Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ciencias Matemáticas
Escuela Académico Profesional de Matemática

El axioma de elección en topología y álgebra

TESINA

Para optar el Título Profesional de Licenciado en Matemática

AUTOR

Abraham Crescencio AGUILAR PONCE

ASESOR

Pedro Celso CONTRERAS CHAMORRO

Lima, Perú

2009

Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-sa/4.0/

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Aguilar, A. (2009). *El axioma de elección en topología y álgebra*. Tesis para optar el título profesional de Licenciado en Matemática. Escuela Académico Profesional de Matemática, Facultad de Ciencias Matemáticas, Universidad Nacional Mayor de San Marcos, Lima, Perú.

Agradecimiento

En estas líneas quiero expresar mi más sincero agradecimiento a mi asesor, el Dr. Pedro Celso Contreras Chamorro, quien con su orientación y apoyo me ha permitido desarrollar y culminar la redacción de este trabajo.

Abraham Aguilar Ponce

Diciembre de 2009

Resumen

En este trabajo se exponen algunos elementos de Lógica Matemática con el propósito de enunciar, posteriormente, los axiomas que rigen la teoría de conjuntos en Matemáticas: los axiomas de Zermelo – Fraenkel, los mismos que son caracterizados mediante el uso de símbolos propios de un lenguaje formal. Uno de los axiomas de esta teoría, el axioma de elección, es presentado y se establece su equivalencia con dos principios: el Lema de Zorn y el Teorema del buen orden. Posteriormente, se muestran algunas aplicaciones del axioma de elección en dos ramas de la Matemática: Topología y Álgebra. En el primer caso se presenta el concepto de filtro y, mediante el uso del axioma, su extensión hacia un ultrafiltro. Finalmente, en el segundo caso, se presenta una definición de bases de Hamel y su existencia. Luego, se establece una equivalencia entre este principio y el axioma de elección.

Palabras claves: Lógica Matemática, Axiomas de Zermelo – Fraenkel, Axioma de Elección, Filtros, Ultrafiltros, Bases de Hamel.

Abstract

In this paper we describe some elements of Mathematical Logic in order to state, the governing axioms of set theory: the axioms of Zermelo - Fraenkel, which are characterized by the use of symbols in a formal language. One of the axioms of this theory, The Axiom of Choice is presented and its equivalence is established by two principles: Zorn's Lemma and The Well-Ordering Theorem. Subsequently, we will show some applications of The Axiom of Choice in two branches of mathematics: Topology and Algebra. In the first case, we introduce the concept of filter and using the axiom, its extension to an ultrafilter. In the second case, we define the Hamel basis and its existence. Finally, an equivalence between this principle and the axiom of choice is established.

Keywords: Mathematical Logic, Axioms of Zermelo – Fraenkel, Axiom of Choice, filters, ultrafilters, Hamel basis.

Índice general

Introducción

Un procedimiento inicial, usual en toda teoría matemática moderna, es el de enunciar una serie de axiomas y derivar resultados a partir de ellos, como por ejemplo, los axiomas de la teoría de grupos, de la teoría de anillos, la topología. En el caso de la teoría de conjuntos, los axiomas de Zermelo – Fraenkel son los que determinan una teoría axiomática, establecida formalmente en el contexto de la lógica de primer orden. Es por ese motivo que en el capítulo 1 del presente trabajo se introducen algunos elementos de Lógica Matemática, como son la sintaxis y la semántica para lenguajes de primer orden.

Posteriormente, en el capítulo 2, se establecen formalmente los axiomas de Zermelo – Fraenkel, y algunas de sus consecuencias. Inicialmente, Zermelo enunció dentro del grupo de axiomas, un axioma determinante en el desarrollo de las matemática moderna: el axioma de elección. En este trabajo se establece tal axioma y se demuestra su equivalencia con otros principios: el Lema de Zorn y el Teorema del buen orden, siendo el Lema de Zorn un principio de capital importancia cuando se trata de garantizar la existencia de elementos maximales. Por otra parte, en el capítulo 3 – relacionado con la Topología general – se establece el teorema de extensión de filtros a ultrafiltros (Teorema del ultrafiltro de Tarski). El principio que establece la existencia de bases de Hamel para un espacio vectorial y su equivalencia con el axioma de elección, es desarrollado en el capítulo 4. Finalmente, se enuncian algunas conclusiones del trabajo y la bibliografía correspondiente.

Capítulo 1

Elementos de Lógica Matemática

El objetivo principal de la lógica matemática es el estudio de las teorías matemáticas como la teoría de conjuntos, la teoría de números, la teoría de estructuras algebraicas, la teoría de grupos, etc., con el propósito de construir herramientas que permitan examinar su consistencia, completitud y todo aquello que concierna a los fundamentos de tales teorías. Los elementos de lógica matemática que mostramos a continuación son tomados del texto de Srivastava [8].

1.1. Lógica de primer orden: Sintaxis

1.1.1. Lenguajes de primer orden

Los objetos de estudio de las ciencias naturales tienen existencia física. En contraste, los objetos matemáticos son conceptos, por ejemplo "conjuntos", "pertenece a ($\in$)", "números naturales", etc.

En una teoría, deben existir conceptos iniciales y estos pueden ser definidos a partir de otros conceptos. Por ejemplo, $x - y$ es el único número z tal que $y + z = x$; o si x y y son conjuntos, $x \subset y$ si para cada elemento z , $z \in x$ implica $z \in y$. De este modo, "sustracción" puede ser "definida" en términos de la "adición" e "inclusión ($\subset$)" en términos de "pertenece a ($\in$)". En principio, se empieza con un número mínimo de conceptos no definidos. Por ejemplo, en la teoría de conjuntos, los conceptos no definidos son "conjunto" y "pertenece a"; en teoría de números, los conceptos no definidos son "números naturales", "cero", "función sucesora". En estos ejemplos se observa que existen dos grupos de conceptos: conjunto de números naturales por una parte; pertenecer a, cero, sucesor, por otra parte. Los conceptos del primer tipo son los objetos principales a estudiarse, mientras que los conceptos del segundo tipo son usados para reflejar las propiedades estructurales básicas de los objetos del primer tipo. A partir de ello se construye un conjunto de axiomas que proporcionan tales propiedades de los objetos en estudio. Se espera que sobre la bases de estos conceptos no definidos y los axiomas, se puedan definir otros conceptos, desarrollando la teoría e introduciendo cada vez más objetos y demostrando más teoremas.

Es claro que ha de considerarse un lenguaje para desarrollar una teoría. Como cualquier otro lenguage natural, un lenguaje adecuado para una teoría matemática también tiene un alfabeto. Pero a diferencia de los lenguajes naturales, un enunciado en teoría matemática es expresado simbólicamente y tiene una construcción sintáctica no ambigua. A continuación algunos ejemplos:

Ejemplo 1.1. Consideremos el siguiente enunciado en teoría de grupos: Para cada x existe y tal que $x.y = e$. Aquí . (punto) es un símbolo para la operación binaria de grupo y e para el elemento identidad. Si usamos el símbolo $\forall$ para denotar "para cada" y $\exists$ para denotar “existe”, podemos representar el enunciado anterior como:

$$\forall x\, \exists y\, (x.y = e).$$

Ejemplo 1.2. Consideremos los siguientes enunciados en teoría de conjuntos:

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

y

$$\neg \exists x\, \forall y\, (y \in x).$$

El primer enunciado es una representación simbólica de “Dados dos conjuntos x y y, hay un conjunto z que contiene tanto a x como a y; el segundo enunciado significa que “ No hay un conjunto x que contenga todos los conjuntos y”

Vemos que el lenguaje para una teoría debe tener “variables” para representar los objetos a estudiarse – por ejemplo, los conjuntos en teoría de conjuntos o los elementos de un grupo en teoría de grupos – y algunos símbolos lógicos como $\exists$ (existe), $\wedge$ (y), $\neg$ (negación), $=$ (igualdad). Estos símbolos son comunes a los lenguajes para todas las teorías, y los llamaremos símbolos lógicos. Por otra parte, existen ciertos alfabetos que representan conceptos no definidos de una teoría específica. Por ejemplo, en teoría de grupos usamos dos símbolos: el punto . para la operación del grupo y un símbolo, digamos e, para el elemento identidad; en teoría de conjuntos tenemos un símbolo de relación binaria $\in$ para el concepto no definido pertenecer a.

En matemáticas, usualmente se utilizan muchos conectivos lógicos y cuantificadores tales como $\vee$ (o), $\wedge$ (y), $\exists$ (existe), $\forall$ (para todo), $\rightarrow$ (si ..., entonces ...), y $\leftrightarrow$ (si y solo si). Sin embargo, si consideramos los siguientes razonamientos “dos enunciados A y B son ambos ciertos " si y solo si "no es cierto que A o B sea falso"; "A implica B" si y solo si " o A es falso o B es cierto" estamos indicando que algunos conectivos lógicos y cuantificadores pueden ser definidos en términos de otros. De este modo, es posible empezar con pocos cuantificadores y conectivos que permitirán desarrollar muchas pruebas de modo simplificado.

Definición 1.1. Un lenguaje de primer orden $\mathcal{L}$ consta de dos tipos de símbolos: **símbolos lógicos** y **símbolos no lógicos**. Los símbolos lógicos lo constituyen una sucesión de **variables** $x_0, x_1, x_2, ...$; **conectivos lógicos** $\neg$ (negación) y $\vee$ (disyunción); un **cuantificador lógico** $\exists$ (cuantificador existencial) y el **símbolo de igualdad** $=$. Al orden en el cual las variables $x_0, x_1, x_2, ...$ son dadas se les denomina **orden alfabético**. Estos símbolos lógicos son comunes a todos los lenguajes de primer orden. Dependiendo de la teoría, los símbolos no lógicos de $\mathcal{L}$ consisten de un conjunto (vacío o no vacío) de **símbolos de constantes** $\{c_i : i \in I\}$; para cada entero positivo n, un conjunto de **símbolos de funciones** n-aria$\{f_j : j \in J_n\}$; y un conjunto de **símbolos de relaciones** n-aria $\{p_k : k \in K_n\}$.

Por otra parte, consideraremos lo siguiente:

- Un lenguaje de primer orden será denominado simplemente lenguaje.
- Para especificar un lenguaje será suficiente especificar sus símbolos no lógicos, puesto que todos los lenguajes tienen los mismos símbolos lógicos.
- En vez de usar los símbolos $x_0, x_1, x_2, ...$, para denotar las variables, usaremos los símbolos x, y, z, u, v, w.

- Cualquier sucesión finita de símbolos de un lenguage $\mathcal{L}$ se denominará una **expresión** en $\mathcal{L}$.

- Un lenguaje $\mathcal{L}$ se denominará **contable** si solamente tiene una cantidad contable de símbolos no lógicos. En caso tenga una cantidad finita de tales símbolos se denominará lenguaje **finito**.

Ejemplo 1.3. El lenguaje de la teoría de conjuntos tiene solamente un símbolo no lógico: el símbolo de la relación binaria $\in$ para "pertenece a."

Ejemplo 1.4. El lenguaje de la teoría de grupos tiene un símbolo constante e (para el elemento identidad) y un símbolo de función binaria . (para la operación de grupo).

Ejemplo 1.5. El lenguaje para la teoría de anillos con identidad tiene dos símbolos de constante 0 y 1 y dos símbolos de función binaria $+$ y $\cdot$.

Ejemplo 1.6. El lenguaje para la teoría de cuerpos ordenados tiene dos símbolos de constante 0 y 1 , dos símbolos de función binaria $+$, $\cdot$ y un símbolo de relación binaria $<$.

Definición 1.2. Un lenguaje de primer orden $\mathcal{L}'$ es llamado una **extensión** de otro lenguaje $\mathcal{L}$, si cada símbolo de constante de $\mathcal{L}$ es un símbolo de constante de $\mathcal{L}'$ y cada símbolo de función (relación) n-aria de $\mathcal{L}$ es un símbolo de función (relación) n-aria de $\mathcal{L}'$.

Ejemplo 1.7. El lenguaje para la teoría de los cuerpos ordenados es una extensión del lenguaje para la teoría de los anillos con identidad.

1.1.2. Términos de un Lenguaje

Hablando en forma general, los **términos** de un lenguaje conrresponden a expresiones algebraicas.

Definición 1.3. El conjunto de todos los términos de un lenguaje $\mathcal{L}$ es el menor conjunto $\mathcal{T}$ de expresiones de $\mathcal{L}$ que contiene todas las variables y símbolos de constantes; además, es cerrado bajo la siguiente operación: siempre que $t_1 \ldots t_n \in \mathcal{T}$, $f_j t_1 \ldots t_n \in \mathcal{T}$, donde f_j es un símbolo de función n-aria de $\mathcal{L}$.

De forma equivalente, todos los téminos de un lenguaje pueden ser inductivamente definidos como sigue:

- Los símbolos de variables y constantes son términos de *rango* 0.
- Si $t_1 \ldots t_n$ son términos de rango $\leq k$ y f_j es un símbolo de función n-aria, entonces $f_j t_1 \ldots t_n$ es un término de rango $\leq k+1$.

Así, el **rango** de un término t es el menor número natural k tal que t es de rango $\leq k$.

Convengamos en usar los paréntesis y comas en la forma *usual* para facilitar la lectura. Por ejemplo, en vez de escribir $f_j t_1 \ldots t_n$ escribiremos $f_j(t_1, \ldots, t_n)$, y $t+s$ en vez de $+ts$. Prescindiremos de los paréntesis cuando no exista posibilidad de confusión. Además, adoptamos la convención de asociación a la derecha. Por ejemplo, en vez de escribir $t_1.(t_2.(t_3.t_4))$ escribiremos $t_1.t_2.t_3.t_4$.

