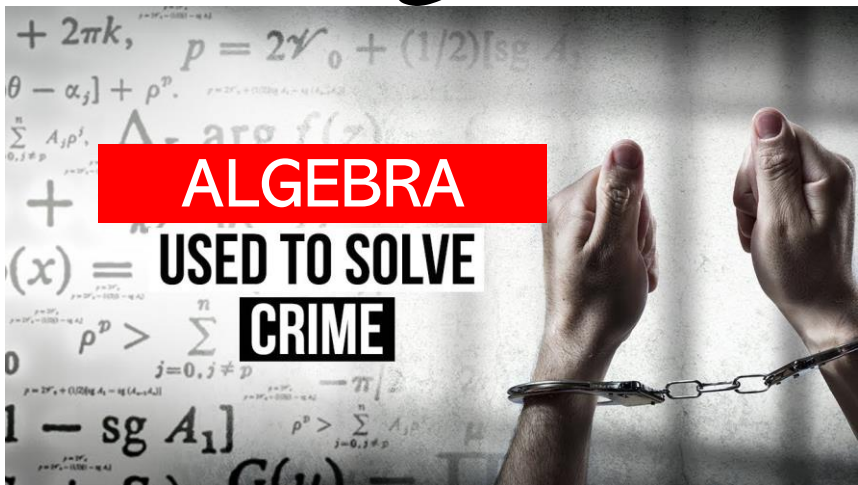


Techniques of Algebra



Dr C.D.H. Cooper
Macquarie University

3rd EDITION January 2022

These notes were prepared for students at Macquarie University in Australia but are freely available to anyone. However if you make use of them and are not a Macquarie University student it would be nice if you could email me at christopherdonaldcooper@gmail.com to let me know where you are from. And, if you are from outside of Australia perhaps you could send me a postcard of where you are from to pin up on my wall (Christopher Cooper, 31 Epping Avenue, EASTWOOD, NSW 2122, Australia).

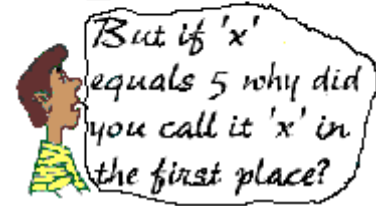
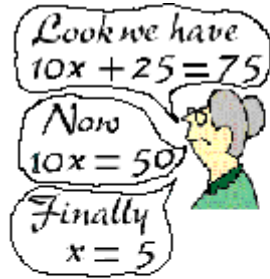
INTRODUCTION

The name “algebra” is derived from the Arabic “al-jabr”, meaning “restoration”. It builds on arithmetic. Instead of carrying out the arithmetic operations of addition, subtraction, multiplication and division with numbers, we include symbols that *represent* numbers.

But algebra goes far beyond the algebra we learnt at school, which is the algebra of real numbers. When we learn about complex numbers we will see that most of high-school algebra works for complex numbers, but not that part of it that involves inequalities.

Polynomials are an important part of algebra and here we take the theory of polynomials somewhat beyond what we learn at school, including solving two polynomial equations in two variables, as well as polynomials in a complex variable.

The final section deals with group theory. This will be your first glimpse of abstract algebra. A group is an algebraic system that consists of a set together with an operation of multiplication. But the elements of the set need not be numbers and the “multiplication” need not have anything to do with multiplication as we know it. All we assume are four basic axioms that regulate the way that this generalized multiplication operates.



While there are groups of numbers, group theory can take us way beyond the confines of mathematics. For example the four ways you can turn a mattress constitute a little group with just four things. A slightly larger group, called the dihedral group of order 8 (meaning that there are 8 things in it) lies behind the kinship rules of the Warlpiri tribe of aborigines (not that they recognised it as a part of group theory).

More important applications are to physics and to certain parts of chemistry. In these notes we merely scratch the surface. We concentrate on finite groups, where we discover that the size of the group gives a lot of information about the structure of the group. There is a set of notes entirely devoted to Group Theory.

An important part of first year mathematics is an area called Linear Algebra, which deals with matrices and abstract vector spaces. These are dealt with in another set of notes.

Most of this material can be found in standard first year algebra textbooks. However there are some novelties, such as the One-Way Euclidean Algorithm in the chapter on integers and divisibility and a discussion of solving systems of polynomial equations in several variables.

