

Second Edition

INTRODUCTORY MODERN ALGEBRA

A Historical Approach

SAUL STAHL

$$x_1x_2 + x_3x_4$$

$$x \pm y\sqrt{-2}$$

$$x^{p^v} - x$$

WILEY

Introductory Modern Algebra

Introductory Modern Algebra A Historical Approach

Second Edition

Saul Stahl

Department of Mathematics
University of Kansas
Lawrence, KS

WILEY

Copyright © 2013 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representation or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print, however, may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Stahl, Saul.

Introductory modern algebra : a historical approach / Saul Stahl, Department of Mathematics, University of Kansas. — Second edition.

p. cm.

Includes bibliographical references and index.

ISBN 978-0-470-87616-9 (cloth)

1. Algebra, Abstract. I. Title.

QA162.S73 2013

512'.02—dc23

2013018928

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

Preface	ix
1 The Early History	1
1.1 The Breakthrough	1
2 Complex Numbers	9
2.1 Rational Functions of Complex Numbers	9
2.2 Complex Roots	17
2.3 Solvability by Radicals I	23
2.4 Ruler-and-Compass Constructibility	26
2.5 Orders of Roots of Unity	36
2.6 The Existence of Complex Numbers*	38
3 Solutions of Equations	45
3.1 The Cubic Formula	45
3.2 Solvability by Radicals II	49
3.3 Other Types of Solutions*	50
4 Modular Arithmetic	57
4.1 Modular Addition, Subtraction, and Multiplication	57
4.2 The Euclidean Algorithm and Modular Inverses	62
4.3 Radicals in Modular Arithmetic*	70
4.4 The Fundamental Theorem of Arithmetic*	71
5 The Binomial Theorem and Modular Powers	75
5.1 The Binomial Theorem	75
5.2 Fermat's Theorem and Modular Exponents	85
5.3 The Multinomial Theorem*	90
5.4 The Euler φ -Function*	93

* Optional

6	Polynomials over a Field	99
6.1	Fields and Their Polynomials	99
6.2	The Factorization of Polynomials	107
6.3	The Euclidean Algorithm for Polynomials	113
6.4	Elementary Symmetric Polynomials*	120
6.5	Lagrange's Solution of the Quartic Equation*	125
7	Galois Fields	131
7.1	Galois's Construction of His Fields	131
7.2	The Galois Polynomial	139
7.3	The Primitive Element Theorem	144
7.4	On the Variety of Galois Fields*	147
8	Permutations	155
8.1	Permuting the Variables of a Function I	155
8.2	Permutations	158
8.3	Permuting the Variables of a Function II	166
8.4	The Parity of a Permutation	169
9	Groups	183
9.1	Permutation Groups	183
9.2	Abstract Groups	192
9.3	Isomorphisms of Groups and Orders of Elements	199
9.4	Subgroups and Their Orders	206
9.5	Cyclic Groups and Subgroups	215
9.6	Cayley's Theorem	218
10	Quotient Groups and Their Uses	225
10.1	Quotient Groups	225
10.2	Group Homomorphisms	234
10.3	The Rigorous Construction of Fields	240
10.4	Galois Groups and Resolvability of Equations	253
11	Topics in Elementary Group Theory	261
11.1	The Direct Product of Groups	261
11.2	More Classifications	265

12	Number Theory	273
12.1	Pythagorean Triples	273
12.2	Sums of Two Squares	278
12.3	Quadratic Reciprocity	285
12.4	The Gaussian Integers	294
12.5	Eulerian Integers and Others	304
12.6	What Is the Essence of Primality?	310
13	The Arithmetic of Ideals	317
13.1	Preliminaries	317
13.2	Integers of a Quadratic Field	319
13.3	Ideals	322
13.4	Cancellation of Ideals	337
13.5	Norms of Ideals	341
13.6	Prime Ideals and Unique Factorization	343
13.7	Constructing Prime Ideals	347
14	Abstract Rings	355
14.1	Rings	355
14.2	Ideals	358
14.3	Domains	361
14.4	Quotients of Rings	367
A	Excerpts: Al-Khwarizmi	377
B	Excerpts: Cardano	383
C	Excerpts: Abel	389
D	Excerpts: Galois	395
E	Excerpts: Cayley	401
F	Mathematical Induction	405

G	Logic, Predicates, Sets, and Functions	413
G.1	Truth Tables	413
G.2	Modeling Implication	415
G.3	Predicates and Their Negation	418
G.4	Two Applications	419
G.5	Sets	421
G.6	Functions	422
	Biographies	427
	Bibliography	431
	Solutions to Selected Exercises	433
	Index	444
	Notation	448

Preface

IT IS COMMON KNOWLEDGE amongst mathematicians that much of modern algebra has its roots in the issue of solvability of equations by radicals. The purpose of this text is to provide the undergraduate mathematics majors and the prospective high school mathematics teachers with a one-semester introduction to modern algebra that keeps this relationship in view at all times.

Most modern algebra texts employ an axiomatic strategy that begins with abstract groups and ends with fields, ignoring the issue of solvability of equations by radicals. By contrast, we follow the paper trail from the Renaissance solution of the cubic equation to Galois's description of his ideas. In the process, all the important concepts are encountered, each in a well-motivated manner.

One year of calculus provides all the information required for the comprehension of all the topics in this text, which has many distinguishing features:

Historical development. Students would prefer to know the real reasons that underlie the creation of the mathematical structures they encounter. They also enjoy being placed in direct contact with the works of the prime movers of mathematics. This text tries to bring them as close to the source as possible.

