UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

APLICACIONES DE LA TEORIA DE CONJUNTOS AL ALGEBRA

T E S I S

Que para obtener el título de

ACTUARIO

p r e s e n t a

DANIEL CORDERO GRAU

FACULTAD DE CIENCIAS
UNAM

Director de Tesis: DR. HUGO ALBERTO RINCON MEJIA

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

MAT. MARGARITA ELVIRA CHÁVEZ CANO
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo de Tesis

"Aplicaciones de la Teoría de Conjuntos al Algebra"

realizado por Cordero Grau Daniel

con número de cuenta 9236842-0 , pasante de la carrera de Actuaría.

Dicho trabajo cuenta con nuestro voto aprobatorio

Atentamente

Director de Tesis Propietario	Dr. Hugo Alberto Rincón Mejía	Hugo G. Rincón M.
Propietario	Dra. Hortensia Galeana Sánchez	H. Galeana
Propietario	Dr. Juan González Hernández	Juan González Hernández
Suplente	M. en C. José Luis Gutiérrez Sánchez	
Suplente	M. en C. Alejandro Alvarado García	

Consejo Departamental de Matemáticas

M. en C. José Antonio Flores Díaz

Aplicaciones de la Teoría de Conjuntos al Algebra

Daniel Cordero Grau

24 de mayo de 2000

A mis padres.

Índice General

0.1 Prólogo

La Teoría de Conjuntos es un lenguaje. Sin ella, no sólo es imposible hacer matemáticas, sino que ni siquiera podemos decir de qué se trata ésta. Hewitt y Stromberg, en su libro "*Real and Abstract Analysis*", dicen: "*Desde el punto de vista de un lógico, las matemáticas son la Teoría de Conjuntos y sus consecuencias*".

Para la introducción a la Teoría de Conjuntos es muy útil trabajar con conjuntos concretos cuyos miembros sean objetos reales, pero los conjuntos de interés en matemáticas siempre tienen por miembros, objetos abstractos: El conjunto de todas las circunferencias en el plano, el conjunto de todos los puntos en una esfera, el conjunto de todos los número, etc. La Teoría Intuitiva de Conjuntos funciona bien para los primeros cursos de matemáticas (Cálculo y Álgebra entre otros). Pero definitivamente, para los cursos de matemáticas superiores es conveniente contar con una Teoría de Conjuntos sólida, pues nociones como las de cardinalidad o aplicaciones del Axioma de Elección son fundamentales e incluso indispensables en tópicos especializados del Análisis, Álgebra, Topología, etc.

En todas las épocas, los matemáticos y filósofos han empleado razonamientos de la Teoría de Conjuntos de modo más o menos consciente. Sin embargo, es necesario separar claramente todas las cuestiones relacionadas con la idea de número cardinal, y en particular, con la noción del infinito, de aquellas en las que solamente intervienen las nociones de pertenencia e inclusión, pues éstas son más intuitivas. Sólo apoyándose en ellas, es como se puede fundamentar una teoría de silogismos o axiomas como "el todo es mayor que cualquiera de sus partes".

A finales del siglo XIX ya no había dificultad alguna en hablar del conjunto de los objetos que poseen tal o cual propiedad; la célebre definición dada por el matemático alemán Georg Ferdinand Ludwig Philipp Cantor (1845-1918)[1]: "*Se entiende por conjunto a la agrupación en un todo de objetos bien diferenciados de nuestra intuición o nuestra mente*", apenas despertó objeciones al momento de su publicación. No sucedió así, cuando a la noción de conjunto vinieron a unirse las de número y magnitud. El problema de la divisibilidad de extensión da lugar a dificultades filosóficas considerables.

[1]Profesor de la Universidad de Halle. Publicó sus artículos básicos en "*Mathematische Annalen*" durante los años 1879-1893. Éstos fueron nuevamente editados por Zermelo en "*Grsammelte Abhandlungen mathematischen und philosophischen Inhalts*" en 1932 junto con una biografía de Cantor escrita también por Zermelo.

Matemáticos y filósofos fracasarían ante la paradoja[2] de una *magnitud finita formada por puntos infinitos "sin medida"*.

Las matemáticas clásicas evitan introducir en sus razonamientos el concepto del infinito "actual", i.e. conjuntos formados por una infinidad de elementos simultáneamente existentes, conformándose por un infinito "potencial" que se refiere a la posibilidad de aumentar toda magnitud dada. Si bien este punto de vista implica algo de hipocresía, permitió al menos, desarrollar la mayor parte de las matemáticas clásicas, incluyendo la Teoría de las Proporciones y más tarde, el Cálculo Infinitesimal.

Las necesidades del Análisis (en particular, el estudio a fondo de las funciones de variables reales que se desarrolló principalmente durante el siglo XIX) son el origen de lo que se convirtió en la Teoría de Conjuntos moderna. Cuando Bolzano, en 1817, demuestra la existencia del extremo inferior de un conjunto de números reales acotado inferiormente, todavía razona como la mayoría de sus contemporáneos: "En comprensión". No hablando de un conjunto cualquiera de números reales, sino de una propiedad arbitraria de estos últimos. Pero cuando treinta años más tarde, redacta sus "Paradoxien des Unendlichen" (Paradojas del Infinito), no duda en reivindicar el derecho de la existencia del infinito "actual" y en hablar de conjuntos arbitrarios. En este trabajo define la noción general de equipotencia de conjuntos, y demuestra que cualesquiera dos intervalos compactos en $\mathbb{R}$ son equipotentes. Observa también que la diferencia fundamental entre conjuntos finito e infinitos radica en que un conjunto infinito Ω es equipotente a un subconjunto distinto de Ω, pero no da ninguna demostración convincente de esta afirmación. Por otra parte, el tono general de esta obra tiene mucho más de filosófico que de matemático; y no pudiendo separar de una forma suficientemente clara la noción de potencia o cardinalidad de un conjunto, de la de magnitud y la de orden de infinitud, fracasa en su tentativa de formar conjuntos infinitos de potencias cada vez mayores, y termina por intercalar en sus razonamientos algunas consideraciones sobre las series divergentes, totalmente fuera de contexto.

La Teoría de Conjuntos, en el sentido que le damos hoy en día, se debe al genio de Georg Cantor. Él parte también del Análisis. Y sus estudios sobre las series trigonométricas, inspirados en los trabajos de Riemann (1826-1866), en 1872 le llevan de modo natural, a un primer intento de clasificación de los conjuntos "excepcionales" que aparecen en dicha teoría; mediante la noción

[2]Del griego $\pi\alpha\rho\grave{\alpha}\delta\delta\xi\alpha$: expectación.

de "*conjuntos derivados sucesivos*", que introduce con este fin. Como consecuencia de estas investigaciones y de su método para definir los números reales, Cantor comienza a interesarse por los problemas de equipotencia, ya que en 1873, hace notar que el conjunto de los números racionales (o el de números algebraicos) es numerable. En su correspondencia con Dedekind, que da comienzo hacia esta fecha, le vemos plantear el problema de equipotencia entre el conjunto de los números enteros y el conjunto de todos los números reales, que resuelve unas semanas más tarde. En 1874, Cantor intuye equivocadamente la imposibilidad de una biyección entre $\mathbb{R}$ y $\mathbb{R}^n$ $(n > 1)$. Posteriormente, descubre que tal correspondencia biunívoca existe.

Una vez en posesión de estos resultados, tan nuevos como sorprendentes, se consagra por entero a la Teoría de Conjuntos. En una serie de seis memorias publicadas en los "*Mathematische Annalen*" entre 1878 y 1884, ataca simultáneamente los problemas de equipotencia, la teoría de conjuntos totalmente ordenados, las propiedades topológicas de $\mathbb{R}$ y $\mathbb{R}^n$, y el problema de la medida. Entre sus manos van deslindándose poco a poco con una claridad admirable, nociones en apariencia indisolublemente unidas en la concepción clásica del "continuo". Ya en 1880, tiene la idea de iterar "transfinitamente" la formación de "*conjuntos derivados*", idea genitiva que fructifica dos años después de la introducción de conjuntos bien ordenados, uno de los descubrimientos más originales de Cantor, que le permite abordar un estudio detallado de los números cardinales y formular el "Problema del Continuo".

Resultaba totalmenta imposible que concepciones tan atrevidas, contrapuestas a una tradición dos veces milenaria, que concluían resultados tan inesperados y de un aspecto tan paradójico, se aceptasen sin resistencia. De hecho, entre los matemáticos influyentes de ese entonces en Alemania, Weiestrass (1815-1897) fue el único en seguir con cierto interés los trabajos de Cantor (que había sido alumno suyo). Pero Cantor se encontró con una actitud de oposición empecinada por parte de Schwarz, y sobre todo de Kronecker. La tensión constante engendrada por la oposición a sus ideas, así como los esfuerzos infructuosos realizados para demostrar la hipótesis del continuo, parecen ser las causas de los primeros síntomas de una enfermedad nerviosa cuyos efectos sobre su producción matemática pronto se hicieron notar.

Dedekind, guiado por sus trabajos en Aritmética y por la Teoría de Ideales, llegó a considerar la noción de conjunto ordenado desde un punto de vista más general que Cantor. Mientras que este último se limita a los conjuntos totalmente ordenados, Dedekind ataca el caso general y realiza un estudio

profundo de los conjuntos reticulados. Estos trabajos no tuvieron gran audiencia en su momento; sus resultados fueron analizados posteriormente por diversos autores, dando lugar a numerosas publicaciones desde 1935. La importancia histórica de los trabajos de Dedekind reside en el hecho de haber constituido uno de los primeros ejemplos de construcción axiomática; sin embargo, las aplicaciones de esta teoría han sido escasas. Por el contrario, los primeros resultados de Cantor sobre conjuntos numerables y la potencia del continuo rápidamente dieron lugar a numerosas e importantes aplicaciones, incluso dentro de las cuestiones más clásicas del Análisis.

Hacia finales del siglo XIX, se completa la formalización de las matemáticas y el método axiomático es universalmente aceptado. Pero simultáneamente, surge una crisis de fundamentos en el mundo matemático que durante más de treinta años, parece desquebrajar no sólo todas las adquisiciones recientes en aquel entonces, sino también las partes más clásicas de las matemáticas.

En 1899, Cantor observa en una carta a Dedekind, que no puede hablarse del "*conjunto de todos los conjuntos*" sin llegar a una contradicción. En 1905, Russell encuentra que la noción del "*conjunto de todos los conjuntos que no son elementos de sí mismos*" es también contradictoria.

Podría pensarse que tales antinomias aparecían únicamente en regiones periféricas de las matemáticas, caracterizadas por considerar conjuntos de una "magnitud" inaccesible a la intuición. Eran razonamientos tan alejados del uso común de los matemáticos, que a muchos de ellos les parecían simples juegos de palabras. No obstante, estas paradojas insistían en señalar la necesidad de una revisión a las bases de la Teoría de Conjuntos, a fin de eliminarlas. Pero si bien, había unanimidad en cuanto a la urgencia de esta revisión, enseguida surgieron divergencias en la forma y el método para llevarla a cabo. Pese a esto, se trató de dar una base axiomática a la Teoría de Conjuntos, como se hizo en el caso de la geometría elemental. Donde no hubiera que ocuparse de a qué cosas se les llama "conjuntos", ni de qué significa $x \in y$, sino que se enumeraran las condiciones impuestas a esta última relación. Naturalmente, esta axiomatización se trató de hacer de tal manera que se pudieran abarcar en todo lo posible, los resultados de Cantor. Teniendo cuidado de evitar la aparición de conjuntos paradójicos.

El primer modelo de este tipo de axiomatización fue dado por Zermelo en 1904. En éste, la introducción de conjuntos "muy grandes" se evita mediante el *axioma de comprensión*, que a grosso modo plantea que para determinar un conjunto con una propiedad $P(x)$, es necesario (y suficiente) que $P(x)$

implique una relación de la forma $x \in A$, para algún conjunto ya existente A. Después aparecieron otras axiomatizaciones de la Teoría de Conjuntos. Citamos principalmente la de Von Neumann, mucho más cercana que la de Zermelo, a la concepción primitiva de Cantor. Cantor había ya propuesto en su correspondencia con Dedekind, la distinción de dos tipos de entes para evitar los conjuntos paradójicos: Las multiplicidades y los conjuntos propiamente dichos; caracterizándose los segundos por ser pensados como un objeto único. Esta idea fue precisada por Von Neumann distinguiendo dos tipos de objetos: Las clases y los conjuntos. En su sistema (casi totalmente formalizado), las clases, a diferencia de los conjuntos, no pueden ser colocadas a la izquierda del signo $\in$. Una de las ventajas de este sistema, es que rehabililita la noción de clase "universal", empleada por los lógicos del siglo XIX. y que naturalmente no es un conjunto. Admás, la introducción de esquemas de axiomas es sustituida por axiomas convenientes, lo que simplifica el estudio lógico. Bernays y Gödel dieron variantes al sistema de Von Neumann.

La axiomatización de la teoría intuitiva de conjuntos de Cantor no sólo fue un acontecimiento muy destacado en los avances de las matemáticas del siglo XX, sino que también estableció que el método axiomático es posiblemente la manera más clara y precisa en la cual se puede dar una representación del conocimiento.

En este texto se presenta la Teoría de Conjuntos basada en los axiomas de Zermelo-Fraenkel y el Axioma de Elección. Una justificación para optar por la axiomatización de Zermelo-Fraenkel es que ésta es la más apropiada para un primer encuentro con la Teoría de Conjuntos y lo más importante es que los números reales, sus operaciones aritméticas y las demostraciones de sus propiedades pueden ser expresados a partir de ésta. Pero no sólo el sistema de los números reales encuentra sustento en los axiomas de Zermelo-Fraenkel, la mayor parte de las matemáticas contemporáneas (quizás la única excepción es la Teoría de Categorías) puede desarrollarse dentro de la Teoría de Conjuntos bajo estos axiomas. Por ejemplo, los objetos fundamentales de Topología, Álgebra o Análisis (espacios topológicos, espacios vectoriales, grupos, anillos, espacios de Banach) son apropiadamente definidos como conjuntos de una clase específica. Propiedades topológicas, algebraicas o analíticas de estos objetos son derivadas a partir de las propiedades de conjuntos, las cuales pueden obtenerse de los axiomas de Zermelo-Fraenkel. En este sentido, la Teoría de Conjuntos sirve como base para otras ramas de las matemáticas.

En el capítulo 1, la noción de propiedad se da de manera intuitiva y se introducen los axiomas del sistema ZF y el Axioma de Elección. En el capí-

tulo 2, se establecen las nociones fundamentales de relación, función, orden y operación; se definen los números naturales abstractos y sus propiedades bajo las operaciones de adición y multiplicación haciendo uso del Teorema de la Recursión. Finalizando este capítulo, se fundamenta la existencia del conjunto infinito $\{x, \mathbb{P}(x), \mathbb{P}(\mathbb{P}(x)), ...\}$ con el Teorema de la Recursión Generalizada. El capítulo 3 trata del Axioma de Elección y algunas de sus equivalencias con otras proposiciones importantes como el Lema de Zorn, el Teorema del Buen Orden y el Principio Máximo de Hausdorff. El propósito de esta información es el de mostrar las vastas aplicaciones de dicho axioma en diversas áreas de la Matemática. El capítulo 4 contiene tópicos de la Teoría de Cardinales. Finalmente, en el capítulo 5 se muestran algunas aplicaciones del Axioma de Elección y sus equivalencias, a la Teoría de Grupos, Teoría de Anillos, Teoría de Campos y espacios vectoriales.

Capítulo 1

AXIOMAS DE ZERMELO-FRAENKEL

1.1 Construcción de conjuntos

La lista que se dará es esencialmente la dada por Zermelo en 1908 con algunas modificaciones hechas por Skolem y Fraenkel en 1922. El sistema de la teoría de conjuntos que definen los axiomas es llamado ZF. Las nociones de "conjunto" y "pertenece a ($\in$)" no son definidas.

Definición 1

$$x \subseteq y \Leftrightarrow (\forall z)(z \in x \Rightarrow z \in y).$$

1.1.1 Igualdad entre conjuntos

Axioma 1 (extensión) *Dos conjuntos son iguales si y sólo si tienen los mismos elementos.*

Otra manera de expresar la condición necesaria y suficiente para la igualdad de dos conjuntos x y y es:

$$(\forall z)((z \in x \Rightarrow z \in y) \wedge (z \in y \Rightarrow z \in x)).$$

O bien,

$$(\forall x)\,(\forall y)\,(x = y \Leftrightarrow x \subseteq y \wedge y \subseteq x)\,.$$

Observación 1

$$\neg(x \subseteq y) \text{ se denota } x \subsetneq y.$$

Y significa

$$(\exists z)(z \in x \wedge z \notin y).$$

1.1.2 El conjunto vacío

Axioma 2 (conjunto vacío) *Existe un conjunto sin elementos.*

Proposición 1 *El conjunto vacío es único.*

Demostración. Suponga que existen $\emptyset_1$ y $\emptyset_2$ conjuntos vacíos tales que

$$\emptyset_1 \neq \emptyset_2,$$

entonces

$$(\exists x)\left(x \in \emptyset_1 \wedge x \notin \emptyset_2 \vee x \notin \emptyset_1 \wedge x \in \emptyset_2\right),$$

entonces

$$x \in \emptyset_1 \vee x \in \emptyset_2, !,$$

entonces

$$(\nexists x)\left(x \in \emptyset_1 \wedge x \notin \emptyset_2 \vee x \notin \emptyset_1 \wedge x \in \emptyset_2\right),$$

entonces

$$\emptyset_1 = \emptyset_2,$$

$\therefore$ el conjunto vacío es único. ■

Se denota por el símbolo $\emptyset$.

1.1.3 La unión entre conjuntos

Axioma 3 (pares) *Dados dos conjuntos cualesquiera x y y, existe un conjunto u cuyos elementos son x y y.*

O bien,

$$(\forall x)(\forall y)(\exists u)(u = \{x, y\}).$$

Este axioma da una manera de construir conjuntos. Teniéndose en particular, para $x = y$:

Dado un conjunto cualquiera x, existe un conjunto u cuyo único elemento es x.

O bien,

$$(\forall x)(\exists u)(u = \{x\}).$$

Axioma 4 (unión) *Dado un conjunto cualquiera x, existe un conjunto que tiene como elementos a los elementos de los elementos de x.*

En otras palabras,

$$(\forall z)\,(z \in \cup x \Leftrightarrow (\exists y)\,(y \in x \wedge z \in y))\,.$$

Así, los axiomas 3 y 4 garantizan la unión de dos conjuntos. Definiendo $x \cup y$ como $\cup\{x, y\}$, la unión de conjuntos finitos está dada de la siguiente manera.

Sean x, y y z conjuntos cualesquiera. Se define $\{x, y, z\}$ como $\cup\{\{x, y\}, \{z\}\}$; así, para $n \geq 3$ y $x_1, x_2, ..., x_n$ conjuntos cualesquiera se define $\{x_1, x_2, ..., x_n\}$ como $\cup\{\{x_1, x_2, , x_{n-1}\}, \{x_n\}\}$.

Observación 2

$$(\forall x)\,(\forall y)\,(\cup x \neq \cup y \Rightarrow x \neq y)\,.$$

Demostración. Sean x y y conjuntos cualesquiera tales que

$$\cup x \neq \cup y,$$

entonces

$$(\exists u)(u \in \cup x \wedge u \notin \cup y \vee u \in \cup y \wedge u \notin \cup x),$$

entonces

$$(\exists v)(u \in v \wedge (v \in x \wedge v \notin y \vee v \in y \wedge v \notin x)),$$

$\therefore x \neq y$. ■

1.1.4 El conjunto potencia

Axioma 5 (conjunto potencia) *Dado cualquier conjunto x, existe un conjunto que contiene todos los subconjuntos de x.*

Se conoce como el conjunto potencia y se denota por $\mathbb{P}(x)$.

Ejemplo 1

$$(\forall x)\,(\cup\mathbb{P}(x) = x)\,.$$

Demostración. $\Rightarrow$) Sean x un conjunto no vacío cualquiera y

$$u \in \cup\mathbb{P}(x),$$

entonces

$$(\exists v)(v \in \mathbb{P}(x) \wedge u \in v),$$

entonces

$$v \subseteq x \wedge u \in x,$$

entonces

$$(\forall u)(u \in \cup\mathbb{P}(x) \Rightarrow u \in x),$$

entonces

$$\cup\mathbb{P}(x) \subseteq x.$$

$\Leftarrow$) Sea $u \in x$, entonces

$$\{u\} \in \mathbb{P}(x) \wedge u \in \cup\mathbb{P}(x),$$

entonces

$$(\forall u)(u \in x \Rightarrow u \in \cup\mathbb{P}(x),$$

entonces

$$x \subseteq \cup\mathbb{P}(x),$$

entonces

$$\cup\mathbb{P}(x) \subseteq x \wedge x \subseteq \cup\mathbb{P}(x),$$

$\therefore x = \cup\mathbb{P}(x)$. ■

Hasta aquí termina el primer grupo de axiomas, que corresponde a las propiedades básicas de conjuntos y construcción de éstos.