Ejemplo 1.8. Sea $\mathcal{L}$ el lenguaje para la teoría de anillos con identidad: $\mathcal{L}$ tiene dos símbolos de constantes, 0 y 1, y dos símbolos de funciones binarias, $+$ y $\cdot$. Consideremos $\underline{m}$ para denotar el término obtenido "sumando" 1 m veces, es decir $\underline{m}$ es el término

$$\underbrace{1 + \cdots + 1}_{\text{m veces}};$$

para todo término t, t^n denota el término obtenido "multiplicando" t n veces, es decir, t^n es el término

$$\underbrace{t \cdot t \cdots t \cdot t}_{\text{n veces}}.$$

Así, $\underline{m}$ y t^n son términos de $\mathcal{L}$.

Ejemplo 1.9. Las variables son los únicos términos del lenguaje para la teoría de conjuntos, porque esta no tiene constantes ni símbolos de función.

Definición 1.4. Sea t un término del lenguaje $\mathcal{L}$. El conjunto de todos los **subtérminos** de t es definido inductivamente como sigue:

- t es subtérmino de t.
- Si $ft_1 \cdots t_n, t_1, ..., t_n \in \mathcal{T}$, es un subtérmino de t, lo es cada t_i, $1 \leq i \leq n$.

Una expresión es un subtérmino de t si ésta es obtenida como se indicó. De este modo, *el conjunto de todos los subtérminos de un término t es el menor conjunto $\mathcal{S}$ de expresiones que contiene a t y tal que si $ft_1 \cdots t_n \in \mathcal{S}$, entonces $t_1, ..., t_n \in \mathcal{S}$.*

Ejemplo 1.10. Sea t el término $x \cdot y \cdot z$ en el lenguaje de la teoría de grupos. Entonces, $x \cdot y \cdot z$, x, $y \cdot z$, y y z son todos los subtérminos de t. De acuerdo con la convención adoptada y la definición de subtérminos, $x \cdot y$ no es un subtérmino de t (recordar la convención de asociación por izquierda).

Sea s un término. Escribimos $s[v_1, ..., v_n]$ para indicar que las variables que ocurren en s están entre $v_1, ..., v_n$. Si s es un término, $s_{v_1,...,v_n}[t_1, ..., t_n]$, o simplemente $s[t_1, ..., t_n]$ cuando no exista posibilidad de confusión, denotará la expresión obtenida a partir de s reemplazando simultáneamente todas las ocurrencias de $v_1, ..., v_n$ en s por $t_1, ..., t_n$ respectivamente.

Ejemplo 1.11. Sea s el término $x \cdot (y + z)$ en el lenguaje de la teoría de anillos con identidad. Entonces

$$s_{x,y,z}[x + z, 1, y \cdot y] = (x + z) \cdot (1 + y \cdot y).$$

1.1.3. Fórmulas de un Lenguaje

Definición 1.5. Una **fórmula atómica** de un lenguaje es definida como sigue: si t y s son términos de $\mathcal{L}$, entonces $t = s$ es una fórmula atómica de $\mathcal{L}$; si p es un símbolo de relación n-aria de $\mathcal{L}$ y $t_1, ..., t_n$ son términos, entonces $pt_1 \cdots t_n$ es una fórmula atómica

Ejemplo 1.12. $v \in w, v = w$, donde v, w son variables, son todas las fórmulas atómicas en el lenguaje de la teoría de conjuntos.

Definición 1.6. Una **fórmula** de un lenguaje es definida inductivamente como sigue:

- Toda fórmula atómica es una fórmula (éstas son todas las fórmulas de **rango** 0).
- Si A y B son fórmulas de rango $\leq k$ y v es una variable, entonces $\neg A$ (negación de A), $\exists v A$ y $\vee AB$ (disyunción de A y B) son fórmulas de rango $\leq k + 1$

El conjunto de cadenas así obtenidas son todas las fórmulas de $\mathcal{L}$. De este modo, *el conjunto de todas las fórmulas de $\mathcal{L}$ es el menor conjunto de todas las expresiones de $\mathcal{L}$ que contiene todas las fórmulas atómicas y es cerrado bajo la negación, disyunción y cuantificación existencial.*

Definición 1.7. Sea A una fórmula del lenguaje $\mathcal{L}$. El **rango** de A es el menor número natural k tal que rango de A es $\leq k$.

Convenciones. A partir de ahora, a menos que se establezca otro caso, adoptaremos las siguientes convenciones

- $\mathcal{L}$ denotará un lenguaje de primer orden, y por un término (o una fórmula) entenderemos un término (o una fórmula) de $\mathcal{L}$.
- Escribiremos $A \vee B$ en vez de $\vee AB$
- Asociación por derecha, omitiendo los paréntesis: $A \vee B \vee C$ en vez de $A \vee (B \vee C)$, $A \vee B \vee C \vee D$ en vez de $A \vee (B \vee (C \vee D))$, y así sucesivamente.

A continuación, se definen algunos conectivos lógicos usuales y cuantificadores:

- $\forall vA$ es una abreviación de $\neg\exists v\neg A$. $\forall$ es denominado **cuantificador universal**.
- $A \wedge B$ abrevia $\neg(\neg A \vee \neg B)$. El conectivo $\wedge$ es denominado **conjunción**.
- $A \to B$ es una abreviación de $(\neg A) \vee B$.

Una fórmula de la forma $\exists vA$ es denominada una **ejemplificación** de A, y una fórmula de la forma $\forall vA$ es denominada una **generalización** de A. Una fórmula es llamada **elemental**, si es una fórmula atómica o una ejemplificación de una fórmula.

Definición 1.8. Una **subfórmula** de una fórmula A es definida inductivamente como sigue: A es una subfórmula de sí misma; si $\neg B$ o $\exists vB$ es una subfórmula de A, entonces lo es B; si $B \vee C$ es una subfórmula de A, entonces B o C son subfórmulas de A; ninguna otra opción distinta a las mencionadas es una subfórmula de A.

De esta forma, el conjunto de subfórmulas de A es el menor conjunto $\mathcal{S}(A)$ de fórmulas de $\mathcal{L}$ que contiene a A y satisface las siguientes condiciones: siempre que $\neg B$ o $\exists vB$ está en $\mathcal{S}(A)$, lo está B , y siempre que $B \vee c$ esté en $\mathcal{S}(A)$, lo están B y C.

Una ocurrencia de una variable v en una fórmula A está **ligada** si esta ocurre en una subfórmula de la forma $\exists vB$; en otro caso, la ocurrencia es llamada **libre**. Una variable es denominada libre en A si esta tiene una ocurrencia libre en A. Escribimos $\varphi[v_0, ..., v_n]$ si φ es una fórmula en la cual todas sus variable libres pertenecen al conjuto $\{v_0, ..., v_n\}$.

Ejemplo 1.13. En la fórmula

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

todas las ocurrencias de y son libres, la primera ocurrencia de x es libre, y las otras ocurrencias de x están ligadas.

Una fórmula sin variables libres se denomina **fórmula cerrada** u **oración**. Una fórmula que no contiene cuantificadores se denomina **fórmula abierta**.

Sea $A[x_0, ..., x_{n-1}]$ una fórmula cuyas variables libres están entre $x_0, ..., x_{n-1}$ y x_{n-1} es libre en A, donde $x_0, ..., x_{n-1}$ son las primeras n variables en orden alfabético. Denominamos

$$\forall x_{n-1} \dots \forall x_0 A$$

la **clausura** de A. Observar que si A es cerrado, A coincide con su clausura. Sea t un término, v una variable y A una fórmula de un lenguaje $\mathcal{L}$. Decimos que el **término** t **es sustituible** por v en A, si para cada variable w que ocurre en t, ninguna subfórmula de A de la forma $\exists wB$ contiene una ocurrencia de v que es libre en A.

Ejemplo 1.14. En la fórmula

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

no se puede sustituir cualquier término que contiene a x por y.

Si t es sustituible por v en A, entonces $A_v[t]$ designa la expresión obtenida a partir de A reemplazando simultáneamente cada ocurrencia libre de v en A por t. Similarmente, si los términos $t_1, ..., t_n$ son sustituibles en A por $v_1, ..., v_n$ respectivamente, entonces $A_{v_1,...,v_n}[t_1, ..., t_n]$, o $A[t_1, ..., t_n]$, cuando no exista posibilidad de confusión, llamado un **ejemplo** de A, denotará la expresión obtenida a partir de A por reemplazo simultáneo de todas las ocurrencias libres de $v_1, ..., v_n$ en A por $t_1, ..., t_n$ respectivamente. Observar que, cuando se hable de $A[t_1, ..., t_n]$, se asume que $t_1, ..., t_n$ son sustituibles en A por $v_1, ..., v_n$, respectivamente.

Ejemplo 1.15. Dada la fórmula

$$x \in y \vee \exists x(x \in y).$$

Entonces $A_x[z]$ es la fórmula $z \in y \vee \exists x(x \in y)$

1.1.4. Teorías de primer orden

Definición 1.9. Una **teoría de primer orden** o simplemente una **teoría** T consiste de un lenguaje de primer orden $\mathcal{L}$ y un conjunto de fórmulas de $\mathcal{L}$. Estas fórmulas son llamadas **axiomas no lógicos** de T. Por términos o fórmulas de T, entenderemos términos o fórmulas respectivamente del lenguaje para T. El lenguaje para T es también denotado por $\mathcal{L}(T)$. Una teoría es llamada **contable**, si su lenguaje es contable. Tal teoría será finita, si el conjunto de símbolos no lógicos es finito. En general, una teoría T cuyo conjunto de símbolos no lógicos es de cardinalidad κ, κ un cardinal infinito, es llamada una $\kappa-$ **teoría.**

Ejemplo 1.16. La teoría de grupos es una teoría cuyos símbolos no lógicos son, un símbolo de constante e y un símbolo de función binaria $\cdot$. Los axiomas no lógicos son las siguientes fórmulas:

1. $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$.

2. $\forall x (x \cdot e = x \wedge e \cdot x = x)$.

3. $\forall x \exists y (x \cdot y = e \wedge y \cdot x = e)$.

Ejemplo 1.17. La teoría de grupos abelianos es la teoría cuyos símbolos no lógicos son un símbolo de constante 0 y un símbolo de función binaria $+$ y cuyos axiomas no lógicos son las fórmulas:

1. $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$.

2. $\forall x (x + 0 = x \wedge 0 + x = x)$.

3. $\forall x \exists y (x + y = 0 \wedge y + x = 0)$.

4. $\forall x \forall y (x + y = y + x)$.

Ejemplo 1.18. El lenguaje para la **teoría de anillos con identidad** tiene dos símbolos de constantes, 0 y 1, y dos símbolos de funciones binarias, $+$ y $\cdot$. Los axiomas no lógicos de esta teoría son los axiomas $(1) - (4)$ de los grupos abelianos, junto con los axiomas:

5. $\forall x \forall y \forall z (x \cdot (y \cdot z = (x \cdot y) \cdot z)$.

6. $\forall x (x \cdot 1 = x \ \wedge \ 1 \cdot x = x)$.

7. $\forall x \forall y \forall z (x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

8. $\forall x \forall y \forall z((y+z) \cdot x = (y \cdot x) + (z \cdot x)$.

Ejemplo 1.19. La teoría de los campos tiene el mismos lenguaje que la teoría de anillos con identidad; sus axiomas no lógicos son los axiomas $(1)-(8)$ de la teoría de anillos con identidad junto con los siguientes axiomas

9. $\forall x \forall y(x \cdot y = y \cdot x)$.

10. $\forall x(\neg(x = 0) \rightarrow \exists y(x \cdot y = 1 \wedge y \cdot x = 1))$.

Ejemplo 1.20. Sea $\mathcal{L}$ el lenguaje con un sólo símbolo no lógico: un símbolo de relación binaria $<$. **La teoría de los conjuntos ordenados linealmente** (OL) es la teoría cuyo lenguaje es $\mathcal{L}$ y cuyos axiomas no lógicos son

1. $\forall x \neg(x < x)$.

2. $\forall x \forall y \forall z((x < y \wedge y < z) \rightarrow x < z)$.

3. $\forall x \forall y(x < y \vee x = y \vee y < x)$.

Ejemplo 1.21. La teoría de densidad de los conjuntos ordenados linealmente (DOL), es obtenida a partir de (OL) adicionando los siguiente axiomas:

4. $\forall x \forall y((x < y) \rightarrow \exists z(x < z \wedge z < y))$.

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

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

Ejemplo 1.22. Sea F la teoría de los campos. Para cada $m \geq 1$, sea A_m la fórmula $\neg(\underline{m} = 0)$. La teoría obtenida por adicionar cada A_m al conjunto de axiomas de $\mathcal{F}$ como un axioma es llamada la **teoría de los campos de característica** 0.

Ejemplo 1.23. Sea F la teoría de los campos. Sea $\mathcal{L}$ una extensión del lenguaje para la teoría de anillos con identidad obtenida por adición de un nuevo símbolo de predicado binario $<$. Considere la teoría CO cuyo lenguaje es $\mathcal{L}$ y cuyos axiomas no lógicos son todos los axiomas no lógicos de F y los siguientes axiomas:

11. $\forall x \neg(x < x)$

12. $\forall x \forall y \forall z((x < y \wedge y < z) \rightarrow (x < z)$.

13. $\forall x \forall y(x < y \vee x = y \vee y < x)$.