Finite groups and fields are rooted in some specific investigations of Lagrange, Gauss, Cauchy, Abel, and Galois regarding the solvability of equations by radicals. This text makes these connections explicit. Gauss's proof of the constructibility of the regular 17-sided polygon is incorporated into the development, and the argument given is merely a paraphrase of that which appears in the *Disquisitiones*. Similarly, the proof of Theorem 8.10 is just a reorganization of that given by Abel in his paper on the quintic equation. The construction of Galois fields is accomplished in the form of a commentary on the opening pages of Galois's paper *On the Theory of Numbers* which are quoted verbatim in the text. Several important documents are also included as appendices. A considerable amount of historical discussion is integrated into the development of the subject matter.

Cohesive organization. The historical development of the material allows for very little flexibility. Each chapter elucidates some of the preceding material and motivates ideas

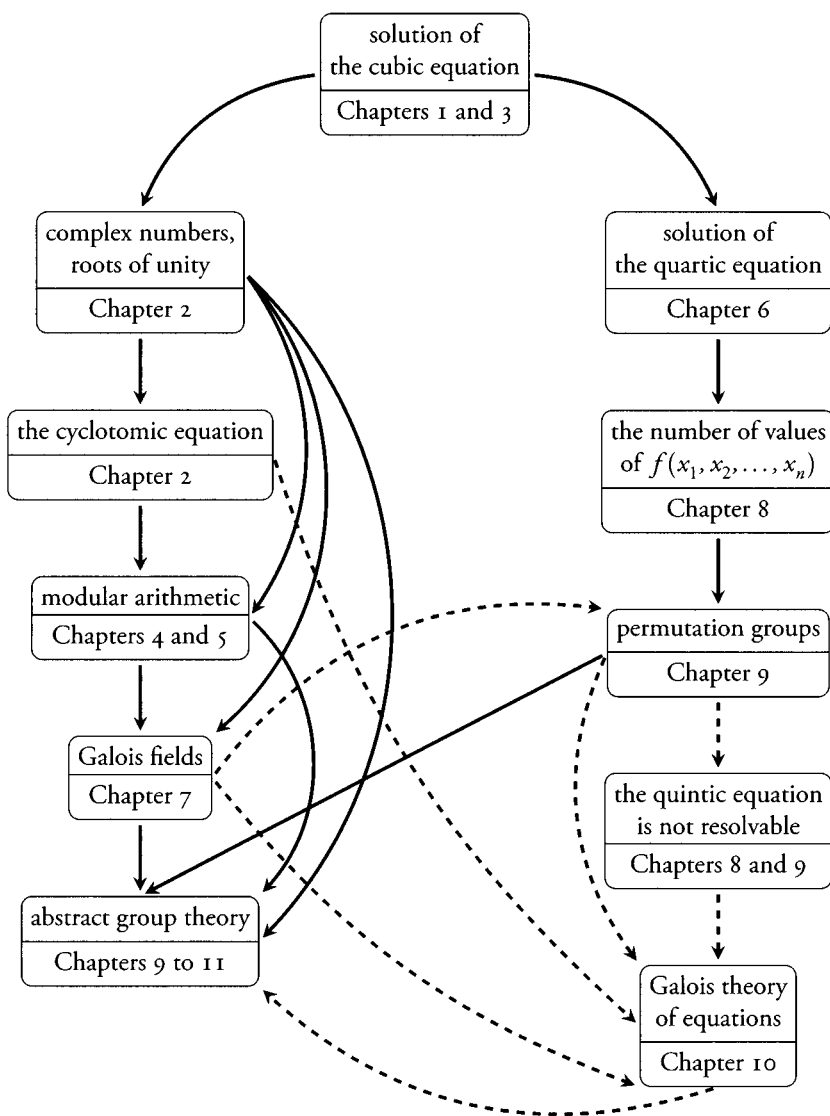


Figure 0.1 The genesis of the theory of finite groups.

that come later. The advantage of this approach is the same as that of good motivation in general: it aids comprehension by providing the students with a framework in which to

fit the various concepts they encounter. A one semester course can be constructed on the basis of Sections 1.1, 2.1–5, 3.1–2, 4.1–2, 5.1–2, 6.1–3, 7.1–3, 8.1–4, 9.1–5, & 10.1.

Figure 0.1 illustrates the author's perception of the evolution of abstract group theory (ignoring all the geometric and much of the number-theoretic contributions). The number in the right of each box denotes the chapter in which this topic is discussed. Solid arrows correspond to connections that are treated in some depth whereas those that are displayed by dashed arrows are touched on only informally.

Chapters 1 to 3 are dedicated to the formalization of the notion of solvability by radicals. Gauss's proof of the constructibility of the regular 17-sided polygon is the capstone theorem of this part of the course. Field theory is developed in Chapters 4 to 7. The Primitive Element Theorem of Section 7.3 serves as a watershed: it unifies many of the important concepts that precede it and motivates the notion of cyclicity that comes later. Group theory is developed in Chapters 8 to 10. This begins with an explanation of the relevance of permutations to solvability by radicals, goes on to the discussion of permutation groups and abstract groups, and concludes with the description of quotient groups. Chapter 11 is meant to acquaint the students with some of the standard tools of elementary group theory.

Exercises. Each section is followed by its own set of exercises. These range from the routine to the challenging. Each chapter has an additional set of easy review exercises added to remind the students of the chapter's main points. There are over 1,000 of these end-of-section and chapter review exercises. The answers to selected odd exercises appear at the end of the book. Most chapters are also accompanied by a collection of supplementary computer and/or mathematical projects. Some of the latter involve open questions.

