Ramón Espinosa Armenta

MATEMÁTICAS *DISCRETAS*

2ª edición

Contenidos Interactivos Web

Alfaomega

Matemáticas Discretas

2ª. edición

Ramón Espinosa Armenta

Alfaomega

Buenos Aires • Bogotá • Ciudad de México • Santiago de Chile

Director Editorial:
Marcelo Grillo Giannetto
mgrillo@alfaomega.com.mx

Jefe de Edición:
Francisco Javier Rodríguez Cruz
jrodriguez@alfaomega.com.mx

Datos catalográficos

Espinosa, Ramón
Matemáticas discretas
Segunda Edición
Alfaomega Grupo Editor, S.A. de C.V., México

ISBN: 978-607-622-752-7

Formato: 17 x 23 cm Páginas: 508

Matemáticas discretas
Ramón Espinosa Armenta

Segunda edición: Alfaomega Grupo Editor, México, diciembre 2016

Dr. Isidoro Olvera (Eje 2 Sur) No. 74, Col. Doctores, C.P. 06720, Ciudad de México

Miembro de la Cámara Nacional de la Industria Editorial Mexicana
Registro No. 2317

Pág. Web: **http://www.alfaomega.com.mx**
E-mail: **atencionalcliente@alfaomega.com.mx**

ISBN: 978-607-622-752-7

Impreso en México. Printed in Mexico.

Empresas del grupo:

México: Alfaomega Grupo Editor, S.A. de C.V. – Dr. Isidoro Olvera (Eje 2 sur) No. 74, Col. Doctores, C.P. 06720, Del. Cuauhtémoc, Ciudad de México – Tel.: (52-55) 5575-5022 – Fax: (52-55) 5575-2420 / 2490. Sin costo: 01-800-020-4396 – E-mail: atencionalcliente@alfaomega.com.mx

Colombia: Alfaomega Colombiana S.A. – Calle 62 No. 20-46, Barrio San Luis, Bogotá, Colombia, Tels.: (57-1) 746 0102 / 210 0415 – E-mail: cliente@alfaomega.com.co

Chile: Alfaomega Grupo Editor, S.A. – Av. Providencia 1443. Oficina 24, Santiago, Chile Tel.: (56-2) 2235-4248 – Fax: (56-2) 2235-5786 – E-mail: agechile@alfaomega.cl

Argentina: Alfaomega Grupo Editor Argentino, S.A. – Av. Córdoba 1215, piso 10, CP: 1055, Buenos Aires, Argentina, – Tel./Fax: (54-11) 4811-0887 y 4811 7183 – E-mail: ventas@alfaomegaeditor.com.ar

Acerca del autor

Ramón Espinosa Armenta es egresado de la Universidad Nacional Autónoma de México (UNAM), donde obtuvo el título de Matemático y los grados de Maestro en Ciencias (Matemáticas) y Doctor en Ingeniería (Investigación de Operaciones). De 1983 a 1988 fue profesor de tiempo completo en la Universidad Autónoma Metropolitana. Desde 1989 es profesor de tiempo completo en el Departamento Académico de Matemáticas del ITAM.

A mi esposa Ely
y a mis hijos David Gibrán y Mariana,
con todo mi amor

Agradecimientos

Al profesor César Rincón, por aquellas inolvidables clases de Álgebra Superior, en la Facultad de Ciencias de la UNAM, que me abrieron las puertas al mundo mágico de las matemáticas.

A Jorge Urrutia, por aquella tarde de domingo, hace más de treinta años, cuando me mostró por primera vez la belleza e importancia de las matemáticas discretas.

A Javier Alfaro y a Marcela González, por más de veinticinco años de retroalimentación constante acerca de la enseñanza del álgebra y las matemáticas discretas. A Shyamal Kumar, por aquellas tardes en las que compartimos nuestras experiencias acerca del galano arte de escribir. A Adolfo Torres Cházaro, por sus valiosos comentarios acerca de la presentación del material en muchas partes del texto.