14. $\forall x \forall y(\neg(x < y \vee x = y) \rightarrow y < x)$.

15. $\forall x \forall y(x < y \rightarrow \forall z(x + z < y + z))$.

16. $\forall x \forall y((0 < x \wedge 0 < y) \rightarrow 0 < x \cdot y)$.

La teoria CO es conocida como la **teoría de los campos ordenados**.

Ejemplo 1.24. A continuación se enuncian una serie de axiomas de la teoría de números, el cual desempeña un papel importante en lógica. Designemos esta teoría por N. Los símbolos no lógicos de N son un símbolo de constante 0, un símbolo de función 1-aria S (función sucesora), dos símbolos de función binaria $+$ y $\cdot$, y un símbolo de relación binaria $<$. Los axiomas no lógicos de N son:

1. $\forall x(\neg(Sx = 0))$.

2. $\forall x \forall y(Sx = Sy \rightarrow x = y)$.

3. $\forall x(x + 0 = x)$.

4. $\forall x \forall y(x + Sy = S(x + y))$.

5. $\forall x(x \cdot 0 = 0)$.

6. $\forall x \forall y(x \cdot Sy = (x \cdot y) + x)$.

7. $\forall x(\neg(x < 0))$.

8. $\forall x \forall y(x < Sy \leftrightarrow (x < y \vee x = y))$.

9. $\forall x(\forall y(x < y \vee x = y \vee y < x))$.

Para cada entero no negativo n, el término

$$\underbrace{S \cdots S}_{m \text{ veces}} 0$$

será denotado por k_n. Estos términos son llamados **numerales**. Observar que k_0 es el símbolo de constante 0.

Ejemplo 1.25. La **Aritmética de Peano** es la teoría obtenida a partir de N eliminando los últimos axiomas y adicionando el siguiente esquema de axioma, llamado esquema de axioma de inducción: para cada fórmula $A[v]$, la fórmula

$$A_v[0] \to \forall v(A \to A_v[Sv]) \to A$$

es llamada un axioma de inducción. Denotamos esta teoría con AP.

Observación 1.1. Los axiomas de la teoría de conjuntos, denominada **Teoría de conjuntos de Zermelo-Fraenkel** y denotada por **ZF**, serán enunciadas en el Capítulo 2 del presente trabajo.

1.2. Lógica de primer orden: Semántica

1.2.1. Estructura de los Lenguajes de primer orden

Definición 1.10. Una **estructura** o una **interpretación** de un lenguaje de primer orden $\mathcal{L}$ consta de:

(E1) Un conjunto no vacío M denominado el **universo** de la estructura.

(E2) Para cada símbolo de constante c de $\mathcal{L}$, un elemento fijado $c_M \in M$.

(E3) Para cada símbolo de función n-aria f de $\mathcal{L}$, hay una aplicación $f_M : M^n \to M$.

(E4) Para cada símbolo de relación n-aria p de $\mathcal{L}$, hay una relación n-aria $p_M \subset M^n$ en M.

La interpretación de $=$ es siempre considerada como la relación de igualdad en M.

Los elementos del universo de M son llamados los **individuos de la estructura**; las aplicaciones f_M las **funciones individuales de la estructura**; y las relaciones p_M **predicados individuales**; c_M, f_M, y p_M serán llamadas interpretaciones del símbolo de constante c, del símbolo de función f, y del símbolo de predicado p respectivamente.

Ejemplo 1.26. Sea $\mathbb{N}$ el conjunto de todos los números naturales y $0, 1, +, \cdot$, y $<$ tienen el significado usual. Es más, sea $S(n) = n+1, n \in \mathbb{N}$. Esta es una estructura para el lenguaje de la teoría N definida en la Sección 1. Esta estructura será llamada la **estructura estándar de** N.

Sea $\mathcal{L}$ una extensión de $\mathcal{L}'$. Ignorando la interpretación de aquellos símbolos no lógicos de $\mathcal{L}$ que no son símbolos de $\mathcal{L}'$, conseguimos una estructura M' de $\mathcal{L}'$. Denominamos a M'

la **restricción** de M a $\mathcal{L}'$ y lo denotamos con $M|\mathcal{L}'$. En este caso también decimos que M es una **expansión** de M' a $\mathcal{L}$.

Recordemos que todos los términos de variable libre pueden ser obtenidos a partir de los símbolos de constante e iterando los símbolos de función sobre ellos. Así, podemos definir una interpretación o significado t_M de cada término de variable libre t de $\mathcal{L}$ en M por inducción sobre el rango de t. La interpretación de un símbolo de constante c ya es dado por la estructura, a saber c_M. Si $t_1, ..., t_n$ son términos de variable libre cuyas interpretaciones han sido definidas y si f es un símbolo de función n-aria de $\mathcal{L}$, entonces se define

$$(ft_1 \cdots t_n)_M = f_M((t_1)_M, ..., (t_1)_M).$$

Ejemplo 1.27. Sea $\mathcal{L}$ el lenguaje para la teoría de anillos con identidad. Para cada entero positivo m, $\underline{m}$ denota el término obtenido por "adicionar´´ 1 así mismo m veces. Sea $P(x)$ una expresión polinomial cuyos coeficientes son todos de la forma $\underline{m}$, es decir $P(x)$ es un término de la forma

$$\underline{m_0} + \underline{m_1}x + \cdots + \underline{m_n}x^n,$$

donde x es una variable. Sea R un anillo con identidad. Entonces la interpretación de $\underline{m}$ en R es el elemento $m \in R$ obtenido por adición de la identidad multiplicativa de R consigo mismo m veces, y por cada término de variable libre t, la interpretación de $P_x[t]$ en R es el elemento $P(t_M)$ de R.

1.2.2. Verdad en una estructura

A continuación, definimos cuándo una fórmula de $\mathcal{L}$ es verdadera y cuándo esta es falsa en una estructura de $\mathcal{L}$. Observar que si tenemos una estructura de $\mathcal{L}$ con universo M y queremos saber si existe un elemento $a \in M$ que satisface una fórmula $\varphi[x]$, pero tenemos un pequeño problema porque φ es un objeto sintáctico, y los elementos de M no lo son. Para evitar este problema, dada una estructura de $\mathcal{L}$ con universo M, en primer lugar describimos una extensión $\mathcal{L}_M$ del lenguaje $\mathcal{L}$.

Definición 1.11. Dado $\mathcal{L}$ y una estructura de $\mathcal{L}$ con universo M. Sea $\mathcal{L}_M$ el lenguaje de primer orden obtenido a partir de $\mathcal{L}$ adicionando un nuevo símbolo de constante i_a por cada $a \in M$. El símbolo i_a es llamado el **nombre** de a. Consideramos al propio M como la expansión de M a $\mathcal{L}_M$ estableciendo la interpretación de i_a como a para cada $a \in M$.

Ahora, podemos definir cuándo una fórmula de $\mathcal{L}$ es verdadera o válida o satisfacible en una estructura M. Para lograrlo, definimos la noción de verdad de una fórmula cerrada o una oración de $\mathcal{L}_M$ en una estructura M. La definición se sustenta en el conocido significado de los conectivos lógicos $\vee$ y $\neg$ y del cuantificador existencial $\exists$. La noción de verdad será definida a partir de la definición de una función que parte del conjuntos de todas las fórmulas cerradas de $\mathcal{L}_M$ y asigna valores en el conjunto $\{verdadero, falso\}$, satisfaciendo algunas condiciones. Esta será dada por inducción sobre el rango de oraciones de $\mathcal{L}_M$. Si una oración toma el valor verdadero, diremos que la oración es verdadera o válida en M; caso contrario esta será llamada falsa en M.

Recordemos que las fórmulas han sido definidas inductivamente empezando por las fórmulas atómicas e iterando $\neg$, $\vee$, y $\exists$ sobre ellos. Una fórmula atómica de variable libre es de la forma $pt_1 \cdots t_n$, donde p es un símbolo de relación n-aria (incluyendo $=$) y $t_1, ..., t_n$ son términos de variable libre. Decimos que $pt_1 \cdots t_n$ es verdadera en la estructura, si se tiene

$$p_M((t_1)_M, ..., (t_n)_M),$$

es decir,

$$((t_1)_M, ..., (t_n)_M) \in p_M \subset M^n.$$

En otro caso, decimos que $pt_1 \cdots t_n$ es falsa en la estructura. Una oración $\neg A$ es verdadera, si y solo si A es falsa. Una oración $A \vee B$ es verdadera si A es verdadera o B es verdadera. Finalmente, una oración $\exists vA$ es verdadera si $A_v[i_a]$ es verdadera para algún $a \in M$. Decimos que una fórmula A de $\mathcal{L}_M$ es verdadera en la estructura si su clausura es verdadera en la estructura. Si una fórmula A de $\mathcal{L}$ es verdadera en una estructura M de $\mathcal{L}$, también decimos que A es **válida en la estructura** y escribimos $M \models A$. Si A no es válida en M, escribimos $M \not\models A$. Observar que si A y B son fórmulas cerradas, entonces

$$M \not\models A \Longleftrightarrow M \models \neg A$$

y

$$M \models A \vee B \Longleftrightarrow M \models A \text{ o } M \models B.$$

1.2.3. Modelo de una Teoría

Definición 1.12. Un **modelo** de una teoría de primer orden T es una estructura de $\mathcal{L}(T)$ con universo M en el cual todos los axiomas no lógicos de T son válidos.

Ejemplo 1.28. Todo grupo es un modelo de la teoría de grupos. Por otra parte, el conjunto de números naturales $\mathbb{N}$ junto con 0 y $+$ como interpretaciones para e y $\cdot$ respectivamente es definitivamente una estructura para el lenguaje de la teoría de grupos pero no un modelo de tal teoría.

Definición 1.13. Un fórmula A de T que es verdadera en todos los modelos de T es llamada **válida** en T. Escribimos $T \models A$ si A es válida en T. Si A no es válida en algún modelo de T, escribimos $T \not\models A$.

Ejemplo 1.29. Sea $\mathcal{L}$ un lenguaje de primer orden sin símbolos lógicos. Para cada $n > 1$, sea A_n la fórmula

$$\exists x_0 \cdots \exists x_{n-1} \wedge_{0 \leq i < j < n} \neg (x_i = x_j).$$

Suponiendo que T es la teoría cuyo lenguaje es $\mathcal{L}$ y cuyos axiomas son $A_2, A_3, ...$ Entonces los modelos de T son precisamente los conjuntos infinitos.

Ejemplo 1.30. El conjunto de todos los números naturales

$$\mathbb{N} = \{0, 1, ...\}$$

con el significado usual de S (función sucesora), $+$, $.$, y $<$ es un modelo de la teoría N y también de la aritmética de Peano.

Capítulo 2

Teoría de conjuntos.

2.1. Axiomas de Zermelo – Fraenkel.

En esta sección presentamos una lista de axiomas debidos esencialmente a E. Zermelo y dados a conocer en 1908, con modificaciones sugeridas por T. Skolem y A. Fraenkel en 1922. El sistema determinado por los axiomas que se indican, es denotado con **ZF**. Antes de ello, debemos indicar que los axiomas de la teoría de conjuntos no contienen definición alguna de "conjunto" o "pertenece a". Estos son únicamente conceptos no definidos, cuyas propiedades son expresadas por los axiomas.

(ZF1) **Axioma de extensión**. Dos conjuntos son iguales, si ellos tienen los mismos elementos:

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

Este principio expresa la propiedad fundamental de que un conjunto es determinado por sus elementos.

A partir de ello, podemos introducir la siguiente

Definición 2.1. $\forall x \forall y$, *x es subconjunto de y*, si $\forall z(z \in x \to z \in y)$. Denotamos ello con $x \subseteq y$.

Así, el axioma de extensión puede ser reescrito como:

$$\forall x \forall y(x = y \leftrightarrow x \subseteq y \wedge y \subseteq x).$$

(ZF2) **Axioma de existencia del conjunto vacío**. Existe un conjunto carente de elementos:

$$\exists x \forall z(\neg(z \in x)).$$

Notación: $x = \varnothing$.

(ZF3) **Axioma de apareamiento**. Dados dos conjuntos x y y, existe un conjunto z que los contiene:

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

Notación: $z = \{x, y\}$. Además, a partir de este axioma y de la notación indicada, se pueden formar conjuntos unitarios, los cuales denotamos con $z = \{x\}$(es suficiente considerar $x = y$).

(ZF4) **Axioma de unión**. Dado cualquier conjunto x, existe un conjunto y que contiene a todos aquellos z que pertenecen a algún miembro de x:

$$\forall x \exists y \forall z \forall u(u \in x \wedge z \in u \to z \in y).$$

Notación. $y = \bigcup x = \{z : z \in u \text{ para algún } u \in x\}$. Por otra parte, dados dos conjuntos x y y, $x \cup y$ consta de todos los elementos de x, junto con todos los elementos de y. De este modo, primero se define el conjunto $\{x, y\}$, de acuerdo con el axioma 3 de **ZF** y apartir de ello se forma $\bigcup\{x, y\}$. Por lo tanto, el axioma de apareamiento y de unión garantizan que la unión de dos conjuntos puede formarse.

Definición 2.2. Dados dos conjuntos x y y, $x \cup y$ significa $\bigcup\{x, y\}$.

(ZF5) **Axioma de conjunto potencia**. Dado cualquier conjunto x, existe un conjunto y que contiene todos los subconjuntos z de x:

$$\forall x \exists y \forall z (\forall u (u \in z \to u \in x) \to z \in y).$$

Notación: $y = \boldsymbol{P}(x)$.

