

Abstract Algebra

A Comprehensive Introduction

Through this book, upper undergraduate mathematics majors will master a challenging yet rewarding subject, and approach advanced studies in algebra, number theory and geometry with confidence. Groups, rings and fields are covered in depth with a strong emphasis on irreducible polynomials, a fresh approach to modules and linear algebra, a fresh take on Gröbner theory, and a group theoretic treatment of Rejewski's deciphering of the Enigma machine. It includes a detailed treatment of the basics on finite groups, including Sylow theory and the structure of finite abelian groups. Galois theory and its applications to polynomial equations and geometric constructions are treated in depth. Those interested in computations will appreciate the novel treatment of division algorithms. This rigorous text “gets to the point,” focusing on concisely demonstrating the concept at hand, taking a “definitions first, examples next” approach. Exercises reinforce the main ideas of the text and encourage students' creativity.

John W. Lawrence is Professor Emeritus at the University of Waterloo. He was born in Ottawa, Canada, and received degrees from Carleton University and McGill University. After a year of postdoctoral work at the University of Chicago, he joined the Pure Mathematics Department of the University of Waterloo. He now lives with his wife Louise, in Thornhill Canada, where he continues his research in mathematics and probability.

Frank A. Zorzitto is Professor Emeritus at the University of Waterloo. After receiving his doctorate at Queen's University in Kingston, Canada, he served for forty years as a researcher in algebra and a professor in the Pure Mathematics Department at the University of Waterloo, and served as Department Chair for twelve years. In recognition of his commitment to the education of students, he received the University's Distinguished Teaching Award. Upon his retirement he was made an Honorary Member of the University. Currently he offers an online course to high school math teachers, based on his ebook *A Taste of Number Theory*. He continues to teach and to write in his retirement.

CAMBRIDGE MATHEMATICAL TEXTBOOKS

Cambridge Mathematical Textbooks is a program of undergraduate and beginning graduate-level textbooks for core courses, new courses, and interdisciplinary courses in pure and applied mathematics. These texts provide motivation with plenty of exercises of varying difficulty, interesting examples, modern applications, and unique approaches to the material.

Advisory Board

Paul T. Allen, *Lewis & Clark College*
Melody Chan, *Brown University*
Teena Gerhardt, *Michigan State University*
Illya Hicks, *Rice University*
Greg Lawler, *University of Chicago*
John M. Lee, *University of Washington*
Lawrence Washington, *University of Maryland, College Park*
Talithia Williams, *Harvey Mudd College*

A complete list of books in the series can be found at www.cambridge.org/mathematics
Recent titles include the following:

Chance, Strategy, and Choice: An Introduction to the Mathematics of Games and Elections, S. B. Smith
Set Theory: A First Course, D. W. Cunningham
Chaotic Dynamics: Fractals, Tilings, and Substitutions, G. R. Goodson
A Second Course in Linear Algebra, S. R. Garcia & R. A. Horn
Introduction to Experimental Mathematics, S. Eilers & R. Johansen
Exploring Mathematics: An Engaging Introduction to Proof, J. Meier & D. Smith
A First Course in Analysis, J. B. Conway
Introduction to Probability, D. F. Anderson, T. Seppäläinen & B. Valkó
Linear Algebra, E. S. Meckes & M. W. Meckes
A Short Course in Differential Topology, B. I. Dundas
Abstract Algebra with Applications, A. Terras
Complex Analysis, D. E. Marshall
Abstract Algebra: A Comprehensive Introduction, J. W. Lawrence & F. A. Zorzitto

Abstract Algebra

A Comprehensive Introduction

John W. Lawrence

University of Waterloo, Ontario

Frank A. Zorzitto

University of Waterloo, Ontario



CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom
One Liberty Plaza, 20th Floor, New York, NY 10006, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India
79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108836654
DOI: 10.1017/9781108874328

© John W. Lawrence and Frank A. Zorzitto 2021

This publication 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 2021

Printed in the United Kingdom by TJ Books Limited, Padstow Cornwall

A catalogue record for this publication is available from the British Library.

ISBN 978-1-108-83665-4 Hardback

Additional resources for this publication at www.cambridge.org/abstract-algebra

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Dedicated to our families...