1.2 El principio de comprensión

Los siguientes dos axiomas están relacionados con el principio de comprensión. Ésta es la parte del sistema original de Zermelo que fue modificado más tarde por Skolem y Fraenkel. Zermelo postuló el axioma de especificación:

> Dado un conjunto cualquiera x, y una "propiedad P", existe un conjunto que tiene todos los elementos de x que poseen la propiedad P.

La noción de "propiedad" nunca fue explicada satisfactoriamente por Zermelo, lo que llevó a Skolem a dar una definición más precisa. Aseverando que el que "x tenga la propiedad P" debe ser representado por una fórmula construida a partir de proposiciones de la forma $a \in b$ o $a = b$, de operaciones lógicas y cuantificadores, lo que lleva a la siguiente definición.

1.2.1 Fórmulas bien formadas

Definición 2 *Se define como fórmula bien formada a toda fórmula construida a partir de proposiciones de la forma $a \in b$ o $a = b$, utilizando operaciones lógicas tales como la conjunción ($\wedge$), la disyunción ($\vee$), la negación ($\neg$) y la implicación ($\Rightarrow$) y los cuantificadores de la manera usual ($\forall$ y $\exists$).*

Axioma 6 (especificación) *Dada cualquier fórmula bien formada $A(y)$ de ZF y un conjunto cualquiera x, existe un conjunto cuyos elementos son todos aquellos elementos y de x para los cuales $A(y)$ vale.*

Ejemplo 2 *Si x es un conjunto cualquiera no vacío, entonces existe el conjunto $\{\{a\} : a \in x\}$.*

Demostración. Sea $a \in x$, entonces

$$\{a\} \in \mathbf{P}(x),$$

entonces, por el axioma 6,

$$\{\{a\} \in \mathbf{P}(x) : a \in x\},$$

$\therefore$ es un conjunto. ■

1.2.2 El conjunto de conjuntos

Proposición 2 *No existe U, el conjunto de conjuntos.*

Demostración. Suponga que existe U, el conjunto de conjuntos. Sea

$$x = \{y \in U : y \notin y\},$$

entonces

$$x \notin x \Rightarrow x \in x.$$

Pero

$$x \in x \Rightarrow x \notin x,$$

entonces

$$x \in x \wedge x \notin x, !,$$

$\therefore$ no existe U, el conjunto de conjuntos. ■

Ejemplo 3 *Si x es un conjunto fijo cualquiera, entonces $\{y : y \sim x\}$[1] no es un conjunto.*

Demostración. Sea

$$u \in x \wedge z \notin x \wedge y = (x \backslash \{u\}) \cup \{z\},$$

entonces

$$x \sim y \wedge z \in y,$$

entonces

$$y \in \{y : y \sim x\} \wedge z \in \cup\{y : y \sim x\},$$

entonces

$$(\forall z)(z \in x \cup \cup\{y : y \sim x\}),$$

entonces

$$x \cup \cup\{y : y \sim x\}$$

es el conjunto de conjuntos, !,
$\therefore \{y : y \sim x\}$ no es un conjunto. ■

[1] Véanse definiciones 26 y 29.

Ejemplo 4 *Si G es un grupo*[2] *fijo cualquiera, entonces $\{H : H$ es un grupo isomorfo a $G\}$ no es un conjunto.*

Demostración. Sea

$$Y \notin G \wedge U \in G \wedge X = (G \backslash \{U\}) \cup \{Y\},$$

entonces

$$X \sim G \wedge Y \in X,$$

definimos $f : X \times X \to X$ tal que:

$$f(a,b) = \left\{ \begin{array}{ll} a \cdot b, & \text{si } a \neq Y \wedge b \neq Y \\ a \cdot U, & \text{si } b = Y \\ U \cdot b, & \text{si } a = Y \\ U \cdot U, & \text{si } a = b = Y \end{array} \right\}$$

donde $\cdot$ es la operación[3] de G, entonces

$$X \in \{H : H \text{ es un grupo isomorfo a } G\},$$

entonces

$$Y \in \cup\{H : H \text{ es un grupo isomorfo a } G\},$$

entonces

$$(\forall Y)(Y \in G \cup \cup\{H : H \text{ es un grupo isomorfo a } G\}),$$

entonces

$$G \cup \cup\{H : H \text{ es un grupo isomorfo a } G\}$$

es el conjunto de conjuntos, !,
$\therefore \{H : H$ es un grupo isomorfo a $G\}$ no es un conjunto. ■

[2]Véanse definiciones 26 y 32.
[3]Véase definición 20.

1.2.3 Funciones como fórmulas bien formadas

Nótese que el axioma de especificación sólo permite construir conjuntos como subconjuntos de algún conjunto dado y no considera conjuntos como

$$\{x, \mathbb{P}(x), \mathbb{P}(\mathbb{P}(x)), ...\}.$$

Esta dificultad fue resuelta por Fraenkel en 1922 al proponer el axioma del reemplazo.

Definición 3 *Una fórmula bien formada $F(x,y)$ define una función si y sólo si*

$$(\forall x)(\forall y)(\forall z)(F(x,y) \wedge F(x,z) \Rightarrow y = z).$$

O bien,

Una fórmula bien formada $F(x,y)$ define una función si y sólo si dado un conjunto cualquiera x, existe a lo más un conjunto y, tal que $F(x,y)$ vale.

Axioma 7 (reemplazo) *Sea $F(x,y)$ una fórmula bien formada de ZF, que define una función. Entonces, dado un conjunto cualquiera u, existe un conjunto v que contiene todos los elementos y tales que $F(x,y)$ vale para algún $x \in u$.*

1.3 Conjuntos infinitos

Los primeros siete axiomas dan las propiedades de los conceptos de pertenencia, unión, intersección y construcción de conjuntos de la manera usual; mas note que la construcción depende de la noción del conjunto de los números naturales y además el axioma del reemplazo no permite construir conjuntos infinitos sin la referencia previa a otro conjunto infinito. Por esto se estableció el siguiente axioma.

Axioma 8 (infinito) *Existe un conjunto x tal que:*

$$\text{i) } \emptyset \in x.$$
$$\text{ii) } (\forall u)(u \in x \Rightarrow u \cup \{u\} \in x).$$

Axioma 9 (fundamentación) *Todo conjunto no vacío x contiene un elemento ajeno a x.*

1.3.1 Las $\in$-sucesiones infinitas

Teorema 1 *No existe una sucesión infinita* $\{x_n\}$ *con* $n \in \mathbb{N}$, *tal que*

$$x_{n+1} \in x_n.$$

Demostración. Sea x un conjunto con elementos $x_0, x_1, x_2, \ldots$.
Suponga que

$$(\forall n \in \mathbb{N})(x_{n+1} \in x_n).$$

Por el axioma 9,

$$(\exists y)(y \in x \wedge x \cap y = \emptyset),$$

entonces

$$(\exists k \in \mathbb{N})(y = x_k),$$

entonces

$$x_{k+1} \in y,$$

entonces

$$x_{k+1} \in x \cap y, !,$$

$\therefore$ no existen dichas sucesiones. ■

Corolario 1 *En particular, si* $x \in x$ *se tendría la sucesión infinita* $\ldots \in x \in x \in x$, *que por el ejemplo anterior, no existe; por lo tanto,*

$$(\forall x)(x \notin x).$$

Teorema 2

$$(\nexists x)(\nexists y)(x \in y \wedge y \in x).$$

Demostración. Suponga que

$$(\exists x)(\exists y)(x \in y \wedge y \in x),$$

entonces se tiene la sucesión infinita

$$\ldots \in x \in y \in x \in y,$$

que por el axioma de la fundamentación, no existe,
$\therefore$ no existen tales conjuntos. ■

Ejemplo 5 *Muestre una sucesión infinita* $x_0, x_1, x_2, \ldots$ *tal que* $x_{n+1} \subseteq x_n$.

Demostración. Sea

$$x_n = \{x \in \mathbf{N} : x > n\},$$

$\therefore x_{n+1} \subseteq x_n$. ■

Teorema 3 *No existen conjuntos* x, y *y* z *tales que* $x \in y \wedge y \in z \wedge z \in x$.

Demostración. Suponga que

$$(\exists x)(\exists y)(\exists z)(x \in y \wedge y \in z \wedge z \in x),$$

entonces se tiene la sucesión infinita

$$\ldots \in x \in y \in z \in x \in y,$$

lo cual contradice el axioma de la fundamentación,
$\therefore$ no existen tales conjuntos. ■

Ejemplo 6 *Una* $\in$*-sucesión descendente es una sucesión de conjuntos* $x_0, x_1, x_2, \ldots$ *tales que* $x_{n+1} \in x_n$. *El axioma de la fundamentación implica que dicha sucesión es finita. Muestre un conjunto que contenga* $\in$*-sucesiones descendentes de longitud arbitraria.*

Demostración. El conjunto x con la propiedad de que

$$x_0 \in x \wedge (\forall x_{i+1} \in x_i)(x_{i+1} \cup \{x_{i+1}\} \in x_i) \wedge i \in \mathbf{N},$$

contiene $\in$-sucesiones descendentes de longitud arbitraria. ■

1.3.2 El conjunto de elecciones

Axioma 10 (elección) *Dado un conjunto no vacío* x*, cuyos elementos son conjuntos no vacíos ajenos dos a dos, existe un conjunto que contiene uno y sólo un elemento de cada conjunto contenido en* x.

El conjunto obtenido se conoce como el conjunto de elecciones. Este axioma fue incluido en la lista original de Zermelo en 1908; sin embargo, generalmente no es incluido en los axiomas de ZF; quizás, porque los matemáticos siempre lo han tratado con suspicacia y últimamente, los investigadores han estado más interesados en la teoría de conjuntos sin él.

Capítulo 2

MATEMÁTICAS EN ZF

2.1 Relaciones y funciones

En este capítulo se definirán los conceptos de par ordenado, función y número natural. Nuestra definición de número natural debe ser comprendida como la definición de "número natural abstracto", que de ninguna manera sustituye la noción y clara intuición que tenemos de los números naturales. Las ideas en esta sección se encargan exclusivamente de demostrar la validez del sistema ZF como un auténtico reflejo de las matemáticas y no redefinen alguna noción previa.

La idea más importante a la que no se hace referencia explícita es la de relación (una función es un caso particular de relación). Anteriormente, hemos considerado una relación como un conjunto de pares ordenados y así será considerada dentro de ZF; pero primero tendremos que definir lo que es un par ordenado. Aunque la definición puede parecer un poco extraña al principio, la formalidad de la definición puede ser olvidada una vez que las propiedades están dadas.

2.1.1 Pares ordenados

Definición 4 *Para conjuntos x y y, el par ordenado de x y y es el conjunto $\{\{x\},\{x,y\}\}$ y se denota (x,y).*

Teorema 4

$$(\forall a)(\forall b)(\forall x)(\forall y)((a,b)=(x,y)\Rightarrow a=x\wedge b=y).$$

Demostración. Sean a, b, x y y conjuntos cualesquiera tales que

$$(a, b) = (x, y),$$

entonces

$$\{a\} = \{x\} \wedge \{a, b\} = \{x, y\} \vee \{a\} = \{x, y\} \wedge \{a, b\} = \{x\},$$

entonces

$$a = x \wedge b = y \vee a = b = x = y,$$

$\therefore a = x \wedge b = y.$ ■

La definición de par ordenado puede ser extendida inductivamente.

Definición 5

i) $(\forall x)(\forall y)(\forall z)((x, y, z) = ((x, y), z))$.
ii) $(\forall x_1)...(\forall x_{n-1})((x_1, ..., x_{n-1}) = ((x_1, ..., x_n), x_{n+1})), \forall n \in \mathbf{N}$.

Ejemplo 7

$$(\forall a)(\forall b)(\forall c)(\forall x)(\forall y)(\forall z)((a, b, c) = (x, y, z) \Rightarrow a = x \wedge b = y \wedge c = z).$$

Demostración. Sean a, b, c, x, y y z conjuntos cualesquiera tales que

$$(a, b, c) = (x, y, z).$$

Como

$$(a, b, c) = ((a, b), c) \wedge (x, y, z) = ((x, y), z),$$

entonces

$$(a, b) = (x, y) \wedge c = z,$$

$\therefore a = x \wedge b = y \wedge c = z.$ ■

Desde aquí (x, y) debe ser visto como un objeto que forma parte de nuestro sistema formal, cuyas propiedades a utilizar no serán más que las propiedades antes demostradas.

Ejemplo 8 $\{(x,y) : x \sim y\}$[1] *no es un conjunto.*

Demostración. Sea x un conjunto no vacío cualquiera.
Sean

$$z \notin x \wedge u \in x \wedge y = (x \backslash \{u\}) \cup \{z\},$$

entonces

$$(x,y) \in \{(x,y) : x \sim y\},$$

entonces

$$x, y \in \cup\cup\{(x,y) : x \sim y\},$$

entonces

$$(\forall z)(z \in (\cup\cup\{(x,y) : x \sim y\}) \cup (\cup\cup\cup\{(x,y) : x \sim y\})),$$

entonces

$$(\cup\cup\{(x,y) : x \sim y\}) \cup (\cup\cup\cup\{(x,y) : x \sim y\})$$

es el conjunto de conjuntos, !,
$\therefore \{(x,y) : x \sim y\}$ no es un conjunto. ■

2.1.2 El producto cartesiano

Como sabemos, el producto cartesiano de dos conjuntos x y y es el conjunto de todos los pares ordenados (a,b) tales que $a \in x \wedge b \in y$. Para construir $x \times y$ en ZF usaremos el axioma de especificación. Si $a \in x \wedge b \in y$, entonces, como

$$(a,b) = \{\{a\}, \{a,b\}\} \subseteq \mathbf{P}(\{a,b\}) \wedge \{a,b\} \subseteq x \cup y,$$

tenemos que

$$(a,b) \subseteq \mathbf{P}(x \cup y),$$

y así,

$$(a,b) \in \mathbf{P}(\mathbf{P}(x \cup y)).$$

[1] Véanse definiciones 26 y 29.

Definición 6

$$(\forall x)(\forall y)(x \times y = \{z \in \mathbf{P}(\mathbf{P}(x \cup y)) : (\exists a)(\exists b)(a \in x \wedge b \in y \wedge z = (a,b))\}).$$

Esta definición puede ser extendida inductivamente.

Definición 7

$$(\forall x_1), ..., (\forall x_{n+1})(x_1 \times ... \times x_{n+1} = (x_1 \times ... \times x_n) \times x_{n+1}), \forall n \in \mathbf{N}.$$

Ejemplo 9

$$(\forall x)(\forall y)(\forall z)(x \times y \times z = \{(a,b,c) : a \in x \wedge b \in y \wedge c \in z\}).$$

Demostración. Sean x, y y z conjuntos cualesquiera,
entonces

$$x \times y \times z = (x \times y) \times z = \{(u,c) : u \in x \times y \wedge c \in z\},$$

pero

$$(\forall u \in x \times y)(\exists a)(\exists b)(a \in x \wedge b \in y \wedge u = (a,b)),$$

entonces

$$(x \times y) \times z = \{((a,b),c) : a \in x \wedge b \in y \wedge c \in z\},$$

$\therefore x \times y \times z = \{(a,b,c) : a \in x \wedge b \in y \wedge c \in z\}$. ■

2.1.3 Relaciones binarias

Definición 8 *Una relación binaria es un subconjunto del producto cartesiano de dos conjuntos; es decir*

$$(\exists x)(\exists y)(z \subseteq x \times y)$$

significa que z es una relación binaria. En particular, una relación binaria en un conjunto x es un subconjunto de $x \times x$.

Definición 9 *El dominio de una relación binaria z es el conjunto de los primeros elementos de los pares ordenados en z; es decir*

$$\{x \in \cup(\cup z) : (\exists y)((x,y) \in z)\}.$$

Definición 10 *El rango de una relación binaria z es el conjunto de los segundos elementos de los pares ordenados en z; es decir*

$$\{y \in \cup(\cup z) : (\exists x)((x,y) \in z)\}.$$

Ejemplo 10 *Si R es una relación binaria, entonces $\{y : (\exists x)((x,y) \in R)\}$ es un conjunto.*

Demostración. Sea $(x,y) \in R$, entonces

$$x \in \cup\cup R \wedge y \in \cup\cup R,$$

de donde

$$(\exists u)(u = \{y \in \cup\cup R : (\exists x)((x,y) \in R)\}),$$

$\therefore \{y \in \cup\cup R : (\exists x)((x,y) \in R\}$ es un conjunto. ■

2.1.4 Relaciones de equivalencia

Definición 11 *z es una relación de equivalencia en x se expresa como:*

$$(z \subseteq x \times x) \wedge (\forall u)(u \in x \Rightarrow (u,u) \in z) \wedge$$
$$(\forall u)(\forall v)(u \in x \wedge v \in x \wedge (u,v) \in z \Rightarrow (v,u) \in z) \wedge$$
$$(\forall u)(\forall v)(\forall w)(u \in x \wedge v \in x \wedge w \in x \wedge (u,v) \in z \wedge (v,w) \in z \Rightarrow (u,w) \in z).$$

Lo que significa que z es una relación binaria en x; que es reflexiva, simétrica y transitiva.

Nótese que, de esta manera, se tiene la relación de equivalencia en un conjunto; la equinumerosidad de conjuntos no es una relación de equivalencia en ese sentido, puesto que al suponerse lo contrario, se llegaría a una contradicción similar a la paradoja de Russell. Además, por un ejemplo previo, sabemos que para cualquier conjunto x, $\{x : x \sim y\}$ no es un conjunto. Sin embargo, si z es una relación de equivalencia en un conjunto x, entonces las clases de equivalencia pueden ser definidas como conjuntos.

2.1.5 Relaciones de orden parcial

Definición 12 *z es una relación de orden parcial en un conjunto x se expresa como:*

$$(z \subseteq x \times x) \wedge (\forall u)(u \in x \Rightarrow (u,u) \in z) \wedge$$
$$(\forall u)(\forall v)(u \in x \wedge v \in x \wedge (u,v) \in z \wedge (v,u) \in z \Rightarrow u = v) \wedge$$
$$(\forall u)(\forall v)(\forall w)(u \in x \wedge v \in x \wedge w \in x \wedge (u,v) \in z \wedge (v,w) \in z \Rightarrow (u,w) \in z).$$

Lo que significa que z es una relación binaria en x; que es reflexiva, antisimétrica y transitiva.

2.1.6 Relaciones de orden total

Definición 13 *z es una relación de orden total en un conjunto x se expresa como:*

$$(z \subseteq x \times x) \wedge (\forall u)(u \in x \Rightarrow (u,u) \in z) \wedge$$
$$(\forall u)(\forall v)(u \in x \wedge v \in x \wedge (u,v) \in z \wedge (v,u) \in z \Rightarrow u = v) \wedge$$
$$(\forall u)(\forall v)(\forall w)(u \in x \wedge v \in x \wedge w \in x \wedge (u,v) \in z \wedge (v,w) \in z \Rightarrow (u,w) \in z) \wedge$$
$$(\forall u)(\forall v)(u \in x \wedge v \in x \Rightarrow (u,v) \in z \vee (v,u) \in z).$$

Lo que significa que z es una relación binaria en x; que es reflexiva, antisimétrica, transitiva y conexa.

Definición 14 *c es una cadena en un conjunto x ordenado por una relación de orden z se expresa como:*

$$(c \subseteq x) \wedge (\forall u)(u \in c \Rightarrow (u,u) \in z) \wedge$$
$$(\forall u)(\forall v)(u \in c \wedge v \in c \wedge (u,v) \in z \wedge (v,u) \in z \Rightarrow u = v) \wedge$$
$$(\forall u)(\forall v)(\forall w)(u \in c \wedge v \in c \wedge w \in c \wedge (u,v) \in c \wedge (v,w) \in c \Rightarrow (u,w) \in z) \wedge$$
$$(\forall u)(\forall v)(u \in c \wedge v \in c \Rightarrow (u,v) \in z \vee (v,u) \in z).$$

Lo que significa que c es un subconjunto de x, que está totalmente ordenado por z.