A la editorial Alfaomega; por su apoyo particular, a Marcelo Grillo, gerente editorial, y muy especialmente al editor Francisco Javier Rodríguez Cruz, cuyos comentarios y notas enriquecieron el libro; fue un placer trabajar con él.

Especialmente a mi hija Mariana, por haber leído cuidadosamente el libro, señalándome errores y comentando acerca del contenido. A mi esposa Ely y a mis hijos David Gibrán y Mariana, por su amor, aliento y apoyo constante.

Por último, agradezco el apoyo de la Asociación Mexicana de Cultura, A. C. y del Instituto Tecnológico Autónomo de México, para la realización de esta obra.

Ramón Espinosa Armenta
Ciudad de México, 2016

Contenido

Prólogo

Lo último que se sabe cuando se escribe un libro
es qué poner primero

Blas Pascal

Un conjunto es discreto si sus elementos están separados. Los conjuntos finitos y los subconjuntos infinitos de números enteros son conjuntos discretos, pero el conjunto de los números reales no lo es. La matemática discreta es el estudio de estructuras matemáticas definidas sobre conjuntos discretos. Aunque los orígenes de la matemática discreta se remontan a la antigüedad, no ha sido sino hasta años recientes que ha cobrado importancia, por sus aplicaciones a diversos campos, en particular a las ciencias de la computación y a la investigación de operaciones.

La presente obra está dirigida a estudiantes de ciencias básicas e ingeniería. Se ha dividido en cuatro partes: Fundamentos, Métodos algebraicos, Enumeración combinatoria y Teoría de grafos. Las últimas tres partes son casi independientes entre sí.

El propósito de la primera parte es familiarizar al alumno con el lenguaje de las matemáticas modernas y con los métodos de demostración, incluyendo el método de inducción matemática. Los cinco capítulos que constituyen esta parte son fundamentales para entender el resto del libro.

La segunda parte está dedicada al estudio de métodos algebraicos. El capítulo 6 es independiente de los demás, pero es recomendable verlo antes de ver la sección de problemas *NP*-completos en el capítulo 7, el cual también es independiente. En este capítulo se discute el problema de computabilidad y la noción de complejidad computacional; es necesario ver la sección de complejidad computacional antes de estudiar la parte IV. Así mismo se recomienda ver el capítulo 8 antes del 9 y 10, que son independientes entre sí. En estos capítulos aparecen diversas aplicaciones: circuitos lógicos, el sistema criptográfico RSA y códigos de grupo.

La tercera parte está dedicada a la enumeración combinatoria. El capítulo 11 es prerrequisito de los demás capítulos de esta parte, los cuales son casi independientes entre sí, con una excepción, la última sección del capítulo de relaciones de recurrencia utiliza la noción de función generadora ordinaria, discutida en el capítulo 13.

La última parte es una breve introducción a la teoría de grafos. En el capítulo 15 se presentan los conceptos básicos, por lo que es prerrequisito de los demás capítulos. El capítulo 16 está dedicado a la importante noción de árbol, mientras que el 17 trata sobre la noción de grafo dirigido; por último, en el capítulo 18 se presentan temas selectos de la teoría de grafos, los cuales son casi independientes entre sí, con excepción de la sección dedicada al problema de los cuatro colores, que utiliza conceptos de grafos aplanables y coloración de vértices.

Registro en la Web de apoyo

Para tener acceso al material de la plataforma de contenidos interactivos de este libro, siga los siguientes pasos:

1. Ir a la página: http://libroweb.alfaomega.com.mx
2. Registrarse como usuario del sitio y propietario del libro.
3. Ingresar al apartado de inscripción de libros y registrar la siguiente clave de acceso:

4. Para navegar en la plataforma virtual de recursos del libro, usar los nombres de Usuario y Contraseña definidos en el punto número dos. El acceso a estos recursos es limitado. Si quiere un número extra de accesos envíe un correo electrónico a webmaster@alfaomega.com.mx.

Estimado profesor: si desea acceder a los contenidos exclusivos para docentes, contacte al representante de la editorial que lo suele visitar o envíe un correo electrónico a webmaster@alfaomega.com.mx.

