DE GRUYTER

TEXTBOOK

Benjamin Fine, Anthony Gaglione, Anja Moldenhauer, Gerhard Rosenberger, Dennis Spellman

ALGEBRA AND NUMBER THEORY

A SELECTION OF HIGHLIGHTS

This two-volume set collects and presents some fundamentals of mathematics in an entertaining and performing manner. The present volume examines many of the most important basic results in algebra and number theory, along with their proofs, and also their history.

- **An exciting collection of fundamental results in algebra and number theory.**
- **Covers number systems, polynomials, and algebra.**
- **Aimed at lecturers, teachers, and students of mathematics, and at all mathematically interested.**
- **Contains many exercises related to the content of each chapter.**

Benjamin Fine

is Professor of Mathematics and Statistics at Fairfield University. He received his Ph.D. form Courant Institute, New York University in 1973. He has had visiting positions at Yale University, University of California, NYU and University of Dortmund.

Anthony Gaglione

is a retired professor of the United States Naval Academy at Annapolis. He has made important and varied contributions to several areas of Infinite Group Theory and Combinatorial Group Theory.

Anja Moldenhauer

studied at the University of Hamburg and graduated 2016 with a doctoral degree. She was involved in various mathematics lectures for different majors at the University of Hamburg and taught at Florida Atlantic University. Her research focus lies on Mathematical Cryptology.

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.

Dennis Spellman

is a professor of the Temple University at Philadelphia. He was involved in the development and advances centered on the Elementary Theory of Groups and the Algebraic Geometry over Groups.

9 783110 515848

www.degruyter.com
ISBN 978-3-11-051584-8

Benjamin Fine, Anthony Gaglione, Anja Moldenhauer, Gerhard Rosenberger, Dennis Spellman

ALGEBRA AND NUMBER THEORY

Benjamin Fine, Anthony Gaglione,
Anja Moldenhauer, Gerhard Rosenberger,
Dennis Spellman

Algebra and Number Theory

A Selection of Highlights

DE GRUYTER

Mathematics Subject Classification 2010
0001, 00A06, 1101, 1201

Authors

Prof. Dr. Benjamin Fine
Fairfield University
Department of Mathematics
1073 North Benson Road
Fairfield, CT 06430
USA

Prof. Dr. Anthony Gaglione
United States Naval Academy
Department of Mathematics
212 Blake Road
Annapolis, MD 21401
USA

Dr. Anja Moldenhauer
University of Hamburg
Department of Mathematics
Bundesstr. 55
20146 Hamburg
Germany

Prof. Dr. Gerhard Rosenberger
University of Hamburg
Department of Mathematics
Bundesstr. 55
20146 Hamburg
Germany

Prof. Dr. Dennis Spellman
Temple University
Department of Mathematics
1801 N Broad Street
Philadelphia, PA 19122
USA

ISBN 978-3-11-051584-8
e-ISBN (PDF) 978-3-11-051614-2
e-ISBN (EPUB) 978-3-11-051626-5

Library of Congress Cataloging-in-Publication Data
A CIP catalog record for this book has been applied for at the Library of Congress.

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

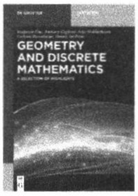
Typesetting: VTeX UAB, Lithuania
Printing and binding: CPI books GmbH, Leck
Cover image: agsandrew / iStock / Getty Images Plus
♾ Printed on acid-free paper
Printed in Germany

MIX
Papier aus verantwortungsvollen Quellen
FSC® C083411

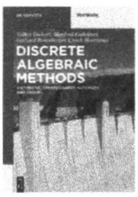
www.degruyter.com

Benjamin Fine, Anthony Gaglione, Anja Moldenhauer, Gerhard Rosenberger, Dennis Spellman
Algebra and Number Theory
De Gruyter Textbook

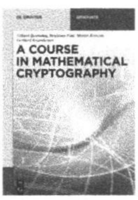
Also of Interest



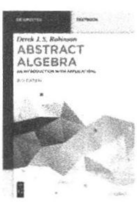
Geometry and Discrete Mathematics. A Selection of Highlights
Benjamin Fine, Anthony Gaglione, Anja Moldenhauer,
Gerhard Rosenberger, Dennis Spellman, 2018
ISBN 978-3-11-052145-0, e-ISBN (PDF) 978-3-11-052150-4,
e-ISBN (EPUB) 978-3-11-052153-5



