Publicaciones Electrónicas
Sociedad Matemática Mexicana

Teoría Cantoriana de los Conjuntos

Juan Antonio Pérez

www.smm.org.mx

Serie: Cursos. Vol. 2 (2012)

Teoría Cantoriana de los Conjuntos

Juan Antonio Pérez
Escuela de Verano de Matemáticas 2011
Universidad Autónoma de Zacatecas

noviembre 2012

El presente material fue elaborado originalmente para usarse como texto en el curso con el mismo título impartido por el autor en el verano de 2011, a una audiencia compuesta es su mayoría de profesores de bachilerato. Tanto el curso como el presente material se proponen proporcionar una introducción algebraica a la Lógica y una revisión, con un mínimo de formalidad de la Teoría Cantoriana de los conjuntos.

El texo se divide en dos partes, que se constituyen, respectivamente, de los capítulos 1 al 4 y del 5 al 9, y que son relativamente independientes. Una de las obligaciones de la comunidad matemática es la elaboración de una teoría en la que el concepto de infinito tenga un lugar natural. El infinito es un objeto de propiedad casi exclusiva de las matemáticas, por lo que resultaría negligente ignorar la monumental aportación de Cantor al esclarecimiento de su naturaleza, por lo que nos proponemos, a través de este texto, ponerla al alcance de los lectores.

El autor agradece al árbitro, sin cuya intervención muchos errores habrían permanecido en el texto. Aquellos que aún se encuentran en las páginas que siguen son, no obstante, responsabilidad única y exclusiva del autor.

Juan Antonio Pérez
Unidad Académica de Matemáticas
Universidad Autónoma de Zacatecas
noviembre de 2012

Índice

1. El campo $\mathbb{F}_2$

El concepto de conjunto se construye con alguna formalidad en el presente texto a partir del capítulo 5, previamente a ello, consideraremos la idea intuitiva de colección como un objeto en el que la relación de pertenencia tiene sentido. Si A es una colección la afirmación $x \in A$ tiene sentido para otra colección x. Los objetos para los cuales se satisface $x \in A$ se dice que son los *elementos* de A. En los capítulos del 1 al 4, el término conjunto se usará de manera informal como sinónimo de colección, familia o clase.

Un conjunto se define como un objeto que satisface un cuerpo axiomático que se desarrollará a partir del capítulo 5. Al igual que la idea de colección, la noción de aplicación se usa de forma intuitiva como una regla que asigna a cada elemento de una *colección dominio*, un único elemento de una *colección codominio*. En este primer capítulo, y para poder proporcionar una introducción algebraica a la Lógica, las nociones de para ordenado y producto cartesiano son consideradas estrictamente objetos de naturaleza intuitiva. Todas estas nociones serán formalizadas satisfactoriamente en los capítulos del 5 al 9.

Una *operación binaria* en un conjunto $A \neq \varnothing$ es una aplicación

$$\mu : A \times A \longrightarrow A.$$

Es constumbre denotar una operación binaria con un símbolo entre los elementos del par sobre el que se aplica.

$$\mu(x, y) = x * y$$

En función de que una operación se define como una aplicación, entonces, la sola regla de correspondencia no determina que una aplicación, sea o no una operación binaria.

Ejemplo 1 *Consideremos el conjunto de los dígitos*

$$D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Nótese que ni la adición ni la multiplicación, ordinarias de los enteros son operaciones binarias sobre D. La suma de dos dígitos no es necesariamente un dígito, y lo mismo ocurre con el producto.

Ejemplo 2 *No obstante, la suma módulo* 10 *y la multiplicación módulo 10 si son operaciones binarias sobre D. En este caso,* $7 + 3 = 0$ *y* $8 + 6 = 4$.

Ejemplo 3 *La adición y la multilicación son operaciones binarias sobre el conjunto de los números naturales* $\mathbb{N} = \{0, 1, 2, \ldots\}$*, pero no es el caso de la diferencia ni de la división. Esta última ni siquiera está definida para todos los pares de naturales. El residuo* r *si es una operación binaria en* $\mathbb{N}$*, pongamos por caso* $r(14, 6) = 2$ *que es el residuo de dividir* 14 *por* 6*.*

Ejemplo 4 *El producto de dos intervalos es un rectángulo. El producto cartesiano no es una operación binaria sobre subespacios de la recta.*

Una operación binaria μ sobre un conjunto A se dice *asociativa* si satisface que

$$\mu(x, \mu(y, z)) = \mu(\mu(x, y), z)$$

o equivalentemente, si

$$x * (y * z) = (x * y) * z$$

para cualesquiera elementos $x, y, z \in A$.

Una operación binaria μ sobre un conjunto A se dice *conmutativa* si satisface que

$$\mu(x, y) = \mu(y, x)$$

o equivalentemente, si

$$x * y = y * x$$

para elementos arbitrarios $x, y \in A$.

Un *grupo* es un par $(G, *)$ tal que $G \neq \varnothing$ es un conjunto y $*$ es una operación binaria que satisface las siguientes propiedades conocidas como *axiomas de grupo*:

1. La operación de grupo "$*$" es asociativa.

2. Existe un elemento $e \in G$ tal que

   $$e * x = x * e = x$$

   para todo $x \in G$. El elemento e se llama *elemento neutro*.

3. Para todo $x \in G$ existe $y \in G$ tal que

   $$x * y = y * x = e.$$

   Se dice que y es el *inverso* de $x \in G$.

Coloquialmente, decimos que G tiene un elemento neutro y elementos inversos. Un grupo G se dice que es un *grupo abeliano* si su operación es conmutativa.

En un grupo aditivo de la forma $(G, +)$ el elemento neutro se denota por "0" y el elemento inverso de $x \in G$ se escribe como $-x$. En un grupo multiplicativo de la forma $(G, \cdot)$ el elemento neutro se denota por "1" y el elemento inverso de $x \in G$ se escribe como x^{-1}. Si $(G, +)$ es un grupo denotamos $G^* = G - \{0\}$

Un *campo* es una terna $(\mathbb{F}, +, \cdot)$ donde $\mathbb{F} \neq \varnothing$ es un conjunto y tanto "+" como "$\cdot$" son operaciones binarias sobre $\mathbb{F}$, llamadas adición y multiplicación respectivamente, de manera que

1. $(\mathbb{F}, +)$ es un grupo abeliano

2. $(\mathbb{F}^*, \cdot)$ es un grupo abeliano.

3. La multiplicación se distribuye respecto de la adición, es decir,

$$(x + y)z = xz + yz$$

para cualesquiera $x, y, z \in \mathbb{F}$. Esta propiedad se conoce como *distributividad*.

Los sistemas de los números racionales $\mathbb{Q}$, de los números reales $\mathbb{R}$ y de los números complejos $\mathbb{C}$ son ejemplos de campos. Para nuestro propósito de desarrollar la Lógica, el campo que nos interesa es el más pequeño posible, el campo con dos elementos $\mathbb{F}_2 = \{0, 1\}$ con las siguientes tablas de adición y de multiplicación, respectivamente.

+	0	1
0	0	1
1	1	0

La tabla anterior informa acerca de que $1 + 1 = 0$ y la siguiente que $1 \cdot 1 = 1$.

$\cdot$	0	1
0	0	0
1	0	1

El campo $\mathbb{F}_2$ tiene únicamente dos elementos, pero ya presenta una estructura de sumo interés, sus elementos son únicamente los elementos identidad aidtivo y multiplicativo, y sin embargo es el modelo adecuado para la definición de los valores y las funciones de verdad. De acuerdo con la terminología de Bourbaki[1], una función es una aplicación con valores en un anillo, y un campo es una clase particular de anillo, como veremos más adelante, entonces, las funciones de verdad son verdaderamente funciones.

[1]Nicolás Bourbaki es un personaje ficticio bajo cuyo nombre se identifica un colectivo de matemáticos particularmente influyente.

2. Cuaderno de ejercicios no. 1

1. Elabore la tabla de adición de $\mathbb{Z}/5$,

+	0	1	2	3	4
0					
1					
2					
3					
4					

e identifique los inversos aditivos.

k	0	1	2	3	4
$-k$					

2. Elabore la tabla de adición de $\mathbb{Z}/6$,

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

e identifique los inversos aditivos.

k	0	1	2	3	4	5
$-k$						

3. Elabore la tabla demultiplicación de $(\mathbb{Z}/5)^*$,

$\times$	1	2	3	4
1				
2				
3				
4				

e identifique los inversos multiplicativos, así como los divisores de cero.

k	0	1	2	3	4
k^{-1}					

4. Elabore la tabla de multiplicación de $(\mathbb{Z}/6)^*$,

$\times$	1	2	3	4	5
1					
2					
3					
4					
5					

e identifique los inversos multiplicativos así como los divisores de cero.

k	0	1	2	3	4	5
k^{-1}						

5. Compare las tablas de multiplicación de $\mathbb{Z}/5$ y de $\mathbb{Z}/6$, reportando tres similitudes y tres diferencias.

6. En la tabla de multiplicación de $\mathbb{Z}/5$ identifique las sucesivas potencias de 2.

2^1	2^2	2^3	2^4
2			

7. Reproduzca la tabla de multiplicación de $\mathbb{Z}/5$ según se indica.

$\times$	1	2	4	3
1				
2				
4				
3				

y compare con la tabla de adición de $\mathbb{Z}/4$.

+	0	1	2	3
0				
1				
2				
3				

Reporte todas sus observaciones.

8. Considere el par $(\mathbb{Z}, *)$ donde

$$m * n = m + n - 1.$$

Determine cuáles de las propiedades de grupo abeliano son satisfechas por este par. Note que en primera instancia debe verificarse que $*$ sea una operación binaria.

9. Considere el par $(\mathbb{Z}, *)$ donde

$$m * n = mn + 1.$$

Determine cuáles de las propiedades de grupo abeliano que son satisfechas por este par.

10. Demuestre que $(\mathbb{Z}/5)^*$ es un grupo abeliano, y que $(\mathbb{Z}/6)^*$ no tiene estructura de grupo.

3. Proposiciones

Si $(G, *)$ y $(H, \Box)$ son grupos y $\varphi : G \to H$ es una aplicación, decimos que φ es un *homomorfismo* de grupos si

$$\varphi(x * y) = \varphi(x) \Box \varphi(y)$$

para todos $x, y \in G$.

Denotemos por $\mathbb{R}_+$ al conjunto de los números reales positivos, y notemos que $(\mathbb{R}, +)$ y $(\mathbb{R}_+, \cdot)$ son ambos grupos abelianos. La función exponencial $\exp : \mathbb{R} \to \mathbb{R}_+$ dada por $\exp(t) = e^t$ es un buen ejemplo de homomorfismo de grupos, con dominio en un grupo aditivo y rango en un grupo multiplicativo.

$$e^{s+t} = e^s e^t$$

Un homomorfismo biyectivo se llama *isomorfismo*. Dos grupos G y H son *grupos isomorfos* si existe un isomorfiso $\varphi : G \to H$. Es fácil ver que la composición de isomorfismos es un isomorfismo. Un isomorfismo $\varphi : G \to G$ se dice que es un *automorfismo* de G.

Ejemplo 5 *La multiplicación por -1 define un automorfismo de $(\mathbb{Z}, +)$.*

Ejemplo 6 *Los grupos abelianos $(\mathbb{R}, +)$ y $(\mathbb{R}_+, \cdot)$ son isomorfos. La exponencial $\exp : \mathbb{R} \to \mathbb{R}_+$ es un isomorfismo posible. Otro isomorfismo posible está dado por $\exp(t) = e^{-t}$. Más generalmente, si a es un número real positivo, la aplicación $\alpha : \mathbb{R} \to \mathbb{R}_+$ dada por $\alpha(t) = a^t$ es un isomorfismo.*

Si $(G, *)$ es un grupo, $H \subseteq G$ y la restricción de $*$ a H hace de éste un grupo, decimos que $(H, *)$ es un *subgrupo* de $(G, *)$ ó simplemente que H es un subgrupo de G, lo que suele denotarse mediante $H < G$. Los *subgrupos triviales* de $(G, *)$ son él mismo y $(\{e\}, *)$.

Ejemplo 7 *Note que $(\mathbb{R}, +)$ no tiene subgrupos finitos no triviales, pero que $C_2 = \{-1, 1\}$ es un subgrupo finito de $(\mathbb{R}^*, \times)$.*

Dado un conjunto A, una aplicación $\eta : A \to A$ se dice que es una *involución* si la composición $\eta \circ \eta$ es la identidad en A. Notemos que una involución es necesariamente biyectiva y que es su propia aplicación inversa.

$$\begin{tikzcd} A \arrow[r, "\eta"] \arrow[dr, "1"'] & A \arrow[d, "\eta"] \\ & A \end{tikzcd}$$

Para una involución se tiene entonces que $\eta(\eta(a)) = a$ para todo $a \in A$.

Ejemplo 8 *Una función dada mediante el cambio de signo es una involución. En lógica, la negación es una involución.*

Una antinomia[2] conocida es la llamada "paradoja del mentiroso":

"Esta frase es falsa".

La veracidad de esta afirmación es indecidible, dado que conlleva una afirmación acerca de la proposición misma. Se hace necesario restringir esta posiblidad a través de la definición de una función de verdad. De esta forma, una *proposición* lo es siempre que sea posible y de forma única asignarle un valor de verdad. Como veremos más adelante, la función de verdad hace las veces de *axioma de regularidad* para la Lógica, lo que se conoce también como *principio de bivalencia*.

Una *función de verdad* sobre un conjunto A es una aplicación $v : A \to \mathbb{F}_2$. El *valor de verdad* de $a \in A$ se define como $v(a) \in \mathbb{F}_2$.

Una afirmación indecidible no es, en la terminología del presente texto, una proposición. Nos interesan las colecciones de objetos que tienen un valor de verdad, es decir, las colecciones de proposiciones.

