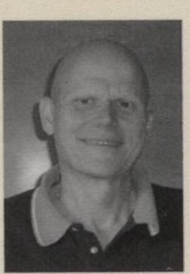
The idea behind this book is to provide the mathematical foundations for assessing modern developments in the Information Age. It deepens and complements the basic concepts, but it also considers instructive and more advanced topics. The treatise starts with a general chapter on algebraic structures; this part provides all the necessary knowledge for the rest of the book. The next chapter gives a concise overview of cryptography. Chapter 3 on number theoretic algorithms is important for developing cryptosystems, Chapter 4 presents the deterministic primality test of Agrawal, Kayal, and Saxena. The account to elliptic curves again focuses on cryptographic applications and algorithms. With combinatorics on words and automata theory, the reader is introduced to two areas of theoretical computer science where semigroups play a fundamental role. The last chapter is devoted to combinatorial group theory and its connections to automata.

- Contains brief chapter summaries as well as examples, problems and solutions.
- References for further reading in every chapter.
- Many illustrations of mathematical derivations.



Volker Diekert
studied in Hamburg and Montpellier. He earned his PhD in algebraic number theory in Regensburg and received the Habilitation in Munich. Since 1991 he holds the chair for Theoretical Informatics at the University of Stuttgart.

Manfred Kufleitner
teaches at the University of Stuttgart where he earned his PhD in computer science under the supervision of Volker Diekert. He has been a guest professor at TU Munich and an acting professor at the University of Hamburg.

Gerhard Rosenberger
did his doctorate in analytic number theory and habilitated in combinatorial group theory. Worldwide he worked for longer terms at nine universities. At present he teaches at the University of Hamburg.

Ulrich Hertrampf
studied Mathematics in Heidelberg, earned his PhD in Augsburg and his Habilitation at the University of Würzburg. Today he works as a Professor in the department for Theoretical Informatics at the University of Stuttgart.

9 783110 413328

www.degruyter.com
ISBN 978-3-11-041332-8

Contents