Louise, Donna, Lisa, Joanna, Angela and Alex

Contents

Preface	<i>page</i> xv
1 A Refresher on the Integers	1
1.1 Euclidean Division and the Greatest Common Divisor	1
1.2 Primes and Unique Factorization	7
1.3 Congruences	12
2 A First Look at Groups	20
2.1 Basic Properties and Examples of Groups	20
2.1.1 The Order of a Group and of Its Elements	27
2.2 The Symmetric Group	33
2.2.1 Equivalence Relations and Partitions	34
2.2.2 The Orbits and Cycles of a Permutation	35
2.2.3 Transpositions and the Parity of a Permutation	42
2.3 Subgroups and Lagrange's Theorem	50
2.3.1 Partitions of a Group by Right Cosets of a Subgroup	52
2.3.2 Subgroups of Cyclic Groups	58
2.4 Conjugation and Normal Subgroups	62
2.4.1 Conjugates in \mathcal{S}_n	65
2.4.2 Normal Subgroups of \mathcal{A}_n	67
2.4.3 Normal Subgroups of the Quaternion Group	71
2.5 Homomorphisms	73
2.5.1 The Kernel and Image of a Homomorphism	76
2.5.2 Isomorphisms	77
2.5.3 Automorphisms of Cyclic Groups	79
2.6 Quotient Groups	81
2.6.1 An Important Theorem of Cauchy	83
2.6.2 The First Isomorphism Theorem	84
2.6.3 The Correspondence Theorem	87
2.7 Products of Groups	91
2.7.1 The External Product	91
2.7.2 The Internal Product of Subgroups	94
2.8 Finite Abelian Groups	99
2.8.1 Groups of Prime Power Order	100

viii Contents

2.8.2	The Primary Decomposition	108
2.8.3	Putting the Bits Together	111
3	Groups Acting on Sets	116
3.1	Definition and Some Illustrations of Actions	116
3.1.1	A Group Action on Left Cosets	119
3.1.2	Groups of Order 6	120
3.2	Orbits and Stabilizers	122
3.2.1	An Action for the Dihedral Groups	125
3.2.2	The Symmetries of a Tetrahedron	128
3.3	The Cauchy–Frobenius–Burnside Formula	131
3.3.1	A Counting Technique Based on Burnside	133
3.4	The Class Equation and Its Implications	138
3.4.1	The Class Equation	138
3.4.2	The Class Equation and p -Groups	142
3.5	The Theorems of Cauchy and Sylow	145
3.5.1	Cauchy’s Theorem	146
3.5.2	Sylow’s Theorem	148
3.6	Semi-direct Products	159
3.6.1	Automorphism Actions of One Group on Another	159
3.6.2	Internal and Semi-direct Products	162
3.6.3	Groups of Order pq – the Full Description	163
3.7	Solvable Groups	170
3.7.1	The Second and Third Isomorphism Theorems	171
3.7.2	Subgroups and Quotients of Solvable Groups	173
3.7.3	Improving the Subnormal Chains for Solvable Groups	175
3.7.4	Commutators and the Derived Series	176
3.8	Breaking the Enigma	181
3.8.1	The Design of the Enigma Machine	181
3.8.2	The Mathematical Representation of the Enigma Machine	183
3.8.3	How the Machine Was Used	186
3.8.4	Finding the First Rotor Wiring	195
4	Basics on Rings – Mostly Commutative	203
4.1	Terminology and Examples	203
4.1.1	Compound Additions and Multiplications	206
4.1.2	Subrings	207
4.2	Units and Zero Divisors	210
4.2.1	The Group of Units	210
4.2.2	Zero Divisors	211
4.2.3	Integral Domains and Fields	213

