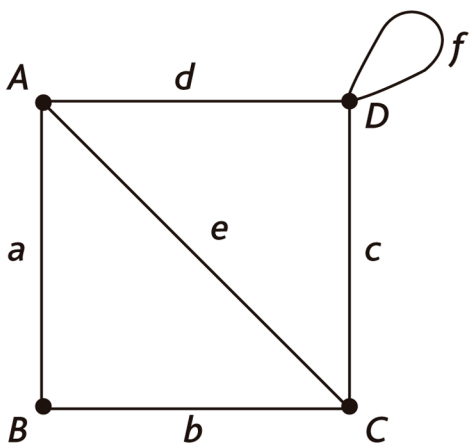


MATEMÁTICA DISCRETA

Segunda edición

J. C. Ferrando / V. Gregori



EDITORIAL REVERTÉ

MATEMÁTICA DISCRETA

Segunda edición

MATEMÁTICA DISCRETA

Segunda edición

J. C. Ferrando / V. Gregori

Profesores de la Universidad
Politécnica de Valencia.

Departamento de Matemática Aplicada.



EDITORIAL
REVERTÉ

Barcelona · Bogotá · Buenos Aires · Caracas · México

Matemática discreta

J. C. Ferrando, V. Gregori

Copyright © J. C. Ferrando, V. Gregori

Edición en español:

© Editorial Reverté. S.A., 1995

Edición en papel

ISBN: 978-84-291-5179-4

Edición ebook (PDF)

ISBN: 978-84-291-9141-7

Propiedad de:

EDITORIAL REVERTÉ, S. A.

Loreto, 13-15. Local B

Tel: (34) 93 419 33 36

Fax: (34) 93 419 51 89

08029 Barcelona. España

reverte@reverte.com

www.reverte.com

Reservados todos los derechos. La reproducción total o parcial de esta obra, por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares de ella mediante alquiler o préstamo públicos, queda rigurosamente prohibida sin la autorización escrita de los titulares del copyright, bajo las sanciones establecidas por las leyes.

A Maite y Carlos
A Amalia, Manuela y Amalia.

PRÓLOGO DEL PROFESOR CARLOS RENTERÍA

Este libro tiene como finalidad primordial ayudar a los estudiantes a conseguir un conocimiento más completo y una mayor destreza en los fundamentos de la matemática discreta. Los autores prestan gran atención al aspecto algorítmico de la matemática, el cual es actualmente indispensable no sólo para la matemática aplicada, sino también para la matemática pura. Se hace una exposición amena y clara de las estructuras algebraicas básicas, a saber, grupos anillos y cuerpos y son hábilmente utilizadas en el resto de la obra. Cada capítulo empieza estableciendo con claridad sus objetivos y definiciones, los teoremas, proposiciones, etc. van acompañados de ejemplos que fortalecen y clarifican su demostración; al final de cada capítulo se presentan ejercicios resueltos que permiten establecer un diálogo interactivo con el estudiante y sirven para ilustrar y ampliar la teoría, enfocan con amplia y aguda perspectiva los aspectos teóricos que son considerados como de difícil comprensión para el estudiante.

Finalmente quiero felicitar a los autores por la claridad de exposición y la acertada selección de los temas.

Dr. Carlos Rentería Márquez
Escuela Superior de Física y Matemáticas
Instituto Politécnico Nacional, México.
Profesor Titular

PREFACIO A LA SEGUNDA EDICIÓN

En esta segunda edición hemos revisado cuidadosamente el texto original, aunque el cambio más importante respecto a la primera sea la inclusión de un Apéndice sobre Lógica de Predicados y Sistemas Formales. Se cubre así una necesidad didáctica que cobra cada día más relevancia en los nuevos planes de estudio de ingeniería informática y se completa de paso la exposición de la lógica proposicional del Capítulo I.