Additional pedagogy. Each chapter begins with an introduction and concludes with a summary. The purposes of both the introduction and the summary are to provide the student with an overview of the chapter, and sometimes to comment on its relationship to the previous chapters. The examples are integrated into the exposition and they are highlighted by a notation in the margin. Each chapter's new terms are listed, together with the pages on which they are defined, following that chapter's summary.

Instructor's manual. An instructor's manual is available. It contains the answers to all the end of section and chapter review exercises. Some suggested homework assignments and tests are also included.

Acknowledgments

First and foremost I wish to acknowledge the substantial contributions made by Fred Galvin who rooted out several inaccuracies in the original development, improved and/or corrected many of the proofs, both in the text and the manual, suggested new exercises, and used the manuscript in his class. Thanks are also due to Todd Eisworth, Andy Magid and Phil Montgomery who also class tested the manuscript and made valuable suggestions as well as to my colleague Paul J. McCarthy who was kind enough to lend me both an ear and his algebraic expertise. It remains to gratefully acknowledge the efforts of Jessica Downey, Steve Quigley, Rosalyn Farkas, and Lisa Van Horn of John Wiley & Sons on behalf of this book.

June 1996

Preface to the Second Edition

Surprisingly, it turned out that the historical approach could be used to teach ring theory as well. The point of departure is the Theorem of Pythagoras, viewed as a diophantine equation. Chapter 12 begins there and goes on to Fermat's characterization of primes that are the sum of two square integers. From there we go on to quadratic reciprocity and the Gaussian integers. The question of Gaussian primes is natural and some attention is given to variant number systems with radicals $\sqrt{-2}$ or $\sqrt{-3}$. The chapter ends with a discussion of Kummer's decision to redefine the notion of primality.

Quadratic fields, quadratic integers, and ideals are defined and the arithmetic of ideals is explored in Chapter 13. It is shown that the arithmetic of ideals does possess the unique factorization property. Finally, Chapter 14 discusses rings and ideals in the abstract manner of today.

The author's understanding of the low level algebraic number theory in Chapter 13 comes from reading one of Keith Conrad's many expository monographs. The solutions to the selected exercises in Chapters 13 and 14 were derived by Grant Serio and are included with his permission. Katie Ballentine, Annika Denkert, and Mark Hunacek debugged portions of the manuscript, which was expertly typeset by Lon Mitchell.

June 2013

Saul Stahl
Lawrence, Kansas

Chapter 1



THE EARLY HISTORY

THIS CHAPTER CONTAINS an informal account of the early history of the issue of solvability of equations of degrees one, two, and three in a single unknown. The formulas that provide the solutions lead in a natural way to the discussion of the origins of complex numbers. We also take this opportunity to review some well-known information about the quadratic equation.

1.1 The Breakthrough

There is a general agreement among historians of mathematics that modern mathematics came into being in the mid sixteenth century when the combined efforts of the Italian mathematicians Scipione del Ferro, Niccolò Tartaglia, and Gerolamo Cardano produced a formula for the solution of cubic equations. For the first time ever west European mathematicians succeeded in cracking a problem whose solution eluded the best mathematical minds of antiquity. Archimedes, one of the greatest mathematicians, scientists, and engineers of all times, had solved some cubic equations in terms of the intersections of a suitable parabola and hyperbola. Omar Khayyam, one of the most prominent of the Arab mathematicians and poets, also expended much effort on his geometrical solutions of special cases of the cubic equation but could not find the general formula. However, the significance of this accomplishment of the Renaissance mathematicians is not limited to the difficulty of the problem that was solved. We shall try to show how the issues raised by this solution eventually led to the creation of modern algebra and the discovery of mathematical landscapes that were undreamt of, even by such imaginative investigators as Archimedes and Khayyam.

The interest in algebraic equations goes back to the beginnings of written history. The *Rhind Mathematical Papyrus*, found in Egypt circa 1856 is a copy of a list of mathematical problems compiled some time during the second half of the nineteenth century BCE, or

possibly even earlier. The twenty-fourth of these problems reads: “A quantity and its $1/7$ added become 19. What is the quantity?” In other words, what is the solution to the equation

$$x + \frac{x}{7} = 19?$$

The method employed by the scribe has come to be known as the *method of false position*. He replaces the unknown by 7 and observes that

$$7 + \frac{7}{7} = 8.$$

From this he concludes that the correct answer is obtained upon multiplying the first guess of 7 by $19/8$:

$$x = 7 \cdot \frac{19}{8} = \frac{133}{8}.$$

Interestingly enough, the scribe does double check his solution by substituting it into the original problem and verifying that

$$\frac{133}{8} + \frac{133/8}{7} = 19.$$

We will not discuss the merits and limitations of the method of false position except to note that the idea of obtaining a correct solution to an equation by starting out with a possibly false guess and then modifying that guess has been refined into powerful techniques for finding numerical solutions, one of which will be described in Section 3.3. We do, however, wish to point out that the general *first-degree equation* is today defined as

$$ax + b = 0, \quad a \neq 0,$$

and that the rules of algebra yield

$$x = -\frac{b}{a}$$

as its unique solution.