2.1.7 Relaciones de buen orden

Definición 15 *z es una relación de buen orden en un conjunto x se expresa como:*

$$(z \subseteq x \times x) \wedge (\forall u)(u \in x \Rightarrow (u,u) \in z) \wedge$$
$$(\forall u)(\forall v)(u \in x \wedge v \in x \wedge (u,v) \in z \wedge (v,u) \in z \Rightarrow u = v) \wedge$$
$$(\forall u)(\forall v)(\forall w)(u \in x \wedge v \in x \wedge w \in x \wedge (u,v) \in z \wedge (v,w) \in z \Rightarrow (u,w) \in z) \wedge$$
$$(\forall u)(\forall v)(u \in x \wedge v \in x \Rightarrow (u,v) \in z \vee (v,u) \in z) \wedge$$
$$(\forall u)(\forall v)(u \subseteq x \wedge v \in u \Rightarrow (\exists! w)(w \in u \wedge (w,v) \in z)).$$

Lo que significa que z es una relación binaria en x; que es reflexiva, antisimétrica, transitiva y conexa; y que todo subconjunto de x tiene un elemento mínimo.

2.1.8 Funciones

Definición 16 *Una función f se expresa como:*

$$(\exists x)(\exists y)(f \subseteq x \times y) \wedge (\forall u)(\forall v)(\forall w)((u,v) \in f \wedge (u,w) \in f \Rightarrow v = w).$$

Lo que significa que f es una relación binaria y f tiene un solo valor para cada elemento del dominio.

Definición 17 *Una función f es inyectiva se expresa como:*

$$(\exists x)(\exists y)(f \subseteq x \times y) \wedge (\forall u)(\forall v)(\forall w)((u,v) \in f \wedge (u,w) \in f \Rightarrow v = w) \wedge$$
$$(\forall u)(\forall v)(\forall w)((u,w) \in f \wedge (v,w) \in f \Rightarrow u = v).$$

Lo que significa que f es una función y f no tiene valores repetidos.

Definición 18 *Una función f es suprayectiva se expresa como:*

$$(\exists x)(\exists y)(f \subseteq x \times y) \wedge (\forall u)(\forall v)(\forall w)((u,v) \in f \wedge (u,w) \in f \Rightarrow v = w) \wedge$$
$$(\forall u)(u \in x \Rightarrow (\exists v)(v \in y \wedge (u,v) \in f)) \wedge$$
$$(\forall u)(u \in y \Rightarrow (\exists v)(v \in x \wedge (v,u) \in f).$$

Lo que significa que f es una función y el conjunto de todos los valores de f es igual al conjunto y.

Definición 19 *Una función f es biyectiva se expresa como:*

$$(\exists x)(\exists y)(f \subseteq x \times y) \wedge (\forall u)(\forall v)(\forall w)((u,v) \in f \wedge (u,w) \in f \Rightarrow v = w) \wedge$$
$$(\forall u)(\forall v)(\forall w)((u,w) \in f \wedge (v,w) \in f \Rightarrow u = v) \wedge$$
$$(\forall u)(u \in x \Rightarrow (\exists v)(v \in y \wedge (u,v) \in f)) \wedge$$
$$(\forall u)(u \in y \Rightarrow (\exists v)(v \in x \wedge (v,u) \in f)).$$

Lo que significa que f es una función inyectiva y suprayectiva.

2.1.9 Operaciones binarias

Definición 20 *Una operación binaria $*$ en un conjunto A es una función $f : A \times A \to A$ tal que*

$$(\forall a, b \in A)(\exists! c \in A)(f(a,b) = c).$$

2.1.10 Composición de funciones

Teorema 5 *Si f y g son funciones tales que $Im(f) \subseteq Dom(g)$, entonces $g \circ f$ existe.*

Demostración. P. d. $g \circ f$ es un conjunto y $g \circ f$ es una función.

$$x \in \text{Dom}\,(g \circ f) \Leftrightarrow (\exists z)((x,z) \in g \circ f) \Leftrightarrow (\exists y)((x,y) \in f \wedge (y,z) \in g) \Leftrightarrow$$
$$x \in \text{Dom}(f) \wedge y = f(x) \in \text{Dom}(g) \wedge z \in \text{Im}(g),$$

entonces

$$g \circ f = \{(x,z) : (\exists y)((x,y) \in f \wedge (y,z) \in g)\}.$$

Sea

$$(x,y) \in g \circ f \wedge (x,z) \in g \circ f,$$

entonces

$$(\exists u)(\exists v)((x,u) \in f \wedge (u,y) \in g \wedge (x,v) \in f \wedge (v,z) \in g),$$

entonces

$$u = v \wedge (v,z) = (u,z),$$

entonces

$$y = z,$$

entonces $g \circ f$ es una función;
$\therefore g \circ f$ existe. ■

El conjunto de todas las funciones de un conjunto a otro puede ser construido de la siguiente manera:

Si x y y son conjuntos y f es una función cuyo dominio es x y su imagen es un subconjunto de y, entonces f es un subconjunto de $x \times y$; es decir $f \in \mathbf{P}(x \times y)$ y así el conjunto de todas las funciones de x a y es:

$$\{f \in \mathbf{P}(x \times y) : (\forall u)(u \in x \Rightarrow (\exists v)(v \in y \wedge (u, v) \in f) \wedge (\forall u)(\forall v)(\forall w)((u, v) \in f \wedge (u, w) \in f \Rightarrow v = w)\}.$$

O bien,

$\{f \in \mathbf{P}(x \times y) :$ dominio de f es x y la imagen de f es de dimensión uno$\}$.

2.1.11 Familias de conjuntos

Utilizando la misma idea de función, podemos establecer la noción de una colección (o familia) de conjuntos en nuestro sistema por medio de la siguiente definición.

Definición 21 *Una familia de conjuntos es una función F de un conjunto índice I a un conjunto rango. Intuitivamente, $\{F(i) : i \in I\}$ es la familia de conjuntos.*

Nótese que una familia es diferente a un conjunto de conjuntos, ya que un conjunto puede repetirse en una familia, pero sólo cuenta una vez como elemento de un conjunto. Por ejemplo, la función $f : \mathbf{N} \to \mathbf{P}(\mathbb{R})$ tal que $f(n) = \mathbb{R}$, $\forall n \in \mathbf{N}$, es una familia, pero $\{f(n) : n \in \mathbf{N}\}$ como conjunto tiene un elemento.

Ejemplo 11 *Para conjuntos cualesquiera x y y, el conjunto de todas las biyecciones de la forma $f : x' \to y'$, donde $x' \subseteq x \wedge y' \subseteq y$, existe.*

Demostración. El conjunto de todas las biyecciones de un subconjunto x' de x a cualquier sunconjunto de y es

$$\begin{aligned} F(x') = \{f \in \mathbb{P}(x' \times y) : (\forall u)(\forall v)(\forall w)((u,v) \in f \wedge (u,w) \in f \Rightarrow v = w) \wedge \\ (\forall u)(u \in x' \Rightarrow (\exists v)(v \in y \wedge (u,v) \in f)) \wedge \\ (\forall u)(u \in y \Rightarrow (\exists v)(v \in x' \wedge (v,u) \in f)) \wedge \\ (\forall u)(\forall v)(\forall w)((u,w) \in f \wedge (v,w) \in f \Rightarrow u = v)\}, \end{aligned}$$

entonces la familia de todas las biyecciones de la forma $f : x' \to y$ es

$$\{F(i) : i \in x\},$$

$\therefore$ el conjunto de todas las biyecciones de la forma $f : x' \to y'$ existe. ■

Ejemplo 12 *Si z es una relación de equivalencia en x, entonces el conjunto de las clases de equivalencia existe i.e. el conjunto cociente.*

Demostración. Sea

$$u \in x \wedge F(u) = \{v \in x : (u,v) \in z\},$$

entonces $F(u)$ es la clase de equivalencia determinada por u, entonces

$$\{F(u) : u \in x\}$$

es el conjunto de las clases de equivalencia de x,
$\therefore$ el conjunto de las clases de equivalencia existe. ■

Así, hemos visto como objetos matemáticos que a primera vista no son conjuntos, pueden ser definidos como tales dentro de la teoría de conjuntos. Igualmente, hemos tratado con nociones básicas que nos dan una buena herramienta para trabajar con álgebra abstracta. Ahora, procederemos a desarrollar y definir los números dentro de nuestra teoría de conjuntos.

2.2 Los números naturales abstractos

Primero daremos una base intuitiva para la definición del conjunto de los números naturales abstractos. Si x es un conjunto, entonces el conjunto $x \cup \{x\}$ se denota por x^+ y se conoce como el sucesor de x. Utilizando la operación sucesor, podemos construir la sucesión de conjuntos $\emptyset, \emptyset^+, \emptyset^{++}, \emptyset^{+++}, ...$

Así, los números naturales abstractos serán los elementos de esta sucesión, a saber:

0 es $\emptyset$
1 es $\emptyset^+$, i.e. $\{\emptyset\}$
2 es $\emptyset^{++}$, i.e. $\{\emptyset, \{\emptyset\}\}$
3 es $\emptyset^{+++}$, i.e. $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, etc.

Obsérvese que 0 es un conjunto sin elementos, 1 es un conjunto con un elemento, 2 tiene dos elementos y 3 tiene tres elementos. En general, si x es un conjunto con n elementos, entonces x^+ tiene $n+1$ elementos y claramente, el número natural abstracto n es un conjunto con n elementos. Los objetos que hemos llamado $0, 1, 2, ...$ son conjuntos de cierta particularidad, mas lo que queremos saber es si la colección de todos ellos $\{0, 1, 2, ...\}$ es un objeto legítimo de discusión en ZF. Como vimos anteriormente, el único método para construir un conjunto infinito a partir de conjuntos finitos es por medio del axioma del infinito, por esto, una de las principales razones por las cuales se estableció, es para garantizar la legitimidad del conjunto $\{0, 1, 2, ...\}$ dentro de ZF. Una vez establecido este axioma, los demás axiomas pueden ser utilizados para construir otros conjuntos infinitos.

2.2.1 Conjuntos inductivos

Definición 22 *Se dice que un conjunto x es un conjunto inductivo si:*

$$\text{i) } \emptyset \in x.$$
$$\text{ii) } (\forall y)(y \in x \Rightarrow y^+ \in x).$$

Nótese que el axioma del infinito por sí mismo, asegura que existe un conjunto inductivo, y que los elementos de la sucesión $\emptyset, \emptyset^+, \emptyset^{++}, ...$ son elementos de cualquier conjunto inductivo. Mas lo que estamos buscando es un conjunto inductivo que no contenga otros elementos.

Teorema 6 *Existe un conjunto inductivo mínimo, i.e. un conjunto inductivo que es subconjunto de cualquier conjunto inductivo.*

Demostración. Por el axioma del infinto,
existe un conjunto inductivo x.
Por los axiomas 5 y 6,

$$(\exists v)(v = \{u \in \mathbf{P}(x) : u \text{ es un conjunto inductivo}\}.$$

Entonces

$$(\forall u)(\forall z)(u \in v \wedge z \subseteq u \Rightarrow z \in v).$$

P. d. $\cap v$ es un conjunto inductivo.
Suponga que

$$(\exists z)(z \in \cap v \wedge z^{+} \in \cap z),$$

entonces

$$(\forall u)(\exists z)(u \in v \wedge z \in u \wedge z+ \notin u), !,$$

$$\therefore \cap v \text{ es indcutivo.}$$

P. d.$\cap v$ es mínimo.
Sea z un conjunto inductivo cualquiera, entonces

$$x \cap z \subseteq x \Rightarrow x \cap z \in v,$$

entonces

$$(\forall z)(z \in v \Rightarrow \cap v \subseteq z),$$

$\therefore \cap v$ es el conjunto inductivo mínimo. ■

Definición 23 *Los números naturales abstractos son los elementos del conjunto inductivo mínimo dado por el teorema anterior. Este conjunto inductivo es denotado por ω. Desde luego, ya que ω es un conjunto inductivo, todos los términos de la sucesión $\emptyset, \emptyset^{+}, \emptyset^{++}, \emptyset^{+++}, \ldots$ son elementos de ω. En otras palabras, habiendo definido $0, 1, 2, 3, \ldots$ como anteriormente se hizo, todos ellos son los números naturales abstractos.*

Este procedimiento algo indirecto fue necesario para evitar métodos intuitivos que no son parte de ZF. Aún no hemos mostrado que los elementos de ω son exclusivamente $0, 1, 2, \ldots$ y nada más. Partiendo del axioma del infinito, trabajamos hacia abajo, por así decirlo, para llegar a ω, ya que los métodos más "naturales" para construir conjuntos a partir de sus elementos no están disponibles en este sistema. El uso de "así sucesivamente" es un proceso intuitivo que debe ser evitado en ZF. Aún habiendo definido ω de esta manera, podemos comenzar a deducir las propiedades de sus elementos. Primero demostraremos que la base que dan los axiomas de Zermelo-Fraenkel satisface los axiomas de Peano. Esto es, que los elementos de ω se comportan como los números naturales.

2.2.2 Los Axiomas de Peano

Teorema 7 $(\omega, +, 0)$ *es un modelo para los axiomas de Peano, i.e.*

$$\text{i) } 0 \in \omega.$$
$$\text{ii) } x^+ \in \omega, \forall x \in \omega.$$
$$\text{iii) Si } x \in \omega, \text{ entonces } x^+ \neq 0.$$
$$\text{iv) Si } x, y \in \omega \wedge x^+ = y^+, \text{ entonces } x = y.$$
$$\text{v) Si } A \subseteq \omega \wedge 0 \in A \wedge (\forall x \in A)(x^+ \in A), \text{ entonces } A = \omega.$$

Demostración. i) Esto es obvio.
ii) Suponga que $x = x^+$, entonces

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

entonces

$$x \subseteq x \cup \{x\} \wedge x \cup \{x\} \subseteq x,$$

entonces

$$x \subseteq x \wedge \{x\} \subseteq x,$$

entonces

$$\{x\} \subseteq x, !,$$

$$\therefore x \neq x^+.$$

iii) Suponga que $x^+ = 0$, entonces

$$x^+ = \emptyset,$$

entonces

$$x \cup \{x\} = \emptyset,$$

entonces

$$x \cup \{x\} \subseteq \emptyset \wedge \emptyset \subseteq x \cup \{x\},$$

entonces

$$x \cup \{x\} \subseteq \emptyset, \ !,$$

$$\therefore x^+ \neq 0.$$

iv) Suponga que $x^+ = y^+$, entonces

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

entonces

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

entonces

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

$$\therefore x = y.$$

v) Suponga que

$$(\forall x \in A)(A \subseteq \omega \wedge 0 \in A \wedge x^+ \in A),$$

entonces A es un conjunto inductivo, pero

$$(\forall S)(S \text{ es un conjunto inductivo} \Rightarrow \omega \subseteq S),$$

entonces

$$A \subseteq \omega \wedge \omega \subseteq A,$$

$\therefore A = \omega$. ■

Ahora, tenemos que definir las operaciones adición y multiplicación verificando que tienen las propiedades necesarias. Para esto, necesitaremos recurrir a un importante teorema llamado el Teorema de la Recursión; pero antes de demostrarlo, consolidaremos lo que tenemos hasta aquí, asentaremos algunas propiedades de ω y sus elementos, y veremos como funciona el principio de inducción en la práctica.

Teorema 8

$$(\forall n \in \omega)(n \in n^+)$$
$$(\forall n \in \omega)(n \subseteq n^+)$$
$$(\forall n \in \omega)(\cup n^+ = n).$$

Demostración. i) Sea $n \in \omega$, entonces

$$n^+ = n \cup \{n\},$$

pero

$$n \in \{n\} \Rightarrow n \in n \cup \{n\} = n^+,$$

$$\therefore n \in n^+.$$

ii) Sea $n \in \omega$, entonces

$$n^+ = n \cup \{n\},$$

pero

$$n \subseteq n \Rightarrow n \subseteq n \cup \{n\},$$

$$\therefore n \subseteq n^+.$$

iii) Sea $n \in \omega$, entonces

$$n^+ = n \cup \{n\},$$

entonces

$$\cup(n \cup \{n\}) = (\cup n) \cup (\cup\{n\}) = (\cup n) \cup n = n,$$

$\therefore \cup n^+ = \cup(n \cup \{n\}) = n.$ ■

Corolario 2

$$m, n \in \omega \wedge m^+ = n^+ \Rightarrow m = n.$$

Demostración. Sean

$$m, n \in \omega \wedge m^+ = n^+,$$

entonces, por el teorema anterior,

$$m = \cup m^+ = \cup n^+ = n,$$

$\therefore m = n.$ ■

2.2.3 El Teorema de la Recursión

Ahora, recordemos la propiedad básica de la definición de la operación adición en **N**.

Existe una función $f : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$ denotada por $+$, con las propiedades:

$$\text{i) } m + 0 = m.$$
$$\text{ii) } m + n\prime = (m + n)\prime.$$

Donde $x\prime = x + 1, \forall x \in \mathbf{N}$.

Debemos verificar que lo anterior se cumple dentro de nuestro conjunto ω de números naturales abstractos y con la operación sucesor. Primero daremos un método para construir funciones del cual, la función denotada por $+$, es un caso particular; éste se conoce como definición por inducción. Naturalmente, está relacionado con el principio de inducción, pero no debe ser confundido con él. Para garantizar la existencia de funciones definidas por métodos inductivos, necesitaremos el Teorema de la Recursión (una consecuencia de los axiomas de ZF). Así, será aplicado a los casos particulares de la adición y la multiplicación.

Teorema 9 (de la Recursión) *Si x es un conjunto cualquiera, $a \in x$ y ϕ es una función de x a x, entonces existe una y sólo una función f de ω a un subconjunto de x tal que:*

$$\text{i) } f(0) = a.$$
$$\text{ii) } f(n^+) = \phi(f(n)), \forall n \in \omega.$$

Demostración. Sea

$$u = \{z \in \mathbf{P}(\omega \times x) : (0,a) \in z \wedge (\forall y)(\forall t)((y,t) \in z \Rightarrow (y^+, f(t)) \in z)\},$$

entonces

$$\omega \times x \in u \Rightarrow u \neq \emptyset.$$

Sea

$$f = \cap u \wedge s = \mathrm{Dom}(f),$$

entonces

$$s \subseteq \omega,$$

entonces

$$f \subseteq u \Rightarrow (0,a) \in f \Rightarrow 0 \in s,$$

entonces, si $n \in s$,

$$((n,t) \in f \Rightarrow (n^+, f(t)) \in f) \Rightarrow n^+ \in s,$$

entonces, por el teorema 7,

$$s = \omega.$$

Sea

$$r = \{y \in \omega : (\exists! b)((b \in x) \wedge (y,b) \in f)\}.$$

Suponga que

$$(\exists c \in x)(a \neq c \wedge (0,c) \in f).$$

Sea

$$f\prime = f \setminus \{(0,c)\},$$

entonces

$$f\prime \in u,$$

entonces

$$\cap u \subseteq f\prime \subset f = \cap u, !,$$

$$\therefore 0 \in r.$$

Suponga que

$$(\exists! b \in x)((y,b) \in f),$$

entonces

$$(y^+, f(b)) \in f.$$

Suponga que

$$(\exists d \in x)((y^+,d) \in f \wedge d \neq f(b)).$$

Sea

$$f\prime\prime = f \setminus \{(y^+,d)\},$$

entonces

$$f\prime\prime \in u,$$

entonces

$$\cap u \subseteq f\prime\prime \subset f = \cap u, !,$$

entonces, por el principio de inducción,

$$y, y^+ \in r, \forall y \in x,$$

$$\therefore r = \omega \wedge f \text{ es una función.}$$

P. d. f es única.
Sea

$$u \subseteq x \wedge \phi : x \to x,$$

y suponga que

$$(\exists f : \omega \to u)(\exists g : \omega \to u)(f(0) = a = g(0) \wedge f(n^+) = \phi(f(n)) \wedge g(n^+) = \phi(g(n))).$$

Por inducción sobre n.
a)

$$f(0) = a = g(0).$$

b) Suponga que

$$f(n) = k = g(n).$$

c) Entonces

$$f(n^+) = \phi(f(n)) = \phi(k) = \phi(g(n)) = g(n^+).$$

Entonces

$$(\forall n \in \omega)(f(n) = g(n)).$$

$\therefore f = g.$ ■

El Teorema de la Recursión también puede ser expresado por medio de diagramas:

$$\begin{array}{ccccc} & & \omega & \xrightarrow{()^+} & \omega \\ \{0\} & \overset{\circ}{\swarrow} & \downarrow \exists! f & & \downarrow \exists! f \\ & & x & \xrightarrow{\phi} & x \end{array}$$

2.2.4 La adición

El desarrollo de la aritmética en ZF viene a partir del Teorema de la Recursión, ya que la definición de la adición y la multiplicación dependen de él.

Sea $m \in \omega$ fijo. Definimos una función s_m aplicando el Teorema de la Recursión tal que:

$$s_m(n) = m + n, \forall n \in \omega.$$

(s_m es la función '$m+$').