Estas colecciones tienen una estructura algebraica de particular interés a las que llamaremos T-álgebras, nombre originado en la voz inglesa "true" cuyo significado es "verdadero". Otra denominación para para T-álgebra es la de *álgebra Booleana* ó *álgebra de Boole*[3].

Una *T-álgebra* es una cuaterna $(\mathcal{A}, \wedge, \neg, v)$ donde:

1. $\mathcal{A}$ es un conjunto no vacío.

[2]Paradoja sin solución.

[3]George Boole (1815,1864), matemático y filósofo británico, a quien se considera como el precursor de las Ciencias de la Computación. Su método de manipulación algebraica de la Lógica se desarrolla en su obra *An investigation of the Laws of Thought*, publicada en 1854.

2. $\wedge$ es una operación binaria asociativa y conmutativa sobre $\mathcal{A}$.

$$\wedge : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$$

3. $\neg$ es una involución.

$$\neg : \mathcal{A} \longrightarrow \mathcal{A}$$

4. v es una *función de verdad*, es decir, una aplicación

$$v : \mathcal{A} \longrightarrow \mathbb{F}_2$$

   tal que:

   a) $v(p \wedge q) = v(p) \cdot v(q)$ para todas $p, q \in \mathcal{A}$.

   b) $v(\neg p) = v(p) + 1$ para toda $p \in \mathcal{A}$.

La operación $\wedge$ se llama *conjunción*, y la involución $\neg$ se llama *negación*. Los elementos de $\mathcal{A}$ se llaman *proposiciones*, y se dice que $v(p) \in \mathbb{F}_2$ es el *valor de verdad* de la proposición $p \in \mathcal{A}$. La expresión $p \wedge q$ se lee "p y q", en tanto que la expresión $\neg p$ se lee "no p". Las *operaciones lógicas* definidas, así como la función de verdad constituyen la estructura de T-álgebra para el conjunto $\mathcal{A}$, por ello, si se da por conocida la estructura, tenemos la libertad de referirnos al conjunto $\mathcal{A}$ como la T-álgebra $\mathcal{A}$.

Si $v(p) = 1$ se dice que p es una *proposición verdadera*, y si $v(p) = 0$ se dice que p es una *proposición falsa*. La *tabla de verdad* de una proposición es un arreglo matricial de sus posibles valores de verdad.

Una operación lógica, es decir, una operación binaria

$$* : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$$

se dice que es *conmutativa*, si

$$v(p * q) = v(q * p)$$

para proposiciones cualesquiera $p, q \in \mathcal{A}$, de la misma manera, se dice que es *asociativa* si

$$v((p * q) * r) = v(p * (q * r))$$

para proposiciones cualesquiera $p, q, r \in \mathcal{A}$.

Equivalentemente, la operación lógica $*$ se dice conmutativa si $p * q$ y $q * p$ tienen tablas de verdad idénticas, y análogamente si la operación es asociativa.

Teorema 1 *La conjunción es una operación asociativa y conmutativa.*

Demostración. Estas propiedades se siguen como consecuencia inmediata de que la multiplicación es asociativa y conmutativa en el campo $\mathbb{F}_2$. ∎

Teorema 2 *La negación es una involución.*

Demostración. Dado que $1+1=0$ en $\mathbb{F}_2$, entonces

$$v(\neg(\neg p)) = v(\neg p) + 1 = v(p)$$

para toda $p \in \mathcal{A}$. ∎

Claramente $x + x = 0$ y $x^2 = x$ para todo $x \in \mathbb{F}_2$, ó dicho técnicamente, los elementos de $\mathbb{F}_2$ tienen 2-*torsión* y son *idempotentes* bajo el producto.

Teorema 3 *Toda proposición es idempotente bajo la conjunción.*

Demostración. Es suficiente notar que para toda $p \in \mathcal{A}$ se satisface

$$v(p \wedge p) = v(p)^2 = v(p),$$

dado que $v(p) \in \mathbb{F}_2$. ∎

Cuaderno de Ejercicios no. 2

1. Demuestre que el par $(\mathbb{R}^*, \times)$ es un grupo abeliano. Demuestre que $\varphi : \mathbb{R}^* \to \mathbb{R}^*$, dada por $\varphi(x) = |x|$ es un homomorfismo de grupos, pero que no es un automorfismo.

2. Encuentre un isomorfismo entre $\mathbb{Z}/2$ y $(\mathbb{Z}/3)^*$. Construya las tablas correspondientes.

3. Observe que $C_2 = \{-1, 1\}$ es un subgrupo multiplicativo de $\mathbb{R}^*$, y encuentre un isomorfismo entre $\mathbb{Z}/2$ y C_2. Construya la tabla de multiplicación de C_2.

4. La *función signo* $\sigma : \mathbb{R}^* \to C_2$ se define mediante

$$\sigma(x) = \frac{x}{|x|}.$$

Demuestre que la función signo es un homomorfismo de grupos.

5. Construya la tabla de verdad de la negación, usando la expresión

$$v(\neg p) = v(p) + 1$$

en la definición de función de verdad.

p	$\neg p$
1	
0	

6. Construya la tabla de verdad de la conjunción, usando la expresión

$$v(p \wedge q) = v(p)v(q)$$

en la definición de función de verdad.

p	q	$p \wedge q$
1	1	
1	0	
0	1	
0	0	

7. Construya la tabla de verdad de la proposición $(\neg p) \wedge q$, calculando en primera instancia una expresión para su valor de verdad.

$$v((\neg p) \wedge q))$$

p	q	$\neg p$	$(\neg p) \wedge q$
1	1		
1	0		
0	1		
0	0		

8. Construya la tabla de verdad de la proposición $(\neg p) \wedge (\neg q)$, calculando en primera instancia una expresión para su valor de verdad.

$$v((\neg p) \wedge (\neg q))$$

p	q	$\neg p$	$\neg q$	$(\neg p) \wedge (\neg q)$
1	1			
1	0			
0	1			
0	0			

4. Proposiciones compuestas

Dadas dos proposiciones p y q en una T-álgebra $\mathcal{A}$, la expresión $p \equiv q$ significa que p y q son *proposiciones equivalentes*, es decir, que son esencialmente la misma proposición. Dos proposiciones equivalentes tienen el mismo valor de verdad, es decir, tienen tablas de verdad idénticas.

Ejemplo 9 *La afirmación de que la conjunción es asociativa y conmutativa se expresa de forma simbólica mediante las expresiones*

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$$

y

$$p \wedge q \equiv q \wedge p$$

respectivamente.

Ejemplo 10 *La negación es una involución, es decir,*

$$(\neg(\neg p) \equiv p$$

para toda $p \in \mathcal{A}$*.*

La operación binaria

$$\vee : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$$

dada mediante

$$p \vee q \equiv \neg((\neg p) \wedge (\neg q))$$

se llama *disyunción*. La expresión $p \vee q$ se lee "p ó q".

Teorema 4 *El valor de verdad de la disyunción está dado por*

$$v(p \vee q) = v(p)v(q) + v(p) + v(q)$$

para cualesquiera $p, q \in \mathcal{A}$*.*

Demostración. Notando primero que

$$v((\neg p) \wedge (\neg q)) = (v(p) + 1)(v(q) + 1)) = v(p)v(q) + v(p) + v(q) + 1$$

se obtiene la conclusión de inmediato. ■

Los resultados siguientes se obtienen como consecuencia del teorema previo.

Corolario 5 *La disyunción es conmutativa.*

Demostración. Basta observar que tanto la adición como la multiplicaón son conmutativas en $\mathbb{F}_2$. $\blacksquare$

Teorema 6 *La disyunción es asociativa.*

Demostración. Sean p, q, r proposiciones cualesquiera, entonces

$$v((p \vee q) \vee r) = [v(p)v(q) + v(p) + v(q)]v(r) + v(p)v(q) + v(p) + v(q) + v(r),$$

de manera que, factorizando en $\mathbb{F}_2$, tenemos

$$v((p \vee q) \vee r) = [v(p) + 1][v(q) + 1][v(r) + 1].$$

Por otra parte,

$$v(p \vee (q \vee r)) = [v(q)v(r) + v(q) + v(r)]v(p) + v(q)v(r) + v(q) + v(r) + v(p),$$

de donde

$$v((p \vee q) \vee r) = [v(q) + 1][v(r) + 1][v(p) + 1],$$

con lo que se concluye la demostración. $\blacksquare$

La operación binaria

$$\Rightarrow : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$$

dada mediante

$$p \Rightarrow q \equiv (\neg p) \vee q$$

se llama *condicional*. La expresión $p \Rightarrow q$ se lee "si p, entonces q" o bien "p implica q". La afirmación contenida en la proposición $p \Rightarrow q$ es que "p es una *condición suficiente* para la ocurrencia de q" o bien que, equivalentemente, "q es una *consecuencia necesaria* de p".

Teorema 7 *El valor de verdad de la condicional está dada por*

$$v(p \Rightarrow q) = v(p)v(q) + v(p) + 1$$

para $p, q \in \mathbb{F}_2$.

Demostración. El cálculo de

$$v((\neg p) \vee q) = (v(p) + 1)(v(q) + 1) + v(q)$$

muestra claramente la veracidad de la afirmación. ■

La definición de $p \Rightarrow q$ no es simétrica en p y q, lo que se observa con transparencia en el cálculo de su valor de verdad, en consecuencia, la condicional es una operación binaria, pero claramente no es conmutativa. De la misma manera, la condicional no es asociativa, y la demostración del hecho se deja como ejercicio para el lector.

Teorema 8 *La equivalencia*

$$p \Rightarrow q \equiv \neg(p \wedge (\neg q))$$

se satisface para cualesquiera p y q en $\mathcal{A}$.

Demostración. Basta observar que, como $v(p \wedge (\neg q)) = v(p)[v(q) + 1]$, entonces

$$v(p \Rightarrow q) = v(p)[v(q) + 1] + 1 = (v(p) + 1)(v(q) + 1) + v(q),$$

dado que $v(q) + v(q) = 0$. ■

La *disyunción exclusiva* de dos proposiciones $p, q \in \mathcal{A}$ se define mediante

$$p \dot{\vee} q \equiv (p \wedge q) \vee [(\neg p) \wedge (\neg q)]$$

que coloquialmente se interpreta como " o bien p o bien q", que se satisface si el valor de verdad de exactamente una de las proposiciones es 1. La disyunción suele ser también llamada *disyunción inclusiva*.

Dado que el producto de valores de verdad es el valor de verdad de la conjunción, entonces, del ejercicio se sigue que $p \wedge p \equiv p$, para toda $p \in \mathcal{A}$. Además también $p \vee p \equiv p$, lo que se sigue inmediatamente de que

$$v(p)^2 + v(p) + v(p) = v(p).$$

Teorema 9 *El valor de verdad de la disyunción exclusiva está dado por*

$$v(p \dot{\vee} q) = v(p) + v(q)$$

para cualesquiera $p, q \in \mathcal{A}$.

Demostración. Usando la definición tenemos

$$\begin{aligned}
v(p \dot{\vee} q) &= v(p)v(q)(v(p)+1)(v(q)+1) + v(p)v(q) + (v(p)+1)(v(q)+1) + 1 \\
&= v(p)v(q)(v(p)+1)(v(q)+1) + v(p) + v(q) \\
&= v(p)^2v(q)^2 + v(p)^2v(q) + v(p)v(q)^2 + v(p)v(q) + v(p) + v(q) \\
&= v(p)v(q) + v(p)v(q) + v(p)v(q) + v(p)v(q) + v(p) + v(q) \\
&= v(p) + v(q)
\end{aligned}$$

como se quería demostrar. ■

De acuerdo con el ejercicio anterior, y el hecho ya demostrado de que $v(p) + v(p) = 0$, el valor de verdad de la fórmula $p \dot{\vee} p$ es siempre cero, de manera que la fórmula es una contradicción, es decir, una proposición compuesta necesariamente falsa.

El bicondicional de dos proposiciones p y q se define mediante

$$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p),$$

y la expresión $p \Leftrightarrow q$ se lee "p si y sólo si q".

Teorema 10 *Si $p, q \in \mathcal{A}$, entonces*

$$v(p \Leftrightarrow q) = v(p) + v(q) + 1.$$

Demostración. Basta simplificar el producto

$$[v(p)v(q) + v(p) + 1][v(p)v(q) + v(q) + 1]$$

sobre $\mathbb{F}_2$. ■

El cálculo de la función de verdad evaluada en la bicondicional, recupera un hecho avalado por la intuición: es verdadera cuando tanto p como q tienen el mismo valor de verdad.

El siguiente resultado se conoce como la *ley de contraposición*, y es el fundamento lógico de las demostraciones por contradicción, conocidas también como por *reducción al absurdo*.

Teorema 11 *La equivalencia*

$$p \Rightarrow q \equiv [(\neg q) \Rightarrow (\neg p)]$$

se satisface para cualesquiera $p, q \in \mathcal{A}$.

Demostración. Basta calcular el valor de verdad del miembro derecho, y notamos que

$$v(\neg q)v(\neg p) + v(\neg q) + 1 = (v(q) + 1)(v(p) + 1) + v(q) = v(p)v(q) + v(p) + 1,$$

como se quería demostrar. ■

Los dos resultados siguientes muestran que el comportamiento de los conectivos lógicos entre sí es bastante peculiar.

Teorema 12 *La conjunción se distribuye respecto de la disyunción, es decir,*

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

para elementos arbitrarios de una T-álgebra $p, q, r \in \mathcal{A}$.□

Teorema 13 *La disyunción se distribuye respecto de la conjunción, es decir, que*

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

para elementos arbitrarios de una T-álgebra $p, q, r \in \mathcal{A}$.□

Las demostraciones de ambos hechos se consideran ejercicios.