Parte I

Fundamentos

CAPÍTULO 1

Lógica y conjuntos

La lógica, como el whisky, pierde sus efectos benéficos cuando se consume en grandes cantidades.

Lord Dunsany

Objetivos

- Exponer las reglas de inferencia y los métodos de demostración.
- Presentar la notación y terminología básica de la teoría de conjuntos.

*Ver *Plataforma de contenidos interactivos*.

1.1 Introducción

Uno de los principales propósitos de la lógica consiste en proporcionar reglas, por medio de la cuales se pueda determinar si un argumento particular es correcto. La lógica se interesa en cualquier tipo de razonamiento, los cuales pueden ser, por ejemplo, argumentos legales, demostraciones matemáticas o conclusiones científicas, basadas todas ellas en ciertas suposiciones.

La teoría moderna de conjuntos comenzó con los trabajos de los matemáticos alemanes Georg Cantor y Richard Dedekind, a fines del siglo XIX. El uso libre de la noción intuitiva de conjunto condujo a paradojas, lo que motivó a Ernest Zermelo a desarrollar en 1908 una teoría axiomática de conjuntos. La teoría fue perfeccionada en 1922 por Abraham Fraenkel. Actualmente la teoría de conjuntos juega un papel fundamental en las matemáticas modernas, pues casi todos los conceptos matemáticos importantes están definidos en términos de conjuntos.

En este capítulo veremos una breve introducción a la lógica simbólica y a la teoría de conjuntos.

1.2 Proposiciones y conectivos lógicos

Una **proposición** es una afirmación que puede ser verdadera o falsa, pero no ambas. Si una proposición es verdadera decimos que su **valor de verdad** es verdadero (V); si la proposición es falsa decimos que su valor de verdad es falso (F).

Ejemplo 1.1.

Las siguientes afirmaciones son proposiciones:

a) Guadalupe Victoria fue el primer presidente de México.
b) Hay un premio Nobel de Matemáticas.
c) Estaba lloviendo en Tenochtitlan el día en el que murió Lorenzo de Médicis.

De las proposiciones anteriores, (a) es verdadera, (b) es falsa, y (c) podría ser verdadera o falsa; sin embargo, es claro que ese día llovió o no en Tenochtitlan, y por lo tanto, podemos asegurar que la afirmación es una proposición.

Ejemplo 1.2.

Las siguientes afirmaciones no son proposiciones:

a) Cierra la puerta.

b) ¡Buenos días!

c) Esta afirmación es falsa.

La afirmación (a) no es una proposición, porque no es verdadera o falsa (es una orden). La afirmación (b) tampoco es verdadera o falsa, es simplemente un saludo. Por último, la afirmación (c) no es una proposición, porque, si suponemos que es verdadera, entonces la afirmación es falsa; análogamente, si la consideramos como falsa, entonces la afirmación es verdadera.

La **negación** de una proposición p, es la proposición $\neg p$, que se lee como "no p". La proposición $\neg p$ tiene el valor de verdad V cuando p tiene el valor de verdad F, y tiene el valor de F cuando p tiene el valor de verdad V . Es decir, $\neg p$ tiene la siguiente tabla de verdad.

p	$\neg p$
V	F
F	V

Ejemplo 1.3.

La negación de la proposición:

p: Está nublado.

Es la proposición:

$\neg p$: Está despejado.

La **conjunción** de dos proposiciones p y q , es la proposición $p \wedge q$, que se lee "p y q". La proposición $p \wedge q$ tiene el valor de verdad V cuando tanto p como q tienen el valor de verdad V, en otro caso su valor de verdad es F. La tabla de verdad de la conjunción es:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Ejemplo 1.4. Consideremos las proposiciones:

p: Está nublado.

q: Hace frío.

La conjunción de estas proposiciones es la proposición:

$p \wedge q$: Está nublado y hace frío.

La **disyunción** de dos proposiciones p y q es la proposición $p \vee q$, que se lee "p o q". Esta proposición $p \vee q$ tiene el valor de verdad F sólo cuando tanto p como q tienen el valor de verdad F, en otro caso su valor de verdad es V. Obsérvese que el operador $\vee$ representa un "o inclusivo".

