

DE GRUYTER

GRADUATE

*Celine Carstensen-Opitz, Benjamin Fine,  
Anja Moldenhauer, Gerhard Rosenberger*

# ABSTRACT ALGEBRA

APPLICATIONS TO GALOIS THEORY, ALGEBRAIC  
GEOMETRY, REPRESENTATION THEORY AND  
CRYPTOGRAPHY

2ND EDITION

DE  
G



# Contents

Preface — V

Preface to the second edition — VII

## 1 Groups, rings and fields — 1

- 1.1 Abstract algebra — 1
- 1.2 Rings — 2
- 1.3 Integral domains and fields — 3
- 1.4 Subrings and ideals — 6
- 1.5 Factor rings and ring homomorphisms — 9
- 1.6 Fields of fractions — 13
- 1.7 Characteristic and prime rings — 14
- 1.8 Groups — 16
- 1.9 Exercises — 19

## 2 Maximal and prime ideals — 21

- 2.1 Maximal and prime ideals — 21
- 2.2 Prime ideals and integral domains — 22
- 2.3 Maximal ideals and fields — 24
- 2.4 The existence of maximal ideals — 25
- 2.5 Principal ideals and principal ideal domains — 26
- 2.6 Exercises — 28

## 3 Prime elements and unique factorization domains — 29

- 3.1 The fundamental theorem of arithmetic — 29
- 3.2 Prime elements, units and irreducibles — 34
- 3.3 Unique factorization domains — 38
- 3.4 Principal ideal domains and unique factorization — 41
- 3.5 Euclidean domains — 44
- 3.6 Overview of integral domains — 50
- 3.7 Exercises — 50

## 4 Polynomials and polynomial rings — 53

- 4.1 Polynomials and polynomial rings — 53
- 4.2 Polynomial rings over fields — 55
- 4.3 Polynomial rings over integral domains — 57
- 4.4 Polynomial rings over unique factorization domains — 59
- 4.5 Exercises — 65

<b>5</b>	<b>Field extensions — 67</b>
5.1	Extension fields and finite extensions — 67
5.2	Finite and algebraic extensions — 70
5.3	Minimal polynomials and simple extensions — 71
5.4	Algebraic closures — 74
5.5	Algebraic and transcendental numbers — 75
5.6	Exercises — 78
<b>6</b>	<b>Field extensions and compass and straightedge constructions — 81</b>
6.1	Geometric constructions — 81
6.2	Constructible numbers and field extensions — 81
6.3	Four classical construction problems — 84
6.3.1	Squaring the circle — 84
6.3.2	The doubling of the cube — 84
6.3.3	The trisection of an angle — 84
6.3.4	Construction of a regular $n$ -gon — 85
6.4	Exercises — 89
<b>7</b>	<b>Kronecker's theorem and algebraic closures — 93</b>
7.1	Kronecker's theorem — 93
7.2	Algebraic closures and algebraically closed fields — 96
7.3	The fundamental theorem of algebra — 101
7.3.1	Splitting fields — 101
7.3.2	Permutations and symmetric polynomials — 102
7.4	The fundamental theorem of algebra — 106
7.5	The fundamental theorem of symmetric polynomials — 109
7.6	Skew field extensions of $\mathbb{C}$ and Frobenius's theorem — 112
7.7	Exercises — 116
<b>8</b>	<b>Splitting fields and normal extensions — 119</b>
8.1	Splitting fields — 119
8.2	Normal extensions — 121
8.3	Exercises — 124
<b>9</b>	<b>Groups, subgroups, and examples — 125</b>
9.1	Groups, subgroups, and isomorphisms — 125
9.2	Examples of groups — 127
9.3	Permutation groups — 130
9.4	Cosets and Lagrange's theorem — 133
9.5	Generators and cyclic groups — 138
9.6	Exercises — 144

A new approach to conveying abstract algebra, the area that studies algebraic structures, such as groups, rings, fields, modules, vector spaces, and algebras, that is essential to various scientific disciplines such as particle physics and cryptology. It provides a well written account of the theoretical foundations and subtly explains the mathematical notions on a phenomenological basis accompanied with many examples and a problem section at the end of each chapter that helps the reader with accessing the subjects. It also includes a chapter on algebraic cryptography.

- ▶ Covering topics not found in competing works: Free groups and group presentations, modules and algebras, extension of rings and algebraic geometry, representations of groups, cryptographic protocols
- ▶ Extended Chapter about the hot topic combinatorial and geometric group theory
- ▶ New chapter about groups, algebras and representations

**Celine Carstensen-Opitz** VOLKSWOHL BUND Versicherungen, Dortmund, Germany

**Benjamin Fine** Fairfield University, Connecticut, USA

**Anja Moldenhauer** StatSoft (Europe) GmbH, Hamburg, Germany

**Gerhard Rosenberger** University of Hamburg, Germany



ID 20 1001 6858

ISBN 9783110603934



9 783110 603934

[www.degruyter.com](http://www.degruyter.com)

ISBN 978-3-11-060393-4