Una proposición compuesta cuyo valor de verdad es 1 con independencia de los valores de verdad de cada una de las proposiciones que la componen se llama *tautología*. En contraparte, una proposición compuesta cuyo valor de verdad es 0 con independencia de los valores de verdad de cada una de las proposiciones que la componen se llama *contradicción*. En lenguaje coloquial, una tautología es siempre verdadera y una contradicción es siempre falsa. Con frecuencia una proposición compuesta recibe el nombre de *fórmula* o bien fórmula lógica.

El ejemplo típico de tautología es la fórmula $p \vee (\neg p)$, dado que su valor de verdad es necesariamente 1, como se observa en el cálculo de su valor de verdad.

$$\begin{aligned} v(p \vee (\neg p)) &= v(p)v(\neg p) + v(p) + v(\neg p) \\ &= v(p)[v(p) + 1] + v(p) + v(p) + 1 \\ &= v(p)^2 + v(p) + 1 \\ &= v(p) + v(p) + 1 \\ &= 1 \end{aligned}$$

Por otra parte, el ejemplo clásico de contradicción lo encontramos en la fórmula $p \wedge (\neg p)$, como vemos en el cálculo que sigue.

$$\begin{aligned} v(p \wedge (\neg p)) &= v(p)v(\neg p) \\ &= v(p)[v(p)+1] \\ &= v(p)^2 + v(p) \\ &= v(p) + v(p) \\ &= 0 \end{aligned}$$

Cuaderno de Ejercicios no. 3

1. Construya la tabla de verdad de la disyunción, usando la función de verdad correspondiente.

p	q	$p \vee q$
1	1	
1	0	
0	1	
0	0	

2. Demuestre la distributividad de la conjunción respecto de la disyunción, es decir, que
$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$
para proposiciones arbitrarias $p, q, r \in \mathcal{A}$. Calcule el valor de verdad de cada uno de los miembros y use el resultado para construir las tablas de verdad correspondientes.

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
1	1	1					
1	1	0					
1	0	1					
1	0	0					
0	1	1					
0	1	0					
0	0	1					
0	0	0					

3. Demuestre la distributividad de la disyunción respecto de la conjunción, es decir, que
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$
para proposiciones arbitrarias $p, q, r \in \mathcal{A}$. Calcule el valor de verdad de cada uno de los miembros y use el resultado para construir las tablas de verdad correspondientes.

p	q	r	$q \vee r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
1	1	1					
1	1	0					
1	0	1					
1	0	0					
0	1	1					
0	1	0					
0	0	1					
0	0	0					

4. Calcule la función de verdad evaluada en la proposición $(\neg p) \vee q$, y construya la tabla de verdad correspondiente.

p	q	$\neg p$	$(\neg p) \vee q$
1	1		
1	0		
0	1		
0	0		

5. Calcule la función de verdad evaluada en la proposición $(\neg p) \vee (\neg q)$, y construya la tabla de verdad correspondiente.

p	q	$\neg p$	$\neg q$	$(\neg p) \vee (\neg q)$
1	1			
1	0			
0	1			
0	0			

6. Construya la tabla de verdad de la condicional $p \Rightarrow q$, usando la función de verdad evaluada en ella.

p	q	$p \Rightarrow q$
1	1	
1	0	
0	1	
0	0	

7. Calcule la función de verdad evaluada en la proposición $\neg(p \wedge (\neg q))$, y construya la tabla de verdad correspondiente.

p	q	$\neg q$	$p \wedge (\neg q)$	$\neg(p \wedge (\neg q))$
1	1			
1	0			
0	1			
0	0			

8. Demuestre que la condicional no es conmutativa, evaluando la función de verdad en $p \Rightarrow q$ y en $q \Rightarrow p$.

9. Demuestre que la condicional no es asociativa, evaluando la función de verdad en $p \Rightarrow (q \Rightarrow r)$ y en $(p \Rightarrow q) \Rightarrow r$.

10. Demuestre que la fórmula $(p \Rightarrow q) \vee p$ es una tautología. Evalúe la función de verdad y construya la tabla de verdad.

p	q	$p \Rightarrow q)$	$(p \Rightarrow q) \vee p$
1	1		
1	0		
0	1		
0	0		

11. Demuestre que la fórmula $[p \wedge (\neg q)] \Rightarrow p$ es una tautología. Evalúe la función de verdad y construya la tabla de verdad.

p	q	$\neg q$	$p \wedge (\neg q)$	$[p \wedge (\neg q)] \Rightarrow p$
1	1			
1	0			
0	1			
0	0			

12. Demuestre que la fórmula $[(p \Rightarrow q) \wedge p] \wedge [(p \Rightarrow q) \wedge (\neg q)]$ es una contradicción. Evalúe la función de verdad y construya la tabla de verdad.

p	q	$(\neg p) \wedge q$	$[(p \Rightarrow q) \wedge p] \wedge [(p \Rightarrow q) \wedge (\neg q)]$
1	1		
1	0		
0	1		
0	0		

13. Demuestre que la fórmula $[(\neg p) \vee q] \wedge (p \wedge (\neg q)]$ es una contradicción. Evalúe la función de verdad y construya la tabla de verdad.

p	q	$(\neg p) \wedge q$	$p \wedge (\neg q)$	$[(\neg p) \vee q] \wedge (p \wedge (\neg q)]$
1	1			
1	0			
0	1			
0	0			

5. Funciones proposicionales

Una función proposicional sobre un conjunto $X \neq \varnothing$ es una aplicación

$$f : X \longrightarrow \mathcal{A}$$

donde $\mathcal{A}$ es una T-álgebra, es decir si $x \in X$ se tiene que $f(x)$ es una proposición.

Los cuantificadores universales constituyen afirmaciones acerca de las condiciones bajo las cuales una función proposicional admite un valor de verdad dado. Los cuantificadores son básicamente dos, a saber: el cuantificador universal y el cuantificador existencial.

En otras palabras, dada una función proposicional f, los cuantificadores son afirmaciones acerca de la imagen de la composición $v \circ f$ donde v es la función de verdad de la T-álgebra considerada.

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, "v\circ f"'] & \mathcal{A} \arrow[d, "v"] \\
& \mathbb{F}_2
\end{tikzcd}$$

La expresión $\forall x(f(x))$ que se lee "para todo x se verifica $f(x)$" es una proposición equivalente con la afirmación de que $\{1\} = \mathrm{im}(v \circ f)$ o bien que $0 \notin \mathrm{im}(v \circ f)$. El significado coloquial es que el todos los elementos $x \in X$ hacen verdadera la función proposicional f.

$$\forall x(f(x)) \equiv \{1\} = \mathrm{im}(v \circ f)$$

El símbolo "$\forall$" se conoce como *cuantificador universal*. Dado que el dominio de nuestras funciones proposicionales es una clase dada X, en realidad, la expresión universal se escribe más propiamente como $\forall x \in X(f(x))$.

Ejemplo 11 *La expresión "todos los gatos son pardos" es una proposición universal, que atribuye una propiedad, en este caso el color, a todos los elementos de una colección dada. Si G representa la clase de los gatos, p la propiedad de "ser pardo", entonces, la proposición dada puede escribirse simbólicamente como sigue:*

$$\forall x \in G(p(x)).$$

Una equivalencia interesante de la proposición universal es entonces la siguiente:

$$\forall x \in X(f(x)) \equiv (x \in X \Rightarrow f(x)).$$

Tenemos entonces que el cuantificador universal no es sino una forma funcional de la condicional.

Ejemplo 12 *La proposición "todo número natural en entero", puede escribirse como* $\forall x \in \mathbb{N}(x \in \mathbb{Z})$*, o equivalentemente como* $x \in \mathbb{N} \Rightarrow x \in \mathbb{Z}$*.*

La expresión $\exists x(f(x))$ se lee "existe un x tal que $f(x)$" es una proposición equivalente $\{1\} \in \mathrm{im}(v \circ f)$ o bien que $\mathrm{im}(v \circ f) \neq \{0\}$. El significado coloquial es que el menos un elemento $x \in X$ hace verdadera la función proposicional f.

$$\exists x(f(x)) \equiv 1 \in \mathrm{im}(v \circ f)$$

El símbolo "$\exists$" se conoce como *cuantificador existencial.*

Los cuantificadores se relacionan de manera muy natural mediante

$$\neg[\forall x(f(x)] \equiv \exists x[\neg f(x)]$$

y

$$\neg[\exists x(f(x)] \equiv \forall x[\neg f(x)].$$

En consecuencia, la equivalencia del cuantificador existencial en términos del universal tiene la siguiente forma:

$$\exists x(f(x) \equiv \neg[\forall x(\neg f(x))],$$

es decir, si el dominio de nuestra función proposicional es la clase X:

$$\exists x \in X(f(x) \equiv \neg[x \in X \Rightarrow (\neg f(x)].$$

El lector no tendrá dificultad para encontrar otras equivalencias interesantes.

Ejemplo 13 *Una expresión como "Ernesto Domínguez tiene al menos un ancestro" es una proposición existencial, se invita al lector a encontrar una expresión simbólica para ella.*

Ejemplo 14 *La afirmación "5 tiene al menos una raíz cuadrada real" tiene la siguiente expresión simbólica:*

$$\exists x \in \mathbb{R}(x^2 = 5).$$

Un uso conjunto de los cuantificadores se ilustra enseguida.

Ejemplo 15 *La propiedad arquimediana de los números reales afirma que dado un número real dado, siempre es posible encontrar un entero mayor que él. Simbólicamente*

$$\forall x \in \mathbb{R}(\exists n \in \mathbb{Z}(x < n)).$$

En Lógica se impone un uso cuidadoso de las expresiones, para que las conclusiones que se obtengan sean rigurosamente correctas. Frases como "no todos los políticos son corruptos" y "todos los políticos no son corruptos", tienen significados opuestos, y sin embargo suelen ser usadas coloquialmente como equivalentes. La primera significa que existe al menos un político que no es corrupto, es decir, se ajusta al uso del cuantificador existencial. La segunda, por su parte, significa que ningún político es corrupto, por lo que se ajusta al uso del cuantificador universal.

Las formas simbólicas de estas dos frases serían

$$\neg(\forall x \in P(x \in C)) \quad \text{y} \quad \forall x \in P(x \notin C)$$

respectivamente, si P es la clase de los políticos, y C la clase de las personas corruptas..

Un conectivo lógico que hasta ahora hemos usado de forma implícita es "$\cdot \ni \cdot$" que se lee "tal que", y que puede ser usado para simplificar la interpretación de algunas expresiones lógicas. Las formas generales de los cuantificadores adquieren entonces las formas simbólicas como:

$$\forall x(\exists y \cdot \ni \cdot f(x, y)).$$

La proposiciones en matemáticas tienen que ver con la existencia de objetos con alguna propiedad en particular, y frecuentemente, la unicidad de la existencia es también un ingrediente importante. Por ello, resulta de utilidad el uso de un cuantificador de *existencia y unicidad*. La expresión $\exists! x(f(x)$ se lee "existe un único x tal que $f(x)$", el significado es que existe un elemento $x \in X$ para el cual $f(x)$ es verdadero y además es el único para el que tal cosa ocurre.

$$\exists! x(f(x)) \equiv \#\{x \in X | f(x)\} = 1$$

Ejemplo 16 *La expresión coloquial "madre sólo hay una" es un buen ejemplo de proposición de existencia y unicidad.*

Ejemplo 17 *Todo grupo tiene un elemento neutro, y el elemento neutro en un grupo es único.*

$$\exists! e \in G(\forall x \in G(xe = x = e * x)).$$

Ejemplo 18 *En un grupo todo elemento tiene un único inverso.*

$$\forall x \in G(\exists! y \in G(xy = e = y * x)).$$

Cuaderno de Ejercicios no. 4

1. Considere la función proposicional dada por $f(x) \equiv (x|77)$. Determine el valor de verdad de $f(11)$, $f(3)$, $f(1)$, $\forall n \in \mathbb{N}(f(n))$ y $\exists n \in \mathbb{N}(f(n))$.

2. Demuestre la siguiente equivalencia.

$$\exists! x_0(f(x_0)) \equiv f(x_0) \wedge [\forall x \neq x_0(\neg f(x)]$$

3. Determine el valor de verdad de cada una de las siguientes proposiciones.

   a) $\forall x \in \mathbb{R}(x^2 > x)$.
   b) $\exists! x \in \mathbb{R}(x = -x)$.
   c) $\exists x \in \mathbb{R}(x^2 < 0)$.
   d) $\exists x \in \mathbb{R}(x^2 > 0)$.
   e) $\forall x \in \mathbb{R}(x^2 < 0)$.
   f) $\forall x \in \mathbb{R}(x > 1 \Rightarrow x^2 > x)$.
   g) $\exists x \in \mathbb{R}(x > 1 \Rightarrow x^2 > x)$.
   h) $\forall x \in \mathbb{R}\left(x > 1 \Rightarrow \frac{x}{x^2+1} < \frac{1}{3}\right)$.
   i) $\exists x \in \mathbb{R}\left(x > 1 \Rightarrow \frac{x}{x^2+1} < \frac{1}{3}\right)$.

4. Escriba la negación de cada una de las proposiciones del ejercicio anterior y determine su valor de verdad.

   a)
   b)
   c)
   d)
   e)
   f)
   g)
   h)
   i)

5. Determine el valor de verdad de cada una de las siguientes proposiciones.

   a) $\forall x \in \mathbb{R}(1 + 4 = 5)$.
   b) $\exists x \in \mathbb{R}(1 + 4 = 5)$.
   c) $\exists! x \in \mathbb{R}(1 + 4 = 5)$.

6. Escriba la negación de cada una de las proposiciones del ejercicio anterior y determine su valor de verdad.

   a)
   b)
   c)

7. Determine el valor de verdad de cada una de las siguientes proposiciones.

   a) $\forall n \in \mathbb{N}(2^n + 1 \text{ es primo})$.
   b) $\exists n \in \mathbb{R}(2^n + 1 \text{ es primo})$.
   c) $\exists! n \in \mathbb{R}(2^n + 1 \text{ es primo})$.