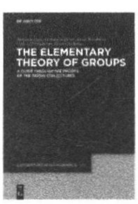
Discrete Algebraic Methods.
Arithmetic, Cryptography, Automata and Groups
Volker Diekert, Manfred Kufleitner, Gerhard Rosenberger,
Ulrich Hertrampf, 2016
ISBN 978-3-11-041332-8, e-ISBN (PDF) 978-3-11-041333-5,
e-ISBN (EPUB) 978-3-11-041632-9



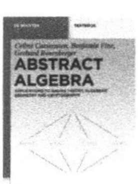
A Course in Mathematical Cryptography
Gilbert Baumslag, Benjamin Fine, Martin Kreuzer,
Gerhard Rosenberger, 2015
ISBN 978-3-11-037276-2, e-ISBN (PDF) 978-3-11-037277-9,
e-ISBN (EPUB) 978-3-11-038616-5



Abstract Algebra.
An Introduction with Applications
Derek J. S. Robinson, 2015
ISBN 978-3-11-034086-0, e-ISBN (PDF) 978-3-11-034087-7,
e-ISBN (EPUB) 978-3-11-038560-1



The Elementary Theory of Groups.
A Guide through the Proofs of the Tarski Conjectures
Benjamin Fine, Anthony Gaglione, Alexei Myasnikov,
Gerhard Rosenberger, Dennis Spellman, 2014
ISBN 978-3-11-034199-7, e-ISBN (PDF) 978-3-11-034203-1,
e-ISBN (EPUB) 978-3-11-038257-0



Abstract Algebra.
Applications to Galois Theory, Algebraic Geometry and Cryptography
Celine Carstensen, Benjamin Fine, Gerhard Rosenberger, 2011
ISBN 978-3-11-025008-4, e-ISBN (PDF) 978-3-11-025009-1

Preface

To many students, as well as to many teachers, mathematics seems like a mundane discipline, filled with rules and algorithms and devoid of beauty and art. However to someone who truly digs deeply into mathematics this is quite far from the truth. The world of mathematics is populated with true gems; results that both astound and point to a unity in both the world and a seemingly chaotic subject. It is often that these gems and their surprising results are used to point to the existence of a force governing the universe; that is, they point to a higher power. Euler's magic formula, $e^{i\pi}+1=0$, which we go over and prove in this book is often cited as a proof of the existence of God. While to someone seeing this statement for the first time it might seem outlandish, however if one delves into how this result is generated naturally from such a disparate collection of numbers it does not seem so strange to attribute to it a certain mystical significance.

Unfortunately most students of mathematics only see bits and pieces of this amazing discipline. In this book, which we call Algebra and Number Theory, we introduce and examine many of these exciting results. We planned this book to be used in courses for teachers and for the general mathematically interested so it is somewhat between a textbook and just a collection of results. We examine these mathematical gems and also their proofs, developing whatever mathematical results and techniques we need along the way. In Germany and the United States we see the book as a Masters Level Book for prospective teachers.

With the increasing demand for education in the STEM subjects, there is the realization that to get better teaching in mathematics, the prospective teachers must both be more knowledgeable in mathematics and excited about the subject. The courses in teacher preparation do not touch many of these results that make the discipline so exciting. This book is intended to address this issue. The first volume is on Algebra and Number Theory. We touch on numbers and number systems, polynomials and polynomial equations, geometry and geometric constructions. These parts are somewhat independent so a professor can pick and choose the areas to concentrate on. Much more material is included than can be covered in a single course. We prove all relevant results that are not too technical or complicated to scare the students. We find that mathematics is also tied to its history so we include many historical comments.

We try to introduce all that is necessary however we do presuppose certain subjects from school and undergraduate mathematics. These include basic knowledge in algebra, geometry and calculus as well as some knowledge of matrices and linear equations. Beyond these the book is self-contained.

This first volume of two is called Algebra and Number Theory. There are fourteen chapters and we think we have introduced a very wide collection of results of the type that we have alluded to above. In Chapters 1–5 we look at highlights on the integers. We examine unique factorization and modular arithmetic and related ideas. We show how these become critical components of modern cryptography especially public key cryp-

DOI 10.1515/9783110516142-201

tographic methods such as RSA. Three of the authors (Fine, Moldenhauer and Rosenberger) work partly as cryptographers so cryptography is mentioned and explained in several places. 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 as well as expressing integers as sums of squares. In Chapters 6–8 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 Chapters 9–12 we look at highlights from the real and complex numbers leading eventually to an explanation and proof of the Fundamental Theorem of Algebra. Along the way we consider the amazing properties of the numbers e and π and prove in detail that these two numbers are transcendent.