The Mesopotamian mathematicians of that time could solve much more intricate equations, and had in fact already developed techniques for solving what we nowadays call quadratic equations. These techniques employed the geometrical method of “completing the square.” The Greeks, Indians, and Arabs all were aware of this method, having either derived them independently or perhaps learnt them from their predecessors and/or neighbors. In the ninth century the Persian mathematician al-Khwarizmi (عَبْدَ اللَّهِ مُحَمَّدُ بْنُ)

المؤسى الخوارزمي wrote the book *Hisab al-jabr w'al-muqa-balah* (الكتاب المختصر في حساب الجبر والمقابلة) in which he carefully explained a compendium of algebraic techniques learnt from several past civilizations. The clarity of his exposition won both him and his book immortality in that the portion *al-jabr* of the title evolved into the word *algebra*, and the author's name is the source of the word *algorithm*. An excerpt from this book expounding the solution to the quadratic equation

$$x^2 + 10x = 39$$

appears in Appendix A. The modern solution of the quadratic also relies on the completion of the square. The general *quadratic equation* has the form

$$ax^2 + bx + c = 0, \quad a \neq 0, \quad (1.1)$$

and its solutions are found by first factoring out the coefficient a and then completing the rest to a perfect square. Thus, we first divide Equation 1.1 through by a to obtain the equation

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0. \quad (1.2)$$

The left side of Equation 1.2 is then transformed to a near perfect square:

$$\begin{aligned} x^2 + \frac{b}{a}x + \frac{c}{a} &= \left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a} \\ &= \left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}. \end{aligned}$$

The original quadratic equation has thus been transformed to

$$\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2} = 0$$

or

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2} \quad \text{or} \quad x + \frac{b}{2a} = \frac{\pm\sqrt{b^2 - 4ac}}{2a}.$$

Hence the general quadratic equation, Equation 1.1, has the two solutions

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{and} \quad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

It is clear that if a , b , and c are real numbers, then these two solutions are real and distinct if $b^2 - 4ac > 0$, they are real and identical if $b^2 - 4ac = 0$, and they are imaginary and distinct if $b^2 - 4ac < 0$. Another important fact to bear in mind (Exercises 1.1.5 and 1.1.6) is that

$$x_1 + x_2 = -\frac{b}{a} \quad \text{and} \quad x_1 x_2 = \frac{c}{a},$$

from which it follows that it is easy to construct a quadratic equation whose roots are prespecified. As we will have several occasions to refer to these identities later, they are stated as a proposition whose proof is relegated to Exercise 1.1.14.

Proposition 1.3 For any two numbers r and s the quadratic equation

$$x^2 - (r + s)x + rs = 0$$

has r and s as its roots.

It is reasonable at this point to raise the ante and ask for a formula that will yield the solution of the general *cubic equation*

$$ax^3 + bx^2 + cx + d = 0. \quad (1.4)$$

There are indications that the Mesopotamians already tried to systematize the search for solutions of cubic equations, and we know for a fact that the Greeks attempted the same. As was mentioned above, the final breakthrough did not occur until the middle of the sixteenth century when it was shown that a solution of the equation

$$x^3 + px + q = 0$$

is given by the expression

$$x = \sqrt[3]{-q/2 + \sqrt{q^2/4 + p^3/27}} - \sqrt[3]{q/2 + \sqrt{q^2/4 + p^3/27}}. \quad (1.5)$$

As we shall see later, very little additional work is required to pass from this formula on to a formula for the general cubic equation (Equation 1.4), and so Formula 1.5 can be considered as the crucial step, even though it does not yield the solution to the most general cubic equation.

In analogy with the ancient solutions of the quadratic, this solution was obtained by a geometrical process of completing the cube. Excerpts from Cardano's description of

the solution are contained in Appendix B. A modern derivation of this formula appears in Chapter 3, and we restrict ourselves here to the examination of some instructive applications of Formula 1.5. Surprisingly, this formula raises some very interesting questions.

Consider the cubic equation $x^3 - 1 = 0$. Here $p = 0$ and $q = -1$, and so Formula 1.5 yields

$$x = \sqrt[3]{1/2 + \sqrt{1/4 + 0}} - \sqrt[3]{-1/2 + \sqrt{1/4 + 0}} = \sqrt[3]{1/2 + 1/2} - \sqrt[3]{-1/2 + 1/2} = 1,$$

which is as it should be. However, for the equation $x^3 + 6x - 20 = 0$, which Cardano uses as an illustration in his *Ars Magna*, the same formula yields the solution

$$x = \sqrt[3]{10 + \sqrt{100 + 8}} - \sqrt[3]{-10 + \sqrt{100 + 8}} = \sqrt[3]{\sqrt{108} + 10} - \sqrt[3]{\sqrt{108} - 10}.$$

It can be easily verified with the aid of a calculator that the above solution agrees with 2 to at least eight decimal places, and the mathematical verification that the agreement is absolute is left to Exercise 1.1.1. Our purpose in presenting this example was to draw attention to the possibility that Formula 1.5 may present a correct solution in an unnecessarily complicated form. This obfuscation becomes much more disturbing in the case of the equation $x^3 - 15x - 4 = 0$, treated by Rafael Bombelli in his *Algebra* (1572). Formula 1.5 yields the solution

$$x = \sqrt[3]{2 + \sqrt{-121}} - \sqrt[3]{-2 + \sqrt{-121}}. \quad (1.6)$$

However, it is easily verified by inspection that $x = 4$ is also a solution of this cubic, and, since

$$x^3 - 15x - 4 = (x - 4)(x^2 + 4x + 1),$$

two more solutions of the original equation are obtained by solving the quadratic

$$x^2 + 4x + 1 = 0.$$

As the solutions of this quadratic are $-2 \pm \sqrt{3}$, we are faced with the question of which of the three numbers 4 or $-2 \pm \sqrt{3}$ is disguised as Expression 1.6. Moreover, this complicated expression involves square roots of negative numbers, in other words, imaginary quantities, whereas 4 and $-2 \pm \sqrt{3}$ are all real numbers. This apparent paradox was

resolved by Bombelli who simplified Expression 1.6 by setting

$$\sqrt[3]{2 \pm \sqrt{-121}} = a \pm b\sqrt{-1},$$

cubing both sides and deriving $a = 2$ and $b = 1$ from the resulting simultaneous equations. Rather than exhibit the details of his solution we simply point out that indeed