8. Escriba la negación de cada una de las proposiciones del ejercicio anterior y determine su valor de verdad.

   a)
   b)
   c)

6. Conjuntos, extensión y vacío

La segunda parte de este material inicia con una exposición breve de la Teoría Cantoriana de los Conjuntos, que una vez formalizada por el sistema axiomático de Zermelo-Fraenkel recibe la denominación de sistema axiomático de Zermelo[4]-Fraenkel[5]-Cantor[6] que es básicamente, la presentación formal de la noción de conjunto que manejamos de forma cotidiana e intuitiva. El sistema de postulados que presentamos en lo que sigue revela que tras la noción ordinaria de conjunto se oculta la suprema belleza de una Teoría que aporta solidez a la matemática conocida.

Como observaremos, el sistema axiomático que expondremos dista mucho de representar la última palabra en lo que se refiere a la sistematización de los conjuntos, pues el axioma que la hace Cantoriana, el axioma de elección tan intuitivamente diáfano, conduce a paradojas como la de Banach-Tarski que golpean la intuición de forma contundente. Estas limitaciones parecen aún lejos de ser superadas, por lo que hasta el momento, este sistema de axiomas es el mejor marco con el que contamos para el estudio y el uso de los conjuntos.

Un conjunto es un objeto de naturaleza estrictamente matemática, de manera que cuando se habla de conjuntos de números, por ejemplo, entendemos que los números pueden ser entendidos como una clase particular de conjuntos. En última instancia todos los objetos de las matemáticas son conjuntos para la Teoría de los Conjuntos. No existe nada en el contexto de las matemáticas como un conjunto de casas o de personas, aunque una colección de casas puede “identificarse” con un conjunto abstracto, como por ejemplo,

[4]Ernst Friedrich Ferdinand Zermelo (1871 - 1953), matemático y filósofo alemán. En 1902 publicó su primer trabajo sobre la adición de cardinales transfinitos, y en 1904, dio con éxito el primer paso sugerido por Hilbert para la hipótesis del continuo, cuando demostró el teorema del buen orden: “todo conjunto puede ser bien ordenado”. En 1908 publicó la primera versión de la axiomática conjuntista. El teorema de Zermelo es equivalente con el axioma de elección.

[5]Adolf Abraham Halevi Fraenkel (1891 - 1965) matemático alemán. Publicó en 1922 la versión actual de la axiomática conjuntista, complementando el trabajo previo de Zermelo.

[6]Georg Ferdinand Ludwig Philipp Cantor (1845 - 1918), matemático alemán, desarrolló en colaboración con sus compatriotas Julius Wilheim Richard Dedekind (1831 - 1916) y Friedrich Ludwig Gottlob Frege (1848 - 1925) la Teoría de Conjuntos. Sus trabajos de investigación sobre los conjuntos infinitos lo condujeron a formalizar la noción de infinito bajo la forma de los números transfinitos, por medio de la teoría de ordinales y cardinales.

cuando a una casa se le asigna un número que la distingue en su calle.

Un "conjunto de casas" es una forma abreviada de expresar que la colección de inmuebles dada se ha "identificado" con un conjunto matemático. Un conjunto es un modelo, que en este caso, se ajusta a la situación práctica a la que específicamente nos enfrentamos.

Informalmente diremos que todo *conjunto* es una *colección* pero no toda colección es un conjunto. En otras palabras, no basta con pronunciar palabras mágicas para que se produzca la existencia de un conjunto, la descripción de sus elementos debe ser precisa e inequívoca. Consideremos como ejemplo la paradoja del barbero: En una cierta población cerrada hay hombres barbados y un barbero; hay dos clases de hombres barbados sin elementos comunes, los que se afeitan a sí mismos, además de los que son afeitados por el barbero, y habrá que decidir a cuál de las dos colecciones pertenece el barbero. Por supuesto esta colecciones no pueden ser consideradas conjuntos, dado que aportan incertidumbre acerca de la pertenecia o no de un elemento particular.

Las paradojas[7] y antinomias[8] producidas por la ausencia de formalización de la Teoría Cantoriana de los conjuntos plantearon la necesidad de axiomatizarla, problema que se resuelve finalmente con la *axiomática de Zermelo-Fraenkel* que exponemos a continuación de manera sucinta. En ella consideramos la *noción de pertenencia* como noción primitiva la cual se expresa mediante la notación $x \in A$, que significa que *x es un elemento de A* o equivalentemente que *x pertenece a* la colección A. A los nueve axiomas de Zermelo-Fraenkel se incorpora el *axioma de elección*, lo que caracteriza la Teoría de Conjuntos de Cantor, con lo que la axiomática que exponemos a continuación se conoce como el *sistema axiomático de Zermelo-Fraenkel-Cantor* (ZFC)[9].

Axioma 1 *Axioma de Extensión.* Dos conjuntos son iguales si y sólo si tienen exactamente los mismos elementos.

Dados dos conjuntos A y B decimos que A es un *subconjunto* de B si $x \in B$ para todo $x \in A$. Esta relación de *inclusión* se denota mediante

[7]Una *paradoja* es un razonamiento que conlleva una contradicción lógica. De acuerdo con su etimología, es una idea que contradice el sentido común.

[8]Una *antinomia* es una paradoja irresoluble. Etimológicamente, significa "contra la regla".

[9]Usualmente se interpreta "ZFC" como la axiomática de Zermelo-Fraenkel con el axioma de elección (choice), adoptamos la terminología indicada bajo la consideración de que el axioma de elección es básicamente una aportación de Cantor.

$A \subseteq B$. Básicamente el axioma de estensión afirma que $A = B$ si y sólo si $A \subseteq B$ y $B \subseteq A$.

De forma coloquial, el axioma de extensión afirma que un conjunto queda determinado por sus elementos. Si $A \subseteq B$ y $A \neq B$, decimos que A es un *subconjunto propio* de B, lo que denotamos mediante $A \subset B$.

Axioma 2 *Axioma del conjunto vacío.* Existe un conjunto que no tiene elementos, al que denotamos por $\varnothing$.

Este segundo axioma es particularmente importante, puesto que indica que la Teoría de conjuntos no se construye ociosamente, en el sentido de que al menos existe un objeto al que puede aplicarse, lo que proporciona sentido al sistema teórico de que nos ocupamos.

Teorema 14 *Si A es un conjunto, entonces $\varnothing \subseteq A$.*

Demostración. Supongamos que $\varnothing \nsubseteq A$, entonces $x \notin A$ para algún $x \in \varnothing$, pero por el axioma del conjunto vacío se tiene que $x \notin \varnothing$ para todo conjunto x. ■

Decimos que el resultado anterior se verifica *por vacuidad*, es decir, porque no hay elementos que satisfagan la propiedad opuesta. Tenemos entonces que el conjunto vacío es un subconjunto de cualquier otro conjunto, el resultado, sin embargo, carece de significado mientras que el conjunto vacío sea el único conjunto visible.

Ciertamente, puede ser un poco desconcertante que el único conjunto de cuya existencia tenemos certeza es un conjunto sin elementos, puesto que intuitivamente pensamos en un conjunto como algo que se caracteriza por poseerlos, sin embargo, el desconcierto puede encontrar algún alivio ante la posibilidad de construir $\{\varnothing\}$ que es un conjunto que tiene un elemento.

Axioma 3 *Axioma de Apareamiento.* Dados dos conjuntos A y B, la colección $\{A, B\}$ es un conjunto.

Se abre, por otra parte, la posibilidad de construir una colección infinita de conjuntos de acuerdo con el resultado siguiente.

Teorema 15 *Existen por lo menos dos conjuntos distintos.*

Demostración. Como hemos visto, el axioma de apareamiento garantiza la existencia de $\{\varnothing\}$, y por el resultado anterior $\varnothing \subseteq \{\varnothing\}$. Ahora bien, $\{\varnothing\} \nsubseteq \varnothing$ porque $\varnothing \notin \varnothing$. ■

Se tiene ya garantizada la existencia de al menos dos conjuntos distintos a y b, un uso reiterado del axioma de apareamiento nos garantiza la existencia de los conjuntos $(a, b) = \{\{a\}, \{a, b\}\}$ y $(b, a) = \{\{b\}, \{a, b\}\}$, a los que llamaremos *pares ordenados*.

Teorema 16 *Se satisface que $a \neq b$ si y sólo si $(a, b) \neq (b, a)$.*

Demostración. Si $a \neq b$ los conjuntos $\{a\}$, $\{b\}$, y $\{a, b\}$ son mutuamente distintos. Recíprocamente, si $(a, b) \neq (b, a)$, entonces $\{a\} \neq \{b\}$, de donde, por el axioma de extensión, $a \neq b$. ■

Esta definición de pares ordenados se debe a Kazimierz Kuratowski[10], y fue popularizada por Paul Halmos[11],y puede ser encontrada en su bello texto *Naive set theory*[12]. Un pequeño problema que impide la generalización, inmediata y mecánica, de esta noción de orden, es que $\{\{a\}\} = (a, a)$. Procediendo entonces de forma análoga al definir $(a, b, c) = \{\{a\}, \{a, b\}, \{a, b, c\}\}$ no sería posible distinguir entre (a, a) y (a, a, a), más aún, no distinguiríamos entre (a, b, b) y (a, a, b). Esta formalización del orden es, no obstante, factible de ser generalizada, y se invita al lector a proponer una generalización aceptable.

Claramente podemos hacer $A = \varnothing = 0$ y $B = \varnothing = 0$ para construir $1 = \{\varnothing\}$, además de que $A = \varnothing$ y $B = \{\varnothing\}$ posibilita la construcción de $2 = \{\varnothing, \{\varnothing\}\}$. La construcción del resto de los números naturales es una tarea que requiere del axioma próximo.

Axioma 4 *Axioma de la Unión.* Dado un conjunto A, existe un conjunto B cuyos elementos son precisamente los elementos de los elementos de A.

[10]Kazimierz Kuratowski (1896 - 1980), matemático polaco, representante de la corriente conocida como La Escuela de Varsovia.

[11]Paul Richard Halmos (1916 - 2006), matemático húngaro nacionalizado norteamericano.

[12]Publicado originalmente por Van Nostrand en 1960. Hay una versión castellana publicada por la desparecida editorial CECSA en 1965, bajo el título *Teoría Intuitiva de los Conjuntos*, y una reimpresión del original publicada por Springer Verlag en 1974.

La notación usual es $B = \cup A$. Si tenemos el caso $A = \{x, y\}$, entonces $B = x \cup y$, y en general, si $A = \{x_\alpha | \alpha \in \mathcal{A}\}$, entonces escribimos $B = \cup A$ o de manera más descriptiva:

$$B = \bigcup_{\alpha \in \mathcal{A}} x_\alpha.$$

Continuando con el ejemplo de la construcción de los números naturales, suponiendo inductivamente que hemos construido el número natural n, entonces, haciendo uso del axioma de apareamiento contruimos $\{n\}$ y $\{n, \{n\}\}$. Finalmente, mediante al auxilio del axioma de la unión arribamos a $n + 1 = n \cup \{n\}$. Tenemos entonces que $n + 1 = \{0, 1, \ldots, n\}$.

El axioma anterior garantiza la existencia de la unión de una colección dada de conjuntos, a condición de que la colección misma sea también un conjunto, como veremos con posterioridad, no toda colección es un conjunto. Una consecuencia inmediata es que para dos conjuntos cualesquiera x, y, existe el conjunto $x \cup y$.

$$x \cup y = \{a | a \in x \vee a \in y\}$$

Debe notarse no obstante que el axioma no garantiza la unicidad de la unión. No tenemos entonces la existencia de "la unión" de un conjunto, el postulado nos dice que existe al menos "una unión" de un conjunto. Se pide en los ejercicios, demostrar que existe a lo sumo una, con lo que tendremos existencia y unicidad.

Cuaderno de Ejercicios no. 5

1. Demuestre que existen al menos tres conjuntos distintos.
2. Exprese $A \subseteq B$ en términos de conectivos lógicos.
3. Demuestre que para conjuntos dados A y B necesariamente se cumple que $A \subseteq A \cup B$.
4. Demuestre que $\{\varnothing\} \nsubseteq \{\{\varnothing\}\}$.
5. Demuestre que $A \subseteq B$ si y sólo si $A \cup B = B$.
6. Demuestre que $A \cup \varnothing = A$ para todo conjunto A.
7. Demuestre la conmutatividad de la unión, es decir, que si A y B son conjuntos, entonces $A \cup B = B \cup A$.
8. Demuestre la asociatividad de la unión, es decir, que si A, B y C son conjuntos, entonces $A \cup (B \cup C) = (A \cup B) \cup C$.
9. Demuestre que $x = y$ si y sólo si (x, y) es un conjunto con un único elemento.
10. Demuestre que la unión $\cup A$ de un conjunto dado A es única.
11. Demuestre que
$$\bigcup_{\alpha \in \mathcal{A}} A_\alpha = \varnothing$$
si y sólo si $A_\alpha = \varnothing$ para todo $\alpha \in \mathcal{A}$.

7. Separación e intersección

El siguiente grupo de axiomas garantiza la existencia de los conjuntos inductivos, en particular, de los ordinales, y más específicamente de los números naturales.

Axioma 5 *Axioma de Infinitud.* Existe un conjunto $\mathcal{N}$ tal que si $\varnothing \in \mathcal{N}$ y $x \in \mathcal{N}$ entonces también $x \cup \{x\} \in \mathcal{N}$.