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Ejemplo 1.5. Consideremos de nuevo las proposiciones:

p: Está nublado.

q: Hace frío.

La disyunción de estas proposiciones es la proposición:

$p \vee q$: Está nublado o hace frío.

Esta proposición es verdadera si está nublado (aunque no haga frío), o si hace frío (aunque esté despejado), o si está nublado y hace frío. La proposición solamente es falsa si está despejado y no hace frío.

Los símbolos $\neg$, $\vee$, $\wedge$, son ejemplos de **conectivos lógicos**. Una proposición formada de la combinación de otras proposiciones utilizando conectivos lógicos es una **proposición compuesta**. Si las proposiciones $p_1, p_2, \ldots, p_n$ se combinan para formar la proposición compuesta p, se escribirá: $p = p(p_1, p_2, \ldots, p_n)$.

Ejemplo 1.6.

Escribir la tabla de verdad de la proposición compuesta

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

Solución:

p	q	r	$p \wedge q$	$\neg r$	$(p \wedge q) \vee (\neg r)$
V	V	V	V	F	V
V	V	F	V	V	V
V	F	V	F	F	F
F	V	V	F	F	F
F	F	V	F	F	F
F	V	F	F	V	V
V	F	F	F	V	V
F	F	F	F	V	V

Se dice que una proposición compuesta a $p = p(p_1, p_2, \ldots, p_n)$ es una **tautología**, si p es verdadera para todos los valores de verdad que se asignen a $p_1, p_2, \ldots, p_n$. Diremos que p es una **contradicción** si es falsa para todos los valores de verdad que se asignen a $p_1, p_2, \ldots, p_n$. Obsérvese que la negación de una tautología es una contradicción y que la negación de una contradicción es una tautología.

Ejemplo 1.7.

La siguiente tabla de verdad muestra que $p \vee \neg p$ es una tautología y que $p \wedge \neg p$ es una contradicción.

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
V	F	V	F
F	V	V	F

1.3 Implicación y equivalencia lógica

El **operador condicional**, denotado por el símbolo $\rightarrow$, está definido por la siguiente tabla de verdad:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

La proposición compuesta $p \to q$ es llamada **proposición condicional**. En este caso la proposición p se llama **hipótesis** (o **antecedente**) y la proposición q se llama **conclusión** (o **consecuente**). La proposición condicional puede expresarse como:

si p entonces q
p sólo si q,
p implica q,
p es una condición suficiente para q,
q es una condición necesaria para p.

Ejemplo 1.8.

En cierta universidad, el reglamento estipula que para aprobar un curso es necesario que el alumno apruebe el examen final. Esta afirmación se puede representar como $p \to q$, donde

p: aprueba el curso,
q: aprueba el examen final.

Obsérvese que la condición q es necesaria, pero no suficiente para p , es decir, si aprueba el examen final no necesariamente aprueba el curso.

Sean $p = p(p_1, p_2, \ldots, p_n)$ y $q = q(p_1, p_2, \ldots, p_n)$ dos proposiciones compuestas, diremos que p **implica lógicamente** a q si $p \to q$ es una tautología. En este caso escribimos $p \Rightarrow q$.

Ejemplo 1.9.

Si p y q son dos proposiciones, entonces $p \wedge q \Rightarrow p$, como lo muestra la siguiente tabla de verdad.

p	q	$p \wedge q$	$p \wedge q \to p$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

La **recíproca** de la proposición condicional $p \to q$ es la proposición $q \to p$. Es posible que una proposición condicional sea verdadera, pero que su recíproca sea falsa.

El **operador bicondicional**, denotado por el símbolo $\leftrightarrow$, está definido por la siguiente tabla de verdad:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Obsérvese que $p \leftrightarrow q$ es verdadera sólo cuando los valores de verdad de p y q coinciden. La proposición compuesta $p \leftrightarrow q$ se llama **proposición bicondicional**. Esta proposición se lee: "p si y sólo si q". La abreviación "sii" se utiliza con frecuencia para representar la frase "si y sólo si".