	Contents	ix
4.3	Polynomials	216
4.3.1	The Definition of Polynomial Rings	217
4.3.2	Properties of the Degree	222
4.3.3	Polynomials in Several Variables	224
4.3.4	The Ring of Formal Power Series	224
4.4	Homomorphisms and Ideals	226
4.4.1	Ring Homomorphisms	227
4.4.2	The Kernel	231
4.4.3	Ideals	232
4.5	Ideals in \mathbb{Z} and in Polynomial Rings	237
4.5.1	Finite Groups of Units in a Field	240
4.6	Quotient Rings and the Isomorphism Theorem	244
4.6.1	The First Isomorphism Theorem for Rings	245
4.6.2	Computing the Euler Function	248
4.6.3	The Correspondence Theorem	249
4.7	Maximal and Prime Ideals	252
4.7.1	Maximal Ideals and the Construction of Fields	253
4.7.2	Existence of Maximal Ideals	254
4.7.3	Prime Ideals and Integral Domains	255
4.7.4	Building Fields from Polynomial Rings	256
4.8	Fractions	259
4.8.1	Localizations at Denominator Sets	259
4.8.2	Uniqueness of Localizations	261
4.8.3	Existence of Localizations	262
5	Primes and Unique Factorization	268
5.1	Primes, Irreducibles and Factoring	268
5.2	Principal Ideal and Noetherian Domains	274
5.2.1	Noetherian Domains	275
5.3	Euclidean Domains	278
5.4	Gaussian Primes and Sums of Squares	281
5.5	Greatest Common Divisors	285
5.6	Polynomials over Unique Factorization Domains	294
5.6.1	Gauss' Lemma	294
5.6.2	The Primes of $A[X]$ and Its Unique Factorization	297
5.7	Irreducible Polynomials	300
5.7.1	The Rational Root Test	301
5.7.2	Using a Natural Extension of Homomorphisms	304
5.7.3	Eisenstein's Criterion	305
5.8	Polynomials over Noetherian Rings	308
5.8.1	Hilbert's Basis Theorem: a Source of Noetherian Rings	309

x	Contents	
	5.8.2 Eisenstein's Criterion for Noetherian Domains	311
	5.8.3 Primes in Rings Coming from Algebraic Integers	314
	5.8.4 A Principal Ideal Domain that Is Not Euclidean	317
6	Algebraic Field Extensions	322
6.1	Algebraic Elements and Degrees of Extensions	322
6.1.1	The Degree of a Field Extension	322
6.1.2	Algebraic Elements	323
6.1.3	The Minimal Polynomial of an Algebraic Element	325
6.1.4	A Basis for a Singly Generated Algebraic Extension	327
6.1.5	Algebraic Elements with the Same Minimal Polynomial	329
6.1.6	The Tower Theorem	330
6.1.7	Fields Generated by Several Algebraic Elements	331
6.1.8	The Algebraic Closure inside a Field Extension	334
6.1.9	The Tower Theorem and Composite Fields	335
6.1.10	The Tower Theorem Used in Conjunction with Eisenstein for Noetherian Domains	337
6.2	Splitting Fields	341
6.2.1	The Synthesis of Algebraic Elements	341
6.2.2	What Is a Splitting Field?	343
6.2.3	Lifting Isomorphisms to Splitting Fields	346
6.2.4	The Uniqueness of Splitting Fields	349
6.2.5	Finite Fields of Equal Size Are Isomorphic	349
6.2.6	Splitting Fields Are Rich with Automorphisms	350
6.2.7	Fixed Fields, F -Maps and F -Conjugates	351
6.2.8	The Normality Theorem	352
6.2.9	A Control on the Degree of a Splitting Field	355
6.2.10	Quadratic Extensions Are Splitting Fields	356
6.3	Separability	360
6.3.1	Derivatives of Polynomials and Repeated Roots	360
6.3.2	Separable Polynomials and the Derivative	362
6.3.3	Finite Fields of All Possible Sizes	364
6.3.4	Factoring $X^{p^n} - X$ in $\mathbb{Z}_p[X]$	365
6.3.5	Perfect Fields	366
6.4	The Galois Group	371
6.4.1	Roots, Generators and Galois Groups	372
6.4.2	Some Examples of Galois Groups	374
6.5	The Core of Galois Theory	379
6.5.1	The Independence of Characters	379
6.5.2	A Bound on the Order of a Galois Group	381
6.5.3	The Fixed Field of an Automorphism Group	382

