leipzig, 1930. Reimpreso, New York, 1946.

Lindenbaum, A., y A. Tarski. "Communication sur les recherches de la théorie des ensembles," *Comptes rendus Varsovie,* Vol. 19 (1926), pp. 299-330.

Mirimanoff, D. "Les antinomies de Russell et de Burali-Forti et le probléme fondamental de la théorie des ensembles," *Enseignement mathématique,* Vol. 19 (1917), pp. 37-52.

Montague, R. "Zermelo-Fraenkel set theory is not a finite extension of Zermelo set theory," *Bull. Amer Math. Soc.,* Vol. 62 (1956), p. 260 (Abstract).

Neumann, J. von. "Zur Einführung der transfiniten Zahlen," *Acta Szeged,* Vol. 1 (1923), pp. 199-208.

——"Eine Axiomatisierung der Mengenlehre," *Journal für die reine und angewandte Mathematik,* Vol. 154 (1925), pp. 219-240.

——"Zur Hilbertschen Beweistheorie," *Math. Zeitschrift,* Vol. 26 (1927), pp. 1-46.

——"Die Axiomatisierung der Mengenlehre," *Math. Zeitschrift,* Vol. 27 (1928a), pp. 669-752.

——"Über die Definition durch transfinite Induktion und verwandte Fragen der allgemeinen Mengenlehre," *Math. Annalen,* Vol. 99 (1928b), pp. 373-391.

——"Über eine Widerspruchsfreiheitsfrage in der axiomatischen Mengenlehre," *Journal für die reine und angewandte Mathematik,* Vol. 160 (1929), pp. 227-241.

Peirce, C. S. *Collected Papers,* Vols. II-IV. Editado por C. Hartshorne y P. Weiss. Cambridge, Mass., 1932.

Quine, W. V. *Mathematical Logic.* New York, 1940.

——"On Frege's way out," *Mind,* Vol. 64 (1955), pp. 145-159.

Ramsey, F. P. "The foundations of mathematics," *Proc. London Math. Soc.,* (2) Vol. 25 (1926), pp. 338-384.

Richard, J. "Les principes de mathématiques et le probléme des ensembles," *Revue gen. des sc.,* Vol. 16 (1905), p. 541.

Robinson, J. "Definability and decision problems in arithmetic," *Journal of Symbolic Logic,* Vol. 14 (1949), pp. 98-114.

Robinson, R. M. "The theory of classes. A modification of von Neumann's system," *Journal of Symbolic Logic,* Vol. 2 (1937), pp. 29-36.

Rosser, J. B. "The Burali-Forti paradox," *Journal of Symbolic Logic,* Vol. 7 (1942), pp. 1-17.

Russell, B. *Principles of Mathematics.* Londres, 1903.

——*Introduction to Mathematical Philosophy,* 2a. edición, Londres, 1920.

Scott, D. "Definitions by abstraction in axiomatic set theory," *Bull. Amer. Math .Soc.,* Vol. 61 (1955), p. 442 (Abstract).

Shepherdson, J. C. "Inner models for set theory: I-III," *Journal of Symbolic Logic,* Vol. 16 (1951), pp. 161-190; Vol. 17 (1952), pp. 225-237; Vol. 18 (1953), pp. 145-167.

Sierpinski, W. "L'axiome de M. Zermelo et son role dans la théorie des ensembles et l'analyse," *Bull. acad. sc. Cracovie,* (1918), pp. 97-152.

———*Lecons sur les nombres transfinis.* París, 1928; 2a. ed., 1950.

———"L'hypothèse généralisée du continu et l'axiome du choix," *Fundamenta Mathematicae,* Vol. 34 (1947), pp. 1-5.

———"Le dernier théorème de Fermat pour les nombres ordinaux," *Fundamenta Mathematicae,* Vol. 37 (1950), pp. 201-205.

———*Hypothèse du continu,* 2a. ed. New York, 1956.

———*Cardinal and Ordinal Numbers.* Warsaw, 1958.

Skolem, T. "Einige Bemerkungen zur axiomatischen Begründung der Mengenlehre," *Wiss. Vorträge gehalten auf dem 5. Kongress der Skandinav. Mathematiken in Helsingfors* 1922 (publicado en 1923), pp. 217-232.

———"Einige Bemerkungen zu der Abhandlung von E. Zermelo: 'Über die Definitheit in der Axiomatik'," *Fundamenta Mathematicae,* Vol. 15 (1930), pp. 337-341.

Slupecki, J. "St. Lesniewski's calculus of names," *Studia Logica,* Vol. 3 (1955), pp. 7-76.

Stäckel, P. "Zu H. Webers Elementarer Mengenlehre," *Jahresber. d. d. M. -V.,* Vol. 16 (1907), p. 425.

Suppes, P. *Introduction to Logic.* Van Nostrand, Princeton, 1957.

Tarski, A. "Sur quelques théorèmes qui équivalent à l'axiome du choix," *Fundamenta Mathematicae.* Vol. 5 (1924a), pp. 147-154.