Definición 24

$$s_m(0) = m.$$
$$s_m(n^+) = (s_m(n))^+, \forall n \in \omega.$$

O bien,

$$\{0\} \overset{0}{\underset{m}{\swarrow}} \begin{array}{ccc} \omega & \xrightarrow{0^+} & \omega \\ \downarrow s_m & & \downarrow s_m \\ \omega & \xrightarrow{0^+} & \omega \end{array}$$

Hemos definido la adición, para $m, n \in \omega$ cualesquiera, como $s_m(n) = m+n$. Sin embargo, quedan por demostrar las leyes conmutativa y asociativa de la adición.

Teorema 10

$$i)\ 0 + n = n, \forall n \in \omega.$$
$$ii)\ m^+ + n = (m + n)^+, \forall m, n \in \omega.$$
$$iii)\ m + n = n + m, \forall m, n \in \omega.$$
$$iv)\ (m + n) + p = m + (n + p), \forall m, n, p \in \omega$$

Demostración. i) Por definición, s_0 es la única función que hace conmutativo el diagrama

$$\begin{array}{ccc} & \omega & \xrightarrow{()^+} & \omega \\ \{0\} \overset{0}{\underset{0}{\swarrow\!\searrow}} & \downarrow s_0 & & \downarrow s_0 \\ & \omega & \xrightarrow{()^+} & \omega \end{array}$$

pero Id_ω también hace conmutativo

$$\begin{array}{ccc} & \omega & \xrightarrow{()^+} & \omega \\ \{0\} \overset{0}{\underset{0}{\swarrow\!\searrow}} & \downarrow Id_\omega & & \downarrow Id_\omega \\ & \omega & \xrightarrow{()^+} & \omega \end{array}$$

entonces, por el Teorema de la Recursión,

$$s_0 = Id_\omega,$$

$$\therefore 0 + m = m, \forall m \in \omega.$$

ii)

$$m^+ + n = s_{m^+}(n) \wedge (m+n)^+ = ()^+ \circ s_m(n).$$

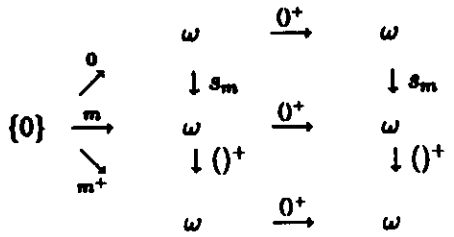
P. d.

$$s_{m^+}(n) = ()^+ \circ s_m(n),$$

por definición, s_{m^+} es la única función $\omega \to \omega$ que hace conmutativo el diagrama

$$\begin{array}{ccc} & \omega & \xrightarrow{()^+} & \omega \\ \{0\} \overset{0}{\underset{m^+}{\swarrow\!\searrow}} & \downarrow s_{m^+} & & \downarrow s_{m^+} \\ & \omega & \xrightarrow{()^+} & \omega \end{array}$$

pero

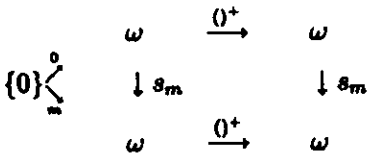


también es conmutativo,
entonces, por el Teorema de la Recursión,

$$s_{m^+}(n) = ()^+ \circ s_m(n),$$

$$\therefore m^+ + n = (m+n)^+, \forall m, n \in \omega.$$

iii) Por inducción sobre m



1) Por i)

$$0 + n = s_0(n) = I_\omega = n,$$

y además, por definición,

$$n + 0 = s_n(0) = n,$$

$$\therefore 0 + n = n + 0.$$

2) Suponga que

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

3) Por ii),

$$m^+ + n = (m + n)^+,$$

por 2),

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

Resta demostrar que

$$n + m^+ = (n + m)^+,$$

pero

$$\begin{array}{ccc} & \omega & \xrightarrow{()^+} & \omega \\ \{0\} \overset{0}{\underset{m}{\swarrow}} & \downarrow s_m & & \downarrow s_m \\ & \omega & \xrightarrow{()^+} & \omega \end{array}$$

entonces

$$s_n(m^+) = s_n \circ ()^+(m) = ()^+ \circ s_n(m) = (n + m)^+;$$

$$\therefore m + n = n + m, \forall m, n \in \omega.$$

iv)

$$(m + n) + p = s_{m+n}(p) \wedge m + (n + p) = s_m \circ s_n(p).$$

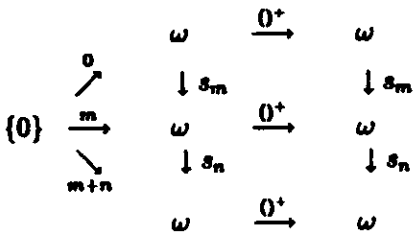
P. d.

$$s_{m+n} = s_m \circ s_n$$

por definición, s_{m+n} es la única función $\omega \to \omega$
que hace conmutativo el diagrama

$$\begin{array}{ccc} & \omega & \xrightarrow{()^+} & \omega \\ \{0\} \overset{0}{\underset{m+n}{\swarrow}} & \downarrow s_{m+n} & & \downarrow s_{m+n} \\ & \omega & \xrightarrow{()^+} & \omega \end{array}$$

pero



también conmuta,
entonces, por el Teorema de la Recursión,

$$s_{m\,|\,n} = s_m \circ s_n,$$

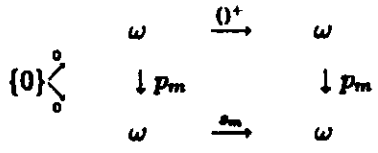
$\therefore (m+n)+p = m+(n+p), \forall m,n,p \in \omega.$ ■

2.2.5 La multiplicación

Definimos p_m para todo $m \in \omega$ tal que:

$$\text{i) } p_m(0) = 0.$$
$$\text{ii) } p_m(n^+) = m + p_m(n), \forall n \in \omega.$$

O bien,



Definimos la multiplicación como $mn = p_m(n)$ para algunos $m,n \in \omega$, mientras que para números arábigos se usará el símbolo $\cdot$ (ejemplo $2 \cdot 3 = 1 \cdot 6$). Primero demostraremos que $x \to m+x$ es una función, la cual está dada por el conjunto

$$\{z \in \omega \times \omega : (\exists x)(\exists y)(z = (x,y) \wedge y = m + x)\}$$

para algún $m \in \omega$ fijo.

Demostración. Sea

$$(x, y) \in z \wedge (x, u) \in z,$$

entonces

$$y = m + x \wedge u = m + x,$$

entonces

$$y = u,$$

$\therefore x \to m + x$ es una función en ω. ■

Ahora, demostraremos las propiedades conocidas tales como las leyes conmutativa, asociativa y distributiva.

Teorema 11

$$i)\ 0 \cdot n = 0, \forall n \in \omega.$$
$$ii)\ m^+ n = mn + n, \forall m, n \in \omega.$$
$$iii)\ mn = nm, \forall m, n \in \omega.$$
$$iv)\ (m + n)r = mr + nr, \forall m, n, r \in \omega.$$
$$v)\ (mn)r = m(nr), \forall m, n, r \in \omega.$$
$$vi)\ 1 \cdot m = m, \forall m \in \omega.$$

Demostración. i) Existe una y sólo una función $O : \omega \to \{0\}$ que hace conmutativo el diagrama

$$\begin{array}{ccc} & \omega & \xrightarrow{0^+} & \omega \\ \{0\} \overset{0}{\underset{0}{\leftarrow}} & \downarrow o & & \downarrow o \\ & \{0\} & \xrightarrow{s_0} & \{0\} \end{array}$$

pero por definición,

$$\begin{array}{ccc} & \omega & \xrightarrow{0^+} & \omega \\ \{0\} \overset{0}{\underset{0}{\leftarrow}} & \downarrow p_0 & & \downarrow p_0 \\ & \{0\} & \xrightarrow{s_0} & \{0\} \end{array}$$

conmuta, entonces

$$O = p_0,$$

i.e.

$$(\forall n \in \omega)(p_0(n) = 0),$$

$$\therefore (\forall n \in \omega)(0 \cdot n = 0).$$

ii) Por inducción sobre n.

$$\begin{array}{ccc} \omega & \xrightarrow{0^+} & \omega \\ \downarrow p_{m^+} & & \downarrow p_{m^+} \\ \omega & \xrightarrow{s_{m^+}} & \omega \end{array} \qquad \{0\}$$

1) Por definición,

$$m^+ \cdot 0 = p_{m^+}(0) = 0,$$

pero

$$(m \cdot 0) + 0 = p_m(0) + 0 = 0 + 0 = s_0(0) = 0,$$

$$\therefore m^+ \cdot 0 = (m \cdot 0) + 0.$$

2) Suponga que

$$m^+ n = mn + n.$$

3) Entonces

$$m^+ n^+ = m^+ + m^+ n = m^+ + (mn + n) = (mn + m + n)^+,$$

pero

$$mn^+ + n^+ = (m + mn) + n^+ = ((mn + m) + n)^+ = (mn + m + n)^+,$$

entonces

$$m^+n^+ = mn^+ + n^+.$$

$$\therefore m + n = mn + n, \forall m, n \in \omega.$$

iii) Por inducción sobre m.

$$\begin{array}{ccc} \omega & \xrightarrow{()^+} & \omega \\ \{0\}\overset{0}{\underset{0}{\leftleftarrows}} & \downarrow p_m & \downarrow p_m \\ \omega & \xrightarrow{s_m} & \omega \end{array}$$

1) Por i),

$$0 \cdot n = 0,$$

y por definición,

$$p_n(0) = n \cdot 0 = 0,$$

$$\therefore 0 \cdot n = n \cdot 0.$$

2) Suponga que

$$mn = nm.$$

3) Por ii),

$$m^+n = mn + n,$$

y por definición,

$$nm^+ = p_n(m^+) = n + p_n(m) = n + nm = nm + n,$$

y por 2),

$$nm + n = mn + n,$$

entonces

$$m^+ n = nm^+.$$

$$\therefore (\forall m, n \in \omega)(mn = nm).$$

iv) Por iii),

$$(m+n)r = r(m+n) = p_r \circ s_m(n),$$

y

$$mr + nr = rm + rn = s_{rm} \circ p_r(n),$$

P. d.

$$p_r \circ s_m = s_{rm} \circ p_r.$$

Por definición, la composición $s_{rm} \circ p_r$ es la única función $\omega \to \omega$ que hace que el siguiente diagrama conmute

$$\begin{array}{ccccc} & & \omega & \xrightarrow{()^+} & \omega \\ & \overset{0}{\nearrow} & \downarrow p_r & & \downarrow p_r \\ \{0\} & \xrightarrow{0} & \omega & \xrightarrow{s_r} & \omega \\ & \underset{rm}{\searrow} & \downarrow s_{rm} & & \downarrow s_{rm} \\ & & \omega & \xrightarrow{s_r} & \omega \end{array}$$

pero la composición $p_r \circ s_m$ hace el siguiente diagrama conmutativo

$$\begin{array}{ccccc} & & \omega & \xrightarrow{()^+} & \omega \\ & \overset{0}{\nearrow} & \downarrow s_m & & \downarrow s_m \\ \{0\} & \xrightarrow{m} & \omega & \xrightarrow{()^+} & \omega \\ & \underset{rm}{\searrow} & \downarrow p_r & & \downarrow p_r \\ & & \omega & \xrightarrow{s_r} & \omega \end{array}$$

entonces

$$p_r \circ s_m = s_{rm} \circ p_r,$$

$$\therefore (m+n)r = mr + nr, \forall m, n, r \in \omega.$$

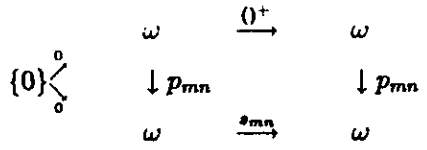
v)

$$(mn)r = p_{mn}(r) \wedge m(nr) = p_m \circ p_n(r).$$

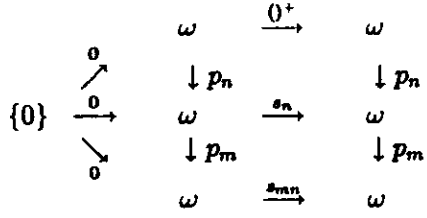
P. d.

$$p_{mn} = p_m \circ p_n.$$

por definición, p_{mn} es la única función
que hace que el diagrama siguiente conmute



pero

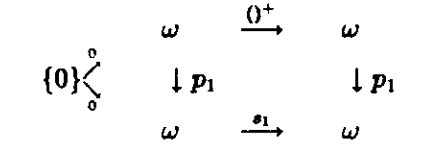


también conmuta, entonces

$$p_{mn} = p_m \circ p_n,$$

$$\therefore (mn)r = m(nr), \forall m, n, r \in \omega.$$

vi) Por definición, p_1 es la única función $\omega \to \omega$
que hace que el siguiente diagrama conmute



pero

$$\begin{array}{ccccc} & & \omega & \xrightarrow{0^+} & \omega \\ \{0\} & \overset{\nearrow}{\underset{\searrow}{}} & \downarrow Id_\omega & & \downarrow Id_\omega \\ & & \omega & \xrightarrow{s_1} & \omega \end{array}$$

entonces

$$p_1 = Id_\omega,$$

$\therefore (\forall n \in \omega)(1 \cdot n = n)$. ■

2.2.6 El orden de los números naturales abstractos

Para establecer el orden de los números naturales dentro de ZF, definimos $m < n$ como:

$$(\exists x)(x \in \omega \wedge x \neq 0 \wedge m + x = n).$$

Siendo ésta, una extensión de nuestro lenguaje formal, las propiedades de $<$ son consecuencia lógica de las propiedades de la adición.

Sin embargo, nuestros números abstractos tienen ciertas propiedades que tal vez no esperamos. Éstas resultan del hecho de que los números han sido definidos como conjuntos. Quizás la más importante esté en el teorema 13, pero para demostrarlo haremos uso del siguiente teorema:

Teorema 12

$$(\forall m, n \in \omega)(m \in m + n^+).$$

Demostración. Sea

$$A = \{y \in \omega : (\forall m \in \omega)(m \in m + y^+)\},$$

entonces, por definición de $+$,

$$m + 0^+ = (m + 0)^+ = m^+,$$

entonces, por el teorema 8,

$$m \in m^+,$$

$$\therefore 0 \in A.$$

Suponga que $y \in A$, i.e.

$$(\forall m \in \omega)(m \in m + y^+);$$

entonces

$$m + (y^+)^+ = (m + y^+)^+,$$

pero

$$(m + y^+)^+ = (m + y^+) \cup \{m + y^+\} \wedge m \in m + y^+,$$

entonces

$$(\forall m \in \omega)(m \in m + (y^+)^+),$$

entonces

$$(\forall y \in \omega)(y^+ \in \omega),$$

$\therefore A = \omega$. ■

Teorema 13

$$(\forall m, n \in \omega)(m < n \Leftrightarrow m \in n).$$

Demostración. $\Rightarrow$) Suponga que

$$m, n \in \omega \wedge m < n,$$

i.e.

$$(\exists x \in \omega)(x \neq 0 \wedge m + x = n),$$

entonces

$$x \neq 0 \Rightarrow (\exists p \in \omega)(x = p^+),$$

entonces

$$m + x = m + p^{+} = n,$$

y por el teorema 12,

$$m \in m + p^{+},$$

$$\therefore m \in n.$$

ii) Sea

$$A = \{y \in \omega : (\forall z)(z \in \omega \wedge z \in y \Rightarrow z < y)\},$$

como

$$(\forall z \in \omega)(z \notin 0),$$

entonces

$$(\forall z \in \omega)(z \in 0 \Rightarrow z < 0)$$

vale,

$$\therefore 0 \in A.$$

Suponga que $y \in A$. Tómese un $z \in \omega$ arbitrario tal que $z \in y^{+}$, pero

$$y^{+} = y \cup \{y\} \Rightarrow z \in y \vee z = y,$$

entonces:
1) Si $z \in y$, por hipótesis de inducción,

$$z \in \omega \wedge z \in y \Rightarrow z < y,$$

entonces

$$(\exists x \in \omega)(x \neq 0 \wedge z + x = y),$$

entonces, por el teorema 10,

$$z + x^{+} = y^{+},$$

$$\therefore z < y^+.$$

2) Si $z = y$, entonces

$$z + 1 = y^+,$$

entonces

$$z < y^+,$$

entonces

$$(\forall z < y)(z < y^+),$$

entonces

$$(\forall y \in A)(y^+ \in A),$$

$\therefore A = \omega$. ■

Tal vez inesperadamente, hemos mostrado que la relación '$\in$' entre números es la misma que '$<$'. No menos interesante es el siguiente teorema.

Teorema 14

i) $(\forall m, n, p \in \omega)(m \in n \wedge n \in p \Rightarrow m \in p)$.
ii) $(\forall m, n \in \omega)(m \in n \Rightarrow m \subseteq n)$.
iii) $m, n \in \omega \wedge m \neq n \wedge m \subseteq n \Rightarrow m \in n$.
iv) ω *es un conjunto transitivo i.e.* $n \in \omega \Rightarrow n \subseteq \omega$.
v) $n = \{m \in \omega : m < n\}, \forall m, n \in \omega$.

Demostración. i) Si

$$m \in n \wedge n \in p \wedge m, n, p \in \omega,$$

entonces

$$(\exists x, y \in (\omega \backslash \{0\}))(m + x = n \wedge n + y = p),$$

entonces

$$(m + x) + y = m + (x + y) = p,$$

entonces

$$m < p,$$

$$\therefore m \in p.$$

ii) Suponga que

$$m, n \in \omega \wedge m \in n,$$

entonces, por i),

$$(\forall k \in m)(k \in n),$$

$$\therefore m \subseteq n.$$

iii) Sea

$$A = \{n \in \omega : (\exists m)(m \in \omega \wedge m \neq n \wedge m \subseteq n \Rightarrow m \in n)\},$$

a)

$$(\forall m \in \omega)(m \subsetneq 0),$$

entonces

$$\neg(m \in \omega \wedge m \neq 0 \wedge m \subseteq 0),$$

entonces

$$(m \in \omega \wedge m \neq 0 \wedge m \subseteq 0) \Rightarrow m \in 0$$

vale.

$$\therefore 0 \in A.$$

b) Suponga que $n \in A$. i.e.

$$(\exists m)(m \in \omega \wedge m \neq n \wedge m \subseteq n \Rightarrow m \in n);$$

c) Suponga que

$$(\exists m)(m \in \omega \wedge m \neq n^+ \wedge m \subseteq n^+),$$

entonces

$$m \in \omega \wedge m \neq n^+ \wedge m \subseteq n \cup \{n\},$$

entonces

$$m \in \omega \wedge m \neq n^+ \wedge (m = n \vee m \subset n).$$

1) Si

$$m \in \omega \wedge m \neq n^+ \wedge m = n,$$

entonces

$$m \in \omega \wedge m \neq n^+ \wedge m \subseteq n^+ \wedge m \in n^+,$$

entonces,

$$m \in \omega \wedge m \neq n^+ \wedge m \subseteq n^+ \Rightarrow m \in n^+$$

vale.
2) Si

$$m \in \omega \wedge m \neq n^+ \wedge m \subset n,$$

entonces,

$$m \in \omega \wedge m \neq n \wedge m \subseteq n.$$

Entonces, por 2),

$$m \in n.$$

Entonces, por i),

$$m \in n \wedge n \in n^+ \Rightarrow m \in n^+.$$

$$\therefore m \in \omega \wedge m \neq n^+ \wedge m \subseteq n^+ \Rightarrow m \in n^+.$$

i.e.

$$(\forall n \in A)(n^+ \in A),$$

$$\therefore A = \omega.$$

iv) Sea

$$B = \{y \in \omega : y \in \omega \Rightarrow y \subseteq \omega\},$$

sabemos que

$$0 \in \omega \wedge 0 \subseteq \omega,$$

entonces

$$0 \in \omega \Rightarrow 0 \subseteq \omega$$

vale

$$\therefore 0 \in B.$$

Suponga que $y \in B$, i.e.

$$y \in \omega \Rightarrow y \subseteq \omega,$$

entonces

$$y^+ \in \omega \Leftrightarrow (y \cup \{y\}) \in \omega,$$

pero

$$y \in \omega \Rightarrow \{y\} \in \mathbf{P}(\omega),$$

entonces

$$\{y\} \subseteq \omega,$$

y además

$$y \in \omega \wedge (y \in \omega \Rightarrow y \subseteq \omega),$$

entonces

$$y \subseteq \omega,$$

entonces

$$y \subseteq \omega \wedge \{y\} \subseteq \omega,$$

entonces

$$(y \cup \{y\}) \subseteq \omega,$$

entonces

$$y^+ \subseteq \omega,$$

entonces

$$y^+ \in \omega \Rightarrow y^+ \subseteq \omega$$

vale, entonces

$$(\forall y \in B)(y^+ \in B),$$

$$\therefore B = \omega.$$

v) Suponga que $n \in \omega$, entonces, por iv),

$$n \subseteq \omega,$$

entonces

$$(\forall m \in n)(m \in \omega),$$

pero, por el teorema 13,

$$m \in n \Leftrightarrow m < n,$$

entonces

$$(\forall m \in n)(m < n),$$

$\therefore n = \{m \in \omega : m < n\}$. ■

Así, hemos establecido por completo la teoría formal de los números en ZF. Las propiedades, métodos y nociones matemáticas han sido formalmente descritas. Cualquier argumento que se tenga sobre dichas nociones , puede ser llevado a nuestro sistema formal, ya que los razonamientos matemáticos son deducciones lógicas; la construcción de sistemas de números son un ejemplo. Los métodos algebraicos conocidos para los números, pueden ser llevados a ZF con sutiles modificaciones, debido a que en ZF las nociones de número natural, adición, multiplicación, orden, función, relación de equivalencia y clase de equivalencia son adecuadas.

