

Undergraduate Texts in Mathematics

Editors

S. Axler

F.W. Gehring

K.A. Ribet

Undergraduate Texts in Mathematics

- Abbott:** Understanding Analysis.
- Anglin:** Mathematics: A Concise History and Philosophy.
Readings in Mathematics.
- Anglin/Lambek:** The Heritage of Thales.
Readings in Mathematics.
- Apostol:** Introduction to Analytic Number Theory. Second edition.
- Armstrong:** Basic Topology.
- Armstrong:** Groups and Symmetry.
- Axler:** Linear Algebra Done Right. Second edition.
- Beardon:** Limits: A New Approach to Real Analysis.
- Bak/Newman:** Complex Analysis. Second edition.
- Banchoff/Wermer:** Linear Algebra Through Geometry. Second edition.
- Berberian:** A First Course in Real Analysis.
- Bix:** Conics and Cubics: A Concrete Introduction to Algebraic Curves.
- Brémaud:** An Introduction to Probabilistic Modeling.
- Bressoud:** Factorization and Primality Testing.
- Bressoud:** Second Year Calculus.
Readings in Mathematics.
- Brickman:** Mathematical Introduction to Linear Programming and Game Theory.
- Browder:** Mathematical Analysis: An Introduction.
- Buchmann:** Introduction to Cryptography.
- Buskes/van Rooij:** Topological Spaces: From Distance to Neighborhood.
- Callahan:** The Geometry of Spacetime: An Introduction to Special and General Relativity.
- Carter/van Brunt:** The Lebesgue–Stieltjes Integral: A Practical Introduction.
- Cederberg:** A Course in Modern Geometries. Second edition.
- Childs:** A Concrete Introduction to Higher Algebra. Second edition.
- Chung:** Elementary Probability Theory with Stochastic Processes. Third edition.
- Cox/Little/O'Shea:** Ideals, Varieties, and Algorithms. Second edition.
- Croom:** Basic Concepts of Algebraic Topology.
- Curtis:** Linear Algebra: An Introductory Approach. Fourth edition.
- Devlin:** The Joy of Sets: Fundamentals of Contemporary Set Theory. Second edition.
- Dixmier:** General Topology.
- Driver:** Why Math?
- Ebbinghaus/Flum/Thomas:** Mathematical Logic. Second edition.
- Edgar:** Measure, Topology, and Fractal Geometry.
- Elaydi:** An Introduction to Difference Equations. Second edition.
- Erdős/Surányi:** Topics in the Theory of Numbers.
- Estep:** Practical Analysis in One Variable.
- Exner:** An Accompaniment to Higher Mathematics.
- Exner:** Inside Calculus.
- Fine/Rosenberger:** The Fundamental Theory of Algebra.
- Fischer:** Intermediate Real Analysis.
- Flanigan/Kazdan:** Calculus Two: Linear and Nonlinear Functions. Second edition.
- Fleming:** Functions of Several Variables. Second edition.
- Foulds:** Combinatorial Optimization for Undergraduates.
- Foulds:** Optimization Techniques: An Introduction.
- Franklin:** Methods of Mathematical Economics.
- Frazier:** An Introduction to Wavelets Through Linear Algebra.

(continued after index)

L. Lovász
J. Pelikán
K. Vesztergombi

Discrete Mathematics

Elementary and Beyond

With 95 Illustrations

 Springer

L. Lovász
Microsoft Corporation
Microsoft Research
One Microsoft Way
Redmond, WA 98052-6399
USA
lovasz@microsoft.com

J. Pelikán
Department of Algebra
and Number Theory
Eötvös Loránd University
Pázmány Péter Sétány 1/C
Budapest H-1117
Hungary
pelikan@cs.eltc.hu

K. Vesztergombi
Department of Mathematics
University of Washington
Box 354-350
Seattle, WA 98195-4350
USA
veszter@math.washington.edu