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 people who were involved in the preparation of the manuscript. Their dedicated participation in translating and proofreading are gratefully acknowledged. In particular, we have to mention Anja Rosenberger, Annika Schürenberg and the many students who have taken the respective courses in Dortmund, Fairfield and Hamburg. 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.

Benjamin Fine
Anthony Gaglione
Anja Moldenhauer
Gerhard Rosenberger
Dennis Spellman

Contents

1 The natural, integral and rational numbers

1.1 Number theory and axiomatic systems

Number theory begins as the study of the whole numbers or counting numbers. Formally the counting numbers $1, 2, \ldots$ are called the *natural numbers* and denoted by $\mathbb{N}$. If we add to this the number zero, denoted by 0, and the negative whole numbers we get a more comprehensive system called the *integers* which we denote by $\mathbb{Z}$. The focus of this book is on important and sometimes surprising results in number theory and then further results in algebra. Many results in number theory, as we shall see, seem like magic. In order to rigorously prove these results we place the whole theory in an axiomatic setting which we now explain.

In mathematics, when developing a concept or a theory it is often not possible, all used terms, properties or claims to prove, especially existence of some mathematical fundamentals. One can solve this problem then by an axiomatic approach. The basis of a theory then is a system of axioms:

- Certain objects and certain properties of these objects are taken as given and accepted.
- A selection of statements (the *axioms*) are considered by definition as true and evident.

A *theorem* in the theory then is a true statement, whose truth can be proved from the axioms with help of true implications. A system of axioms is consistent if one can not prove a statement of the form "A and not A". The verification is in individual cases often a complicated or even an unsolvable problem. We are satisfied, if we can quote a *model* for the system of axioms, that is, a system of concrete objects, which meet all the given axioms. A system of axioms is called *categorical* if essentially there exists only one model. By this we mean that for any two models we always get from one model to the other by renaming of the objects. If this is true then we have an *axiomatic characterization* of the model.

In the next section we introduce the natural numbers axiomatically.

1.2 The natural numbers and induction

The natural numbers $\mathbb{N}$ are presented by the system of axioms developed by G. Peano (1858–1932). This is done as follows.

The set $\mathbb{N}$ of the natural numbers is described by the following axioms:

($\mathbb{N}$ 1) $1 \in \mathbb{N}$.

($\mathbb{N}$ 2) Each $a \in \mathbb{N}$ has exactly one successor $a^+ \in \mathbb{N}$.

($\mathbb{N}$ 3) Always is $a^+ \neq 1$, and for each $b \neq 1$ there exists an $a \in \mathbb{N}$ with $b = a^+$.

($\mathbb{N}$ 4) $a \neq b \Rightarrow a^+ \neq b^+$.

DOI 10.1515/9783110516142-001

($\mathbb{N}$ 5) If $T \subset \mathbb{N}$, $1 \in T$, and if together with $a \in T$ also $a^+ \in T$, then $T = \mathbb{N}$.
(Axiom of *mathematical induction* or just induction.)

Remarks 1.1. (1) ($\mathbb{N}$ 2) and ($\mathbb{N}$ 4) mean that the map

$$\sigma : \mathbb{N} \to \mathbb{N}$$
$$a \mapsto a^+$$

is injective.
(2) From the Peano axioms we get per definition an addition, a multiplication and an ordering for $\mathbb{N}$:
(i) $a + 1 := a^+$,
$a + b^+ := (a + b)^+$,
(ii) $a \cdot 1 := a$,
$a \cdot b^+ := ab + a$,
(iii) $a < b :\Leftrightarrow \exists\, x \in \mathbb{N}$ with $a + x = b$ ("a smaller than b"),
$a \leq b :\Leftrightarrow a = b$ or $a < b$ ("a equal or smaller than b").

We need to recall some definitions.

A *semigroup* is a set $H \neq \varnothing$ together with a binary operation $\cdot : H \times H \to H$ that satisfies the associative property for all $a, b, c \in H$:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

The semigroup is *commutative* if

$$a \cdot b = b \cdot a.$$

In the commutative case we often write the operation as addition + instead of multiplication $\cdot$.

A *monoid* S is a semigroup with a unity element e, that is, an element e with $a \cdot e = a = e \cdot a$ for all $a \in S$; e is uniquely determined.

Moreover, a monoid S is called a *group* if for each $a \in S$ there exists an inverse element $a^{-1} \in S$ with $aa^{-1} = a^{-1}a = e$. The monoid or group is named commutative or abelian if in addition

$$a \cdot b = b \cdot a \quad \text{for all } a, b \in S.$$

We often write 1 instead of e. We also often drop $\cdot$ and use just juxtaposition for this operation. If we use the addition + we often write 0 instead of e and call 0 the *zero element* of S.