(ZF6) **Axioma de separación**. Para cada fórmula $\varphi[x, w_1, ..., w_n]$,

$$\forall z \forall w_1 \cdots \forall w_n (\exists y \forall x (x \in y \leftrightarrow x \in z \wedge \varphi))$$

es un axioma. Este axioma dice que dada cualquier "propiedad de conjuntos" expresada por una fórmula $\varphi[x, w_1, ..., w_n]$, para cualquier parámetro $w_1, ..., w_n$ y para cada conjunto z, existe un conjunto y que contiene precisamente aquellos $x \in z$ que satisfacen $\varphi[x, w_1, ..., w_n]$. Es importante observar que este axioma no es un solo axioma. Es un esquema axiomático, es decir existen infinitos axiomas para cada fórmula $\varphi[x, w_1, ..., w_n]$. A partir de este axioma, tenemos la

Definición 2.3. Sean x y y dos conjuntos, se define la intersección

$$x \cap y = \{z \in x : z \in y\}.$$

(ZF7) **Axioma de reemplazo**. Para cada fórmula $\varphi[x, y, z, u_1, ..., u_n]$,

$$\forall z \forall u_1 \cdots \forall u_n (\forall x \in z \exists! y \varphi \to \exists v \forall x (x \in z \to \exists y (y \in v \wedge \varphi)))$$

es un axioma, donde $\exists! y \varphi$ es la abreviación de la fórmula

$$\varphi \wedge \forall u (\varphi_y[u] \to u = y).$$

Este axioma, nos dice que la imagen de una "función" sobre un conjunto z, que es definido por una fórmula φ, es un conjunto.

(ZF8) **Axioma de infinitud**. Existe un conjunto que es infinito:

$$\exists z (\exists w (\forall y (y \notin w) \wedge w \in z) \wedge \forall x (x \in z \to \exists y (\forall w (w \in y \leftrightarrow (w \in x \vee w = x)) \wedge y \in z))),$$

donde $(y \notin w)$ es la abreviación de la fórmula $\neg(y \in w)$.

Este axioma no hace más que garantizar la existencia de un conjunto que es infinito.

Una versión relativamente intuitiva del axioma es:

"Existe un conjunto x tal que $\varnothing \in x$, y tal que para cada conjunto $u \in x$, también se tiene $u \cup \{u\} \in x$.

(ZF9) **Axioma de fundación**.

$$\forall x (\exists y (y \in x) \to \exists y (y \in x \wedge \neg \exists z (z \in x \wedge z \in y))).$$

Este axioma implica la imposibilidad de tener $x \in x$.

2.1.1. Matemáticas en ZF

Definición 2.4. Dados dos conjuntos x y y, el conjunto $\{\{x\}, \{x, y\}\}$ es llamado *par ordenado* de x y y , además, es denotado por (x, y).

La definición de par ordenado puede ser extendida inductivamente a triples ordenados, cuádruples ordenados, etc.

Definición 2.5.

(i) (x, y, z) denota $((x, y), z)$ para x, y, z conjuntos.

(ii) Para cada número natural n, si $x_1, \cdots, x_{n+1}$ son conjuntos, definimos $(x_1, \cdots, x_{n+1})$ como $((x_1, \cdots, x_n), x_{n+1})$.

El producto cartesiano de dos conjuntos, x y y, sabemos que está constituido por el conjunto de todos los pares ordenados (a, b) con $a \in x$ y $b \in y$. Para adaptar esto en **ZF** usamos el axioma de separación para construir $x \times y$. Si $a \in x$ y $b \in y$, entonces, como $(a, b) = \{\{a\}, \{a, b\}\}$ es un subconjunto de $\boldsymbol{P}(\{a, b\})$, y $\{a, b\}$ es un subconjunto de $x \cup y$, tenemos $(a, b) \subseteq \boldsymbol{P}(x \cup y)$, y de este modo $(a, b) \in \boldsymbol{P}(\boldsymbol{P}(x \cup y))$.

Definición 2.6. Dados dos conjuntos x y y, el *producto cartesiano de* x y y es dado por

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

Esta definición puede ser extendida inductivamente para un producto cartesiano arbitrariamente finito: para cada número natural n, si $x_1, \cdots, x_{n+1}$ son conjuntos, entonces $x_1 \times \cdots \times x_{n+1} = (x_1 \times \cdots \times x_n) \times x_{n+1}$.

Definición 2.7.

(i) Una *relación binaria* es un subconjunto del producto cartesiano de dos conjuntos. Esto es: $\exists x \exists y (z \subseteq x \times y)$ significa que z es una relación binaria. Asimismo, puede definirse una relación n-aria para cada número natural n. Una relación binaria en un conjunto x es un subconjunto de $x \times x$.

(ii) El *dominio* de una relación binaria z es el conjunto de los primeros elementos de los pares ordenados en z. Esto es, el conjunto $\{x \in \bigcup(\bigcup z) : \exists y\,((x,y) \in z)\}$. La *imagen* de z es definida como el conjunto formado por las segundas componentes de los pares ordenados de z.

Un tipo de relación de particular importancia es dada en la siguiente

Definición 2.8. *f es una función* y puede ser expresada – en el contexto de **ZF** – por:

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

Por otra parte, se puede establecer el conjunto de todas las funciones de un conjunto a otro. Este puede ser construido en **ZF** aplicando el axioma de separación. Si x y y son conjuntos y f es cualquier función cuyo dominio es x y cuya imagen es un subconjunto de y, entonces f es un subconjunto de $x \times y$, es decir $f \in \boldsymbol{P}(x \times y)$. Así, el conjunto de todas las funciones de x en y es

$$\begin{aligned} \{f \in \boldsymbol{P}(x \times y) \quad &: \quad \forall u(u \in x \rightarrow \exists v(v \in y \wedge (u,v) \in f) \\ &\wedge \quad \forall u \forall v \forall w(((u,v) \in f \wedge (u,w) \in f) \rightarrow (u = w)))\}. \end{aligned}$$

Usando la noción de función, definimos la colección indexada de conjuntos (familia) en el sistema **ZF** por medio de la

Definición 2.9. Una *familia de conjuntos* es una función F que parte de un conjunto de índices I hacia algún conjunto donde la función toma valores. Intuitivamente $\{F(i) : i \in I\}$ denota una familia de conjuntos.

Por otra parte, debe observarse que una familia de conjuntos es distinta a un conjunto de conjuntos, puesto que un conjunto puede ser repetido en una familia, pero puede contarse solamente como un elemento de un conjunto. Por ejemplo, la función F de $\mathbb{N}$ a $\boldsymbol{P}(\mathbb{R})$, tal que $F(n) = \mathbb{R}$, para cada $n \in \mathbb{N}$, es una familia, pero $\{F(n) : n \in \mathbb{N}\}$ como un conjunto tiene precisamente un elemento: $\mathbb{R}$

A continuación establecemos otra definición importante en matemáticas:

Definición 2.10. Una relación z en x se denomina *relación de equivalencia* , si

$$\begin{aligned}(z \subseteq x \times x) \quad &\wedge \quad \forall u(u \in x \to (u,u) \in z)\\ &\wedge \quad \forall u \forall v((u,v) \in z \to (v,u) \in z)\\ &\wedge \quad \forall u \forall v \forall w(((u,v) \in z \wedge (v,w) \in z) \to (u,w) \in z),\end{aligned}$$

es decir z es una relación binaria en x que es reflexiva, simétrica y transitiva.

Finalizamos esta sección con la definición de *relación de orden.*

Definición 2.11. Una relación z en x se denomina *relación de orden*, si

$$\begin{aligned}(z \subseteq x \times x) \quad &\wedge \quad \forall u(u \in x \to (u,u) \in z)\\ &\wedge \quad \forall u \forall v((u,v) \in z \wedge (v,u) \in z \to (u = v))\\ &\wedge \quad \forall u \forall v \forall w(((u,v) \in z \wedge (v,w) \in z) \to (u,w) \in z),\end{aligned}$$

es decir, z es una relación binaria en x que es reflexiva, antisimétrica y transitiva.

2.2. Axiomas de Zermelo – Fraenkel y el Axioma de Elección.

2.2.1. El axioma de elección (AE)

El axioma de elección asegura la existencia de ciertos conjuntos sin la necesidad de dar una descripción sobre ellos. Intuitivamente, este dice que si tenemos un conjunto que consiste solamente de conjuntos no vacíos, entonces existe una función la cual toma un elemento de cada uno esos conjuntos no vacíos sin proporcionar una descripción "definida" de tal función.

Otra versión del axioma de elección es aquella que considerando una colección de conjuntos no vacíos y disjuntos "dos a dos", garantiza la existencia de un conjunto, de modo que tal conjunto interceptado con cualquier conjunto de la colección, presenta cardinal uno.

De este modo, tenemos el

Axioma de elección (AE).

Sea $X \neq \varnothing$ un conjunto tal que

$$\forall x(x \in X \to x \neq \varnothing) \wedge \forall x \forall y(\{x, y\} \subseteq X \wedge x \neq y \to x \cap y = \varnothing),$$

entonces,

$$\exists z : \operatorname{card}(z \cap x) = 1, \forall x \in X.$$

Antes de enunciar el axioma de elección en una versión que involucra la existencia de funciones de elección, introducimos la noción de producto cartesiano de una familia infinita de conjuntos.

Definición 2.12. El producto cartesiano de una familia F (con índices en un conjunto I) es el conjunto de todas las funciones f de I hacia la unión de todos los conjuntos $F(i)$ con $i \in I$.

Notación: $\prod_{i \in I} F(i)$.

Observar que los elementos del producto cartesiano $\prod_{i \in I} F(i)$ son *funciones de elección*, es decir, funciones de la forma

$$f : I \to \bigcup_{i \in I} F(i),$$

con $f(i) = f_i \in F(i)$, para cada $i \in I$.

Notación: $(f(i))_{i \in I}$.

A partir de ello, tenemos una segunda versión del axioma:

Axioma de elección (AE$'$).

Para cada familia $(F(i))_{i \in I}$ de conjuntos no vacíos $F(i)$, el producto cartesiano de la familia $\prod_{i \in I} F(i)$ es no vacío.

Comentario 2.1. El axioma de elección, formulado por Zermelo en 1904, es un axioma no constructivo, es decir, este axioma asegura la **existencia** de un conjunto (función de elección) sin definirlo, a diferencia de los otros axiomas de **ZF** (por citar el axioma de apareamiento o el axioma del conjunto potencia). Sin embargo, en algunos casos particulares, la existencia de una función de elección puede ser probada en **ZF**, como por ejemplo, si la familia F está constituida por conjuntos de la forma $\{a, b\}$, siendo a y b números reales. En este caso, la función $f(\{a, b\}) = min(a, b)$, es una función de elección en F. También puede construirse una función de elección para una familia cuyos conjuntos son unitarios (para ello basta con *elegir* el único elemento de cada conjunto). Además, si F es una familia finita de conjuntos no vacíos, puede demostrarse la existencia de una función de elección usando inducción sobre la cardinalidad de F.

Así, la idea de elegir una función de elección en cada familia de conjuntos no vacíos no es contraria al pensamiento matemático. Sin embargo, pretender construir una función de elección sobre la familia de todos los subconjuntos no vacíos de números reales, no parece ser "claro". Este es un tipo de objeción que se le puede plantear al axioma de elección puesto que – como veremos más adelante – el uso del axioma de elección permitirá establecer que $\mathbb{R}$ (conjunto de números reales) es bien ordenado.

A continuación establecemos la equivalencia de ambas versiones del axioma de elección.

Teorema 2.1. *(AE) es equivalente a (AE′)*

Prueba.

Primero probamos que (AE′) implica (AE).

En efecto, sea $X \neq \varnothing$ un conjunto tal que

$$\forall x(x \in X \to x \neq \varnothing) \wedge \forall x \forall y(\{x, y\} \subseteq X \wedge x \neq y \to x \cap y = \varnothing).$$

Entonces, por (AE′), existe una función f con $Dom(f) = X$ y $f(x) \in x$, $\forall x \in X$, es decir

$$\begin{aligned} f: \quad X &\longrightarrow Im(f) \\ x &\longmapsto f(x) \in x. \end{aligned}$$

Definiendo $z := Im(f)$, entonces $\text{card}(z \cap x) = 1, \forall x \in X$, dado que f es una función.

Ahora probamos que (AE) implica (AE′).

Sea $X \neq \varnothing$, tal que $\forall x \in X, x \neq \varnothing$. Consideremos el conjunto $T := \{\{x\} \times x \,:\, x \in X\}$. A partir de ello, tenemos

- $T \neq \varnothing$ (porque $X \neq \varnothing$).

- Todo elemento de T es no vacío (porque $\forall x \in X, x \neq \varnothing$).

- Dos a dos, los elementos de T son disjuntos (porque si $x_1, x_2 \in X, x_1 \neq x_2$ es tal que $(\{x_1\} \times x_1) \cap (\{x_2\} \times x_2) \neq \varnothing$, entonces existe un par ordenado (a, b) en ambos productos, con lo cual concluiríamos que $a = x_1 = x_2$ siendo esto una contradicción).