Juan Carlos Ferrando
Valentín Gregori

PREFACIO A LA PRIMERA EDICIÓN

Últimamente parecen estar cobrando un mayor protagonismo los aspectos llamados *algorítmicos* de las matemáticas, en detrimento de los llamados *dialécticos*. Esto quiere decir que en la propia investigación matemática y en el *hacer* matemático en general, despiertan cada vez mayor interés las cuestiones de tipo constructivista frente a aquellas de carácter existencialista. Pudiera parecer que es natural que así ocurra en el campo de la *matemática aplicada*, más interesada siempre en los aspectos *instrumentales* que en aquellas cuestiones que revisten un carácter más *esencial*; pero la naturaleza de este fenómeno va más allá que la de su mera presencia en el campo de la matemática aplicada, aunque una causa del mismo haya que buscarla precisamente en el creciente desarrollo de la misma, impulsada por una fuerte demanda social e institucional en lo que al aporte de fondos para la investigación se refiere. Sus métodos, basados en gran medida en el uso del ordenador como instrumento de cálculo, y, por consiguiente, de naturaleza fuertemente algorítmica, están ejerciendo una considerable influencia en el trabajo matemático actual. El interés por los aspectos algorítmicos también se está materializando en el desarrollo de nuevos campos de investigación con una mayor abstracción matemática, como son la Informática Teórica y la Inteligencia Artificial, cuyos métodos también están imbuidos de un fuerte carácter *procedimental*.

Este cambio de paradigma al que estamos asistiendo tiene su natural incidencia en las cuestiones relativas a la enseñanza de las matemáticas. Por ello, en cuanto a los aspectos metodológicos y didácticos se refiere, en los libros de texto y en las lecciones magistrales se está produciendo una progresiva desaparición de la exposición de carácter estructuralista, fuertemente influenciada por la escuela francesa, tan en boga desde la explosión de la filosofía del mismo nombre. Esto se traduce en el aumento progresivo del interés por los contenidos procedimentales del conocimiento matemático, o sea, por los contenidos relativos a habilidades, destrezas, estrategias y reconocimiento y formulación de algoritmos, en detrimento de los contenidos puramente conceptuales, que eran hasta hace muy poco el objetivo prioritario de los diseños curriculares de esta disciplina en los diferentes niveles de enseñanza. Ello no significa en modo

alguno que estemos asistiendo a la vuelta de las tesis constructivistas clásicas, según las cuales sólo existen aquellos objetos matemáticos que puedan ser contruidos con un argumento finitista que no use ningún proceso de reducción al absurdo. No es que se discuta la validez metodológica de los teoremas que hayan sido probados mediante algún tipo de argumento no constructivista, sino que se presta más atención a los argumentos de tipo algorítmico que a los de carácter existencial o dialéctico. Por otro lado, no sólo se resaltan los aspectos algorítmicos en la metodología de la enseñanza de las matemáticas, sino que el estudio del propio concepto de algoritmo es objeto de investigación matemática y, en consecuencia, de exposición didáctica. Temas como el Análisis de Algoritmos y las Funciones Recursivas son pues objeto de investigación a la vez que parte del contenido de los textos destinados a la enseñanza matemática.

Para poner de manifiesto la diferente naturaleza de los aspectos algorítmicos frente a los dialécticos vamos a dar un ejemplo que permita dilucidar esta cuestión. Consideremos la ecuación diofántica

$$ax + by + c = 0$$

en la que a y b son dos números enteros distintos de cero y c es un número entero cualquiera. Si a y b son primos entre sí, esto es, si a y b no tienen más divisores positivos comunes que la unidad, y (u, v) es una solución particular de la ecuación anterior con u y v enteros, entonces es fácil demostrar que cualquier solución (x, y) de la ecuación anterior —con x e y enteros— es de la forma