Sean $p = p(p_1, p_2, \ldots, p_n)$ y $q = q(p_1, p_2, \ldots, p_n)$ dos proposiciones compuestas, diremos que p y q son **lógicamente equivalentes** si $p \leftrightarrow q$ es una tautología. En este caso escribimos $p \Leftrightarrow q$. En otras palabras, dos proposiciones compuestas son lógicamente equivalentes si y sólo si sus valores de verdad coinciden.

Ejemplo 1.10.

La proposición bicondicional $p \leftrightarrow q$ es lógicamente equivalente a la proposición $n\ (p \to q) \wedge (q \to p)$, como lo muestra la siguiente tabla de verdad.

p	q	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Por esta razón la proposición bicondicional $p \leftrightarrow q$ también puede expresarse como: "p es una condición necesaria y suficiente para q".

Ejemplo 1.11.

La siguiente tabla de verdad muestra que la proposición $\neg(p \to q)$ es lógicamente equivalente a la proposición $p \wedge \neg q$.

p	q	$\neg q$	$\neg(p \to q)$	$p \wedge \neg q$
V	V	F	F	F
V	F	V	V	V
F	V	F	F	F
F	F	V	F	F

Ejemplo 1.12.

La **contrarrecíproca** de la proposición condicional $p \to q$ es la proposición $\neg q \to \neg p$. La siguiente tabla muestra que toda proposición condicional es lógicamente equivalente a su contrarrecíproca.

p	q	$p \to q$	$\neg q \to \neg p$	$(p \to q) \leftrightarrow (\neg q \to \neg p)$
V	V	V	V	V
V	F	F	F	V
F	V	V	V	V
F	F	V	V	V

Ejemplo 1.13.

La siguiente tabla muestra que la implicación condicional $p \to q$ es lógicamente equivalente a la proposición $p \wedge \neg q \to c$, donde c es una contradicción.

p	q	$\neg q$	$p \wedge \neg q$	c	$p \wedge \neg q \to c$
V	V	F	F	F	V
V	F	V	V	F	F
F	V	F	F	F	V
F	F	V	F	F	V

1.4 Reglas de inferencia

Un **argumento lógico** es una sucesión de proposiciones escritas como sigue:

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ p_n \\ \hline \therefore\ q \end{array}$$

Las proposiciones $p_1, p_2, \ldots, p_n$ son llamadas **hipótesis** o **premisas**; la proposición q es la **conclusión**. El símbolo $\therefore$ se lee como "por lo tanto", o "por consiguiente", "se sigue que" o "de aquí que". Se dice que un argumento lógico es **válido** si

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \Rightarrow q$$

se cumple, es decir, $p_1 \wedge p_2 \wedge \cdots \wedge p_n \rightarrow q$ es una tautología. Los argumentos lógicos válidos también son llamados **reglas de inferencia**. Una **falacia** es un argumento lógico que no es válido. A continuación describimos las principales reglas de inferencia.

Adición

$$\begin{array}{l} p \\ \hline \therefore\ p \vee q \end{array}$$

Simplificación

$$\begin{array}{l} p \wedge q \\ \hline \therefore\ p \end{array}$$

Silogismo disyuntivo

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore\ q \end{array}$$

Silogismo hipotético

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore\ p \rightarrow r \end{array}$$

Conjunción

$$\begin{array}{l} p \\ q \\ \hline \therefore\ p \wedge q \end{array}$$

Modus ponens

$$\frac{\begin{array}{c} p \\ p \rightarrow q \end{array}}{\therefore q}$$

Modus tollens

$$\frac{\begin{array}{c} \neg q \\ p \rightarrow q \end{array}}{\therefore \neg p}$$

Lo que distingue a las matemáticas de otras disciplinas, es que, a excepción de ciertas afirmaciones básicas llamadas **axiomas**, nada es considerado como cierto a menos que que haya sido probado utilizando un argumento lógico válido.