$$\begin{aligned} (2 + \sqrt{-1})^3 &= 2^3 + 3 \cdot 2^2 \sqrt{-1} + 3 \cdot 2 \cdot (\sqrt{-1})^2 + (\sqrt{-1})^3 \\ &= 8 + 12\sqrt{-1} - 6 - \sqrt{-1} \\ &= 2 + 11\sqrt{-1} = 2 + \sqrt{-121} \end{aligned}$$

and similarly

$$(-2 + \sqrt{-1})^3 = -2 + \sqrt{-121}.$$

Consequently,

$$\sqrt[3]{2 + \sqrt{-121}} - \sqrt[3]{-2 + \sqrt{-121}} = 2 + \sqrt{-1} - (-2 + \sqrt{-1}) = 4.$$

Thus, users of the cubic formula ignore the so-called *imaginary numbers* at their peril. Such prejudices come at the cost of losing some real solutions to real equations. This is further borne out by the innocent-looking equation $x^3 - 3x = 0$. Formula 1.5 yields the solution

$$x = \sqrt[3]{\sqrt{-1}} - \sqrt[3]{\sqrt{-1}},$$

and even if one is very skeptical about the existence of imaginary quantities it is very tempting to believe in them just long enough for the above radicals to cancel out and to yield the root $x = 0$, which we know to be correct.

The solution to the cubic equation is the context within which imaginary numbers were first discussed by mathematicians. Cardano toyed with them and then rejected them as useless. Bombelli gave them more credence, but it wasn't until about 200 years later that the work of Leonhard Euler, Pierre-Simon de Laplace, and later that of Carl Friedrich Gauss, Augustin-Louis Cauchy, and Niels Abel turned the complex number system, consisting of both the real and imaginary numbers, into an indispensable tool for mathematical researchers.

The Ferro-Tartaglia-Cardano Formula 1.5 suffers from a serious deficiency. This formula yields at most one solution for any cubic equation, even when such an equation

is known to have three distinct real roots, as is the case for $x^3 - x = 0$ whose roots are 0 and ± 1 . In view of the fact that the quadratic formula of Equation 1.1 does succeed in incorporating all the solutions into one expression it would not seem unreasonable to expect the same of the cubic counterpart. As we shall see in the next chapter, the *complex numbers* will enable us to find just such an expression.

Exercises 1.1

1. Prove that $\sqrt[3]{\sqrt{108} + 10} - \sqrt[3]{\sqrt{108} - 10} = 2$.
2. Prove that $\sqrt{28 - 10\sqrt{3}} - \sqrt{7 - 4\sqrt{3}} = 3$.
3. Solve the equation $3x^2 - 2x - 2 = 0$.
4. Solve the equation $x^4 - 3x^2 + 2 = 0$.

If r and s are the roots of the quadratic equation $ax^2 + bx + c = 0$, prove the identities in Exercises 1.1.5 to 1.1.7.

5. $r + s = -b/a$
7. $r^2 + s^2 = (b^2 - 2ac)/a^2$
6. $rs = c/a$

If r and s are the roots of the quadratic equation $ax^2 + bx + c = 0$, rewrite the expressions in Exercises 1.1.8 to 1.1.13 in terms of a , b , and c . Wherever necessary, you may assume that the denominators are not zero.

8. $1/r + 1/s$
10. $r^2s + rs^2$
12. $1/r^2 + 1/s^2$
9. $r^3 + s^3$
11. $(r - s)^2$
13. $1/r^2s + 1/rs^2$

14. Prove Proposition 1.3.
15. If r and s are the roots of the equation $x^2 + px + q = 0$, what is the quadratic equation whose roots are $r + s$ and rs ?
16. If $r, s \neq 0$ are the roots of the equation $x^2 + px + q = 0$, what is the quadratic equation whose roots are $1/r$ and $1/s$?
17. For what real values of α are the roots of the equation $x^2 + \alpha x + \alpha = 0$ real?
18. For what values of m will the equation $x^2 - 2x(1 + 3m) + (3 + 2m) = 0$ have equal roots?

Chapter Summary

This introductory chapter was used to briefly review the solutions of the first- and second-degree equations in a single unknown. The history of the solution of the cubic equation was also discussed and the relationship of this formula to the complex number system was examined.

Chapter Review Exercises

Mark the following true or false.

1. Every real number is the solution of some equation.
2. Every pair of real numbers is the solution set of some quadratic equation.
3. Every equation has at least one solution.

New Terms

cubic equation, 4

first-degree equation, 2

method of false position, 2

quadratic equation, 3

Chapter 2



COMPLEX NUMBERS

THROUGHOUT HISTORY, the introduction of new numbers has been greeted with considerable resistance on the part of mathematicians. Legend has it that the discoverer of irrational numbers was rewarded by being drowned by his fellow Greeks. Be that as it may, the fact is that these numbers have been tagged with the pejorative label of *irrational*, a word which, when used in nonmathematical contexts, has definite derogatory connotations. The same, of course, applies to the *negative* numbers. The *imaginary* numbers have been cursed with what is arguably the worst nomenclature in mathematics. Given the considerable difficulties that the average students face in learning the rigorous discipline of mathematics, can they be blamed for balking at having to contend with quantities that mathematicians themselves admit are imaginary?

The best way to overcome people's resistance to a new concept is to convince them of its utility. Accordingly, it will be shown that the widening of our field of operations to include the complex numbers greatly enhances the power of the Ferro-Tartaglia-Cardano cubic formula. Next, the complex numbers will be used to solve some ruler-and-compass construction problems of plane geometry. Only in this chapter's last section will the issue of the existence of the complex numbers be addressed.