Editorial Board

S. Axler
Mathematics Department
San Francisco State
University
San Francisco, CA 94132
USA
axler@sfsu.edu

F. W. Gehring
Mathematics Department
East Hall
University of Michigan
Ann Arbor, MI 48109
USA
fgehring@math.lsa.umich.edu

K. A. Ribet
Mathematics Department
University of California,
Berkeley
Berkeley, CA 94720-3840
USA
ribet@math.berkeley.edu

Mathematics Subject Classification (2000): 28-01, 30-01

Library of Congress Cataloging-in-Publication Data

Lovász, László, 1948–

Discrete mathematics / László Lovász, József Pelikán, Katalin L. Vesztergombi.
p. cm. — (Undergraduate texts in mathematics)
Includes bibliographical references and index.

ISBN 978-0-387-95585-8 ISBN 978-0-387-21777-2 (eBook)

DOI 10.1007/978-0-387-21777-2

1. Mathematics. 2. Computer science—Mathematics. I. Pelikán, József.
II. Vesztergombi, Katalin L. III. Title. III. Series.

QA39.3.L68 2003

510–dc21

2002030585

Printed on acid-free paper.

© 2003 Springer Science+Business Media, LLC

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

9 8 7 6

springer.com

Preface

For most students, the first and often only course in college mathematics is calculus. It is true that calculus is the single most important field of mathematics, whose emergence in the seventeenth century signaled the birth of modern mathematics and was the key to the successful applications of mathematics in the sciences and engineering.

But calculus (or analysis) is also very technical. It takes a lot of work even to introduce its fundamental notions like continuity and the derivative (after all, it took two centuries just to develop the proper definition of these notions). To get a feeling for the power of its methods, say by describing one of its important applications in detail, takes years of study.

If you want to become a mathematician, computer scientist, or engineer, this investment is necessary. But if your goal is to develop a feeling for what mathematics is all about, where mathematical methods can be helpful, and what kinds of questions do mathematicians work on, you may want to look for the answer in some other fields of mathematics.

There are many success stories of applied mathematics outside calculus. A recent hot topic is mathematical cryptography, which is based on number theory (the study of the positive integers $1, 2, 3, \dots$), and is widely applied, for example, in computer security and electronic banking. Other important areas in applied mathematics are linear programming, coding theory, and the theory of computing. The mathematical content in these applications is collectively called *discrete mathematics*. (The word “discrete” is used in the sense of “separated from each other,” the opposite of “continuous;” it is also often used in the more restrictive sense of “finite.” The more everyday version of this word, meaning “circumspect,” is spelled “discreet.”)

The aim of this book is not to cover “discrete mathematics” in depth (it should be clear from the description above that such a task would be ill-defined and impossible anyway). Rather, we discuss a number of selected results and methods, mostly from the areas of combinatorics and graph theory, with a little elementary number theory, probability, and combinatorial geometry.

It is important to realize that there is no mathematics without *proofs*. Merely stating the facts, without saying something about why these facts are valid, would be terribly far from the spirit of mathematics and would make it impossible to give any idea about how it works. Thus, wherever possible, we will give the proofs of the theorems we state. Sometimes this is not possible; quite simple, elementary facts can be extremely difficult to prove, and some such proofs may take advanced courses to go through. In these cases, we will at least state that the proof is highly technical and goes beyond the scope of this book.

Another important ingredient of mathematics is *problem solving*. You won't be able to learn any mathematics without dirtying your hands and trying out the ideas you learn about in the solution of problems. To some, this may sound frightening, but in fact, most people pursue this type of activity almost every day: Everybody who plays a game of chess or solves a puzzle is solving discrete mathematical problems. The reader is strongly advised to answer the questions posed in the text and to go through the problems at the end of each chapter of this book. Treat it as puzzle solving, and if you find that some idea that you came up with in the solution plays some role later, be satisfied that you are beginning to get the essence of how mathematics develops.

We hope that we can illustrate that mathematics is a building, where results are built on earlier results, often going back to the great Greek mathematicians; that mathematics is alive, with more new ideas and more pressing unsolved problems than ever; and that mathematics is also an art, where the beauty of ideas and methods is as important as their difficulty or applicability.