2.2.7 El Teorema de la Recursión Generalizada

Existe un detalle, mencionado en la página 4, que no hemos justificado en ZF, este es la construcción del conjunto $\{x, \mathbf{P}(x), \mathbf{P}(\mathbf{P}(x)), ...\}$, donde x es un conjunto cualquiera, y la construcción de una función f cuyo dominio sea ω tal que $f(n) = \mathbf{P}^n(x)$. Puede parecer a primera vista que el Teorema de la Recursión es suficiente, puesto que podemos escribir

$$f(n) = \left\{ \begin{array}{c} f(0) = x \\ f(n^+) = \mathbf{P}(f(x)), \forall n \in \omega \end{array} \right\}$$

y por el axioma del reemplazo, el conjunto $\{x, \mathbf{P}(x), \mathbf{P}(\mathbf{P}(x)), ...\}$ es la imagen de f en ω.

Esto no puede ser porque $\mathbf{P}$ no es una función. Es decir, dado un conjunto cualquiera x, $\mathbf{P}(x)$ denota su conjunto potencia, pero $x \rightarrow \mathbf{P}(x)$ no puede ser una función porque su dominio sería el conjunto de conjuntos que por la Proposición 2, sabemos que no existe. Por esto, estableceremos un principio aún más general.

Teorema 15 (de la Recursión Generalizada) *Si $F(x, y)$ es una fórmula de ZF tal que para cada conjunto x existe uno y sólo un conjunto y tal que $F(x, y)$ vale, entonces dado un conjunto a, existe una única función f con dominio ω tal que:*

$$\begin{array}{c} \text{i) } f(0) = a. \\ \text{ii) } F(f(n), f(n^+)) \text{ , } \forall n \in \omega. \end{array}$$

Demostración. Sea

$$A = \{n \in \omega : (\forall m < n)(\exists f_n)(\exists a)(\mathrm{Dom}(f_n) = \{0, 1, ..., n\} \wedge f_n(0) = a \wedge F(f_n(m), f_n(m^+)))\}.$$

P.d. $A = \omega$.
a) La función $f_0 : \{0\} \to \{a\}$ es tal que

$$(\forall m < 0)(\exists a)(f_0(0) = a \wedge F(f_0(m), f_0(m^+))).$$

$$\therefore 0 \in A.$$

b) Suponga que $n \in A$. i.e.

$$(\forall m < n)(\exists f_n)(\exists a)(\mathrm{Dom}(f_n) = \{0, 1, ..., n\} \wedge f_n(0) = a \wedge F(f_n(m), f_n(m^+))).$$

c) Por definición de $F(x, y)$,

$$(\exists! y)(F(f_{n^+}(n^+), y)).$$

Defínase

$$f_{n^+}(m) = \left\{ \begin{array}{ll} f_n(m), & \text{si } m < n^+ \\ y, & \text{si } m = n^+ \end{array} \right\}.$$

Entonces

$$(\forall m < n^+)(\exists a)(\mathrm{Dom}(f_{n^+}) = \{0, 1, ..., n^+\} \wedge f_{n^+}(0) = a \wedge F(f_{n^+}(m), f_{n^+}(m^+))).$$

Entonces,

$$n^+ \in A.$$

$$\therefore A = \omega.$$

P.d. f_n es única.

Sean f_n y g_n tales que

$$(\forall m < n)(\exists a)(\mathrm{Dom}(f_n) = \{0, 1, ..., n\} = \mathrm{Dom}(g_n) \wedge$$
$$f_n(0) = a = g_n(0) \wedge F(f_n(m), f_n(m^+)) \wedge F(g_n(m), g_n(m^+))).$$

a)

$$f_n(0) = a = g_n(0).$$

b) Suponga que

$$f_n(m) = g_n(m).$$

c) Entonces

$$F(f_n(m), f_n(m^+)) = F(g_n(m), f_n(m^+)) = F(g_n(m), g_n(m^+)).$$

$$\therefore f_n = g_n.$$

Sea $G(u, y)$ tal que

$$u \in \omega \wedge (\exists v)(v \text{ es una función con dominio } u^+ \wedge v(0) = a \wedge$$
$$(\forall z)(z \in u \Rightarrow F(v(z), v(z^+))) \wedge y = v(u));$$

i.e. para algún $n \in \omega$,

$$u = n \wedge y = f_n(n).$$

$G(u, y)$ determina una función porque

$$G(u, y) = G(u, z) \Rightarrow v(u) = v(z),$$

y

$$v(u) = v(z) \Leftrightarrow u = z.$$

Entonces, por el axioma del reemplazo, existe un conjunto

$$s = \{f_n(n) : \forall n \in \omega\}.$$

La función que se busca es

$$f = \{(x, y) \in \omega \times s : x = n \wedge y = f_n(n)\}.$$

Porque

$$f(0) = f_0(0) = a,$$

y

$$F(f(n), f(n^+));$$

porque

$$(\forall n \in \omega)(f(n) = f_n(n)),$$

y por definición de A,

$$(\forall n \in \omega)F(f_n(n), f_n(n^+)).$$

P.d. f es única.
Sean f y g dos funciones con dominio ω tales que

$$(\forall n \in \omega)(f(0) = a = g(0) \wedge F(f(n), f(n^+)) \wedge F(g(n), g(n^+)).$$

a)

$$f(0) = a = g(0).$$

b) Suponga que

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

c) Entonces

$$F(f(n), f(n^+)) = F(g(n), f(n^+)) = F(g(n), g(n^+)).$$

Entonces

$$f(n^+) = g(n^+).$$

$\therefore f = g.$ ■

Capítulo 3

EL AXIOMA DE ELECCIÓN

En esta sección discutiremos un principio que es de los más importantes, y al mismo tiempo controversiales de las matemáticas. En 1904 Ernst Zermelo en su "Demostración de que todo conjunto puede ser bien ordenado" puso atención a una suposición que se usaba implícitamente en una variedad de argumentos matemáticos. Esta suposición no se deduce de los axiomas previamente conocidos de la matemática o de la lógica, por lo tanto, debe ser tomado como un nuevo axioma; Zermelo lo llamó el Axioma de Elección.

El Axioma de Elección es útil porque muchas suposiciones que parece natural suponer verdaderas, no podrían demostrarse sin su ayuda; además, tiene implicaciones significativas en muchas ramas de las matemáticas y en consecuencias tan poderosas que algunas veces son difíciles de aceptar. Pero no siempre es indispensable, puesto que los temas en cuyo contexto se plantean dichas proposiciones continúan subsistiendo también en su ausencia, si bien en forma algo mutilada.

"Todo conjunto infinito tiene una infinidad numerable de elementos"; pensemos en como sería demostrada la proposición anterior sin el Axioma de Elección. Dado un conjunto infinito cualquiera A, tómese un elemento a de A; luego, tómese un elemento b de A distinto de a; luego, tómese un elemento de $A\backslash\{a,b\}$, y así sucesivamente. Como A es infinito, dicho proceso nunca termina; la sucesión $a, b, c, ...$ obtenida de distintos elementos de A constituyen un subconjunto numerable de A. Este argumento algo persuasivo justifica - de manera intuitiva - la conclusión. Sin embargo, hay algo de informalidad en él, que ha inquietado a los matemáticos; i.e. que en "nuestra

realidad", no podemos realizar el proceso interminable de elecciones sucesivas; además, los principios en los que se basa la prueba son vagos, por no decir más. Lo informal y vago del argumento puede resolverse recurriendo a nuestro Axioma de Elección.

3.1 La Función de Elección

Una aseveración equivalente al Axioma de Elección que no requiere la condición de conjuntos ajenos dos a dos es la siguiente.

Axioma 11 *Dado un conjunto x, cuyos elementos son conjuntos no vacíos, existe una función f tal que $f(a) \in a$, para toda $a \in x$.*

La función f es conocida como una función de elección para x.

Teorema 16 *El axioma 10 y el axioma 11 son equivalentes.*

Demostración. $\Rightarrow$) Sea F un conjunto de conjuntos no vacíos no necesariamente ajenos.
Sea

$$Y = \{\{x\} \times x : x \in F\}.$$

P. d.

$$(\forall x)(\forall z)(x \in F \wedge z \in F \Rightarrow \{x\} \times x \cap \{z\} \times z = \emptyset).$$

Sean

$$x \in F \wedge z \in F,$$

Suponga que

$$(\{x\} \times x) \cap (\{z\} \times z) \neq \emptyset \ \wedge x \neq z,$$

entonces

$$(\exists (a,b) \in \cup Y)((a,b) \in \{x\} \times x \wedge (a,b) \in \{z\} \times z),$$

entonces

$$a \in \{x\} \wedge a \in \{z\},$$

entonces

$$a = x \wedge a = z,$$

pero

$$(a = x \wedge a = z) \Rightarrow \ x = z,$$

entonces

$$x = z, !,$$

$$\therefore (\forall x)(\forall z)(x \in F \wedge z \in F \Rightarrow \{x\} \times x \cap \{z\} \times z = \emptyset).$$

Entonces los elementos de Y son ajenos dos a dos.
entonces, por el axioma 10, existe un conjunto elección E para Y
que consta de un elemento de cada $\{x\} \times x, \forall x \in F$,
éstos son de la forma (x, y) para uno y sólo un $y \in x$.
Sea f una función tal que

$$f(x) = y \Leftrightarrow x \in F \wedge (x, y) \in E,$$

entonces f es una función con dominio F tal que

$$(\forall x \in F)(f(x) \in x).$$

i.e. f es una función de elección para F.
$\Leftarrow$) Sea F un conjunto de conjuntos no vacíos ajenos dos a dos,
entonces, por el axioma 11, existe una función f tal que

$$(\forall x \in F)(f(x) \in x).$$

Sea

$$E = \{f(x) : x \in F\},$$

entonces E contiene uno y sólo un elemento de $x, \forall x \in F$,
$\therefore E$ es un conjunto elección para F. ■

3.2 El Axioma de Elección y el sistema ZF

El Axioma de Elección parece afirmar una verdad intuitiva, aceptada hoy en día por la mayoría de los matemáticos. Sin embargo, existen 3 argumentos sujetos a duda: Uno, el de sus implicaciones que algunos matemáticos sostienen que son paradójicas; y los otros dos, de tipo filosófico: El axioma 11 es una aseveración hecha sobre todo conjunto de conjuntos no vacíos, por lo tanto, deberemos tener claro lo que significa "todo conjunto de conjuntos no vacíos" al afirmarla como cierta. Además, la naturaleza del concepto de "conjunto" no está universalmente acordada o entendida. Bajo el mismo argumento se puede discutir que el Axioma de Elección es demasiado comprensible pero infundado para ser importante.

El Axioma de Elección difiere de los axiomas ZF (axiomas 1 a 9) por asegurar la existencia de un conjunto i.e. una función de elección, sin describir a este conjunto como una colección de objetos que tienen una propiedad particular. Éste es precisamente el aspecto que lo hace inaceptable para un grupo de matemáticos llamados intuicionistas, quienes afirman que la existencia matemática y la constructibilidad son la misma cosa - aunque exponer la teoría intuicionista no es propósito de este libro. De hecho, es interesante saber cuándo una proposición matemática puede ser demostrada sin usar el Axioma de Elección.

Antes de eso, aclaremos el plano en el que estaremos trabajando. Una afirmación como "el Axioma de Elección es equivalente al Lema de Zorn" no será tan significativa si no comprendemos claramente los principios que se usan en la demostración.

En 1938 K. Gödel probó que el Axioma de Elección es consistente con los axiomas ZF, es decir, no es contradictorio con ellos; tampoco es una consecuencia, como lo demostró P. J. Cohen en 1963. Así, este axioma tiene la misma categoría de otros axiomas famosos en matemáticas, como el quinto postulado de Euclides. Podemos tener entonces una teoría de conjuntos estándar ZFC si aceptamos el Axioma de Elección, y una teoría de conjuntos no estándar ZF en la cual aceptemos postulados alternativos al Axioma de Elección. Es importante recordar que trabajaremos en ZF (sin el axioma 10), a menos que formulemos específicamente el Axioma de Elección.

Es imposible, por razones del párrafo anterior, hacer una decisión en pro

o en contra basada en argumentos de lógica pura acerca de la validez del Axioma de Elección. También, dado que el Axioma de Elección involucra un área de las matemáticas - a saber, los conjuntos infinitos - que esta fuera de nuestra experiencia real, nunca será posible confirmar o rechazar el axioma por observación; así, la decisión es puramente personal.

3.3 El Lema de Zorn, el Teorema del Buen Orden y el Principio Máximo de Hausdorff

En la literatura hay varias formulaciones diferentes al Axioma de Elección las cuales son equivalentes a nuestro axioma 10. Aquí presentaremos cinco de estas proposiciones.

El Lema de Zorn es una herramienta indispensable en muchas áreas de las matemáticas; el Teorema del Buen Orden es quizás menos relevante en el trabajo matemático. Su utilidad reside en la fundamentos de las matemáticas, por ejemplo en la definición y uso de los conjuntos de los números cardinales y ordinales. Nótese que tanto el Lema de Zorn como el Teorema del Buen Orden no son constructivos como lo es el Axioma de Elección. Solamente aseguran la existencia, en el primer caso, de un elemento máximo en un conjunto ordenado, y en el otro caso, de una relación de buen orden en todo conjunto, sin dar el procedimiento de cómo construir el objeto en cuestión.

El Teorema del Buen Orden dice que todo conjunto puede ser bien ordenado, esto sin importar que tan grande es o la naturaleza de sus elementos. De donde podemos inferir que existe un procedimiento general para ordenar bien todos los elementos de $\mathbb{R}$ o de cualquier conjunto no numerable. Obsérvese que lo que se asegura en este teorema es sólo la posibilidad; sabemos que no existe un método práctico para ordenar bien los elementos de $\mathbb{R}$.

El Teorema del Buen Orden fue propuesto originalmente por Cantor y aunque el no dio ninguna demostración, en 1900 D. Hilbert en el Congreso Internacional de Matemáticas en París se refirió al Teorema del Buen Orden como un resultado de Cantor. Zermelo fue el primero en demostrarlo, sin embargo, debido a la paradoja de Burali-Forti y a que su demostración hacía uso de Inducción Transfinita, esa primera demostración de Zermelo no fue

muy aceptada. Para responder a las críticas, en 1908 Zermelo publicó otra demostración en la que se eliminaba el uso de ordinales. Se dice que la forma axiomática de Zermelo para la teoría de conjuntos está fuertemente influenciada por la segunda demostración ya que él seleccionó las formas más débiles para los axiomas en los cuales pudiera justificar su demostración.

La segunda formulación del Axioma de Elección la realizó Bertrand Russell en 1906 bajo el nombre de Axioma Multiplicativo. Aunque Russell anunció que su principio era un sustituto del principio de Zermelo, pues creía que el Axioma Multiplicativo era más débil. Después, en 1909 F. Hausdorff propuso el Principio Máximo; sin embargo, Hausdorff no lo menciona en su libro Mengenlehre de 1914 y aparece hasta la segunda edición de 1927. Kuratowski redescubrió el Principio Máximo en 1922 y dio otra demostración del Teorema del Buen Orden. El segundo redescubrimiento lo realizó Zorn en 1935, en esta ocasión el Principio Máximo fue decisivamente convincente, el resultado se conoce como el Lema de Zorn.

Teorema 17 *Las siguientes proposiciones son equivalentes:*

a) *El Axioma de Elección.*

b) *Lema de Zorn: Si x es un conjunto no vacío ordenado cualquiera tal que toda cadena tiene una cota superior en x, entonces x tiene un elemento máximo.*

c) *Teorema del Buen Orden: Todo conjunto puede ser bien ordenado.*

d) *Principio Máximo de Hausdorff: Todo conjunto no vacío ordenado contiene una cadena $\subseteq$-máxima.*

e) *Toda función suprayectiva tiene inversa derecha.*

Demostración. a) $\Rightarrow$ b)
Sea X un conjunto no vacío ordenado por la relación R tal que toda cadena tiene un supremo en X. Sea

$$S(x) = \{y \in X : xRy \wedge x \neq y\}, \forall x \in X;$$

nótese que

$$(\forall x \in X)(S(x) = \emptyset \Leftrightarrow x \text{ es máximo en } X).$$

Suponga que X no tiene elementos máximos. Sea

$$S = \{S(x) : x \in X\},$$

entonces, por el Axioma de Elección, existe una función F tal que

$$(\forall S(x) \in S)(F(S(x)) \in S(x)).$$

Sea $f : X \to X$ tal que

$$(\forall x \in X)(f(x) = F(S(x))).$$

Nótese que f es tal que

$$(\forall x \in X)(xRf(x) \wedge x \neq f(x)).$$

Sea F_a el conjunto de subconjuntos B de X tal que:

i) $a \in B$.

ii) $x \in B \Rightarrow aRx$.

iii) $x \in B \Rightarrow f(x) \in B$.

iv) $C \subseteq B \wedge C$ es una cadena en $X \Rightarrow$ el supremo de C es un elemento de B.