2.1 Rational Functions of Complex Numbers

Just as was done by the mathematicians of the eighteenth and nineteenth centuries, we assume here the existence of a number i which has the property that $i^2 = -1$.

The rigorous proof of i 's existence is deferred to Section 2.6. In the meantime, the number i is to be treated just like a variable, with the sole additional stipulation that whenever i^2 occurs within an algebraic expression, it can be replaced by -1 . A *complex number* is an expression of the form $a + bi$ where a and b are any real numbers. When

$b = 0$ such a number is called an *imaginary number* and when $b = 0$ it is said to be *real*. These complex numbers can be added and subtracted as polynomials. Thus,

$$(5 - 3i) + (-2 + 5i) = 5 - 3i - 2 + 5i = 3 + 2i,$$

$$(5 - 3i) - (-2 + 5i) = 5 - 3i + 2 - 5i = 7 - 8i.$$

The multiplication of complex numbers also resembles that of polynomials, except that each occurrence of i^2 is replaced by -1 . Thus,

$$\begin{aligned}(5 - 3i)(-2 + 5i) &= -10 + 25i + 6i - 15i^2 \\ &= -10 + 31i - 15(-1) \\ &= -10 + 31i + 15 = 5 + 31i.\end{aligned}$$

The division of complex numbers mimics the well-known process of rationalizing denominators. Thus,

$$\frac{5 - 3i}{-2 + 5i} = \frac{5 - 3i}{-2 + 5i} \cdot \frac{-2 - 5i}{-2 - 5i} = \frac{-10 - 25i + 6i - 15}{(-2)^2 - (5i)^2} = \frac{-25 - 19i}{4 + 25} = \frac{-25}{29} - \frac{19}{29}i.$$

Surprisingly, all of these arithmetical operations can be given very interesting visual, or geometric, interpretations. To accomplish this, we represent each complex number $a + bi$ by the point (a, b) of the Cartesian plane. The point (a, b) is called the *Cartesian representation* of the complex number $a + bi$. Given two complex numbers $a + bi$ and $c + di$, let their Cartesian representations be $P = (a, b)$ and $Q = (c, d)$ (Figure 2.1). Their sum

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

is represented by the point $R = (a + c, b + d)$. However,

$$\text{slope of } PR = \frac{(b + d) - b}{(a + c) - a} = \frac{d}{c} = \text{slope of } OQ$$

and

$$\text{slope of } QR = \frac{(b + d) - d}{(a + c) - c} = \frac{b}{a} = \text{slope of } OP.$$

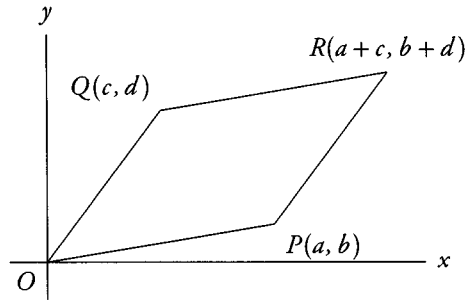


Figure 2.1 Complex addition

Consequently, $PR \parallel OQ$ and $QR \parallel OP$ and so $OPRQ$ is a parallelogram. Thus we see that the addition of complex numbers resembles that of vectors. These considerations are summarized as follows.

Proposition 2.1 Let O denote the origin of the Cartesian plane and let P and Q be the Cartesian representations of the complex numbers $a + bi$ and $c + di$, respectively. If the sum of the two complex numbers is represented by the point R , then the quadrilateral $OPRQ$ is a parallelogram.

To give the multiplication of complex numbers a visual interpretation, it is convenient to begin by establishing some conventions. In the sequel, the general complex number $a + bi$ will frequently be abbreviated as z . If either a or b is 0, it is omitted from $a + bi$. Thus, $3 + 0i = 3$ and $0 - 5i = -5i$.

Let $P = (a, b)$ be the Cartesian representation of the complex number $z = a + bi$ (Figure 2.2). The *modulus* of z , denoted by $|z|$, is the length of the line segment OP . In other words $|a + bi| = \sqrt{a^2 + b^2}$. Thus, for example,

$$|2 + 3i| = \sqrt{2^2 + 3^2} = 13,$$

$$|3 - 4i| = \sqrt{3^2 + (-4)^2} = 5,$$

$$|-2i| = \sqrt{0^2 + (-2)^2} = 2.$$

It is clear that the modulus of the real number $a + 0i$ is just its absolute value. Thus the modulus should be regarded as the extension of the notion of absolute value to the complex numbers. The *argument* of $z = a + bi$, denoted $\arg(z)$, is the counterclockwise angle from the positive x -axis to the ray OP where P is the Cartesian representation of z . As can be seen in Figure 2.3, the arguments of 3 , $1 + i$, $3i$, -2 , $-2 - 2i$, and

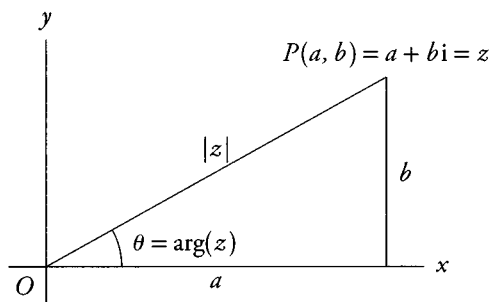


Figure 2.2 The argument and the modulus

$3 - 3i$ are $0, \pi/4, \pi/2, \pi, 5\pi/4$, and $7\pi/4$, respectively. For our purposes here it is convenient to identify angles whose measures differ by the full angle of 2π . Thus it will be convenient sometimes to regard 1 as having argument 2π or 4π rather than 0. The reasons for this will become clear after we have discussed the geometrical interpretation of the multiplication of complex numbers.