$$x = u - bk, \quad y = v + ak$$

para cada entero k . Para obtener *todas* las soluciones de la ecuación anterior basta pues encontrar una solución particular (u, v) . Pero, ¿existe realmente alguna solución en el caso de que c sea distinto de cero? Para responder a esta cuestión hay que demostrar que tal solución existe. Esto puede hacerse de dos modos, a saber: mediante un argumento puramente existencial que no proporcione ningún método para obtener la solución, o mediante un argumento constructivista que nos dé un método para obtener esta solución. Un argumento de tipo dialéctico o existencialista es el siguiente: Supongamos que $c = 1$; entonces la ecuación de partida se puede escribir como $a(-x) + b(-y) = 1$. Consideremos el menor entero positivo k de todos los números enteros de la forma $af + bg$, con f y g enteros. Sean m y n dos enteros tales que $k = am + bn$. Si k no dividiera al número a , entonces a sería de la forma $a = kq + r$, donde q y r son el cociente y el resto respectivamente, de la división euclídea de a por k y, por lo que acabamos de suponer, necesariamente $0 < r < k$. Así pues,

$$r = a - qk = a - q(am + bn) = a(1 - qm) + b(-qn)$$

Pero esto quiere decir que r es de la forma $af + bg$ (con $f = 1 - qm$ y $g = -qn$). Como r es positivo y es menor que k , esto es una contradicción. Por ello, k tiene que dividir al número a . Y puesto que un razonamiento análogo demostrará que k divide al número b , entonces k necesariamente ha de ser igual a 1, ya que a y b son primos entre sí. Esto prueba que $am + bn = 1$, y en consecuencia, que $x = -m$ e $y = -n$ es una solución de la ecuación considerada en el caso particular de que c sea igual a uno. En el caso general, $x = -mc$ e $y = -nc$ son una solución particular de la ecuación $ax + by + c = 0$. Así pues, el razonamiento precedente nos dice que el par $(-mc, -nc)$ es una solución particular de la ecuación diofántica considerada, pero todo lo que sabemos respecto a m y n es que existen y verifican que $am + bn = 1$, y no disponemos de ningún método efectivo de obtenerlos.

Desde un punto de vista algorítmico, puede demostrarse que una solución particular (x, y) de la ecuación $ax + by + c = 0$ es de la forma

$$x = (-1)^{n-1}cQ_{n-1}, \quad y = (-1)^n cP_{n-1}$$

donde si $q_1, q_2, \dots, q_n$ son los cocientes incompletos del desarrollo de la fracción irreducible a/b en fracción continua, es decir, si

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{\vdots}{q_{n-1} + \frac{1}{q_n}}}}$$

entonces $P_0 = 1, P_1 = q_1, Q_0 = 0, Q_1 = 1$ y

$$\begin{aligned} P_k &= q_k P_{k-1} + P_{k-2} \\ Q_k &= q_k Q_{k-1} + Q_{k-2} \end{aligned}$$

Por ejemplo, en la ecuación $105x + 38y + 4 = 0$, se tiene que

q_k		2	1	3	4	2
P_k	1	2	3	11	47	105
Q_k	0	1	1	4	17	38

con lo que $x = 4 \times 17 = 68$, $y = -4 \times 47 = -188$ es una solución particular, siendo $x = 68 - 38k$, $y = -188 + 105k$, con k entero, la solución general.