Obsérvese que el conjunto

$$\{x \in X : aRx\}$$

satisface las 4 condiciones, entonces

$$F_a \neq \emptyset.$$

Sea

$$A = \cap F_a \wedge O_a = \{x \in X : aRx\}.$$

P. d.

$$A \in F_a$$

i) Es obvio.

ii) Sea $x \in A$, entonces

$$x \in \cap F_a,$$

pero

$$O_a \in F_a,$$

entonces

$$x \in O_a.$$

$$\therefore aRx.$$

iii) Sea $x \in A$, entonces

$$(\forall B \in F_a)(x \in B),$$

entonces B satisface iii), $\forall B \in F_a$. i.e.

$$(\forall B \in F_a)(x \in B \Rightarrow f(x) \in B),$$

entonces

$$(\forall B \in F_a)(f(x) \in B),$$

entonces

$$f(x) \in \cap F_a,$$

$$\therefore f(x) \in A.$$

iv) Sea $C \subseteq A$ tal que C es una cadena en X y c es el supremo de C, entonces

$$(\forall x \in C)(xRc),$$

entonces

$$c \in S(x),$$

entonces, por el Axioma de Elección. existe una función F tal que

$$F(S(x)) = c \in S(x),$$

pero

$$f(x) = F(S(x)) = c,$$

entonces. por iii).

$$f(x) \in A,$$

entonces

$$c \in A.$$

$$\therefore A \in F_a.$$

Sea

$$I = \{x \in A : y \in A \wedge yRx \wedge y \neq x \Rightarrow f(y)Rx\}$$

y

$$b \in I \wedge I_b = \{x \in A : xRb \vee f(b)Rx\}.$$

P. d.

$$I_b = A.$$

i) Sea $x \in I$, entonces

$$x \in A,$$

entonces

$$aRx,$$

$$\therefore a \in I_b.$$

ii) Sea $x \in I_b$, entonces

$$x \in A,$$

$$\therefore aRx.$$

iii) Sea $x \in I_b$, entonces

$$xRb \vee f(x)Rx,$$

y sabemos que

$$xRf(x).$$

Si

$$xRb \wedge x = b,$$

entonces

$$f(x) = f(b),$$

entonces, por la antisimetría de R,

$$f(x)Rf(b) \wedge f(b)Rf(x),$$

entonces

$$f(b)Rf(x).$$

Si

$$xRb \wedge x \neq b,$$

entonces, como $b \in I$,

$$f(x)Rb.$$

Si

$$f(b)Rx,$$

entonces, por la transitividad de R,

$$f(b)Rf(x),$$

entonces

$$f(x)Rb \vee f(b)Rf(x),$$

$$\therefore f(x) \in I_b.$$

iv) Sea C una cadena en $I_b \wedge c$ el supremo de C; pero

$$I_b \subseteq A \subseteq X \wedge A \in F_a,$$

entonces

$$C \subseteq A \wedge C \text{ es una cadena en } X \Rightarrow c \in A;$$

como $C \subseteq I_b$, entonces

$$(\forall x \in C)(xRb \vee f(b)Rx).$$

Si

$$(\forall x \in C)(xRb),$$

entonces b es una cota superior de C. entonces, por definición de c,

$$cRb.$$

Si

$$f(b)Rx,$$

entonces

$$f(b)Rx \wedge xRc,$$

entonces

$$f(b)Rc,$$

entonces

$$cRb \vee f(b)Rc,$$

entonces

$$c \in I_b.$$

Entonces

$$I_b \in F_a,$$

entonces

$$A \subseteq I_b \wedge I_b \subseteq A,$$

$$\therefore I_b = A.$$

P. d.

$$I = A.$$

i) Si $x \in I$, entonces

$$x \in A,$$

pero

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

entonces

$$\neg(\exists x \in A)(xRa \wedge x \neq a),$$

entonces

$$x \in A \wedge xRa \wedge x \neq a \Rightarrow f(x)Ra$$

vale,

$$\therefore a \in I.$$

ii) Si $x \in I$, entonces

$$x \in A,$$

entonces

$$aRx.$$

iii) Sean

$$x \in I \wedge y \in A \wedge yRf(x) \wedge y \neq f(x)$$

pero $A = I_b$, entonces

$$yRx \vee f(x)Ry;$$

entonces

$$\neg(f(x)Ry)$$

porque, por hipótesis,

$$yRf(x),$$

entonces

$$yRx.$$

Si $y = x$, entonces

$$f(y) = f(x),$$

entonces

$$f(y)Rf(x).$$

Si $y \neq x$, entonces

$$x \in I \wedge y \in A \wedge yRx \wedge y \neq x,$$

entonces

$$f(y)Rx,$$

pero

$$f(y)Rx \wedge xRf(x) \Rightarrow f(y)Rf(x),$$

$$\therefore f(x) \in I.$$

iv) Sea $C \subseteq I$ una cadena en X, pero

$$I \subseteq A \Rightarrow c \in A,$$

donde c es el supremo de C. Suponga que

$$y \in A \wedge yRc \wedge y \neq c,$$

pero

$$(\forall y \in A)(I_b = A \Leftrightarrow y \in I_b),$$

entonces

$$(\forall b \in I)(yRb \vee f(b)Ry),$$

en particular, $\forall b \in C$. Si yRb, entonces

$$y = b \vee y \neq b.$$

Si $y \neq b$, entonces

$$b \in I \wedge y \in A \wedge yRb \wedge y \neq b \Rightarrow f(y)Rb,$$

pero

$$(\forall b \in C)(bRc),$$

entonces

$$f(y)Rc.$$

Si $y = b$. entonces

$$y = b \wedge y \neq c \Rightarrow b \neq c,$$

con $b \in C$, entonces

$$b \in C \subseteq I \Rightarrow (y \in A \wedge yRb \wedge y \neq b \Rightarrow f(y)Rb),$$

pero

$$(\forall b \in C)(bRc),$$

entonces

$$f(y)Rc.$$

Si $f(b)Ry$, entonces

$$(\forall b \in C)(bRy),$$

entonces y es una cota superior para C.
pero, por definición de supremo.

$$cRy,$$

lo que contradice la hipótesis.

$$\therefore c \in I.$$

Entonces $I \in F_a$, entonces

$$I \subseteq A \wedge A \subseteq I \Leftrightarrow A = I;$$

$$\therefore A = I = I_b.$$

P. d. A es una cadena en X.
Sean $x, y \in A$, entonces

$$x \in I \wedge y \in I_x,$$

entonces

$$yRx \vee f(x)Ry,$$

pero

$$xRf(x) \Rightarrow xRy,$$

entonces

$$yRx \vee xRy,$$

entonces A está ordenado bajo R, entonces

$$A \subseteq X \wedge R \text{ es una relación de orden para} A,$$

$$\therefore A \text{ es una cadena en } X.$$

Entonces A tiene un supremo en X.
Sea $m \in X$ un supremo de A,
entonces, por iv),

$$m \in A,$$

entonces, por iii),

$$f(m) \in A,$$

entonces

$$(\forall x \in A)(f(m) \in A \wedge xRm),$$

entonces

$$f(m)Rm,$$

entonces

$$f(m)Rm \wedge mRf(m),$$

entonces

$$m = f(m) = F(S(m)) \in S(m), !,$$

entonces

$$S(m) \notin S,$$

entonces

$$S(m) = \emptyset,$$

entonces X tiene elementos máximos,
$\therefore X$ tiene un elemento máximo (al menos). ■

Demostración. b) $\Rightarrow$ c)
Sea x un conjunto no vacío cualquiera,
sea w el conjunto de los subconjuntos bien ordenados de x, i.e.

$$w = \{(A, R) : A \subseteq x \wedge R \text{ es una relación de buen orden en } A\},$$

definimos $(A, R) \preccurlyeq (B, S)$ si

$$(\forall a \in B \backslash A)(b \in B)(A \subseteq B \wedge R \text{ es la restricción de } S \text{ para } A \wedge S \text{ es tal que } a \leq b),$$

i.e. A es un segmento inicial de B.
P. d. $\preccurlyeq$ es una relación de orden en w.
i) Prop. reflexiva.
Sea $(A, R) \in w$, sabemos que $A \subseteq A$, y además

$$(\forall a \in A)(A \backslash A = \emptyset = 0 \Rightarrow 0 \leq a),$$

entonces

$$(\forall a \in A \backslash A)(\forall b \in A)(A \subseteq A \wedge R \text{ es la restricción de } R \text{ para } A \wedge a \leq b),$$

$$\therefore (A, R) \preccurlyeq (A, R).$$

ii) Prop. antisimétrica.
Sean $(A, R), (B, S) \in w$ tales que

$$(A, R) \preccurlyeq (B, S) \wedge (B, S) \preccurlyeq (A, R),$$

entonces, por definición,

$$A \subseteq B \wedge B \subseteq A \Leftrightarrow A = B,$$

y además, R es la restricción de S para A,
y S es la restricción de R para B, entonces

$$R = S;$$

luego

$$a \leq b \wedge b \leq a \Rightarrow a = b, \forall a \in A, b \in B.$$

$$\therefore (A, R) = (B, S).$$

iii) Transitividad.
Sean $(A, R), (B, S), (C, T) \in w$ tales que

$$(A, R) \preccurlyeq (B, S) \wedge (B, S) \wedge (C, T),$$

entonces

$$A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C,$$

y además, R es la restricción de S para A,
y S es la restricción de T para B,
entonces R es la restricción de T para A; sea

$$a \in A \wedge b \in B \backslash A \wedge c \in C \backslash B,$$

entonces

$$a \leq b \wedge b \leq c \Rightarrow a \leq c,$$

como

$$(\forall B)(\forall b)(A \subseteq B \wedge b \in B \backslash A \Rightarrow a \leq b),$$

entonces

$$/(\forall c \in C \backslash A)(a \leq b \wedge b \leq c \Rightarrow a \leq c),$$

$$\therefore (A,R) \preccurlyeq (C,T),$$

$$\therefore \preccurlyeq \text{ es una relación de orden.}$$

Sea C una cadena en $w \wedge a, b \in \cup C$. entonces

$$(\exists (A,R),(B,S) \in C)(a \in A \wedge b \in B),$$

sin pérdida de generalidad. supongamos que

$$(A,R) \preccurlyeq (B,S),$$

entonces

$$A \subseteq B,$$

entonces

$$a, b \in B,$$

así, a y b están relacionados bajo S.
Diremos que aRb si

$$a \leq b \wedge aSb,$$

entonces R será un buen orden para $\cup C$.
P. d. a) R está bien definido.
b) R es una relación de orden.
c) $\cup C$ es una cota superior para C.
a) Retomando la hipótesis anterior. suponga que

$$a, b \in D \wedge (D,T) \in C \wedge (D,T) \neq (B,S),$$

entonces (D,T) está relacionado con (A,R) bajo $\preccurlyeq$.
por definición. a y b también están relacionados bajo $\leq$ y bajo T.
entonces el orden $\leq$ de a y b no cambia $\forall (D,T)$ que los contenga. así.

$$(\forall (D,T))(aRb),$$

$$\therefore R \text{ está bien definido.}$$

b) i) Prop. reflexiva.
Sea $a \in \cup C$, entonces

$$(\exists (B,S) \in C)(a \in B),$$

pero

$$(B,S) \preccurlyeq (B,S) \wedge ((B,S) \preccurlyeq (B,S) \Rightarrow aSa \wedge a \leq a),$$

$$\therefore aRa.$$

ii) Prop. antisimétrica.
Sean $a, b \in \cup C$ tales que

$$aRb \wedge bRa,$$

entonces

$$(\exists (A,R),(B,S) \in C)(a \in (A,R) \wedge b \in (B,S)),$$

y además

$$aSb \wedge bSa \wedge a \leq b \wedge b \leq a,$$

entonces

$$a \leq b \wedge b \leq a \Rightarrow a = b,$$

$$\therefore a = b.$$

iii) Transitividad.
Suponga que

$$aRb \wedge bRc,$$

entonces

$$(\exists (A,R),(B,S),(D,T) \in C)(a \in (A,R) \wedge b \in (B,S) \wedge c \in (D,T)),$$

y además

$$A, B \subseteq D \wedge a \leq b \wedge b \leq c,$$

pero

$(a \leq b \wedge b \leq c \Rightarrow a \leq c) \wedge a, b$ y c están relacionados bajo T,

entonces

$$a \leq c \wedge aTc,$$

entonces

$$aRc.$$

$$\therefore R \text{ es una relación de orden para } \cup C.$$

c)

$$C \subseteq w \wedge w \subseteq \mathbb{P}(x) \Rightarrow C \subseteq \mathbb{P}(x),$$

entonces,

$$\cup C \subseteq \cup \mathbb{P}(x),$$

pero por el ejemplo 1.

$$\cup C \subseteq x,$$

entonces, por a) y b),

$$(\cup C, R) \in w;$$

sea (A, R) el elemento máximo de $\cup C$, entonces

$$(B, S) \preccurlyeq (A, R), \forall (B, S) \in \cup C.$$

Sea $(D, T) \in C$, pero $\cup C \in w$, entonces, si

$$E \in (D, T) \wedge (E, U) \in \cup C,$$

entonces

$$(E,U) \preccurlyeq (A,R), \forall E \in (D,T),$$

$\therefore$ toda cadena en w tiene cota superior.

Por el Lema de Zorn, w tiene un elemento máximo,
sea (M,R) el elemento máximo de w,
suponga que $M \subset x$, entonces

$$(\exists y \in x \backslash M)((M,R) \preccurlyeq (M \cup \{y\}, R \cup \{(a,r) : a \in M \cup \{y\}\}), !,$$

entonces

$$M = x,$$

entonces R es un buen orden para x,
$\therefore x$ puede ser bien ordenado. ■

Demostración. c) $\Rightarrow$ a)
Sea x un conjunto no vacío cualquiera,
entonces, por el Teorema del Buen Orden,
z puede ser bien ordenado, $\forall z \in x$;
definimos $f : x \rightarrow \cup x$ tal que

$$(\forall z \in x)(f(z) = \text{mín}(z)),$$

entonces

$$(\forall z \in x)(f(z) \in z),$$

$\therefore f$ es una función de elección para x. ■

Antes de comenzar la demostración de b) $\Rightarrow$ d), demostraremos una aseveración que nos será de utilidad.

Teorema 18 *El Lema de Zorn implica que si P es un conjunto ordenado tal que toda cadena tiene una cota superior en P, entonces*

$$(\forall p \in P)(\exists q \in P)(pRq \wedge \neg(qRp)),$$

donde R es una relación de orden para P.

Demostración. Sea P un conjunto ordenado tal que
toda cadena tiene una cota superior en P. Sea

$$p \in P \wedge Q = \{q \in P : pRq\},$$

donde R es una relación de orden para P, entonces

$$Q \subseteq P \Rightarrow \text{toda cadena en } Q \text{ tiene una cota superior en } Q,$$

entonces, por el Lema de Zorn, Q tiene un elemento máximo.
Sea r un elemento máximo en Q, entonces

$$(\forall q \in Q)(qRr \wedge q \neq r),$$

entonces, por transitividad,

$$(\forall p \in P)(pRr \wedge p \neq r),$$

$\therefore pRr \wedge r$ es máximo en P. ■

Demostración. b) $\Rightarrow$ d)
Sea X un conjunto ordenado y F el conjunto de todas las cadenas en X,
entonces F es ordenado bajo $\subseteq$.
Sea C una cadena en F,
entonces

$$\cup C \subseteq X,$$

entonces

$$(\forall C \subseteq F)(\cup C \in F \wedge C \subseteq \cup C),$$

entonces

$$(\forall C \subseteq F)(C \subseteq \cup C),$$

entonces, por el teorema 17,

$$(\exists K)(K \in F \wedge C \subseteq K \wedge K \text{ es máximo en } F),$$

$\therefore X$ tiene una cadena $\subseteq$-máxima. ■

Demostración. d) $\Rightarrow$ b)
Sea x un conjunto no vacío ordenado tal que
toda cadena tiene una cota superior,
entonces, por el Principio Máximo de Hausdorff,
existe una cadena $M \subseteq x$ tal que M es $\subseteq$-máxima,
sea $m \in x$ una cota superior de M,
suponga que m no es máximo, entonces

$$(\exists y \in x)(m < y),$$

entonces

$$M \subseteq M \cup \{y\}, !,$$

$\therefore m$ es un elemento máximo de x. ■

Demostración. a) $\Rightarrow$ e)
Sea $f : X \to Y$ una función suprayectiva, entonces

$$y \in Y \Rightarrow (\exists x \in X)(f(x) = y).$$

Sea

$$A_y = \{x \in X : f(x) = y\}, \forall y \in Y,$$

entonces

$$A_y \subseteq X \wedge (A_y \cap A_{y'} = \emptyset \Leftrightarrow y \neq y').$$

Sea

$$A = \{A_y \subseteq X : \forall y \in Y\},$$

entonces A es un conjunto de conjuntos ajenos dos a dos,
entonces, por el Axioma de Elección, existe un conjunto E
que contiene uno y sólo un elemento de cada elemento de A, entonces

$$E \subseteq X;$$

sea $g : Y \to X$ tal que

$$g(y) = x \wedge x \in E,$$

entonces

$$f \times g(y) = f(g(y)) = f(x) = y, \forall y \in Y,$$

entonces

$$f \times g = Id_Y,$$

$\therefore g : Y \to X$ es inversa derecha de $f : X \to Y$. ■

Demostración. e) $\Rightarrow$ a)
Sea F un conjunto de conjuntos no vacíos ajenos dos a dos,
sea $f : \cup F \to F$ tal que

$$f(v) = x \Leftrightarrow v \in x,$$

entonces

$$f(\cup F) = F,$$

i.e. $f : \cup F \to F$ es suprayectiva, entonces, por e),

$$(\exists g : F \to \cup F)(f \times g(x) = f(g(x)) = x),$$

pero

$$f(g(x)) = x \Leftrightarrow g(x) \in x, \forall x \in F.$$

Sea

$$A = \{g(x) : \forall x \in F\},$$

entonces A tiene uno y sólo un elemento de cada elemento de F,
$\therefore A$ es un conjunto elección para F. ■

Así, queda demostrado el teorema 17.[1]

[1] Recientemente se ha demostrado que el Axioma de Elección es equivalente a que todo espacio vectorial tiene base.

Capítulo 4

LOS NUMEROS CARDINALES

4.1 Conjuntos numerables

4.1.1 Conjuntos numerables finitos

El número cardinal de un conjunto es el tamaño relativo del mismo con otros conjuntos, desde el punto de vista de funciones entre ellos.

Definición 25 *Un conjunto no vacío A es finito si existe $n \in \mathbf{N}$ y una biyección de $\{1, ..., n\}$ a A.*

De lo contrario, es infinito. Por convención, el conjunto vacío es finito.

Definición 26 *Dos conjuntos A y B son equinumerosos si existe una biyección de A a B.*

Y se denota como $A \sim B$.

Teorema 19 *Para conjuntos cualesquiera A, B y C:*

$$\text{i) } A \sim A.$$
$$\text{ii) } A \sim B \Rightarrow B \sim A.$$
$$\text{iii) } A \sim B \wedge B \sim C \Rightarrow A \sim C.$$

Demostración. i) La función identidad es una biyección de A a A,

$$\therefore A \sim A.$$

ii) Sea

$$f : A \to B$$

una biyección, entonces

$$f^{-1} : B \to A$$

existe, y es una biyección,

$$\therefore B \sim A.$$

iii) Suponga que

$$A \sim B \wedge B \sim C,$$

entonces existen biyecciones

$$g : A \to B \wedge f : B \to C,$$

entonces

$$\mathrm{Im}(g) = \mathrm{Dom}(f),$$

entonces $f \circ g$ es una biyección de A a C,
$\therefore A \sim C$. ■

Definición 27 *Para conjuntos cualesquiera A y B, A es dominado por B si existe una función inyectiva de A a B.*

Se denota como $A \preccurlyeq B$.

4.1.2 Conjuntos numerables infinitos

Definición 28 *Un conjunto A es numerable si:*

a) Es finito, o
b) es infinito y $\mathbf{N} \sim A$.

Teorema 20 *Un conjunto A es numerable si y sólo si existe una función inyectiva $A \to \mathbf{N}$, i.e. $A \preccurlyeq \mathbf{N}$.*

Demostración. $\Rightarrow$) Suponga que A es numerable.
Si A es finito, entonces

$$(\exists n)(n \in \mathbf{N} \wedge A = \{a_1, ..., a_n\}).$$

entonces la función que mapea a_k en k $(1 \leq k \leq n)$,
es una función inyectiva $A \to \mathbf{N}$.
Si A es infinito, entonces, por las definiciones 25 y 27,
existe una biyección $\mathbf{N} \to A$,
cuya inversa es una función inyectiva $A \to \mathbf{N}$.
$\Leftarrow$) Suponga que existe una función inyectiva

$$h : A \to \mathbf{N},$$

entonces

$$h(A) \subseteq \mathbf{N},$$

entonces $h(A)$ es numerable; entonces

$$h : A \to h(A)$$

es una biyección. Entonces, si $h(A)$ es finito, A es finito y numerable.
Si $h(A)$ es infinito, entonces $h(A)$ es equinumeroso a $\mathbf{N}$, i.e.

$$h(A) \sim \mathbf{N}.$$

Pero

$$A \sim h(A),$$

entonces, por el teorema 19,

$$A \sim \mathbf{N},$$

$\therefore A$ es numerable. ■

Corolario 3 *Un conjunto no vacío A es numerable si y sólo si existe una suprayección* $\mathbf{N} \rightarrow A$.

Demostración. $\Rightarrow$) Sea A un conjunto no vacío numerable, entonces, por el teorema 20, existe una función inyectiva

$$f : A \rightarrow \mathbf{N},$$

entonces f es una biyección

$$A \rightarrow f(A),$$

entonces existe la biyección

$$f^{-1} : f(A) \rightarrow A.$$

Defínase $g : \mathbf{N} \rightarrow A$ tal que

$$g(n) = \left\{ \begin{array}{ll} f^{-1}(n) & \text{si } n \in f(A) \\ a_0 & \text{si } n \notin f(A) \end{array} \right\} \wedge a_0 \in A.$$

$$\therefore g \text{ es una suprayección } \mathbf{N} \rightarrow A.$$

$\Leftarrow$) Suponga que existe una suprayección

$$g : \mathbf{N} \rightarrow A.$$

Defínase $f : A \rightarrow \mathbf{N}$ tal que

$$f(a) = \text{mín}\{n \in N : g(n) = a\},$$

entonces f es una función inyectiva $A \rightarrow \mathbf{N}$,
$\therefore A$ es numerable. ■

Teorema 21 *La unión de dos conjuntos numerables es numerable.*

Demostración. Sean A y B conjuntos numerables y

$$f : \mathbf{N} \rightarrow A \wedge g : \mathbf{N} \rightarrow B$$

suprayecciones. Defínase $h : \mathbf{N} \to A \cup B$ tal que

$$h(x) = \left\{ \begin{array}{ll} f(n), & \text{si } x = 2n+1 \\ g(n), & \text{si } x = 2n \end{array} \right\} \wedge (n \in \mathbf{N}).$$

Entonces h es una suprayección

$$\mathbf{N} \to A \cup B,$$

$\therefore A \cup B$ es numerable. ■

Teorema 22 *El producto cartesiano de dos conjuntos numerables es numerable.*

Demostración. Sean A y B conjuntos numerables. y

$$f : A \to \mathbf{N} \wedge g : B \to \mathbf{N}$$

funciones inyectivas, entonces $h : A \times B \to \mathbf{N}$ tal que

$$h(a,b) = (2^{f(a)})(3^{g(b)})$$

es una función inyectiva

$$A \times B \to \mathbf{N},$$

porque

$$h(a,b) = h(c,d) \Rightarrow (2^{f(a)})(3^{g(b)}) = (2^{f(c)})(3^{g(d)}),$$

pero, por el teorema fundamental de la aritmética,

$$f(a) = f(c) \wedge g(b) = g(d),$$

y por la inyectividad de f y de g,

$$a = c \wedge b = d,$$

entonces

$$(a,b) = (c,d),$$

$\therefore A \times B$ es numerable. ■

4.2 Conjuntos no numerables

Teorema 23 (de Cantor-Schröder-Bernstein) *Si A y B son conjuntos tales que existen funciones inyectivas $f : A \to B$ y $g : B \to A$, entonces existe una biyección entre A y B; i.e.*

$$|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|.$$

Demostración. Sean

$$f : A \to B \wedge g : B \to A$$

funciones inyectivas. Sea $b_1 \in B$. Si $b_1 \in \text{Im}(f)$, entonces

$$(\exists! a_1 \in A)(f(a_1) = b_1).$$

Si $a_1 \in \text{Im}(g)$, entonces

$$(\exists! b_2 \in B)(g(b_2) = a_1).$$

Continuando sucesivamente, obtenemos la sucesión

$$b_1 \xleftarrow{f} a_1 \xleftarrow{g} b_2 \xleftarrow{f} a_2 \xleftarrow{g} \ldots$$

Tenemos tres posibilidades:

La sucesión anterior termina en algún a_i porque $a_i \notin \text{Im}(g)$.

