CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

CONCRETE ABSTRACT ALGEBRA

From Numbers to Gröbner Bases

Concrete Abstract Algebra develops the theory of abstract algebra from numbers to Gröbner bases, whilst taking in all the usual material of a traditional introductory course. In addition there is a rich supply of topics such as cryptography, factoring algorithms for integers, quadratic residues, finite fields, factoring algorithms for polynomials and systems of non-linear equations. A special feature is that Gröbner bases do not appear as an isolated example. They are fully integrated as a subject that can be taught successfully in an undergraduate context.

Lauritzen's approach to teaching abstract algebra is based on an extensive use of examples, applications and exercises. The basic philosophy is that inspiring, non-trivial, applications and examples give motivation and ease the learning of abstract concepts. This book is built on several years of experience teaching introductory abstract algebra at Aarhus, where the emphasis on concrete examples has improved student performance significantly.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

CONCRETE ABSTRACT ALGEBRA

From Numbers to Gröbner Bases

NIELS LAURITZEN
Department of Mathematical Sciences
University of Aarhus
Denmark

CAMBRIDGE
UNIVERSITY PRESS

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011–4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

© Cambridge University Press 2003

This book is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 2003

Printed in the United Kingdom at the University Press, Cambridge

Typeface Times 9/13 pt. *System* LaTeX 2$_\varepsilon$ [TB]

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in Publication data

Lauritzen, Niels, 1964–
Concrete abstract algebra: from numbers to Gröbner bases / Niels Lauritzen.
p. cm.
Includes bibliographical references and index.
ISBN 0 521 82679 9 (hardback) – ISBN 0 521 53410 0 (paperback)
1. Algebra, abstract. 1. Title
QA162.L43 2003
512′.02–dc21 2003051248

ISBN 0 521 82679 9 hardback
ISBN 0 521 53410 0 paperback

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

For Helle and William

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

Contents

Preface *page* xi
Acknowledgements xiv
1 Numbers 1
1.1 The natural numbers and the integers 3
1.1.1 Well ordering and mathematical induction 3
1.2 Division with remainder 4
1.3 Congruences 5
1.3.1 Repeated squaring – an example 7
1.4 Greatest common divisor 8
1.5 The Euclidean algorithm 9
1.6 The Chinese remainder theorem 14
1.7 Euler's theorem 17
1.8 Prime numbers 19
1.8.1 There are infinitely many prime numbers 20
1.8.2 Unique factorization 22
1.8.3 How to compute $\varphi(n)$ 24
1.9 RSA explained 24
1.9.1 Encryption and decryption exponents 25
1.9.2 Finding astronomical prime numbers 26
1.10 Algorithms for prime factorization 30
1.10.1 The birthday problem 30
1.10.2 Pollard's ρ-algorithm 31
1.10.3 Pollard's $(p-1)$-algorithm 33
1.10.4 The Fermat–Kraitchik algorithm 34
1.11 Quadratic residues 36
1.12 Exercises 41

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

2 Groups 50
2.1 Definition 50
2.1.1 Groups and congruences 51
2.1.2 The composition table 53
2.1.3 Associativity 54
2.1.4 The first non-abelian group 54
2.1.5 Uniqueness of neutral and inverse elements 55
2.1.6 Multiplication by $g \in G$ is bijective 56
2.1.7 More examples of groups 57
2.2 Subgroups and cosets 60
2.2.1 Subgroups of $\mathbb{Z}$ 61
2.2.2 Cosets 61
2.3 Normal subgroups 64
2.3.1 Quotient groups of the integers 66
2.3.2 The multiplicative group of prime residue classes 66
2.4 Group homomorphisms 68
2.5 The isomorphism theorem 71
2.6 Order of a group element 72
2.7 Cyclic groups 74
2.8 Groups and numbers 76
2.8.1 Euler's theorem 76
2.8.2 Product groups 76
2.8.3 The Chinese remainder theorem 77
2.9 Symmetric and alternating groups 78
2.9.1 Cycles 79
2.9.2 Simple transpositions and "bubble" sort 82
2.9.3 The alternating group 85
2.9.4 Simple groups 86
2.9.5 The 15-puzzle 88
2.10 Actions of groups 92
2.10.1 Conjugacy classes 98
2.10.2 Conjugacy classes in the symmetric group 98
2.10.3 Groups of order p^r 100
2.10.4 The Sylow theorems 101
2.11 Exercises 104
3 Rings 111
3.1 Definition 112
3.1.1 Ideals 115
3.2 Quotient rings 116
3.2.1 Quotient rings of $\mathbb{Z}$ 117