Una **demostración** es una sucesión de afirmaciones que representan una argumentación de la validez de un enunciado matemático. Algunas de las afirmaciones que aparecen en una demostración pueden considerarse verdades *a priori*, éstas incluyen axiomas, definiciones o resultados establecidos previamente. Otras pueden ser las hipótesis del enunciado, las cuales se suponen verdaderas en el argumento. Por último, algunas pueden ser inferidas de otras afirmaciones cuya validez fue probada al principio de la demostración.

Supongamos que queremos probar un enunciado de la forma: si P entonces Q. Una demostración **directa** comienza suponiendo que P es verdadera y de ahí concluye que Q es verdadera. Una demostración **indirecta** comienza suponiendo que $\neg Q$ es verdadera y de ahí concluye que $\neg P$ es verdadera. Una demostración por **contradicción** o **reducción al absurdo**, comienza suponiendo que P es verdadera y Q es falsa, con lo cual se llega a una contradicción; esto significa que la conclusión debe ser verdadera.

Una proposición matemática cuya veracidad ha sido probada es llamada un **teorema**. Un **lema** es un resultado que no es considerado importante, pero que es útil para probar un teorema. Un resultado que puede probarse fácilmente a partir de un teorema se considera un **corolario** de ese teorema. Cabe mencionar que, en libros avanzados y en artículos de investigación, los teoremas sencillos se enuncian como proposiciones (dando a esta palabra un significado distinto al que se ha utilizado en este capítulo), utilizando la palabra, teorema, solamente para los resultados más importantes. Claramente esta distinción es subjetiva; algunos autores se han visto muy modestos enunciando como proposiciones, o incluso como lemas, resultados que a la postre han mostrado ser importantes.

Entender la demostración de un teorema requiere con frecuencia de un gran esfuerzo. Cada paso de una demostración debe tener una justificación lógica, la cual no siempre es fácil de encontrar. Al leer una demostración, el lector debe tratar de entender cuáles son las ideas matemáticas detrás de ese razonamiento, pues sólo así será capaz de

hacer demostraciones por sí mismo. Al escribir una demostración o la solución de un problema matemático, el lector debe procurar ser lo más claro, conciso y preciso posible.

Las matemáticas no son fáciles (ni siquiera para los matemáticos profesionales), el lector no debe desilusionarse si siente que no puede avanzar tan rápido como quisiera. El trabajo constante y sistemático tarde o temprano comienza a rendir frutos. Con el tiempo el estudiante aprenderá a disfrutar de las matemáticas, de la misma manera que puede disfrutar de la música o de la literatura.

1.5 Conjuntos

Hasta principios del siglo XX, un conjunto era entendido como cualquier colección de objetos de nuestra intuición o imaginación. En 1902, el matemático *Gotlob Frege* estaba a punto de publicar un monumental trabajo, en el cual la aritmética se construía sobre la base de esta noción de conjunto. En este punto, Frege recibió una carta de *Bertrand Russell*, tras lo cual decide añadir el siguiente párrafo, con el que termina el segundo volumen de su obra: "Nada es menos apetecible para un hombre de ciencia, que cuando está a punto de terminar su obra se le derrumben los cimientos. En esta situación me coloca una carta del señor Bertrand Russell, recibida cuando la obra estaba a punto de salir de la imprenta."

En su carta, Russell planteaba la siguiente paradoja: Existen dos tipos de conjuntos, los conjuntos regulares y los conjuntos no regulares. Los conjuntos regulares son aquellos que no se contienen a sí mismos como elementos. Un ejemplo de un conjunto no regular es el conjunto de todos los conjuntos describibles con menos de cincuenta palabras en español.

Consideremos ahora el conjunto R, cuyos elementos son todos los conjuntos regulares. Ahora bien, R mismo debe ser un conjunto regular o un conjunto no regular. Si R es regular, entonces se contiene a sí mismo como elemento, y por lo tanto es no regular, lo cual es una contradicción. Pero si R es no regular, entonces R no se contiene a sí mismo como elemento y es por lo tanto regular, lo cual otra vez es una contradicción.

La moraleja es ésta: el uso libre de la noción intuitiva de 'conjunto' puede conducir a contradicciones. La noción de conjunto puede servir como base firme para las matemáticas sólo si se emplea una aproximación más sofisticada.