El axioma de infinitud garantiza la existencia de conjuntos infinitos, y en particular, la existencia del conjunto de los números naturales al que denotamos usualmente por $\mathbb{N}$. En este punto parece conveniente invitar al lector a definir la adición en $\mathbb{N}$ y a deducir las propiedades conocidas de ella. El axioma de infinitud es lo que tradicionalmente conocemos como *Principio de Inducción*, según el cual si $A \subseteq \mathbb{N}$ es tal que contiene a $\varnothing$ y al sucesor de cada uno de sus elementos, entonces $A = \mathbb{N}$.

Siendo rigurosos, el axioma de infinitud abre el paso a la construcción de los ordinales finitos, y a un conjunto que los contenga a todos ellos. Este último conjunto, por supuesto, ya no es finito, y suele hacerse referencia a él como el *primer ordinal numerable*, al que se denota por ω. Sus elementos son los conjuntos inductivos generados por $\varnothing$, a los que solemos conocer como los *números naturales.* Entonces

$$\omega = \{0, 1, 2, \ldots\}.$$

El conjunto ω se denota como $\mathbb{N}$, una vez que está provisto de la estructura algebraica que le conocemos. Nos encontramos ahora en el proceso de construir tal estructura.

Axioma 6 *Axioma de Separación.* Dados un conjunto X y una proposición $p(x)$, existe entonces un conjunto que contiene los elementos de X que hacen verdadera a $p(x)$.

Este axioma se conoce también como el *axioma del subconjunto* o bien el *axioma de especificación*, pues en particular garantiza la existencia de subconjuntos de un conjunto dado. Si A es conjunto y $p(x)$ es una función proposicional, entonces, tenemos ahora la garantía de que existe un conjunto B dado por

$$B = \{x \in A | p(x)\},$$

cuyos elementos son los de A que atisfacen la propiedad p, o si se prefiere, los elementos de A para los cuales $v(p(x)) = 1$, donde v es la función de verdad correspondiente al álgebra Booleana a la que pertenece $p(x)$.

Apoyados en este axioma es que usualmente adoptamos un conjunto como el *conjunto universal* correspondiente a una situación dada. El conjunto universal es el conjunto que contiene a todos los conjuntos a los que se refiere un contexto específico.

Adquirimos también con este axioma la posibilidad de construir la *intersección* A y B, dado que, considerando la función proposicional $p(x)$ como $x \in B$, podemos construir el conjunto

$$A \cap B = \{x \in A | x \in B\}$$

o bien

$$A \cap B = \{x | x \in A \wedge x \in B\}.$$

Dada una colección de conjuntos, por ejemlo, si $A = \{X_\alpha | \alpha \in \mathcal{A}\}$, entonces escribimos $B = \cap A$ o de manera más alegórica:

$$B = \bigcap_{\alpha \in \mathcal{A}} X_\alpha$$

para el conjunto $\{x | x \in X_\alpha \ \forall \alpha \in \mathcal{A}\}$.

En este punto se antoja conveniente hacer un alto, para reflexionar acerca de que ya hemos adquirido la capacidad de construir uniones e intersecciones de conjuntos arbitrarios, de alguna manera entonces, la infinitud ha dejado de ser un obstáculo.

Consideremos un conjunto dado U, y una función proposicional $p(x)$ con dominio en U. Debido al axioma de separación tenemos garantizada la existencia del conjunto $A = \{x \in U | p(x)\}$. Ahora bien, claramente también $\neg p(x)$ es una función proposicional con dominio en U, de suerte que el conjunto $A^c_U = \{x \in U | \neg p(x)\}$ existe, por el axioma de especificación. Decimos que A^c_U es el *complemento* de A en U. Otra notación para una situación como esta es $U - A = A^c_U$, en la que escribimos el complemento como una *diferencia* de conjuntos.

En un contexto específico, U podría contener todos los elementos que nos interesa considerar, y en tal caso, es común referirse a U como el *conjunto universal*. Si es claro que U es el conjunto universal, la notación para A^c_U puede simplificarse a A^c.

La *diferencia de conjuntos* puede formularse en un escenario más general, mediante el uso del axioma de separación. Dados dos conjuntos A y B, definimos

$$A - B = \{x \in A | x \notin B\},$$

y notamos que esta definición es completamente independiente de las relaciones de inclusión entre los conjuntos A y B. En este contexto, el complemento es tan sólo un caso particular de la diferencia.

Axioma 7 *Axioma de Sustitución.* Dado un conjunto A y una aplicación f con dominio A, existe un conjunto $I_f(A)$ tal que $f(x) \in I_f(A)$ si y sólo si $x \in A$. Por razones obvias este axioma es también conocido como el *axioma de la imagen.*

Podría pensarse que el axioma de sustitución es prematuro ya que no tenemos la noción de función, sin embargo, un momento de reflexión nos indica que, dado que tenemos pares ordenados, también tenemos productos cartesianos, y por el axioma de separación tenemos aplicaciones[13]. Recordemos que una aplicación $f : A \to B$ es un subconjunto de $A \times B$ con la propiedad de que para todo $a \in A$ existe un único elemento $f(a) \in B$ tal que el par $(a, f(a))$ pertenece a la aplicación.

Por otra parte, dado que al parecer se está definiendo un subconjunto de B, nos bastaría con el axioma de separación, sin embargo, debemos notar que no hay referencia alguna al conjunto B. Finalmente, diremos que la aplicación más importante de este axioma radica en la posibilidad de contar más allá de los números naturales, abriendo la puerta a los números transfinitos. El axioma de sustitución garantiza la existencia de su imagen.

La formulación que se reproduce arriba del axioma de sustitución es la que originalmente se encuentra en la formulación de Fraenkel de 1921, misma que fue introducida por primera vez por el propio Fraenkel en 1929, y apareció también en los trabajos de Church[14] [1942]. Una forma más débil

[13]Formalmente una *aplicación* es el objeto que se define en el texto, si $f : A \to B$ es una aplicación, el *dominio* de f es A, y su *codominio* es B. Una *función* es una aplicación cuyo codominio es un anillo.

[14]Alonzo Church (1903 - 1995), matemático norteamericano, conocido básicamente por sus contribuciones a la matemática de la computación, en particular, el principio conocido como la conjetura de Church-Turing: "todo lo que es computable es computable por una máquina de Turing". Es creador del λ-Cálculo, que proporciona una semántica adecuada para la computación.

de este esquema axiomático a parece en los trabajos de Tarski[15] [1948].

Teorema 17 *Dados dos conjuntos A y B, existe un único conjunto $A \times B$ tal que $(a,b) \in A \times B$ si y sólo si $a \in A$ y $b \in B$.*

Demostración. Tomemos $a \in A$, y para cada $b \in B$ constrúyase el par (a,b), usando el axioma de los pares, el cual es útil también para construir el conjunto $\{(a,b)\}$. Usando ahora el axioma de las uniones puede construirse el conjunto

$$\{a\} \times B = \bigcup_{b \in B} \{(a,b)\} = \{(a,b) | b \in B\}.$$

Una nueva aplicación del axioma de las uniones nos permite construir

$$A \times B = \{(a,b) | a \in A \wedge b \in B\}.$$

Este conjunto es único, dada la unicidad de la unión. ■

Corolario 18 *Dados dos conjuntos A y B se satisface que $A \times B = \varnothing$ si y sólo si $A = \varnothing$ ó $B = \varnothing$.*

Demostración. Procedemos por contradicción. Si $A \times B \neq \varnothing$, tómese $(a,b) \in A \times B$, de donde $a \in A$ y $b \in B$ con lo que $A \neq \varnothing$ y $B \neq \varnothing$. Recíprocamente, es claro que si tanto A como B tienen al menos un elemento cada uno, entonces $A \times B$ tiene al menos un elemento. ■

Como puede observarse, para construir el producto cartesiano[16] es suficiente conocer la unión de conjuntos, incluso en el caso de una colección infinita de conjuntos, que debe ser a su vez un conjunto.

Axioma 8 *Axioma de las Potencias.* Dados un conjunto A, existe un conjunto $\mathcal{P}(A)$ cuyos elementos son todos los subconjuntos de A.

[15] Alfred Tarski (1902 - 1983), matemático y filósofo polaco. La formulación de referencia puede encontrarse también en su texto "Cardinal Algebras", publicado por Oxford University Press en 1949.

[16] El producto cartesiano recibe su nombre gracias a René Descartes (1596 - 1650), matemático y filósofo francés. Claramente Descartes no pudo proponer el producto de conjuntos, sin embargo, su formulación de la Geometría Analítica, en la que considera al Plano Euclidiano como el producto de dos copias de la recta le ha valido el uso de su nombre para el producto de conjuntos.

El conjunto recién definido se conoce como el *conjunto potencia* de A. Otra notación usual para este conjunto es 2^A, notación cuya conveniencia será clara, cuando tengamos a nuestra disposición la teoría de los números ordinales.

Consideremos provisionalmente $2 = \{0, 1\}$. Cada aplicación $f : A \to 2$ determina de forma única un subconjunto de A, digamos $f^{-1}(1) = \{a \in A | f(a) = 1\}$, conjunto que existe gracias al axioma de especificación. De forma análoga, cada subconjunto $B \subseteq A$ define de forma única una aplicación $f : A \to 2$, mediante $f(a) = 1$ si $a \in B$ y $f(a) = 0$ si $a \notin A$.

Proposición 19 *Existe una biyección entre el conjunto potencia de A y el conjunto de las aplicaciones $f : A \to 2$.*$\square$

Luego de esta primera observación intentemos una nueva óptica para el conjunto potencia. Consideremos ahora $3 = \{0, 1, 2\}$ y el conjunto de las aplicaciones $f : 3 \to 2$. El número de tales aplicaciones se identifica en la aritmética ordinaria mediante 2^3, lo que explica, al menos en parte, el nombre de conjunto potencia para el conjunto de los subconjuntos.

Axioma 9 *Axioma de Regularidad.* Todo conjunto A tiene un elemento B tal que $A \cap B = \varnothing$.

Este axioma se conoce también como el *axioma fundacional* ya que resuelve problemas estructurales como el revelado por la paradoja de Russell, semejante a la paradoja del barbero. Consideremos el conjunto $\mathcal{A}$ de todos los conjuntos que no se pertenecen a sí mismos, es decir $\mathcal{A} = \{A | A \notin A\}$, tenemos entonces dos posibilidades:

1. Si $\mathcal{A} \in \mathcal{A}$, entonces por definición $\mathcal{A} \notin \mathcal{A}$.
2. Si $\mathcal{A} \notin \mathcal{A}$, entonces por definición $\mathcal{A} \in \mathcal{A}$.

Un hecho intuitivamente necesario es que los conjuntos sean colecciones que no son elementos de sí mismos, entonces la colección $\mathcal{A}$ no puede ser un conjunto, es decir, no existe el conjunto de todos los conjuntos.

Teorema 20 *Si A es un conjunto, entonces $A \notin A$.*

Demostración. Por vacuidad es claro que $\varnothing \notin \varnothing$. Supóngase ahora que $A \neq \varnothing$ es un conjunto y que $A \in A$, entonces $\{A\}$ es un subconjunto de A gracias al axioma de separación y claramente $A \cap A = A$, de manera que $\{A\}$ no satisface el axioma de regularidad. ■

No toda colección es entonces un conjunto, aunque ciertamente, es posible tratar con colecciones más generales en un contexto más amplio, como el provisto por la *teoría de las categorías*. Los dos resultados siguientes serán de utilidad posteriormente.

Corolario 21 *Si A es un conjunto, entonces $A \cup \{A\} \nsubseteq A$.*□

Proposición 22 *Si $x \in y$, entonces $y \notin x$.*

Demostración. Basta notar que si se satisfacen simultáneamente $x \in y$ y $y \in x$, entonces el $\{x, y\}$ no satisface el axioma de regularidad. ■

La Teoría Cantoriana de los Conjuntos es Cantoriana, debido justamente al siguiente postulado.

Axioma 10 *Axioma de Elección.* El producto cartesiano de un conjunto no vacío de conjuntos no vacíos es no vacío.

Como puede verse claramente, este axioma es equivalente con la afirmación de que si $\mathcal{A}$ es un conjunto cuyos elementos son conjuntos no vacíos y mutuamente ajenos, existe un conjunto que tiene exactamente un elemento de cada uno de los elementos de $\mathcal{A}$. Esta es la forma más común en la que se presenta el axioma de elección, que ha mostrado ser una pieza fundamental de la Teoría Cantoriana de los conjuntos.

El axioma de elección fue propuesto originalmente por Georg Cantor[17], por lo que su incorporación a la axiomática de Zermelo-Fraenkel, hace que la teoría misma se convierta en el cuerpo axiomático de Zermelo-Fraenkel-Cantor.

La noción de infinito era un problema que ocupaba los esfuerzos de muchos matemáticos en la época de Cantor, y la teoría de los conjuntos, a través de los ordinales y los cardinales, le permitió formalizar el concepto de

[17]Georg Ferdinand Ludwig Philipp Cantor (1845 - 1918), matemático alemán.

infinitud, logrando además la formulación de la aritmética de los números transfinitos.

El concepto de infinito es propio de la matemáticas, y sin embargo, no siempre ha sido bien aceptado por los matemáticos. Por ejemplo Gauss[18], el llamado "príncipe de las matemáticas", se pronunciaba por no aceptar a "la magnitud infinita como algo completo", señalando que el infinito no es más que "una manera de hablar". Con ello observamos que el infinito no siempre se entendió con claridad, ni siquiera por mentes tan lúcidas como la de Gauss.

Se debe a Dedekind[19] la primera formulación del infinito, lo que consiguió usando como modelo el conjunto de los números naturales. Sus investigaciones acerca de los fundamentos de la Aritmética, le condujeron a esta formulación, y a concebir la primera axiomática para lon números naturales, misma que fuera publicada con posterioridad por el italiano Giuseppe Peano[20], a quien debemos también la introducción de los símbolos que hoy conocemos para la unión y la intersección de conjuntos. Esta forma de denotar uniones e intersecciones aparece por primera vez en su obra *Applicazioni Geometriche del Calcolo Infinitesimale*, publicada en 1887.