The argument θ of the general complex number $z = a + bi$ is easily computed (Figure 2.2) from the relation $\tan \theta = b/a$, but the quadrant in which z lies must be taken into account. Thus

$$\arg(1 + i) = \arctan \frac{1}{1} = \frac{\pi}{4},$$

whereas

$$\arg(-2 - 2i) = \pi + \arctan \frac{-2}{-2} = \frac{5\pi}{4}.$$

Observe that if the complex number $z = a + bi$ has argument θ , then, by Figure 2.2,

$$z = a + bi = |z| \left(\frac{a}{|z|} + \frac{b}{|z|}i \right) = |z|(\cos \theta + i \sin \theta).$$

We refer to $|z|(\cos \theta + i \sin \theta)$ as the *polar form* of z . For example, the complex numbers $1 + i$, 5 , i , and $-2i$ have polar forms $\sqrt{2}(\cos \pi/4 + i \sin \pi/4)$, $5(\cos 0 + i \sin 0)$, $\cos \pi/2 + i \sin \pi/2$, and $2(\cos 3\pi/2 + i \sin 3\pi/2)$, respectively. On the other hand, the number $3 + 4i$ has polar form $5(\cos \alpha + i \sin \alpha)$ where $\alpha = \arctan 4/3 \approx 53.13^\circ$.

Just as the addition of complex numbers has a geometrical interpretation in terms of Cartesian coordinates, so their multiplication can be easily visualized in terms of their polar forms. Let the complex numbers z and w be given in terms of their polar forms $z = |z|(\cos \theta + i \sin \theta)$ and $w = |w|(\cos \varphi + i \sin \varphi)$.

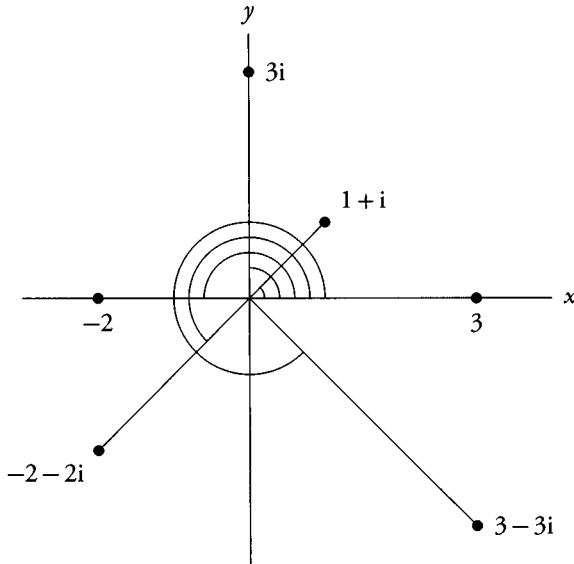


Figure 2.3 Some complex numbers

The trigonometric formulas for the functions of the sums of two angles yield

$$\begin{aligned}
 zw &= |z||w|(\cos \theta + i \sin \theta)(\cos \varphi + i \sin \varphi) \\
 &= |z||w|[(\cos \theta \cos \varphi - \sin \theta \sin \varphi) + i(\cos \theta \sin \varphi + \sin \theta \cos \varphi)] \\
 &= |z||w|[\cos(\theta + \varphi) + i \sin(\theta + \varphi)].
 \end{aligned}$$

Thus, the product zw has polar form $|z||w|[\cos(\theta + \varphi) + i \sin(\theta + \varphi)]$. Since it follows from Figure 2.2 that every complex number is completely determined by its argument and modulus, we conclude that $\arg(zw) = \theta + \varphi$ and $|zw| = |z||w|$. Hence, we have proved the following theorem.

Theorem 2.2 Let z and w be any two complex numbers. Then $\arg(zw) = \arg(z) + \arg(w)$ and $|zw| = |z||w|$.

If $z = i$ and $w = 1 + i$, then $zw = i(1 + i) = -1 + i$ and so

$$\arg(z) + \arg(w) = \frac{\pi}{2} + \frac{\pi}{4} = \frac{3\pi}{4} = \arg(zw)$$

and $|z||w| = 1 \cdot \sqrt{2} = \sqrt{2} = |zw|$.

Angles whose measures differ by integer multiples of 2π are considered to be identical. Thus, the number i has all the following as its arguments:

$$\dots, \frac{-7\pi}{2}, \frac{-3\pi}{2}, \frac{\pi}{2}, \frac{5\pi}{2}, \frac{9\pi}{2}, \dots$$

This is necessitated by such observations as the fact that

$$\pi/2 = \arg(i) = \arg[(-1)(-i)] = \arg(-1) + \arg(-i) = \pi + 3\pi/2 = 5\pi/2.$$

This fact, which appears to be a nuisance at this point will in fact turn out to be very useful in the next section. Some more light will be shed on this in Section 9.4. Theorem 2.2 is commonly referred to as the *argument principle*. It has many interesting and useful consequences. For example, it clearly implies that $\arg(z^2) = 2\arg(z)$ and $|z^2| = |z|^2$. Similarly, $\arg(z^3) = 3\arg(z)$ and $|z^3| = |z|^3$. In fact, a simple induction procedure yields the following observation.

Corollary 2.3 If z is any nonzero complex number and k is any positive integer, then $\arg(z^k) = k\arg(z)$ and $|z^k| = |z|^k$.