En 1908, *Ernest Zermelo* estableció las bases de una teoría axiomática de conjuntos. Esta teoría fue perfeccionada en 1922 por *Abraham Fraenkel*. La definición de 'conjunto' no está incluida en esta teoría; en lugar de ello los axiomas describen lo que uno puede hacer con conjuntos. Veremos a continuación la notación y terminología básica de la teoría de conjuntos.

Un **conjunto**, como se le entiende intuitivamente, tiene **elementos**. Si A es un conjunto y x es un elemento de A escribiremos $x \in A$. En este caso también se acostumbra decir que x **pertenece** a A. La notación $x \notin A$ significa que x no es un elemento de A (o que x **no pertenece** a A). La propiedad más importante de la pertenencia la establece el siguiente axioma.

Axioma de extensión. Dos conjuntos A y B son **iguales** si cada elemento de A pertenece a B, y cada elemento de B pertenece a A. En este caso escribimos $A = B$.

Una manera de describir un conjunto es enlistando sus elementos. Por ejemplo,

$$\{3, \spadesuit, b\}$$

es el conjunto cuyos elementos son 3, ♠ y b. El orden en que aparecen los elementos es irrelevante, así

$$\{3, \spadesuit, b\} = \{3, b, \spadesuit\} = \{\spadesuit, 3, b\} = \{\spadesuit, b, 3\} = \{b, 3, \spadesuit\} = \{3, b, \spadesuit\}$$

Si existe un elemento en un conjunto que no pertenece al otro conjunto, diremos que los conjuntos son **distintos** y escribiremos $A \neq B$. Por ejemplo,

$$\{a, b, c\} \neq \{a, c\}.$$

Axioma del conjunto vacío. Existe un conjunto que no tiene elementos.

El axioma de extensión implica que sólo puede haber un conjunto sin elementos. Este conjunto se denota por el símbolo $\varnothing$ y es llamado el **conjunto vacío.**[1]

Sean A y B dos conjuntos. Se dice que A es un **subconjunto** de B, si todo elemento de A pertenece a B. En este caso escribimos $A \subseteq B$. También se dice que B **contiene** a A. Si $A \subseteq B$ pero $A \neq B$, diremos que A es un **subconjunto propio** de B, y escribiremos $A \subset B$. Obsérvese que $A = B$ si y sólo si $A \subseteq B$ y $B \subseteq A$.

Ejemplo 1.14.

Todo conjunto A es un subconjunto de sí mismo, es decir, $A \subseteq A$, pero no es un subconjunto propio de sí mismo.

Ejemplo 1.15.

El conjunto vacío $\varnothing$ es un subconjunto de cualquier conjunto A, porque si no fuera así existiría $x \in \varnothing$ tal que $x \notin A$, lo cual no es posible, porque el conjunto vacío no tiene elementos.

[1] El símbolo que se utiliza para denotar el conjunto vacío, proviene de la letra ∅ en el alfabeto noruego, y fue presentado por André Weil en 1939.

Ejemplo 1.16.

Sean A, B y C conjuntos tales que $A \subseteq B$ y $B \subset C$. Probar que $A \subset C$.

Demostración. Sea $a \in A$, como $A \subseteq B$ se sigue que $a \in B$, y como $B \subset C$, tenemos que $a \in C$, y por lo tanto $A \subseteq C$. Por otra parte, como $B \subset C$, existe $c \in C$ tal que $c \notin B$ y por lo tanto $c \notin A$. De ahí que $A \subset C$.

Axioma del conjunto potencia. Para cualquier conjunto X existe un conjunto cuyos elementos son todos los subconjuntos de X.

El único conjunto cuyos elementos son todos los subconjuntos de X, es llamado el **conjunto potencia** de X, y se denota $\wp(X)$. Obsérvese que $\varnothing \in \wp(X)$ y $X \in \wp(X)$.

Ejemplo 1.17.

Si $X = \{a, b\}$, entonces

$$\wp(X) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$$

Ejemplo 1.18.