Cantor se preguntaba acerca de la posibilidad de formular con rigor el concepto de infinito, con independencia de los números naturales, lo que finalmente logró mediante la introducción de la teoría de los ordinales. Aun que la semilla de la aritmética transfinita se encuentra en las ideas de Dedekind, cuando hace una distinción clara entre infinitud y continuidad, la formalización se alcanza en las contribuciones de Cantor.

La teoría de los conjuntos es, como toda contribución científica significativa, el producto de una gran cantidad de contribuciones individuales, muchas de ellas realizadas en colaboración. No puede entenderse su desarrollo, así como la fundamentación de la Aritmética sin referencia a los trabajos de

[18]Johann Carl Friedrich Gauss (1777 1855), matemático, astrónomo y físico alemán que contribuyó significativamente en muchos campos, incluida la teoría de números, el análisis matemático, la geometría diferencial, la geodesia, el magnetismo y la óptica. Considerado "el príncipe de las matemáticas" y "el matemático más grande desde la antigüedad", Gauss tuvo influencia notable en muchos campos de la matemática y de la Ciencia, y es considerado uno de los matemáticos que más influencia ha tenido en la Historia, extendiendo por vez primera el concepto de divisibilidad.

[19]Julius Wilhelm Richard Dedekind (1831 - 1916), matemático alemán, que contribuyó a la fundamentación del Análisis Matemático a través de su célebre concepto de *cortadura*.

[20]Giuseppe Peano (1858 1932) matemático y filósofo italiano, conocido por sus contribuciones a la Teoría de los conjuntos. Se hizo célebre como del profesor de Cálculo en la Universidad de Turín.

Frege[21], en los que se encuentran una gran cantidad de ideas esclarecedoras a propósito de lo que un conjunto es, y de su fortaleza en la construcción del concepto de número. Es justo considerar a Cantor, Dedekind y Frege, como los principales precursores de la Teoría de los conjuntos, sin olvidar que sus trabajos se generaron gracias a las contribuciones y reflexiones de todo un ejército de matemáticos y filósofos.

El axioma de elección, a pesar de su enorme carga intuitiva, dista mucho de ser trivial, si por trivial se entiende desprovisto de importancia. El axioma de elección produce resultados poco intuitivos como la paradoja de Banach[22]-Tarski[23], según la cual, por ejemplo, es posible descomponer una esfera de radio 1 en dos esferas de radio 1. Resulta claro, por lo menos de manera intuitiva que tal descomposición es imposible si es finita, lo que hace intervenir de nueva cuenta, como protagonista, al infinito.

Los alcances del axioma de elección son realmente notables, llegando hasta la Topología, y en particular al concepto de compacidad. En 1950 Kelley[24] demostró la equivalencia entre el teorema de Tychonoff[25] y el axioma de elección. El teorema de Tychonoff afirma que un producto arbitrario de espacios topológicos compactos es un espacio compacto.

Además de estas consecuencias impresionantes, el axioma de elección es equivalente también con el lema de Zorn y el Teorema de Zermelo, cuyos enunciados posponemos para la siguiente sección.

[21]Friedrich Ludwig Gottlob Frege (1848 - 1925), matemático y filósofo alemán, precursor de la llamada filosofía analítica, término que se refiere al ejercicio de la filosofía con fundamento en la Lógica Formal. Frege es ampliamente reconocido como el mayor de los lógicos desde Aristóteles.

[22]Stefan Banach (1892 - 1945), matemático polaco, notable por haber sido autodidacta, su talento fue descubierto accidentalmente por Juliusz Mien y Hugo Steinhaus.

[23]Alfred Tarski (1902 - 1983), originalmente Alfred Teitelbaum, matemático y filósofo polaco.

[24]John Leroy Kelley (1916 - 1999), matemático norteamericano, autor de varias contribuciones en Topología y Análisis Fucional.

[25]Andrey Nikolayevich Tychonoff (1906 1993), matemático soviético ruso, conocido por sus contribuciones en Topología, Análisis Funcional y Física Matemática.

Cuaderno de Ejercicios no. 6

1. Demuestre que para dos conjuntos cualesquiera A y B se satisface que $A \cap B \subseteq A$.

2. Demuestre que para todo conjunto A se satisface que $A \cap \varnothing = \varnothing$

3. Demuestre que $A \subseteq B$ si y sólo si $A \cap B = A$.

4. Demuestre que $\varnothing \notin \{\{\varnothing\}\}$.

5. Demuestre la conmutatividad de la intersección, es decir, que si A y B son conjuntos, entonces $A \cap B = B \cap A$.

6. Demuestre la asociatividad de la intersección, es decir, que si A, B y C son conjuntos, entonces $A \cap (B \cap C) = (A \cap B) \cap C$.

7. Demuestre las propiedades distributivas de la unión e intersección, es decir, que para tres conjuntos cualesquiera se satisfacen:

   a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

8. Demuestre que en un conjunto universal U se satisface que $A - B = A \cap B^c$.

9. Demuestre que la intersección $\cap A$ de un conjunto dado A es única.

10. Dos conjuntos A y B se dicen *ajenos* ó *disjuntos* si $A \cap B = \varnothing$. Demuestre que dados conjuntos cualesquiera A y B, los conjuntos $A \times \{0\}$ y $B \times \{1\}$ son ajenos.

11. Demuestre que
$$\bigcap_{\alpha \in \mathcal{A}} A_\alpha = \varnothing$$
si y sólo si existe $\alpha \in \mathcal{A}$ tal que $A_\alpha = \varnothing$.

12. La forma en la que enunciamos el axioma de elección es conocido también como el *principio de no vacuidad del producto*. Una versión más popular dice que dado un conjunto no vacío de conjuntos no vacíos, existe un conjunto que tiene exactamente un elemento de cada conjunto en la colección. Demuestre que estas dos versiones son equivalentes.

8. Álgebra de Conjuntos

Ya hemos definido el significado de *aplicación* de un conjunto A en un conjunto B, lo que denotamos por

$$f : A \to B.$$

Se usa también el término *función* como sinónimo de aplicación, aunque algunos autores, particularmente en Análisis Matemático suelen reservar en término función para el caso en el que B tiene estructura de anillo. A lo largo de la presente exposición usaremos indistintamente los términos función y aplicación con el mismo significado.

Si se consideran conocidos los conjuntos A y B decimos que la función se llama simplemente f, de no ser así, la función es una terna (f, A, B). El conjunto A se llama *dominio* de f y se denota como

$$D(f) = A,$$

en tanto que el conjunto B se llama *codominio* y se denota mediante

$$C(f) = B.$$

El *rango* también llamado *imagen* de f se define como

$$Im(f) = f(A) = I_f(A) \cap B,$$

donde $I_f(A)$ es el conjunto cuya existencia garantiza el axioma de sustitución. Si $C \subset A$ entonces definimos la restricción $f|_C$ como la intersección $f \cap (C \times B)$, es decir,

$$f|_C = f \cap (C \times B),$$

de manera entonces que $f(C) = Im(f|_C)$ es *la imagen de C bajo la función f*. Si $E \subset B$, la *preimagen* de E se define por $f^{-1}(E) = \{x \in A | f(x) \in E\}$. Dado un elemento $y \in E$, la preimagen $f^{-1}(\{y\})$ se denota mediante $f^{-1}(y)$, y se dice que es la *fibra* de f sobre y.

Teorema 23 *Dada la colección de conjuntos $\{A_\alpha | \alpha \in \mathcal{A}\}$ cada uno de los cuales está contenido en el conjunto universal U se satisface:*

1. *El complemento de la intersección es la unión de los complementos.*

$$\left(\bigcap_{\alpha \in \mathcal{A}} A_\alpha \right)^c = \bigcup_{\alpha \in \mathcal{A}} A_\alpha^c$$

2. El complemento de la unión es la intersección de los complementos.

$$\left(\bigcup_{\alpha\in\mathcal{A}} A_\alpha\right)^c = \bigcap_{\alpha\in\mathcal{A}} A_\alpha^c.$$

Demostración. Se considera ejercicio[26]. ■

Propiedades interesantes de las funciones, además de muy útiles en el estudio de la Topología y el Álgebra son aquellas que tienen que ver con preimágenes.

Teorema 24 *Dados dos conjuntos A, B y una función $f : A \to B$, entonces se satisfacen las afirmaciones siguientes:*

1. $f(\varnothing) = \varnothing$.
2. *Si* $A_1 \subseteq A_2 \subseteq A$, *entonces* $f(A_1) \subseteq f(A_2) \subseteq B$
3. *Si* $\{A_\alpha | \alpha \in \mathcal{A}\} \subseteq \mathcal{P}(A)$, *entonces*
$$f\left(\bigcup_{\alpha\in\mathcal{A}} A_\alpha\right) = \bigcup_{\alpha\in\mathcal{A}} f(A_\alpha)$$
4. *Si* $\{A_\alpha | \alpha \in \mathcal{A}\} \subseteq \mathcal{P}(A)$, *entonces*
$$f\left(\bigcap_{\alpha\in\mathcal{A}} A_\alpha\right) \subseteq \bigcap_{\alpha\in\mathcal{A}} f(A_\alpha).$$

Demostración. Ejercicio. ■

Ejemplo 19 *Consideremos la función $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$. Notemos por una parte que*

$$f([0,\infty)) = f((-\infty, 0]) = [0,\infty).$$

[26] Por el axioma de extensión habrá que demostrar la igualdad de conjuntos demostrando la inclusión en ambas direcciones. La técnica para demostrar las inclusiones es el uso de un argumento puntual, es decir, tomar un elemento arbitrario en uno de los conjuntos y demostrar que debe estar en el otro.

Por otro lado $[0,\infty)\cap(-\infty,0]=\{0\}$ *y claramente* $f(0)=0$*, en tanto que*

$$f\left([0,\infty)\right)\cap f\left((-\infty,0]\right)=[0,\infty).$$

Esto ilustra el hecho de que el aserto del punto 4 en el teorema anterior es el mejor resultado posible.

El comportamiento de las preimágenes es bastante más generoso que los de las imágenes.

Teorema 25 *Dados dos conjuntos* A *y* B *y una función* $f:A\to B$*, entonces se satisfacen las afirmaciones siguientes:*

1. $f^{-1}(\varnothing)=\varnothing$.
2. $f^{-1}(B)=A$.
3. *Si* $B_1\subseteq B_2\subseteq B$*, entonces* $f^{-1}(B_1)\subseteq f^{-1}(B_2)\subseteq A$
4. *Si* $\{B_\beta|\beta\in\mathcal{B}\}\subseteq\mathcal{P}(B)$*, entonces*
$$f^{-1}\left(\bigcup_{\beta\in\mathcal{B}}B_\beta\right)=\bigcup_{\beta\in\mathcal{B}}f^{-1}\left(B_\beta\right)$$
5. *Si* $\{B_\beta|\beta\in\mathcal{B}\}\subseteq\mathcal{P}(B)$*, entonces*
$$f^{-1}\left(\bigcap_{\beta\in\mathcal{B}}B_\beta\right)=\bigcap_{\alpha\in\mathcal{B}}f^{-1}\left(B_\beta\right)$$
6. *Si* $B_0\subseteq B$*, entonces*
$$f^{-1}(B_0^c)=f^{-1}(B_0)^c.$$

Demostración. Ejercicio. ∎

Cuaderno de Ejercicios no. 7

1. Construya demostraciones formales de los resultados enunciados en la sección anterior.

2. Tome dos funciones $f, g \in B^A$. Considerándolas como conjuntos, determine $f \cap g$ y discuta su significado.

3. Tome dos funciones $f, g \in B^A$. Considerándolas como conjuntos, determine $f \cup g$ y discuta su significado.

4. Determine las circunstancias bajo las cuales

$$B^A \cap D^C \neq \varnothing$$

   y discuta el significado.

5. Una *n-ordenación* de un conjunto A es una biyección $\theta : n \to A$. Supóngase que A admite una 3-ordenación, determine el número de 3-ordenaciones distintas que admite.

6. Supóngase que A admite una n-ordenación, determine el número de n-ordenaciones distintas que admite.

7. Una 2-*partición* de un conjunto X es un conjunto $\{x, y\}$ de dos elementos tales que $x \cup y = X$ y además $x \cap y = \varnothing$. Encuentre el conjunto de las 2-particiones ordenadas del ordinal n. Compare con 2^n.

8. Denote mediante $\mathcal{P}_2(X)$ el conjunto de las 2-particiones ordenadas del conjunto X. Determine el número de las 2-particiones ordenadas de un conjunto finito X.

9. Determine el número de las 2-particiones no ordenadas de un conjunto finito X.

10. Una 3-*partición* de un conjunto X es un conjunto $\{x, y, z\}$ de dos elementos tales que $x \cup y \cup z = X$, además de que $x \cap y = \varnothing$, $x \cap z = \varnothing$ y $y \cap z = \varnothing$. Encuentre el conjunto de las 3-particiones ordenadas de $\varnothing$. Compare con 3^n.

11. Denote mediante $\mathcal{P}_3(X)$ el conjunto de las 3-particiones ordenadas del conjunto X. Determine el número de las 3-particiones ordenadas de un conjunto finito X.

12. Determine el número de las 3-particiones no ordenadas de un conjunto finito X.

13. Una *n-partición* de un conjunto X es un conjunto $\{x_1, x_2, \ldots, x_n\}$ de n elementos tales que $x_1 \cup x_2 \cup \ldots \cup x_n = X$ y además $x_i \cap x_j = \varnothing$ para $i \neq j$. Encuentre el conjunto de las n-particiones ordenadas de $\varnothing$.

14. Determine el número de las n-particiones no ordenadas de un conjunto finito X.

15. Denote mediante $\mathcal{P}_n(X)$ el conjunto de las n-particiones ordenadas del conjunto X. Determine el número de las n-particiones ordenadas de un conjunto finito X.