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

3.2.2 Prime ideals 118
3.2.3 Maximal ideals 118
3.3 Ring homomorphisms 119
3.3.1 The unique ring homomorphism from $\mathbb{Z}$ 120
3.3.2 Freshman's Dream 121
3.4 Fields of fractions 123
3.5 Unique factorization 125
3.5.1 Divisibility and greatest common divisor 126
3.5.2 Irreducible elements 126
3.5.3 Prime elements 127
3.5.4 Euclidean domains 130
3.5.5 Fermat's two-square theorem 132
3.5.6 The Euclidean algorithm strikes again 134
3.5.7 Prime numbers congruent to 1 modulo 4 135
3.5.8 Fermat's last theorem 137
3.6 Exercises 138
4 Polynomials 143
4.1 Polynomial rings 144
4.1.1 Binomial coefficients modulo a prime number 146
4.2 Division of polynomials 147
4.3 Roots of polynomials 150
4.3.1 Differentiation of polynomials 153
4.4 Cyclotomic polynomials 154
4.5 Primitive roots 157
4.5.1 Decimal expansions and primitive roots 159
4.5.2 Primitive roots and public key cryptography 160
4.5.3 Yet another application of cyclotomic polynomials 160
4.6 Ideals in polynomial rings 161
4.6.1 Polynomial rings modulo ideals 164
4.7 Theorema Aureum: the law of quadratic reciprocity 167
4.8 Finite fields 170
4.8.1 Existence of finite fields 172
4.8.2 Uniqueness of finite fields 172
4.8.3 A beautiful identity 173
4.9 Berlekamp's algorithm 176
4.10 Exercises 179
5 Gröbner bases 186
5.1 Polynomials in several variables 187
5.1.1 Term orderings 189

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

5.2 The initial term of a polynomial 193
5.3 The division algorithm 194
5.4 Gröbner bases 196
5.4.1 Hilbert's basis theorem 198
5.5 Newton revisited 200
5.6 Buchberger's S-criterion 203
5.6.1 The S-polynomials 204
5.6.2 The S-criterion 208
5.7 Buchberger's algorithm 208
5.8 The reduced Gröbner basis 212
5.9 Solving equations using Gröbner bases 214
5.10 Exercises 217
Appendix A Relations 223
A.1 Basic definitions and properties 223
A.2 Equivalence relations 224
A.2.1 Construction of the integers $\mathbb{Z}$ 226
A.2.2 Construction of the rational numbers $\mathbb{Q}$ 227
A.3 Partial orderings 228
Appendix B Linear algebra 230
B.1 Linear independence 231
B.2 Dimension 232

References 234
Index 236

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

Preface

Imagine that you have a very persistent piano teacher insisting that you study notes and practice scales for three years before you are allowed to listen to or play any real music. How is that going to affect your level of inspiration? Are you going to attend every lesson with passion or practice absolutely ignited with energy? Abstract algebra is like piano playing. You can kill your inspiration and motivation spending years on formalism before seeing the beauty of the subject. This book is written with the intent that every chapter should contain some real music, matters which involve practice of the notes and scales in a surprising and unexpected way. It is an attempt to include a lot of non-trivial and fun topics in an introductory abstract algebra course. Having inspiring goals makes the learning easier. The topics covered in this book are numbers, groups, rings, polynomials and Gröbner bases.

Knowledge of linear algebra and complex numbers is assumed in some examples. However, most of the text is accessible with only basic mathematical topics such as sets, maps, elementary logic and proofs.

Gröbner bases are usually not treated at an undergraduate level. My feeling four years ago when including this topic in the syllabus at Aarhus was one of hesitation. I was afraid that the material would be too advanced for the students. It turned out that the students liked the concrete nature of the material and enjoyed the non-trivial computations with polynomials. They found it easier than the traditional topics of groups and rings.

Unlike most treatments on Gröbner bases, I have not included any implementations of algorithms in a pseudo-language. My personal experience is that it disturbs the flow of the mathematics when teaching the basic ideas of the algorithms. Once the mathematical concepts and a few examples are understood, it is easy to extract the algorithms for implementation on a computer. In fact

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

students are very much encouraged to experiment using a computer algebra system especially when learning about numbers and Gröbner bases.

Chapter 1 is on numbers. It is mostly based on the RSA cryptosystem and the mystery that it seems much easier to multiply numbers than to factor them. The 617-digit number on the cover of this book is a product of two prime numbers. If you can find them you should write to RSA Labs and claim the $200, 000 prize. Going through the first chapter you will learn basic number theory: division with remainder, congruences, the Euclidean algorithm, the Chinese remainder theorem, prime numbers, how prime numbers uncovered the infamous FDIV bug in Intel's Pentium processor, Fermat's little theorem and how it is used to produce 100-digit prime numbers for the modern information age, three modern algorithms for factoring numbers much faster than by trial division, quadratic residues and the quadratic reciprocity theorem (which will be proved in Chapter 4).