CONTENTS

PART A: FUNDAMENTAL CONCEPTS

1. REAL NUMBERS

1.1 The History of Number	11
1.2 The Laws of Algebra	19
1.3 Basic Algebraic Identities	26
1.4 Solving Linear Equations	28
1.5 Quadratic Equations	30
1.6 Sum and Product of Zeros	34
1.7 Fractions	36
1.8 Surd Equations	39
Exercises for Chapter 1	42
Solutions for Chapter 1	43

2. INEQUALITIES AND ABSOLUTE VALUES

2.1 The Ordering of the Real Numbers	47
2.2 Inequalities	50
2.3 Intervals	53
2.4 Harder Inequalities	54
2.5 Absolute Value	60

3. INDUCTION AND FINITE SERIES

3.1 Mathematical Induction	65
3.2 Inductive Definitions	70
3.3 Arithmetic	74
3.4 Geometric Series	78
3.5 Sigma Notation	85
Exercises for Chapter 3	85
Solutions for Chapter 3	85

4. THE BINOMIAL THEOREM

4.1 Number of Arrangements	89
4.2 Number of Choices	91
4.3 Pascal's Triangle	97
4.4 The Binomial Theorem	98
4.5 Binomial Probability	101
Exercises for Chapter 4	104
Solutions for Chapter 4	105

5. INTEGERS AND DIVISIBILITY

5.1 The System of Integers	109
5.2 The Euclidean Algorithm	114
5.3 The One-Way Euclidean Algorithm	117
5.4 Prime Numbers	119
5.5 Generating Prime Numbers	122
Exercises for Chapter 5	126
Solutions for Chapter 5	126

6. LOGS AND EXPONENTIALS	
6.1 Powers	129
6.2 What Do We Mean by 2^x ?	131
6.3 Logs	132
6.4 Powers and Logs on Calculators	138
7. TRIGONOMETRIC FUNCTIONS	
7.1 Elementary Trigonometry	143
7.2 Special Angles	147
7.3 Sum and Difference of Angles	148
7.4 Completing Triangles	151
7.5 Rotations in the x-y Plane	155
7.6 Radian Measure	158
7.7 The Functions $\sin x$, $\cos x$ and $\tan x$	159
8. COMPLEX NUMBERS	
8.1 If It Doesn't Exist – Invent It	165
8.2 The Field of Complex Numbers	168
8.3 Geometrical Interpretation	170
8.4 Conjugates	172
8.5 De Moivre's Theorem	174
8.6 n 'th Roots of Complex Numbers	176
8.7 The Geometry of Complex Numbers	180
8.8 Application of Complex Numbers to Alternating Current	182
Exercises for Chapter 8	190
Solutions for Chapter 8	194

PART B: POLYNOMIALS

9. POLYNOMIALS

9.1 Definition of a Polynomial	205
9.2 Degree of a Polynomial	207
9.3 Addition and Multiplication of a Polynomial	208
9.4 Division and Remainder	210
9.5 Greatest Common Divisors	212
9.6 Roots of Polynomials	216
9.7 Sum and Product of Roots	219
9.8 Zeros of a Polynomial	220
9.9 Multiplicities of Zeros	221
9.10 Solving Systems of Polynomial Equations in One Variable	223
9.11 Real and Complex Zeros	226
Exercises for Chapter 9	231
Solutions for Chapter 9	235

10. SOLVING POLYNOMIAL EQUATIONS

10.1 Quadratic Equations	245
10.2 Solving Quadratic Equations	247
10.3 Solving Cubic Equations	251
10.4 Solving Quartic Equations	254
10.5 Solving Quintic Equations and Beyond	257
10.6 Solving Two Polynomials in Two Variables ...	263
Exercises for Chapter 10	266
Solutions for Chapter 10	267

11. \mathbb{Z}_2 POLYNOMIALS AND CRYPTOGRAPHY

11.1 \mathbb{Z}_2 The Fool's Field	277
11.2 Irreducible \mathbb{Z}_2 Polynomials	280
11.3 Complex \mathbb{Z}_2 Numbers	283
11.4 Extensions of \mathbb{Z}_2 and Cryptography	287

PART C: GROUP THEORY

12. INTRODUCTION TO GROUPS

12.1 Symmetry	291
12.2 Symmetry Groups	294
12.3 Multiplication Tables of Symmetry Groups	296
12.4 Applications to Mattress Turning	298
12.5 The Dihedral Group of Order 8	301
12.6 Galois and His Groups	306
12.7 Applications of Groups	310
Exercises for Chapter 12	319
Solutions for Chapter 12	323

13. GROUP AXIOMS AND PROPERTIES

13.1 Abstract Groups and the Group Axioms	329
13.2 Examples of Groups	332
13.3 Basic Properties of Groups	333
13.4 Powers	325
13.5 More Properties of Groups	337
13.6 Cyclic Groups	339
Exercises for Chapter 13	342
Solutions for Chapter 13	348

14. DIHEDRAL GROUPS

14.1 Subgroups	357
14.2 Cosets	358
14.3 Lagrange's Theorem	361
14.4 Euler's Theorem	362
14.5 Generators and Relations	364
14.6 Dihedral Groups	366
14.7 Dihedral Arithmetic	367
14.8 Groups of Order $2p$	370
14.9 The Thirty Nine Steps	372
Exercises for Chapter 14	376
Solutions for Chapter 14	381