Hay también en la actualidad una acusada tendencia a *discretizar* las matemáticas. Esto quiere decir que se están potenciando los métodos en los que no se requiera ninguna operación de *paso al límite*, lo cual implica cierta preponderancia de los métodos algebraicos y combinatorios frente a los métodos topológicos clásicos del Análisis Funcional. En este contexto hay que situar la *Teoría de Grafos*, los métodos combinatorios lógicos, los nuevos métodos de análisis numérico como el de los *Elementos Finitos* —cuyo objeto es la resolución aproximada de problemas de contorno de ecuaciones en derivadas parciales— y el llamado *Análisis no Estándar*. Con relación a este último, y a título de ejemplo, señalemos que ha conseguido *discretizar* el proceso del *paso al límite* de una manera notable con la definición rigurosa de los *infinitésimos*: números positivos o negativos infinitamente *pequeños* que tienen propiedades análogas a las de los números reales. Con ayuda de estos *números* el cálculo diferencial se reduce al cálculo algebraico de cocientes entre infinitésimos. Se trata de una reformulación rigurosa desde el punto de vista lógico de los métodos infinitesimales de cálculo tan queridos por los físicos y los ingenieros que, aun a sabiendas de su falta de rigor formal, nunca los abandonaron, a pesar de que el Análisis Funcional moderno ya los había condenado al ostracismo. La esencia del Análisis no Estándar se basa en la construcción de un conjunto con estructura de cuerpo que contiene al cuerpo $\mathbb{R}$ de los reales y extiende adecuadamente las propiedades de éstos. Así, en el conjunto ω de todas las sucesiones de números reales se define una relación de equivalencia del modo siguiente: $(x_n) \mathfrak{R} (y_n)$ si el conjunto M de todos los índices k tales que $x_k = y_k$ tiene un complementario finito en el conjunto $\mathbb{N}$ de los números naturales. Se denota por $\mathbb{H}$ el conjunto cociente $\omega / \mathfrak{R}$. Los elementos del conjunto $\mathbb{H}$ se denominan números *hiperreales*.

Si denotamos por $[(x_n)]$ la clase de equivalencia asociada a la sucesión (x_n) , se define en $\mathbb{H}$ la siguiente relación de orden: $[(x_n)] \leq [(y_n)]$ si el conjunto de los índices k tales que $x_k \leq y_k$ tiene complementario finito en $\mathbb{N}$. Identificando $\mathbb{R}$ con el subconjunto de $\mathbb{H}$ formado por las sucesiones constantes $[(x)]$, este orden preserva el de $\mathbb{R}$, pues si $[(x)] \leq [(y)]$, entonces necesariamente $x \leq y$, y si $x \leq y$, claramente $[(x)] \leq [(y)]$. Los elementos de $\mathbb{H}$ que corresponden a los números reales clásicos se llaman números *estándar*. El conjunto $\mathbb{H}$ tiene estructura de cuerpo con las operaciones

$$\begin{aligned} [(x_n)] + [(y_n)] &:= [(x_n + y_n)] \\ [(x_n)] [(y_n)] &:= [(x_n y_n)] \end{aligned}$$

Se demuestra que esta relación de orden en $\mathbb{H}$ es un orden total, por lo que se puede definir el valor absoluto del modo usual, es decir, dado $x \in \mathbb{H}$, $|x| = x$ si $x > 0$ y $|x| = -x$ si $x < 0$, donde $-x$ denota el opuesto de x respecto a la ley aditiva. Un elemento $a \in \mathbb{H}$ se dice que es un número hiperreal *infinito* si $|a| > x$ para cada número positivo estándar x . Un elemento a de $\mathbb{H}$ se dice *finito* en el caso de que $|a| \leq x$ para algún $x > 0$ estándar, y un $a \in \mathbb{H}$ se dice *infinitesimal* si $|a| \leq x$ para cada número positivo estándar x . Claramente, $\varepsilon = [(1/n)]$ es un número hiperreal infinitesimal, mientras que $[(n)]$ es un elemento infinito de $\mathbb{H}$. Dos números hiperreales x e y se dicen infinitamente próximos si $x - y$ es un número hiperreal infinitesimal.

El mayor énfasis que se pone actualmente en los métodos algorítmicos y en los contenidos de carácter discreto proviene de factores diversos, entre los que cabe destacar la creciente influencia que el desarrollo de la industria informática está ejerciendo en nuestra sociedad, y como consecuencia de ello, en el hacer matemático. Esta influencia, como se ha dicho, es múltiple: por un lado, hay una tendencia a discretizar el cálculo diferencial clásico aprovechando el poder de cálculo de los ordenadores. Por otro lado, se han desarrollado campos nuevos de investigación relacionados con la informática, como la Teoría de Autómatas, la Teoría de Lenguajes, la Informática Teórica y la Inteligencia Artificial, que tienen muchos puntos de contacto con las matemáticas y que inciden todos ellos en los aspectos algorítmicos y en los contenidos de matemática discreta; no obstante es difícil establecer una frontera entre lo que es y lo que no es matemáticas. Además se ha creado una lógica alternativa, denominada *Lógica Borrosa*, que también tiene aplicaciones informáticas y que a su vez se está aplicando con éxito en la industria. También se están usando los ordenadores para la refutación de conjeturas, especialmente en la Teoría de Números. Un ejemplo es la refutación de la célebre conjetura de Euler, que afirmaba que ninguna n -ésima potencia natural de grado mayor que 2 podía ser una suma de menos de n potencias n -ésimas de números enteros. Para $n = 5$ esta conjetura es falsa, ya que, como pudo establecerse con ayuda del ordenador,

