Preface

To many students, as well as to many teachers, mathematics may seem like a mundane discipline, filled with rules and algorithms and devoid of beauty, culture and art. However, the world of mathematics is populated with true gems and results that astound. In our series Highlights in Mathematics we introduce and examine many of these mathematical highlights, thoroughly developing whatever mathematical results and techniques we need along the way.

We regard our Highlights as a book for graduate studies as well as for general mathematically interested, and planned it to be used in courses for teachers, so it is somewhat between a textbook and a collection of results. We assume that the reader is familiar with basic knowledge in algebra, geometry and calculus, as well as some knowledge of matrices and linear equations. Beyond these the book is self-contained. The chapters of the book are largely independent, and we invite the reader to choose areas to concentrate on.

We structure our book in 14 chapters.

In the first five chapters we look at highlights of the integers. We examine unique factorization and modular arithmetic and related ideas. We show to what extent these are critical components of modern cryptography especially public key cryptographic methods such as RSA. The first three authors worked partly as cryptographers, so cryptography is mentioned and explained in several places. In this second edition, we present in Chapter 2 a brand new and simple proof of the Fundamental Theorem of Arithmetic that is well suited for school settings.

In Chapters 4 and 5 we look at exceptional classes of integers such as the Fibonacci numbers as well as the Fermat numbers, Mersenne numbers, perfect numbers and Pythagorean triples. We explain the golden section and how to express integers as sums of squares. In this edition, we include some additional results on perfect and triangular numbers as well as the unique representation of each natural number as a sum of pairwise different Fibonacci numbers. We also mention the new results about Mersenne prime numbers.

In Chapters 6 to 8 we look at results involving polynomials and polynomial equations. We explain field extensions at an understandable level and then prove the insolvability of the quintic and beyond. The insolvability of the quintic in general is one of the important results of modern mathematics.

In Chapter 8 we consider in detail the permutation groups. For this we only use some definitions and very elementary facts about groups. In the second edition, we added Section 8.4 on general group theory where we describe and prove the fundamentals of group theory, as there are, for instance, the theorem of Lagrange, the isomorphism theorem, the class equation, the theorems of Sylow and the classification of finitely generated Abelian groups.

In Chapters 9 to 12 we look at highlights from the real and complex numbers leading eventually to an explanation and proof of the Fundamental Theorem of Algebra. Along

https://doi.org/10.1515/9783110790283-201

the way we consider the amazing properties of the numbers e and π and prove in detail that these two numbers are transcendent.

The main subject of Chapter 9 is the Cauchy completion of the rational numbers with Ostrowski's classification theorem at the end. It was suggested by the readers of the first edition to add some material on p-adic integers and their importance in number theory, and we devoted five new subsections in Section 9.7 to this topic. In Chapter 10 we show that in general a polynomial equation $f(x) = 0$ is not solvable by radicals, where $f(x)$ is a polynomial over a field with degree 5. In this context, we have written a new Section 10.5 on Galois theory to completely give the classification of the solvability of a polynomial equation $f(x) = 0$ using the theory of solvable groups considered in the new Section 8.4.

Chapter 13 is concerned with the classical problem of geometric constructions and uses the material we developed on field extensions to prove the impossibility of certain constructions. Finally, in Chapter 14 we look at Euclidean Vector Spaces. We give several geometric applications and look, for instance, at a secret sharing protocol using the closest vector theorem.

We would like to thank the many people who were involved in the preparation of the manuscript as well as those who have used the first edition in classes and seminars for their helpful suggestions. In particular, we have to mention Anja Rosenberger for her dedicated participation in translating and proofreading. Those mathematical, stylistic, and orthographic errors that undoubtedly remain shall be charged to the authors. Last but not least, we thank De Gruyter for publishing our book. We hope that our readers, old and new, will find pleasure in this reviewed and extended edition.

Sadly, our coauthor and longtime friend Benjamin Fine died during the preparation of this book. The remaining authors dedicate the book to the memory of Ben and to all the work that he inspired.

Anja Moldenhauer
Gerhard Rosenberger
Annika Schürenberg
Leonard Wienke