Luego, el conjunto T satisface las hipótesis de (AE). Por lo tanto

$$\exists z : \operatorname{card}(z \cap u) = 1, \ \forall u \in T.$$

Así, si $u \in T$, entonces $u = (x, s)$con $x \in X \wedge s \in x$. Por lo tanto,

$$z = \{(x, s) : \ x \in X \wedge s \in x\}$$

es una función, porque $\operatorname{card}(z \cap u) = 1$ garantiza la veracidad de la implicación

$$\text{si } \ \underbrace{(x, s')}_{\in u} \wedge \underbrace{(x, s'')}_{\in u} \in z, \ \text{ entonces } \ s' = s''.$$

Por lo tanto,

$$\exists z \ \text{ función } : \ \ z(x) = s \in x, \forall x \in X.$$

■

En las dos subsecciones siguientes enunciamos el Lema de Zorn y el Principio del buen orden, siendo posiblemente el Lema de Zorn uno de los axiomas más utilizados en matemáticas (axioma – pues como veremos al finalizar el presente capítulo – es equivalente tanto al axioma de elección como al Principio del buen orden.)

2.2.2. El Lema de Zorn.

Antes de enunciar el Lema de Zorn, estableceremos algunas definiciones relacionadas con los conjuntos ordenados y las relaciones de orden.

Definición 2.13. Un *orden* $\mathcal{R}$ en X es cualquier relación binaria $\mathcal{R}$ en X tal que $\mathcal{R}$ es reflexiva, antisimétrica y transitiva. (Ver Definición 2.11)

Notación: $(X, \mathcal{R})$.

Si $Y \subseteq X$ y $\mathcal{R}$ es un orden en X, la *restricción* de $\mathcal{R}$ a Y será denotada por $\mathcal{R}|_Y$.

Definición 2.14. Sea $(X, \mathcal{R})$ un conjunto ordenado, y $a \in X$. Decimos que a es

- **mínimo**, si $\forall x \in X,\ a\mathcal{R}x$;
- **máximo**, si $\forall x \in X,\ x\mathcal{R}a$;
- **minimal**, si $\forall x \in X \ \wedge \ x\mathcal{R}a \ \rightarrow \ x = a$;
- **maximal**, si $\forall x \in X \ \wedge \ a\mathcal{R}x \ \rightarrow \ a = x$.

Definición 2.15. Un orden $\mathcal{R}$ en X es un *orden total*, si

$$\forall x, x' \in X, \ \ x\mathcal{R}x' \ \vee \ x'\mathcal{R}x.$$

En este caso, decimos que $(X, \mathcal{R})$ es totalmente ordenado.

Definición 2.16. Una *cadena* en $(X, \mathcal{R})$ es cualquier subconjunto Y de X tal que $(Y, \mathcal{R}|_Y)$ es totalmente ordenado.

Definición 2.17. Sea $(X, \mathcal{R})$ un conjunto totalmente ordenado. Decimos que $\mathcal{R}$ es un *buen orden* en X, si todo subconjunto no vacío de X contiene un mínimo, es decir

$$\forall\, Y \subseteq X, \ \ Y \neq \varnothing \ \rightarrow \ \exists a \in Y : \ \forall y \in Y, \ a\mathcal{R}y.$$

En este caso, decimos simplemente que el conjunto X es bien ordenado.

Definición 2.18. Sea X un conjunto bien ordenado por la relación $\mathcal{R}$. El *segmento inicial* de X determinado por un elemento $a \in X$ es el conjunto

$$X_a := \{y \in X : \; y\mathcal{R}a \;\; \wedge \;\; y \neq a\}.$$

Además, si consideramos la restricción de $\mathcal{R}$ a X_a, $\mathcal{R}|_{X_a}$, el conjunto X_a es bien ordenado.

Lema de Zorn (LZ).

Si X es un conjunto no vacío y ordenado, de modo tal que toda cadena en X tiene una cota superior, entonces X posee un elemento maximal.

Existe un principio, aparentemente débil, que es equivalente al Lema de Zorn:

Lema de Zorn (LZ$_-$).

Si X es un conjunto no vacío y ordenado, de modo que toda cadena en X tiene un supremo en X, entonces X posee un elemento maximal.

A continuación, establecemos el

Teorema 2.2. *(LZ) es equivalente a (LZ$_-$)*

Prueba.

La proposición (LZ) implica (LZ$_-$) es clara, pues al considerar $(X, \mathcal{R})$ ordenado y que toda cadena en X tiene un supremo, estamos garantizando que toda cadena posee una cota superior (porque el supremo es una cota superior de la cadena). De este modo, se satisfacen las hipótesis de (LZ), con lo cual la existencia de un elemento maximal para X está asegurada.

Por otra parte, para demostrar que (LZ$_-$) implica (LZ), consideremos un conjunto X ordenado por la relación $\mathcal{R}$: $(X, \mathcal{R})$, de modo tal que toda cadena en X tiene una cota superior en X. Denotemos con $\mathscr{H}$ al conjunto de todas las cadenas en X. Ciertamente $\mathscr{H}$ es ordenado por la inclusión. Sea $\mathscr{C}$ una cadena en $\mathscr{H}$.

Afirmación. $\bigcup \mathscr{C}$ es una cadena en X, es decir $\bigcup \mathscr{C} \in \mathscr{H}$.

En efecto, sean a, $b \in \bigcup \mathscr{C}$. Entonces $a \in C_1$ y $b \in C_2$ para algún $C_1 \in \mathscr{C}, C_2 \in \mathscr{C}$. Puesto que $\mathscr{C}$ es una cadena, se tiene $C_1 \subseteq C_2$ o $C_2 \subseteq C_1$. Sin pérdida de generalidad podemos suponer que $C_1 \subseteq C_2$, con lo cual a, $b \in C_2$ y, siendo C_2 una cadena en X, se tiene $a\mathcal{R}b$ o $b\mathcal{R}a$.

Tras probar la afirmación, se concluye que la cadena $\mathscr{C}$ tiene una cota superior en $\mathscr{H}$. Es más, $\bigcup \mathscr{C}$ no es simplemente una cota superior de $\mathscr{C}$, sino que es la menor cota superior (porque $\bigcup \mathscr{C}$ es el menor conjunto que contiene como subconjuntos todos los elementos de $\mathscr{C}$). Por lo tanto – por hipótesis – es posible aplicar(LZ$_-$) a $\mathscr{H}$. Sea C_0 un elemento maximal de $\mathscr{H}$. Entonces C_0 es una cadena en X y – en consecuencia – tiene una cota superior u en X.

Afirmación. u es un elemento maximal de X.

En efecto, si suponemos que existe $x \in X$ con $u\mathcal{R}x$ y $u \neq x$, entonces $C_0 \cup \{x\}$ sería una cadena en X conteniendo estrictamente a C_0, lo cual contradice la maximalidad de C_0.

Por lo tanto, se ha demostrado que X posee un elemento maximal, lo cual culmina la prueba del teorema.

■

2.2.3. El Teorema del buen orden

Dado cualquier conjunto X, existe una relación binaria $\mathcal{R}$ en X de modo que $(X, \mathcal{R})$ es un conjunto bien ordenado.

2.2.4. Equivalencia clásica de principios

Teorema 2.3. *Los siguientes principios son equivalentes:*

(AE) *El Axioma de Elección.*

(LZ) *El Lema de Zorn.*

(BO) *El Teorema del buen orden.*

Prueba.

La estrategia que seguiremos para la demostración del teorema será la cadena de implicaciones:

(a) (BO) $\longrightarrow$ (AE)

(b) (LZ) $\longrightarrow$ (BO)

(c) (AE) $\longrightarrow$ (LZ$_-$)

Empezamos con la prueba de la primera implicación.

(a) (BO) $\longrightarrow$ (AE)

Sea $X \neq \varnothing$ cualquier colección de conjuntos, de modo que para todo x en X , $x \neq \varnothing$. Consideremos la unión de todos los conjuntos de la colección, $\bigcup X$. Además, para cada $x \in X$, $x \subseteq \bigcup X$. Por el Teorema del buen orden, existe una relación $\mathcal{R}$ tal que $(X, \bigcup X)$ es un conjunto bien ordenado. Por lo tanto, para todo $x \in X$, existe un único mínimo. De este modo, definimos la función

$$f(x) := \min x \in x, \ \ \forall x \in X.$$

Luego, concluimos que existe f función tal que $Dom(f) = X$ y $f(x) \in x, \forall x \in X$.

(b) (LZ) $\longrightarrow$ (BO)

Dado cualquier conjunto X, debemos demostrar que existe una relación de orden sobre X de modo que tal relación sea un buen orden. Sea W la colección de todos los subconjuntos de X bien ordenados, es decir

$$W = \{(A, \mathcal{R}) : \; A \subseteq X \; \wedge \; \mathcal{R} \text{ es un buen orden en } A\}.$$

Dotamos a W con la siguiente relación de orden: $(A, \mathcal{R}) \preccurlyeq (B, \mathcal{S})$ si $A \subseteq B$, $\mathcal{R} = \mathcal{S}|_A$, y $\mathcal{S}$ es tal que cada elemento de A precede cada elemento de $B \backslash A$. Esto puede ser expresado diciendo que A es un segmento inicial de B. De esta manera, puede verificarse que $(W, \preccurlyeq)$ es un conjunto ordenado.

Para aplicar el Lema de Zorn debemos mostrar que toda cadena en W tiene una cota superior en W. Sea $\mathscr{C}$ una cadena en W. La unión de los conjuntos en $\mathscr{C}$ proporcionará la cota superior buscada, pero se requiere verificar que este sea bien ordenado. En efecto, si a y b pertenecen a la unión , entonces existen $(C_1, \mathcal{R}_1)$ y $(C_2, \mathcal{R}_2)$ en $\mathscr{C}$ con $a \in C_1$ y $b \in C_2$. Sin pérdida de generalidad podemos suponer que $(C_1, \mathcal{R}_1) \preccurlyeq (C_2, \mathcal{R}_2)$, de modo que $C_1 \subseteq C_2$ y C_2 contiene tanto a a como a b. Así, a y b están relacionados bajo $\mathcal{R}_2$.

Por otra parte, decimos que $a\mathcal{R}b$ si $a\mathcal{R}_2b$. Que este proceso está bien definido, producirá un orden $\mathcal{R}$ en la unión de los conjuntos en $\mathscr{C}$. Que $\mathcal{R}$ es un buen orden, y que esta unión, ordenada por $\mathcal{R}$, es una cota superior para $\mathscr{C}$ se logran verificar. El Lema de Zorn asegura la existencia de un elemento maximal $(M, \mathcal{R}_0)$, digamos, en W. Así, deberá tenerse que $M = X$, caso contrario podemos elegir $x \in X \backslash M$ dotar de un buen orden a $M \cup \{x\}$ por la relación $\mathcal{R}_0'$, siendo $\mathcal{R}_0' = \mathcal{R}_0 \cup \{(a, x) \; : \; a \in M \cup \{x\}\}$.

La consecuencia de este hecho, es que cada elemento de M precede x en el orden $\mathcal{R}_0'$. Entonces $(M \cup \{x\}, \mathcal{R}_0')$ pertenece a W, y extiende $(M, \mathcal{R}_0)$, hecho que contradice la maximalidad de $(M, \mathcal{R}_0)$. De este modo, $X = M$, y $\mathcal{R}_0$ es un buen orden de X, tal como se requería.

(c) (AE) $\longrightarrow$ (LZ$_-$)

Sea$(X, \mathcal{R})$ un conjunto ordenado no vacío, tal que toda cadena en X tiene supremo en X. Para cualquier $x \in X$, definimos (garantizado por el axioma de separación)

$$S(x) := \{y \in X : \ x\mathcal{R}y \ \wedge \ x \neq y\}.$$

De esta manera, se presentan dos opciones:$(\exists x, S(x) = \varnothing) \vee (\forall x, S(x) \neq \varnothing)$, con lo cual tenemos

Afirmación 1. $(\exists x, S(x) = \varnothing) \leftrightarrow x$ es un elemento maximal en X.

Supongamos que x no es un elemento maximal en X. Entonces existe $y_0 \in X$, tal que $x\mathcal{R}y_0 \wedge x \neq y_0$, con lo cual se concluye que $y_0 \in S(x)$ contrario al supuesto: $S(x) \neq \varnothing$. Recíprocamente, si $S(x) \neq \varnothing$, entonces existe $y_0 \in X$ tal que $x\mathcal{R}y_0 \wedge x \neq y_0$, contradiciendo la maximalidad de x en X.

Afirmación 2. $\neg(\forall x \in X, S(x) \neq \varnothing)$.

En efecto, supongamos que $(\forall x \in X, S(x) \neq \varnothing)$. Consideremos el conjunto (por el axioma de separación aplicado a $\boldsymbol{P}$(X))

$$\mathscr{C} := \{S(x) \in \boldsymbol{P}(X) : \ x \in X\}.$$

De este modo, $\mathscr{C} \neq \varnothing \wedge S(x) \neq \varnothing, \forall x \in X$. Bajo estas condiciones, es posible aplicar el axioma de elección (AC') al conjunto $\mathscr{C}$. Así, existe una función selectora F tal que

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

Por otra parte, definimos la función

$$\begin{aligned} f : X &\longrightarrow X \\ x &\longmapsto f(x) := F(S(x)). \end{aligned}$$

De este modo, tenemos

$$\forall x (x \in X \rightarrow x\mathcal{R}f(x) \wedge x \neq f(x)),$$

(por definición de f: $\forall x, f(x) = F(S(x))$ y por definición de $S(x)$, $x\mathcal{R}f(x) \wedge x \neq f(x)$).

Fijemos un elemento a en X y consideremos la colección $\mathscr{H}_a$, de todos los subconjuntos B de X que satisfacen las condiciones:

1. $a \in B$.
2. Si $x \in B$, entonces $a\mathcal{R}x$.
3. Si $x \in B$, entonces $f(x) \in B$.
4. Para cada $C \subseteq B$, que es una cadena en X, el supremo de C está en B.