This observation can be put to good use in computing large powers of complex numbers. Consider the problem of computing $(1+i)^{100}$. By Corollary 2.3,

$$\arg[(1+i)^{100}] = 100\arg(1+i) = 100 \cdot (\pi/4) = 25\pi = \pi$$

and $|(1+i)^{100}| = |1+i|^{100} = (\sqrt{2})^{100} = 2^{50}$. Hence, $(1+i)^{100} = 2^{50}(\cos \pi + i \sin \pi) = -2^{50}$.

Corollary 2.3 also holds for nonpositive exponents if we define $z^0 = 1$ for all z and $z^{-k} = (1/z)^k$ for $z \neq 0$ and $k = 1, 2, 3, \dots$

The proof of this fact is relegated to Exercise 2.1.29. Exercise 2.1.28 calls for proving that integer powers of complex numbers obey the same rules as do the more familiar powers of real numbers, to wit, $z^m z^n = z^{m+n}$ and $(z^m)^n = z^{mn}$.

If $z = a + bi$ is any complex number, where a and b are real, we define $\bar{z}$, the *conjugate* of z , to be $a - bi$. Thus, $\overline{-2 + 3i} = -2 - 3i$ and $\overline{3 - 4i} = 3 + 4i$.

Theorem 2.4 If $z = a + bi$ is any complex number,

- (a) z and $\bar{z}$ are symmetrical with respect to the x -axis;
- (b) $z\bar{z} = |z|^2$; $\arg(z\bar{z}) = \arg(z) + \arg(\bar{z})$;
- (c) $\overline{z + w} = \bar{z} + \bar{w}$; $\overline{zw} = \bar{z}\bar{w}$; $\bar{z}^{-1} = \overline{z^{-1}}$;
- (d) $\bar{z} = z$ if and only if z is real.

Proof. See Exercise 2.1.27. ■

Exercises 2.1

Find the argument and modulus of each of the complex numbers in Exercises 2.1.1 to 2.1.4

- 1. $2 + 3i$
- 2. $3 - 2i$
- 3. $-3 - 4i$
- 4. $-1 + 7i$

Express the complex quantities in Exercises 2.1.5 to 2.1.21 in the form $a + bi$, where a and b are real numbers.

- 5. $(2 + 3i) + (5 - i)$
- 6. $(17 - 3i) + (2 + 3i)$
- 7. $(2 + 3i)(5 - i)$
- 8. $(17 - 3i) - (2 + 3i)$
- 9. $(2 + 3i)(5 - i)$
- 10. $(17 - 3i)(2 + 3i)$
- 11. $(2 + 3i)/(5 - i)$
- 12. $(17 - 3i)/(2 + 3i)$
- 13. $(\sqrt{3} + 5i)/(2 - \sqrt{3}i)$
- 14. $(a + bi)/(a - bi) - (a - bi)/(a + bi)$
- 15. $(2 - i)^2/(1 + i)$
- 16. $(1 + i)^4$
- 17. $(1 - 2i)^4$
- 18. $(1 - i)^{63}$
- 19. $i^{4 \cdot 321}$
- 20. $((1 - i)/(1 + i))^{127}$
- 21. i^{4n+3} (n is an integer)

Solve the equations in Exercises 2.1.22 to 2.1.25 for z and w :

- 22. $(1 + 2i)z + 5 = 0$
- 23. $(1 + i)z + 5i = \frac{z}{1-i} - 2$
- 24. $iz - w = 1 + i$ and $(1 + i)z + iw = 1$
- 25. $(1 - i)z + iw = i$ and $2z - (2 + i)w = 1$
- 26. Prove that if z and w are any two complex numbers, then $|z + w| \leq |z| + |w|$.

27. Prove the following:

(a) Theorem 2.4(a)

(c) Theorem 2.4(c)

(b) Theorem 2.4(b)

(d) Theorem 2.4(d)

(e) If a , b , c , and d are any real numbers, prove that z is a root of the equation $ax^3 + bx^2 + cx + d = 0$ if and only if $\bar{z}$ is also a root of the same equation.

28. Prove that if z is any complex number and m and n are any integers, then $z^m z^n = z^{m+n}$ and $(z^m)^n = z^{mn}$.

29. Prove that Corollary 2.3 holds for every integer k .

30. Prove that the three distinct complex numbers z_1 , z_2 , and z_3 are collinear if and only if there exists a real number λ such that $z_2 = (1 - \lambda)z_1 + \lambda z_3$. (Hint: examine the expression $(z_2 - z_1)/(z_3 - z_1)$.)

31. Prove that if z and w are two complex numbers, then the distance between them equals $|z - w|$.

32. Prove that the midpoint of the line segment joining the complex numbers z and w is $(z + w)/2$.

33. Prove that the four complex numbers z_1 , z_2 , z_3 , and z_4 lie on either a common straight line or a common circle if and only if the number

$$\frac{(z_1 - z_3)/(z_1 - z_2)}{(z_4 - z_3)/(z_4 - z_2)}$$

is real.

34. Let z_1 , z_2 , z_3 , and z_4 be four complex numbers such that $|z_1| = |z_2| = |z_3| = |z_4| = 1$. Prove that z_1 , z_2 , z_3 , and z_4 form a rectangle if and only if $z_1 + z_2 + z_3 + z_4 = 0$.

35. Prove that the center of gravity of the triangle whose vertices are the complex numbers z_1 , z_2 , and z_3 is $(z_1 + z_2 + z_3)/3$. (Hint: recall that the center of gravity of a triangle coincides with the intersection of its three medians.)

36. Prove that if $|\xi| = 1$, then there is a real number b such that $(1 + \xi)/(1 - \xi) = bi$.

37. Prove that if $z = a + bi$, where a and b are real, then $(|a| + |b|)/\sqrt{2} \leq |z| \leq |a| + |b|$.