Si $X = \{a, b, c\}$ entonces

$$\wp(X) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Hemos visto que los elementos de un conjunto pueden ser conjuntos por sí mismos. Sin embargo, la teoría de conjuntos incluye un axioma, llamado **axioma de regularidad**, que garantiza que un conjunto no se puede contener a sí mismo como elemento.

1.6 Predicados y cuantificadores

Enunciados como "x es mexicano" o "a es hijo de b", no son proposiciones, ya que no son necesariamente verdaderos o falsos. Sin embargo, cuando asignamos valores a las variables que intervienen en estas afirmaciones éstas se convierten en proposiciones. Este tipo de enunciados son llamados **predicados**.

El predicado "x es mexicano" puede representarse como $P(x)$, análogamente el predicado "a es hijo de b" puede representarse como $Q(a, b)$. Los valores de las variables que aparecen en un predicado deben pertenecer a un conjunto, llamado el **universo de discurso** (o simplemente **universo**). Para ser precisos es necesario establecer explícitamente el universo de discurso; sin embargo, con frecuencia el universo de discurso se entiende implícitamente.

El principio más importante de la teoría de conjuntos es el siguiente.

Axioma de especificación. Dado un conjunto X y un predicado $P(x)$, existe un conjunto cuyos elementos son aquellos elementos $x \in X$ para los cuales $P(x)$ es verdadera.

Utilizaremos la notación

$$\{x \in X \mid P(x)\},$$

para denotar al conjunto de elementos de X para los cuales $P(x)$ es verdadera. También podemos escribir

$$\{P(x) \mid x \in X\}.$$

Por ejemplo, si X es el conjunto de todos los seres humanos, podemos escribir

$$M = \{m \in X \mid m \text{ es mujer}\}$$

para denotar al conjunto de las mujeres.

Una manera de convertir un predicado en una proposición es asignar un valor a cada una de las variables. Otra manera, utilizada con frecuencia en matemáticas, es cuantificar las variables para las cuales el predicado es válido.

El **cuantificador universal** $\forall$ se utiliza para construir proposiciones como:

$$\forall\, x \in X \qquad P(x)$$

que se lee: "para toda $x \in X$, $P(x)$ es verdadera". La proposición anterior es verdadera sólo si $P(x)$ es verdadera para cualquier valor de x en el universo de discurso X. El símbolo $\forall$ puede leerse "para todo", "para cada" o "para cualquier".

El **cuantificador existencial** $\exists$ se utiliza para construir proposiciones de la forma:

$$\exists\, x \in X \qquad P(x)$$

que significa "existe $x \in X$ tal que $P(x)$ es verdadera". El símbolo $\exists$ puede leerse "existe", o "para algún" o "para al menos un".

La negación de la proposición

$$\forall\, x \in X \qquad P(x)$$

es la proposición

$$\exists\, x \in X \qquad \neg P(x).$$

Equivalentemente, para mostrar que la proposición $\forall\, x \in X\, P(x)$ es falsa, basta exhibir un elemento $x \in X$ tal que $P(x)$ sea falsa. Tal elemento es llamado un **contraejemplo**.

Análogamente, la negación de la proposición

$$\exists\, x \in X \qquad P(x)$$

es la proposición

$$\forall\, x \in X \qquad \neg P(x).$$

Para mostrar que una afirmación de la forma:

$$\forall\, x \in X \qquad P(x) \Rightarrow Q(x)$$

es falsa, hay que encontrar un elemento $x \in X$ para el cual $P(x)$ sea verdadera y $Q(x)$ sea falsa.

Algunas proposiciones involucran más de un cuantificador. Por ejemplo, la negación de la proposición:

$$\forall\, a \in A \quad \exists\, b \in B \quad P(a, b),$$

es la proposición:

$$\exists\, a \in A \quad \forall\, b \in B \quad \neg P(a, b).$$

1.7 Operaciones con conjuntos

En esta sección supondremos que todos los conjuntos en consideración son subconjuntos de un conjunto X.

La **unión** de dos conjuntos A y B es el conjunto

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$