A continuación, aseveramos que $\mathscr{H}_a \neq \varnothing$. Para ello, consideremos el conjunto

$$B = \{x \in X : \ a\mathcal{R}x\}$$

y debemos mostrar que $B \in \mathscr{H}_a$, verificando las condiciones $1 - 4$. En efecto:

Condición 1: $a \in B$, porque $a\mathcal{R}a$.

Condición 2: $x \in B$ implica $a\mathcal{R}a$, por la definición de B.

Condición 3: Si $x \in B$, entonces $a\mathcal{R}x \wedge x\mathcal{R}f(x)$ (por definición de f). Luego, por transitividad, $a\mathcal{R}f(x)$, así $f(x) \in B$.

Condición 4: Sea $C \subseteq B$ una cadena en X, entonces existe $c_0 := \sup C$ (recordemos que, por hipótesis, toda cadena admite un supremo). Luego, $\forall c \in C$, $c\,\mathcal{R}c_0$, y como $c \in B$, se tiene que $\forall c \in C, c\,\mathcal{R}c_0 \wedge a\mathcal{R}c$. La transitividad de $\mathcal{R}$ permite concluir que $c_0 \in B$.

Continuando con la prueba de la afirmación, definimos

$$A := \bigcap \mathscr{H}_a.$$

Debemos mostrar que $A \in \mathscr{H}_a$, verificando las condiciones $1-4$:

Condición 1: $\forall B \in \mathscr{H}_a$, $a \in B \to a \in A$.

Condición 2: Como $x \in A \to x \in B$, $\forall B \in \mathscr{H}_a$, entonces $a\mathcal{R}x$, $\forall B \in \mathscr{H}_a$. Luego, $a\mathcal{R}x$, $\forall x \in A$.

Condición 3: Como $x \in A \to x \in B$, $\forall B \in \mathscr{H}_a$, entonces $f(x) \in B, \forall B \in \mathscr{H}_a$, de modo que $f(x) \in B, \forall x \in A$.

Condición 4: Si $C \subseteq A$ es una cadena en X tal que $c_0 := \sup C$, y como $C \subseteq A = \bigcap \mathscr{H}_a$, se tiene $C \subseteq B, \forall B \in \mathscr{H}_a$, y siendo $c_0 := \sup C$, entonces $c_0 \in B, \forall B \in \mathscr{H}_a$. Por lo tanto, $c_0 \in A$.

Por otra parte, afirmamos que **A es una cadena en X**[1]. En consecuencia, existe $a_0 \in X$, tal que $a_0 = \sup A$. Además, $a_0 \in A$, porque $A \in \mathscr{H}_a$ y A es una cadena en X que cumple con la condición 2. Por lo tanto, $f(a_0) \in A$ y $f(a_0)\mathcal{R}a_0$, y, por definición de f, se concluye que $f(a_0) = a_0$. Sin embargo, la conclusión que acabamos de obtener

[1] La prueba detallada de tal afirmación, se presenta al final de este capítulo.

es una **contradicción**, puesto que f satisface la condición:

$$\forall x \in X,\ x\mathcal{R}f(x)\ \wedge\ x \neq f(x).$$

Finalmente, se concluye que existe $x \in X$ tal que $S(x) \neq \varnothing$, es decir, existe x que es un elemento maximal en X.

$\blacksquare$

Afirmación: A *es una cadena en* X.

(Viene de la demostración del teorema 2.3c, afirmación 2)

Prueba

Considerando el axioma de separación aplicado al conjunto A, definimos

$$A^* := \{x \in A :\ y \in A\ \wedge\ y\mathcal{R}x\ \wedge\ y \neq x\ \ \rightarrow\ \ f(y)\mathcal{R}x\}.$$

Además, para cada $b \in A^*$, se define

$$A_b := \{x \in A :\ x\mathcal{R}b\ \vee\ f(b)\mathcal{R}x\}.$$

A partir de ello, mostraremos dos resultados:

- $$\forall b \in A^*,\ A_b \in \mathscr{H}_a\ \ \wedge\ \ A_b = A.$$

  En efecto, para mostrar que $A_b \in \mathscr{H}_a$, se deben verificar las condiciones $1-4$.

  Condición 1: Como $b \in A^*$ y $A \subseteq A$, se tendrá que $b \in A$. Dado que $A \in \mathscr{H}_a$ y cumple con la condición 2, $a\mathcal{R}b$. De este modo, $a \in A_b$.

  Condición 2: Sea $x \in A_b$, entonces $x \in A$ y $A \in \mathscr{H}_a$. Así, $a\mathcal{R}x$ (por la condición 2 cumplida por A).

  Condición 3: Sea $x \in A_b$, entonces $x \in A$, tal que $x\mathcal{R}b \vee f(b)\mathcal{R}x$. Además, $x\mathcal{R}f(x)$ (por definición de f). A partir de ello, se tienen los siguientes casos:

- Si $x\mathcal{R}b \wedge x = b$, entonces $f(x) = f(b)$, con lo cual $f(b)\mathcal{R}f(x)$.
- Si $x\mathcal{R}b \wedge x \neq b$, entonces como $b \in A^*$, $f(x)\mathcal{R}b$.
- Si $f(b)\mathcal{R}x \wedge x\mathcal{R}f(x)$, entonces $f(b)\mathcal{R}f(x)$.

Se observa que en cualquiera de los casos, $f(x) \in A_b$.

Condición 4: Sea C una cadena en $A_b \subseteq A$. Entonces C es una cadena en A y por tanto, existe $c_0 := \sup C$. Siendo $A \in \mathscr{H}_a$, se cumple la condición 4, con lo cual, $c_0 \in A$. Además, $C \subseteq A_b$ implica dos condiciones

$$(x\mathcal{R}b,\ \forall x \in C) \qquad \vee \qquad (\exists c \in C : f(b)\mathcal{R}c),\ \text{ lo cual implica,}$$

$$\sup C = c_0\mathcal{R}b \qquad \vee \qquad f(b)\mathcal{R}c_0.$$

En ambos casos, $c_o \in A_b$. Por lo tanto, $A_b \in \mathscr{H}_a$.

Por otra parte, por definición de A_b, $A_b \subseteq A$ y como $A_b \in \mathscr{H}_a$, entonces $A \subseteq A_b$, con lo cual se concluye que $A = A_b$.

- $$A^* \in \mathscr{H}_a \ \wedge \ A^* = A.$$

Para que $A^* \in \mathscr{H}_a$, como en el caso anterior, debemos verificar las condiciones $1 - 4$.

Condición 1: $\forall x \in A, a\mathcal{R}x$ $(A \in \mathscr{H}_a)$. Además, la siguiente implicación es verdadera:

$$y \in A \ \wedge \ y\mathcal{R}a \ \wedge \ y \neq a \ \longrightarrow \ f(y)\mathcal{R}x$$

$$a\mathcal{R}y \ \wedge \ y\mathcal{R}a \ \wedge \ y \neq a$$

pues las dos primeras conjunciones implican $y = a$, que junto con la tercera, $y \neq a$ permiten establecer la falsedad del antecedente. En consecuencia, $a \in A^*$.

Condición 2: Sea $x \in A^*$. Como $A \subseteq A$ y $A \in \mathscr{H}_a$, entonces $a\mathscr{R}x$.

Condición 3: Si $x \in A^*$, entonces $A = A_x$ (por el primer resultado obtenido). Luego,

$\forall y \in A$, se tiene que $y\mathcal{R}x \vee f(x)\mathcal{R}y$. Por otra parte, sea $y \in A \wedge y\mathcal{R}f(x) \wedge y \neq f(x)$. Debemos probar que $f(y)\mathcal{R}f(x)$. En efecto,

- Si $f(x)\mathcal{R}y \wedge y\mathcal{R}f(x)$, entonces $y = f(x)$, lo cual es una contradicción. Por lo tanto, la única posibilidad es $y\mathcal{R}x$.

  Luego,

- Si $y\mathcal{R}x \wedge y = x$, entonces $f(y) = f(x)$, con lo cual se tiene $f(y)\mathcal{R}f(x)$.

- Si $y\mathcal{R}x \wedge y \neq x$, por hipótesis $x \in A^*$, es decir:

$$y \in A \wedge y\mathcal{R}x \wedge y \neq x \longrightarrow f(y)\mathcal{R}.$$

  Así, $f(y)\mathcal{R}x$; además, por definición de f, $x\mathcal{R}f(x)$. Por lo tanto, $f(y)\mathcal{R}f(x)$, es decir $f(x) \in A^*$.

Condición 4: Sea C una cadena en $A^* \subseteq A$. Entonces C es una cadena en A. Luego, si $c_0 := \sup C$, entonces $c_0 \in A$ (porque $A \in \mathscr{H}_a$ y cumple con 4). Sea $y \in A \wedge y\mathcal{R}c_0 \wedge y \neq c_0$. Debemos probar que $f(y)\mathcal{R}c_0$. Como para cada $b \in A^*, A_b = A$ (por el primer resultado obtenido). Entonces, $\forall c \in C, A_c = A$ (porque $C \subseteq A^*$). Así, $y \in A_c, \forall c \in C$, con lo cual $y\mathcal{R}c \vee f(c)\mathcal{R}y, \forall c \in C$. De aquí se tiene

$$(\exists c_1 : y\mathcal{R}c_1) \vee (f(c)\mathcal{R}y, \forall c \in C)$$

- Si $f(c)\mathcal{R}y$, $\forall c \in C$, entonces $c\mathcal{R}y, \forall c \in C$. De aquí se desprende que $c_0\mathcal{R}y$, lo cual es una contradicción. Concluimos que la única opción es $y\mathcal{R}c_1$, para algún $c_1 \in C$.

  Luego,

- Si $c_1 \neq y \wedge y\mathcal{R}c_1$, entonces $f(y)\mathcal{R}c_1$ (porque $c_1 \in A^*$), de modo que $f(y)\mathcal{R}c_0$.

- Si $c_1 = y \wedge y\mathcal{R}c_1$, entonces, siendo $y \neq c_0$, se tiene $c_1 \neq c_0$. Por lo tanto, existe $c_2 \in C$, tal que $y\mathcal{R}c_2 \wedge c_2 \neq y$. De aquí, $c_2\mathcal{R}c_0 \wedge f(y)\mathcal{R}c_2$ implican $f(y)\mathcal{R}c_0$.

  En ambos casos, $f(y)\mathcal{R}c_0$, es decir $c_0 \in A^*$. Concluimos que $A^* \in \mathscr{H}_a$.

  Por otra parte, como $A^* \subseteq A$ y siendo A un elemento de $\mathscr{H}_a$, se tiene $A \subseteq A^*$.

  Además, $A^* \in \mathscr{A}_a$ implica $A^* \subseteq A$. Concluimos que $A^* = A$.

- $$\forall x, y \in A, (x\mathcal{R}y \vee y\mathcal{R}x).$$

  Sea $x \in A$, entonces $x \in A^*$. Si $y \in A_x := \{z \in A : z\mathcal{R}x \vee f(x)\mathcal{R}z\}$, pues $A = A_x$.

  Así, $y\mathcal{R}x \vee f(x)\mathcal{R}y$. Pero $x\mathcal{R}f(x)$. con lo cual se concluye que $y\mathcal{R}x \vee x\mathcal{R}y$.

Finalmente, concluimos que A es una cadena en X.

$\blacksquare$

Capítulo 3

El Axioma de Elección en Topología

En este capítulo se presenta el concepto de filtro y se garantiza – mediante el teorema de Tarski – que es posible extender un filtro hacia un ultrafiltro. El uso de filtros en Topología está relacionado con el concepto de convergencia, tal como se verá en la sección final del presente capítulo.

3.1. Filtros

Definición 3.1. Un *filtro* sobre un conjunto S es una colección F de subconjuntos de S tal que:

(F1) $S \in F$;

(F2) si $X \in F$ y $Y \in F$, entonces $X \cap Y \in F$;

(F3) si $X, Y \subseteq S$, $X \in F$, y $X \subseteq Y$, entonces $Y \in F$.

Definición 3.2. Un filtro F sobre un conjunto S es *propio*, si $\varnothing \notin F$.

Observación 3.1. En adelante, consideraremos solamente filtros propios. Así, se asumirá que $S \neq \varnothing$ y

(F4) $\varnothing \notin F$.

Definición 3.3. Sea $S \neq \varnothing$ y β una colección de subconjuntos de S. β es una *base de filtro en* S, si

1. $\beta \neq \varnothing$
2. $\varnothing \notin \beta$, es decir, $\forall A \subseteq \beta,\ A \neq \varnothing$
3. Si $A, B \in \beta$, entonces existe $C \in \beta$ tal que $C \subseteq A \cap B$

Observación 3.2. Todo filtro en S es una base de filtro en S.

Ejemplo 3.1. A continuación, se muestran tres ejemplos de filtros conocidos en Topología:

1. Sea S un conjunto . El filtro *trivial* es $F = \{S\}$.

2. Sea X_0 un subconjunto no vacío de S. El filtro

$$F = \{X \subseteq S :\ X \supseteq X_0\}.$$

   se denomina filtro *principal.*

3. Sea S un conjunto infinito. La colección

$$F = \{X \subseteq S :\ S - X \text{ es finito}\}$$

   es un filtro. F es denominado filtro de *Fréchet* sobre S.

Proposición 3.1. Sea S un conjunto no vacío y β una base de filtro en S. La colección

$$F(\beta) = \{A \subseteq S : \exists B \in \beta,\ B \subseteq A\}$$

es un filtro en S, denominado *filtro generado por* β.

Prueba.

1. $F(\beta) \neq \varnothing$, pues $\beta \neq \varnothing$ por ser una base de filtro.