	Contents	xi
6.5.4	Galois Extensions	383
6.5.5	Artin's Theorem	386
6.5.6	The Galois Correspondence	387
6.5.7	The Fundamental Theorem of Galois Theory	388
6.5.8	The Normality Connection	389
7	Applications of Galois Theory	397
7.1	Three Classical Theorems	397
7.1.1	The Primitive Generator Theorem	397
7.1.2	The Fundamental Theorem of Algebra	399
7.1.3	The Symmetric Function Theorem	399
7.2	Special Extensions and Their Galois Groups	403
7.2.1	The Galois Correspondence in Finite Fields	403
7.2.2	The Galois Groups of Cubics	405
7.2.3	Cyclotomic Extensions	408
7.3	Solvability of Equations by Radicals	414
7.3.1	Cardano's Formula	414
7.3.2	Extensions by a Single Radical and Cyclic Galois Groups	418
7.3.3	Radical Towers	420
7.3.4	Solvable Polynomials Have Solvable Galois Groups	424
7.3.5	Polynomials with Solvable Galois Groups Are Solvable	426
7.4	Ruler and Compass Constructions	428
7.4.1	Constructible Points, Lines and Circles	429
7.4.2	Constructible Real Numbers	433
7.4.3	Constructible Real Numbers and Field Towers	435
7.4.4	Constructible Complex Numbers	440
7.5	The Inverse Galois Problem over \mathbb{Q}	444
8	Modules over Principal Ideal Domains	450
8.1	The Language and Tools of Modules	450
8.1.1	Examples of Modules	451
8.1.2	Module Homomorphisms	452
8.1.3	Submodules	453
8.1.4	Free Modules	454
8.1.5	Quotient Modules and the First Isomorphism Theorem	457
8.1.6	Cyclic Modules and Annihilator Ideals	459
8.1.7	Direct Sums of Submodules	460
8.1.8	Free Modules Are Projective	462
8.2	Modules over Integral Domains	464
8.2.1	Torsion Elements and Modules	465
8.2.2	Rank	466

xii Contents

8.3	Modules over Principal Ideal Domains	468
8.3.1	Splitting Torsion from Torsion-Free	469
8.3.2	Torsion Modules over a Principal Ideal Domain	471
8.3.3	Primary Modules over a Principal Ideal Domain	475
8.3.4	Structure of Finitely Generated Modules over a Principal Ideal Domain	479
8.4	Linear Algebra and Modules	488
9	Division Algorithms	507
9.1	Well-Partial Orders	508
9.1.1	Well-Ordered Sets: Total and Partial	508
9.1.2	The Dickson Basis	513
9.1.3	Extensions of Well-Partial Orders	514
9.2	Gröbner Domains	520
9.2.1	Gröbner Functions	520
9.2.2	The Gröbner Basis of an Ideal	522
9.2.3	Polynomials in Several Variables Are Gröbner Domains	524
9.2.4	A Division Algorithm for Complete Reductions	527
9.3	Buchberger's Algorithm	539
9.3.1	Detecting Gröbner Bases via S -Polynomials	539
9.3.2	Buchberger's Algorithm	545
9.4	Applications of Gröbner Bases	553
9.4.1	Gröbner Bases for Ideal Intersections	554
9.4.2	Units and Zero Divisors in Finitely Generated Algebras	559
9.4.3	Normal Forms	563
9.4.4	Finite Varieties	570
9.4.5	Hilbert's Nullstellensatz and Idempotents	575
A	Infinite Sets	593
A.1	Zorn's Lemma	593
A.1.1	Choice Functions	593
A.1.2	Chains of Subsets	593
A.1.3	Chain Maximality in Partially Ordered Sets	595
A.1.4	Choice Implies Zorn	597
A.1.5	The Well-Ordering Principle	597
A.1.6	Zorn Implies Choice	599
A.2	The Size of Infinite Sets	600
A.2.1	Infinite Sets and the Positive Integers	600
A.2.2	Comparing Sets	601
A.2.3	Countable Sets	602
A.2.4	The Cantor–Schröder–Bernstein Theorem	603

	Contents	xiii
A.2.5	Total Ordering by Cardinality	604
A.2.6	The Unboundedness of Cardinality	605
A.2.7	A Bit of Cardinal Arithmetic	606
A.3	The Algebraic Closure of a Field	611
	Index	617