———"Sur les ensembles finis," *Fundamenta Mathematicae,* Vol. 6 (1924b), pp. 45-95.

———"Über unerreichbare Kardinalzahlen," *Fundamenta Mathematicae,* Vol. 30 (1938), pp. 68-89.

———"On well-ordered subsets of any set," *Fundamenta Mathematicae,* Vol. 32 (1939), pp. 176-183.

———*Logic, Semantics, Metamathematics: Papers from* 1923 *to* 1938. Traducido por J. H. Woodger. Oxford, 1956.

Teichmüller, O. "Braucht der Algebraiker das Auswahlaxiom?" *Deutsche Math.,* Vol. 4 (1939), pp. 567-577.

Tukey, J. W. *Convergence and uniformity in Topology.* Annals of Math. Studies, No. 2, Princeton, 1940.

Whitehead, A. N., y B. Russell. *Principia Mathematica,* 3 vols. Cambridge, England, 1910, 1912, 1913. 2a. edición, 1925, 1927, 1927.

Wiener, N. "A simplification of the logic of relations," *Proc. of the Cambridge Philosophical Soc.,* Vol. 17 (1914), pp. 387-390.

Zermelo, E. "Beweis, dass jede Menge wohlgeordnet werden kann," *Math. Annalen,* Vol. 59 (1904), pp. 514-516.

———"Untersuchungen über die Grundlagen der Mengenlehre: I," *Math. Annalen,* Vol. 65 (1908), pp. 261-281.

———"Sur les ensembles finis et le principe de l'induction complète," *Acta Math.,* Vol. 32 (1909), pp. 185-193 (paper dated 1907).

———"Über den Begriff der Definitheit in der Axiomatik," *Fundamenta Mathematicae,"* Vol. 14 (1929), pp. 339-344.

———"Über Grenzzahlen und Mengenbereiche," *Fundamenta Mathematicae,* Vol. 16 (1930), pp. 29-47.

Zorn, M. "A remark on method in transfinite algebra," *Bull. Amer. Math. Soc.,* Vol. 41 (1935), pp. 667-670.

GLOSARIO DE SIMBOLOS

SIMBOLO	NOMBRE DEL SIMBOLO	PAGINA
$-$	Negación	3
$\&$	Conjunción	3
$\vee$	Disyunción	3
$\rightarrow$	Implicación	3
$\leftrightarrow$	Equivalencia	3
$(\forall v)$	Cuantificador universal	3
$(\exists v)$	Cuantificador existencial	3
$(E!v)$	Cuantificador de unicidad	3
$=$	Identidad	3,11
$\in$	Pertenencia a un conjunto	4,11
0	Conjunto vacío	11
$\notin$	No pertenencia a un conjunto	16
$\subseteq$	Inclusión entre conjuntos	17
$\subset$	Inclusión propia	17
$A \cap B$	Intersección	18
$A \cup B$	Unión	19
$A \sim B$	Diferencia	20
$\langle x,y \rangle$	Pareja ordenada	22
$\{x: \varphi(x)\}$	Definición por abstracción	23
$\cup A$	Unión o suma de A	25,29
$\cap A$	Intersección de A	27,29
$\mathcal{P}A$	Conjunto potencia de A	31
$A \times B$	Producto cartesiano	32
$\mathfrak{D}A$	Dominio de A	38
$\mathfrak{R}A$	Recorrido de A	39
$\mathfrak{F}A$	Campo de A	39
$\breve{A}$	Conversa de A	39
A/B	Producto relativo de A y B	40
$R \vert A$	R restringida a A	41
$R``A$	Imagen de A bajo R	42
$\mathcal{I}A$	Relación de identidad en A	44
$\mathcal{S}(A, R, x)$	R-segmento de A generado por x	49
$R[x]$	R-clase de equivalencia de x	51
$\Pi(R)$	Partición de A generada por R	53
$\mathbf{R}(\Pi)$	Relación generada por una partición	54
$f \circ g$	Composición de funciones	55

SIMBOLO	NOMBRE DEL SIMBOLO	PAGINA
A^B	Conjunto de todas las funciones de B hacia A	56
$\approx$	Equipotencia	58
$\preceq$	Igual o menos potente	60
$\prec$	Menos potente que	61
$\overline{\overline{A}}$	Número cardinal del conjunto A	69,152
$\mathcal{K}(A)$	Número cardinal del conjunto A	70
$\mathfrak{m}'$	Sucesor del cardinal	74
$\mathfrak{Q}(\mathfrak{m})$	Conjunto de todos los precedentes del cardinal	75
$<\|A$	Menor que, restringido a A	78
εA	Relación de pertenencia sobre A	82
A'	Sucesor del conjunto A	84
ω	Conjunto de todos los ordinales finitos	88
$\mathfrak{S}_A$	Función sucesor, restringida a A	89
$\aleph_0$	Alef sub-cero	98
$\|x\|$	Valor absoluto de x	108
$\mathfrak{c}$	Número cardinal del continuo	121
$\{\alpha_\xi\}_{\xi<\mu}$	-sucesión de ordinales	136

INDICE DE AUTORES

INDICE