2. Sean A, $D \in F(\beta)$. Debe probarse que existe $C \in F(\beta)$ tal que $C \subseteq A \cap D$. En efecto, existen B, B' tales que $B \subseteq A$ y $B' \subseteq D$. Por condición de filtro, existe $B'' \in \beta$ tal que $B'' \subseteq B \cap B' \subseteq A \cap D$, es decir $B'' \subseteq A \cap B$. Luego, $A \cap B \in F(\beta)$.

3. $\varnothing \notin F(\beta)$, pues $\varnothing \notin \beta$.

4. Sea $A \in F(\beta)$, $A \subseteq B$. Veamos que $B \in F(\beta)$. En efecto, como $A \in F(\beta)$, existe $C \in \beta$ tal que $C \subseteq A$ y como $A \subseteq B$, se tiene $C \subseteq B$. Luego, $B \in F(\beta)$.

■

Ejemplo 3.2. Sea X un conjunto no vacío y τ una topología en X (el par (X, τ) se denomina espacio topológico). Para cada $x \in X$, la colección de todas las vecindades de x en (X, τ), $V_X(x)$, es un filtro en X denominado *filtro de vecindades* de x en (X, τ) y se denota con $\beta(x)$.

Ejemplo 3.3. Sean X y Y dos conjuntos no vacíos y $f : X \to Y$ una aplicación. Si β es una base de filtro en X, el filtro

$$f(\beta) = \{f(U) : U \in \beta\}$$

es una base de filtro en Y. El filtro $F(f(\beta))$ generado por $f(\beta)$ se denomina *filtro imagen* de β por f.

Definición 3.4. Sean $X \neq \varnothing$, F un filtro en X y $\beta \subseteq F$. Decimos que β es una *base del filtro* F, si

$$\forall A \in F, \exists B \in \beta \, : \, B \subseteq A.$$

Observación 3.3. β es una base del filtro $F(\beta)$.

Proposición 3.2. Sea $X \neq \varnothing$, F un filtro en X y β una base del filtro F, entonces β es una base de filtro en X y $F(\beta) = F$.

Prueba.

1. $\beta \neq \varnothing$, pues $\beta \subseteq F$.

2. $\varnothing \notin \beta$. En efecto, sea $U \subseteq \beta$. Veamos que $U \neq \varnothing$. Si $U = \varnothing$, se tendría $\varnothing \in F$, lo cual es una contradicción.

3. Sean $A, B \in F$. Veamos que existe $C \in \beta$, tal que $C \subseteq A \cap B$. En efecto, como $A, B \in F$ y como F es filtro, $A \cap B \in F$. Además β es una base del filtro F con lo cual existe $C \in \beta$ tal que $C \subseteq A \cap B$. Luego, β es una base de filtro en X y $F(\beta) = F$.

$\blacksquare$

Definición 3.5. Una familia G de conjuntos satisface la *propiedad de la intersección finita*, si cada colección finita $H = \{X_1, \ldots, X_n\}$ tiene intersección no vacía: $X_1 \cap \cdots \cap X_n \neq \varnothing$.

Lema 3.1.

(a) Si $\mathscr{F}$ es una familia de filtros sobre S, entonces $\bigcap \mathscr{F}$ es un filtro sobre S.

(b) Si $\mathscr{C}$ es una $\subseteq$–cadena de filtros sobre S, entonces $\bigcup\mathscr{C}$ es un filtro sobre S.

(c) Si $G \subset \boldsymbol{P}(S)$ satisface la propiedad de la intersección finita, entonces existe un filtro $\mathcal{F}$ sobre S, tal que $G \subseteq F$.

Prueba.

Probamos la última. Sea F el conjunto formado por todos los subconjuntos X de S tal que existe una colección finita $H = \{X_1, \ldots, X_n\} \subseteq G$ con $X_1 \cap \cdots \cap X_n \subseteq X$. Entonces, F es un filtro y $F \supseteq G$.

■

Observación 3.4. Puesto que todo filtro $F \supseteq G$ debe contener todas las intersecciones finitas de conjuntos en G, se sigue que el filtro F construido en la prueba del Lema 3.1*c* es el menor filtro sobre S que extiende G:

$$F = \bigcup\{D :\ D \text{ es un filtro sobre } S \text{ y } G \subseteq D\}.$$

En este caso, decimos que el filtro F es *generado* por G.

3.2. Ultrafiltros

Definición 3.6. Un filtro U sobre un conjunto S es un *ultrafiltro* si,

$$\forall X \subseteq S,\ \ X \in U \ \ \vee \ \ S - X \in U.$$

Observación 3.5. De acuerdo con la observación 3.1, la disyunción dada en la definición de ultrafiltro es excluyente, caso contrario tendríamos que $\varnothing \in U$.

Observación 3.6. Si U es un ultrafiltro y $X \cap Y \in U$, entonces o $X \in U$ o $Y \in U$.

Ejemplo 3.4. Sea S un conjunto no vacío y $x \in S$. La colección

$$U = \{M \subseteq S\ : x \in M\}$$

es un ultrafiltro.

Ejemplo 3.5. Sean X y Y dos conjuntos no vacíos y $f:\ X \to Y$ una aplicación. Sea U un ultrafiltro en X, entonces

$$f(U) = \{f(M)\ : M \in U\}$$

es una base de filtro en Y. El filtro generado por $f(U)$ es un ultrafiltro en Y.

Definición 3.7. Un filtro F sobre un conjunto S se denomina *maximal*, si no existe un filtro F' sobre S tal que $F \subseteq F'$.

Lema 3.2. *Un filtro F sobre S es un ultrafiltro si y solamente si es maximal.*

Prueba.

Primero demostramos que un ultrafiltro U es un filtro maximal. En efecto, supongamos que $U \subset F$ y $X \in F - U$. Entonces $S - X \in U$, y de este modo se tiene $S - X$ y $X \in F$, lo cual es una contradicción.

Por otra parte, supongamos que F es un filtro que no es ultrafiltro. Debemos construir F' tal que $F' \supset F$. Para ello, consideremos $Y \subseteq S$ tal que ni Y ni $S - Y$ pertenecen a F. Sea $G = F \cup \{Y\}$, aseveramos que G satisface la propiedad de la intersección finita. En efecto, si $X \in F$, entonces $X \cap Y \neq \varnothing$, para cualquier otro caso, se tendrá $S - Y \supseteq X$ y $S - F \in F$. Así, si $X_1, \ldots, X_n \in F$, entonces $X_1 \cap \cdots \cap X_n \in F$ de modo que

$$Y \cap X_1 \cap \cdots \cap X_n \neq \varnothing.$$

Por lo tanto, G satisface la propiedad de la intersección finita, y por el Lema 3.1c existe un filtro F' tal que $F' \supseteq G$. Como $Y \in F' - F$, se tiene $F \subset F'$.

$\blacksquare$

3.3. Teorema del ultrafiltro de Tarski

Teorema 3.1. *Todo filtro sobre S puede ser extendido a un ultrafiltro.*

Prueba.

Sea F_0 un filtro sobre S. Sea P el conjunto de todos los filtros F sobre S, tal que $F \supseteq F_0$ y consideremos el conjunto ordenado $(P, \subset)$. Si $\mathscr{C}$ es una cadena en P, entonces por el Lema 3.1c, $\bigcup \mathscr{C}$ es un filtro; además, es una cota superior de $\mathscr{C}$ en P. Por el Lema de Zorn, existe un elemento maximal U en P. Tal elemento maximal es un ultrafiltro, de acuerdo con el Lema 3.2.

$\blacksquare$

Comentario 3.1. Podemos observar en la demostración del teorema 3.1 (teorema del ultrafiltro de Tarski) que un ultrafiltro no es más que un elemento maximal del conjunto de todos los filtros sobre un conjunto específico, siendo garantizada su existencia por el lema de Zorn. Como se indicó y demostró en el capítulo precedente, dicho lema es equivalente al axioma de elección. Además, el teorema del ultrafiltro de Tarski implica el axioma de elección (Ver [3,p 16]), de modo que podemos considerar tal teorema como un principio de elección.

3.4. Convergencia de filtros

En esta sección desarrollamos algunos resultados importantes que se obtienen a partir de la definición de filtro. Uno de ellos es la convergencia de filtros en espacios topológicos, la cual desempeña un papel similar al de las sucesiones en espacios métricos.

Definición 3.8. Sea (X, τ) un espacio topológico, y F un filtro en X. Se dice que el filtro F *converge* a x en X si $\beta(x) \subseteq F$, es decir, si F es *más fino* que el filtro de vecindades de x.

Notación: $F \longrightarrow x$.

Ejemplo 3.6.

1. Sea (X, τ) un espacio topológico. Para cada $x \in X$, el filtro de vecindades de x, $\beta(x)$, converge a x.

2. Sea X un conjunto infinito. La colección

$$\tau = \{U \subseteq X \ : \ X - U \ \text{es finito}\}$$

es una topología en X denominada la *topología de los complementos finitos*. El filtro de Fréchet (ver ejemplo $3.1 - 3$) converge a cada punto de X.

3. Sea X un conjunto. La colección $\tau = \{\varnothing, X\}$ es una topología en X denominada *topología indiscreta o trivial*. Con esta topología, todo filtro en X converge a cualquier punto en X

4. Dado un conjunto X y $\varnothing \neq A \subseteq X$. Consideremos la topología $\{\varnothing, A, X - A, X\}$ en X, y el filtro trivial $F = \{X\}$. Entonces F no converge a ningún punto en X. Sin

embargo, el mismo filtro converge a cada punto de $X - A$, si consideramos la topología $\{\varnothing, A, X\}$.

Observación 3.7. A partir del ejemplo 3.6, podemos inferir que un filtro

- no necesariamente converge a un punto en el espacio topológico, o
- puede converger exactamente a un punto, o
- puede converger a más de uno, de hecho, puede converger a infinitos puntos en el espacio topológico.

Definición 3.9. Un espacio topológico (X, τ) es un *espacio T_2* o un *espacio de Hausdorff* , si

$$\forall x, y \in X,\ x \neq y,\ \exists U \in V_X(x)\ \wedge\ \exists V \in V_X(y)\ :\ U \cap V = \varnothing.$$

La última aseveración dada en la observación 3.7 no se presenta en los espacios de Hausdorff, como se muestra a continuación.

Proposición 3.3. Sea (X, τ) un espacio topológico. X es un espacio de Hausdorff, si y solamente si todo filtro tiene a lo más un límite.

Prueba.

Supongamos que X sea un espacio de Hausdorff y consideremos x y y en X, con $x \neq y$. Entonces existen vecindades U y V de x y y respectivamente, con $U \cap V = \varnothing$. Así, ningún filtro contiene tanto a U como a V, en consecuencia, ningún filtro puede converger a x y a y simultáneamente. Por lo tanto, todos los filtros en un espacio de Hausdorff tienen a lo más un límite.

Recíprocamente, supongamos que x y y no tienen vecindades disjuntas. Entonces, $V_X(x) \cup V_X(y)$ forma una subbase para un filtro que converge tanto a x como a y. Luego, si todo filtro tiene a lo más un límite, entonces es de Hausdorff.

■

Comentario 3.2. Como se indicó al inicio de esta sección, un modo de describir la convergencia en espacios topológicos es mediante la definición de filtros, de modo que requerir que un espacio sea de Hausdorff es equivalente a requerir la unicidad del límite (en caso exista), de acuerdo con lo establecido en la Proposición 3.3. Además, bajo la descripción de convergencia mediante filtros, se establecen las nociones de continuidad y completitud en espacios métricos.

Definición 3.10. Sea (X, τ) un espacio topológico y F un filtro en X. Un punto $x \in X$ es un *punto adherente* a F en (X, τ), si

$$x \in \bigcap_{M \in F} \overline{M},$$

siendo $\overline{M}$ la adherencia de M en (X, τ).

Proposición 3.4. Sea (X, τ) un espacio topológico y F un filtro en X. $x \in X$ es un punto adherente a F en (X, τ), si y solamente si existe un filtro más fino que F convergente a x.

Prueba.

Supongamos que x es punto adherente a F en (X, τ), es decir $x \in \bigcap_{M \in F} \overline{M}$, lo cual implica que

$$x \in \overline{M},\ \forall\, \overline{M},\ M \in F;$$

así,

$$V \cap M \neq \varnothing,\ \forall\, V \in \beta(x).$$

Sea

$$\beta = \{V \cap M \ : \ M \in F,\, V \in \beta(x)\}.$$

β es una base de filtro en X y $G = F(\beta)$ es el filtro generado por β que es más fino que F. En efecto, si $U \in F$, $U = U \cap X$ con $X \in \beta(x)$. Luego, $U \in G$ con lo cual $F \subseteq G$. Además, $\beta(x) \subseteq G$, pues si $W \in \beta(x)$, $W \cap M \subseteq W$; es decir $W \in G$.

Por otra parte, para demostrar el enunciado recíproco, consideremos un filtro G en X tal que $F \subseteq G$. Debe probarse que $x \in \bigcap\limits_{M \in F} \overline{M}$. Sea $V \in \beta(x)$ y $M \in F$. Veamos que $V \cap M \neq \varnothing$. En efecto, $V \in G$ y $M \in G$. Como G es filtro, $\varnothing \neq V \cap M \in G$. Luego, $V \cap M \neq \varnothing$.