16. Determine el número de las 3-particiones ordenadas de un conjunto finito X.

17. El conjunto potencia 2^X puede interpretarse como la colección de todas las 2-particiones ordenadas de X. Encuentre una biyección entre 2^X y $\mathcal{P}_2(X)$.

18. El conjunto potencia 3^X puede interpretarse como la colección de todas las 3-particiones ordenadas de X. Encuentre una biyección entre 3^X y $\mathcal{P}_3(X)$.

19. El conjunto potencia n^X puede interpretarse como la colección de todas las n-particiones ordenadas de X. Encuentre una biyección entre n^X y $\mathcal{P}_n(X)$.

9. Ordinales y Cardinales

Una *relación* $\mathcal{R}$ en una colección A es una subcolección de $A \times A$. Es usual denotar $a\mathcal{R}b$ con el mismo significado que $(a, b) \in \mathcal{R}$. Una relación $\leq$ se dice que es un *orden parcial* sobre el conjunto A si es *reflexiva*, *antisimétrica* y *transitiva*, es decir, si:

1. $a \leq a$ para todo $a \in A$.
2. Si $a \leq b$ y $b \leq a$, entonces $a = b$.
3. Si $a \leq b$ y $b \leq c$, entonces $a \leq c$.

Dado un conjunto A y una relación de orden parcial $\leq$ sobre A, decimos que el par $(A, \leq)$ es un *conjunto parcialmente ordenado* o bien que es un *poset*[27]Un orden parcial sobre un conjunto A es un *orden lineal* o equivalentemente un *orden total* si para cualesquiera dos elementos de $a, b \in A$ se verifica al menos una de las proposiciones $a \leq b$ ó $b \leq a$.

Ejemplo 20 *Sean A un conjunto y 2^A su conjunto potencia, entonces $(A, \subseteq)$ es un poset, pero no es linealmente ordenado.*

$$\begin{tikzcd}
& \{0\} \arrow[dr, "\subseteq"] & \\
\varnothing \arrow[ur, "\subseteq"] \arrow[dr, "\subseteq"'] & & \{0,1\} \\
& \{1\} \arrow[ur, "\subseteq"'] &
\end{tikzcd}$$

Como se observa en el diagrama previo, no hay relación de inclusión entre $\{0\}$ y $\{1\}$.

Un poset $(A, \leq)$ se dice que es un *conjunto bien ordenado* o que $\leq$ es un *buen orden* sobre el conjunto A, si dado un subconjunto no vacío $B \subseteq A$ existe un elemento $b_0 \in B$ tal que $b_0 \leq b$ para todo $b \in B$, y en tal caso se dice que b_0 es un *elemento inicial* ó *primer elemento* de B.

Notemos que la relación de inclusión es un orden parcial sobre la colección $\mathcal{C}$ de los conjuntos, no obstante, el par $(\mathcal{C}, \subseteq)$ no es un poset, dado que, por el

[27]Partially ordered set.

axioma de regularidad $\mathcal{C}$ no es un conjunto. Una colección arbitraria admite también un buen orden: una colección percialmente ordenada se dice que es bien ordenada si todo subconjunto no vacío de ella tiene un primer elemento.

Ejemplo 21 *El poset* $(A, \subseteq)$ *tiene un elemento inicial, que es* $\varnothing$*, pero si* A *tiene más de un elemento, entonces no es bien ordenado, dado que* $2^A - \varnothing$ *no tiene elemento mínimo.*

Tenemos ahora suficiente información como para enunciar otro equivalente del axioma de elección: el *teorema de Zermelo.*

Teorema de Zermelo. *Todo conjunto admite un buen orden.*

Para un principiante, el resultado de Zermelo parece afirmar más de lo que en realidad postula. A un conjunto dado se le puede dotar de un buen orden. Si el conjunto es ordenado, es probable que deba definirse un orden distinto para hacerlo bien ordenado.

Otro resultado, también equivalente con el axioma de elección es el llamado *lema de Zorn*[28], publicado el 1935, mismo que fuera originalmente descubierto por Kuratowski[29] en 1922.

Si $(A, \preceq)$ es un poset y $B \subseteq A$, claramente la restricción de "$\preceq$" a B es también un orden parcial, de manera que $(B, \preceq)$ es un poset, y decimos que es un *subposet* de $(A, \preceq)$. Una *cadena* C en un poset A es un subposet totalmente ordenado. Dados un poset $(A, \preceq)$ y $B \subseteq A$, se dice que $a \in A$ es una *cota superior* para B si $b \preceq a$ para todo $b \in B$. Si además $a \in B$, se dice que a es un *elemento maximal* de B.

Lema de Zorn. *Si toda cadena* C *es un poset* P *tiene una cota superior, entonces* P *tiene un elemento maximal.*

De todo orden parcial puede contruirse un *orden estricto* como sigue: dados dos elementos a y b en un poset X, se dice que $a < b$ si $a \leq b$ y además $a \neq b$. Por otra parte, las expresiones $b > a$ y $b \geq a$ son equivalentes respectivamente con $a < b$ y $a \leq b$.

[28]Max August Zorn (1906 - 1993), matemático alemán nacionalizado norteamericano, contribuyó significativamente en Teoría de Grupos y Análisis Numérico.

[29]Kazimierz Kuratowski (1896 1980), matemático polaco, uno de los más importantes precursores de la Topología moderna.

Dado un conjunto X, una función $s : \mathbb{N} \to X$ se dice que es una *sucesión* en X, y es constumbre escribir $s(n) = x_n$, y denotar la sucesión mediante $s = (x_n)$. Una sucesión es *creciente* si para todo $n \in \mathbb{N}$ se tiene que $x_n \leq x_{n+1}$ y se dice que es *estrictamente creciente* si para todo $n \in \mathbb{N}$ se tiene que $x_n \leq x_{n+1}$. De manera análoga se definen las sucesiones decrecientes y estrictamente decrecientes. El siguiente resultado cuya demostración es prácticamente innecesaria, constituyó un poderoso instrumento en manos de Pierre de Fermat[30] quien desarrolló en *método de descenso infinito* para demostrar propiedades de lo números naturales.

Proposición 26 *Un conjunto bien ordenado no admite sucesiones estrictamente decrecientes.*

Demostración. Sean $\mathcal{C}$ un conjunto bien ordenado y $s = (z_n)$ una sucesión estrictamente decreciente de elementos de $\mathcal{C}$. Por definición el conjunto $Im(s) = \{z_n | n \in \mathbb{N}\}$ tiene un primer elemento, es decir, existe $k \in \mathbb{N}$ tal que x_k es el primer elemento de $Im(s)$, y en particular $x_k \leq x_{k+1}$, sin embargo, por hipótesis, dado que s es estrictamente decreciente $x_{k+1} < x_k$, lo que representa una contradicción. ■

Se dice que α es un *conjunto transitivo* si $x \in y \in \alpha$ implica $x \in \alpha$. la siguiente proposición no es sino una reformulación de la definición.

Proposición 27 *Si α es un conjunto transitivo y $x \in \alpha$, entonces $x \subseteq \alpha$.*□

Se dice que α es un *conjunto $\in$-transitivo* si $x \in y \in z \in \alpha$ implica $x \in z$. La siguiente proposición tiene el mismo carácter que la anterior, afirma esencialmente que un conjunto $\in$-transitivo es un conjunto de conjuntos transitivos.

Proposición 28 *Si α es un conjunto $\in$-transitivo y $x \in \alpha$, entonces x es un conjunto transitivo.*□

Un conjunto α se dice que es un *ordinal* si es transitivo y $\in$-transitivo, es decir, si se satisfacen las dos propiedades simultáneamente.

[30]Pierre de Fermat (1601 - 1665), abogado francés que fuera juez en la ciudad de Tolouse. Conocido como el "príncipe de los aficionados", sentó las bases del Cálculo, y es ampliamente conocido por la conjetura de que para $n > 2$, la ecuación $a^n + b^n = c^n$ no tiene soluciones enteras; demostró el caso $n = 3$, y el caso general fue demostrado por el británico Andrew Wiles en 2005.

1. Si $x \in y \in \alpha$ entonces $x \in \alpha$.
2. Si $x \in y \in z \in \alpha$ entonces $x \in z$.

Entonces, un ordinal es un conjunto transitivo de conjuntos transitivos. La colección de todos los ordinales se denota por **Ord**.

Teorema 29 *Se verifican las siguientes afirmaciones:*

1. $\varnothing \in \mathbf{Ord}$.
2. *Si* $\alpha \in \mathbf{Ord}$, *entonces* $\alpha \cup \{\alpha\} \in \mathbf{Ord}$.

Demostración. El conjunto vacío es transitivo y $\in$-transitivo por vacuidad. Supóngase por otra parte que $\alpha \in \mathbf{Ord}$, y consideremos $\beta = \alpha \cup \{\alpha\}$. Supongamos que $x \in y \in \beta$, entonces claramente $x \in \alpha$ ó $x = \alpha$. En el primer caso $x \in \alpha \subset \beta$, de donde $x \in \beta$, en tanto, para la segunda opción, $x = \alpha \in \beta$, con lo que se tiene demostrada la transitividad de β. Supongamos ahora que $x \in \beta$, si $x \neq \alpha$, entonces $x \in \alpha$, de manera que en cualquier caso x es un conjunto transitivo y β es $\in$-transitivo. ■

Corolario 30 *Todo ordinal es un conjunto de ordinales.*

Demostración. Dado que un ordinal es $\in$-transitivo, sus elementos son transitivos. Ahora bien, si $\beta \in \alpha$ y $x \in y \in z \in \beta$, entonces por transitividad $\beta \in \alpha$ y $x \in y \in z \in \alpha$, con lo que $x \in z$ y β es $\in$-transitivo. ■

Como veremos, el recíproco de este resultado no se cumple.

Teorema 31 *Se verifican las siguientes afirmaciones:*

1. *Si* $\mathcal{A} \subseteq \mathbf{Ord}$, *entonces* $\cup\mathcal{A} \in \mathbf{Ord}$.
2. *Si* $\varnothing \neq \mathcal{A} \subseteq \mathbf{Ord}$, *entonces* $\cap\mathcal{A} \in \mathbf{Ord}$.

Demostración. Denotemos $B = \cup\mathcal{A}$, y supongamos que $x \in y \in B$, entonces $x \in y \in A$ para algún $A \in \mathcal{A}$, de manera que $x \in A \subseteq B$, y por tanto B es transitivo. Los elementos de los elementos de $\mathcal{A}$ son conjuntos transitivos, de manera B es $\in$-transitivo. Supongamos ahora que $\varnothing \neq \mathcal{A}$, y denotemos $C = \cap\mathcal{A}$, claramente, los elementos de C son transitivos, con lo que C es

$\in$-transitivo; finalmente, C es obviamente transitivo. ■

En adelante adoptaremos la notación $\alpha + 1 = \alpha \cup \{\alpha\}$, y decimos que $\alpha + 1$ es el *sucesor* de α, de manera que tenemos ya que $\varnothing$ es un ordinal, y que el sucesor de todo ordinal es a su vez un ordinal. Supongamos ahora que

$$x \in y \in \mathbf{Ord},$$

como y es $\in$-transitivo, entonces x es transitivo y $x \subseteq y$, de manera que x es $\in$-transitivo, es entonces un ordinal y $x \in \mathbf{Ord}$, de donde **Ord** es transitivo. Ahora bien, dado que sus elementos son ordinales, son en particular transitivos y **Ord** es $\in$-transitivo.

Teorema 32 *La colección* **Ord** *es transitiva y $\in$-transitiva.*□

Tenemos entonces que si **Ord** fuese un conjunto, entonces $\mathbf{Ord} \in \mathbf{Ord}$, de donde se sigue claramente el siguiente resultado.

Teorema 33 *La colección* **Ord** *no es un conjunto.*□

La colección **Ord** sería un buen candidato para ser el mayor de todos los ordinales, sin embargo, por las propiedades demostradas de los ordinales, no únicamente $\mathbf{Ord} \in \mathbf{Ord}$ sino que además $\mathbf{Ord} + 1 \in \mathbf{Ord}$, de manera entonces que $\mathbf{Ord} + 1 \subseteq \mathbf{Ord}$, lo que se conoce como la *paradoja de Burali-Forti*[31]. Dado que los ordinales son conjuntos, la colección **Ord** no es un ordinal, dado que no es un conjunto, de manera pues que $\mathbf{Ord} \in \mathbf{Ord}$ carece totalmente de sentido.

Recordemos que la expresión $A \subset B$ indica inclusión propia, es decir, que $A \subseteq B$ y $A \neq B$. Sobre los ordinales denotamos $\alpha < \beta$ para $\alpha \subset \beta$ y $\alpha \leq \beta$ para $\alpha \subseteq \beta$.

Teorema 34 *Dados $\alpha, \beta \in \mathbf{Ord}$, entonces $\alpha < \beta$ si y sólo si $\alpha \in \beta$.*

Demostración. Si $\alpha < \beta$, entonces $\alpha \subset \beta$, de manera que $\alpha = \alpha \cap \beta$ y $\beta = \alpha \cup \beta$. ■

Teorema 35 *La relación de inclusión $\subseteq$ es un buen orden sobre* **Ord**.

[31]Cesare Buralli-Forti (1861 - 1931), matemático italiano, que fuera asistente de Peano. Nótese que se trata de una persona y no dos.