La sucesión anterior termina en algún b_j porque $b_j \notin \text{Im}(f)$.

La sucesión anterior no termina.

Sean

$$B_A = \{b_k \in B : \text{la sucesión anterior termina en algún } a_i \text{ porque } a_i \notin \text{Im}(g)\},$$

$$B_B = \{b_k \in B : \text{la sucesión anterior termina en algún } b_i \text{ porque } b_i \notin \text{Im}(f)\}$$

y

$$B_\infty = \{b_k \in B : \text{la sucesión anterior no termina}\}.$$

Tomando un a_1, bajo el mismo razonamiento, obtenemos la sucesión

$$a_1 \xleftarrow{g} b_1 \xleftarrow{f} a_2 \xleftarrow{g} b_2 \xleftarrow{f} \ldots$$

Quedando la mismas tres posibilidades anteriores.
Defínanse análogamente A_A, A_B y A_∞. Obsérvese que

$$A_A \overset{f|_{A_A}}{\longrightarrow} B_A$$

es una biyección porque, si la sucesión

$$a_1 \xleftarrow{g} b_1 \xleftarrow{f} a_2 \xleftarrow{g} b_2 \xleftarrow{f} \ldots \xleftarrow{f} a_n$$

terminó, entonces la sucesión

$$f(a_1) \xleftarrow{f} a_1 \xleftarrow{g} b_1 \xleftarrow{f} a_2 \xleftarrow{g} b_2 \xleftarrow{f} \ldots \xleftarrow{f} a_n$$

también terminó; para cualquier $b_k = f(a_i) \in B_A$.
Es claro que cada elemento de B_A viene de uno y sólo un elemento de A_A.
De la misma manera,

$$B_B \overset{g|_{B_B}}{\longrightarrow} A_B$$

es una biyección, y

$$A_\infty \overset{f|_{A_\infty}}{\longrightarrow} B_\infty$$

también es una biyección, por lo tanto,

$$|A_A| = |B_A| \wedge |A_B| = |B_B| \wedge |A_\infty| \wedge |B_\infty|.$$

Entonces

$$|A_A \cup A_B \cup A_\infty| = |B_A \cup B_B \cup B_\infty|$$

$\therefore |A| = |B|$. ■

4.3 Números cardinales

Definición 29 *Dos conjuntos cualquiera A y B tienen el mismo número cardinal si existe una biyección entre ellos.*

Queda implícito que conjuntos equinumerosos tienen el mismo número cardinal. Para conjuntos finitos, podemos decir que el número cardinal de un conjunto es el número de elementos en él. Y para conjuntos infinitos, como principales casos tendremos los conjuntos equinumerosos a $\mathbf{N}$ y los conjuntos equinumerosos a $\mathbf{R}$. Cuyos símbolos para ambos números cardinales infinitos serán:

$\aleph_0$ (alev 0) es el número cardinal de $\mathbf{N}$.

$\aleph$(alev) es el número cardinal de $\mathbf{R}$.

Por el momento, decir que un conjunto tiene el número cardinal $\aleph_0$ significa que el conjunto es equinumeroso a $\mathbf{N}$ (de la misma manera para $\aleph$ en relación a $\mathbf{R}$).

Notación:

Se usarán las letras griegas minúsculas $\kappa, \lambda, \mu, \ldots$ para denotar números cardinales; y para conjuntos A y B las abreviaturas card A = card B y card $A = \kappa$.

Obsérvese que todas las afirmaciones y resultados sobre los números cardinales en esta sección, son afirmaciones sobre biyecciones o inyecciones entre conjuntos.

Definición 30 *Para conjuntos cualesquiera A y B, se dice que card $A \leq$ card B, si A es dominado por B, i.e. si existe una función inyectiva de A a B.*

Definiremos las operaciones sobre conjuntos conocidas en términos de números cardinales. Por ejemplo: La unión y el producto cartesiano. Primero, consideraremos a los conjuntos finitos.

Dados dos conjuntos finitos cualesquiera A y B con m y n elementos respectivamente:

Si $A \cap B = \emptyset$, entonces $A \cup B$ contiene $m + n$ elementos.
$A \times B$ contiene mn elementos.
$\mathbf{P}(A)$ contiene 2^m elementos.

Resultados semejantes valen para conjuntos infinitos al extender las nociones de suma, producto y potencia.

Teorema 24 *Sean A, B, C y D conjuntos tales que $A \sim C$ y $B \sim D$. Entonces:*

i) si $A \cap B = \emptyset$ y $C \cap D = \emptyset$ entonces $A \cup B \sim C \cup D$.
ii) $A \times B \sim C \times D$.

Demostración. Sean biyecciones

$$f : A \to C \wedge g : B \to D.$$

i) Sea $h : A \cup B \to C \cup D$ tal que

$$h(x) = \left\{ \begin{array}{l} f(x) \text{ si } x \in A \\ g(x) \text{ si } x \in B \end{array} \right\}$$

a) suponga que

$$(\exists x, y \in A \cup B)(h(x) = h(y)),$$

entonces

$$f(x) = f(y) \vee g(x) = g(y),$$

pero por la inyectividad de f y de g,

$$x = y \vee x = y,$$

$$\therefore h \text{ es inyectiva.}$$

b) Sea $x \in C \cup D$, entonces

$$x \in C \vee x \in D,$$

entonces, por la suprayectividad de f y de g,

$$(\exists y \in A \cup B)(f(y) = x \vee g(y) = x),$$

entonces h es suprayectiva, entonces h es una biyección,

$$\therefore A \cup B \sim C \cup D.$$

ii) Sea $k : A \times B \to C \times D$ tal que

$$k(x, y) = (f(x), g(y)) \wedge x \in A \wedge y \in B.$$

a) Suponga que

$$(\exists w, x \in A)(\exists y, z \in B)(k(x, y) = k(w, z)),$$

entonces

$$(f(x), g(y)) = (f(w), g(z)),$$

entonces

$$f(x) = f(w) \wedge g(y) = g(z),$$

y por la inyectividad de f y de g,

$$x = w \wedge y = z,$$

$$\therefore k \text{ es inyectiva.}$$

b) Sea

$$(x, y) \in C \times D,$$

entonces, por la suprayectividad de f y de g,

$$(\exists w \in A \wedge z \in B)(f(w) = x \wedge g(z) = y),$$

entonces

$$(x, y) = (f(w), g(z)) = k(w, z),$$

$$\therefore k \text{ es suprayectiva.}$$

$$\therefore k \text{ es una biyección.}$$

$\therefore A \times B \sim C \times D.$ ■

Definición 31 *Sean κ y λ dos números cardinales:*

i) *La suma, $\kappa + \lambda$, es el número cardinal de $A \cup B$, donde A y B son conjuntos tales que card $A = \kappa$, card $B = \lambda$ y $A \cap B = \emptyset$.*
ii) *El producto, $\kappa\lambda$, es el número cardinal de $A \times B$, donde A y B son conjuntos cualesquiera con card $A = \kappa$ y card $B = \lambda$.*

Obsérvese que el teorema 28 muestra que las nociones de suma y producto están bien definidas independientemente de la elección de los conjuntos A y B.

Para los números cardinales finitos, las operaciones de suma y producto bajo esta definición son las mismas que para los números naturales. Pero para los números cardinales infinitos, las mismas operaciones dan resultados distintos.

Teorema 25

$$i)\ (\forall n \in \mathbf{Z}^+)(n + \aleph_0 = \aleph_0 \wedge n\aleph_0 = \aleph_0).$$
$$ii)\ \aleph_0 + \aleph_0 = \aleph_0 \wedge \aleph_0\aleph_0 = \aleph_0.$$

Demostración. i) Sean A y B conjuntos tales que

$$\text{card } A = n \wedge \text{card } B = \aleph_0 \wedge A \cap B = \emptyset,$$

entonces,por el teorema 21, $A \cup B$ es numerable,
y como B es infinito, $A \cup B$ es infinito. Entonces, por definición,

$$A \cup B \sim \mathbf{N},$$

por lo que

$$\text{card } A \cup B = \aleph_0.$$

$$\therefore n + \aleph_0 = \aleph_0.$$

Como B es infinito, $A \times B$ es infinito,
y por el teorema 22, $A \times B$ es numerable, entonces

$$\text{card } (A \times B) = \aleph_0,$$

pero, por definición,

$$\text{card } (A \times B) = n\aleph_0,$$

$$\therefore n\aleph_0 = \aleph_0.$$

ii) Sean A y B conjuntos tales que

$$\text{card } A = \aleph_0 \wedge \text{card } B = \aleph_0 \wedge A \cap B = \emptyset,$$

entonces, por definición

$$\text{card } A \cup B = \aleph_0 + \aleph_0,$$

pero, $A \cup B$ es infinito, y por el teorema 21, es numerable, entonces

$$\text{card } A \cup B = \aleph_0,$$

$$\therefore \aleph_0 + \aleph_0 = \aleph_0.$$

Por otro lado,

$$\text{card } A \times B = \aleph_0\aleph_0,$$

pero, $A \times B$ es infinito, y por el teorema 22, es numerable, entonces

$$\text{card } A \times B = \aleph_0,$$

$\therefore \aleph_0\aleph_0 = \aleph_0$. ■

Lema 1 *Sean κ, λ y μ números cardinales infinitos tales que $\kappa \leq \lambda$. Entonces*

$$\kappa + \mu \leq \lambda + \mu \wedge \kappa\mu \leq \lambda\mu.$$

Demostración. Sean A, B y C conjuntos tales que

$$|A| = \kappa \wedge |B| = \lambda \wedge |C| = \mu \wedge |A| \leq |B| \wedge A \cap C = \emptyset = B \cap C.$$

Entonces,

$$(\exists f : A \rightarrow B)(f \text{ es inyectiva}).$$

i) Defínase $g : A \cup C \rightarrow B \cup C$ tal que

$$g(a) = \left\{ \begin{array}{ll} f(a), & \text{si } a \in A \\ a, & \text{si } a \in C \end{array} \right\}$$

Entonces g es inyectiva.

$$\therefore \kappa + \mu \leq \lambda + \mu.$$

ii) Defínase $g : A \times C \rightarrow B \times C$ tal que

$$g(a, b) = (f(a), b).$$

Entonces g es inyectiva.

$$\therefore \kappa\mu \leq \lambda\mu.$$

$\therefore \kappa + \mu \leq \lambda + \mu \wedge \kappa\mu \leq \lambda\mu.$ ■

Puede mostrarse, bajo un argumento derivado del Axioma de Elección, que para todo número cardinal infinto κ,

$$\kappa\kappa = \kappa.$$

Una consecuencia de esto, es el siguiente teorema que muestra que la adición y multiplicación de números cardinales infinitos es trivial.

Teorema 26 *Sean κ y λ dos números cardinales infinitos tales que $\kappa \leq \lambda$. Entonces*

$$\kappa + \lambda = \lambda \wedge \kappa\lambda = \lambda.$$

Demostración. Sean κ y λ dos números cardinales infinitos tales que

$$\kappa \leq \lambda.$$

i) Entonces

$$\lambda \leq \kappa + \lambda \leq \lambda + \lambda \leq 2\lambda \leq \lambda\lambda = \lambda.$$

$$\therefore \kappa + \lambda = \lambda.$$

ii)

$$\lambda \leq \kappa\lambda \leq \lambda\lambda = \lambda.$$

$$\therefore \kappa\lambda = \lambda.$$

$\therefore \kappa + \lambda = \lambda \wedge \kappa\lambda = \lambda.$ ■

Capítulo 5

APLICACIONES

5.1 Al Algebra

Aplicación 1 *Si A y B son dos conjuntos cualesquiera, entonces*

$$|A| \leq |B| \vee |B| \leq |A|.$$

Demostración. Si

$$A = \emptyset \wedge B \neq \emptyset \vee A \neq \emptyset \wedge B = \emptyset \vee A = \emptyset = B,$$

entonces

$$|A| \leq |B| \vee |B| \leq |A| \vee (|A| \leq |B| \wedge |B| \leq |A|).$$

$$\therefore |A| \leq |B| \vee |B| \leq |A|.$$

Suponga que

$$A \neq \emptyset \wedge B \neq \emptyset.$$

Por el Teorema del Buen Orden, A y B pueden ser bien ordenados. Sea

$$\Omega = \{f_x : x \to B : x \subseteq A \wedge f \text{ es una función inyectiva}\}.$$

Ω es no vacío porque

$$f : \{\text{mín}(A)\} \to B$$

tal que

$$f(\text{mín}(A)) = \text{mín}(B)$$

es inyectiva,

$$\therefore f \in \Omega \wedge \Omega \neq \emptyset.$$

Defínase $\precsim$ como:

$$f_x \precsim f_y \Leftrightarrow x \subseteq y \wedge f_x = (f_y)_{|x}.$$

Sea $f_x \in \Omega$, entonces

$$x \subseteq x \wedge f_x \in \Omega \Rightarrow f_x = (f_x)_{|x}.$$

Entonces

$$(\forall (f \in \Omega))(f \precsim f).$$

$$\therefore \precsim \text{ es reflexiva.}$$

Suponga que

$$(\exists f_x)(\exists f_y)(f_x \in \Omega \wedge f_y \in \Omega \wedge f_x \precsim f_y \wedge f_y \precsim f_x).$$

Entonces

$$f_x = (f_y)_{|x} \wedge f_y = (f_x)_{|y},$$

Pero

$$f_x \precsim f_y \wedge f_y \precsim f_x \Rightarrow x \subseteq y \wedge y \subseteq x \Rightarrow x = y.$$

Entonces

$$f_x = ((f_x)_{|y})_{|x} = ((f_y)_{|y})_{|y} = f_y.$$

$$\therefore \precsim \text{ es antisimétrica.}$$

Suponga que

$$f_x \precsim f_y \wedge f_y \precsim f_z,$$

entonces

$$x \subseteq y \wedge y \subseteq z \wedge f_x = (f_y)_{|x} \wedge f_y = (f_z)_{|y}.$$

Entonces

$$x \subseteq z \wedge f_x = ((f_z)_{|y})_{|x} = (f_z)_{|x},$$

entonces

$$f_x \precsim f_z,$$

$$\therefore \precsim \text{ es transitiva.}$$

Sea C una cadena cualquiera en Ω.
P. d. a) $\cup C$ está bien definida.
b)

$$\cup C \in \Omega.$$

c) Si C es una cadena cualquiera,

$$(\forall f)(f \in C \Rightarrow f \precsim \cup C).$$

a) Sean

$$(x, y) \in \cup C \wedge (x, z) \in \cup C,$$

entonces

$$(\exists f_i)(\exists f_j)(f_i \in C \wedge f_j \in C \wedge f_i(x) = y \wedge f_j(x) = z).$$

Entonces

$$f_i \precsim f_j \vee f_j \precsim f_i,$$

entonces

$$f_i = f_{j_{ij}} \vee f_j = f_{i_{ij}},$$

entonces

$$f_i(x) = f_{j_{ij}}(x) = f_j(x) \vee f_j(x) = f_{i_{ij}}(x) = f_i(x).$$

$$\therefore y = z.$$

b)

$$\mathrm{Dom}(\cup C) = \mathrm{Dom}(f_1) \cup \ldots \cup \mathrm{Dom}(f_n).$$

Pero

$$(\forall i \in I)(\mathrm{Dom}(f_i) \subseteq A).$$

$$\therefore \mathrm{Dom}(\cup C) \subseteq A.$$

Suponga que

$$(x, z) \in \cup C \wedge (y, z) \in \cup C.$$

Entonces

$$(\exists f_i)(\exists f_j)(f_i \in C \wedge f_j \in C \wedge f_i(x) = z = f_j(y)).$$

Pero

$$f_i \precsim f_j \vee f_j \precsim f_i,$$

entonces

$$f_i = f_{j_{ij}} \vee f_j = f_{i_{ij}},$$

entonces

$$f_i(x) = f_{j_{ij}}(x) = f_j(x) \vee f_j(x) = f_{i_{ij}}(x) = f_i(x).$$

Entonces

$$f_j(x) = f_j(y) \vee f_i(x) = f_i(y).$$

$$\therefore x = y.$$

$$\therefore \cup C \in \Omega.$$

c) Sea $f_k \in C$, entonces

$$k = \mathrm{Dom}(f_k) \subseteq \mathrm{Dom}(f_1) \cup \ldots \cup \mathrm{Dom}(f_n) = \mathrm{Dom}(\cup C).$$

$$\therefore k \subseteq \mathrm{Dom}(\cup C).$$

Sea $(x, y) \in f_k$, entonces $(x, y) \in \cup C$. Entonces

$$(\forall f_k)(\forall (x,y))(f_k \in C \wedge (x,y) \in f_k \Rightarrow (x,y) \in \cup C).$$

$$\therefore (\forall f_k)(f_k \in C \Rightarrow f_k \precsim \cup C).$$

Entonces, por el Lema de Zorn,

$$(\forall f_k)(\exists f_M)(f_k \in \Omega \wedge f_M \in \Omega \Rightarrow f_k \precsim f_M).$$

Pero

$$M \subseteq A \Rightarrow M \subset A \vee M = A.$$

Entonces

$$M \subset A \Rightarrow B \leq A.$$

Y como f_M puede no ser biyectiva,

$$M = A \Rightarrow A \leq B.$$

$\therefore |A| \leq |B| \vee |B| \leq |A|$. ■

5.1.1 A los espacios vectoriales

Aplicación 2 *Todo espacio vectorial tiene base.*

Demostración. Sea V un espacio vectorial y

$$F = \{x \subseteq V : x \text{ es linealmente independiente}\},$$

entonces, F está ordenado bajo $\subseteq$;
sea C una cadena en F. P. d.

$$\cup C \in F.$$

Sean

$$v_1, ..., v_n \in \cup C \wedge a_1, ..., a_n \in \mathbb{R},$$

tal que

$$a_1 v_1 + ... + a_n v_n = 0,$$

entonces,

$$(\exists C_1, ..., C_m \in C)(v_1 \in C_1, ..., v_n \in C_m) \wedge m \leq n;$$

como $C \subseteq F$ es una cadena ordenada bajo $\subseteq$,

$$\{C_1, ..., C_m\}$$

debe tener un elemento mayor bajo $\subseteq$. Sea C_k el elemento mayor, entonces

$$C_i \subseteq C_k \wedge 1 \leq i \leq m \wedge i \neq k,$$

entonces

$$v_1, ..., v_n \in C_k,$$

pero $C_k \in F$, entonces C_k es linealment e independiente, entonces

$$a_1 = a_2 = ... = a_n = 0,$$

entonces $\cup C$ es linealmente independiente, entonces

$$\cup C \in F \wedge C \subseteq \cup C, \forall C \in F,$$

entonces, por el Lema de Zorn, F tiene un elemento $\subseteq$-máximo,
i.e. un subconjunto linealmente independiente máximo de V,
$\therefore V$ tiene una base. ■

Aplicación 3 *Todas las bases de un espacio vectorial V tienen el mismo cardinal.*

Demostración. Sean A y B dos bases cualesquiera para V.
Considere el conjunto

$$\Omega = \{(I_x, F_x) : I_x \subseteq A \wedge F_x : I_x \to B \text{ es inyectiva} \wedge B \backslash (F_x(I_x)) \cup I_x \text{ es l. i.}\}.$$

Defina un orden $\precapprox$ en Ω como:

$$(I_x, F_x) \precapprox (I_y, F_y) \Leftrightarrow I_x \subseteq I_y \wedge F_x = F_{y|_{I_x}}.$$