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Incluso se están usando ordenadores para pruebas intrincadas de tipo combinatorio, como para la demostración del no menos célebre teorema de los cuatro colores; para la denominada teoría de demostración automática en Inteligencia Artificial, etc.

Como reflejo de todo ello, y tal como ha sido dicho, la enseñanza de las matemáticas incide cada vez más en los aspectos algorítmicos y discretos de esta disciplina, en detrimento de los métodos dialécticos y analíticos de la misma. Este texto es una consecuencia de todo esto: en el mismo se recogen un buen

número de temas de lo que se ha dado en denominar *Matemática Discreta*, algunas de cuyas fuentes hay que buscarlas en el Álgebra Abstracta en relación con los contenidos conceptuales, aunque con un carácter menos dialéctico que ésta y por tanto con un mayor énfasis en los aspectos algorítmicos y procedimentales. Nuestra exposición incide con frecuencia en estos aspectos, sin renunciar a un nivel estructural y conceptual básico, sin olvidar los aspectos heurísticos y de aplicabilidad, pero sin eludir demostraciones de carácter dialéctico cuando las exigencias de rigor lo determinen.

Dado que no existe un currículo preciso en lo que respecta a los contenidos de esta disciplina, la selección de los temas tratados puede parecer un tanto arbitraria; no obstante, creemos que es apropiada para cualquier estudiante de los primeros cursos de ingeniería, y en especial para los estudiantes de Informática en general.

El texto recoge y amplía de hecho una parte del programa impartido por los autores en el curso académico 92-93 en la asignatura de Álgebra y la totalidad del programa correspondiente al primer cuatrimestre del curso 93-94 en la asignatura de Matemática Discreta en la Escuela de Informática de la Universidad Politécnica de Valencia. La obra presenta algunas novedades importantes respecto a los textos estándar de Matemática Discreta, tanto en lo relativo a los temas seleccionados como en su tratamiento, a la vez riguroso y ameno. Así, tras los Capítulos 1, 2 y 3, dedicados respectivamente al estudio de la lógica binaria, la teoría ingenua de conjuntos y las estructuras básicas, el Capítulo 4 se dedica íntegramente al estudio del álgebra de Boole. En el Capítulo 5, además de los métodos combinatorios clásicos, los grafos eulerianos y los grafos coloreados, se presenta una introducción a la teoría de las funciones recursivas, de gran importancia en Computación. En el Capítulo 6 se presenta una introducción rigurosa al estudio de las máquinas y autómatas finitos, de importancia en Informática Teórica y Computación. En el Capítulo 7 se desarrolla con cierta extensión la teoría de Ramsey, que puede considerarse una de las partes más interesantes de los métodos combinatorios lógicos. En el Capítulo 8 se introducen los conjuntos borrosos, la teoría de códigos lineales y las máquinas de Turing. Los dos primeros temas tienen importancia práctica en Informática Aplicada, y el tercero tiene interés en Informática Teórica. Por otro lado, el carácter teórico-práctico del texto lo hace muy útil desde el punto de vista didáctico y como texto de autoaprendizaje.