Demostración. Es claro que la relación de inclusión es un orden parcial sobre **Ord**. Ahora bien, si $\varnothing \neq \mathcal{A} \subseteq \mathbf{Ord}$, entonces, si $\varnothing \in \mathcal{A}$, de modo que claramente $\varnothing = \min \mathcal{A}$. Si por el contrario $\varnothing \notin \mathcal{A}$ por el axioma de regularidad, sea $\alpha \in \mathcal{A}$ tal que $\alpha \cap \mathcal{A} = \varnothing$, y sea $\beta \in \mathcal{A}$ un elemento arbitrario. ■

Corolario 36 *Un ordinal es un conjunto bien ordenado.*

Demostración. Sean $\alpha \in \mathbf{Ord}$ y $\varnothing \neq A \subseteq \alpha$. Si $\varnothing \in A$, entonces claramente $\varnothing = \min A$. En otro caso úsese el axioma de regularidad como en la demostración anterior. ■

Corolario 37 *Un ordinal es un conjunto totalmente ordenado.*

Demostración. Si $x \in y \in \beta \subset \alpha$, entonces, por transitividad $x \in \beta$, pero además $x \in y \in \alpha$ de donde $x \in \alpha$. Existe entonces $v \in \alpha$ tal que $v \cap \alpha = \beta$, y claramente $v = \beta$, de donde $\beta \in \alpha$. ■

Los ordinales son entonces, con toda propiedad, el paradigma de la buena ordenación. Con el siguiente resultado formalizamos el orden estricto.

Teorema 38 *Si* $\alpha, \beta \in \mathbf{Ord}$, *entonces:*

1. *Si* $\beta \in \alpha$ *entonces* $\beta + 1 = \alpha$ *ó* $\beta + 1 \in \alpha$.
2. $\alpha = \cup(\alpha + 1)$.
3. $\alpha = \cup\alpha$ *o bien* $\alpha = (\cup\alpha) + 1$
4. $\alpha = \{\lambda \in \mathbf{Ord} | \lambda \subset \alpha\}$.

Demostración. Ejercicio. ■

Una función $f : A \to B$ se dice *suprayectiva* si $Im(f) = B$ y se dice *inyectiva* si $f(x_0) = f(x_1)$ implica $x_0 = x_1$. Una función que es inyectiva y suprayectiva se dice que es *biyectiva*. Un conjunto A se dice que tiene la misma *cardinalidad* que el conjunto B si existe una *biyección* $f : A \to B$. Si los conjuntos A y B tienen la misma cardinalidad se dice que son *equipotentes* y se escribe $|A| = |B|$.

Sea A un conjunto arbitrario, dado que la colección de los números ordinales o simplemente ordinales está bien ordenada por la inclusión, entonces la colección

$$\{\alpha \in \mathbf{Ord} : |A| = |\alpha|\}$$

tiene un elemento mínimo. Este elemento mínimo se dice que es el *número cardinal* o bien la *cardinalidad* del conjunto A y se denota por $\#(A)$. Tenemos entonces que en símbolos

$$\#(A) = \text{mín}\{\alpha \in \mathbf{Ord} : |A| = |\alpha|\}.$$

Es natural que al inicio resulte extraño pensar en el elemento mínimo de una colección de conjuntos que tienen todos el "mismo tamaño", pero las definiciones que siguen disolverán cualquier posible confusión. Antes de Cantor, cualquier referencia a la infinitud pasaba por una comparación con los números naturales. Cantor buscaba una definición de infinito intrínseca, sin referencias externas, lo que felizmente le condujo a la Teoría de los *Números Transfinitos*.

Un conjunto se dice que es un *conjunto infinito* si tiene un subconjunto propio con la misma cardinalidad que él; más precisamente, un conjunto A es infinito si existe $B \subset A$ tal que $|A| = |B|$. Un conjunto que no es infinito se dice que es un *conjunto finito*.

Un número natural es un ordinal finito, y más aún, todo ordinal finito es su propio cardinal.

La colección de los números ordinales será denotada mediante **Card** y claramente de entre los cardinales encontramos cardinales finitos e infinitos. Denostaremos por ω_0 y simplemente por ω el conjunto de los cardinales finitos. Ya antes nos hemos tomado la libertad de simbolizar este conjunto mediante $\mathbb{N}$ y este parece un punto oportuno para corregir el error. El símbolo $\mathbb{N}$ hace referencia a la estructura algebraica que posee ω una vez que se construyen las operaciones de adición y multiplicación que definiremos en breve.

Dados dos cardinales α y β definimos:

1. La *suma* de α y β mediante

$$\alpha + \beta = \#\left[(\alpha \times \{0\}) \cup (\beta \times \{1\})\right].$$

2. El *producto* de α y β como

$$\alpha\beta = \#\left(\alpha \times \beta\right).$$

3. La β-ésima *potencia* de α por

$$\alpha^{\beta} = \#\{f : \beta \to \alpha | f \text{ es una función}\}.$$

Consideremos un conjunto X y una función arbitraria $f : X \to \{0, 1\}$. Si $A = f^{-1}(1)$, entonces decimos que f es la *función característica* de A en X y se denota por $\chi_{_A}$.

Lema 39 *Para todo conjunto X se tiene que*

$$\#\left(\mathcal{P}(X)\right) = 2^{\#(X)}.$$

Demostración. Por definición $2 = \{0, 1\}$, entonces el conjunto $\mathcal{F}(X, 2)$ de las funciones de X en 2 tiene cardinalidad $2^{\#(X)}$. Es suficiente entonces encontrar una biyección de $\mathcal{P}(X)$ en $\mathcal{F}(X, 2)$, para lo cual basta establecer la correspondencia $A \mapsto \chi_{_A}$. ■

Una de las relaciones más interesantes en la Teoría de los Conjuntos es la que guardan un cardinal α y la potencia 2^{α}. George Cantor demostró el resultado siguiente mediante una aguda observación que reproducimos en la demostración.

Teorema 40 *Para cualquier conjunto X se satisface*

$$\#(X) < \#\left(\mathcal{P}(X)\right).$$

Demostración. La función $X \to \mathcal{P}(X)$ dada por $x \mapsto \{x\}$ es claramente inyectiva por lo que entonces $\#(X) \leq 2^{\#(X)}$. Supongamos ahora que existe una función suprayectiva $f : X \to \mathcal{P}(X)$ y considérese el conjunto $A = \{x | x \notin f(x)\} \in \mathcal{P}(X)$, y sea $y \in X$ tal que $f(y) = A$. Si $y \in A$, entonces $y \notin A$ y recíprocamente, por lo que no existe tal función suprayectiva. ■

Cuaderno de Ejercicios no. 8

1. Resuelva los ejercicios propuestos dentro del texto se la sección anterior.
2. Sea X un conjunto no vacío, demuestre que $(2^X, \subseteq)$ es un poset que no es totalmente ordenado ni bien ordenado.
3. Sea X un conjunto no vacío, demuestre que $(2^X, \supseteq)$ es un poset que no es totalmente ordenado ni bien ordenado.
4. Demuestre que $\{3, 4, 5, 6\}$ es un conjunto $\in$-transitivo, pero que no es transitivo.
5. Demuestre que $\{0, 1, 2, 3, 4, 5\}$ es un ordinal.
6. Demuestre que $\cup\{2, 4, 8\}$ es un ordinal.
7. Demuestre que $\cap\{2, 4, 8\}$ es un ordinal.
8. Demuestre que el conjunto de los pares es un conjunto bien ordenado bajo la inclusión.
9. Demuestre que todo subconjunto de un conjunto bien ordenado es bien ordenado.
10. Demuestre que si $\beta \in \alpha$ entonces $\beta + 1 = \alpha$ ó $\beta + 1 \in \alpha$, para ordinales α y β.
11. Demuestre que $\alpha = \cup(\alpha + 1)$ para todo ordional α.
12. Demuestre que si α es un ordinal no vacío, entonces $\alpha = (\cup\alpha) + 1$.
13. Discuta el significado de $2^0 = 1$, entendido como conjunto de aplicaciones.
14. Discuta el significado de $1^n = 1$, entendido como conjunto de aplicaciones.
15. Determine 2^3 y 3^2 como conjuntos de aplicaciones.

10. La Hipótesis del Continuo

Un conjunto se dice *numerable* si tiene la misma cardinalidad que ω. La cardinalidad de ω se define como $\aleph_0$, y de hecho puede demostrarse que $\omega = \aleph_0$, tenemos entonces que $\aleph_0$ es la cardinalidad de los conjuntos numerales. Por otra parte, denotamos por ω_1 el primer ordinal no numerable y por $\aleph_1$ su cardinalidad, de manera que entonces también por definición $\omega_1 = \aleph_1$.

Hipótesis del Continuo. $\aleph_1 = 2^{\aleph_0}$.

La hipótesis del continuo ha ejercido una poderosa fascinación durante muchos años en la comunidad matemática de todo el planeta. Cantor creía en la veracidad de la hipótesis del continuo e intentó obtener una demostración sin éxito. La célebre lista de problemas abiertos propuestos por David Hilbert[32] en 1900 en París contenía como el primero de ellos a la hipótesis del continuo.

Kurt Gödel[33] demostró alrededor de 1940 que la hipótesis del continuo es independiente de los axiomas de ZFC, en particular, que su falsedad no puede ser demostrada usando tal axiomática. Para 1963 Paul Cohen[34] obtuvo una demostración de que la veracidad de la hipótesis del continuo no puede ser demostrada con apoyo de la axiomática de ZFC. Tanto el trabajo de Gödel como el de Cohen parten del popular supuesto de que la axiomática de ZFC no contiene contradicciones.

Tomemos un cardinal arbitrario α, consideremos $\{\beta \in \mathbf{Card} | \alpha < \beta\}$ y definamos

---

[32] David Hilbert (1862 - 1943), matemático alemán, uno de los más influyentes de la transición entre los siglos XIX y XX. En el Congreso Internacional de Matemáticos de 1900, con sede en París, propuso una lista de 23 problemas, que a la postre demostraron ser la columna vertebral de la investigación matemática en el siglo XX.

[33] Kurt Gödel (1906 - 1978), matemático húngaro. Cuando buscaba asilo político en los Estados Unidos, con la ayuda de su amigo personal Albert Einstein, propuso hacer algunas modificaciones a la Constitución Política de ese país, con el fin de evitar una dictadura. Muere de inanición víctima de su paranoia, la que le hacía creer que había personas interesadas en envenenarlo.

[34] Paul Joseph Cohen (1934 - 2007), matemático norteamericano. En 1966 le fue concedida la *medalla Fields* por sus trabajos en la Hipótesis del Continuo, lo que también le mereció la *Medalla Nacional de Ciencias* de los Estados Unidos. Es el único matemático en ganar la Fields por un trabajo en Lógica Matemática.

$$\alpha^+ = \text{mín}\{\beta \in \mathbf{Card} | \alpha < \beta\}.$$

Los números transfinitos pueden ser entonces definidos recursivamente mediante

$$\aleph_{k+1} = \aleph_k^+,$$

lo cual, de acuerdo con la hipótesis del continuo generalizada puede ser escrito como

$$\aleph_{k+1} = 2^{\aleph}_k.$$

La expresión anterior es una bella construcción que, debido a su independencia lógica podría adoptarse como uno más de los axioma de la Teoría de los conjuntos de Zermelo-Fraenkel-Cantor.

Por otra parte, la cardinalidad de la recta real es otro de los interrogantes se sumo interés. Para calcularla notemos que todo número real x en el intervalo $[0,1]$ puede ser escrito en base 2 como la serie

$$x = \sum_{k=1}^{\infty} \frac{x_n}{2^n}$$

donde $x \in \{0,1\}$, es decir, cada una de estas series, y en consecuencia cada uno de estos números reales se asocia de forma única con una función

$$\mathbb{N} \to \{0,1\}$$

con lo que

$$\#[0,1] = 2^{\#(\mathbb{N})} = \#(\mathcal{P}(\mathbb{N})),$$

es decir, dado que $[0,1]$ y $\mathbb{R}$ tienen la misma cardinalidad, entonces

$$\#[0,1] = 2^{\aleph_0} = \aleph_1 = \#(\mathbb{R}).$$

El siguiente resultado es un teorema de la Teoría de los Conjuntos de ZFC, sin embargo, si A es un conjunto arbitrario, la afirmación que sigue es equivalente con la hipótesis del continuo.

Teorema 41 *Si $A \subseteq \mathbb{R}$ es un conjunto de Borel, entonces $\#(A) = \#(\mathbb{N})$ ó bien $\#(A) = \#(\mathbb{R})$.*

Un *conjunto de Borel*[35] es un conjunto que se obtiene mediante uniones e intersecciones a lo sumo numerables, de abiertos y cerrados de la recta real.

La hipótesis del continuo, dada su independencia lógica, puede incorporarse como un axioma más en la Teoría de los conjuntos. Una vez hecha la incorporación, podemos referirnos al cuerpo teórico como *la axiomática de Zermelo-Fraenkel-Cantor-Cohen* (ZFCC).

[35]Félix Édouard Justin Émile Borel (1871 - 1956), matemático y político francés.

Referencias

[1] Bourbaki, N. *Theory of Sets*. Hermann Publishers, California, 1968.

[2] Barnes, Donald W and Mack, John M. *Una Introducción Matemática a la Lógica*. Editorial Unibar, Barcelona, 1978.

[3] Couturant, Louis. *L'algebre de la Logique*. Albert Blanchard, Paris, 1980.

[4] Davis, Sheldon. *Topology*. MacGraw Hill, New York, 2005.

[5] Enderton, H. B. *Una Introducción Matemática a la Lógica*. UNAM, México, 1987.

[6] Halmos, Paul R. *Naive Set Theory*. Van Nostrand Co., New York, 1961.

[7] Hawking,Stephen W. "Cohen and Set Theory", *The Bulletin of Symbolic Logic*. **14**-3 (2008), 351-378.

[8] Kamke, E. *Theory of Sets*. Dover Publications, New York, 1950.

[9] Kelley, John L. *General Topology*. Van Nostrand Co., New York, 1955.

[10] Zuckerman,Martin M. *Sets and Transfinite Numbers*. Macmilllan., New York, 1974.

Índice alfabético

Zacatecas, Zac., noviembre 24 de 2012