Preface

Every practitioner of mathematics, pure or applied, could use some algebra. Algebra includes an adherence to precise definitions, a willingness to examine concrete problems through meaningful abstractions, and a thirst for lucid proofs based on the axiomatic method. Despite its challenges, algebra has for a long time now been a mainstay of the curriculum in mathematics programs. Not to mention that some people are actually drawn to its puzzles and surprises. Since Bartel Leendert van der Waerden's seminal book *Moderne Algebra* was published in 1930, a multitude of authors have offered their take on this subject. By means of this book we hope to make our contribution.

Our book is intended for senior undergraduate students of modern abstract algebra. Those more gifted in mathematics can well profit from it sooner. Beginning graduate students who need a refresher could find it useful as well. We expect that our reader comes with a bit of exposure to rigorous proofs, some familiarity with the common language of sets such as injective and surjective mappings, and some understanding of linear algebra including such notions as finite-dimensional vector spaces, non-singular matrices, and linear transformations.

In order for any mathematics book to be effective, it must be precise with the mathematics but also approachable to the student. We have tried to meet this goal by walking a fine line between proper mathematical formality and reader friendliness. We hope to have not written too much, but also not too little. There seem to be two points of view regarding the introduction of a concept. One is that the student should be gently exposed to motivating examples first. Another aims for efficiency, presenting the definitions and theorems at the outset. By and large we have taken a “definitions first – examples next” approach, thinking that too much effort at motivation can in its own way be distracting. Yet we have tried not to go overboard with this approach, and to offer motivating examples soon enough.

Obviously, the exercises are for learning. If the exercises in a book are too easy, the student will not learn enough, and quickly become bored. If they are too hard, discouragement can set in. We have decided to limit the number of exercises that are utterly routine. Yet once a student has digested a section, the bulk of the exercises that follow it should be of reasonable difficulty. Those exercises which might be considered hard are marked with an asterisk. In the end, the difficulty of the exercises will depend on the preparation, skill and stamina of the student.

Algebra now comprises several large areas and many special topics within them. This makes it challenging for authors to select which topics will meet the expectations of a broad segment of algebra instructors, whose task it is to pick a book for their students. We structured our

xvi Preface

book along the traditional lines of groups, rings, fields and Galois theory. For something extra we offer an in depth discussion of modules over principal ideal domains and of Gröbner bases, a subject which may be of interest to those who relish computing.

We open our book with a short discussion on the integers, primes and congruences, in order to ensure the student sees the ways of algebra within a truly basic example. These matters are treated in the spirit of a review, which could well be familiar to many a reader.

Our book more properly begins with Chapter 2 where we discuss groups, with an emphasis on finite groups, using a well trodden approach. The symmetric group gets a careful discussion. The fundamentals of Lagrange's theorem (including the failure of its converse), normal subgroups, homomorphisms, quotient groups, the first isomorphism theorem, internal and external products of groups, are covered along familiar lines. We close the chapter with a proof of the structure theorem for finite abelian groups. Since by its very nature this will demand a bit more of the student, we go at it with patience.

Chapter 3 focuses on group actions, orbits, stabilizers, some counting problems, the class equation, and the substantial Sylow theory. We introduce semi-direct products as a way to describe some groups. In anticipation of their use in Galois theory the chapter closes with the basics about solvable groups. Even though this is primarily a book in pure mathematics, we decided to close Chapter 3 with a discussion of the Enigma machine and how group theory was used to break the Enigma code. This is an interesting story of how abstract algebra influenced history.

Chapters 4 and 5 are about rings, with commutative domains as the primary focus. In Chapter 4 we cover the essential notions of units, zero divisors, ideals, integral domains, quotient rings, homomorphisms, the first isomorphism theorem, the correspondence theorem, maximal and prime ideals, and fraction fields. We also offer a somewhat more leisurely treatment of the notion of polynomials, which of course can be glossed over by those who feel it might be unnecessary. Chapter 5 is about primes, unique factorization, Euclidean domains, Gauss' lemma, irreducibility of polynomials, and the Hilbert basis theorem for Noetherian rings. We also introduce a souped up version of Eisenstein's criterion, which can be used in unexpected ways to compute degrees of field extensions.