Para la redacción de este manual, autocontenido en la medida de lo posible, ha sido decisivo el contacto con los alumnos. Por ello, un buen número de observaciones advierten contra posibles equívocos o resaltan detalles que pudieran haber pasado inadvertidos en una primera lectura. Por otro lado, se ha procurado utilizar una terminología revestida de un lenguaje sencillo, a veces

enfocado como un diálogo con el lector, incluso en la minuciosa resolución de los ejercicios que se han propuesto al final de cada capítulo. La selección de los mismos ha sido realizada en función tanto de la aplicación de los contenidos conceptuales y procedimentales de cada capítulo, como de su carácter de completación de la parte teórica.

Agradecemos la colaboración de las profesoras de la Escuela de Informática de la U.P.V. Carmen Alegre, Pilar Bravo, Maite Gassó y Ana Martínez y a los alumnos que han contribuido a que este texto viera la luz. También queremos agradecer el amable prólogo del profesor Carlos Rentería y a la Editorial Reverté el interés y el gran esfuerzo que ha realizado en la cuidadosa edición de este texto.

Cuantos errores se observen son sólo imputables a los autores, que recogerán con satisfacción cualquier sugerencia tendente a la mejora de este manual, si procediera una revisión del mismo en el futuro.

Juan Carlos Ferrando
Valentín Gregori

“A mí, Parménides, me parece más razonable lo siguiente: que las *Ideas* permanecen en la naturaleza a modo de paradigmas, que las cosas están hechas a imagen de ellas y son sus copias, y que esta participación que las cosas llegan a tener en las *Ideas* no es sino un estar hechas a su imagen.”

Platón: Parménides. Primera parte.

“Un *razonamiento* es un discurso (*logos*) en el que, sentadas ciertas cosas, se da necesariamente a la vez, a través de lo establecido, algo distinto de lo establecido. Hay *demonstración* cuando el razonamiento parte de cosas verdaderas y primordiales, o de cosas cuyo conocimiento se origina a través de cosas primordiales y verdaderas; en cambio, es dialéctico el razonamiento construido a partir de cosas plausibles.”

Aristóteles: Organon. Tópicos, Libro I.

SÍMBOLOS Y NOTACIÓN

En la redacción de este texto no se ha querido abusar de notación matemática. No obstante, el deseo de facilitar su lectura nos aconseja indicar parte de la terminología empleada, que por otra parte es la usual.

$\mathbb{C}$	Complejos
$\mathbb{N}$	Naturales
$\mathbb{Q}$	Racionales
$\mathbb{R}$	Reales
$\mathbb{Z}$	Enteros
$\mathbb{Z}_n$	Enteros módulo n (también $\mathbb{Z}/n$ o $\mathbb{Z}/n\mathbb{Z}$)
$\wedge$	Conjunción lógica
$\vee$	Disyunción lógica
$\neg$	Negación lógica
$\rightarrow$	Condicional lógico
$\Rightarrow$	Implicación
$\leftrightarrow$	Doble condicional
$\Leftrightarrow$	Doble implicación
Δ	Disyunción exclusiva, diferencia simétrica
$\emptyset$	Contradicción, conjunto vacío
τ	Tautología
$\equiv$	Equivalencia, relación de congruencia
$\in$	Pertenencia
$\notin$	No pertenencia
$\subset$	Inclusión (también $\subseteq$)
$\not\subset$	No inclusión
$\cup$	Unión
$\cap$	Intersección
$\forall$	Cuantificador universal
$\exists$	Cuantificador existencial
$\sum$	Sumatorio
$\prod$	Productorio
$:$	Tal que (también $ $)
$ $	Valor absoluto, módulo
$\leq$	Relación de orden
A^c	Complementario del conjunto A
$P(E)$	Partes de E
$A - B$	Diferencia de conjuntos (también $A \setminus B$)
$\text{Cd}(A)$	Cardinal del conjunto A
f^n	Composición n -ésima (también f^n)

$f \circ g$	Composición de aplicaciones
sii	Si y sólo si
$\bar{a}$	Clase de equivalencia (también $[a]$)
a'	Complementario del elemento a (capítulo 4)
$\bar{f}$	Función complementaria (también f')
$x \mid y$	x divide a y
$a \mathfrak{R} b$	a está relacionado con b
$a \nmathfrak{R} b$	a no está relacionado con b
$\models$	Deducción semántica
$\vdash$	Deducción lógica
fbf	Fórmula bien formada