■

Comentario 3.3. Para finalizar este capítulo, hemos de indicar que un resultado importante en Topología General es el teorema de Tychonoff. Tal teorema establece que si tenemos una familia indexada de espacios topológicos compactos, $\{X_i \ : \ i \in I\}$, entonces el espacio $X = \prod\limits_{i \in I}$ es compacto, con la topología del producto. Una prueba de este teorema se presenta en el texto de Sze-Tsen Hu, *Introduction to General Topology* [2]. En dicha prueba, se utiliza inevitablemente el axioma de elección a través de una de sus equivalencias: El Lema de Tukey, el cual establece que toda familia no vacía de conjuntos que tiene carácter finito [3] posee un elemento maximal (maximal con respecto a la relación de inclusión entre conjuntos). Es decir que la demostración se sustenta en un axioma no constructivo de la teoría de conjuntos. Posteriormente, J. Kelley [4] en 1950 establece que

[2]Sze-Tsen Hu, *Introduction to General Topology.* Holden- Day , California. 1966. Páginas 64, 65 y 66.

[3]Una familia de conjuntos $\mathscr{F}$ tiene *carácter finito* si para cada X, X pertenece a $\mathscr{F}$ si y solamente si cada subconjunto finito de X pertenece a $\mathscr{F}$.

[4]J. L. Kelley, *The Tychonoff product theorem implies the axiom of choice*, Fund. Math. 37 (1950), 75−76

el teorema de Tychonoff implica el axioma de elección, siendo tal demostración corregida en el año 2003 por Sangho Kum [5]. Todo ello nos permite concluir que el teorema de Tychonoff puede establecerse como un principio de elección por ser equivalente al axioma de elección.

[5]Kum, S. *A Correction of Kelley's proof on the equivalence between the Tychonoff product theorem and the axiom of choice*, Journal of the Chungcheong Mathematical Society. 16 (2003), $75-78$.

Capítulo 4

El Axioma de Elección en Álgebra

En este capítulo presentamos la definición de base de Hamel y garantizamos su existencia mediante el lema de Zorn. Posteriormente se demuestra que el hecho de garantizar la existencia de una base para un espacio vectorial no trivial implica el axioma de elección. Hemos de indicar que para establecer tal demostración, se utiliza un axioma equivalente al axioma de elección: el axioma de múltiple elección.

4.1. Bases de Hamel

El matemático alemán Hamel concibió la noción de una "base" para todos los números reales como sigue: Sea H un conjunto de números reales con las propiedades

1. Si $x_1, \ldots, x_n$ es cualquier subconjunto finito de H y si $r_1, \ldots, r_n$ son números racionales para los cuales $r_1x_1 + \cdots + r_nx_n = 0$, entonces $r_1 = \ldots = r_n = 0$.

2. Cada número real x puede ser expresado como una combinación lineal finita de elementos de H, con coeficientes racionales.

En términos de esa base, Hamel examinó a continuación las funciones reales que satisfacen la ecuación $f(x+y) = f(x)+f(y)$, para todo real x y y. Si H es una base en el sentido explicado, una función real f es definida como sigue: Si $x \in H$, asignar valores de $f(x)$ arbitrariamente. Cada número real x tiene representación única $x = r_1x_1+\cdots+r_nx_n$, donde $x_1, \ldots, x_n$ están en H y $r_1, \ldots, r_n$ son racionales (ciertamente, n puede variar con x). A apartir de ello, se define $f(x) = r_1f(x_1)+\cdots+r_nf(x_n)$, los valores de $f(x_1), \ldots, f(x_n)$ ya han sido asignados. Como resultado de esta definición, f satisface la condición $f(x + y) = f(x) + f(y)$, para todo x y y. Este procedimiento proporciona todas las funciones posibles f que satisfacen tal condición.

Para mostrar la existencia de una base para todos los números reales, Hamel usó un argumento basado en la proposición de que todo conjunto puede ser bien ordenado. Esta proposición es equivalente al axioma de elección o al Lema de Zorn.

Definición 4.1. Sea X un espacio vectorial no nulo[6]. Un conjunto $H \subset X$ se denomina una *base de Hamel* de X, si:

1. H es un subconjunto linealmente independiente de X.

2. El subespacio vectorial generado por H es todo el espacio X.

4.2. Teorema de existencia de bases

Teorema 4.1. *El Lema de Zorn implica que todo espacio vectorial no nulo contiene una base*

[6]Espacio vectorial que no está constituido únicamente por el neutro aditivo.

Prueba.

Consideremos la colección $\mathscr{H}$ de todos los subconjuntos linealmente independientes de un $\mathbb{K}$-espacio vectorial $X \neq \{0\}$. Claramente $\mathscr{H}$ es ordenado por la relación de inclusión entre conjuntos, $\subseteq$. Sea $\mathscr{C}$ una cadena en $\mathscr{H}$.

Afirmación. $\bigcup \mathscr{C} \in \mathscr{H}$.

En efecto, sean $x_1, \ldots, x_n \in \bigcup \mathscr{C}$, y $r_1, \ldots, r_n$ escalares, tales que

$$r_1 x_1 + \cdots + r_n x_n = 0.$$

Así, existen conjuntos $C_1, \ldots, C_n \in \mathscr{C}$ con $x_1 \in C_1, \ldots, x_n \in C_n$. Pero, como $\mathscr{C}$ es una cadena, debe tener un máximo (bajo la relación de inclusión entre conjuntos). Supongamos que tal elemento máximo es C_k. Por lo tanto $x_1 \in C_k, \ldots, x_n \in C_k$. Pero C_k es un subconjunto linealmente independiente, con lo cual $r_1 = \cdots = r_n = 0$. Así, la afirmación está probada.

Continuando con la prueba del teorema, dado que a partir de la afirmación se concluye que $\bigcup \mathscr{C}$ es un subconjunto linealmente independiente, las hipótesis del Lema de Zorn se satisfacen. Por lo tanto, existe en X un subconjunto maximal linealmente independiente, es decir, existe una base.

$\blacksquare$

4.3. El teorema de existencia de bases como principio de elección

Antes de enunciar el teorema que permite establecer una equivalencia entre principios, hemos de enunciar un axioma que es equivalente al axioma de elección:

Axioma de elección múltiple (AEM)

Para cada familia $(X_i)_{i\in I}$ de conjuntos no vacíos, existe una familia $(F_i)_{i\in I}$ de conjuntos finitos no vacíos, con $F_i \subseteq X_i$ para cada $i \in I$.

La prueba de esta equivalencia es dada en [3, p.11].

Teorema 4.2. *La proposición "todo espacio vectorial contiene una base" implica el axioma de elección.*

Prueba.

En realidad, se probará que la proposición indicada implica el Axioma de elección múltiple (AEM). Sea $(X_i)_{i\in I}$ una familia de conjuntos no vacíos, disjuntos dos a dos. Consideremos un campo arbitrario $\mathbb{K}$ y sea $\mathbb{K}(X)$ el campo de las funciones racionales en las variables $x \in X = \bigcup_{i\in I} X_i$, sobre $\mathbb{K}$. Para monomios, es decir elementos de $\mathbb{K}(X)$ los cuales tienen la forma $p = \alpha \cdot x_1^{n_1} \cdot x_2^{n_2} \cdots x_m^{n_m}$. Definimos para cada $i \in I$, el i–grado de p como $d_i(p) = \sum_{x_k \in X_i} n_k$. Un elemento de $\mathbb{K}(X)$, $\alpha = \dfrac{p_1 + \cdots + p_n}{q_1 + \cdots + q_m}$ donde p_k y q_k son monomios, serán llamados i–homogéneos de grado d con tal que todos los q_k tengan el mismo i–grado, digamos d_1, y todos los p_k tengan el mismo i–grado $d_2 = d_1 + d$. Entonces

$$K = \{a \in \mathbb{K}(X) :\ a \text{ es } i - \text{homogénea de grado } 0 \text{ para cada } i \in I\}$$

es un subcampo de $\mathbb{K}(X)$. Así $\mathbb{K}(X)$ es un espacio vectorial sobre K. Por hipótesis, $\mathbb{K}(X)$ tiene una base B. Para cada $x \in X$ el monomio x puede ser expresado únicamente en la forma $x = \sum_{b\in B(x)} a_b(x) \cdot b$, donde $B(x)$ es un subconjunto finito de B y cada $a_b(x) \in K \backslash \{0\}$.

Sean x y y elementos del mismo X_i. Entonces

$$y = \frac{y}{x} \cdot x = \sum_{b \in B(x)} \frac{y}{x}\, a_b(x) \cdot b = \sum_{b \in B(y)} a_b(y) \cdot b.$$

Dado que $\frac{y}{x} \in K$, esto implica que $B(x) = B(y)$ y $\frac{a_b(y)}{y} = \frac{a_b(x)}{x}$ para cada $b \in B(x)$. Así, los conjuntos $B(x)$ y los elementos $\frac{a_b(x)}{x}$ dependen solamente de i y no de $x \in X_i$. Denotémoslos con B_i y $\alpha(b,i)$ respectivamente. Puesto que los $a_b(x)$ son i–homogéneos de grado 0, los $\alpha(b,i) = \frac{a_b(x)}{x}$ son i–homogéneos de grado -1. Así, si $\alpha(b,i)$ es escrito como un cociente de polinomios en forma reducida, algún $x \in X_i$ debe ocurrir en el denominador. Por lo tanto el conjunto F_i, consistente de todos los $x \in X_i$ que ocurren en el denominador de $\alpha(b,i)$ en su forma reducida para algún $b \in B_i$, es un subconjunto no vacío y finito de X_i. Esto establece el axioma de elección múltiple (AEM).

■

Comentario 4.1. Un espacio vectorial puede admitir muchas bases de Hamel, sin embargo, ellas presentan el mismo cardinal, es decir el mismo número de elementos. Para justificar tal afirmación, consideremos dos bases de Hamel S y T de un espacio vectorial X. Supongamos que S es finito y está compuesto por n elementos $x_1, x_2, \ldots, x_n$. Si T estuviera conformado por $n+1$ elementos, $y_1, y_2, \ldots, y_n, y_{n+1}$, entonces

$$y_i = \sum_{i=1}^{n} a_{ij} x_j, \quad i = 1, \ldots, n.$$

Dado que $y_1, y_2, \ldots, y_n$ son linealmente independientes, la matriz formada con los coeficientes a_{ij} tiene rango n. Sin embargo,

$$y_{n+1} = \sum_{j=1}^{n} a_{n+1j}\, x_j$$

y el vector $(a_{n+1,1} \ldots, a_{n+1,n})$ son una combinación lineal de los vectores fila de la matriz (a_{ij}). Pero esto implica que $y_1, y_2, \ldots, y_n, y_{n+1}$ no son linealmente independientes. Por lo tanto, T tiene $m \leq n$ elementos. Análogamente, $n \leq m$ y se tiene la igualdad de cardinales en caso las bases sean finitas.

Por otra parte, supongamos que S es infinito y tiene cardinal a. Sea b el número cardinal de T. Cada $y \in T$ es una combinación lineal, con coeficientes no ceros, de un número finito $x_1, x_2, \ldots, x_n$ de elementos de S, y solamente un número finito n de elementos de T están asociados de este modo con el mismo conjunto $x_1, x_2, \ldots, x_n$ o algún subconjunto de este. Puesto que el número cardinal del conjunto de subconjuntos finitos de S es igual al del propio S, se sigue que $b \leq \aleph_0.a = a$. Análogamente, $a \leq b$, de modo que $a = b$. Este comentario puede resumirse a través de una

Proposición 4.1. Si X es un espacio vectorial de dimensión finita o infinita, todas las bases de Hamel de X tienen el mismo número cardinal.

Conclusiones

Finalizado el desarrollo del trabajo, podemos concluir:

- El uso de los lenguajes formales, en el caso específico de los lenguajes de primer orden, permiten establecer y estudiar los axiomas de la teoría de conjuntos: los axiomas de Zermelo – Fraenkel, de manera que se pueda analizar todo aquello que concierna a los fundamentos de dicha teoría (consistencia, completitud).

- El axioma de elección – uno de los axiomas de Zermelo - Fraenkel – garantiza la existencia de conjuntos sin definirlos, es decir, este axioma es no constructivo. Asimismo, el Lema de Zorn y el Teorema del buen orden son principios equivalentes al axioma de elección. Por lo tanto, estos también son principios no constructivos.

- Existen diversas implicaciones y equivalencias con el axioma de elección, desarrolladas en distintas áreas de la matemática. Una implicación de tal axioma, en Topología, es garantizar la extensión de un filtro hacia un ultrafiltro; mientras que en el Álgebra, tenemos la equivalencia entre el axioma de elección y la proposición que garantiza la existencia de bases para un espacio vectorial, tal como se ha desarrollado en este trabajo.

Bibliografía

[1] Goffman, C., “First course in Functional Analysis.” Second edition. American Mathematical Society, USA. (1983)

[2] Hamilton, A. G., “Numbers, sets and axioms: the apparatus of mathematics.” First edition. Cambridge University Press, Cambridge. (1982)

[3] Herrlich, H. “Axiom of Choice.” Springer-Verlag, The Netherlands. (2006)

[4] Jech, T. J., “The Axiom of Choice.” North - Holland Publishing Company, Amsterdam. (1973)

[5] Jech, T. J., “Set Theory.” Academic Press, Inc., New York. (1978)

[6] Murdeshwar, M. G., “General Topology.” New Age International (P) Ltd, Publishers, Nueva Delhi. (1990)

[7] Rubin, H. y Rubin, J. E., “Equivalents of the Axiom of Choice, II.” Elsevier Science Publishers B. V., Amsterdam. (1985)

[8] Srivastava, S. M., “A Course on Mathematical Logic.” First edition. Springer Science+Business Media, LLC, New York. (2008)