Theorem 1.2. (1) *The addition for $\mathbb{N}$ is associative, that is,*

$$a + (b + c) = (a + b) + c,$$

and commutative, that is,

$$a + b = b + a.$$

This means, $\mathbb{N}$ is a commutative semigroup with respect to the addition.

(2) *The multiplication for $\mathbb{N}$ is associative, that is,*

$$a(bc) = (ab)c,$$

and commutative, that is,

$$ab = ba.$$

$\mathbb{N}$ has also the unity element 1 for the multiplication. Therefore, $\mathbb{N}$ is a commutative monoid with respect to the multiplication.

(3) *The multiplication is distributive with respect to the addition, that is,*

$$(a + b)c = ac + bc.$$

(4) *For $a, b \in \mathbb{N}$ exactly one of the following is true:*

$$a < b, \quad a = b \quad \text{or} \quad b < a.$$

(5) *If $a \le b$ and $c \le d$ then $a + c \le b + d$ and $ac \le bd$.*

Proof. The statements follow directly from the definition and the Peano axioms. We leave the proofs as an exercise. As an example we prove (3) using (1) and (2): Let $a, b \in \mathbb{N}$ be arbitrary and $T \subset \mathbb{N}$ the set of the $c \in \mathbb{N}$ with $(a + b)c = ac + bc$. We have $1 \in T$ because

$$(a + b) \cdot 1 = a + b = a \cdot 1 + b \cdot 1.$$

Now, let $c \in T$. Then

$$\begin{aligned}(a + b)c^+ &= (a + b)c + (a + b) = ac + bc + a + b = ac + a + bc + b \\ &= ac^+ + bc^+.\end{aligned}$$

Hence $c^+ \in T$ and so $T = \mathbb{N}$. □

As usual we write a^n for $\underbrace{a \cdot a \cdots a}_{n \text{ times}}$ and na for $\underbrace{a + a + \cdots + a}_{n \text{ times}}$, when $a, n \in \mathbb{N}$.

Remarks 1.3. (1) By the development of the addition in $\mathbb{N}$ we suggest the usual representation of natural numbers as numerals:

$$\begin{aligned}&2 = 1^+ = 1 + 1, \quad 3 = 2^+ = 2 + 1, \\ &4 = 3^+ = 3 + 1 \quad \text{and so on.}\end{aligned}$$

(2) From the Peano axioms we also get that for each natural number n there exist exactly one natural number m with $m \le n < m + 1$. The set $\mathbb{N}$ is therefore a set unbounded from above.

(3) Theorem 1.2 also allows to subtract smaller natural numbers from larger ones. If $a, b \in \mathbb{N}$ with $a < b$, then there is an $x \in \mathbb{N}$ with $a + x = b$. We define the subtraction by

$$x := b - a$$

and say "x is equal b minus a".
Example 1.4.

$$3 = 11 - 8 = 17 - 14,$$
$$31 = 50 - 19.$$

(4) The mathematical proof technique *mathematical induction* is based on the Peano axiom ($\mathbb{N}$ 5). It is a form of direct proof, and it is done in two steps.
The first step, known as the *base case*, is to prove the given statement $A(n)$, which is definable for all $n \in \mathbb{N}$, for the first natural number 1. The second step, known as the *induction step*, is to prove that the given statement $A(n)$ is true for any natural number n implies the given statement is true for the next natural number. In other words, if $A(1)$ is true and if we can show that under the assumption that $A(n)$ is true for any n, then $A(n+1)$ is true, then $A(n)$ is true for all $n \in \mathbb{N}$.
We call the mathematical induction the *first induction principle* or the *principle of mathematical induction* (*PMI*).
It is clear that we may start with the mathematical induction with any natural number $n_0 > 1$ instead of 1, we just need a base. This can be done with the approach $B(n) := A(n_0 - 1 + n)$.

Examples 1.5. (1) **Claim.**

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \quad \textit{for all } n \in \mathbb{N}.$$

Proof. Let $A(n)$, $n \in \mathbb{N}$, be the asserted statement.
(a) $A(1)$ is true because

$$\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}.$$

(b) Assume that $A(n)$ is true for $n \in \mathbb{N}$. We have to show that $A(n+1)$ is true:

$$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1) = \frac{n(n+1)}{2} + (n+1)$$
$$= \frac{(n+1)(n+2)}{2},$$

and this is $A(n+1)$. □