The level of abstraction is increased in Chapter 2. Here the mathematical object is a group. A group is defined using a composition on a set and it satisfies three simple rules. This definition has proved extremely important and invaluable to modern algebra. You get a framework for many proofs and concepts from basic number theory. We treat the basics of group theory, the symmetric and alternating groups, how to solve the 15-puzzle using groups, actions of groups, counting and the Sylow theorems.

In Chapter 3 we treat rings. A ring is an abelian group with multiplication as an added composition. We touch briefly on non-commutative rings, with the quaternions as an example. We then move on to commutative rings, Freshman's Dream, fields, domains, principal ideal domains, Euclidean domains and unique factorization domains. The Fermat two-square theorem (every prime number leaving a remainder of 1 when divided by 4 can be written as a sum of two unique squares (e. g. $13 = 3^2 + 2^2$)) is a prime example in this chapter. You will see the infinitude of prime numbers leaving a remainder of 1 when divided by 4, further use of quadratic residues and an effective algorithm for computing the two squares in the two-square theorem.

Polynomials form a central topic. In Chapter 4 we treat polynomials in one variable. Here the highlights are: cyclotomic polynomials, a proof of the law of quadratic reciprocity using only basic properties of rings of polynomials, how to use floating point arithmetic to compute the order of specific elements in a well known cyclic group, the ElGamal cryptosystem, the infinitude of prime numbers congruent to 1 modulo a natural number > 1 and the existence and uniqueness of finite fields, along with algorithms for factoring polynomials over finite fields.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

In Chapter 5 polynomials in several variables and Gröbner bases are treated. Gröbner bases form an exciting and relatively new branch of algebra. They are very concrete and computational. The distance from understanding the abstract concepts involved to computing with them is small. They provide a framework for solving non-linear equations (used in most computer algebra systems) with applications in many areas inside and outside algebra. In Chapter 5 you will see term orders, the fundamental Dickson's lemma, the division algorithm for polynomials in several variables, the existence of Gröbner bases, Hilbert's basis theorem, Buchberger's S-criterion and algorithm, how to write $X^4 + Y^4$ as a polynomial in $X + Y$ and XY (like writing $X^2 + Y^2$ as $(X + Y)^2 - 2XY$) using Gröbner bases and how to solve certain non-linear equations in several variables systematically.

A few exercises are marked **HOF**. This indicates that they are "hall of fame" exercises, far beyond what is required in an introductory abstract algebra course. They usually call for an extraordinary amount of ingenuity. A student capable of solving one of these deserves to be inducted into the hall of fame of creative problem solvers. A hall of fame museum can be suitably maintained using a course home page.

Suggestions for teaching a one-semester course

The book contains too much material for a one-semester course in introductory abstract algebra. So, a selection of material must be made. A possible procedure would be to leave out factoring algorithms from Chapter 1, quadratic reciprocity from Chapters 1 and 4 and the Sylow theorems from Chapter 2. This plan would give a one-semester course ending with Gröbner bases; it would cover the usual topics in an introductory course.

Leaving out Gröbner bases completely, Chapters 1 through 4 would form an in-depth traditional introductory abstract algebra course with many examples.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Frontmatter
More information

Acknowledgements

I wish to thank all the students of Algebra 1 at the University of Aarhus during the past four years for carefully listening, asking questions, looking puzzled at the right (or wrong) times and for inspiring me to change my exposition several times. I wish in particular to thank R. Villemoes for many valuable comments and for a set of detailed TEX-solutions to the exercises (available through Cambridge University Press).

Many people influenced this book either by discussions and comments or by patiently answering my numerous questions: T. B. Andersen, H. H. Andersen, M. Bökstedt, J. Brandt, A. Buch, A. L. Christophersen, I. Damgaard, R. Faber Larsen, P. de Place Friis, S. Galatius Smith, W. J. Haboush, J. P. Hansen, G. Hellmund, C. U. Jensen, T. H. Lynderup, T. Høholdt, T. Laframboise, M. Skov Madsen, K. Nielsen, U. Raben Pedersen, M. S. Risager, A. Skovborg, H. G. Spalk, J. Tornehave, H. Vosegaard and A. Venkov.

I am particularly indebted to J. C. Jantzen for reading carefully earlier versions of my Algebra 1 notes. His comments were (as always) extremely relevant and helpful. J. F. Thomsen also read earlier versions of the notes and made detailed comments on the 15-puzzle, which led to substantial improvements. H. A. Salomonsen pointed out a substantial simplification that moved the proof of quadratic reciprocity from the context of finite fields to the more student-friendly environment of the basic theory of polynomials. An anonymous referee from the US made meticulous comments and suggestions which greatly facilitated the process of turning my incomplete notes into the present book. J. Walthoe at Cambridge University Press has been extremely helpful making several insightful suggestions.

This book is for Helle and William. They have unselfishly fueled my writing with their love.

© Cambridge University Press www.cambridge.org