ÍNDICE ANALÍTICO

PRÓLOGO DEL PROFESOR CARLOS RENTERÍA	VII
PREFACIO A LA SEGUNDA EDICIÓN	IX
PREFACIO A LA PRIMERA EDICIÓN	XI
SÍMBOLOS Y NOTACIÓN	XXI
CAPÍTULO 1 INTRODUCCIÓN A LA LÓGICA	1
1.1 Cálculo proposicional	1
1.2 Inferencia lógica	8
1.3 Funciones proposicionales y cuantificadores	15
Ejercicios resueltos	18
CAPÍTULO 2 TEORÍA DE CONJUNTOS	33
2.1 Conjuntos	33
2.2 Correspondencias y relaciones	39
2.3 Relación binaria de equivalencia	43
2.4 Relación binaria de orden	45
2.5 Aplicaciones	48
2.6 Cardinalidad	54
2.7 Notas y comentarios generales	59
Ejercicios resueltos	62
CAPÍTULO 3 LEYES DE COMPOSICIÓN INTERNA: GRUPOS, ANILLOS Y CUERPOS	79
3.1 Grupos	79
3.2 Compatibilidad con una relación	87
3.3 Subgrupos	90
3.4 Teorema de Lagrange. Grupo cociente	91
3.5 Grupos monógenos y cíclicos	94
3.6 Teoremas de Euler y Fermat	97

3.7 Homomorfismo de grupos	99
3.8 Anillos	103
3.9 Cuerpos	108
Ejercicios resueltos.	112
CAPÍTULO 4 ÁLGEBRAS DE BOOLE	129
4.1 Álgebras de Boole	129
4.2 Retículos de Boole	133
4.3 Funciones booleanas	135
4.4 Simplificación de funciones booleanas	145
Ejercicios resueltos.	153
CAPÍTULO 5 MÉTODOS COMBINATORIOS, RECURSIVIDAD Y GRAFOS	163
5.1 Combinaciones	164
5.2 Variaciones y permutaciones	172
5.3 Variaciones y permutaciones con repetición	174
5.4 Particiones de un conjunto finito. Particiones ordenadas	176
5.5 Funciones recursivas	178
5.6 Grafos eulerianos.	184
5.7 Grafos coloreados	189
5.8 Notas y comentarios	194
Ejercicios resueltos.	197
CAPÍTULO 6 MÁQUINAS Y AUTÓMATAS FINITOS.	207
6.1 Lenguajes formales	207
6.2 Máquinas secuenciales finitas	208
6.3 Extensión a palabras de la entrada y la salida.	209
6.4 Estados equivalentes	212
6.5 Minimización de máquinas secuenciales	214
6.6 Autómatas finitos	217
6.7 Acción de una máquina secuencial	219
6.8 Teorema de existencia	221
6.9 Notas y comentarios	224
Ejercicios resueltos.	226
CAPÍTULO 7 TEORÍA DE RAMSEY	233
7.1 Conjuntos de conocidos y extraños en una reunión	233
7.2 Números de Ramsey	235
7.3 El teorema de Ramsey en el caso infinito	239

7.4 Teoremas de Ramsey de tipo euclídeo	243
7.5 El teorema de Van der Waerden	246
7.6 Nota final	251
Ejercicios resueltos	252
CAPÍTULO 8 CONJUNTOS BORROSOS, CÓDIGOS LINEALES Y	
MÁQUINAS DE TURING	257
8.1 Conjuntos borrosos	257
8.2 Códigos lineales	263
8.3 Máquinas de Turing	267
Ejercicios resueltos	271
APÉNDICE. LÓGICA DE PREDICADOS Y SISTEMAS FORMALES	277
A.1 Introducción	272
A.2 Funciones proposicionales y predicados	279
A.3 Fórmulas bien formadas	280
A.4 Reglas de inferencia	281
A.5 Sistemas formales	283
A.6 Una nota sobre el teorema de incompletitud de Gödel	286
BIBLIOGRAFÍA	289
ÍNDICE ALFABÉTICO	293