In Chapter 6 we cover algebraic field extensions, splitting fields, separable polynomials, and the Galois group. Here the reader will find an unhurried treatment of the Galois correspondence. Some of the more important applications of Galois theory are offered in Chapter 7, including, of course, Galois' contribution on the solvability of polynomial equations by radicals. There is also a comprehensive treatment of ruler and compass constructions, which at one point uses a bit of Galois theory.

Chapter 8 deals with the structure theorem for finitely generated modules over principal ideal domains along with its application to the Jordan canonical form for matrices. Of course it also applies to finite (and even finitely generated) abelian groups, but that topic is dealt with in Chapter 2. A small bit of redundancy is useful because not every student will get to Chapter 8, and because students can benefit from seeing the same ideas more than once.

An expert may notice that our proofs of a few difficult points differ somewhat from the mainstream. We hope that the reader will like the way we have organized this challenging material.

Our treatment of Gröbner bases in Chapter 9 is more daring. We want to present the concept of a Gröbner basis in the setting of abstract algebra. For this reason we open up with a discussion of what we call a Gröbner domain. These can be seen as a generalization of Euclidean domains, which permits division algorithms in a larger context. Even though our chief example is the ring of polynomials in several variables over a field, we try to remain within the abstraction of Gröbner domains as much as possible.

Our closing Appendix A offers some informal set theory, including the equivalence of the axiom of choice and Zorn's lemma, a discussion of cardinality, and the use of these ideas to build the algebraic closure of any field. The preceding chapters do not make significant use of Appendix A. The proof that rings have maximal ideals is the main (and easy) application of Zorn's lemma. The material of Appendix A is offered for the student who might find it handy to have it here, and might appreciate our effort to make this abstract material approachable.

The book contains more than enough material for two semesters of instruction. We find it difficult to advise how much is to be covered in a given semester. This is because the length of a semester can differ across various jurisdictions, and also because classes can differ in their abilities and institutions can differ in their expectations. In our home university in a third year one semester course we typically would assume Chapter 1, and then cover much of Chapters 2, 3, 4 and 5 on groups and rings, possibly skipping a few themes such as semi-direct products, solvable groups, the Enigma machine, and irreducibility over Noetherian domains. This would be followed up in a second semester with an in depth discussion of field and Galois theory including a discussion of solvable groups. If the class is up to it, we might also treat Chapter 9 on Gröbner bases or possibly modules over principal ideal domains.

Here are some suggested ways to use our book for a one semester course:

- Chapters 1, 2, 3 for a course on groups
- Chapters 1, 4, 5, 6, 7 for a substantial course on commutative rings, fields and Galois theory
- Chapters 1, 4, 5, 8 for a course on commutative rings and modules
- Chapters 1, 4, 5, 9 for a course on rings and division algorithms.

Some instructors believe it is better to teach commutative rings before groups. Even though we have followed the common order of groups-rings-fields, an instructor who wishes to teach rings first should be able to jump into Chapter 4 from the get go. Our treatment of rings makes a small use of the basic facts about groups, but the very slight amount of group theory needed can readily be filled in by the instructor.

The book can also be used in algebra courses of a more general nature. We have tried to adopt a style that is student friendly by explaining the ideas and proofs in a detailed and self contained manner.

xviii Preface

One irritant which we have tried to minimize is the somewhat distracting practice of referring to exercises or to other proofs within the proof of a result. Another distracting habit is to leave steps within a proof as an exercise. Of course this is deemed to encourage the student to work through some details. It can also be a reflection of an author's impatience. These features cannot be avoided entirely, but by proving virtually everything we claim at the moment we claim it, we think that reading our text will lead to a more seamless experience.

Our gratitude goes out to our Pure Mathematics Department at the University of Waterloo, which gave us the opportunity to teach courses in algebra and thereby come to appreciate what might be interesting, what might be important, and what might be fun. Our never ending streams of committed and often brilliant students taught us that algebra can be a pleasure to learn and to teach.