László Lovász

József Pelikán

Katalin Vesztergombi

Contents

Preface	v
1 Let's Count!	1
1.1 A Party	1
1.2 Sets and the Like	4
1.3 The Number of Subsets	9
1.4 The Approximate Number of Subsets	14
1.5 Sequences	15
1.6 Permutations	17
1.7 The Number of Ordered Subsets	19
1.8 The Number of Subsets of a Given Size	20
2 Combinatorial Tools	25
2.1 Induction	25
2.2 Comparing and Estimating Numbers	30
2.3 Inclusion-Exclusion	32
2.4 Pigeonholes	34
2.5 The Twin Paradox and the Good Old Logarithm	37
3 Binomial Coefficients and Pascal's Triangle	43
3.1 The Binomial Theorem	43
3.2 Distributing Presents	45
3.3 Anagrams	46
3.4 Distributing Money	48

3.5	Pascal's Triangle	49
3.6	Identities in Pascal's Triangle	50
3.7	A Bird's-Eye View of Pascal's Triangle	54
3.8	An Eagle's-Eye View: Fine Details	57
4	Fibonacci Numbers	65
4.1	Fibonacci's Exercise	65
4.2	Lots of Identities	68
4.3	A Formula for the Fibonacci Numbers	71
5	Combinatorial Probability	77
5.1	Events and Probabilities	77
5.2	Independent Repetition of an Experiment	79
5.3	The Law of Large Numbers	80
5.4	The Law of Small Numbers and the Law of Very Large Numbers	83
6	Integers, Divisors, and Primes	87
6.1	Divisibility of Integers	87
6.2	Primes and Their History	88
6.3	Factorization into Primes	90
6.4	On the Set of Primes	93
6.5	Fermat's "Little" Theorem	97
6.6	The Euclidean Algorithm	99
6.7	Congruences	105
6.8	Strange Numbers	107
6.9	Number Theory and Combinatorics	114
6.10	How to Test Whether a Number is a Prime?	117
7	Graphs	125
7.1	Even and Odd Degrees	125
7.2	Paths, Cycles, and Connectivity	130
7.3	Eulerian Walks and Hamiltonian Cycles	135
8	Trees	141
8.1	How to Define Trees	141
8.2	How to Grow Trees	143
8.3	How to Count Trees?	146
8.4	How to Store Trees	148
8.5	The Number of Unlabeled Trees	153
9	Finding the Optimum	157
9.1	Finding the Best Tree	157
9.2	The Traveling Salesman Problem	161
10	Matchings in Graphs	165

10.1 A Dancing Problem	165
10.2 Another matching problem	167
10.3 The Main Theorem	169
10.4 How to Find a Perfect Matching	171
11 Combinatorics in Geometry	179
11.1 Intersections of Diagonals	179
11.2 Counting regions	181
11.3 Convex Polygons	184
12 Euler’s Formula	189
12.1 A Planet Under Attack	189
12.2 Planar Graphs	192
12.3 Euler’s Formula for Polyhedra	194
13 Coloring Maps and Graphs	197
13.1 Coloring Regions with Two Colors	197
13.2 Coloring Graphs with Two Colors	199
13.3 Coloring graphs with many colors	202
13.4 Map Coloring and the Four Color Theorem	204
14 Finite Geometries, Codes, Latin Squares, and Other Pretty Creatures	211
14.1 Small Exotic Worlds	211
14.2 Finite Affine and Projective Planes	217
14.3 Block Designs	220
14.4 Steiner Systems	224
14.5 Latin Squares	229
14.6 Codes	232
15 A Glimpse of Complexity and Cryptography	239
15.1 A Connecticut Class in King Arthur’s Court	239
15.2 Classical Cryptography	242
15.3 How to Save the Last Move in Chess	244
15.4 How to Verify a Password—Without Learning it	246
15.5 How to Find These Primes	246
15.6 Public Key Cryptography	247
16 Answers to Exercises	251
Index	287