Muestre que Ω es no vacío, que $\precapprox$ es un orden parcial y que
toda cadena en Ω está acotada superiormente.
Aplique el Lema de Zorn a Ω. Concluya. ■

Aplicación 4 *El cardinal de un espacio vectorial V es el máximo entre el cardinal de su campo F y la dimensión del espacio V. i.e.*

$$|V_F| = máx(|F|, \dim(V)).$$

Demostración.

$$|V_F| = \text{card}\{f : \beta \to F : (\exists x \in \beta)(f(x) = 0)\}.$$

Donde β es una base para V y, como sabemos, $|\beta| = \dim V$.
Pero

$$\begin{gathered}\{f : \beta \to F : (\exists x \in \beta)(f(x) = 0)\} = \\ \{f : \beta \to F : (\exists! x \in \beta)(f(x) = 0)\} \cup \\ \{f : \beta \to F : (\exists! x \in \beta)(\exists! y \in \beta)(f(x) = 0 = f(y) \wedge x \neq y)\} \cup ... \\ \{f : \beta \to F : (\exists! x \in \beta)(f(x) \neq 0)\}.\end{gathered}$$

Sean $n \in \omega \wedge \kappa$ y λ dos números cardinales infinitos tales que $\kappa \leq \lambda$.
Entonces:
i) Si $|F| = n \wedge |\beta| = \kappa$,

$$\begin{gathered}\text{card}\{f : \beta \to F : (\exists x \in \beta)(f(x) = 0)\} = \kappa + \kappa^2 + ... + \kappa^{n-1} = \\ \kappa + \kappa + ... + \kappa = (n-1)\kappa = \kappa.\end{gathered}$$

ii) Si $|F| = \kappa \wedge |\beta| = n$,

$$\text{card}\{f : \beta \to F : (\exists x \in \beta)(f(x) = 0)\} = n + n^2 + ...n^{\kappa-2} + n^{\kappa-1} =$$
$n + n^2 + ... + n^\kappa + n^\kappa = n + n^2 + ... + \kappa + \kappa = c + m\kappa = \kappa$. Para algún $m \in \omega$.

iii) Si $|F| = \kappa \wedge |\beta| = \lambda$,

$$\text{card}\{f : \beta \to F : (\exists x \in \beta)(f(x) = 0)\} = \lambda + \lambda^2 + ... + \lambda^{\kappa-1} =$$
$$\lambda + \lambda + ... + \lambda^{\kappa-3} + \lambda^{\kappa-2} + \lambda^{\kappa-1} = n\lambda + ... + \lambda^\kappa + \lambda^\kappa + \lambda^\kappa =$$
$$n\lambda + m\lambda = \lambda + \lambda = \lambda. \text{ Para algunos } m, n \in \omega.$$

iv) Si $|F| = \lambda \wedge |\beta| = \kappa$,

$$\text{card}\{f : \beta \to F : (\exists x \in \beta)(f(x) = 0)\} = \kappa + \kappa^2 + ... + \kappa^{\lambda-2} + \kappa^{\lambda-1} =$$
$$\kappa + \kappa + ... + \kappa^\lambda + \kappa^\lambda = n\kappa + m\lambda = \kappa + \lambda = \lambda.$$

$\therefore |V_F| = \text{máx}(|F|, \dim(V))$. ■

5.1.2 A la Teoría de Grupos

Definición 32 *Un grupo $(G, *)$ es un conjunto G, junto con una operación binaria en G, tal que:*

i) La operación binaria $*$ es asociativa.
ii) $(\forall x \in G)(\exists e \in G)(\exists x' \in G)(e * x = x * e = e \wedge x * x' = x' * x = e)$.

Definición 33 *Un subconjunto no vacío H de un grupo $(G, *)$ es un subgrupo de G si*

$$(e \in H) \wedge$$
$$(\forall x, y \in H)(\exists x' \in H)(e * x = x * e = e \wedge x * x' = x' * x = e \wedge x * y \in H).$$

Y se denota $H \leq G$.

Definición 34 *Un grupo G es abeliano si su operación binaria $*$ es conmutativa.*

Definición 35 *Un grupo abeliano libre G es un grupo abeliano que contiene a una base X para G.*

Definición 36 *Un subgrupo H de un grupo G es un subgrupo normal de G si*

$$(\forall g \in G)(g^{-1}Hg = H).$$

i.e. si H permanece invariante bajo todo automorfismo interno de G.

Teorema 27 (Segundo Teorema de Isomorfismos) *Si N y T son subgrupos de G y N es normal, entonces $N \cap T$ es normal en T y*

$$T/(N \cap T) \cong (N + T)/N.^{[3]}$$

Lema 2 *Sea $\{A_k : k \in K\}$ una familia de subgrupos de un grupo G. Las siguientes afirmaciones son equivalentes:*

$$\text{i) } G \cong \sum_{k \in K} A_k.$$

ii) Todo $g \in G$ puede ser expresado de manera única en la forma

$$g = \sum_{k \in K} a_k.$$

iii)

$$G = \langle \bigcup_{k \in K} A_k \rangle \wedge (\forall j \in K)(A_j \cap \langle \bigcup_{k \neq j} A_k \rangle = 0).^{[9]}$$

Donde $\langle x \rangle$ es el grupo generado por x.

Corolario 4 *Si $H \leq G$ y G/H es abeliano libre, entonces*

$$G = H \oplus K.^{[9]}$$

Donde

$$K \leq G \wedge K \cong G/H.^{[9]}$$

Aplicación 5 *Todo subgrupo H de un grupo abeliano libre G es abeliano libre.*

Demostración. Sea $\{x_k : k \in K\}$ una base para F.
Donde K es un conjunto índice bien ordenado. Defínase

$$F'_k = \langle x_j : j < k\rangle \wedge F_k = \langle x_j : j \leq k\rangle = F'_k \oplus \langle x_k\rangle, (\forall k \in K);$$

y

$$H'_k = H \cap F'_k \wedge H_k = H \cap F_k.$$

Obsérvese que

$$F = \cup F_k \wedge H = \cup H_k.$$

Entonces

$$H'_k = H \cap F'_k = H_k \cap F'_k,$$

entonces, por el Segundo Teorema de Isomorfismos,

$$H_k/H'_k = H_k/(H_k \cap F'_k) \cong (H_k + F'_k)/F'_k \leq F_k/F'_k \cong \mathbf{Z}.$$

Entonces, por el corolario,

$$H_k = H'_k \vee H_k = H'_k \oplus \langle x_k\rangle.$$

Como

$$F = \cup F_k.$$

Defínase

$$f(h) = \text{mín}(k : k \in K \wedge h \in F_k).$$

Sea H^* el subgrupo generado por todas las h_k. P. d.

$$H^* = H.$$

Sea

$$j = \text{mín}\{f(h) : h \in H \wedge h \notin H^*\}$$

Tómese $h\prime \in H$ tal que

$$f(h\prime) = j.$$

Entonces

$$h\prime \in H \cap F_j,$$

entonces

$$h\prime = a + mh_j \wedge a \in H'_j \wedge m \in \mathbf{Z}.$$

Así,

$$a = h\prime - mh_j \in H \wedge a \notin H^* \wedge f(a) < j, !.$$

$$\therefore H = H^*.$$

Por el lema 1, queda por demostrar que las combinaciones lineales de h_k son únicas. Es suficiente con demostrar que

$$m_1 h_{k_1} + ... + m_n h_{k_n} = 0 \Rightarrow m_i = 0.$$

Donde

$$k_1 < ... < k_n.$$

Entonces

$$m_n h_{k_n} \in \langle h \rangle \cap H'_{k_n} = 0, !.$$

$\therefore H$ es libre abeliano. ■

5.1.3 A la Teoría de Anillos

Definición 37 *Un anillo $\langle N, +, * \rangle$ es un conjunto N, junto con dos operaciones binarias $+$ y $*$, tal que:*

i) $\langle N, + \rangle$ es un grupo abeliano.

ii) $*$ es asociativa.

iii) $(\forall x, y, z \in N)(x * (y + z) = (x * y) + (x * z) \wedge (x + y) * z = (x * z) + (y * z)$.

Definición 38 *Un ideal es un subgrupo aditivo* $\langle N, + \rangle$ *de un anillo* R *que satisface*

$$rN \subseteq N \wedge Nr \subseteq N.$$

Definición 39 *Los múltiplos* ax *de un elemento* x *forman un ideal principal.*

Se denota (x).

Definición 40 *Un ideal máximo de un anillo* R *es un ideal* M *diferente de* R *tal que no existe ningún ideal propio* N *de* R *que contenga propiamente a* M.

Teorema 28 *Todo anillo* $A \neq 0$ *tiene al menos un ideal máximo.*[1]

Aplicación 6 *Todo ideal* $\alpha \neq (1)$ *de un anillo* A *está incluido en un ideal máximo.*

Demostración. Sea

$$\Sigma = \{\alpha \subseteq A : \alpha \text{ es un ideal} \wedge \alpha \neq (1)\}.$$

Entonces $\subseteq$ es un orden para Σ.
Σ es no vacío porque el ideal $0 \in \Sigma$. Sea

$$C = \{\alpha_1, ..., \alpha_k\}$$

una cadena de ideales cualquiera en Σ. Por definición de cadena,

$$(\alpha_i \subseteq \alpha_j \vee \alpha_j \subseteq \alpha_i) \wedge 1 \leq i \leq j \leq k.$$

Sea

$$\beta = \bigcup_{n=1}^{k} \alpha_n.$$

Como

$$(\forall n \in \{1, ..., k\})(\alpha_n \in \Sigma \subseteq A),$$

entonces

$$\bigcup_{n=1}^{k} \alpha_n \subseteq \Sigma \subseteq A,$$

entonces

$$\beta \subseteq A.$$

Y si

$$x \in \beta \wedge y \in A,$$

entonces

$$x \in \alpha_m \wedge m \in \{1, ..., k\}.$$

Pero

$$xy \in \alpha_m,$$

entonces

$$xy \in \beta.$$

De manera trivial,

$$0 \in \beta.$$

$$\therefore \beta \text{ es un ideal de } A.$$

Y $1 \notin \beta$ porque

$$(\forall n \in \{1, ..., k\})(1 \notin \alpha_n).$$

$$\therefore \beta \in \Sigma.$$

Y como

$$(\forall C \subseteq \Sigma)(\beta \subseteq C),$$

entonces β es una cota superior para Σ en Σ.
Entonces, por el Lema de Zorn, Σ tiene un elemento máximo.
$\therefore (\forall \alpha \subseteq A)(\exists m \subseteq A)(\alpha \text{ es un ideal} \Rightarrow m \text{ es un ideal} \wedge m \neq (1) \wedge \alpha \subseteq m).$

■

5.1.4 A la Teoría de Campos

Definición 41 *Un anillo con unitario R es un anillo con identidad multiplicativa 1 tal que*

$$(\forall x \in R)(1x = x1 = x).$$

Definición 42 *Un elemento u en un anillo con unitario R es una unidad si existe $u\prime \in R$ tal que*

$$uu\prime = 1.$$

Definición 43 *Un anillo con división R es un anillo con unitario tal que todo elemento distinto de cero es una unidad.*

Definición 44 *Un campo F es un anillo conmutativo con división.*

Definición 45 *$F[x]$ es el conjunto de todos los polinomios en x sobre un campo F.*

Definición 46 *Un polinomio no constante $f(x) \in F[x]$ es irreducible sobre F si $f(x)$ no puede expresarse como producto $g(x)h(x)$ de dos polinomios $g(x)$ y $h(x)$ en $F[x]$, ambos de grado menor que $f(x)$.*

Definición 47 *Un campo E es un campo de extensión de F si $F \leq E$.*

Definición 48 *Un elemento α de un campo de extensión E de un campo F es algebraico sobre F si*

$$(\exists f(x) \in F[x])(f(x) \neq 0 \wedge f(\alpha) = 0).$$

De lo contrario, es trascendente sobre F.

Definición 49 *Un polinomio mónico es un polinomio con el coeficiente de la potencia mayor de x igual a* 1.

Definición 50 *El polinomio irreducible para α sobre F es el polinomio mónico para α sobre F.*

Y se denota $\mathrm{irr}(\alpha, F)$.

Definición 51 *El grado de* $irr(\alpha, F)$ *es el grado de* α *sobre* F.

Y se denota $\text{grad}(\alpha, F)$.

Definición 52 *Un campo de extensión* E *de un campo* F *es una extensión algebraica de* F *si todo elemento en* E *es algebraico sobre* F.

Definición 53 *Un campo* F *está algebraicamente cerrado si todo polinomio no constante en* $F[x]$ *tiene algún cero en* F.

Teorema 29 *Sea* E *un campo de extensión de* F *y sea* $\alpha \in E$ *algebraico sobre* F. *Si* $grad(\alpha, F) = n$, *entonces* $F(\alpha)$ *es un espacio vectorial* n-*dimensional sobre* F *con base* $\{1, \alpha, ..., \alpha^{n-1}\}$.*Más aún, todo elemento* $\beta \in F(\alpha)$ *es algebraico sobre* F *y* $grad(\beta, F) \leq grad(\alpha, F)$.[3]

Teorema 30 *Sea* E *una extensión algebraica de un campo* F. *Entonces existe un número finito de elementos* $\alpha_1, .., \alpha_n$ *tal que* $E = F(\alpha_1, .., \alpha_n)$ *si y sólo si* E *es un espacio vectorial de dimensión finita sobre* F, *i.e. si y sólo si* E *es una extensión finita de* F.[3]

Teorema 31 *Si* E *es un campo de extensión finita de un campo* F *y* K *es un campo de extensión finita de* E, *entonces* K *es una extensión finita de* F.[3]

Teorema 32 *Un campo de extensión finita* E *de un campo* F *es un extensión algebraica* F.[3]

Definición 54 *Una cerradura algebraica de un campo* F *es una extensión algebraica* F' *que está algebraicamente cerrada.*

Aplicación 7 *Todo campo* F *tiene una cerradura algebraica* F'.

Demostración. Sea

$$A = \{\omega_{f_i} : f \in F[x] \wedge f(\omega_{f_i}) = 0 \wedge i \in \{1, ..., (\text{grado de } f)\}\}.$$

i.e. A tiene un elemento para todo 0 posible de cualquier $f(x) \in F[x]$. Sea Ω tal que

$$A \cup F \subset \Omega.$$

Considérense todos los campos posibles que sean extensiones
algebraicas de F y que como conjuntos, consten de elementos de Ω.
Una de dichas extensiones es F mismo.
Si E es cualquier campo de extensión de F,
y si $\gamma \in E$ es un cero de $f(x) \in F[x]$, donde

$$\gamma \in F \wedge \text{grad}(\gamma, F) = n,$$

entonces, redenominando γ como ω para

$$\omega \in \Omega \wedge \omega \notin F,$$

y a los elementos

$$a_0 + a_1\gamma + ... + a_{n-1}\gamma^{n-1}$$

de $F(\gamma)$ como distintos elementos de Ω,
conforme a_i varía sobre F,podemos considerar $F(\gamma)$
como un campo de extensión algebraica $F(\omega)$ de F tal que

$$F(\omega) \subset \Omega \wedge f(\omega) = 0.$$

El conjunto Ω tiene elementos suficientes para formar $F(\omega)$, pues Ω
tiene más que elementos suficientes para proporcionar n ceros diferentes
para cada elemento de cada grado n en cualquier subconjunto de $F[x]$.
Todos los campos de extensión algebraica E_j de F con $E_j \subseteq \Omega$,
forman un conjunto

$$S = \{E_j : j \in J\}$$

parcialmente ordenado bajo la inclusión usual de subcampos.
F mismo es un elemento de S.
Lo anterior muestra que si F está lejos de ser algebraicamente cerrado,
habrá muchos campos E_j en S. Sea

$$T = \{E_{j_k}\}$$

una cadena cualquiera en S y sea

$$W = \underset{k}{\cup} E_{j_k}.$$

P. d. W es un campo. Sean $\alpha, \beta \in W$. Entonces

$$(\exists E_{j_1}, E_{j_2} \in S)(\alpha \in E_{j_1} \wedge \beta \in E_{j_2}).$$

Como T es una cadena,

$$E_{j_1} \leq E_{j_2} \vee E_{j_2} \leq E_{j_1}.$$

Sin pérdida de generalidad, suponga que

$$E_{j_1} \leq E_{j_2}.$$

Entonces

$$\alpha, \beta \in E_{j_2}.$$

Usamos las operaciones de E_{j_2}
para definir la suma de α y β en W como $(\alpha + \beta) \in E_{j_2}$,
y así mismo, el producto como $(\alpha\beta) \in E_{j_2}$.
Estas operaciones están bien definidas en W;
son independientes de la selección de $E_{j_1} \leq E_{j_2}$.
Porque si E_{j_3} para E_{j_3} en T, entonces

$$E_{j_2} \leq E_{j_3} \vee E_{j_3} \leq E_{j_2}.$$

Así, tenemos definidas en W las operaciones de suma y multiplicación.
Todos los axiomas de campo para W bajo estas operaciones se siguen
del hecho de que estas operaciones se definieron en términos de suma
y multiplicación en campos. Así, por ejemplo, $1 \in F$ sirve como identidad
multiplicactiva en W ya que

$$(\forall \alpha \in W)(1, \alpha \in E_{j_1} \Rightarrow 1\alpha = \alpha \in E_{j_1}) \Rightarrow 1\alpha = \alpha \in W,$$

por definición de multiplicación en W.
Para verificar las leyes distributivas:
Sean $\alpha, \beta, \gamma \in W$. Como T es una cadena, podemos encontrar algún
campo en T que contenga los tres elementos α, β y γ,
y en este campo se cumplan las leyes distributivas para α, β y γ.
Entonces, las leyes distributivas se cumplen en W.
$\therefore W$ es un campo.

Y por construcción,

$$(\forall E_{j_k} \in T)(E_{j_k} \leq W).$$

Pero

$$\alpha \in W \Rightarrow (\exists E_{j_r} \in T)(\alpha \in E_{j_r}),$$

entonces α es algebraica sobre F.
Entonces W es una extensión algebraica de F,
entonces $W \in S$ y W es una cota superior para T.
Por lo tanto, se satisface la hipótesis del Lema de Zorn,
entonces existe algún elemento máximo $F\prime \in S$.
Afirmamos que $F\prime$ está algebraicamente cerrado.
Sea $f(x) \in F\prime[x]$, donde $f(x) \notin F\prime$.
Suponga que $f(x)$ no tiene ceros en $F\prime$.
Como Ω tiene muchos más elementos que $F\prime$,
podemos tomar $\omega \in \Omega$ donde $\omega \notin F\prime$,
y formar un campo $F\prime(\omega) \subseteq \Omega$ con ω un cerò de $f(x)$,
como vimos al principio de la demosración.
Sea $\beta \in F\prime(\omega)$. Entonces por el teorema 28, β es un cero del polinomio

$$g(x) = \alpha_0 + \alpha_1 x + ... + \alpha_n x^n$$

en $F\prime[x]$ con $\alpha_i \in F\prime$, y por lo tanto α_i es algebraico sobre F.
Entonces, por el teorema 29,

$$F(\alpha_1, .., \alpha_n)$$

es una extensión finita de F,
y como β es algebraico sobre $F(\alpha_1, .., \alpha_n)$,

$$F(\alpha_1, .., \alpha_n, \beta)$$

es una extensión finita sobre $F(\alpha_1, .., \alpha_n)$.
Entonces, por el teorema 30,

$$F(\alpha_1, .., \alpha_n, \beta)$$

es una extensión finita de F. Entonces, por el teorema 31,

β es algebraico sobre F. Entonces

$$F\prime(\omega) \in S \wedge F' \leq F'(\omega), !.$$

Porque $F\prime$ es un máximo en S.
Entonces $f(x)$ debe tener algún cero en $F\prime$,
$\therefore$ $F\prime$ está cerrado algebraicamente. ■

Índice de Materias

Bibliografía

[1] Atiyah, M.F. *Inroduction to Commutative Algebra.* Addison-Wesley Pub. Co., 1969.

[2] Devlin, K. *The Joy of Sets.* Springer-Verlag, 1992.

[3] Fraleigh, J.B. *Abstract Algebra.* Addison-Wesley Pub. Co., 1987.

[4] Herstein, I.N. *Topics in Algebra.* Blaisdell Pub. Co., 1986.

[5] Hamilton, A.G. *Numbers, Sets and Axioms.* Cambridge University Press, 1982.

[6] Hernández, H.F. *Teoría de Conjuntos.* Sociedad Matemática Mexicana, 1998.

[7] Kaplanski, E. *Set Theory and Metric Spaces.* Chelsea Pub. Co., 1977.

[8] Mendelson, E. *Introduction to Mathematical Logic.* D. Van Nostrand, 1964.

[9] Rotman, J.J. *An Introduction to the Theory of Groups.* Springer-Verlag, 1994.