INTRODUCCIÓN A LA LÓGICA

El propósito de este capítulo es introducir el método deductivo de la matemática actual. Para ello expondremos de una manera sencilla la teoría proposicional de la inferencia. Cabe mencionar aquí que, desde el punto de vista de la lógica digital, el soporte tecnológico principal de los ordenadores está constituido por los denominados *circuitos de conmutación*, también llamados *circuitos lógicos* por el hecho de que las formas elementales de la lógica y los circuitos de conmutación tienen un modelo matemático común: el *álgebra de Boole binaria*.

1.1 CÁLCULO PROPOSICIONAL

1.1.1 PROPOSICIÓN

Llamaremos **proposición** a toda afirmación de la que se pueda decir sin ambigüedad y de manera excluyente que es cierta o falsa. Cuando es cierta se le atribuye el valor lógico **1** ó **V** (Verdadera) y si es falsa **0** ó **F** (Falsa). Las proposiciones más sencillas posibles se denominan **atómicas** y se acostumbra a representarlas por letras minúsculas. Las proposiciones constituidas por proposiciones atómicas y otras partículas que sirven de nexo se llaman **moleculares** y se las suele nombrar con letras mayúsculas. El **cálculo proposicional** se ocupa de la formación de proposiciones moleculares y de su valor lógico, atendiendo a la estructura y a los componentes de la proposición.

Ejemplo 1.1 Sea p la proposición *El hierro es un metal* y sea q la proposición $2 + 2 = 5$. Claramente, el valor lógico de p es 1 (V), mientras que el valor lógico de q es 0 (F).

1.1.2 CONECTORES LÓGICOS

Se llaman **conectores** (o **conectivos**) **lógicos** a las partículas que se utilizan para formar las proposiciones moleculares. Distinguimos los siguientes:

- La **disyunción** «o» (inclusiva), que simbolizaremos por $\vee$, y que se define de manera que la proposición $p \vee q$ (se lee: p o q) es falsa sólo en el caso de que p y q sean falsas simultáneamente.
- La **conjunción** «y», que simbolizaremos por $\wedge$, y que se define de manera que la proposición $p \wedge q$ (se lee: p y q) es cierta sólo cuando p y q son ciertas a la vez.
- La **negación** «no», que simbolizaremos por $\neg$, y que se define de manera que la proposición $\neg p$ (se lee: no p) es cierta sólo cuando p es falsa.
- El **condicional** «si ..., entonces ...», que simbolizaremos por $\rightarrow$, y que se define de manera que la proposición $p \rightarrow q$ (se lee: si p , entonces q) es falsa sólo cuando p es cierta y q es falsa. Se dice que p es el **antecedente**, y q el **consecuente** del condicional.
- El **doble condicional** «... si, y sólo si ...» que simbolizaremos por $\leftrightarrow$, se define de modo que la proposición $p \leftrightarrow q$ (se lee: p si, y sólo si q) es cierta sólo cuando p y q son a la vez ciertas, o son a la vez falsas.

Las definiciones anteriores se esquematizan mediante las siguientes tablas, llamadas **tablas de verdad**:

p	q	$p \vee q$	$p \wedge q$	$\neg p$	$p \rightarrow q$	$p \leftrightarrow q$
1	1	1	1	0	1	1
1	0	1	0	0	0	0
0	1	1	0	1	1	0
0	0	0	0	1	1	1

En el ejemplo 1.1 $p \vee q$ es verdadero (V ó 1), $p \wedge q$ es falso (F ó 0), $\neg p$ es falso (F ó 0), $\neg q$ es verdadero (V ó 1), $p \rightarrow q$ es falso (F ó 0), $q \rightarrow p$ es verdadero (V ó 1) y $p \leftrightarrow q$ es falso (F ó 0).